514.2

Strategic Roadmap Development

SANS | GIAC CERTIFICATIONS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

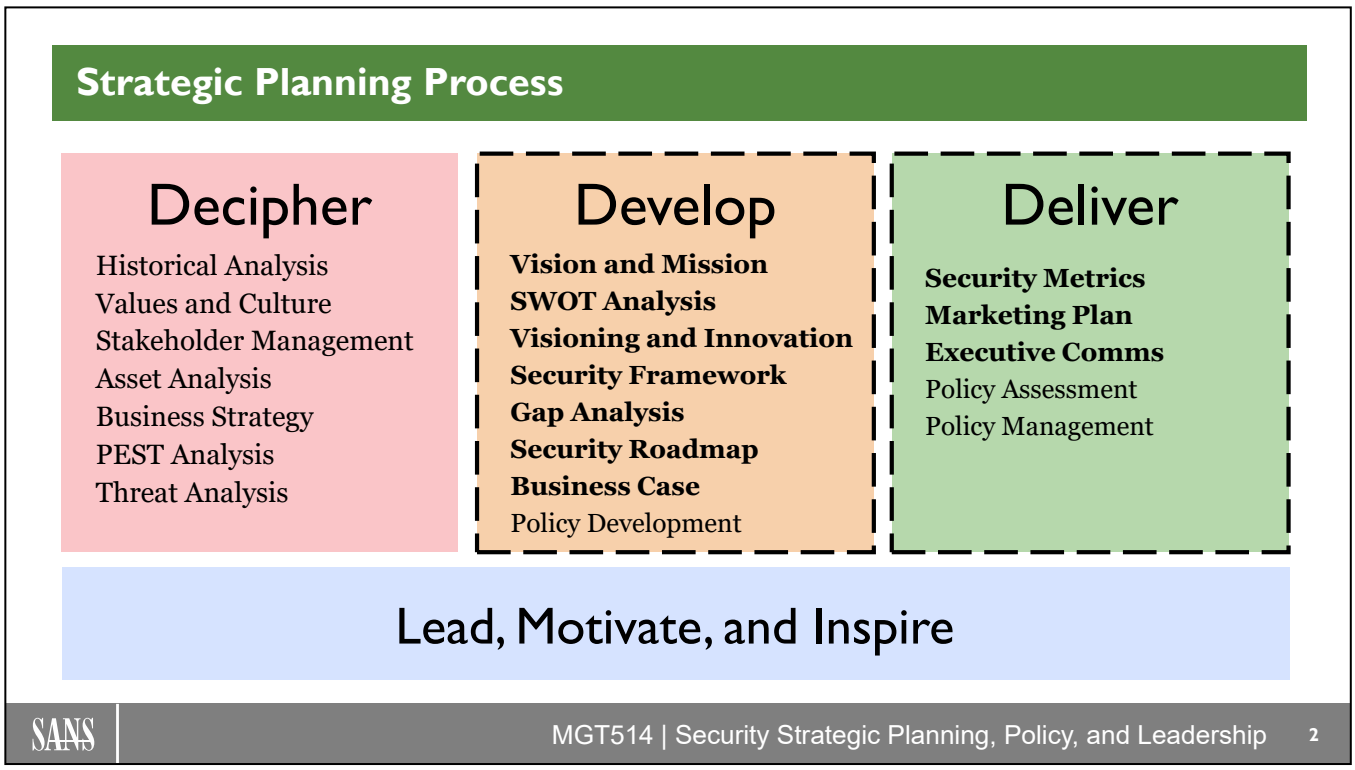
All reference links are operational in the browser-based delivery of the electronic workbook.

MGT514.2 | Security Strategic Planning, Policy, and Leadership

SANS

Strategic Roadmap Development

This page intentionally left blank.



In the previous section, we covered topics and tools for understanding the business and the threat landscape in the Decipher phase. In this section, we'll expand the discussion to cover other phases of the strategic planning process, specifically the Develop and Deliver phases.

In Section 2, we cover the topics that are in bold on the slide above.

Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- ***Define Current State***
  - Vision and Mission
    - Lab #1: Mission Statement
  - SWOT Analysis
    - Lab #2: SWOT Exercise
- Develop the Plan
  - Visioning and Innovation
  - Security Framework
  - Security Roadmap
    - Gap Analysis
    - Lab #3: Roadmap Development
  - Business Case Development
- Deliver the Program
  - Security Metrics Program
  - Marketing and Exec Communications

This page intentionally left blank.

How To Define Current State

1) Figure out why the organization exists and what it's trying to achieve
   - Understand the vision and mission

2) Understand where you are strong and weak
   - Analyze your Strengths, Weaknesses, Opportunities, and Threats (SWOT)

Analyzing your current state is key to developing an effective strategic plan. An understanding of your current state comes from:

1) Understanding what the organization is trying to achieve
   - Knowing the organization's vision and mission

2) Understanding where you are strong and weak
   - By analyzing your Strengths, Weaknesses, Opportunities, and Threats (SWOT), you can determine where you should focus and invest

Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Define Current State
  - ***Vision and Mission***
    - Lab #1: Mission Statement
  - SWOT Analysis
    - Lab #2: SWOT Exercise
- Develop the Plan
  - Visioning and Innovation
  - Security Framework
  - Security Roadmap
    - Gap Analysis
    - Lab #3: Roadmap Development
  - Business Case Development
- Deliver the Program
  - Security Metrics Program
  - Marketing and Exec Communications

This page intentionally left blank.

Vision and Mission

- Goals of this section:
  - Understand the difference between a vision and mission
  - Determine how security can support the organization's vision and mission
  - Learn how to develop a security team mission statement that aligns with organizational goals

In this section, we cover the differences between vision and mission statements, review examples of good and bad statements, and learn how to develop a security team mission statement that supports organizational goals.

What Is the Difference Between a Vision and Mission Statement?

- Vision statement:
  - Represents "why" the company exists
  - The noble purpose
  - The seemingly unachievable goal
- Mission statement:
  - Represents "what" the company does today
  - What we are and what we do today

Vision and mission statements are commonly confused.

Think of the vision as what the organization wants to be in the longer term—its goals and aspirations for the future. The vision represents "why" the company exists and its noble, seemingly unreachable goal.

The mission, on the other hand, is what the organization does today—its current purpose, what it does, and for whom. The mission should focus on the here and now.

Purpose of a Vision Statement

- Vision statement
  - What the company wants to be when it "grows up"
  - Focuses on where you will be at the end of the strategic planning horizon
- Why is the vision important for strategic planning?
  - Serves as the guiding light for the team
- Let's look at some well-known vision statements
  - Discuss how they help us understand the goals of the business

A vision statement is, by nature, aspirational. It is not about what the company is, but what it hopes to become in the future. It typically is a stretch for the company and includes ideals to achieve. A vision statement should focus on what the organization can achieve by the end of the strategic planning horizon.

In Stephen Covey's book, *The 7 Habits of Highly Effective People,* he describes beginning with the end in mind: "When we begin with the end in mind, we have a personal direction to guide our daily activities, without which we will accomplish little toward our own goals.[1] Beginning with the end in mind is part of the process of personal leadership, taking control of our own lives." With this concept in mind, the vision can serve as a guiding light for the team as it tries to accomplish the end goal.

Security teams should also have "stretch" goals that may seem difficult to achieve. In this section, we look at some well-known vision statements and discuss how they help us understand the goals of the business and inform the work of the security team.

Reference:
[1] https://www.stephencovey.com/7habits/7habits.php

Is This a Good Vision Statement?

- "Inspire the World, Create the Future"

This new vision reflects Samsung Electronics' commitment to inspiring its communities by leveraging Samsung's three key strengths: "New Technology," "Innovative Products," and "Creative Solutions"—and to promoting new value for Samsung's core networks—Industry, Partners, and Employees. Through these efforts, Samsung hopes to contribute to a better world and a richer experience for all.

As part of this vision, Samsung has mapped out a specific plan of reaching $400 billion in revenue and becoming one of the world's top five brands. To this end, Samsung has also established three strategic approaches in its management: "Creativity," "Partnership," and "Talent."

Samsung is excited about the future. As we build on our previous accomplishments, we look forward to exploring new territories, including health, medicine, and biotechnology. Samsung is committed to being a creative leader in new markets and becoming a truly No. 1 business going forward.

The vision statement of Samsung Electronics, a large multinational corporation with product lines that include smartphones, television sets, chip fabrication, shipbuilding, construction, and insurance, is "Inspire the World, Create the Future."[1] With such a diverse array of businesses, it is not a surprise that the company's vision statement is extremely broad. It wants to utilize "New Technology," "Innovative Products," and "Creative Solutions" that will ultimately help the company be "a creative leader in new markets and a truly No. 1 business going forward."

However, this vision statement is extremely vague. There is no clear and concrete end state and no clear aspiration that can drive the organization forward.

Reference:
[1] https://www.samsung.com/levant/aboutsamsung.html/aboutsamsung

DRIVE the Vision

- Directional
  - Does it help you decide what activities to pursue?
- Relevant
  - Takes into account the organization's history, current state, culture, and values, thereby making it visible. Is it authentic and true to the organization?
- Inspirational
  - Inspires people to commit to a shared goal. Captures the hearts and minds. Do you find it personally inspiring?
- Vivid
  - Clear and concrete. Describes the future in a way that is easy to imagine. Would it be greeted with enthusiasm by most people in the organization?
- Extremely Bold
  - Audacious. Does it feel potentially unattainable?

Good vision statements have the following five characteristics:

- **Directional:** It is obvious where the organization is going—so obvious, in fact, that a vision statement that is directional can even help people decide which activities to pursue on a daily basis.
- **Relevant**: Takes into account the organization's history, current state, culture, and values, thereby ensuring that the direction is not only visible but also authentic and true to the organization.
- **Inspirational:** Inspires people to commit to a shared goal. Captures the hearts and minds. Individuals find the vision personally inspiring.
- **Vivid**: Clear with enough detail to make it concrete. Describes the future in a way that is easy to imagine.
- **Extremely bold:** Seems almost impossible to achieve and audacious.

Space Vision

> "I believe that this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to the Earth."

On May 25, 1961, U.S. President John F. Kennedy announced before a special joint session of Congress the ambitious goal of sending an American to the moon and back by the end of the decade. This vision had all five elements of successful vision statements:

- **Directional:** It was extremely clear what needed to be accomplished and by when.
- **Relevant:** During the Cold War, the United States was in a race for technological dominance with the Soviet Union. At the time, the Soviet Union had already had successful space missions, and the perception was that the United States was falling behind.
- **Inspirational:** Shortly after this announcement, JFK was touring NASA headquarters for the first time. He introduced himself to a janitor who was sweeping the floor and asked him what he did at NASA. The janitor replied, "I'm helping put a man on the moon." The simple announcement helped inspire many people in the country.
- **Vivid:** It was very easy to imagine. Not just sending a man to the moon but "returning him safely to the Earth."
- **Extremely Bold:** This type of space travel had never been accomplished and, at the time, was considered an audacious goal.

Eight years later, on July 20, 1969, the mission was accomplished.

In 1980, Bill Gates's vision was "A computer on every desk and in every home." At the time, the concept of a computer in every home was almost inconceivable. Incumbents like IBM scoffed at the idea.

What Microsoft didn't articulate publicly was its actual vision: "A computer on every desk and in every home *running Microsoft software*." Microsoft ruthlessly achieved this vision with Office, Internet Explorer, and of course, Windows. One could argue that once Microsoft achieved its vision from the 1980s, that's when the company started to falter. What is its rallying cry now?

But, this vision guided Microsoft for decades because it was:

- **Directional:** Microsoft created compelling software and partnerships to help make this vision a reality.
- **Relevant:** It wasn't obvious to many in the early 1980s, but decreasing technology costs coupled with the convenience of having the power of a computer on your desk made this vision especially relevant for the times.
- **Inspirational:** Everyone could buy into this shared goal.
- **Vivid:** It was very simple and easy to imagine.
- **Extremely Bold:** Given that only large corporations or the extremely rich could afford a computer, this vision was definitely a bold proclamation at the time.

Vision Statement Keyword Examples

- Aspires
- Preeminent
- Strives to achieve
- Sustains growth
- Best
- Center of excellence
- Inspires
- Top performing
- Fulfilling
- Innovative
- Excellent

If you spend an hour surfing the web looking at various vision statements, you will see certain words appear again and again. The majority of the time, these organizations have gone through a process to determine what "they want to be when they grow up." If your vision statement does not have any of the words on the slide, or words similar to these, you might want to look it over again and see if it truly expresses vision.

Purpose of a Mission Statement

- Mission statement
  - Describes what we are and what we do today
- Why is the mission important for strategic planning?
  - As we set goals, priorities, and intermediate steps, the mission statement reminds us of our purpose and helps keep us on track
- Let's look at some corporate mission statements for various industries
  - Discuss how they might impact security

A mission statement describes what we are and what the organization does today. As we set goals, priorities, and intermediate steps, the mission statement reminds us of our purpose and that helps keep us on track. When we look at a new task, we can determine whether or not expending resources on it will help us achieve our goals. If not, we should elect to defer or delete that task.

According to Karen Scharf, "A well-defined mission statement will keep you from spreading yourself too thin. As entrepreneurs, we're constantly coming up with new ideas and inspiration. However, not all of our ideas are the perfect fit for our business. But once your mission statement is created, you'll have a barometer to measure each new idea by. You'll know that every new project you take on is one that is propelling your business forward."[1]

Individuals also use mission statements to help guide their efforts toward setting and achieving personal goals.

Reference:
[1] http://ezinearticles.com/?Small-Business-Marketing---Making-Use-of-a-Mission-Statement&id=4401845

Is This a Good Mission Statement?

- State of North Carolina

  The Enterprise Security and Risk Management Office (ESRMO) provides leadership in the development, delivery, and maintenance of an information security and risk management program that safeguards the state's information assets and the supporting infrastructure against unauthorized use, disclosure, modification, damage or loss.

  The ESRMO supports a comprehensive statewide program that encompasses information security implementation, monitoring, threat and vulnerability management, cyber incident management, and enterprise business continuity management.

  The ESRMO works with executive branch agencies to help them comply with legal and regulatory requirements, the statewide technical architecture, policies, industry best practices, and other requirements.

  Working with state agencies, federal and local governments, citizens and private sector businesses, ESRMO helps to manage risk to support secure and sustainable information technology services to meet the needs of our citizens.

This mission statement is from the security department at the State of North Carolina.[1] It says that the department is responsible for security and risk management and describes what the department does to support the state and executive branch while working with state agencies, federal and local governments, citizens, and the private sector. However, this extremely verbose mission statement does not map back to the larger organizational mission of which security is a part.

The most successful security team mission statements will be informed by the mission of the larger organization and show a direct link to how it helps meet corporate goals. To see how the mission of the larger organization can impact the security team, let's review some real-world corporate mission statements.

Reference:
[1] http://it.nc.gov/statewide-resources/cybersecurity-and-risk-management

Retail Industry Mission (1)

"To provide outstanding service, every day, one customer at a time."

This mission statement is for Nordstrom, which is an upscale clothing retailer in the United States headquartered in Seattle, Washington. Nordstrom, from its founding, was focused primarily on providing outstanding customer service. According to John W. Nordstrom, the founder, this is best exemplified by the famous "tire story."[1] Mr. Nordstrom was at a store in Fairbanks, Alaska, meeting with the sales and management team when they saw a gentleman rolling a tire into the store so that he could return it. Obviously, an upscale clothing retailer does not sell car tires, but Mr. Nordstrom advised the manager to let the salesclerk handle the situation to see what he would do. It turns out that there was a tire shop at that location before Nordstrom opened. The gentleman was obviously confused, but the salesclerk happily volunteered to take the tire back without a receipt and gave him $25. To this day, that tire is nailed to a wall at the back of the store as a reminder about providing outstanding customer service and empowering employees to make their own decisions and "do the right thing."

In this type of environment, what can security do to be more successful? It is likely that, in an organization so focused on customer service, this would permeate the internal culture, also. This means that security, instead of being the group that simply says "no," would have to find ways to partner with internal stakeholders and provide solutions that empower employees to make more secure decisions.

Reference:
[1] https://www.gsb.stanford.edu/faculty-research/working-papers/what-are-your-signature-stories

Retail Industry Mission (2)

"To save people money
so they can live better."

This mission statement is for Walmart, which operates a chain of discount retail stores and warehouses around the world. In the retail industry, where profit margins are already very thin, Walmart is extremely focused on maintaining low cost.

In this type of environment, what can security do to be more successful? Security activities would ideally be tied to cost-saving measures with strong justification for any security spend.

Higher Education Mission

"We strive to create knowledge, to open the minds of students to that knowledge, and to enable students to take the best advantage of their educational opportunities.

We seek to identify and to remove restraints on students' full participation so that individuals may explore their capabilities and interests and may develop their full intellectual and human potential."

Harvard College is the undergraduate school at Harvard University. Its mission is to "remove restraints on students' full participation so that individuals may explore their capabilities and interests and may develop their full intellectual and human potential."[1] Like many educational institutions, Harvard wants to remove barriers to learning. Doing so can be a challenge for security, which typically wants to introduce additional controls.

In this type of environment, what can security do to be more successful? Instead of saying "no," security will have to find ways to minimize risk while still providing an open environment for faculty, students, and staff to share information and further their academic goals.

Reference:
[1] http://compact.org/resource-posts/the-mission-of-harvard-college (link no longer active)

Mission Statement Keyword Examples

- Branding
- Consistency
- Core
- Detail
- Dominant player
- Enterprising
- Innovation
- Inspire
- Profit
- Quality
- Research
- Service
- Social responsibility
- Opportunity

These are examples of some words you will commonly see in a mission statement.

Example of Long but Clear Mission Goals

- NSA's Information Assurance Directorate (IAD)
  - "IAD is responsible for NSA's defensive mission and is widely acknowledged for leading innovative security solutions."

    IAD delivers mission enhancing cybersecurity technologies, products, and services that enable customers and clients to secure their networks; trusted engineering solutions that provide customers with flexible, timely and risk-sensitive security solutions; as well as traditional IA engineering and fielded solutions support.

    Information Assurance Operations which include remote and deployed operational groups, with 24X7 integrated support as needed that protect critical national security networks.

    Fusion, Analysis, and Mitigations teams that analyze and characterize large volumes of IA data, using an automated and persistent approach to identify vulnerabilities, and develop solutions to mitigate them.

    Training and security awareness support.

    The Key Management Infrastructure that provisions end cryptographic units.

The Information Assurance Directorate (IAD) within the National Security Agency (NSA) of the United States is responsible for protecting and defending national security information and systems. Its website makes it clear that the IAD provides five things:[1]

1. Security products, services, and engineering
2. Security operations to protect critical national security networks
3. Vulnerability management including analysis and mitigation
4. Training and security awareness
5. The key management infrastructure

If only the security goals at most enterprises were so straightforward. Unlike the IAD, most security departments have to struggle with creating a mission that resonates with the rest of the organization and the business.

Reference:
[1] https://www.nsa.gov/ia/ia_at_nsa (link no longer active)

Departmental Mission Statements

- Must be aligned with the mission of the larger org
  - Useful for keeping the security team focused
- If a departmental mission statement exists:
  - Review and update it if necessary
  - Organizations change over time and your goal from 10 years ago may not be the same today
- If you need to update or create one from scratch:
  - Focus on the purpose of the organization
  - Be realistic—does it represent what you are now?
  - Keep it short and focused—can you tweet it?

If you have an existing mission statement for your department, then review and update it as necessary. It is simply reality; organizations change over time and your purpose of 10 years ago may not be the same purpose today. Apple used to be primarily focused on selling endpoint computers and some servers. Then, a tremendous part of the company's income was the iPod, then later the iPhone, and then iPad. The strategic planning process should generate a number of questions or issues to help evaluate the mission statement. For example, one of the questions should be: "Is our mission statement focused on satisfying customer needs rather than being focused on the product?"

If your security department does not have a mission statement, then you will need to develop one. The key is to tell the world the purpose and the focus of your organization. Keep in mind the vision statement is what you aspire to become; the mission statement is what you are. Work hard to reduce this statement to the minimum number of words. People are unlikely to read anything that runs on. Additionally, it is easier for your employees to remember a short, pithy mission statement. Be sure to try out your mission statement on several people and ask them to state what it means in their own words. Sometimes, we write things that look correct to us, but other people interpret the words differently than we would think.

Creating a Mission Statement for the Security Department

- A good mission statement guides our decisions
- Consider what IT or security can do to:
  - Protect the company (prevent failure)
  - Enable the business (ensure success)
- If you're stuck, you can use this as a starter:
  - "To advance *company's* mission by securing, defending, and monitoring our *most important assets*."
- Or follow the four-step process for creating a mission statement
  - From nonprofithub.org

A good mission statement helps guide the decisions that the security department needs to make. How can the security team better protect the company and enable the business? By crafting a simple, meaningful mission statement that resonates with key stakeholders in the company, you will be that much closer to making security relevant and understandable to non-IT and non-security leaders.

It can be very difficult to create a mission statement. If you're stuck, you can use the following template as a starting point:

"To advance the <*insert company's mission*> by securing, defending, and monitoring <*insert company's most important assets*>"

Alternatively, you can follow the "Step-by-step Exercise for Creating a Mission Statement" developed by nonprofithub.org to create a mission statement for your security team.[1] That is what we will do in the rest of this section.

Reference:
[1] https://web.archive.org/web/20150421002621/https://nonprofithub.org/wp-content/themes/nonprofithub/img/landing-pages/mission/nonprofithub-missionstatement.pdf

PharmaCo Introduction

- Paul Williams was recently hired as CISO at PharmaCo
  - Asked by his boss, the CFO, to create a strategic plan for improving security
    - This includes developing relationships, identifying business value, centralizing security
    - Ultimately executing on the strategic objectives and leading change throughout the organization
- PharmaCo is a large pharmaceutical company
  - Created breakthrough drugs that have helped millions lead longer, healthier lives
  - $25 billion in revenue
  - 70,000 employees around the world
  - Increasing competition: Pressure to create new drugs
  - Decentralized operations: R&D centers and manufacturing around the world
  - Recent evidence of intrusions: Leaked documents containing sensitive product development plans

Your good friend, Paul Williams, works for a large pharmaceutical company, PharmaCo. He was recently hired as the CISO and has been asked by his boss, the CFO, to create a strategic plan to improve the effectiveness of the organization's security operations. This includes developing relationships, identifying business value, centralizing security, and anything else he uncovers that needs improvement. At your monthly dinner, he expresses that he's having a hard time understanding the organization and how to structure his approach to deliver what the CFO has asked for. Paul looks to you for guidance and counsel on how he can get his arms around the enormity of this task, and prioritize efforts for a strategic plan.

PharmaCo is a large multinational organization with $25 billion in annual revenue, 70,000 employees, and offices across six continents. At the heart of PharmaCo's culture is a heavy focus on innovation and R&D. In fact, it has created breakthrough drugs for the treatment of numerous medical ailments and has helped millions of people lead longer, healthier lives. Due to its success, competitors are constantly looking to take market share. There is increasing pressure to speed up the creation of new drugs in the face of this competition and the increasingly difficult regulatory environment. At PharmaCo, each individual business unit runs its own research and development and operations functions. As a result, security is currently decentralized across business units. Historically, this has not posed a problem, but recently there has been evidence of intrusions. Sensitive documents about product development plans have been found in the hands of outsiders.

You can clearly see from Paul's conversation with you that he has a big job ahead, but the good news from your point of view is that he has a high-level understanding of PharmaCo, and more importantly, he has a stated objective from the CFO to create a plan to improve security for the organization.

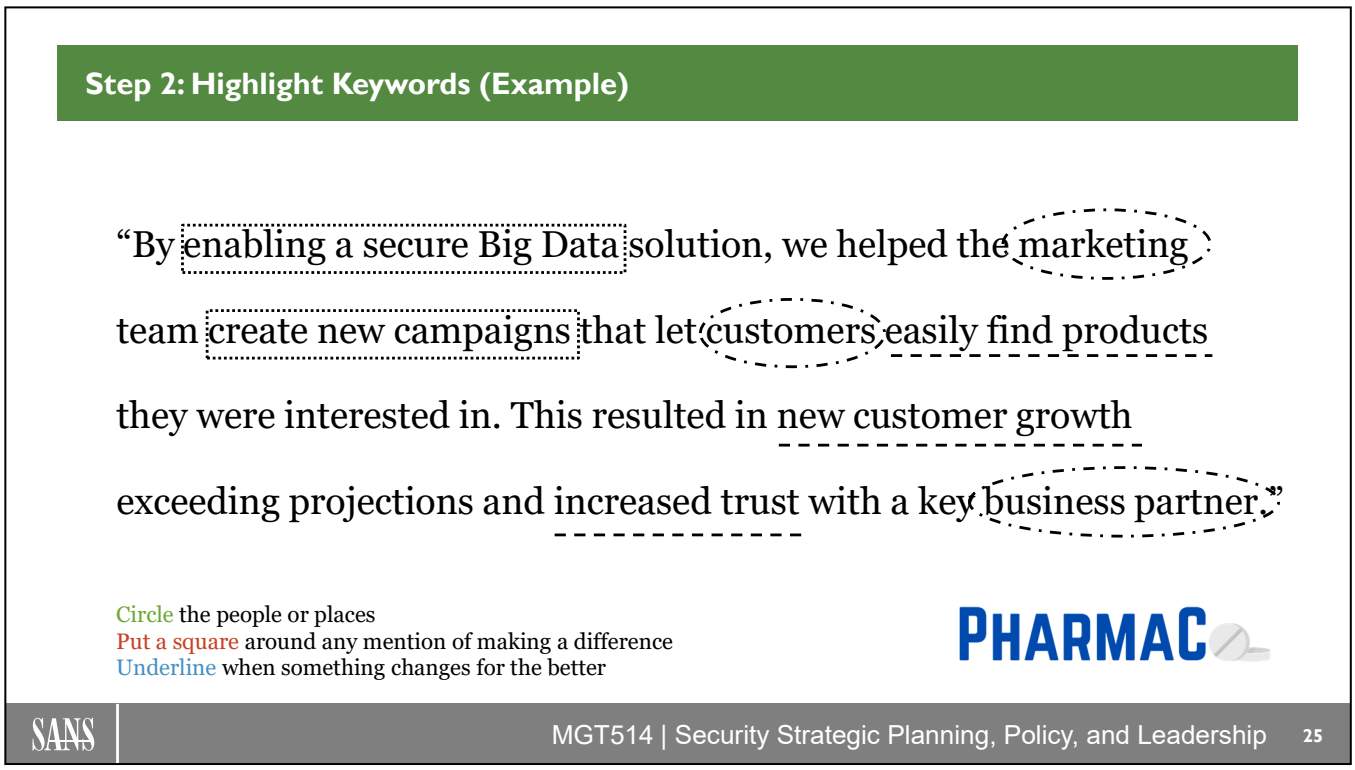
Step 1: Tell a Story (Example)

"By enabling a secure Big Data solution, we helped the marketing team create new campaigns that let customers easily find products they were interested in. This resulted in new customer growth exceeding projections and increased trust with a key business partner."

PHARMAC

In Step 1, tell a story about a time the security team did something meaningful. It doesn't have to be something that changed the world, saved a life, or prevented a dramatic attack. It can be something as simple as a time when another team really appreciated the output or service the security team provided. If you are stuck trying to think about a good story, ask yourself, "What *does* it look like when we're doing our best work?" This question can prompt some good ideas. If you still can't think of a good story, then just make one up. Ask yourself, "What *would* it look like when we're doing our best work?"

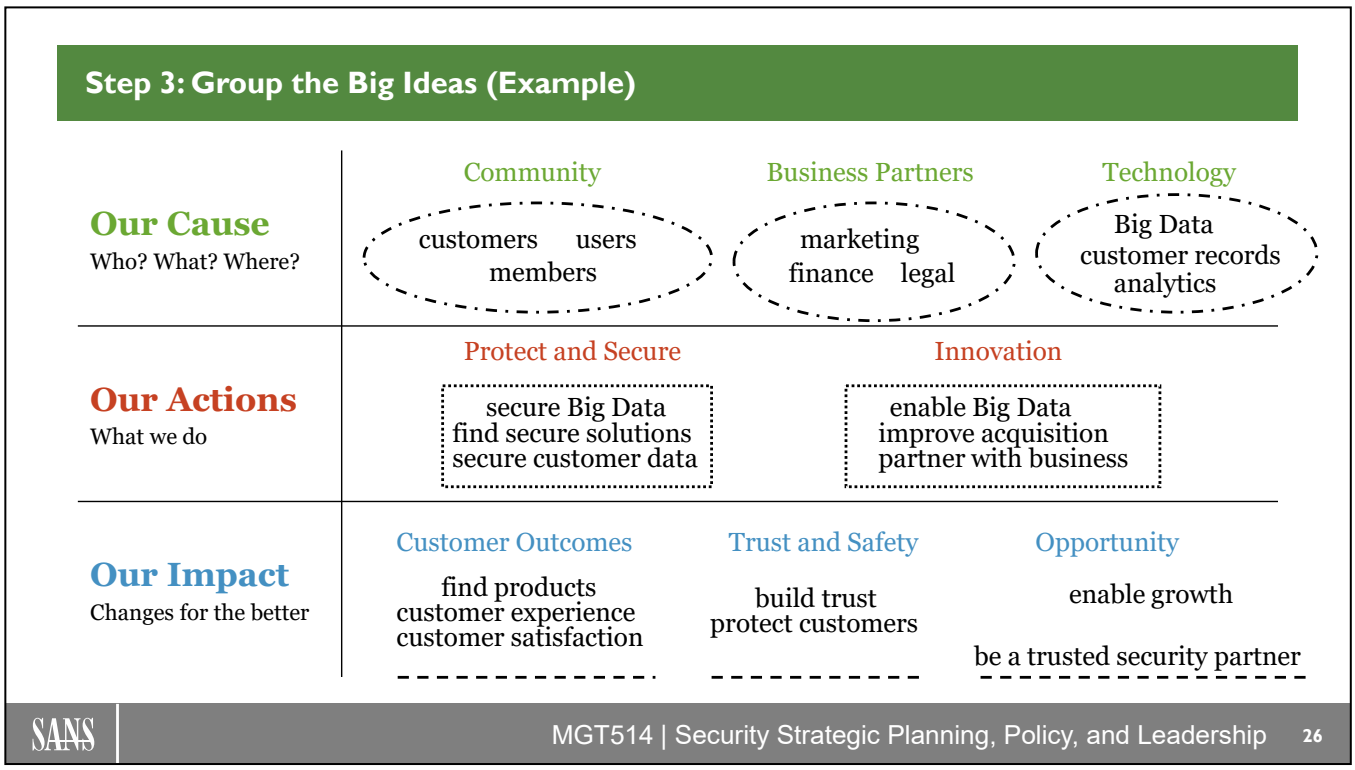
The story on this slide is about the security team working with marketing. Oftentimes, the marketing team deploys a new website or campaign and, after the fact if at all, seeks security team input. This is because security is often seen as a blocker that will slow down the marketing team. Instead, by working proactively to enable a secure Big Data solution, the security team was able to help the marketing team meet their goals and become a more trusted partner.



In Step 2, simply highlight the keywords in your story:

- **Circle** any time you mention a specific person or place.
- **Draw** a square around items that describe your team making a difference or taking action.
- **Underline** anything in the story when something changes for the better.

This step helps you identify the important parts of your story so that you can share them with your team.



In Step 3, group the big ideas. Start by writing down all the highlighted words and phrases from Step 2. Patterns and similarities will develop naturally. Group them together like we've done on this slide.

In some cases, your story might lead you to write down other ideas that preceded the story itself. For example, how did you know that Big Data was a potential solution? You may have partnered with someone in marketing and discovered that they were looking for solutions to improve the outcomes of their campaigns. As a result, "partner with business" and "improve acquisition" are listed under "Innovation" on the slide.

As another example, you may know that securing the Big Data platform and corresponding customer information has to be done before deploying the solution. This is why these items are listed under "Protect and Secure" on the slide.

The section titled "Our Impact" is arguably the most important one. Succinctly categorizing the overall change for the better is what truly matters to your stakeholders. This is why "customer experience" and "customer satisfaction" are listed under "Customer Outcomes."

Grouping and naming the common ideas in your story helps identify themes that you can use to craft your actual mission statement.

Step 4: Draft the Mission (Example)

"Through security and innovation, we promote trust and safety with our customers."

"We provide business partners with secure tools to improve customer outcomes."

"Help customers maintain control of their data by enabling and securing innovative business solutions."

PHARMAC

In Step 4, you actually create the mission statement. Creating a mission statement can be a difficult process. However, by telling a story, identifying keywords, and grouping the big ideas, you can draft a mission statement that will resonate with your key business partners.

Here, we have taken the previously circled, squared, and underlined words and crafted three sample mission statements.

Lab 2.1: Creating a Mission Statement (1)

Estimated Time: 20 Minutes

- Goal of this exercise
  - Draft a mission statement for Paul's security department at PharmaCo
- Step 1: Tell a story
  - Review the story about a time the PharmaCo security team did something meaningful
- Step 2: Highlight keywords
  - Circle the people or places
  - Put a square around any mention of making a difference
  - Underline when something changes for the better

PHARMAC

The goal of this exercise is to create a mission statement for Paul's security team at PharmaCo by going through the four-step process we just discussed.

Step 1
Normally, this process starts with telling a story about a time your security team did something meaningful. It can be about anything. Any situation that you are proud of when the team did its best work. In this case, the story has already been identified for you.

Step 2
Next, highlight the keywords. Circle the important people or places. Put a square around any mention of making a difference. Finally, underline the items when something changes for the better.

Lab 2.1: Creating a Mission Statement (2)

- Step 3: Group the items in each category
  - Find the Big Ideas
- Step 4: Draft the mission statement
  - Incorporate the Big Ideas
  - Don't worry about word choice; keep it short and simple
  - If no one disagrees with it, then it's too generic
- Bonus
  - Create a mission statement for your security team
  - Identify a time when your team did something meaningful
  - What *does* it or *would* it look like when you're doing your best work?

Step 3
Then, group the Big Ideas. There is an empty worksheet on the upcoming page that you can use.

Step 4
Finally, try to write a draft of the mission statement for your security team by incorporating the big ideas you have just identified. Don't worry about making the words perfect. Try to keep the statement short and simple by conveying the main point. If no one else disagrees with the draft mission statement, then it may be too generic. In that case, you may want to incorporate more big ideas.

Bonus
Create a mission statement for your security team. Start by identifying a time when your team did something meaningful. Something that your key stakeholders appreciated. If you can't think of a story, then make one up. What *would* it look like when the security team is doing its best work?

Lab 2.1: Highlight Keywords

"By providing secure mobile apps, we helped our scientists and researchers receive faster feedback from clinical trials that allowed us to get new drugs to market faster. This allowed patients to have more time with their families and saved many of them from death."

Circle the people or places
Put a square around any mention of making a difference
Underline when something changes for the better

PHARMAC

The story on this slide is about a time that the PharmaCo security team worked to build security into the mobile apps used by scientists and researchers for clinical trials. The data obtained during clinical trials is extremely important in determining the efficacy of new drugs. As a result, it's extremely important to keep this data secure. Moreover, clinical trials can take a long time. This can delay the drug development and ultimately regulatory approval process. By getting effective drugs to market faster, PharmaCo gives patients a better chance to eliminate illness, prolong life, and spend more time with their families and loved ones.

Go ahead and circle the people or places (the nouns), put a square around any mention of making a difference, and underline the big change for the better that is introduced by PharmaCo's actions.

Lab 2.1: Group the Big Ideas

Our Cause Who? What? Where?	
Our Actions What we do	
Our Impact Changes for the better	

In the first row labeled "Our Cause", write down the people or places you circled on the previous page.

In the second row labeled "Our Actions", write down the mentions of making a difference you put a square around on the previous page.

In the third row labeled "Our Impact", write down the big changes for the better that you underlined on the previous page.

Next, for each row, try to think about other items that are related to the words you wrote down. Then, group them into categories. This can be challenging. For example, in the first row, you might have words like "patients", "families", and "children" that are grouped into a category called "Community."

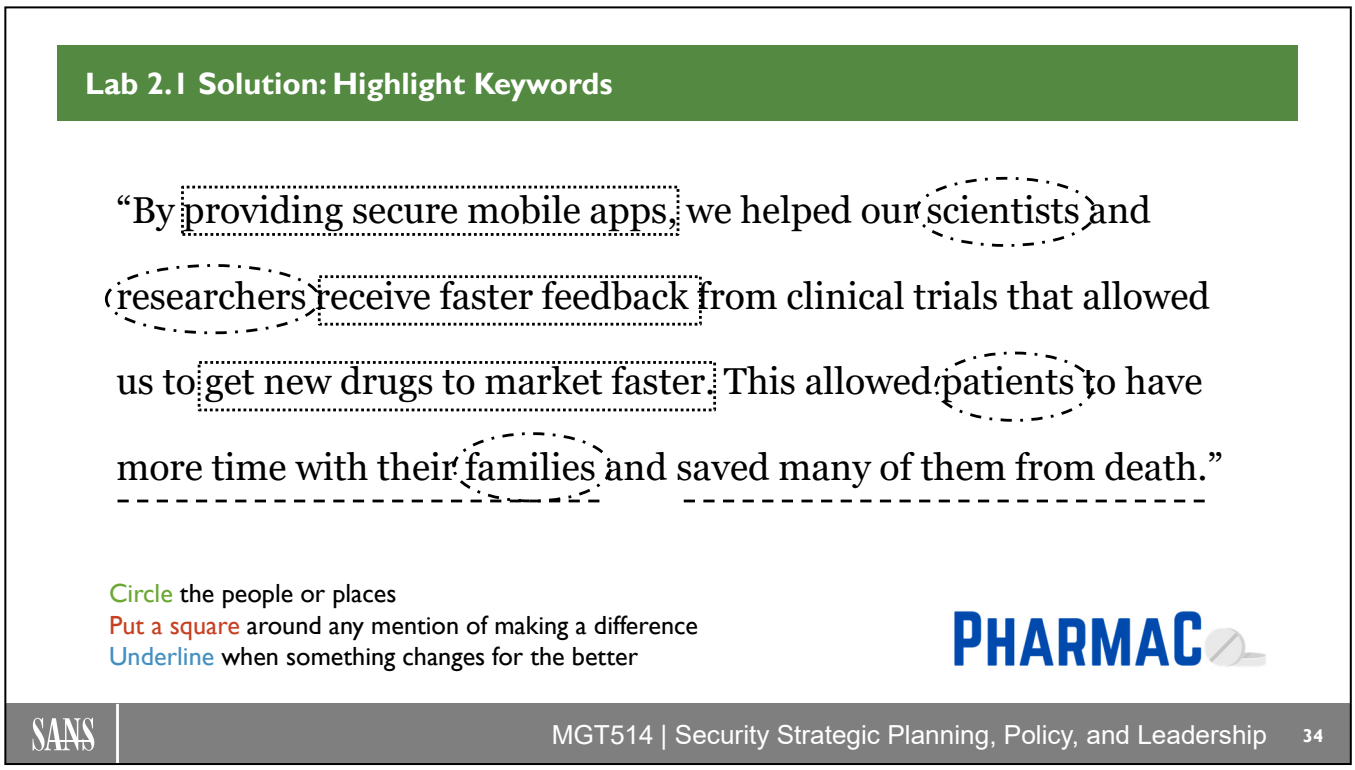
Finally, draft the mission statement for the security team at PharmaCo.

There is space to draft three different versions of your mission statement if needed in the space above or below.

Lab Debrief

Note that this section contains a debrief and potential lab answers

This page intentionally left blank.



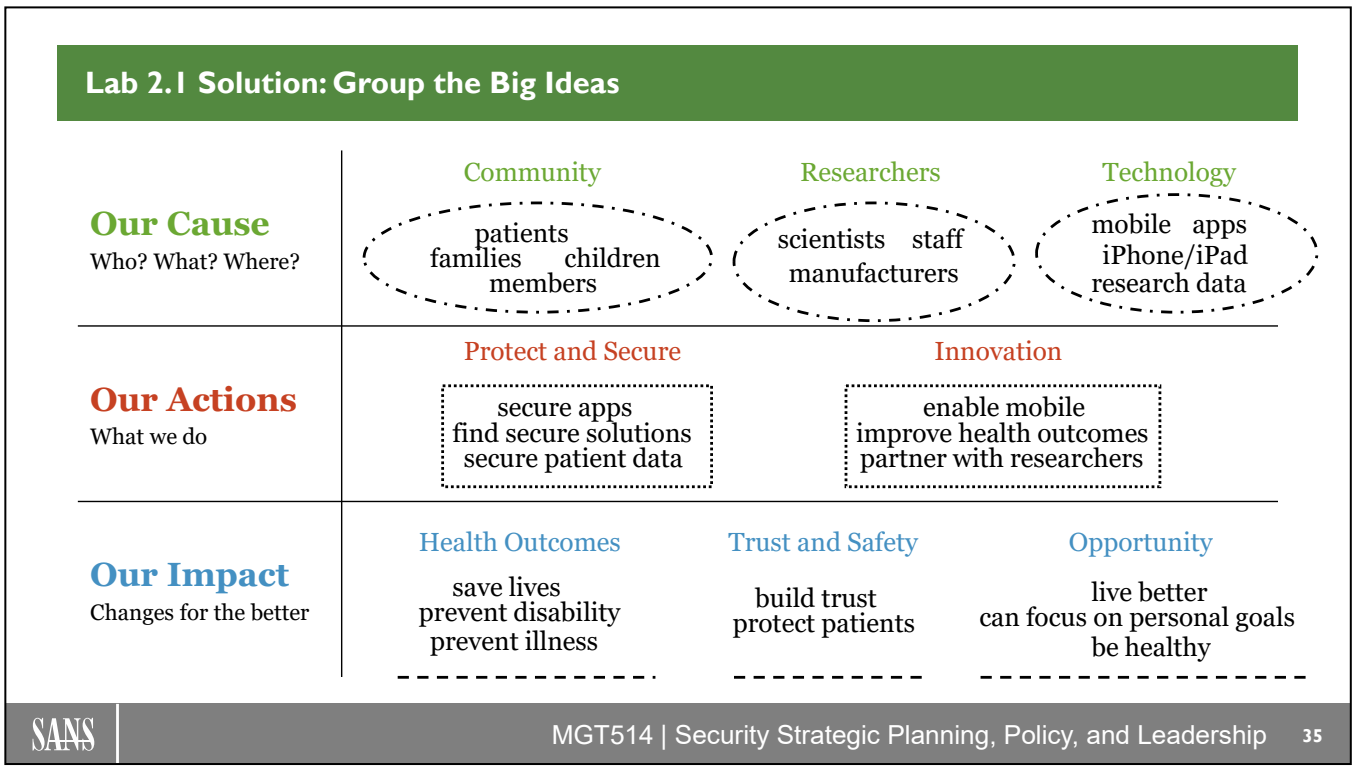
In the PharmaCo story, you:

1) Circled the people or places
   a) "scientists"
   b) "researchers"
   c) "patients"
   d) "families"

2) Put a square around any mention of making a difference
   a) "providing secure mobile apps"
   b) "receive faster feedback"
   c) "get new drugs to market faster"

3) Underlined when something changes for the better
   a) "more time with their families"
   b) "saved many of them from death"

This step helps you identify the important parts of your story so that you can group them in the next step.



Next, group the big ideas by taking the words and phrases from the previous step. Patterns and similarities should develop naturally.

For "Our Cause", we've taken words from the story like "families" and "patients" and added additional stakeholders like "children" who are part of the "Community" that the organization serves. Another group called "Researchers" includes "scientists" and "staff." Finally, those constituents are supported by the use of "Technology" such as "mobile" and "apps" that utilize important "research data."

For "Our Actions", we want to "Protect and Secure" the environment while also enabling the "Innovation" that the business requires. This leads us to write down other ideas that preceded the story. For example, how did you know that you needed to secure mobile apps? You may have partnered with some researchers and discovered that they were looking for solutions to speed up execution and analysis of clinical trials. As a result, "partner with doctors" and "improve health outcomes" are listed under "Innovation" on the slide.

For "Our Impact", we want to succinctly categorize the overall change for the better, which is what truly matters to your stakeholders. This is why "save lives," "prevent disability," and "prevent illness" are listed under "Health Outcomes."

Grouping and naming the common ideas in your story helps identify themes that you can use to craft your actual mission statement.

Here, we have taken the previously circled, squared, and underlined words and crafted three sample mission statements. Creating a mission statement can be a difficult process. However, by telling a story, identifying keywords, and grouping the big ideas, you can draft a mission statement that will resonate with your key business partners.

Going forward, we will use the last sentence as the mission statement for the security team at PharmaCo:

"Help people lead healthier lives by creating safe spaces for drug research and innovation."

In Summary

- As a manager and leader:
  - You are expected to understand what the organization does and is trying to achieve
  - Understanding the mission and vision are key
- Crafting a team mission statement
  - Maps back to the mission of the larger org
  - Shows that you understand organizational goals
  - Helps your team focus on work that is important to the organization

As a manager and leader, you are expected to understand what the organization does today and what it is trying to achieve in the future. This is why understanding the mission and the vision of the organization are so important. This understanding helps you set the appropriate direction for your team and identify security initiatives that will be valuable to key stakeholders; it also helps your team focus on work that is important to the organization.

Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Define Current State
  - Vision and Mission
    - Lab #1: Mission Statement
  - ***SWOT Analysis***
    - Lab #2: SWOT Exercise
- Develop the Plan
  - Visioning and Innovation
  - Security Framework
  - Security Roadmap
    - Gap Analysis
    - Lab #3: Roadmap Development
  - Business Case Development
- Deliver the Program
  - Security Metrics Program
  - Marketing and Exec Communications

This page intentionally left blank.

What Is SWOT Analysis?

- A structured discovery and planning tool used:
  - To evaluate strengths, weaknesses, opportunities, and threats
  - For your business initiatives, teams, and/or individuals
- SWOT stands for:
  - **S**trengths
    - Favorable characteristics of the business that are working well
    - These will work to your advantage
  - **W**eaknesses
    - Unfavorable conditions of the business that put you at a disadvantage
    - These should be mitigated as soon as possible
  - **O**pportunities
    - External situations that the organization might leverage to its advantage
  - **T**hreats
    - External factors that might be potential sources of failure

SWOT analysis is a structured discovery and planning tool that is useful in helping you understand your **s**trengths and **w**eaknesses, identify both the **o**pportunities that are open to you and identify the **t**hreats that you face. This tool can be used for your business initiatives, teams, and/or individuals.

SWOT analysis can be used in a number of decision-making situations. As an example, when used in the business initiative context, it helps you to understand and maintain your niche in your particular market. Used in the team context, it helps you understand how to strengthen and manage high-performing teams. Used in the individual context, it can help identify talent, abilities, and develop career paths. SWOT can also be used in pre-incident/crisis planning and preventive incident/crisis management or used in creating a recommendation during a viability study.

The acronym SWOT stands for:

- **Strengths**: Favorable characteristics of your business that are working well and you can use to your advantage. These are generally internal to your organization.
- **Weaknesses**: Unfavorable conditions of the business that put you at a disadvantage or detract from your ability to achieve your desired goal. These should be mitigated as soon as possible.
- **Opportunities**: External situations that your organization might leverage or propel to your advantage.
- **Threats**: External factors that might be potential sources of failure, place the group's mission or operation at risk, and should be managed or eliminated as soon as possible through contingency planning.

The origins of the SWOT analysis are generally credited to Albert Humphrey, who led a convention at the Stanford Research Institute in the 1960s and 1970s using data from Fortune 500 companies. Humphrey himself does not claim the creation of SWOT, and the origins remain somewhat obscure.

Like PEST and Porter's Five Forces, over the course of time, many variants have been created. Heinz Weihrich, author, management consultant, and a professor of global management and behavioral science at the University of San Francisco, introduced the TOWS Matrix, a conceptual framework that aids in finding the

most efficient actions. Weihrich claimed that some users found it difficult to translate the results of the SWOT analysis into meaningful actions that could be adopted within the wider corporate strategy.

Comparative SWOT analysis is another variant that facilitates the groups and comparison of competing SWOT analysis such as different projects and/or markets. Finally, there is a SWOT landscape analysis that systematically deploys the relationship between the overall objective and underlying SWOT factors and provides an interactive query-able 3D landscape.

Setting aside the variations of SWOT, the framework you will learn in this section is the most widely recognized and utilized SWOT analysis framework. SWOT should be used as a complementary tool to PEST and Porter's Five Forces in developing your strategy.

References:

https://en.wikipedia.org/wiki/SWOT_analysis
https://en.wikipedia.org/wiki/Heinz_Weihrich
https://en.wikipedia.org/wiki/Albert_S._Humphrey
http://www.businessnewsdaily.com/4245-swot-analysis.html
https://www.mindtools.com/pages/article/newTMC_05.htm

Why We Need To Do SWOT Analysis

- Will help you focus on vital components of your efforts by:
  - Uncovering strengths and opportunities to build upon and exploit
  - Detecting weaknesses and threats that can be eliminated and/or managed
- Used in strategic planning to:
  - Prioritize for successful outcomes
  - Develop short-term and long-term plans
  - Gain and maintain a competitive advantage

SWOT analysis highlights the areas in which major strengths and weaknesses are evident. It also highlights opportunities that you may be well positioned to exploit and threats that you would want to manage and eliminate over time. In addition, by looking at yourself and your competitors using the SWOT tool, you can further refine and focus your strategy on vital components that distinguish you from your competitors with a greater likelihood of success.

The SWOT analysis framework is beneficial in so many ways. It can help set objectives by defining what your organization is going to do. It can help you with an environmental scan so you better understand how you are positioned in your particular industry. It can help you see what changes you need to make in your current operations or existing strategies. SWOT analysis helps organizations decide whether or not an objective is obtainable or in exploring avenues for new initiatives. It can also be used as a monitoring mechanism for an initiative underway to determine whether refinement or redirection efforts are needed.

In summary, identification of the SWOT elements is important because it can determine vital steps that should be included in planning to achieve the desired outcome.

Reference:
http://www.businessnewsdaily.com/4245-swot-analysis.html

SWOT Analysis

- Strengths and Weaknesses are often internal to your org
- Opportunities and Threats are generally external factors

Strengths	Weaknesses
Opportunities	Threats

Strengths and weaknesses are often internal to your organization, whereas opportunities and threats generally relate to external factors. For this reason, the SWOT analysis is sometimes called "Internal-External (IE) analysis," and the SWOT Matrix is sometimes called the "IE Matrix." It's probably obvious but still worth stating that strengths and opportunities are helpful, whereas weaknesses and threats are harmful.

Strengths are favorable characteristics of your business that are working well and you can use to your advantage. These are internal to your organization. You'll want to consider your strengths from an internal perspective, also from the point of view of your customers, and others in the marketplace as well as your competitors. Think about your strengths in relation to your competitors. For example, if all of your competitors provide high-quality products, and high-quality production processes are not a strength in your organization, it might be a necessity to compete in that specific market.

Weaknesses are unfavorable conditions of the business that put you at a disadvantage or detract from your ability to achieve your desired goal. These should be mitigated as soon as possible. Although this is often internal to your organization, you'll also want to consider looking at this from the eyes of external people as well. For example, do other people outside your organization seem to perceive weaknesses that you possibly don't see, or are your competitors doing better than you? It's best to be brutally honest and realistic in this section and face the unpleasant truths so you have the opportunity to do something about them.

Opportunities are external situations that your organization may leverage or propel to your advantage. Useful opportunities can come from such things as changes in technology and markets on a broad and narrow scale, or changes in government policy related to your field, changes in social patterns, population profiles, and lifestyles and local events. A useful approach when looking at opportunities is to look at your strengths and weaknesses and ask yourself whether they open up any opportunities if you leverage your strengths or eliminate threats.

Threats are external factors that might be potential sources of failure or place the group's mission or operation at risk and should be managed or eliminated as soon as possible through contingency planning. You might also want to look at your strengths and weaknesses to determine the threat of successes turning into weaknesses and weaknesses turning into real threats.

Strengths

- Favorable characteristics of the business that are done right and working well
  - These will work to your advantage
- Perspectives to consider
  - Internal
  - Customers' point of view
  - Others in the marketplace
  - Competitors
- Key questions to ask
  - Does your organization have any advantages over others?
  - What do you do better than anyone else?
  - Do you have unique capabilities and/or attributes?
  - How do others in the marketplace view your strengths?
  - Do you have a unique value proposition?

As a reminder, strengths are favorable characteristics of your business that are working well and you can use to your advantage. These are internal to your organization. You'll want to consider your strengths from an internal perspective, from the point of view of your customers, others in the marketplace, and your competitors.

A good place to begin analyzing the strengths is to determine what advantages the organization has: What do you do better than anyone else, what are the unique capabilities and/or attributes you can draw on that others can't, what do other people in your market see as your strengths, and what is your unique value proposition?

Other examples for consideration internally for you are financial resources such as funding availability, sources of income and investment opportunities, physical resources (such as location, facilities, and equipment), human resource elements (such as employees, volunteers, and target audiences), and the role of key staff members. Access to natural resources, trademarks, patents and copyrights, and current processes (such as employee programs, training, etc.) should also be considered. You might also want to look at departmental hierarchies and company culture and image, and don't forget to consider any technology advantage or disadvantage. You can look at operational efficiency and operational potential. These examples could also be considered for the Weakness quadrant.

If you're having difficulty identifying strengths, this is where the brainstorming and the aid of various people can come into play. Begin by writing down a list of your organization's characteristics. Some of these ideas will likely be strengths that you can build on.

References:
http://www.businessnewsdaily.com/4245-swot-analysis.html
https://www.mindtools.com/pages/article/newTMC_05.htm

Thunderbolt SWOT Analysis – Strengths

Strengths	Weaknesses
• Understanding of key business drivers • Investment in business enabling technology • Familial, employee focused culture • Hiring key leadership roles (CDTO & CIO) • Early recognition of need for a CISO • Ability to solicit input from stakeholders	
Opportunities	**Threats**

So far in class, we have learned about Thunderbolt and their efforts so far with their cloud migration. Let's summarize what we know by placing information about Thunderbolt into a SWOT analysis.

Thunderbolt, as a company, has grown over the years to become a major player in global shipping and logistics. This has been accomplished by having a strong understanding of key business drivers and investing in business enabling technology systems. This is in combination with building a familial, employee focused culture that has engendered a lot of loyalty.

In recent times they have realized they need to take the next step and have done so by hiring key leadership roles such as the CDTO and CIO. This is on top of their early recognition that there should be one senior person responsible for all of security.

Much of this progress seems to be based on their ability to solicit input from various employees to understand the current state of affairs.

Weaknesses

- Unfavorable conditions of the business that put you at a disadvantage
  - It's best to be realistic in this section so you can mitigate risk as soon as possible
- Perspectives to consider
  - Internal
  - Customers' point of view
  - Others in the marketplace
  - Competitors
- Key questions to ask
  - Are there areas that others in your market would likely see as a weakness?
  - What factors would lose credibility for you?
  - Is there anything my competitors are doing better than me?

As a reminder, weaknesses are unfavorable conditions of the business that put you at a disadvantage or detract from your ability to achieve your desired goal. These should be mitigated as soon as possible. Although this is often internal to your organization, you'll also want to consider looking at this through the eyes of external people. For example, do other people outside your organization seem to perceive weaknesses that you possibly don't see, or are your competitors doing better than you? Don't forget to be brutally honest and realistic in this section.

A good place to begin analyzing the weaknesses is to determine where you can improve, what you can avoid, what people in the market are likely to see as your weaknesses, what factors lose credibility for you, and what your competitors are doing better than you.

Weaknesses can include limited financial resources, constrained physical resources (e.g. location, facilities, and equipment), employees with the wrong skill sets, limited access to natural resources, and a weak patents library. You should also determine whether current processes are broken or non-existent, or if you have inadequate employee programs such as training. You might also want to consider whether departmental hierarchies are detrimental and cause a weakness or whether the company culture or image shows as a weakness. Don't forget to consider any technology disadvantage or any operational inefficiency and lack of operational potential, which are all starting points.

References:
http://www.businessnewsdaily.com/4245-swot-analysis.html
https://www.mindtools.com/pages/article/newTMC_05.htm

Thunderbolt SWOT Analysis – Weaknesses

Strengths	Weaknesses
• Understanding of key business drivers • Investment in business enabling technology • Familial, employee focused culture • Hiring key leadership roles (CDTO & CIO) • Early recognition of need for a CISO • Ability to solicit input from stakeholders	• Uncoordinated approach to cloud adoption • Limited understanding of cloud data storage risks • Lack of systems and processes to support cloud • Technology teams lacking cloud experience • Resistance from security team members
Opportunities	**Threats**

In relation to cloud, Thunderbolt has some issues. They currently have one business unit (ThunderPrint) deployed 100% in the cloud and a number of other sprinklings of cloud usage throughout the organization. Their cloud adoption plan is uncoordinated at best. As a result, they also have a limited understanding of the cloud security risk and lack of systems and processes to support the cloud. This is evidenced by the technology and security teams' lack of cloud knowledge and experience. On top of that, many security team members are resistant to the cloud overall.

Opportunities

- External situations that the organization can leverage or exploit to its advantage
- Perspectives to consider
  - Strengths and Weaknesses you've already documented
  - Include output of PEST analysis to ensure you haven't overlooked any factors such as demographics, employment trends, etc.
- Key questions to ask:
  - What interesting trends are you aware of?
  - Are there any significant changes in technology and markets?
  - What government and/or regulatory policy relate to your field?
  - How can you leverage social patterns such as population profiles, lifestyle changes, etc.?

As a reminder, opportunities are external situations that your organization may leverage or propel to your advantage. Useful opportunities can come from such things as changes in technology and markets on both a broad and narrow scale, or changes in government policy related to your field, changes in social patterns, population profiles, lifestyle changes, and local events.

A useful approach when looking at your opportunities is to look at your strengths and weaknesses and ask yourself if they open up any opportunities if you leverage your strengths or eliminate threats. You may also want to include output of your PEST analysis to ensure you haven't overlooked any factors such as demographics, employment trends, etc.

External forces influence and affect every company, organization, and individual, whether they are directly or indirectly connected to an opportunity or threat. It's important to consider all items that were generated as a result of the brainstorming activities.

References:
http://www.businessnewsdaily.com/4245-swot-analysis.html
https://www.mindtools.com/pages/article/newTMC_05.htm

Thunderbolt SWOT Analysis – Opportunities

Strengths	Weaknesses
• Understanding of key business drivers • Investment in business enabling technology • Familial, employee focused culture • Hiring key leadership roles (CDTO & CIO) • Early recognition of need for a CISO • Ability to solicit input from stakeholders	• Uncoordinated approach to cloud adoption • Limited understanding of cloud data storage risks • Lack of systems and processes to support cloud • Technology teams lacking cloud experience • Resistance from security team members
Opportunities	**Threats**
• Trend of increasing cloud adoption • Desire of people to use and learn cloud computing • Attract and retain young and skilled employees • Reduce technology and support costs • Improve employee productivity • Increase agility and speed to market	

Despite the challenges, Thunderbolt does want to move toward formal adoption because of the larger opportunities and benefits related to cloud. There is a desire to use and learn about the latest cloud services given larger industry trends. To stay competitive, Thunderbolt wants to leverage cloud as one factor in attracting and retaining younger workers. This also has the benefit of reducing legacy technology costs, improving employee productivity, and increasing overall speed to market.

Threats

- External factors that can be potential sources of failure or cause trouble for the business
- Perspectives to consider
  - Include output of PEST analysis to ensure you haven't overlooked any factors such as government regulations and technology changes
- Key questions to ask:
  - What obstacles do you face?
  - What are your competitors doing?
  - Are quality standards or specifications for your job changing?
  - Is changing technology threatening your position?
  - Does your company have cash-flow problems?
  - Could any of your weaknesses seriously threaten your business?

As a reminder, threats are external factors that can be potential sources of failure or place the group's mission or operation at risk and should be managed or eliminated as soon as possible through contingency planning. For this quadrant, you might also want to include the output of your PEST analysis to ensure you haven't overlooked any critical areas such as government regulations or technology changes.

A good place to start your brainstorming for this quadrant is to look at some of the obstacles you, your organization, and your company face. You'll want to look at what your competitors are doing. If they are doing the same thing better than you, this would certainly be a threat. You'll need to determine whether quality standards and/or specifications for your job are changing. In security, this might be any new regulatory mandate, for instance. You should also look at technology and answer, "Is there any threat to your position?" Although in security, that is highly unlikely. You shouldn't, however, discount looking into this question and making sure the answer is as it appears. You should also look at your company and the financial aspect, for example, and answer, "Does it have cash-flow problems and is its credit rating at risk?"

And most importantly, you'd like to know whether any of your weaknesses seriously threaten your business, as is the case of the development plans that have been found in the hands of outsiders. We know from our Porter's Five Forces the importance of understanding competitive rivalry. Therefore, if sensitive research and development documents or sensitive documents related to clinical trials were to be leaked to the competitors, it might be a going-out-of-business event.

Lab 2.2: SWOT Exercise

Estimated Time: 20 Minutes

- Goal of this exercise
  - Identify & summarize threats in the SWOT analysis
- Read the case study
  - Think about what is missing from the existing analysis
- On the next page, answer these questions:
  - What are the business concerns?
  - What are the technology concerns?
  - What are the security concerns?

READ

Read the 1/2-page case study below

It takes approximately 5 minutes to read the case

Cloud and Business Enablement

Leslie Franks (CISO) reviewed the list of technologies and categories attached to the meeting invite. She knew the transition would likely happen, but she sensed there was still a question of which systems would move to the cloud and when these systems would move. To make sure she was prepared to outline the risks of the project, she noted several concerns, and put them in the following categories:

1. Business Concerns: What are the true costs of on-premise systems versus cloud-based systems and how can they be quantified? What is the cost and business impact of the transfer and what will change with upgrades and maintenance? What can be done to get resistant parties on board?

2. Technology Concerns: How can the staff be upskilled to meet the requirements of increased cloud adoption? What can be done to retain key talent and make work attractive to younger team members? What will the impacts be to the speed of executing IT engineering requests and the response time of business needs?

3. Security Concerns: What is the true security risk of on-premise systems versus cloud-based systems? Should Thunderbolt work with only one cloud provider, or spread data across multiple providers? In case of an attack, what is involved in the backup/restore process, and what would be the impact to the business? And finally, how can the migration proceed in a way that satisfies those who are fearful or resistant?

As Franks was winding down for the evening, Peter Yang (CIO) stopped by her office. “Did you get the invite? Looks like we’re moving forward with cloud migration.”

“It does look that way,” she responded in the most neutral tone she could muster.

“I think you’ll see that it’s the best thing for the business.”

Franks took a breath before responding. “Peter” she said calmly. “You and I both want what’s best for the business.”

Lab 2.2: SWOT Exercise

Strengths	Weaknesses
• Understanding of key business drivers • Investment in business enabling technology • Familial, employee focused culture • Hiring key leadership roles (CDTO & CIO) • Early recognition of need for a CISO • Ability to solicit input from stakeholders	• Uncoordinated approach to cloud adoption • Limited understanding of cloud data storage risks • Lack of systems and processes to support cloud • Technology teams lacking cloud experience • Resistance from security team members
Opportunities	**Threats**
• Trend of increasing cloud adoption • Desire of people to use and learn cloud computing • Attract and retain young and skilled employees • Reduce technology and support costs • Improve employee productivity • Increase agility and speed to market	

After reading the portion of the case study, answer these three questions to determine the threats that Thunderbolt is facing when considering increased cloud adoption. Specifically, try to identify additional concerns that are *not* listed in the case study itself.

1) What are the business concerns?

2) What are the technology concerns?

3) What are the security concerns?

Lab Debrief

Note that this section contains a debrief and potential lab answers

This page intentionally left blank.

Thunderbolt SWOT Analysis Debrief

Strengths	Weaknesses
• Understanding of key business drivers • Investment in business enabling technology • Familial, employee focused culture • Hiring key leadership roles (CDTO & CIO) • Early recognition of need for a CISO • Ability to solicit input from stakeholders	• Uncoordinated approach to cloud adoption • Limited understanding of cloud data storage risks • Lack of systems and processes to support cloud • Technology teams lacking cloud experience • Resistance from security team members
Opportunities	**Threats**

• Trend of increasing cloud adoption
• Desire of people to use and learn cloud computing
• Attract and retain young and skilled employees
• Reduce technology and support costs
• Improve employee productivity
• Increase agility and speed to market
	• Business concerns
	  • Rise of shadow IT; Total cost of ownership
	  • Continuity issues; Obtaining buy-in
	• Technology concerns
	  • Upskilling existing staff; Minimizing staff attrition
	• Security concerns
	  • Data protection; Leveraging modern practices

Thunderbolt has identified three areas of concern related to BYOD.

From a security perspective, there are risks of both adopting and not adopting cloud. With cloud, there are concerns around data control and visibility. Can Thunderbolt develop the required capabilities and modern practices to use the cloud securely and appropriately protect data? However, if nothing is done, there is a risk of enabling shadow IT, which would increase the adoption of cloud in an uncoordinated and perhaps insecure manner.

There are also technology concerns. Moving to the cloud will help modernize the technology stack and minimize staff attrition. However, there are many team members who need to be trained on these new technologies. A comprehensive training plan needs to be developed.

For the business overall there are cost concerns. Thunderbolt believes that the cloud will aid in cost savings, but is this entirely the case? The company makes a living shipping what you need when you need it. Careful attention must be paid to ensure that there are no disruptions to key business operations with the use of new technology. As a result, there is still a lot of work to do in creating a roadmap and obtaining buy-in.

In Summary

- SWOT Analysis is used:
  - As part of the strategic planning process
    - Evaluate strengths, weaknesses, opportunities, and threats
    - Help develop short-term and long-term plans
    - Prioritize security investments for successful outcomes
  - To help you have more meaningful dialogue with business leaders
    - How security can respond, enable, and support business goals and market trends

In summary, the SWOT analysis is a structured discovery and planning tool that is useful in helping you understand your strengths, weaknesses, opportunities, and the threats to your business initiatives, teams, and/or individuals. It should be used as part of the strategic planning process to help develop short-term and long-term plans. This will help you prioritize security investments for successful outcomes and, most importantly, the results will provide you with the right information to have a more meaningful dialogue with your business leaders and illustrate to them in their terminology how security can respond, enable, and support business goals and market trends.

Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Define Current State
  - Vision and Mission
    - Lab #1: Mission Statement
  - SWOT Analysis
    - Lab #2: SWOT Exercise
- ***Develop the Plan***
  - Visioning and Innovation
  - Security Framework
  - Security Roadmap
    - Gap Analysis
    - Lab #3: Roadmap Development
  - Business Case Development
- Deliver the Program
  - Security Metrics Program
  - Marketing and Exec Communications

This page intentionally left blank.

How to Develop the Plan

1) Determine where you want to go
   - Create a vision that fosters innovation
2) Create a structure to follow
   - Utilize a security framework
3) Understand what it takes to reach the goal
   - Analyze your gaps
4) Create a plan
   - Develop the roadmap
5) Gain support and funding
   - Learn approaches to building a security business case

Developing a roadmap for your security team or program is not just about identifying technical capabilities and tools to deploy. An effective roadmap is developed by:

1) Determining where you want to go
   - By defining a vision for an improved future state, you as a leader can create an environment that allows people to think in innovative new ways.

2) Creating a structure
   - It's not just about the grand plan or vision. Making this practical requires following a structure for the security team. This can be done by creating or utilizing a security framework.

3) Understanding what it takes to reach the goal
   - By understanding the current state and analyzing the resulting gaps, you can identify discrete actions that need to be taken to reach the goal.

4) Creating a plan
   - With the end goal, program structure, and gaps identified, you can create the roadmap for your team to follow.

5) Gain support and funding
   - Without support and funding, your initiatives will not get off the ground. Understanding how to build a viable security business case is an important part of obtaining this support.

Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Define Current State
  - Vision and Mission
    - Lab #1: Mission Statement
  - SWOT Analysis
    - Lab #2: SWOT Exercise
- Develop the Plan
  - ***Visioning and Innovation***
  - Security Framework
  - Security Roadmap
    - Gap Analysis
    - Lab #3: Roadmap Development
  - Business Case Development
- Deliver the Program
  - Security Metrics Program
  - Marketing and Exec Communications

This page intentionally left blank.

Visioning and Innovation

- Goals of this section:
  - Incorporate visioning into strategic planning
  - Learn to be innovative with the business
    - By solving their "jobs to be done"

> "If I'd asked people what they wanted, they would have said faster horses."
> - Henry Ford

Henry Ford is the famous founder of Ford Motor Company, which brought affordable automobiles to the masses by pioneering the assembly line technique of mass production. In a time when automobiles were extremely expensive and reserved for the wealthy, Ford had a vision of providing inexpensive goods and high wages for workers. He was able to envision an alternate future that was not dominated by horses and carriages. This vision led to business process innovation that resulted in solving the problem of affordable and convenient transportation for millions of people around the world.

Visioning

- Process of thinking about how the world will be in the future
  - Helps "stretch" strategic planning
- Without the visioning step
  - Will likely end up producing a tactical plan instead of a strategic plan

Visioning is not the same thing as a vision statement. A vision statement is what we want to become and what we aspire to be. Visioning helps us to think about the world we are most likely to face.

Visioning, or futurism, is the process of thinking about what the world will be like 10 or even 20 years from today. It is an invaluable tool in strategic planning because it forces us to think about the unknown world. We tend to be short-term focused in security, partly because we are constantly responding to new threats. We also tend to skip doing things that are hard. What operating system and computing device will your organization use in 5 years? What about 10 years? You don't know and we do not either, but we do expect we will have operating systems and computing devices.

Skipping the visioning process is not recommended. If you do, you will almost certainly end up with a tactical plan.

Practical Tips to Succeed

- Visioning is hard
  - People tend to jump straight to tactical planning and solutions
- Institute regular visioning sessions
  - Come up with 10 ideas every day
  - Create a collaborative work environment
- Praise every idea
  - Praise to criticism ratio
    - 5.6 to 1 in highest performing teams
    - 1.9 to 1 in medium performing teams
    - .36 to 1 in low performing teams

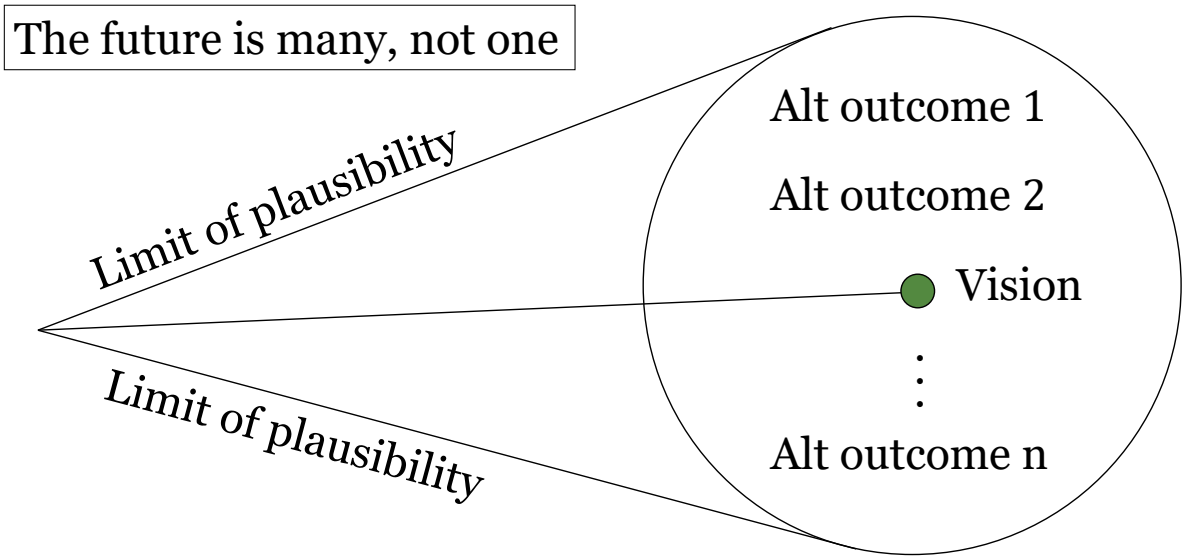
Visioning is a difficult process. Just as people tend to jump straight into creating solutions when presented with a problem, people tend to jump straight into tactical planning when doing strategic planning.

Often, the mind has to be trained to think in innovative ways. James Altucher is an entrepreneur and author who founded StockPickr, sold it to TheStreet.com for $10 million and lost $15 million in two years on failed investments. This enabled him to reevaluate his approach to business and life. He has an article titled, "The Ultimate Guide for Becoming an Idea Machine."[1] He says, "It's important to exercise the idea muscle right now. If your idea muscle atrophies, then even at your lowest point, you won't have any ideas." Among other things, he says that you should come up with 10 ideas every day. Start the idea muscle working. That's it.

At work, you can institute collaborative work environments that can help with visioning and innovation—perhaps something similar to English coffee houses in the 17th and 18th century that might have contributed to The Enlightenment.[2] No matter how you create these collaborative environments, one thing is clear. You, as a manager and leader, should praise every idea. You probably can't say "I agree with that" or "That's a great idea" often enough. Research has shown that the highest-performing teams compliment each other up to 15 times more often than the lowest-performing teams.[3] Similar research has shown comparable results when looking at the rate of married couples getting divorced vs. staying together. This can even apply to acts of non-verbal communication such as high fives and fist bumps on sports teams.[4]

References:
[1] http://www.jamesaltucher.com/2014/05/the-ultimate-guide-for-becoming-an-idea-machine/
[2] https://en.wikipedia.org/wiki/English_coffeehouses_in_the_17th_and_18th_centuries#The_Enlightenment
[3] https://hbr.org/2013/03/the-ideal-praise-to-criticism/
[4] http://espn.go.com/blog/truehoop/post/_/id/13761/study-good-players-arent-afraid-to-touch-teammates

The Cone of Plausibility



Even if you implement regular visioning sessions and create a nurturing environment for innovative ideas, visioning is still very hard. The good news is that we do not have to be pinpoint accurate to gain benefits from visioning. As long as we respect the limits of plausibility (in the next 10 years, faster-than-light travel, cold fusion, world peace, etc., are not within the limits of plausibility), we have a good chance of being close enough to position our organization to what actually happens to take advantage of perceived opportunity.

Dick Tracy: Two-Way Wrist Radio

What is on his wrist?

Dick Tracy is a fictional, comic book crime fighter who came into being in 1931, and his two-way wrist radio first appeared in 1946. This is within the cone of plausibility, perhaps not within 10 years, but given enough time.

References:
https://en.wikipedia.org/wiki/Dick_Tracy
http://dailyspeculations.com/DickTracy.png

Strategic Plan: Dick Tracy's Watch

- Miniaturization of electronics
- Power source that scales
- Wireless or cellular connectivity
- Impact resistance
- Strong, efficient encryption
  - He does fight organized crime

Say it is 1935 and we are a company that believes in the future and that there will be two-way voice and video communication devices. What are the big problems that need to be solved to make such a communications device a reality? If we were planning strategically, what would need to happen to make this plausible? Some of them are:

- Miniaturization of electronics
- Power source that scales
- Wireless or cellular connectivity
- Impact resistance
- Strong, but efficient encryption

Jules Verne (1828 – 1905)

- French novelist who wrote:
  - *Journey to the Center of the Earth* (1864)
  - *From the Earth to the Moon* (1865)
  - *Twenty Thousand Leagues Under the Sea* (1870)
  - *Around the World in Eighty Days* (1873)
- He predicted many modern inventions:
  - Electric submarines
  - Lunar modules
  - Video conferencing
  - Taser
  - Skywriting: "Atmospheric advertisements"
  - Newscasts: "Instead of being printed the news will be spoken to subscribers"

Jules Verne is a French novelist who is most well-known for his adventure novels and influence on the science fiction genre.[1] His ideas were often a century ahead of his time. He predicted many modern inventions, such as electric submarines, lunar modules, video conferencing, the Taser, skywriting, and newscasts.[2]

References:
[1] https://en.wikipedia.org/wiki/Jules_Verne
[2] https://www.nationalgeographic.com/science/article/110208-jules-verne-google-doodle-183rd-birthday-anniversary

Nikola Tesla (1856 – 1943)

- Famous inventor who created:
  - Alternating current
  - Radio
  - Radar
  - X-rays
  - Hydroelectric power
  - Transistor
  - Remote control
  - Neon lighting
  - Electric motor
  - Wireless communications
- Good overview from *The Oatmeal*
  - "Why Nikola Tesla was the greatest geek that ever lived"
  - http://theoatmeal.com/comics/tesla

Nikola Tesla is a famous inventor who not only thought of amazing ideas, but he actually brought them to life. Among his most significant contributions are those inventions related to energy. He created alternating current, built the first hydroelectric power plant at Niagara Falls, and came up with a system for wirelessly charging your home. He even created a tower near New York City that would have provided free wireless energy to the entire world. The project was scrapped when the investor realized there would be no way to regulate the energy and, therefore, charge for it.

Reference:
https://theoatmeal.com/comics/tesla

Hedgehog Concept

- Based on an ancient Greek parable
  - "The fox knows many things, but the hedgehog knows one big thing."
- To be successful, focus on doing one thing extremely well
- Find your "Hedgehog Concept" by understanding what:
  - You are deeply passionate about
  - You can be the best in the world at
  - Drives your economic engine

The concept behind the Hedgehog Concept is based on a Greek poem about a fox and a hedgehog. A cunning and brilliant fox grasps the complexity of the woods around him. He sets his mind on eating a hedgehog and spends hours plotting the perfect attack. Meanwhile, the simple hedgehog goes about its business unaware. When the fox attacks, the hedgehog rolls himself into a spiny, impenetrable ball. The fox keeps re-strategizing, but the pattern repeats itself. "The fox knows many things, but the hedgehog knows one big thing." This understanding of developing what you can be the best at by focusing on doing one thing extremely well was described by philosopher Isaiah Berlin in his 1953 essay, "The Hedgehog and the Fox." Jim Collins further developed this idea in his 2001 book, *Good to Great: Why Some Companies Make the Leap…and Others don't*.

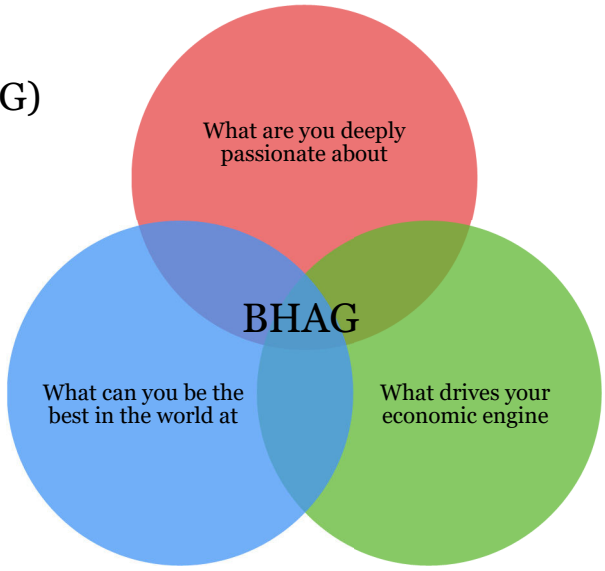
To find your Hedgehog Concept, you must understand three things:

- What you are deeply passionate about
- What you can be the best in the world at
- What drives your economic engine

Jim Collins refers to this as your "Big Hairy Audacious Goal (BHAG)."

BHAG

- Big Hairy Audacious Goal (BHAG)
  - Defines visionary goals
  - Common envisioned future



A deep understanding of the three intersecting circles is required to go from good to great. The most crucial point is that the Hedgehog Concept is not a goal to be the best, a strategy to be the best, an intention to be the best, and a plan to be the best. It is an understanding of what you can be the best at. The distinction is absolutely crucial.

A BHAG (pronounced bee-hag, short for "Big Hairy Audacious Goal") is a huge and daunting goal—like a big mountain to climb. It is clear and compelling, and people "get it" right away. A BHAG serves as a unifying focal point of effort, galvanizing people and creating team spirit as people strive toward a finish line. Like the 1960s NASA moon mission, a BHAG captures the imagination and grabs people in the gut. Good BHAGs flow from understanding; bad BHAGs flow from bravado. Great BHAGs sit right smack in the middle of the three circles.

The good-to-great companies did not say, "Okay, folks, let's get passionate about what we do." Sensibly, they went the other way entirely: We should do those things that only we can get passionate about.

To go from good to great requires transcending the curse of competence. It requires the discipline to say, "Just because we are good at it—just because we're making money and generating growth—doesn't necessarily mean we can become the best at it." The good-to-great companies understand that doing what you are good at will only make you good—focusing solely on what you can potentially do better than any other organization is the only path to greatness.

A company does not need to be in a great industry to become a great company. All good-to-great companies build a fabulous economic engine, regardless of the industry. They are able to do this because they attain profound insights into their economics. The denominator can be quite subtle, sometimes even unobvious. The key is to use the question of the denominator to gain understanding and insight into your economic model.

An essential point: "Growth" is not a Hedgehog Concept. Rather, if you have the right Hedgehog Concept and make decisions relentlessly consistent with it, you will create such momentum that your main problem will not be how to grow, but how not to grow too fast.

Innovation Discussion

- Brainstorm characteristics and different types of innovation
- Write down:
  - Three characteristics of innovation
    - Goal is to determine "What is innovation?"
  - Three companies you think are innovative
  - Three companies you think are not innovative

The goal of this exercise is to understand the characteristics of innovation and the different types of innovation. Start by writing down your answers to the questions below. Then, we'll discuss your responses and how they answer the question, "What is innovation?"

What are three characteristics of innovation?

1) _____

2) _____

3) _____

List three companies you think are innovative.

1) _____

2) _____

3) _____

List three companies you think are *not* innovative.

1) _____

2) _____

3) _____

Innovation

- Innovation is anything new and useful
  - If it's not useful, it's just an invention
- Three types of innovation:
  - Business model
  - Process
  - Product or service

When people think about innovation, the following characteristics might come to mind:

- Solves a problem
- Makes something easier
- Creates desire
- Is novel or new (e.g., technology)
- Is useful

These characteristics can be handy indicators, but how can you measure innovation? Revenue is an indicator that a company is producing items that meet customer needs but is not, in and of itself, a characteristic of innovation. Oftentimes, companies might measure the number of researchers or number of patents as an indicator of innovation. Are patents an innovation? Does a product have to be brought to market to be an innovation? Does it have to actually be useful?

If you are an engineer, you probably believe that products need to be useful. For example, what use is a blueprint for a bridge if you don't actually build the bridge? However, if you are a scientist, do you care if an idea is useful? A scientist would probably say, "It doesn't matter," because the act of discovery itself is what is important. That is what differentiates innovation from invention. Innovation is anything new and useful. If something is not useful, it's just an invention.

Many companies have produced useful things, but certain companies have a perception of being innovative or not. For example, Apple is cited as an innovator for its products like the Mac, iPhone, and iPad. However, products are just one form of innovation. One of Apple's biggest innovations is the iTunes store, the unbundling of single songs from the larger album, and the creation of an online distribution platform to sell these songs. This was an important business model innovation. On the other end of the spectrum, Dell is seen as a boring, low-margin computer maker. But Dell's innovation was not in the product space but in its capability to build extremely low-cost computers consistently and in massive quantities. Dell's was a process innovation.

Sustaining vs. Disruptive Innovation

- Sustaining innovation
  - Does not create a new market
    - Evolves an existing technology or process
- Disruptive innovation
  - Creates a new market
    - Eventually displacing an earlier technology or process
    - Typically starts with low-end disruption that serves least profitable customers with minimal functionality
  - Described in *The Innovator's Dilemma*
    - By Clayton Christensen

The Innovator's Dilemma by Clayton Christensen is often cited as one of the most influential business books in history.[1,2] It describes how successful, incumbent companies often fail because they are focused on maximizing profits and meeting the needs of existing customers. By offering an ever-increasing number of features, performance, and higher quality products that will lead to greater profits, these companies neglect opportunities based on new technologies that don't serve the needs of current customers, don't fit with their existing business models, and provide lower margins. This leaves the door open to competitors who excel at different tasks and, as their products mature, take over the market. A prime example of this is with mobile phones and tablets, which have disrupted the traditional PC market. Mobile devices offer fewer features than PCs, but they provide other benefits like mobility that customers value in more situations. As these mobile devices continue to improve, the existing technology gets further displaced.

A sustaining innovation, on the other hand, is one that does not create a new market but simply evolves or improves upon an existing technology or process. In computing, this includes things like increased memory capacity, speed, and screen resolution or improving the process for assembling computers to reduce costs and inefficiencies.

References:
[1] http://www.claytonchristensen.com/books/the-innovators-dilemma/
[2] https://www.wired.com/insights/2014/12/understanding-the-innovators-dilemma/

Examples of Disruptive Innovation

- Cars (mass produced)
- Digital music
- Digital photography
- PCs
- Smartphones
- Telephones
- Wikipedia

There are many examples of disruptive innovations throughout business history. Cars replaced the horse and buggy, streetcars, and rail transportation. Digital music disrupted physical music sales and the business model of record labels. Digital photography displaced chemical photography. PCs disrupted typewriters and dedicated word processors. Smartphones then, in turn, disrupted the PC. The telephone disrupted the telegraph. Wikipedia disrupted print encyclopedias.

Jobs To Be Done Theory

- Idea that customers don't just buy products
  - They hire solutions to get various jobs done
  - The customer "simply has a job to be done and is seeking to 'hire' the best product or service to do it"
- The theory helps you:
  - Understand what your customers want
  - Gain new insights to innovate with the business

The "jobs to be done" theory is best illustrated by a famous story about milkshakes from Clayton Christensen.[1]

There was a fast food restaurant that wanted to increase milkshake sales. So, it hired some expensive consultants to do an analysis, ask customers what they wanted, segment the market by products and demographics, and come up with a recommendation. After analyzing all the data and changing the milkshakes per their research, what happened? Nothing. Sales did not improve.

The company then decided to hire a different expensive consultant. This time, though, it wound up hiring one of Clayton Christensen's fellow researchers. He spent a whole day sitting in one of these fast food restaurants carefully observing everyone who bought a milkshake, what time they bought it, and whether they drank it on-site. He found that 40% of milkshakes were bought to go first thing in the morning by commuters.

He came back the next day and asked these customers what job they hired the milkshake to do. He found that most customers had a long, boring commute and wanted something to make the drive more interesting. They weren't hungry yet but would be by 10 a.m. and were in a hurry with only one free hand because they were driving. This needed something tidy and distracting. Trying to suck a thick liquid through a straw gave these commuters something to do. So, the fast-food chain made milkshakes that were thicker to last through the commute and more interesting (with chunks of fruit). Milkshake sales increased drastically.

The idea is that customers don't just buy products. They hire solutions to get various jobs done. The theory helps us understand what customers actually want and value. It allows us to gain new insights on how we can innovate with the business.

Reference:
[1] https://hbswk.hbs.edu/item/6496.html

Innovation Key Questions

- How do we create value for our stakeholders?
  - That is the essence of strategy
- How do we innovate?
- Why does anyone need us?
  - What the problem is that needs to be solved
  - The aspiration that needs to be fulfilled

At the heart of disruptive innovation and jobs to be done theory is the question of creating value for our customers. What problems do stakeholders have that we can make better? The answer to this question is the essence of strategy.

By figuring out how to innovate with the business, we as the security team can increase our value. Oftentimes, the value that the security team provides is not clear. By identifying the problems that our key stakeholders need solved, we can help them fulfill the goals of the larger organization.

Tips for Your Security Team

- Never ask for the money
- Instead, articulate the vision
  - How will you solve a problem being faced by your key stakeholders?
- By stating the problem and the aspiration:
  - You can increase commitment
  - You can turn stakeholders into partners

Simon Sinek is an author well known for creating the concept of the "golden circle," which describes how great leaders inspire others by starting with "why" instead of the "how" or the "what." He states, "People don't buy what you do, they buy why you do it."[1] An example from his book, *Start with Why*, helps illustrate this point:

"Samuel Pierpont Langley set out in the early 1900s to be the first man to pilot an airplane. Highly regarded, he was a senior officer at the Smithsonian Institution, a mathematics professor who had also worked at Harvard. His friends included some of the most powerful men in government and business, including Andrew Carnegie and Alexander Graham Bell. Langley was given a $50,000 grant from the War Department to fund his project, a tremendous amount of money for the time. He pulled together the best minds of the day, a veritable dream team of talent and know-how. Langley and his team used the finest materials, and the press followed him everywhere. People all over the country were riveted to the story, waiting to read that he had achieved his goal."[2]

Just a few hundred miles away, Wilbur and Orville Wright were also working on their own flying machine. They had no grants, no funding, no powerful connections, no advanced degrees, or even college educations. The odds were stacked against them, but on December 17, 1903, they successfully got a man to take flight for the first time in history. Why did the Wright Brothers succeed where Langley did not? They had a passion to fly that inspired all those around them. Their team didn't just want a job, they wanted to be part of the mission. Langley, on the other hand, quit shortly after hearing about the Wright Brothers' success.

When asking for funding, never ask for the money. Instead, articulate the vision. By stating the problem and your aspiration, you can increase commitment and turn stakeholders into partners. "People don't buy what you do, they buy why you do it."[1]

References:
[1] https://www.youtube.com/watch?v=sioZd3AxmnE
[2] https://www.startwithwhy.com/Books.aspx

In Summary

- Stakeholders don't value expertise
  - They value results
- By understanding what they value:
  - We can learn to innovate with the business

"The best way to predict the future is to invent it."
- Alan Kay

When thinking about the future, about innovation, or about jobs to be done, the common theme is understanding "why" something needs to be done. By selling your vision and understanding what your key stakeholders' value is, you can create results that further business innovation. Your stakeholders aren't interested in how many vulnerabilities you patched, how many attacks were blocked, or how many scans you conducted. But, tying those important security activities to the results that they are driving toward can help you create results that transform stakeholders into partners.

This page intentionally left blank.

CYBER42

Event #4

Debrief

This page intentionally left blank.

Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Define Current State
  - Vision and Mission
    - Lab #1: Mission Statement
  - SWOT Analysis
    - Lab #2: SWOT Exercise
- Develop the Plan
  - Visioning and Innovation
  - ***Security Framework***
  - Security Roadmap
    - Gap Analysis
    - Lab #3: Roadmap Development
  - Business Case Development
- Deliver the Program
  - Security Metrics Program
  - Marketing and Exec Communications

This page intentionally left blank.

Security Framework

- Goals of this section:
  - Introduce a framework that can be used to provide a high-level view of the security program
  - Learn how to convey maturity of the security program

Recently, Paul Williams's teams completed a SWOT analysis. Since then, Paul has met with a number of C-level executives and business unit leaders to learn more about the organization and how security can contribute. It's clear from these conversations that these other leaders don't understand security. He decides to utilize an industry-defined framework to frame his strategic plan and convey the maturity of the security program in a way that is understandable to senior executives.

Need for a Security Framework

- Security frameworks provide a blueprint for:
  - Building security programs
  - Managing risk
  - Communicating about security
- Many frameworks share common security concepts
- Common *program* frameworks include:
  - ISO 27000 Series
    - 27001: ISMS requirements
    - 27002: Code of practice
    - 27003: Implementation guidance
    - 27004: Measurement
    - 27005: Risk management
  - COBIT
  - ENISA Evaluation Framework
  - ISF Standard of Good Practice
  - NIST Cybersecurity Framework

Security frameworks provide a blueprint for building security programs, managing risk, and communicating about security using a common vocabulary. There are many security-related frameworks, and it might sometimes be difficult to decide which one to use. Fortunately, many of these frameworks share common security concepts. Some common examples include:

ISO 27000
The ISO 27000 series was developed by the International Standards Organization and provides a broad information security framework.[1] It is applicable to any industry and can be used to map to multiple regulations with which your organization might need to comply (for example, PCI, HIPAA, SOX, and FFIEC). ISO 27001 defines the requirements for the program, whereas ISO 27002 defines the code of practice. This is a very comprehensive framework and implementation can be long and involved. Achieving ISO 27000 certification is often important for cloud service providers looking to demonstrate a rigorous security program.[2]

COBIT
COBIT is a framework for managing and governing Enterprise Information Technology (IT) of which information security is an important component. COBIT started with a focus on reducing technical risks but, with COBIT 5, has evolved to include aligning IT with business and strategic goals. It is commonly used in relation to achieving SOX compliance.

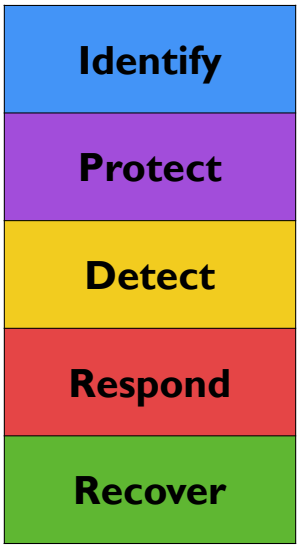
ENISA Evaluation Framework
ENISA, the European Union Agency for Network and Information Security, has published "An Evaluation Framework for National Cyber Security Strategies," which includes 1) review the cyber-security strategies of EU member states 2) identification of best practices conducted by these member states 3) development of an evaluation framework and 4) creation of key performance indicators (KPIs) to measure the security program.[3]

Information Security Forum (ISF)[4]
ISF is a not-for-profit membership-driven organization that provides tools, guidance, and consulting on information security. They have developed a Standard of Good Practice for Information Security, which defines various Control Categories and associated Guidelines that can be used to structure and manage your security program.

NIST Cybersecurity Framework
NIST, the National Institute of Standards and Technology, has published the "Framework for Improving Critical Infrastructure Cybersecurity." The framework "created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."[5]

References:
[1] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[2] http://www.isaca.org/cobit
[3] https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[4] https://www.securityforum.org
[5] https://www.nist.gov/cyberframework

NIST Cybersecurity Framework (CSF)



- Composed of three parts
  - Core, Implementation Tiers, and Profiles
- Defines a common language for managing security risk
  - Core has five functions that provide a high-level, strategic view of the security life cycle
- Helps organizations ask:
  - What are we doing today?
  - How are we doing?
  - Where do we want to go?
  - When do we want to get there?

In February 2013, President Barack Obama issued Executive Order 13636, which ordered that actions be taken to improve critical infrastructure cybersecurity.[1] One of the directives of the executive order included the creation of a cybersecurity framework. As a result, the National Institute of Standards and Technology (NIST) published the first version of the "Framework for Improving Critical Infrastructure Cybersecurity" in February 2014. It is commonly referred to as the "NIST Cybersecurity Framework" or simply the "Cybersecurity Framework."[2]

The framework consists of five functions that provide a high-level, strategic view of the life cycle of managing security risk. These five functions comprise the "Framework Core" and they are:

Identify: Planning activities to understand business needs and threats so that initiatives can be prioritized based on risk
Protect: Activities that prevent or contain the impact of security incidents
Detect: Activities that identify security incidents
Respond: Incident response activities
Recover: Activities that restore normal operations and reduce impact of security incidents

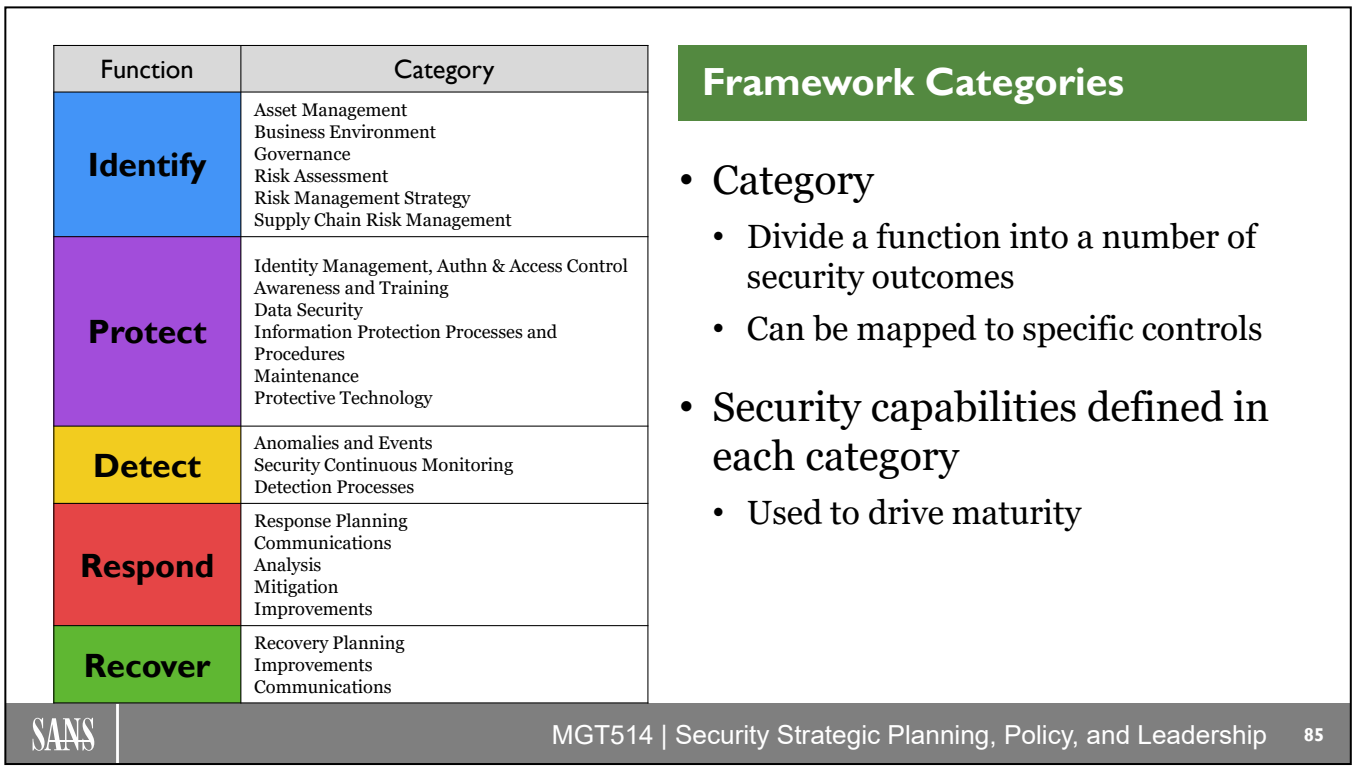
By breaking down a security program into these five functions, the framework helps organizations:

1) Describe their current cybersecurity posture.
2) Describe their target state for cybersecurity.
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
4) Assess progress toward the target state.
5) Communicate among internal and external stakeholders about cybersecurity risk.

These benefits are taken from page 9 of the framework document. [3]

Since its publication, many organization around the world have started to adopt the framework. In May 2017, President Donald Trump issued an executive order requiring U.S. federal agencies to apply the Framework to federal information systems.[4]

References:
[1] http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
[2] https://www.nist.gov/cyberframework
[3] https://doi.org/10.6028/NIST.CSWP.04162018
[4] https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure



Each high-level function is broken up into a number of categories that represent the security outcomes for that particular area. These categories can be used to drive maturity and improvements for the higher-level functions. As an example, the Identify function is composed of the following six categories:

Asset Management
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and risk strategy.

Business Environment
The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Governance
The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Risk Assessment
The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Risk Management Strategy
The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Supply Chain Risk Management
The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

Framework Subcategory Examples

Function	Category	Subcategory	Informative References
Protect	ID Mgt, Authn, Access (PR.AC)	PR.AC-1: Identities and credentials are managed PR.AC-2: Physical access to assets is managed PR.AC-3: Remote access is managed PR.AC-4: Access permissions are managed PR.AC-5: Network integrity is protected	CIS 4, 5, 6, 13, 15; NIST 800-53 AC-1, AC-2 NIST 800-53 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 CIS 4, 6, 13; NIST 800-53 AC-1, AC-17, AC-19, AC-20, SC-15 CIS 3, 5, 6; NIST 800-53 AC-1, AC-2, AC-3, AC-5, AC-16, AC-14 CIS 3, 9, 12, 13, 16; NIST 800-53 AC-4, AC-10, SC-7
	Awareness and Training (PR.AT)	PR.AT-1: All users are informed and trained PR.AT-2: Privileged users understand roles and responsibilities PR.AT-3: Third-party stakeholders understand roles and responsibilities PR.AT-4: Senior executives understand roles and responsibilities PR.AT-5: Physical & security personnel understand roles and responsibilities	CIS 14, 16, 17; NIST 800-53 AT-2, PM-13 CIS 14, 16; NIST 800-53 AT-3, PM-13 CIS 15; NIST 800-53 PS-7, SA-9, SA-16 CIS 14; NIST 800-53 AT-3, PM-13 CIS 14; NIST 800-53 AT-3, IR-2, PM-13
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected PR.DS-3: Assets are formally managed PR.DS-4: Adequate capacity to ensure availability PR.DS-5: Protections against data leaks are implemented PR.DS-6: Integrity checking mechanisms are used	CIS 3, 16; NIST 800-53 MP-8, SC-12, SC-28 CIS 3, 12, 16; NIST 800-53 SC-8, SC-11, SC-12 CIS 1, 3, 12; NIST 800-53 CM-8, MP-6, PE-16 NIST 800-53 AU-4, CP-2, SC-5 CIS 3, 16; NIST 800-53 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13 CIS 9; NIST 800-53 SC-16, SI-7
	Info Protection Processes and Procedures (PR.IP)	PR.IP-1: Baseline configuration created and maintained PR.IP-2: System Development Life Cycle implemented PR.IP-3: Configuration change control processes PR.IP-4: Backups conducted, maintained, and tested PR.IP-5: Policy and regulations of physical environment PR.IP-6: Data is destroyed according to policy PR.IP-7: Protection processes are continuously improved PR.IP-8: Effectiveness of protection technologies is shared PR.IP-9: Response and recovery plans in place PR.IP-10: Response and recovery plans are tested PR.IP-11: Cyber security is included in HR PR.IP-12: Vulnerability management plan	CIS 2, 4, 9, 16; NIST 800-53 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 CIS 16; NIST 800-53 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17 NIST 800-53 CM-3, CM-4, SA-10 CIS 9; NIST 800-53 CP-4, CP-6, CP-9 NIST 800-53 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 CIS 3; NIST 800-53 MP-6 CIS 16, 18; NIST 800-53 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 NIST 800-53 AC-21, CA-7, SI-4 CIS 9, 17; NIST 800-53 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 CIS 17; NIST 800-53 CP-4, IR-3, PM-14 CIS 6; NIST 800-53 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 CIS 7; NIST 800-53 RA-3, RA-5, SI-2
	Protective Technology (PR.PT)	PR.PT-1: Audit/log records reviewed per policy PR.PT-2: Removable media is protected PR.PT-3: Least functionality is implemented PR.PT-4: Communications and control networks protected	CIS 8; NIST 800-53 AU Family CIS 3, 10; NIST 800-53 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 CIS 2, 13; NIST 800-53 AC-3, CM-7 CIS 12; NIST 800-53 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21

The categories in the Protect function are:

Identity Management, Authentication, and Access Control (PR.AC)
Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Awareness and Training (PR.AT)
The organization's personnel and partners are provided cyber-security awareness education and are adequately trained to perform their information security–related duties and responsibilities consistent with related policies, procedures, and agreements.

Data Security (PR.DS)
Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Information Protection Processes and Procedures (PR.IP)
Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets.

Maintenance (PR.MA): Note that this category has been left off the slide due to space limitations.
Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

Protective Technology (PR.PT)
Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Each category is composed of a number of subcategories that can be mapped to specific technical or management objectives. The Cybersecurity Framework includes Informative References that refer to standards, best practices, and guidelines like the CIS Controls, NIST 800-53, and ISO 27001. This helps to map specific controls and objectives to the subcategory, category, and function.

Tips for Using the Cybersecurity Framework

- Not everyone can or should implement the full Cybersecurity Framework immediately
  - New programs
  - Small security teams
  - Small- and medium-sized businesses (SMBs)
- Goal is to provide an industry-recognized approach
  - That can be used to frame what is required by the security program

The Cybersecurity Framework defines a comprehensive set of activities that can be conducted by your security program. Depending on where you are in your journey, you might not want to implement the full framework immediately. Oftentimes, new programs can use the framework as a guiding light for what can be achieved in the future. Part of this plan has to incorporate the reality of available resources or lack thereof. Small security teams and small- to medium-sized businesses (SMBs) do not have the resources of multi-billion-dollar enterprises. Large enterprises might have dozens or hundreds of people working on information security-related activities.

In the United States, the Small Business Administration defines what constitutes an SMB based on industry, ownership structure, revenue, and number of employees. SMBs generally have up to 500 employees, but it can be as high as 1,500 in some cases. In the European Union (EU), micro-enterprises have up to 10 employees, small enterprises have up to 50 employees, and medium-sized enterprises have up to 250 employees. It's clear that an SMB with only 50 employees will not be able to dedicate 20% of its staff to security activities. The goal is not to follow any framework blindly but to frame the work of the security team in a manner that makes sense for the current business risks and landscape.

Measuring Maturity

- Can't do everything at once
  - Need to define a progression of maturity
- Implementation Tiers
  - Defined in the Cybersecurity Framework
    - Tier 4: Adaptive
    - Tier 3: Repeatable
    - Tier 2: Risk Informed
    - Tier 1: Partial

"Tiers do not represent maturity levels. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective."

- Need a way to measure maturity and determine where to invest

The Cybersecurity Framework defines four Implementation Tiers that represent an "increasing degree of rigor and sophistication in cybersecurity risk management practices." These Implementation Tiers are composed of three categories:

Tier	Risk Management Process	Integrated Risk Management Program	External Participation
Tier 1 Partial	Practices are not formalized, ad-hoc, and reactive	Limited awareness of security risk at the organizational level	No processes to coordinate with external entities
Tier 2 Risk Informed	Practices are approved by management but not by organization-wide policy	Awareness of risk organizationally but organization-wide approach to risk has not been established	No formalized capabilities to interact and share information externally
Tier 3 Repeatable	Practices formally approved and expressed as policy	Organization-wide approach to manage risk is defined	Enables collaboration with partners and receives information in response to events
Tier 4 Adaptive	Practices based on lessons learned and predictive indicators from previous and current activities	Security risk management is part of the culture and evolves based on various inputs	Actively shares information with partners before events occur

Maturity Models

- Maturity models provide a standard way to:
  - Measure organizational capabilities
  - Identify areas for improvement
- Examples include:
  - Capability Maturity Model Integration (CMMI)
  - Enterprise Strategy Group (ESG) Maturity Model
  - Gartner ITScore
  - Cybersecurity Capability Maturity Model (C2M2)
  - Building Security In Maturity Model (BSIMM)
  - Open Software Assurance Maturity Model (OpenSAMM)
  - Capability Immaturity Model (CIMM)

Maturity models provide a standard way to measure organizational capabilities and identify areas for improvement. There are many security-related maturity models. Some examples include:

Capability Maturity Model Integration (CMMI)[1]
Originally developed to measure the maturity of software development practices, the core concepts have been extended to apply to a number of other domains. It is discussed in more detail on the upcoming slides.

ESG Maturity Model[2]
The Enterprise Strategy Group (ESG) is an IT research, analysis, and strategy firm. It has created a basic security maturity model discussed on an upcoming slide.

Gartner ITScore[3]
Gartner is an IT research and advisory firm that gathers industry data and publishes it under the ITScore umbrella. ITScore allows you to compare your IT and security activities in relation to other firms and other companies in your own industry.

Cybersecurity Capability Maturity Model (C2M2)[4]
The Cybersecurity Capability Maturity Model (C2M2) was created by the U.S. Department of Energy (DOE) with work focused on the electricity and oil/gas subsectors. It has been updated so that it can be used by any organization and provides a self-evaluation methodology and toolkit.

Building Security In Maturity Model (BSIMM)[5]
The BSIMM is designed to help you understand and improve software security programs and was created by analyzing data and activities of real-world software security initiatives. While focused on software security, it contains data and concepts like strategy and risk management that are applicable to any security program.

Open Software Assurance Maturity Model (OpenSAMM)[6]
OpenSAMM is an open, vendor-neutral maturity model for improving software security from the Open Web Application Security Project (OWASP). It is used by a number of organizations to determine which software security-related activities to prioritize.

Capability Immaturity Model (CIMM)[7]
Humorously, the Capability Immaturity Model was developed as a parody to the popular Capability Maturity Model (CMM). It defines a negative scale of maturity that arises in dysfunctional organizations. It was created to highlight the fact that management of specific projects is dysfunctional because negative maturity can exist even in organizations with overall positive CMM levels. The immaturity levels include:

- Level 0: Negligent: Level 1 assumes eventual success, whereas Level 0 organizations generally fail to produce anything
- Level -1: Obstructive: Processes are implemented that tend to obstruct real work from being accomplished. For example, many government contracts require a certain level of CMM maturity. In some cases, this results in contractors performing work related to simply documenting and following CMM processes.
- Level -2: Contemptuous: Ineffective processes become institutionalized with measures of activity (e.g., test cases written, lines of code written, and hours worked) replacing measures of productivity (e.g., test success rates and % of functions completed).
- Level -3: Undermining: Rival teams downplay or sabotage efforts of other teams in a competition for scarce resources (e.g., people, funding, etc.).

References:
[1] https://cmmiinstitute.com
[2] http://resources.idgenterprise.com/original/AST-0135469_ESG-Brief-HP-Maturity-Model-Oct-2014.pdf
[3] https://www.gartner.com/doc/2507916/itscore-information-security
[4] https://en.wikipedia.org/wiki/Capability_Immaturity_Model
[5] https://www.bsimm.com
[6] http://www.opensamm.org
[7] http://en.wikipedia.org/wiki/Capability_Immaturity_Model

Enterprise Strategy Group (ESG) Security Maturity Model

Category	Basic Organizations	Progressing Organizations	Advanced Organizations
Philosophy	Cybersecurity is a "necessary evil."	Cybersecurity must be more integrated into the business	Cybersecurity is part of the culture.
People	CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.	CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled.	CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.
Process	Informal and ad-hoc. Subservient to IT.	Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors.	Documented and formal with an eye toward more scale and automation.
Technology	Elementary security technologies with simple configurations. De-centralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance.	More advanced use of security technologies and adoption of new tools for incident detection and security analytics.	Building an enterprise security technology architecture. Focus on incident prevention, detection, and response. Adding elements of identity management and data security to deal with cloud and mobile computing security.

Source: Enterprise Strategy Group, 2014.

This table is from the Enterprise Strategy Group (ESG) and was taken from an article by Brian Krebs titled "What's Your Security Maturity Level?"[1,2] It lays out a progression for basic, progressing, and advanced organizations. An important component of this is the "philosophy," which indicates where an organization might be in relation to the need for managing security risk. Many organizations are finding that it is not sufficient to view security as a "necessary evil," but that it must be more integrated into the business. In the long term, perhaps security can even become part of the culture.

References:
[1] http://resources.idgenterprise.com/original/AST-0135469_ESG-Brief-HP-Maturity-Model-Oct-2014.pdf
[2] http://krebsonsecurity.com/2015/04/whats-your-security-maturity-level/

Capability Maturity Model Integration (CMMI)

- Process model that defines what should be done to improve performance
  - Originally created to improve software development practices
  - Now expanded to cover development, services, and acquisitions
- Defines five maturity levels
  - Widely recognized and understood by executives, business leaders, and technology managers

The CMMI originally started as the CMM by the Software Engineering Institute (SEI) at Carnegie Mellon University for improving the process of software development. The CMMI supersedes the CMM and was developed by representatives from commercial, defense, government, and academic institutions and is now operated and maintained by the CMMI Institute, which is now a part of ISACA.[1]

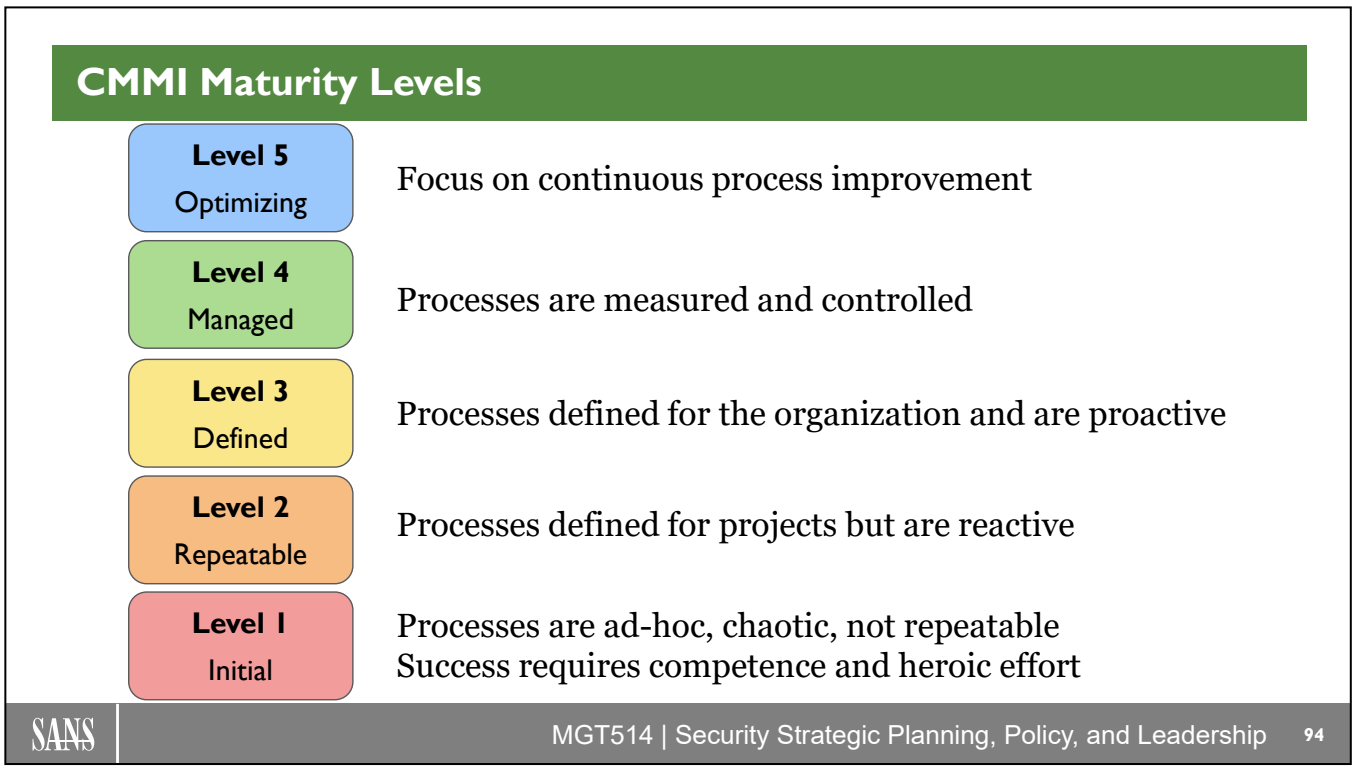
The CMMI currently addresses three areas of focus:

1) CMMI for Development (CMMI-DEV) for product and service development
2) CMMI for Services (CMMI-SVC) for service establishment and management
3) CMMI for Acquisition (CMMI-ACQ) for product service and acquisition

It is one of the most widely used and understood maturity models.

Reference:

[1] https://cmmiinstitute.com



The five-point scale utilized in the CMMI is widely recognized and understood by executives, business leaders, and technology managers.

Level 1: Initial
Information security is weak and conducted in an ad-hoc manner. Security activities are typically not repeatable and focused on technical IT tasks. No formal security program exists.

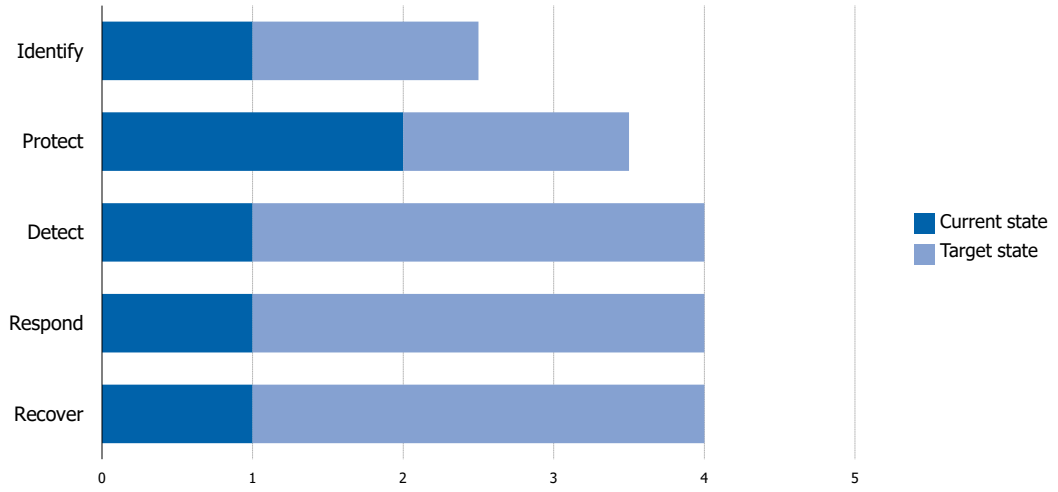
Level 2: Repeatable
Processes are defined for specific projects but are reactive. Various stakeholders are beginning to communicate about security activities.

Level 3: Defined
Policies and rules are in place and some information security roles and responsibilities are established, but there is little accountability or enforcement. Information security efforts are still primarily IT-focused, and enterprise security awareness is still limited.

Level 4: Managed
Information security roles and responsibilities are clearly defined, and a formal information security committee with participation from business unit managers has been established. The enterprise is moving away from an IT-centric approach to information security, but business unit owners have not yet accepted explicit accountability for residual risk.

Level 5: Optimizing
Business unit managers now explicitly accept the residual risk associated with their use of information and technology and are accountable for security failures and policy violations. Continuous self-improvement practices are in place and are used to create a security-aware culture in the organization.

Maturity Model Example



This is a useful way to visually represent the maturity of your security program. On the x-axis, we are using the five-point scale from the Capability Maturity Model. The y-axis has the five functional areas defined in the NIST Cybersecurity Framework. The current state and future state are clearly identified on the associated bars for each function. In this example, you can see that the Protect function has a higher maturity than the other areas. Perhaps this was by design or perhaps this is a result of an unintentional overinvestment in preventive security capabilities. By laying out security maturity in this manner, these types of trends can be identified and addressed by the leadership team.

Assessing Security Maturity

- FFIEC Cybersecurity Assessment Tool
  - Helps institutions identify risk and cybersecurity preparedness
  - Defines five security domains
    - Cyber Risk Management and Oversight
    - Threat Intelligence and Collaboration
    - Cybersecurity Controls
    - External Dependency Management
    - Cyber Incident Management and Resilience
- Financial Services Sector Cybersecurity Profile
  - Defines impact based on:
    - National/Super-National, Subnational, Sector, Localized

Two tools that help assess the state of security specifically designed for the financial services industry:

FFIEC Cybersecurity Assessment Tool
FFIEC, the Federal Financial Institutions Examination Council, is a U.S. government body composed of five banking regulators that prescribes principles, standards, and forms for financial institutions in the United States. In 2015, they released their Cybersecurity Assessment Tool which helps leaders at financial institutions understand their security expectations, increase security awareness and knowledge of risks, and helps them assess and mitigate these risks.[1,2]

The term "Assessment" in the name of the tool is a bit of a distractor as it is not simply an assessment tool. It helps financial institutions measure cybersecurity maturity across the five domains below. It even has a mapping to the NIST Cybersecurity Framework.

Domain 1: Cyber Risk Management and Oversight
Domain 2: Threat Intelligence and Collaboration
Domain 3: Cybersecurity Controls
Domain 4: External Dependency Management
Domain 5: Cyber Incident Management and Resilience

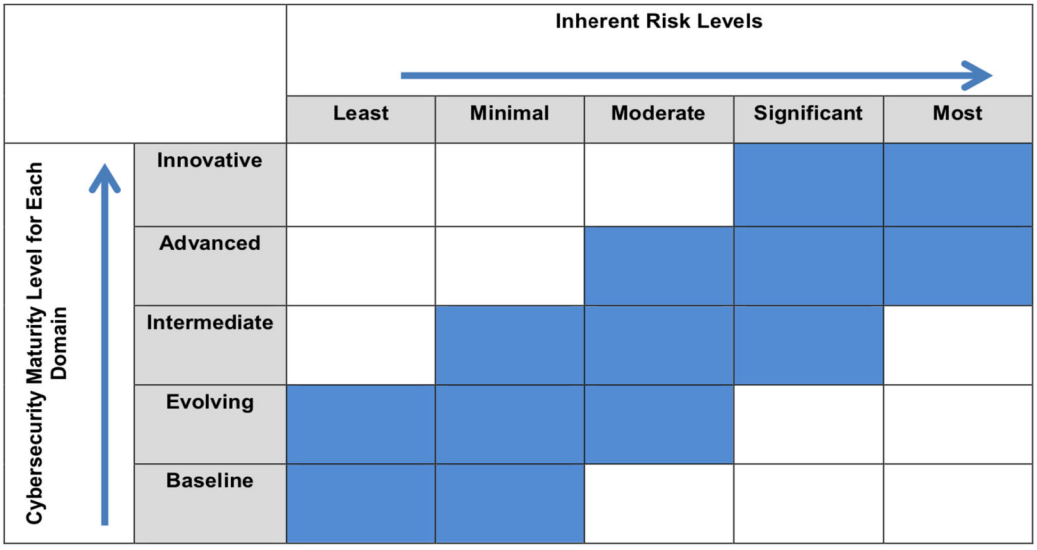
Financial Services Sector Cybersecurity Profile
FSSCC, the Financial Services Sector Coordinating Council, has a mission to strengthen the financial sector against attacks and other threats to critical infrastructure. Their Financial Services Sector Cybersecurity Profile ("Profile") can be used to assess security of the target organization. Its design is based on the NIST Cybersecurity Framework's five functions, categories, and subcategories as well as the FFIEC Cybersecurity Assessment Tool.[3]

The Profile extends upon these tools by adding Diagnostic Statements, which simplify overlapping requirements, and includes an “Impact Tiering” questionnaire to identify the potential market risk presented by financial institutions of differing complexity and sizes. The Profile defines the Tiers as follows:

> **Tier 1: National/Super-National Impact:** These institutions are designated most critical and assumes the cyber risk exposure of an institution would have the most potential adverse impact to the overall stability of the North American economy, and potentially, the global market.
> **Tier 2: Subnational Impact:** These institutions provide mission critical services with millions of customer accounts. This category assumes the cyber risk exposure of an institution or service would have the potential for a substantial adverse impact to the financial services sector and subnational regional economy.
> **Tier 3: Sector Impact:** These institutions have a high degree of interconnectedness, with certain institutions acting as key nodes within, and for, the sector. The nature of the services that these institutions provide to the sector plays a significant role in determining their criticality.
> **Tier 4: Localized Impact:** These institutions have a limited impact on the overall financial services sector and national economy. Typical characteristics include: (a) institutions with a local presence and less than 1 million customers (e.g., community banks, state banks); and (b) providers of low criticality services.

References:
[1] https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf
[2] https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf
[3] https://cyberriskinstitute.org/the-profile

FFIEC CAT Maturity Levels



The FFIEC CAT defines by Maturity Levels and Inherent Risk Levels.

As an organization's inherent risk level increases (from Least, Minimal, Moderate, Significant, Most) then the maturity level should change as well. Over time as threats, vulnerabilities, and operational environments change, this Maturity will change between Baseline, Evolving, Intermediate Advanced, and Innovative. As a result, management must reevaluate the risk profile regularly.

The CAT defines specific thresholds for different risk levels. Here is an example for "Cloud computing services hosted externally to support critical activities":[1]

Least: No cloud providers
Minimal: Few cloud providers; private cloud only (1– 3)
Moderate: Several cloud providers (4–7)
Significant: Significant number of cloud providers (8– 10); cloud-provider locations used include international; use of public cloud
Most: Substantial number of cloud providers (>10); cloud-provider locations used include international; use of public cloud

Reference:
[1] https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

Security Controls

- Strong security controls are the foundation of any program
  - This class is not intended to be a comprehensive review of control standards
- Commonly used *control* frameworks include:
  - NIST SP 800-53
  - Critical Security Controls (CSC)
  - Australian Signals Directorate (ASD) Mitigation Strategies

The maturity of individual security capability areas (e.g., functions) is driven by the maturity of the people, process, and technology of associated security controls. Strong security controls are at the heart of any security program. There are a number of commonly used control standards, including:

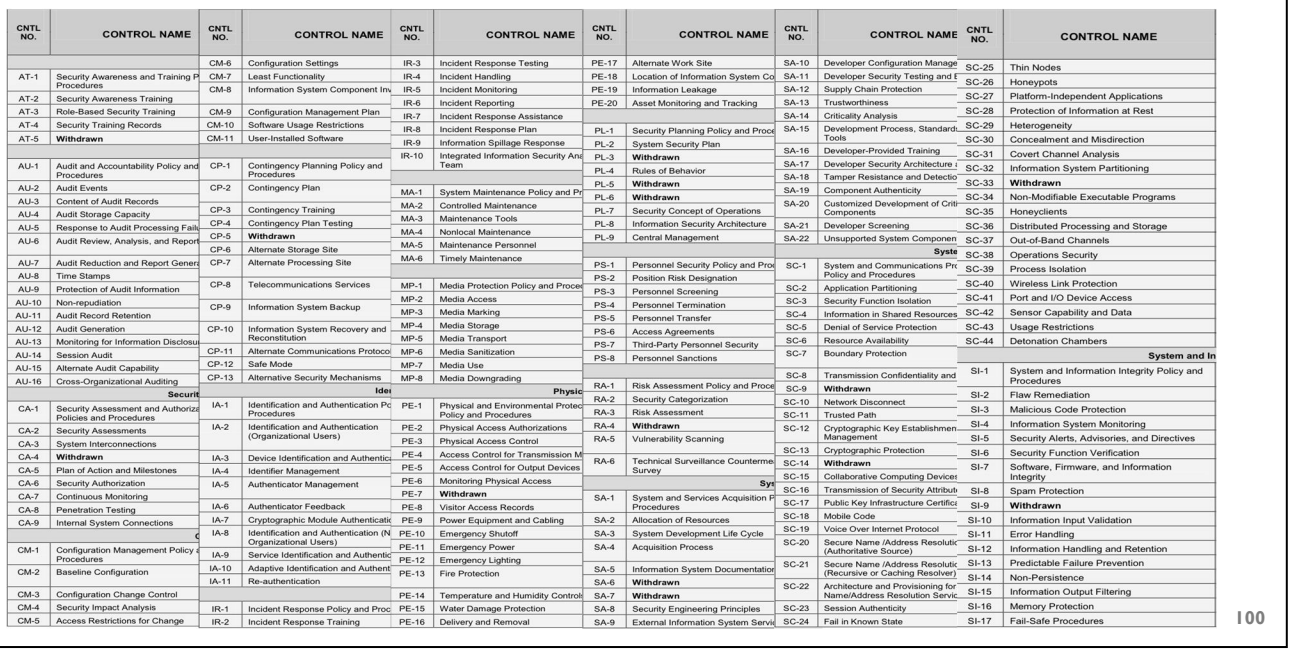
NIST SP 800-53
This is the standard required by U.S. government agencies to comply with the Federal Information Processing Standards (FIPS) 200 requirements. Although NIST SP 800-53 was created with government agencies in mind, it can also be applied to other industries and has been used as a model upon which other frameworks have been initiated.[1]

CIS Controls
The CIS Controls are recommended actions that provide actionable ways to thwart the most pervasive attacks.[2]

ASD Strategies to Mitigate Cyber Security Incidents
The Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) have developed "Strategies to Mitigate Cyber Security Incidents" by analyzing cyber incidents, vulnerability assessments, and penetration tests conducted for various Australian government agencies.[3] This list of strategies is ranked based on effectiveness, which has been calculated by including user resistance, upfront costs, and maintenance costs.

References:
[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[2] https://www.cisecurity.org/controls
[3] https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

NIST SP 800-53



CNTL NO.	CONTROL NAME
AT-1	Security Awareness and Training P Procedures
AT-2	Security Awareness Training
AT-3	Role-Based Security Training
AT-4	Security Training Records
AT-5	**Withdrawn**
AU-1	Audit and Accountability Policy and Procedures
AU-2	Audit Events
AU-3	Content of Audit Records
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failu
AU-6	Audit Review, Analysis, and Report
AU-7	Audit Reduction and Report Gener
AU-8	Time Stamps
AU-9	Protection of Audit Information
AU-10	Non-repudiation
AU-11	Audit Record Retention
AU-12	Audit Generation
AU-13	Monitoring for Information Disclosu
AU-14	Session Audit
AU-15	Alternate Audit Capability
AU-16	Cross-Organizational Auditing
	Securit
CA-1	Security Assessment and Authoriz Policies and Procedures
CA-2	Security Assessments
CA-3	System Interconnections
CA-4	**Withdrawn**
CA-5	Plan of Action and Milestones
CA-6	Security Authorization
CA-7	Continuous Monitoring
CA-8	Penetration Testing
CA-9	Internal System Connections
	C
CM-1	Configuration Management Policy Procedures
CM-2	Baseline Configuration
CM-3	Configuration Change Control
CM-4	Security Impact Analysis
CM-5	Access Restrictions for Change

CNTL NO.	CONTROL NAME
CM-6	Configuration Settings
CM-7	Least Functionality
CM-8	Information System Component Inv
CM-9	Configuration Management Plan
CM-10	Software Usage Restrictions
CM-11	User-Installed Software
CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan
CP-3	Contingency Training
CP-4	Contingency Plan Testing
CP-5	**Withdrawn**
CP-6	Alternate Storage Site
CP-7	Alternate Processing Site
CP-8	Telecommunications Services
CP-9	Information System Backup
CP-10	Information System Recovery and Reconstitution
CP-11	Alternate Communications Protoco
CP-12	Safe Mode
CP-13	Alternative Security Mechanisms
	Ide
IA-1	Identification and Authentication Po Procedures
IA-2	Identification and Authentication (Organizational Users)
IA-3	Device Identification and Authentic
IA-4	Identifier Management
IA-5	Authenticator Management
IA-6	Authenticator Feedback
IA-7	Cryptographic Module Authenticati
IA-8	Identification and Authentication (N Organizational Users)
IA-9	Service Identification and Authentic
IA-10	Adaptive Identification and Authent
IA-11	Re-authentication
IR-1	Incident Response Policy and Proc
IR-2	Incident Response Training

CNTL NO.	CONTROL NAME
IR-3	Incident Response Testing
IR-4	Incident Handling
IR-5	Incident Monitoring
IR-6	Incident Reporting
IR-7	Incident Response Assistance
IR-8	Incident Response Plan
IR-9	Information Spillage Response
IR-10	Integrated Information Security Ana Team
MA-1	System Maintenance Policy and Pr
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-4	Nonlocal Maintenance
MA-5	Maintenance Personnel
MA-6	Timely Maintenance
MP-1	Media Protection Policy and Proce
MP-2	Media Access
MP-3	Media Marking
MP-4	Media Storage
MP-5	Media Transport
MP-6	Media Sanitization
MP-7	Media Use
MP-8	Media Downgrading
	Physic
PE-1	Physical and Environmental Protec Policy and Procedures
PE-2	Physical Access Authorizations
PE-3	Physical Access Control
PE-4	Access Control for Transmission M
PE-5	Access Control for Output Devices
PE-6	Monitoring Physical Access
PE-7	**Withdrawn**
PE-8	Visitor Access Records
PE-9	Power Equipment and Cabling
PE-10	Emergency Shutoff
PE-11	Emergency Power
PE-12	Emergency Lighting
PE-13	Fire Protection
PE-14	Temperature and Humidity Controls
PE-15	Water Damage Protection
PE-16	Delivery and Removal

CNTL NO.	CONTROL NAME
PE-17	Alternate Work Site
PE-18	Location of Information System Co
PE-19	Information Leakage
PE-20	Asset Monitoring and Tracking
PL-1	Security Planning Policy and Proce
PL-2	System Security Plan
PL-3	**Withdrawn**
PL-4	Rules of Behavior
PL-5	**Withdrawn**
PL-6	**Withdrawn**
PL-7	Security Concept of Operations
PL-8	Information Security Architecture
PL-9	Central Management
PS-1	Personnel Security Policy and Proc
PS-2	Position Risk Designation
PS-3	Personnel Screening
PS-4	Personnel Termination
PS-5	Personnel Transfer
PS-6	Access Agreements
PS-7	Third-Party Personnel Security
PS-8	Personnel Sanctions
RA-1	Risk Assessment Policy and Proce
RA-2	Security Categorization
RA-3	Risk Assessment
RA-4	**Withdrawn**
RA-5	Vulnerability Scanning
RA-6	Technical Surveillance Counterme Survey
	Sy
SA-1	System and Services Acquisition P Procedures
SA-2	Allocation of Resources
SA-3	System Development Life Cycle
SA-4	Acquisition Process
SA-5	Information System Documentatio
SA-6	**Withdrawn**
SA-7	**Withdrawn**
SA-8	Security Engineering Principles
SA-9	External Information System Servi

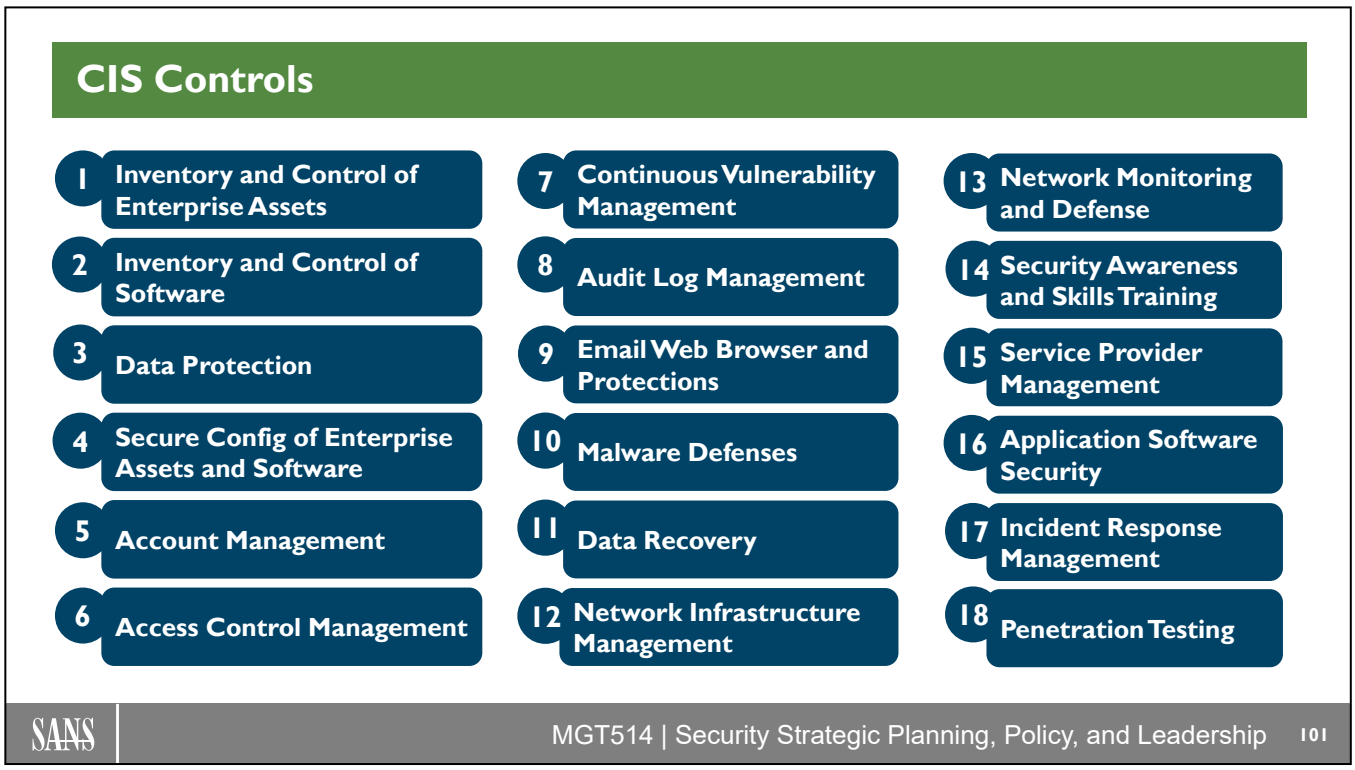
CNTL NO.	CONTROL NAME
SA-10	Developer Configuration Manage
SA-11	Developer Security Testing and E
SA-12	Supply Chain Protection
SA-13	Trustworthiness
SA-14	Criticality Analysis
SA-15	Development Process, Standard Tools
SA-16	Developer-Provided Training
SA-17	Developer Security Architecture
SA-18	Tamper Resistance and Detectio
SA-19	Component Authenticity
SA-20	Customized Development of Criti Components
SA-21	Developer Screening
SA-22	Unsupported System Componen
	Syste
SC-1	System and Communications Pr Policy and Procedures
SC-2	Application Partitioning
SC-3	Security Function Isolation
SC-4	Information in Shared Resources
SC-5	Denial of Service Protection
SC-6	Resource Availability
SC-7	Boundary Protection
SC-8	Transmission Confidentiality and
SC-9	**Withdrawn**
SC-10	Network Disconnect
SC-11	Trusted Path
SC-12	Cryptographic Key Establishmen Management
SC-13	Cryptographic Protection
SC-14	**Withdrawn**
SC-15	Collaborative Computing Device
SC-16	Transmission of Security Attribu
SC-17	Public Key Infrastructure Certific
SC-18	Mobile Code
SC-19	Voice Over Internet Protocol
SC-20	Secure Name /Address Resolutio (Authoritative Source)
SC-21	Secure Name /Address Resolutio (Recursive or Caching Resolver)
SC-22	Architecture and Provisioning for Name/Address Resolution Servic
SC-23	Session Authenticity
SC-24	Fail in Known State

CNTL NO.	CONTROL NAME
SC-25	Thin Nodes
SC-26	Honeypots
SC-27	Platform-Independent Applications
SC-28	Protection of Information at Rest
SC-29	Heterogeneity
SC-30	Concealment and Misdirection
SC-31	Covert Channel Analysis
SC-32	Information System Partitioning
SC-33	**Withdrawn**
SC-34	Non-Modifiable Executable Programs
SC-35	Honeyclients
SC-36	Distributed Processing and Storage
SC-37	Out-of-Band Channels
SC-38	Operations Security
SC-39	Process Isolation
SC-40	Wireless Link Protection
SC-41	Port and I/O Device Access
SC-42	Sensor Capability and Data
SC-43	Usage Restrictions
SC-44	Detonation Chambers
	System and In
SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-4	Information System Monitoring
SI-5	Security Alerts, Advisories, and Directives
SI-6	Security Function Verification
SI-7	Software, Firmware, and Information Integrity
SI-8	Spam Protection
SI-9	**Withdrawn**
SI-10	Information Input Validation
SI-11	Error Handling
SI-12	Information Handling and Retention
SI-13	Predictable Failure Prevention
SI-14	Non-Persistence
SI-15	Information Output Filtering
SI-16	Memory Protection
SI-17	Fail-Safe Procedures

100

These are screenshots from the NIST Special Publication 800-53 revision 4 document titled, "Security and Privacy Controls for Federal Information Systems and Organizations."[1] NIST 800-53 is a comprehensive control catalog containing a large number of security controls that you can potentially use in your program.

Reference:
[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

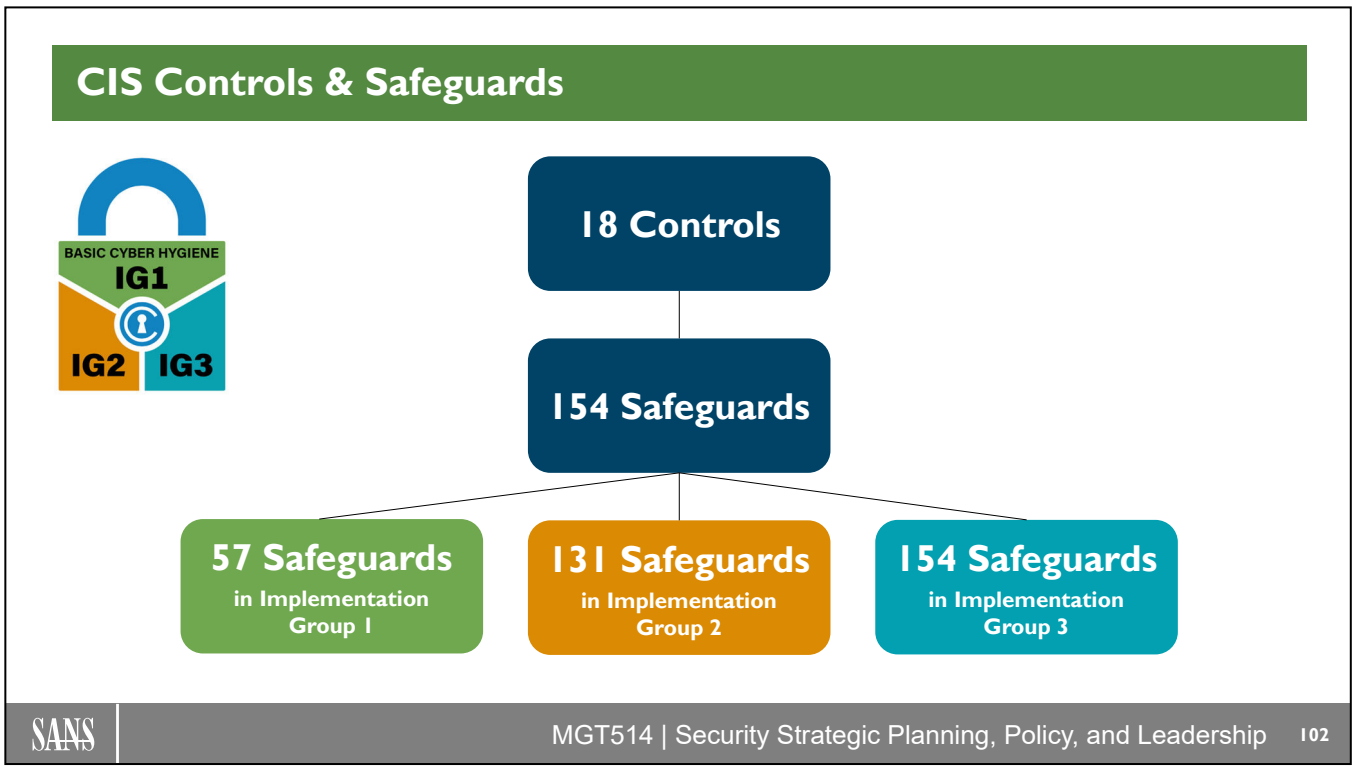


The CIS Controls, formerly known as the Critical Security Controls (CSC), are currently managed and maintained by the Center for Internet Security (CIS) and were originally released in 2008.[1] The most recent version 8 was released in 2021 after extensive community feedback and vetting. This helps ensure that the Controls are in the right order and are aligned with the latest threat information.

The CIS Controls help security leaders focus our time, talent, and resources to identify controls that map to known attacks, prioritize implementation of security controls, and map security controls to various compliance and regulatory requirements.

As you review the eighteen CIS Controls, it is easy to get overwhelmed. Be encouraged – you really can do them and do them very well! Some examples follow of organizations that made a significant increase in their security posture by remaining focused and creating intentional projects to help solve for these discrete items over the course of several years. You are encouraged to start with the foundational controls since they represent the essentials for what the Center for Internet Security calls basic cyber hygiene. When these foundational controls are in place, working on the remaining Controls will be less of a burden, since many of the other controls can take advantage of these and serve to make later Controls easier to achieve.

Reference:
[1] https://www.cisecurity.org/controls/



It can be a little confusing when we say that there are 18 CIS Controls as people might think, "Great, I should be able to get these 18 controls implemented in no time." However, a closer reading reveals that there are actually 154 total Safeguards (i.e., sub-controls) as CIS refers to them. This is much less than the 1190 controls and control enhancements in NIST 800-53, but it is still a lot.

In prior versions CIS implied that people could implement basic, foundational, and organizational controls which were numbered in ascending order. However, this sequential approach proved to be too simplistic. Many organizations struggled to complete even the basic controls. As a result, CIS adopted an approach based on Implementation Groups (IG). These are a subset of the Controls that the community has assessed as being appropriate for small to large organizations. Since each IG builds on the prior one a smaller organization can focus on IG1 (basic cyber hygiene) while a large enterprise can focus on IG3 with incremental improvements along the way.

CIS defines the Implementation Groups[1] as follows:
"An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks.
An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Safeguards selected for IG2 help security teams cope with increased operational complexity.
An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks."

Reference:
[1] https://www.cisecurity.org/controls/implementation-groups

Mapping Controls to the Security Framework

- CIS Mapping
  - Maps CIS Controls to NIST CSF
- NIST Informative References Program
  - Maps NIST 800-53 controls to CSF and many more
- Secure Controls Framework (SCF)
  - Maps various controls to different international standards and the Secure Controls Framework (SCF)
  - Created by Tom Cornelius

The primary control guidance utilized in SANS courses are the CIS Controls. However, different organizations might already use various security frameworks and control guidance. To help people rationalize the activities of their program with the Controls, CIS has published a spreadsheet[1] that maps each of the CIS Controls and Safeguards to the corresponding NIST CSF Subcategory. NIST themselves have also published a spreadsheet as part of their Informative References Program[2] that does the same thing but with the NIST 800-53 controls mapped to the NIST CSF Subcategories.

Finally, the Secure Controls Framework (SCF)[3] is an online tool that lets you specify a multitude of international standards and mandates to map to each other. It was created by Tom Cornelius and provides mappings to over 100 international security mandates, standards, and compliance frameworks. The "comprehensive listing of nearly 750 cybersecurity and privacy controls is categorized into 32 domains that are mapped to over 100 statutory, regulatory and contractual frameworks." In addition to a spreadsheet containing all mappings, you can customize the SCF by specifying just the mandates that apply to your organization.[4] These include mandates from the following categories as outlined by the SCF:

Statutory Obligations: Laws (e.g., US state, federal and international laws)
Regulatory Obligations: Requirements from regulatory bodies or governmental agencies
Contractual Obligations: Requirements that are stipulated in contracts, vendor agreements, etc.
Industry Recognized Practices: Requirements that are based on an organization's specific industry that are considered reasonably expected practices

Moreover, the SCF provides a Security Privacy Maturity Model (SP-CMM) that defines criteria to establish expectations for security and privacy programs. Each SCF control has SP-CMM level 0-5 defined, which you can use to track maturity.

References:
[1] https://www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-nist-csf
[2] https://csrc.nist.gov/projects/olir/informative-reference-catalog/details/10024
[3] https://www.securecontrolsframework.com/download-scf
[4] https://www.securecontrolsframework.com/customize-the-scf

Third-Party Certifications

- SOC 2 Type II
  - Focuses on five Trust Services Principles
    - Privacy, Security, Availability, Processing Integrity, Confidentiality
  - Addresses operational effectiveness of specified controls over a specified time
- ISO 27001
  - Validates that the information security management system (ISMS) is properly designed, implemented, and in operation
- FedRAMP
  - US government program that defines standard security approach for cloud products and services

Up to this point, we have discussed different frameworks that you can use to build your security program. Depending on your business requirements, you may also need to obtain independent validation from a third-party that your security program is following industry best practices. This requires that you implement a certain set of controls and have an external auditor certify that you have met certain requirements. There are various third-party certifications used in different industries and parts of the world, but we focus here on three of the most common:

System and Organization Controls (SOC)[1]
If you are a "service organization", you likely need to obtain a SOC report to prove to your customers that you have appropriate security controls in place. The SOC requirements are defined by the American Institute of Certified Public Accountants (AICPA) and include a review of up to five different Trust Services principles: Privacy, Security, Availability, Processing Integrity, and Confidentiality. You define the scope of your SOC audit by choosing the specific Principles you want reviewed.

There are three different types of SOC audits that you can obtain:
SOC 1 – review of financial reporting controls
SOC 2 – review of the Trust Services Principles controls
SOC 3 – same as the SOC 2 but the resulting report is intended for general use

For information security purposes, the SOC 2 is the most commonly obtained report. But it gets just a little more confusing because you can obtain two levels of SOC reports: Type I or Type II. The Type I report simply describes the controls you have in place while the Type II describes the controls and their effectiveness over a specified period of time. The Type II report is typically what most service organizations obtain.

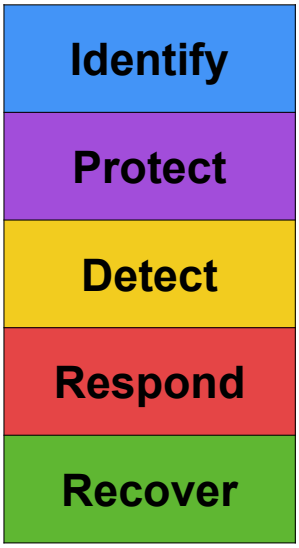
ISO 27001[2]
Certification audits are conducted by ISO 27001 lead auditors and consists of two phases:
Stage 1 – Informal review of the ISMS, associated documentation, and policy
Stage 2 – More detailed compliance audit and independent testing of the ISMS. Confirms that the program is properly designed, implemented, and in operation. This includes ensuring that a security leadership committee meets regularly to oversee the program.

FedRAMP[3]
This is a US government program that provides a standardized approach to security for cloud products and services. The program was started “to provide a cost-effective, risk-based approach for the adoption and use of cloud services to Executive departments and agencies.”[4]Audits are conducted by third-party assessment organizations that are accredited by the American Association for Laboratory Accreditation (A2LA). FedRAMP requires specific certified cloud services and platforms to be used.

References:
[1] https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html
[2] http://www.27000.org/ismsprocess.htm
[3] https://www.fedramp.gov/
[4] https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf

In Summary

- Difficult to communicate need for security controls
  - Board, CEO, CFO, and business leaders don't understand security
  - Security often seen as a tax
- Utilizing a simple framework, we can highlight:
  - What security is doing
  - Areas of risk
  - Areas of over or under investment



With the growing number of data breaches and cyber intrusions, business leaders have an understanding of the importance of cybersecurity and the need to effectively manage security risks. However, these same business leaders have a difficult time understanding what it is that security needs to accomplish and how much should be invested. This is understandable. These business leaders are not and should not be expected to be security experts. They want to know the risk to the organization, what security is doing about it, and any areas that need additional investment. Using a commonly understood framework, like the NIST Cybersecurity Framework, can help frame the work of the security team in an easier-to-understand manner. By determining the current and target state maturity of these various capability areas, the security team can greatly improve the dialogue with senior business leaders.

Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Define Current State
  - Vision and Mission
    - Lab #1: Mission Statement
  - SWOT Analysis
    - Lab #2: SWOT Exercise
- Develop the Plan
  - Visioning and Innovation
  - Security Framework
  - ***Security Roadmap***
    - Gap Analysis
    - Lab #3: Roadmap Development
  - Business Case Development
- Deliver the Program
  - Security Metrics Program
  - Marketing and Exec Communications

This page intentionally left blank.

Security Roadmap

- Goals of this section:
  - Learn the steps for developing a roadmap for your security program
  - Understand how previous steps in the strategic planning process assist in developing your roadmap

In this section, you will learn the steps for creating a roadmap for your security program and how previous steps in the strategic planning process inform that roadmap.

Gap Analysis Overview

- Gap analysis consists of three steps
  - Identify future state
  - Analyze current situation
  - Define initiatives that bridge the gap
- In our PharmaCo scenario, Paul has already:
  - Defined future state
    - At a very high level
  - Analyzed current state
    - Using historical analysis, asset analysis, PEST, and SWOT
- Now he needs to bridge the gap
  - And take the plan to the next level of detail

Gap Analysis consists of performing three steps:

1) Identifying the future state
2) Analyzing the current situation
3) Defining initiatives that bridge the gap between current and future state

It's been nearly six months since you had dinner with your good friend, Paul Williams. When you last spoke, he had just taken a job at PharmaCo as CISO. At dinner, you can tell that it has been an exhausting six months trying to get his arms around the scope and scale of security at such a large enterprise. The good news is that he seems to have established a number of strong relationships and has a good understanding of not just the strengths and weaknesses of his team, but also what is most valuable to the business.

He put forward a seemingly simple security vision to "Help people lead healthier lives by creating safe spaces for drug research and innovation." Historically, security at PharmaCo was treated as just an IT issue related to locking down the network and associated PCs. His business partners found it refreshing that he wanted to know what was most important to them; namely getting new drugs to market faster. He incorporated this into his security vision and, coupled with his personal relationships, was able to start a dialogue about how security could be an enabler. Now he needs to flush out the details of the high-level plan and identify specific actions and projects that he needs to initiate.

Gap Analysis – Current and Future

Function	Current Situation	Initiatives	Future State
Identify	Security is decentralized across business units		Centralized security governance to provide comprehensive risk management
Protect	Security protections are not consistently applied		Protect key systems and processes used for drug research, development, & trials
Detect	Inability to detect malicious or negligent activity		Ability to quickly detect threats targeting intellectual property
Respond	Inability to mitigate attacks and limit the amount of data lost		Ability to minimize data loss, block attacks, and determine root cause
Recover	Recovery and business continuity is decentralized		Capability to quickly return to normal operations and limit business impact of incidents

In our example, Paul Williams has already defined the future state at a very high level. Through the visioning process and conversations with C-level and business leaders, he has identified a vision for security at PharmaCo: "Help people lead healthier lives by creating safe spaces for drug research and innovation." His engagement with senior leaders in developing this mutually agreed-upon vision is key. It turns stakeholders into partners by obtaining their buy-in. Paul has also done the hard work of analyzing the current state of the organization using historical analysis, understanding the values and culture of the organization, and performing a SWOT analysis. This helps ensure that he understands current organizational obstacles, determines the norms for getting work done, and identifies areas of strength and weakness. Now, Paul just needs to identify actions that will bridge the gap.

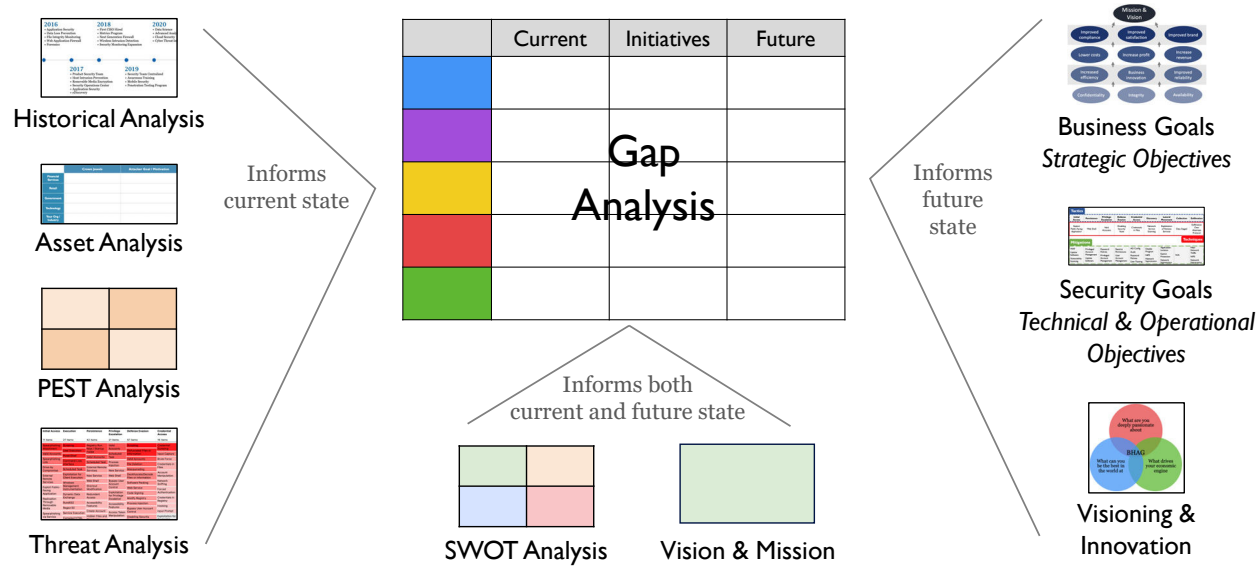
Based on his analysis, Paul has mapped his security team's weaknesses to the five functions from the Cybersecurity Framework:

- **Identify**: Security is decentralized across business units.
- **Protect**: Security protections are not consistently applied.
- **Detect**: Inability to detect malicious or negligent activity.
- **Respond**: Inability to mitigate attacks and limit the amount of data lost.
- **Recover**: Recovery and business continuity is decentralized.

He has also identified the future state goal for each of these five functions:

- **Identify**: Centralized security governance to provide comprehensive risk management
- **Protect**: Protect key systems and processes used for drug research, development, and trials
- **Detect**: Ability to quickly detect threats targeting intellectual property
- **Respond**: Ability to minimize data loss, block attacks, and determine root cause
- **Recover**: Capability to quickly return to normal operations and limit business impact of security incidents

Gap Analysis Inputs



Gap Analysis helps you identify key actions to improve your program. These actions can be qualitative or quantitative. For example, using metrics like "reducing response time by 25%" or "increasing ability to detect advanced threats by 20%" can help your team identify specific measures that need to be taken to reach the goal.

Oftentimes, security teams focus on technology-based solutions. It's important to remember that technology is just one component of the overall solution. Based on your understanding of the organization (from Historical Analysis, Asset Analysis, PEST, and Threat Analysis), you need to be aware of key obstacles and constraints that might exist in the organization. For example, a culture without a strong focus on process can make it difficult for the security team to implement new process-driven initiatives that require regular input from key business stakeholders. Additionally, certain influential people in the organization might not agree with certain security activities (Stakeholder Management). As a leader and manager, you have to recognize these obstacles and develop the appropriate countermeasures to ensure the success of your initiatives based on the organization's Vision and Mission and the current state as summarized in the SWOT.

Gap Analysis – Sample Initiatives

Function	Current Situation	Initiatives	Future State
Identify	Security is decentralized across business units	Create steering committee Develop central policy library Implement vuln management program	Centralized security governance to provide comprehensive risk management
Protect	Security protections are not consistently applied	Decrease patch deployment time Protect clinical trial systems Deploy systems in blocking mode	Protect key systems and processes used for drug research, development, and trials
Detect	Inability to detect malicious or negligent activity	Deploy continuous monitoring and log management capability Advanced analytics and reporting Implement DLP to monitor IP loss	Ability to quickly detect threats targeting intellectual property
Respond	Inability to mitigate attacks and limit the amount of data lost	Build and staff 24x7 SOC Develop advanced forensics team Create threat intelligence capability	Ability to minimize data loss, block attacks, and determine root cause
Recover	Recovery and business continuity is decentralized	Develop business continuity plan Regularly test response plan Socialize and communicate with BUs	Capability to quickly return to normal operations and limit business impact of incidents

This slide identifies some potential actions that PharmaCo could take to improve its security program. For example, in the "Identify" row, the current state of security being decentralized across business units can make it more challenging to provide comprehensive governance and risk management. Creating a steering committee with overall enterprise accountability for security risk can help move the organization toward a more centralized governance structure. Developing a centralized policy library will also help. It's important to keep in mind, though, that just having a central policy library alone will not drive the organization. Establishing a policy steering committee with representation from key stakeholders helps institutionalize the work of the security team and helps ensure that key stakeholders are engaged in the process of governing the organization.

As another example, in the "Detect" row, the current state is an inability to detect malicious or negligent activity. This includes key intellectual property that might be lost or stolen. One potential solution is implementing a Data Loss Prevention (DLP) capability. However, in addition to the technology, it is important to remember identifying a business owner for this new initiative will be key. The business owner must weigh in on what constitutes intellectual property and what actions should be taken to mitigate risk.

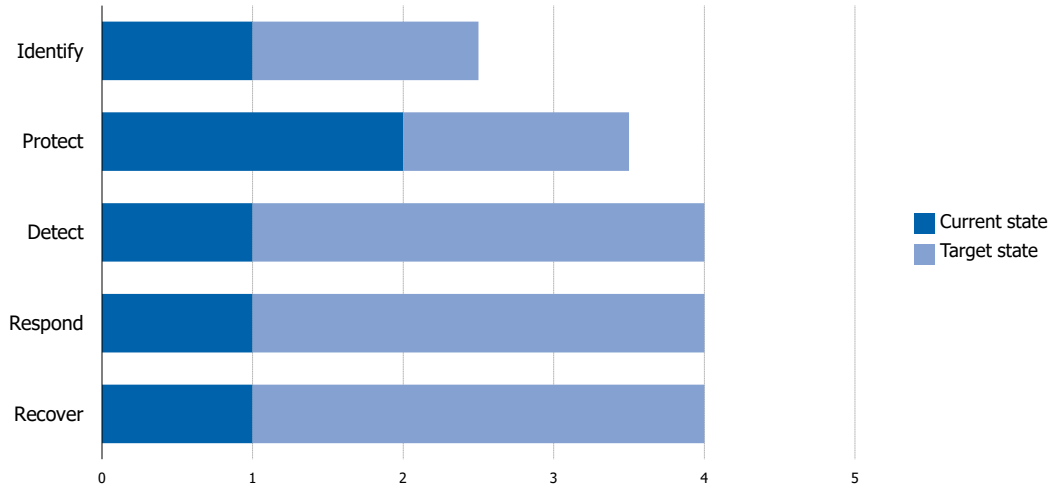
There are a number of potential actions listed on this slide that can be taken by the security team. However, they can't all be done at the same time. The next step is to develop a roadmap for ordering these important initiatives.

PharmaCo Case Scenario

- Paul Williams and his team:
  - Completed the gap analysis
  - Identified numerous initiatives to close gaps
  - Want to move forward with implementing solutions
- Don't have resources to do everything at once
  - Budget and staff need to be put in place
  - Can only mature security capabilities at the rate
    - At which the organization can accept them
    - That you can successfully deploy them

Paul Williams and his team have completed the gap analysis and identified numerous initiatives to close the gaps. They are eager to move forward on implementing solutions but don't have the resources to do everything at once. It takes time to put the budget and corresponding staff in place. Additionally, it takes time to implement new capabilities. Paul recognizes that it can take 3-5 years to build and mature a world-class security program and that he can roll out new capabilities only at the rate at which the larger organization can accept them. As a result, he is rightly focused on developing a roadmap that lays out the activities of the security program in the step-wise fashion.

Maturity Model Example



This is the example maturity model from a previous section that shows the current state and target state for each of the five Cybersecurity Framework functions. Given the amount of work it takes to get from Level 1 to Level 4, it should be obvious that this cannot be accomplished overnight. Instead, this slide is a reminder that we have to make a gradual progression in improving the maturity of the security program.

Roadmap Development

Three-step process:

1) Document what is being done today
2) Map current capabilities to maturity levels
3) Prioritize new initiatives to increase maturity

Developing a roadmap consists of three steps:

1) **Document what is being done today**
   By cataloging the work of the security team, you not only begin to identify what else needs to be done, but you also take credit for all the work that has been done to date. Don't underestimate the power of highlighting to leadership everything that the team has and is currently working on.

2) **Map current capabilities to maturity levels**
   Ideally, the framework that you utilize will define capabilities that are required for each maturity level. However, many frameworks often do not get into enough detail to provide useful guidance in measuring current state maturity. This is in part due to the fact that every organization is, in fact, different. This is why various consulting firms offer maturity assessments because they can normalize information that they receive from various assessments across their customer base. Different organizations have different priorities and business drivers that affect where they are and where they might want to go on their security journey. As a result, the identification of specific capabilities in maturity level can sometimes be specific to the organization at hand.

3) **Prioritize new initiatives to increase maturity**
   With the understanding that security initiatives can be organization-specific, the final step is to prioritize the work so that it can be done in an order that provides the most value for the organization.

Step 1: Document Current Capabilities

- Document current activities
  - Must take credit for work done to date
- Examples from the "Protect" function include:
  - VPN, firewall, and network segmentation
  - Endpoint encryption, antivirus, and antimalware
  - Web single sign-on (SSO)
  - Awareness training
  - Security standards

Step 1 of roadmap development includes identifying current capabilities. What is it that the security team does today?

As an example, let's take the "Protect" function of the Cybersecurity Framework. This function includes many traditional security capabilities like network security (e.g., VPN, firewall, and network segmentation), endpoint protection (e.g., encryption, antivirus, and antimalware), authentication (e.g., SSO), as well as training and standards. Identifying the work done to date helps inform subsequent steps.

Step 2: Map to Maturity Levels

Function	Category	Level 1	Level 2	Level 3	Level 4	Level 5
Protect	Access Control	VPN Firewall Segmentation	Web SSO	Federated SSO		
	Awareness and Training	Basic awareness training	Phishing exercises			
	Data Security	Encryption data at rest and in-transit	Data segregation Asset destruction			
	Processes and Procedures	Security standards Change control	Integration with HR processes Incident response plan	Security development process		
	Protective Technology	Network and host security	Web application security program	Mobile application security		

Done today (regular font)
Started doing (underline)
Start immediately (bold italic)
Plan to start (italic)

Step 2 of roadmap development includes mapping the initiatives identified in the previous step to specific maturity levels. For example, most people would agree that "basic" protections like VPN and firewall are Level 1 capabilities. On the slide, you can see that they are part of the "Access Control" category defined in the Cybersecurity Framework. More advanced capabilities would be implemented at higher maturity levels.

It's also useful to differentiate items that are done today, items that you have started doing, and items that you should start immediately or plan to start sometime in the future.

Step 3: Prioritize New Initiatives

- Determine which initiatives to prioritize to bridge the gap
  - Cost should not be the only factor
  - Incorporate business value and threat defense
  - Takes into account the ability to execute and organizational support

Step 3 of roadmap developing includes prioritizing initiatives. What should be done first? A number of factors should be taken into account when prioritizing new initiatives including cost, value to the business, ability to defend against threats, and the ability to actually execute on the work and implement the solution.

Decision Matrix Analysis

- Tool to rank initiatives and inform decisions
  - While taking multiple factors into account
- Rank each factor from 0-5

Initiative	Cost	Ability to Execute	Stakeholder Support	Threat Defense	Total
Initiative #1					
Initiative #2					
Initiative #3					
Initiative #4					
Initiative #5					

Decision Matrix Analysis is a simple tool that can be used to rank initiatives and inform your decision making. It is the simplest form of Multiple Criteria Decision Analysis (MCDA) and provides a way for you to rank multiple factors in your decision making. In this example, we are ranking initiatives based on four key factors:

1) **Cost**
   How much does this initiative cost? Will we get a better bang for the buck by investing in a different initiative? Again, this should be only one factor in your decision-making process.

2) **Ability to Execute**
   If we decide to move forward with a specific initiative, do we have the skills and ability to execute? If we want to build an advanced analytics capability, do we even have basic analysis capabilities on hand to serve as a foundation? Or, do we need to hire an entirely new skill set?

3) **Stakeholder Support**
   This item is meant to encompass overall business support and value. Do our key stakeholders value the initiative? What problem is it solving for them? Have we articulated the vision appropriately?

4) **Threat Defense**
   How well does this capability protect us against existing and emerging threats? Does it allow us to detect threats more effectively? Is there overlap with other security capabilities?

Decision Matrix Analysis Example

- Simple tool to start ranking initiatives

Initiative	Cost	Ability to Execute	Stakeholder Support	Threat Defense	Total
Mobile and BYOD	3	5	5	4	17
DLP	2	3	4	5	14
Centralized Vulnerability Management	2	4	3	5	14
Risk-Based Authentication	3	3	4	3	13
Network Access Control	1	2	2	4	9

This slide lists five sample initiatives from the PharmaCo Gap Analysis in a previous section.

In the "Cost" column, a higher number indicates a more favorable score in that the initiative is not that expensive. For example, overhauling the network design to implement Network Access Control is an expensive proposition and received a low score of "1." In the other columns (Ability to Execute, Stakeholder Support, and Threat Defense), higher scores also indicate a better ability to deliver on those initiatives.

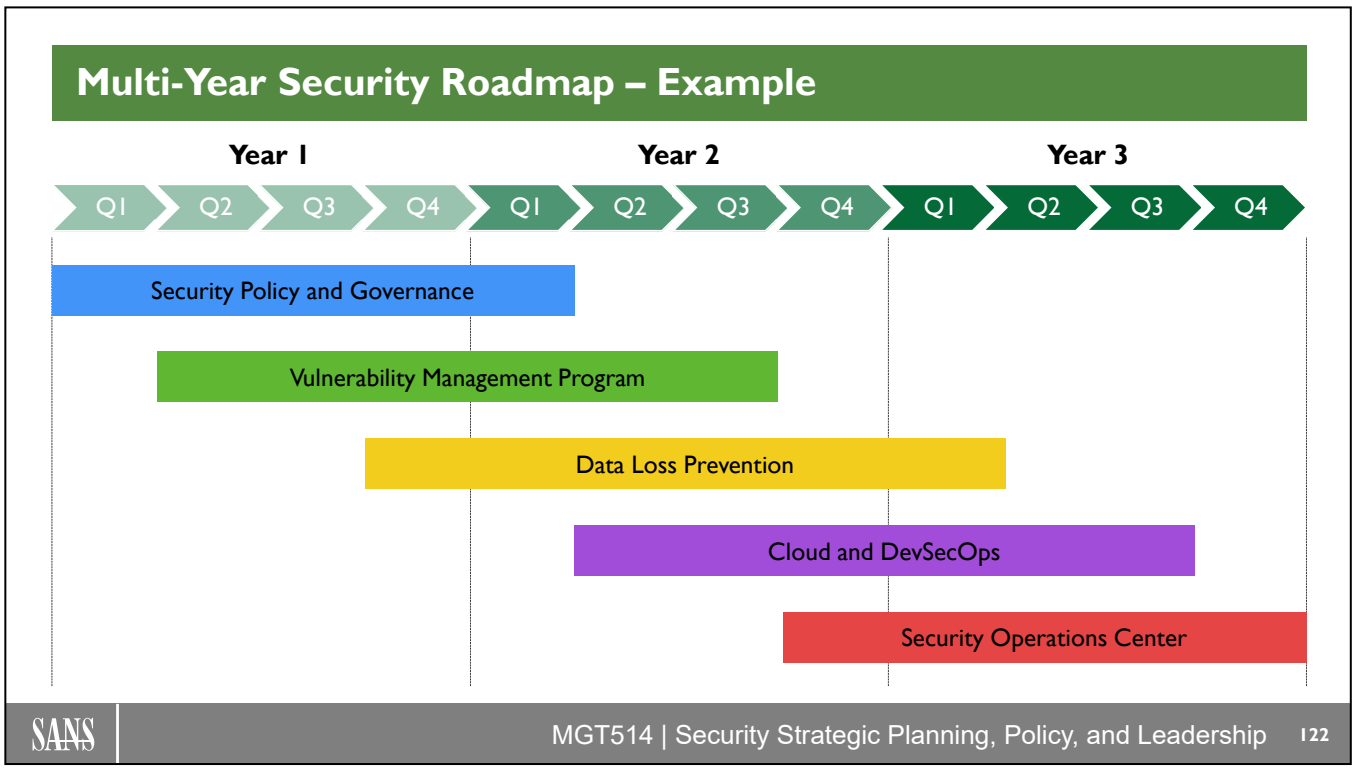
The "Total" column simply adds up the scores of the other columns. This simple analysis can be modified to weigh certain factors more heavily than others. For example, in an extremely cost-conscious organization, you might weigh the "Cost" column more heavily, whereas, in a very consensus-driven organization, you might weigh "Stakeholder Support" more heavily.

Protect Function Example Roadmap

Function	Category	Level 1	Level 2	Level 3	Level 4	Level 5
Protect	Access Control	VPN Firewall Segmentation	Web SSO	Federated SSO	***Risk-based authentication***	*Network Access Control*
	Awareness and Training	Basic awareness training	Phishing exercises	***Role-based training***	*Executive education*	*Third-party training program*
	Data Security	Encryption data at rest and in-transit	Data segregation Asset destruction	***DLP (email and host)***	***DLP (cloud data storage)***	*Self-protecting data*
	Processes and Procedures	Security standards Change control	Integration with HR processes Incident response plan	Security development process	***Centralized vulnerability management***	*Continuous feedback with business processes*
	Protective Technology	Network and host security	Web application security program	Mobile application security	***BYOD security***	*Cloud security program*

Done today (regular font) ***Start immediately*** (bold italic)
Started doing (underline) *Plan to start* (italic)

Once the analysis is complete and you have prioritized your new initiatives, you can update your roadmap table to look something like the following. By placing different initiatives at varying maturity levels and marking them as "Done today," "Started doing," and "Start immediately," you convey to leadership that you have a plan (that follows a high-level framework) for improving the maturity of the security program. At this point, based on detailed project plans and staffing estimates, you can also assign target dates to the various initiatives and maturity levels.



Once you have identified the gaps and corresponding security projects to fill those gaps, it is useful to aggregate that work into higher-level projects. For example, your Vulnerability Management Program might include enhancing an asset inventory, acquiring and deploying various scanning solutions, developing a vulnerability prioritization mechanism, creating regular reports and dashboards, and ultimately creating processes to remediate discovered vulnerabilities. By aggregating these more discrete steps into a higher-level initiative that spans multiple years, you can better communicate to senior leadership the overall plan and track corresponding progress.

Lab 2.3: Roadmap Development

Estimated Time: 20 Minutes

- Goal of this exercise
  - See how a roadmap can be developed for an initiative
- Read the case study
  - Read the case study below and review the cloud adoption model on the next slide
- Answer these questions on the next page:
  - How would you tier the work associated with cloud adoption?
  - What needs to be done to implement the cloud adoption model?

READ

Read the case study below

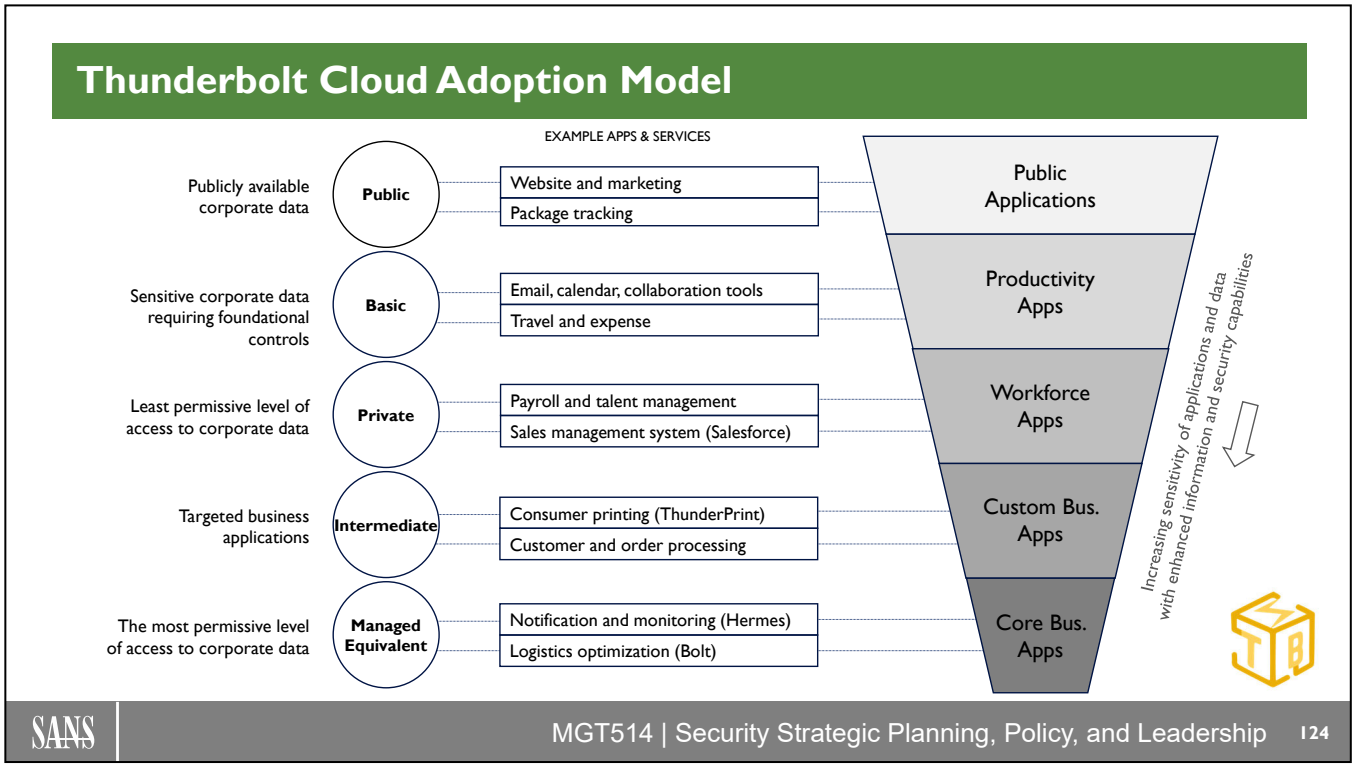
It takes 5-10 minutes to read the case and review the diagram

The Road Ahead

Franks realizes that, as the CISO, she needs to find a way to support the cloud migration. It is inevitable. As a result, she has to get her team on board and trained to support this key business directive. As reticent as she has been about the cloud there are definitely benefits. Sure, she and her team won't have seemingly the identical level of control and visibility to corporate data but leveraging modern technology could have benefits to her security operations as well.

The meeting to discuss the cloud migration strategy is right around the corner. She needs to provide direction and guidance to both her team and to the other leaders in the organization. In a spark of inspiration, she sketches out an approach which she calls the Cloud Adoption Model.

She wonders how her colleagues will take this. Will it be enough to show that security has a plan?



After reading the case and reviewing the cloud adoption model above, answer these two questions:

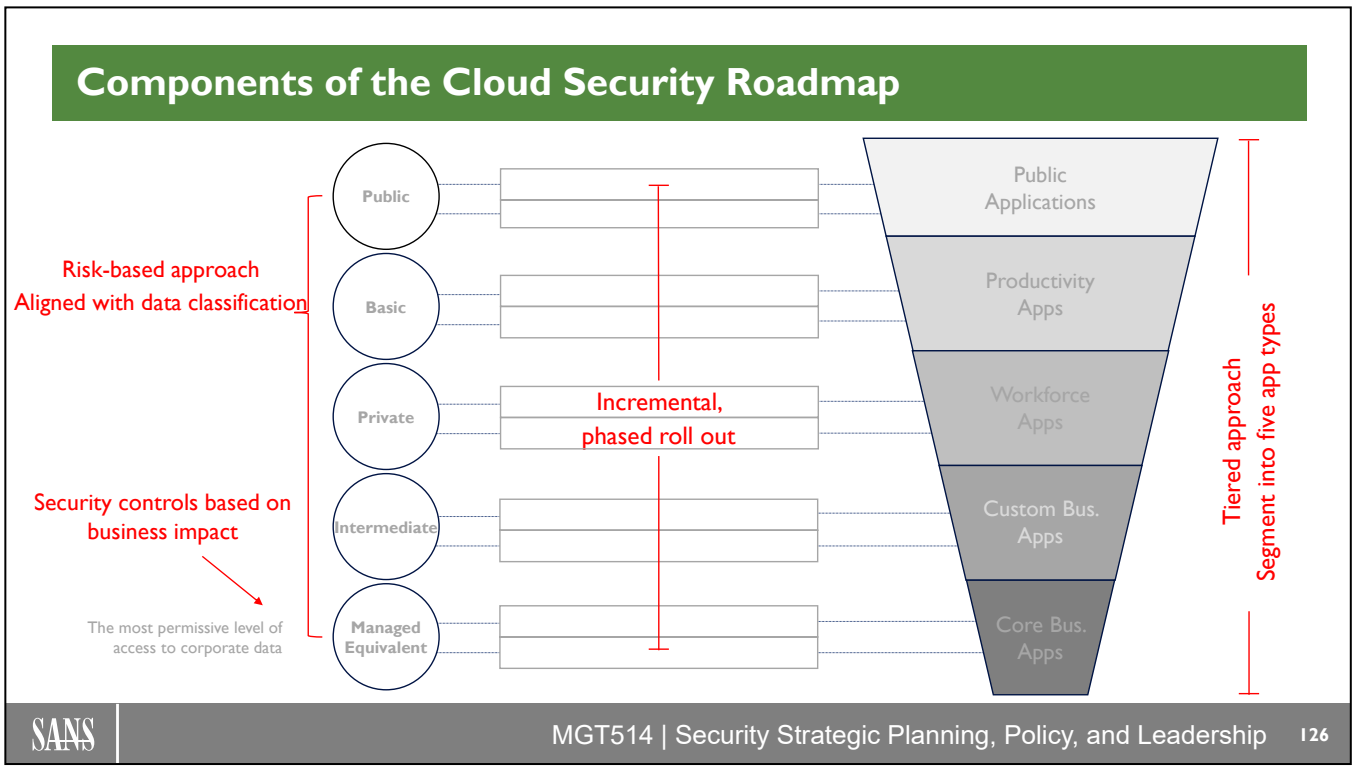
1) How is Thunderbolt tiering the work associated with cloud adoption?

2) What needs to be done to implement the cloud adoption model?

Lab Debrief

Note that this section contains a debrief and potential exercise answers

This page intentionally left blank.



With a diverse set of business units and applications Leslie Franks (CISO) understands that it's not feasible to move all systems to the cloud simultaneously. People need to be trained and plans put in place based on the benefits to the business. So, she has mapped the cloud migration plans to a data classification and overall risk management model.

By segmenting the types of applications into five different levels, Thunderbolt can develop a roadmap for increasing security controls as it provides access to increasingly sensitive data.

For example, "Basic" functionality in the cloud encompasses common productivity apps such as email, calendar, and other collaboration tools. As we learned in the case, Thunderbolt has already moved these types of applications to the cloud. At the next level, migration of "Private" functionality would require additional oversight and reviews. The "Intermediate" level is where security will need to work with the development teams to ensure that appropriate controls and processes are put in place to enable a more thorough cloud security architecture.

It's important to note the language for "Managed Equivalent." Stating that it is the "most permissive level of access" focuses on risk to the organization and the importance of systems like Bolt and Hermes. Typically, security might call this tier the "most locked down access." Thunderbolt has flipped the language to focus on the positive. We see this on the original diagram where it says, "Increasing sensitivity of applications and data with enhanced information and security capabilities." This, while true, is also a great bit of marketing.

Scaling Your Strategic Plan

- How can you create a comprehensive roadmap for the entire org?
  - Diverse business units, product teams, and technologies in different areas
- Steps
  - Start from the bottom up
  - Apply the strategic planning process to different scopes
    - Project, initiative, security program, business unit
  - Segment and categorize your crown jewels
  - Find common themes (group big ideas)
  - Connect the dots and highlight related items
    - Simply the core message
    - Highlight differences across business units

We just looked at an example of the components that can be included in a roadmap for a specific initiative (i.e., cloud security). Prior to that, we discussed how you could create a roadmap for your overall security program. In a sense a roadmap is just a higher-level project plan that defines what you want to achieve and by what time.

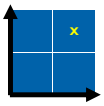
In some cases it may be more challenging to create this roadmap. The author has encountered numerous situations where you may want to create a comprehensive roadmap for your entire organization. However, this is complicated by the fact that there are numerous business units around the world with their own objectives, different product teams with their own agendas, and various technology teams using different tools. In such cases it can be hard to create one single strategic plan and roadmap.

Not to worry as we suggest just sticking with the strategic planning process you have learned throughout this course. Start from the bottom up applying the strategic planning tools to different scopes (e.g., specific project, overall security program, different business units). As you do this analysis you will see that each area has differing business assets. Segment these crown jewels into different buckets (like you saw in the Thunderbolt cloud adoption model) and find common themes. Connect these dots to highlight related items. This helps to show that you have taken all the input and simplified in a way that others can understand. Then, by highlighting the differences across business units you also show that you have a deeper understanding of the business.

In Summary

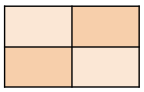
- Topics we have covered in the strategic planning process:
  - Leads up to the creation of your roadmap
- Understanding of the business and threats make it much easier to create your roadmap

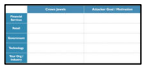

Historical Analysis


Stakeholder Management

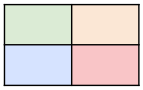

Strategy Map


Vision & Mission


PEST Analysis


Asset Analysis


Threat Analysis


SWOT Analysis

In many respects, the roadmap is the end product of the strategic planning. All the activities that you previously conducted to understand the business (e.g., Vision and Mission, Strategy Map, Stakeholder Analysis), understand the threats (e.g., Threat Analysis), and analyze current state (e.g., Values and Culture, SWOT) have led you to this roadmap. Although it appears simple, all the deep thinking, analysis, and relationship building you performed throughout the process have made it much easier for you to create the roadmap.

Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Define Current State
  - Vision and Mission
    - Lab #1: Mission Statement
  - SWOT Analysis
    - Lab #2: SWOT Exercise
- Develop the Plan
  - Visioning and Innovation
  - Security Framework
  - Security Roadmap
    - Gap Analysis
    - Lab #3: Roadmap Development
  - ***Business Case Development***
- Deliver the Program
  - Security Metrics Program
  - Marketing and Exec Communications

This page intentionally left blank.

Business Case

- Goals of this section
  - Learn approaches to building a business case
    - How to justify your resource requests
  - Understand the components of a business case
    - Most companies have a formal business case template

In this section, you will learn approaches to building a security business case. Typically, IT security investments are a "cost of doing business" because they do not generate a return on investment. As a result, it's extremely critical that your resource requests have appropriate justification. By understanding the basic components of a business case and leveraging formal business case templates that you might have in your organization, you can gain improved support for your security initiatives.

Why Create a Business Case?

- Executive leadership is responsible for making sound decisions on the effective use of company resources
  - Business case helps estimate the costs and benefits of various initiatives
  - Helps management determine resource allocations
    - Level of effort and upcoming projects
    - Understand broader organizational constraints

Before gaining support for our security initiatives, we must understand that executive leadership is looking at security as just one risk and opportunity that needs to be addressed. By creating a comprehensive business case, we help management prioritize and determine appropriate resource allocations. For example, should executive leadership invest in new factory upgrades that could improve production or invest a portion of that money in improving information security? By providing a business case that clearly lays out the estimated costs and associated benefits, we put executive leadership in a position to make sound decisions that incorporate broader organizational constraints.

What Is a Business Case?

- Captures the reason for initiating the effort
  - Includes underlying assumptions and rationale
- Clearly estimates the cost and benefits
  - This usually means revenue
- Provides a detailed description and analysis of the initiative
  - Can be created in many forms including document, presentation, or spreadsheet

Simply put, a business case captures the reason for an initiative. It lays out a problem and the potential solution(s). Typically, this involves a new investment that could result in increased revenue. But, in the case of information security, the hard costs are usually associated with softer benefits. The more details that can be included in the analysis will go a long way in making executives more comfortable with your funding request. Your organization might have a standard template that includes documents, presentations, and spreadsheets for analysis.

Security Business Case Traps

- "If we don't do this, we'll get hacked"
- "It's the right thing to do"
- "This new technology will solve all our problems"
- "It doesn't cost that much"
- "Management doesn't get it"

Technical security professionals sometimes get frustrated with executive management for a perceived lack of interest in information security. To them, it seems obvious that a lack of security investment will result in getting hacked. Building out advanced security capabilities are obviously the "right thing to do." Sometimes, solutions are technology focused: "This new technology will solve all our problems." These reasons, which presume that "Management doesn't get it," will not get you support or funding. Instead, the focus should be on building a comprehensive business case that incorporates a number of different factors for justifying the investment.

Approaches to Building a Security Business Case

- Cost approach
  - How much does it cost to recover?
- Industry comparison approach
  - What are comparable firms doing and paying?
- Business innovation approach
  - What can I gain from doing this?

Before getting into the approaches to building a security business case, let's talk about the three approaches for appraising real estate. When you get an appraisal of your home, the report includes three approaches for calculating value:

1) **Cost approach:** How much would it cost to rebuild your home if it was destroyed?
2) **Sales comparison approach:** What are others paying for similar homes? This typically is calculated on a cost-per-square-foot basis.
3) **Income approach:** What is the revenue that I can make on this property?

The most appropriate appraisal method depends on the type of property and the type of buyer. For commercial real estate (e.g., office buildings), appraisers might prefer the income approach. For single-family homes, the sales comparison approach is preferred. And for special-use properties (e.g., marina), appraisers might prefer the cost approach. The key word here is *prefer* because the choice of a valuation method can depend upon the circumstances. For example, a single-family home that is located in a neighborhood with primarily rental units might prefer a combination of the sales comparison and income approaches. All three approaches can inform the value of the property.

We can take a similar approach to building a security business case by focusing on the following:

1) **Cost approach:** If I get breached, how much will it cost to recover?
2) **Industry comparison approach:** What are comparable firms doing and paying?
3) **Business innovation approach:** What can I gain from investing in security?

Cost Approach

- Typically calculated using cost-per-record lost
  - Overestimates cost of large breaches
  - Underestimates cost of small breaches
- Ponemon Cost of Data Breach Study
  - $164 USD per record global average
  - This includes direct and indirect costs
    - Engaging forensics experts, free credit monitoring
    - In-house investigations and communication
    - Extrapolated value of customer loss
- Verizon analyzed cyber insurance claims data
  - Resulted in an estimated loss of only 58 cents per record

Every year, the Ponemon Institute publishes its Cost of Data Breach Study,[1] which analyzes security breaches around the world. Over time, the cost-per-record lost has been gradually increasing. Specifically, the figure increased from $146 to $164 USD per record from 2020 to 2022. There is also significant variation among different parts of the world as shown by the average cost of data breach in Turkey being $1.11M versus the United States being $9.44M USD.

These numbers include direct costs such as engaging forensics experts, providing free credit monitoring to affected customers, as well as conducting in-house investigations and communications. Also included are indirect costs such as customer loss, diminished customer acquisition rates, reputational damage, and loss of goodwill.

You have to be careful using this cost-per-record lost. A simple, linear cost calculation would result in overestimating the cost of large breaches by a significant amount. On the other end of the spectrum, a linear cost-per-record approach would also underestimate the cost of small breaches. This is perhaps one reason why Ponemon does not include data breaches of more than 102,000 records in its analysis.

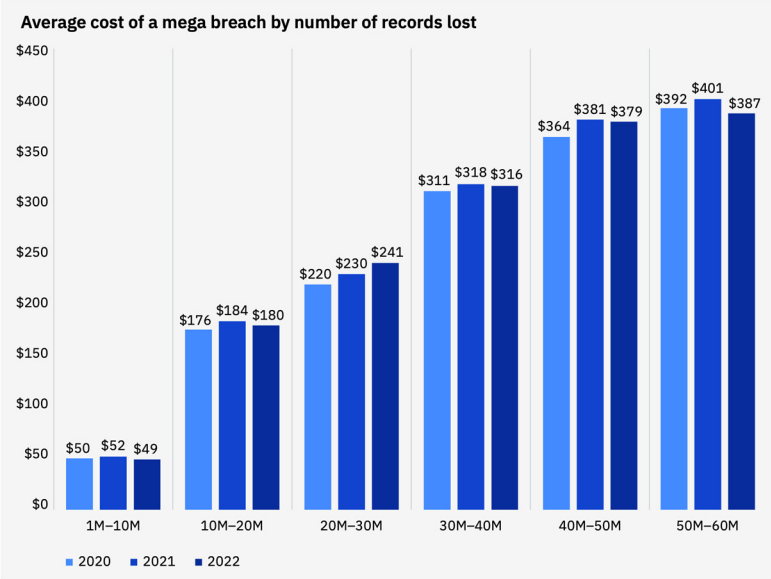
Given this issue, what other data can be used to inform the cost approach? In a prior Data Breach Investigations Report, Verizon started to develop a modified approach.[2] They analyzed data provided by NetDiligence about real losses paid on 191 cyber insurance claims. By conducting a log-scale analysis instead of a linear cost-per-record analysis, it estimated breach costs of only 58 cents per record! This low figure is problematic because indirect costs aren't included in the insurance claim data. Obviously, this isn't very helpful.

References:
[1] Ponemon Cost of Data Breach Study, https://www.ibm.com/reports/data-breach
[2] http://www.verizonenterprise.com/verizon-insights-lab/dbir

Ranges of Expected Loss

- Ponemon analyzed mega breaches
  - Breaches of 1 to 60 million records
- Cost-per-record lost
  - Ranges from $7.74 to $49 USD

Measured in USD millions



Ponemon[1] advises that the cost-per-record lost should not be used to simply calculate the cost of what they refer to as a "mega breach" which is defined as a breach of more than one million compromised records. To get a better idea of the cost of a mega breach they studied 13 companies that experienced breaches of 1 to 60 million records. Using this data set they conducted a Monte Carlo simulation to generate 150,000 random outcomes. The results of these trials are shown above.

Smaller mega breaches of 1-10 million records have an average cost of $49M USD. The larger mega breaches of 50-60 million records have a higher cost of $387M USD. This results in a much lower and more reasonable cost per record loss of between $7.74 and $49.00. Note that this is calculated by taking the data of the larger sized breaches ($387M average cost / 50M records lost) and the data of the smallest sized breach ($49M average cost / 1M records lost) . Of course, this is still an imperfect calculation, but it is much more realistic than that global $164 per record average. Providing more realistic ranges makes your business case that much more sensible.

Reference:
[1] Ponemon Cost of Data Breach Study, https://www.ibm.com/reports/data-breach

Approaches to Building a Security Business Case

- Cost approach
  - How much does it cost to recover?
- Industry comparison approach
  - What are comparable firms doing and paying?
- Business innovation approach
  - What can I gain from doing this?

This page intentionally left blank.

Industry Comparison Approach

- What is reasonable for security, based on:
  - Industry
  - Size
  - Market position
  - Region
- Can be analyzed via:
  - Spending comparison
  - Maturity comparison

Executives and business leaders want to know what a "reasonable" level of security spending is. They want to make sure that limited resources are being spent appropriately and that the firm is not overinvesting or underinvesting in certain areas. Basically, business leaders are looking to you to help answer the question, "How much should I spend on security?" The answer is complex and depends on a number of factors.

Certain industries tend to spend more on cybersecurity. For example, the financial services industry tends to spend more on security. James Dimon, the CEO of JPMorgan Chase, stated that the company would double its spending on cybersecurity from $250 million annually over the next five years.[1] This was in response to a breach that affected 76 million households.[2] So, it's not only because JPMorgan Chase is a financial services company. It's also because of its size. It holds a large amount of sensitive customer information. As a global company, it is one of the worldwide leaders and brands in financial services. In short, it has a lot to lose by not investing in a world-class cybersecurity organization.

In contrast, a small credit union that serves a specific state or county does not have as much at stake. Even though the credit union is also in the financial services industry, its profile is vastly different from that of JPMorgan Chase. Moreover, differences also exist based on country. This is represented in the Ponemon breach costs with Brazil having a much lower cost-per-record breach cost than the United States ($69 vs. $242).[3]

Spending is one way that maturity can be compared across firms. Comparing the maturity of security capabilities is another useful approach that we cover later in this section.

References:
[1] http://www.wsj.com/articles/j-p-morgans-dimon-to-speak-at-financial-conference-1412944976
[2] http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372
[3] Ponemon Cost of Data Breach Study, https://www.ibm.com/security/data-breach

Spending Comparison

- Percent of IT budget spent on security
  - Provides only a rough understanding of performance
  - Industry consensus
    - 5% is a useful rubric
    - Ranges from 1% to 13% depending on industry and maturity
- Can be a problematic metric
  - Do not make this the sole or primary focus of your business case
  - Depends on what is included in the percentage
  - Depends on your risk appetite and current state of security

One way to compare your security spending to that of other organizations is by looking at the percent of the IT budget that is spent on security. According to a Gartner study, organizations on average spend 5.6% of their IT budget on security with ranges for all organizations varying from 1 percent to 13 percent. [1,2] Historical data shows that the percentage has been gradually increasing. In a Gartner research paper titled, "Don't Be the Next Target - IT Security Spending Priorities", companies, on average, spent 5.1% of the IT budget on security.[3]

This measure provides a rough understanding of organizational maturity and can indicate whether spending has been focused solely on meeting mandatory requirements (e.g., compliance), has expanded to necessary requirements (e.g., improving due diligence), or has progressed to elective spending (e.g., optimizing security capabilities). Although this metric can help highlight certain areas that might need further analysis, it is also very problematic. These spending averages might not be a fit for every organization because of differences in industry, size, region, culture, and business goals. Moreover, different organizations might include varying items in the overall "security" budget. For example, some organizations might include identity and access management, business continuity, and disaster recovery costs in these numbers, whereas others might not. The main takeaway is that this metric should not be the sole focus of your business case.

References:
[1] https://www.gartner.com/en/newsroom/press-releases/2016-12-09-gartner-says-many-organizations-falsely-equate-it-security-spending-with-maturity
[2] https://www.theregister.co.uk/2016/12/09/gartner_security_spending
[3] https://www.gartner.com/doc/2703221/dont-target--it-security

Maturity Comparison

- What are other companies doing?
  - What is a reasonable level of maturity?
- Where can we get comparable data?
  - Information Sharing and Analysis Centers (ISAC)
    - FS-ISAC, REN-ISAC, etc.
  - Community projects
    - BSIMM, OpenSAMM, etc.
  - Research and consulting organizations
    - Gartner, Big Four, security service firms, etc.

Comparing maturity of security capabilities is a good way to get a sense of what other companies are doing and, by extension, what is a reasonable level of security for your organization. However, one problem exists. Where do you get the data to compare yourself with others?

One good way to get information is by joining an Information Sharing and Analysis Center (ISAC). Various ISACs have been formed to represent different sectors of critical infrastructure such as Financial Services (FS-ISAC), Research and Education (REN-ISAC), and National Health (NH-ISAC). The mission of ISACs is to "advance the physical and cybersecurity of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government."[1] ISACs provide a forum to develop relationships with industry peers, share information and best practices, and even conduct incident response exercises. The information gleaned from these interactions can help you gauge your relative level of maturity.

The data from various community projects can also be useful in evaluating your organization's maturity. The Building Security In Maturity Model (BSIMM) is a collection of data about software security programs at leading organizations.[2] The Open Software Assurance Maturity Model provides a similar framework for software security programs.[3] Although these two models are focused only on a subset of information security, they contain broader components, like strategy and vulnerability management, that are central to information security.

It can be difficult to obtain current and comprehensive data regarding your industry peers. As a result, many organizations hire a third-party firm to conduct maturity assessments. This can provide some assurance that an appropriate level of benchmarking against actual data was conducted. Gartner, the Big Four (Deloitte, PwC, EY, and KPMG), and other firms provide consulting services around industry benchmarking and analysis.

References:
[1] https://www.nationalisacs.org
[2] https://www.bsimm.com
[3] http://www.opensamm.org

Creating Credibility

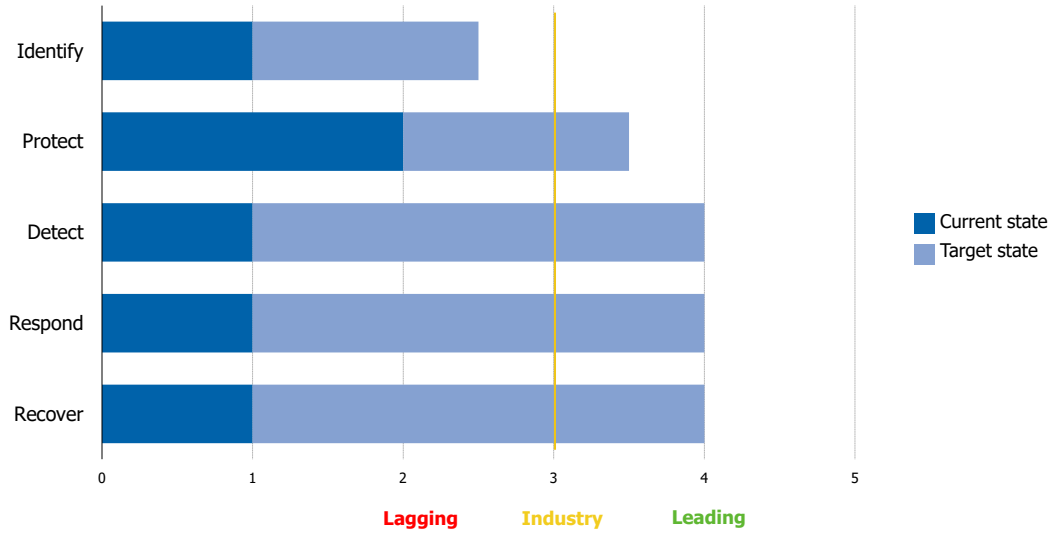
"A big part of being believable and building our trust is showing us how we compare to competitors, other industries, some kind of standards or benchmarks."

- Board Member

Alan Paller and John Pescatore have conducted a number of "CISO Hot Topic" sessions to determine what works for the most successful CISOs. In their webcast "Briefing the Board: Lessons Learned from CISOs and Directors" they describe a number of successful and unsuccessful examples of board and executive communication.[1] One board member gives some very good advice on building trust with the Board. Show "how we compare to competitors, other industries, some kind of standards or benchmarks."

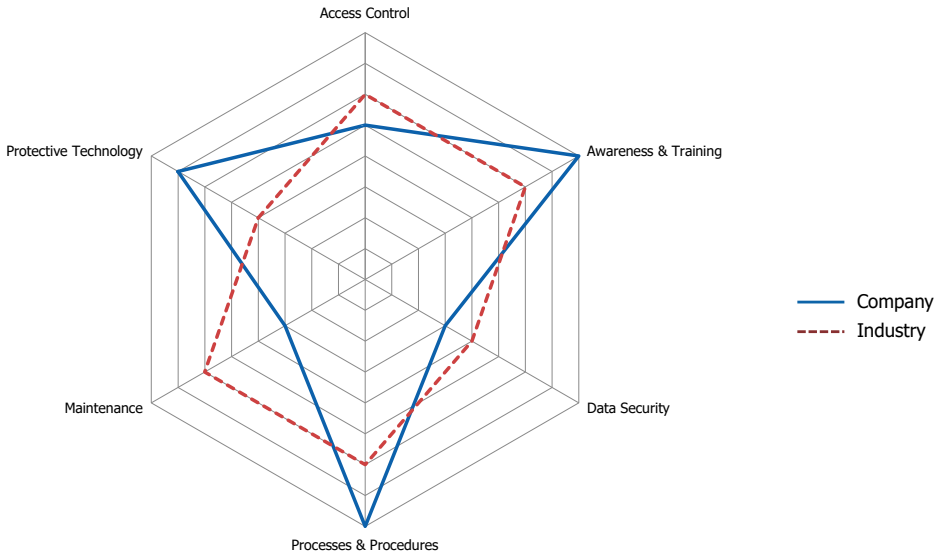
Reference:
[1] https://www.sans.org/webcasts/influencing-effectively-communicating-ceos-boards-directors-103927

Maturity Comparison Example



This is the example maturity model graph from earlier in the course. Each bar graph represents the current and target state maturity for each security capability area (Identify, Protect, Detect, Respond, and Recover). By agreeing upon an "industry standard" level of maturity, your company can begin to determine the appropriate level of investment required for each security capability. Over time, you can show incremental progress toward the target state by updating the maturity level for each specific capability.

BSIMM Maturity Comparison Example



This is an example radar chart (also known as a spider chart, or star chart) that represents your company's maturity level compared to your overall industry for various security capabilities in the Protect area of the NIST Cybersecurity Framework.

For example, the left-hand side of the radar chart shows that your firm is extremely strong in Protective Technology compared to the rest of the industry. This could indicate an overinvestment in this area or it could indicate a purposeful, strategic decision to grow this capability due to the nature of the organization's business. These radar charts are very helpful for showing differences in industry maturity levels for varying capabilities. In this specific case, it is important for Dennis to understand why certain areas might have an over or underinvestment.

Approaches to Building a Security Business Case

- Cost approach
  - How much does it cost to recover?
- Industry comparison approach
  - What are comparable firms doing and paying?
- Business innovation approach
  - What can I gain from doing this?

This page intentionally left blank.

Business Innovation Approach

- Plan security investments based on:
  - Business opportunities
    - Key enterprise initiatives
    - Process improvement opportunities
    - New product support
  - Business requirements
    - Compliance, regulatory
  - Business risk
    - Annualized Loss Expectancy (ALE = ARO x SLE)
    - Provide estimates based on business risk

A good way to gain support for security investments is by aligning the work of the security team to key business opportunities. For example, if your company is moving to support new enterprise initiatives like BYOD, mobile, cloud, or Big Data, you can gain support by helping business unit leaders deploy those technologies in a more secure manner. Providing security solutions before problems arise makes it easier not only for your key stakeholders but also for the security team by getting involved earlier in the system development process.

Process improvement opportunities are ways for security to provide value to the business. In large organizations, there are typically many systems all with different user IDs and passwords. Even if users choose the same password for all systems, they might be required to sign on dozens of times per day. Reducing the number of times a user has to sign on increases productivity and decreases support costs by reducing the amount of password reset calls to the help desk. In this way, security can gain support for deploying a Single Sign-On (SSO) solution that reduces time spent signing on to the multiple systems and allows users to focus on critical business tasks.

Security can also support business innovation by providing services to new products being rolled out by the company. These can be products utilized by customers such as new websites and mobile apps or even new systems that are important to the organization, such as order processing or inventory systems.

Compliance and regulatory requirements are an obvious area in which security can provide services to the company. For example, deploying PCI-compliant security infrastructure allows you to accept credit card payments. However, compliance often results in mandatory spending. It is the non-mandatory spending associated with overall business risk that is much harder to quantify. One approach for doing this is by using annualized loss expectancy (ALE), which is calculated by multiplying the annual rate of occurrence (ARO) of an event with the single loss expectancy (SLE):

ALE = ARO x SLE

First, you have to calculate single loss expectancy (SLE). This is based on exposure factor (EF) and the value of the asset. It's important to remember that exposure factor (EF) is a subjective, estimated percentage of loss to an asset if a specific threat is realized. It can be based on security vulnerabilities, threats, and the overall risk management framework used in your organization. For example, if you have an asset valued at $100,000 and an EF of 20%, then your SLE is $20,000.

Taking this SLE of $20,000, you can then multiply it by the annual rate of occurrence (ARO), which is an estimate of how likely it is that you will have a loss in one year. Again, the key word here is "estimate." By using a simple estimate of 10% likelihood in year 1, 20% in year 2, and so on, you can calculate that the ALE is $2,000 (10% x $20,000).

The key point here is that these are estimates. But, by using these estimates as a starting point, you can start to make the case that over five years the ALE is $10,000 (50% x $20,000). If the security control costs only $1,000, this could be a worthwhile investment. Point being, don't spend more protecting something than it's worth.

Elements of a Business Case

- Executive Summary
  - Problem
  - Assessment
  - Recommendation
- Introduction
  - Business drivers
  - Scope
  - Finance
- Analysis
  - Assumptions
  - Costs/Benefits
  - Key risks
  - Dependencies/Synergies
  - Options
- Appendix

Different organizations might utilize different templates for creating business cases. However, the core elements of a business case will remain the same.

Executive Summary
This section is written for key decision makers and summarizes the problem at hand, your assessment of the situation, and the overall recommendation. The recommendation can be as simple as choosing to invest in a new security capability or, even better, it can ask key decision makers to choose from a set of options to solve the problem at hand. Providing at least three options involves decision makers in the process and turns them into active participants. The executive summary section, although it comes first in the business case, is usually created last after all the other analysis has been conducted. This ensures that you can more easily summarize the actual information in the overall case.

Introduction
This section provides background information about business drivers (e.g., new business initiatives, revenue, and cost drivers) and the threat landscape (e.g., recent breaches, internal security incidents, etc.). This is where you lay out the scope of your business case. For example, does it touch all public facilities, office buildings, employees, customers, etc.? The scope will have a direct impact on the associated costs. This is where you can incorporate financial information related to the cost, industry comparison, and business innovation approaches we discussed previously.

Analysis
This is the meat of your business case and includes any assumptions that you have made in your model, the cost/benefit analysis, as well as key risks and dependencies/synergies. If your business case will be reviewed by a large number of key stakeholders, it is extremely important to include dependencies on other teams, as well as synergies that might help other teams. For example, if you are deploying a new patch management tool that has a side effect of reducing the number of hours that the IT operations team spends on managing systems, you would certainly want to highlight this fact to gain support from that key stakeholder. Finally, your analysis should include details about the various options that you considered or are proposing.

Appendix
What is included in this section depends largely on what key decision makers want to see and are interested in. Imagine that you have a CIO who is extremely focused on technology innovation and is a big picture thinker. She might not be as interested in the details of the 10-year financial forecast. However, if you have a CIO who is focused on improving current operations and reducing costs, the 10-year financial forecast probably shouldn't be relegated solely to the Appendix.

Tips for Creating a Security Business Case

- As a manager and leader, you are expected to:
  - Understand the vision and mission of the company
  - Make security understandable to business leaders
- Don't just ask for the money
  - Sell the vision and how you will solve business problems
  - Use all the approaches to justify your request
    - Cost, Industry Comparison, and Business Innovation Approaches
- Let the case speak for itself
  - Allow decision makers to come to their own conclusion
  - Outline three options with various pros and cons
    - Let them pick one

Ultimately, a business case is about getting funding for your security initiatives. However, the framing associated with the request is extremely important. Instead of simply asking for the money, a better approach is to articulate the vision for the security program and the business problems that will be solved. By focusing on the problem and the eventual solution, you can increase commitment and turn stakeholders into partners.

By using the approaches discussed in this section to justify your request and letting the case speak for itself, you allow key decision makers to come to their own conclusions. Executives want to have a say in how to run the business and many are realizing that managing security risk is a key component of running the business. By outlining three options with various pros and cons, you can provide a say in how to manage business risk.

Provide Options

- Highlight trade-offs with business value, risk reduction, cost:

	Option A	Option B	Option C
Business value	✓	✓✓	✓✓✓
Risk reduction	🔒	🔒🔒	🔒🔒🔒
Cost	$	$$	$$$

The options that you present should clearly show how different levers can be turned to provide increased business value, increased risk reduction, and varying levels of cost. This helps highlight to key decision makers the pros and cons of various approaches. When presenting three different options, always make sure to highlight your specific recommendation with an appropriate justification.

This page intentionally left blank.

CYBER42

Event #5

Debrief

This page intentionally left blank.

Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Define Current State
  - Vision and Mission
    - Lab #1: Mission Statement
  - SWOT Analysis
    - Lab #2: SWOT Exercise
- Develop the Plan
  - Visioning and Innovation
  - Security Framework
  - Security Roadmap
    - Gap Analysis
    - Lab #3: Roadmap Development
  - Business Case Development
- ***Deliver the Program***
  - Security Metrics Program
  - Marketing and Exec Communications

This page intentionally left blank.

How to Deliver the Program

1) Measure and report on security activities
   - Build metrics and dashboards

2) Promote your strategic efforts
   - Develop effective marketing and executive communications

Building an effective security program is not just about developing a vision, developing a strategic plan, and executing on the technical aspects of that plan. As a leader and manager, you must also:

1) **Measure and report on security activities**
   There's a saying, "What gets measured gets managed." Successful security leaders build metrics and dashboards that can be suitable for various levels of the organization.

2) **Promote your strategic efforts**
   Our key stakeholders are extremely busy. Sometimes, we have to remind them of the great work being done by the security team. This means that you have to develop effective marketing and executive communications.

Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Define Current State
  - Vision and Mission
    - Lab #1: Mission Statement
  - SWOT Analysis
    - Lab #2: SWOT Exercise
- Develop the Plan
  - Visioning and Innovation
  - Security Framework
  - Security Roadmap
    - Gap Analysis
    - Lab #3: Roadmap Development
  - Business Case Development
- Deliver the Program
  - ***Security Metrics Program***
  - Marketing and Exec Communications

This page intentionally left blank.

Security Metrics Overview

- By the end of this section, you will understand:
  - Why metrics are important and the critical concern around security metrics
  - Various types of metrics including those beyond traditional technical metrics
    - Financial
    - Customer/stakeholder satisfaction
    - Business process
  - How to tailor your metrics program to specific audiences
    - Executive
    - Operational
    - Technical
  - How to use metrics to drive process improvement

Paving the road to success depends on you, and your leadership team being well informed and having the right information to make the right decisions. As a security professional, it's your job to do just that—understand the quality and progress of your "business of security," and communicate value and risks to your leadership in a manner that is easy to consume, and relevant enough to make well-informed decisions.

There is not a better, more effective way to understand and communicate all aspects of business than metrics. It's a common language that all leaders understand and has been used for decades.

Security is not exempt from demonstrating strategic value and operational effectiveness in organizations, but historically this has proven to be a significant challenge for many security organizations. In this security metrics section, we will cover topics related to metrics that will help you rise to the challenge of demonstrating value and will help you communicate more effectively.

We will also demonstrate how you can leverage various types of metrics such as security, financial, customer satisfaction, and business processes to help you, your leadership, and your company become more holistically informed and make better decisions.

We will share security frameworks that you can leverage to build a metrics program and show you how you can translate business activities, security vision, and strategy into your metrics program.

We will show you how to tailor your metrics for specific audiences such as executives and stakeholders, and operations and technical; how to apply multi-dimensional views to effectively show the overall health and security posture of your organization; and how you can use metrics to identify improvement opportunities and drive process improvement.

We will also share visualization tips, communication channels to socialize your metrics program, and pitfalls to avoid when creating your metrics program.

Security Metrics: A Critical Concern

- Problem
  - Many executives are searching for security statistics that are important, so they know when to pay attention
    - Metrics the security organizations track and present to management are not often aligned with business objectives
    - They often convey little information on a security program's effectiveness in reducing overall risk
    - They are often difficult to understand
- Solution
  - Provide essential metrics that transform and communicate complicated data into business language that can be easily understood

As pressure increases on security as a priority for many organizations, it's not unusual for executives and directors of boards to take an active interest in security. As reports of breaches hit the news almost daily, top executives want to be informed of the current and evolving threat landscape, as well as organizational risk, readiness, and response plan for incidents.

Security professionals are being brought before executives and asked to demonstrate the effectiveness of their security programs. It's not unusual for executives to be given volumes of data that is not relevant or aligned to the business objectives, convey little to no information on the effectiveness of security, are difficult to understand, and often lead to more questions than answers.

As stated previously, numbers are the common language of business that all leaders understand and rely on to make important business decisions. You must accept the fact that security metrics are no different than the metrics other business verticals would use to communicate value (such as Finance, Sales and Marketing, or even IT). It is your responsibility as a security professional to provide metrics that transform and communicate large quantities of complicated data into business-consumable language that can be easily understood, provide business value, and facilitate the decision-making process.

Executives and board members want to understand whether the decision they made to fund security has helped achieve a competitive advantage and will keep them out of the news. They want information that will help them determine whether they are spending too little or too much on security, how their investments to date have improved the organizational risk posture, and/or where the accountability needs focus to influence culture and behavior change.

Why Metrics Are Important

- In today's performance-focused environment, it's important to:
  - Measure performance
  - Monitor progress
  - Communicate value
- Metrics help you manage your "business of security" more effectively and efficiently through:
  - Data-driven decision-making support
  - Closer alignment with the business and business objectives
  - Increased accountability

Metrics are an essential tool for security professionals to understand all aspects of the "business of security" and encompassing components, such as understanding performance on specific technology capabilities and processes, progress toward pre-defined goals addressing security and risk posture, and how those security initiatives are paying off. Metrics can also help you build your business case to support organizational demand for security support on strategic initiatives that might require additional resources.

Metrics will help you further understand whether your security controls are producing the desired results, such as fewer malware infections as a result of your network segmentation and anti-malware programs. Time to containment and mitigation for incidents is within an established norm. Workstations and servers are patched well within an acceptable level of risk tolerance the organization has agreed upon.

If metrics are done right, security managers will better understand their business, which in turn will allow them to more effectively communicate and inform executives, stakeholders, and board members the complexities and risks of security, quantify security outcomes through the effectiveness of controls and processes, and demonstrate considerable value and alignment to the organization.

Metrics provide more than funding justification for more resources and shiny new technology. Properly designed metrics will facilitate objective data-driven decision making to critical areas such as making adjustments to your strategy based on the diagnosis of a problem or gaining more comprehensive understanding of an issue or root cause. Metrics can also drive performance and operational improvements such as improved SLAs, customer satisfaction, and improved tuning of technologies to improve security outcomes. Metrics will also aid in your overall organizational approach to risk by determining which initiatives will be funded and in what order.

Security metrics can shine a light on the organization's state of compliance against internal security guidelines and policies, ultimately increasing accountability across business units. Comparing business unit result to an agreed upon risk tolerance level will increase motivation to improve results.

Technical Measures: CIS Controls

- CIS Controls Measures and Metrics
  - Pre-defined measures for each of the CIS Controls

Function	Example Measures
Identify	% of networks have not recently been scanned by an active asset discovery tool % of networks are not being monitored by a passive asset discovery tool % of DHCP servers do not have logging enabled % of hardware assets are not presently included in asset inventory % of hardware assets as a whole are not documented in asset inventory with the appropriate network address, hardware address, machine name, data asset owner, and department for each asset % of network switches are not configured to require network-based port level access control for all client connections % of network switches are not configured to require network-based port level access control utilizing client certificates % of software are not presently included in software inventory % of software applications or operating systems are not currently supported by the software's vendor % of hardware assets have not recently been scanned by a software inventory tool to document the software installed on the system % of software assets are not documented in a software inventory system that tracks the name, version, publisher, and install date for all software, including operating systems authorized by the organization

CIS has published a measurement companion to the CIS Controls called "Measures and Metrics for CIS Controls V7."

On this page, we have completed a mapping between the CIS Measures and the NIST CSF to illustrate how you can align your framework, controls, and proposed measurement in an effort to help you measure the effectiveness and implementation of your security program. We have provided the same mapping for the remainder of the NIST functions: Protect, Detect, Respond, and Recover on subsequent slides.

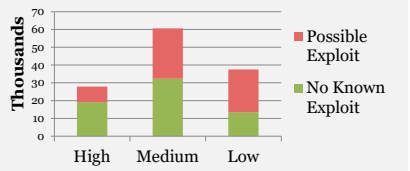
A mapping exercise such as this might be time intensive to build in the beginning, but the effort you invest in organizing your information with reputable and recognizable frameworks and controls will greatly benefit you and your team in the long run as you look to develop your reporting and communication efforts to share with your leadership team, executives, customers, and stakeholders.

Function	Example Measures
Protect	% of unauthorized assets have not been removed from the network, quarantined or added to the inventory in a timely manner
	% of the organization's unauthorized software are either removed or the inventory is updated in a timely manner
	% of hardware assets are not utilizing application allowlisting technology to block unauthorized applications
	% of hardware assets are not utilizing application allowlisting technology to block unauthorized applications at the library level
	% of hardware assets are not utilizing application allowlisting technology to block unauthorized scripts from executing
	% of high risk business applications have not been physically or logically segregated from other business systems
	% of hardware assets have not recently utilized automated tools to inventory all administrative accounts
	% of systems utilize default passwords for accounts with elevated capabilities
	% of user accounts with elevated rights do not utilize a dedicated or secondary account for elevated activities
	% of hardware assets not configured to utilize multi-factor authentication and encrypted channels for all elevated accounts
	% of system administrators not required to use a dedicated machine for all administrative tasks or tasks requiring elevated access
	% of systems limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users
	% of the organization's hardware assets are not configured to issue a log entry and alert when an account is added to or removed
	% of hardware assets are not configured to issue a log entry and alert on unsuccessful logins to an administrative account
	% of authorized operating systems and software does not have a documented, standard security configuration
	% of hardware assets are not based upon secure images or templates based on approved configuration standards
	% of master images are not stored on securely configured servers, validated with integrity checking tools, to ensure that only authorized changes to the images are possible
	% of hardware assets are not automatically configured via system configuration management tools that automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals
	% of hardware assets have not recently been scanned by an SCAP-compliant configuration monitoring system to verify all security configuration elements, and alert when unauthorized changes occur
	% of hardware assets are running unsupported web browsers and email client software
	% of hardware assets are utilizing unauthorized browser or email client plugins or add-on applications
	% of hardware assets are utilizing unauthorized scripting languages that run in all web browsers and email clients
	% of hardware assets (whether physically at an organization's facilities or not) are not required to utilize network-based URL filters
	% of hardware assets (whether physically at an organization's facilities or not) are not required to log all URL requests
	% of DNS servers are using DNS filtering to help block access to known malicious domains
	% of hardware assets are not configured to not auto-run content from removable media
	% of hardware assets do not associate active ports, services and protocols to the hardware assets in the asset inventory
	% of hardware assets are not configured to require that only network ports, protocols, and services listening on a system with validated business needs, are running on each system
	% of hardware assets are not utilizing host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed
	% of critical servers are not required to utilize application layer firewalls to verify and validate the traffic going to the server
	% of network devices do not utilize a standard, documented security configuration standard for the device
	% of network devices do not have all configuration rules that allow traffic to flow through network devices be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need
	% of network devices are not regularly compared against approved security configurations defined for each network device in use and alert when any deviations are discovered
	% of network devices are not utilizing the latest stable version of any security-related updates
	% of network devices are not managed using multi-factor authentication and encrypted sessions
	% of network engineers are not utilizing a dedicated machine for all administrative tasks or tasks requiring elevated access to network devices
	% of network engineers are not utilizing a dedicated machine, located on a dedicated management network, for all administrative tasks or tasks requiring elevated access to network devices
	% of hardware assets have not recently been scanned to identify unauthorized network boundaries
	% of network boundaries are not configured to record network packets passing through the boundary
	% of network boundaries are not configured to require network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems the boundary
	% of organization's network boundaries are not configured to require network-based Intrusion Prevention Systems (IPS) sensors to look for unusual attack mechanisms and detect compromise of these systems the boundary

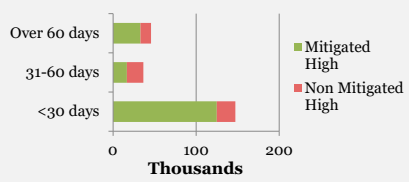
Function	Example Measures
Detect	% of hardware assets have not recently been scanned by an SCAP compliant configuration monitoring system to identify all potential vulnerabilities on systems % of hardware assets have not recently been scanned by an SCAP compliant configuration monitoring system to identify all potential vulnerabilities on systems utilizing an authenticated connection to the system % of hardware assets have not recently been scanned by an SCAP compliant configuration monitoring system to identify all potential vulnerabilities on systems utilizing a dedicated service account and host-based restrictions % of hardware assets do not utilize at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent % of hardware assets are not configured to require local logging on the asset % of hardware assets are not configured to require local logging to include detailed information such as a event source, date, timestamp, source addresses, destination addresses, and other useful elements on the asset % of hardware assets do not have adequate storage space for the logs generated % of hardware assets are not configured to aggregate appropriate logs to a central log management system for analysis and review % of hardware assets are not configured to aggregate appropriate logs to a Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis % of hardware assets have not had their logs reviewed recently to identify anomalies or abnormal events % of SIEM systems have not recently been tuned to better identify actionable events and decrease event noise % of hardware assets do not utilize centrally managed anti-malware software to continuously monitor and defend each of workstations and servers % of hardware assets do not utilize recently updated, centrally managed anti-malware software to continuously monitor and defend each of workstations and servers % of hardware assets are not configured to require anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables % of hardware assets are not configured so that they automatically conduct an anti-malware scan of removable media when inserted or connected % of hardware assets do not utilize centrally managed anti-malware software to continuously monitor and defend each of workstations and servers % of Domain Name System (DNS) servers are not configured to require query logging to detect hostname lookups for known malicious domains % of hardware assets have not enabled command-line audit logging for command shells, such as Python or Windows PowerShell with enhanced logging enabled % of hardware assets are not regularly scanned by a port scanner to alert if unauthorized ports are detected on a system
Respond	% of hardware assets are not regularly updated by an automated software update tool in order to ensure that the operating systems are running the most recent security updates provided by the software vendor % of hardware assets are not regularly updated by an automated software update tool in order to ensure that third-party software is running the most recent security updates provided by the software vendor % of identified vulnerabilities have not been remediated in a timely manner Has the organization ensured that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management Has the organization assigned job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution Has the organization designated management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles Has the organization assembled and maintained information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners Has the organization planned and conducted routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats
Recover	% of hardware assets are not configured to back up system data automatically on a regular basis % of hardware assets are not configured to back up the complete asset automatically on a regular basis % of hardware asset backups have not been tested recently to ensure that the backup is working properly % of hardware asset backups are not properly protected via physical security or encryption when they are stored, as well as when they are moved across the network (this includes remote backups and cloud services as well) % of hardware assets does not have at least one backup destination that is not continuously addressable through operating system calls

Technical Metrics Examples

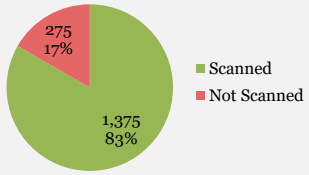
Server Vulnerabilities Detected By Risk



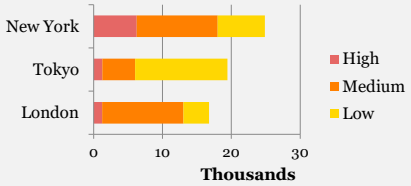
Mitigated and Non-Mitigated High Server Vulnerabilities Aging



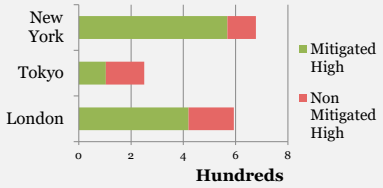
Scanning Coverage Servers



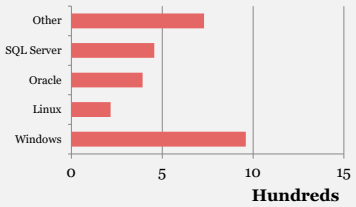
Server Vulnerabilities Detected By Region



High Server Vulnerabilities Over 60 Days By Region



Top 5 High Server Vulnerabilities



SANS | MGT514 | Security Strategic Planning, Policy, and Leadership 162

This is an illustrative sample of technical metrics designed for discussion purposes only. There are hundreds, if not thousands, of technical metrics and data variations that can be generated to display security controls, understanding of threats, and vulnerabilities and evaluation processes.

These examples are focused around server vulnerabilities. Shown here are six ways to view the data related to server vulnerabilities. Each graph displays important data in an effort to further the assessment and understanding of vulnerabilities.

Technical Metrics Examples: What's Wrong?

- What's wrong with these metrics?
  - Message is diluted in operational details
    - They do not increase your understanding of security and risk
    - They are not ideal to increase security's visibility and generate awareness
  - They are not business consumable
    - Not aligned with the business or their objectives
    - They are not relevant for senior leaders, executives, or stakeholders
    - Will not boost your credibility
  - They do not measure progress and demonstrate value
    - Provides a snapshot in time only
    - Do not provide trending to determine progress, increased or decreased risk

There is an enormous amount of data that is waiting to be mined and displayed in various forms of graphs and/or charts with the hopeful outcome that you can present to your leadership, stakeholders, and company executives; and they immediately identify value in what you've provided, which in turn will lead to facilitated discussion that will ultimately ensure your metrics are leveraged to make data-driven decisions or provide the perfect amount of information where they feel well-informed.

The metrics on the previous page are not those metrics described above. They are not the kind of metrics where executives can feel like they understand what is going on and they are well informed. They are not the kind of metrics that will enable an executive to respond quickly to make important decisions about security.

The message in these server vulnerability metrics is diluted because they focus on very technical operational details, which are spread over several metrics. They tell an incomplete story of security and risk, and they require far too many assumptions to be made or erroneous conclusions to be filled in by the imagination of the recipient.

These server vulnerability metric examples are not business consumable. They do not satisfy a specific business requirement or address the question on every executive's mind, "So what?"

They are not aligned with the business or its objectives (unless your company's business objectives happen to minimize vulnerabilities in the server environment). Your audience is not likely to understand the value of "Possible Exploit" versus "No Known Exploit," nor will they understand the real threat behind the Top 5 High Server Vulnerabilities list, or why an aging report is relevant to determining how long risk has been in your environment.

These metrics are not relevant for senior leaders, executives, or stakeholders. Presenting these detailed, technical metrics to this audience will leave them with more questions than answers. This approach will not boost your credibility.

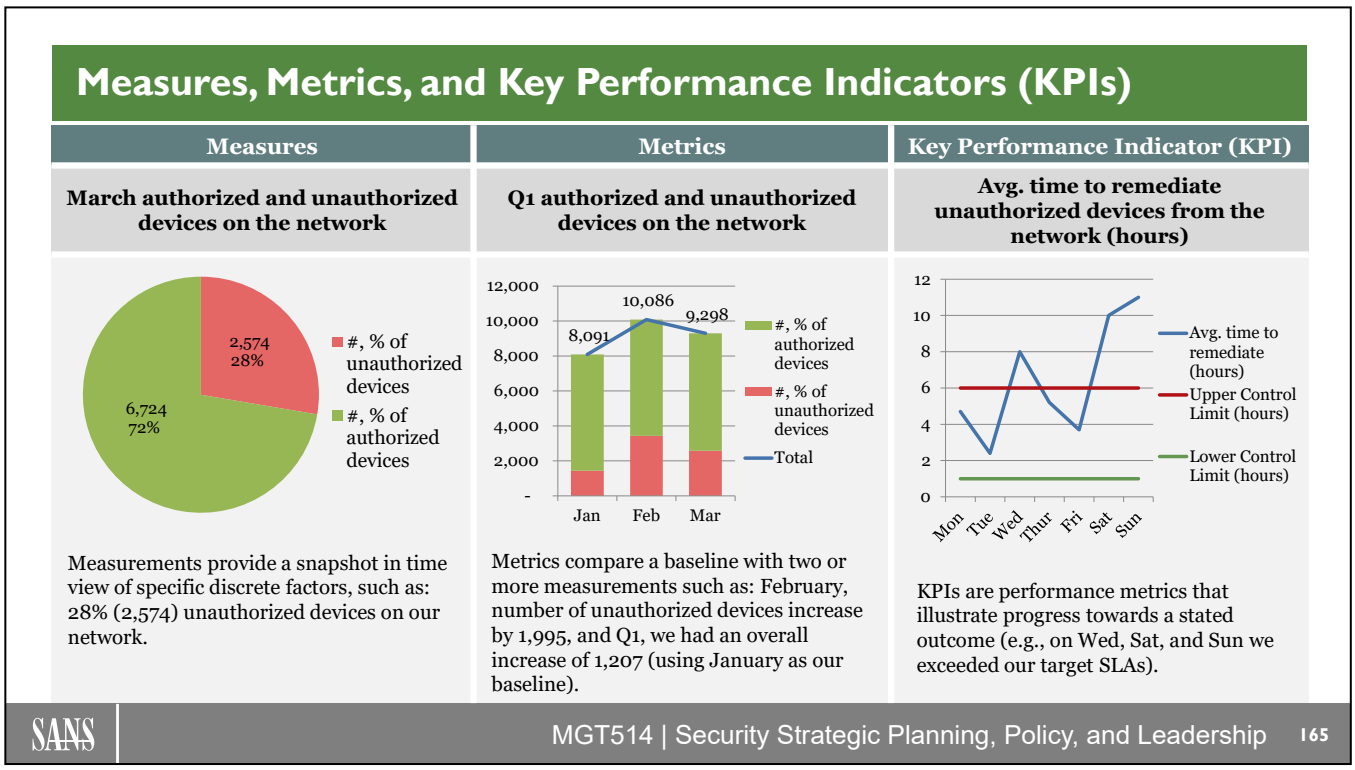
These metrics do not measure progress or demonstrate value. They provide a snapshot in time, and they do not include trending data to determine progress or increased or decreased level of risk. The Aging metrics attempt to illustrate risk, but doesn't tell us whether we are getting better or worse at mitigating server vulnerabilities. The scanning coverage is a nice, clean measurement, but there is no context to let the audience know whether this is an appropriate coverage level.

Here is an example to illustrate the context of value around scanning coverage metrics. Of the "Not Scanned" servers, how many of those servers contain regulated or sensitive data? If you have a high percentage of "Not Scanned" servers that are critical to business operations, then your risk is greater. You can ask the same questions with the Top % High Server Vulnerabilities metric. How many of these are on critical business applications?

The metrics you select should satisfy a specific business requirement and those metrics should be metrics that someone needs to know about. If there is not a compelling business need for the metrics, you should not share it with your stakeholders, executives, and/or board of directions. Again, you will likely cause more concern and questions to arise than you anticipated.

Effective metrics should:

- Measure performance using baselines and trends
- Monitor progress toward stated goals
- Help the metric owner communicate value
- Facilitate the use of data for decision-making support
- Be closely aligned with the business, and business objectives
- Provide line of sight to risks, ultimately increasing accountability



There are similarities between measures and metrics in that both can be qualitative or quantitative. There is also a distinction that is often unclear. This distinction between measures and metrics is important to understand. The main difference is that metrics are measurements that use a baseline to establish normal operating levels and uses this baseline to compare when something is abnormal.

Another way to look at the distinction between measurement and metrics is that measurements provide a snapshot in time view of specific discrete factors. Measurements are objective raw data and generated by counting, such as "I have one widget." Using a security measurement example, you might count 28% (2,574) unauthorized devices on our network.

Comparing a baseline that has been established with two or more measurements taken over time generates metrics. Metrics are generated from analysis, such as "I have 10 more widgets than I did yesterday, and I have 15 more widgets than when I started." Using a security metrics example, you might illustrate: In February, we had an increase of 1,995 unauthorized devices on the network, and in Q1, we had an overall increase of 1,207 (using January as our baseline).

KPIs are performance metrics that illustrate progress toward a stated outcome. KPIs are used across all industries and are used to monitor how the organization is doing relative to goals. They are also used to monitor implementation and effectiveness of organizational strategies, and to determine the gap between actuals and targets.

Companies will use KPIs, such as profit and loss statements, new membership growth, earnings per shareholder, etc. For security, KPIs should be customizable for the business unit(s) your security organization supports and might include areas like avoiding a data breach or meeting regulatory and compliance requirements.

For security, let's say that minimizing unauthorized devices on the network is a business imperative. You'll want to determine your thresholds or state your goals. For this example, we can use an upper and lower control limit to show the effectiveness threshold we want to operate in. Obviously, the closer we get to the lower

threshold of removing unauthorized devices within one hour, the more effective we are in our security controls. When performance moves closer to or exceeds the upper threshold of six hours, we have cause for alarm, and we would need to look deeper at our performance and make necessary adjustments.

Developing relevant and actionable security KPIs is a critical step to providing value and building credibility for your security organization. The key to successful security KPIs is to map closely to business KPIs. In other words, develop KPIs that are important to the business, not just security.

Good KPIs will include the following attributes:

- Monitors the implementation and effectiveness of organization's strategies
- Determines effectiveness and operational efficiency
  - Effectiveness is "Doing the right thing."
  - Efficiency is "Doing the thing right."
- Determines the gap between actual and targeted performance
- Provides focus for what matters most
- Is not limited to work being performed; it illustrates accomplishment
- Provides business-consumable context in a common language that facilitates communication

Benjamin Franklin on Planning

"By failing to prepare,
you are preparing to fail."
- Benjamin Franklin

Benjamin Franklin was a leading author, politician, scientist, and investor.[1] He was also a renowned polymath, a person whose expertise spans a significant number of different subject areas. This term is often used to describe great thinkers of the Renaissance and the Enlightenment who excelled at several fields in science and the arts.

Franklin was also a printer, political theorist, Freemason, postmaster, inventor, civic activist, statesman, and diplomat. One of Franklin's most notable discoveries was through his electrical experiments, which led to his invention of the lightning rod.

In a 1772 letter to Joseph Priestley, an 18th-century English theologian, dissenting clergyman, and natural political theorist, Franklin describes the earliest known description of a planning technique using the Pro & Con list.[2] He writes "... my way is to divide half a sheet of paper by a line into two columns, writing over the one Pro, and over the other Con. Then during three or four days' consideration, I put down under the different heads short hints of the different motives that at different times occur to me for or against the measure. When I have thus got them all together in one view, I endeavor to estimate their respective weights; and where I find two, one on each side, that seem equal, I strike them both out, If I find a reason pro equal to some two reasons con, I strike out the three. If I judge some two reasons con equal to some three reasons pro, I strike out the five; and thus, proceeding I find at length where the balance lies; and if after a day or two of further consideration nothing new that is of importance occurs on either side, I come to a determination accordingly."

References:
[1] https://en.wikipedia.org/wiki/Benjamin_Franklin
[2] https://en.wikipedia.org/wiki/Joseph_Priestley

Planning Is Fundamental

- Creating a plan will ensure success of your metrics program
  - State your program goals
  - Define the metrics that will help you reach your goals
    - Addressing the "so what" your organization cares about
  - Determine your method
    - Identify metric owners: Accountable for the people, process, and/or technology associated with each metric
    - Define metric classification: For example, data spill prevention: Count of unencrypted outbound email
    - Describe business purpose: For example, visibility to email activity where sensitive information is leaving company
    - Determine data source: For example, data loss prevention system
    - Decide publication frequency: For example, weekly, monthly, quarterly, etc.
    - Build operational definitions: Define acronyms, processes, teams, etc., that will be useful to your audience
    - Establish review process: For example, leadership, legal, communications etc.
    - Metrics hierarchy classification: For example, Balanced Scorecards, Operational Dashboards, or Technical charts and graphs

Creating a measurement plan will aid in the success of your metrics program. Planning is fundamental and will aid in the assurance of your metrics plan success. It will also align expectations between your teams, your leadership, customers and stakeholders, executives, and ultimately benefit the board of directors.

State your program goals
You first need to understand and define the goals of your metrics program. Without these stated and defined goals, you might end up somewhere you didn't intend your program to be. It's important to also remember that the goals of the program should extend beyond traditional security and include more than what "you" want to see. Your program should include what your customers, stakeholders, and executives "need" to know. If you want to make progress with the business, take your security hat off and put your consumer hat on.

The goals of your metrics program could be any combination of, or all of the examples listed below. These examples are not exhaustive, and you might find you have your own unique drivers for your metrics program.

The goal of the metrics program is to:

- More effectively align with what our customers and stakeholders value, drive transparency, and communicate more effectively
- Optimally manage my business of security
- Identify improvement opportunities to minimize risk and optimize costs
- Drive compliance and behavior change
- Improve specific security capabilities (e.g., password protection, vulnerability management, etc.)

Define the metrics that will help you reach your goals
Include various types of metrics that address the "so what" for your organization. The metrics you select should be aligned with your goals and tell you what you are going to measure to achieve those stated goals. On the following page, we've outlined in further detail some metrics considerations.

Determine your method
A measurement plan is your roadmap that defines the who, what, why, when, and where of your metrics program. A measurement plan is critical to the success of your metrics program because it will drive accountability, and ensure a repeatable process and more reliable output results. The components of a measurement plan are listed below:

- **Identify metric owners:** Metric owners are the individuals accountable for the people, process and/or technology associated with a specific metric. You will have many metrics owners within your metrics plan. Metric owners are accountable to create a measurement plan for their respective area of responsibility.

- **Define metric classification:** You should create a high-level classification schema. This will give you greater flexibility on your reporting capabilities down the road, such as reporting all metrics that are related to data spill prevention or vulnerability management. You might want to include subdomain as well, such as unencrypted outbound emails, which will give you even more flexibility in your reporting down the line.

- **Describe business purpose:** This component of your measurement plan is critical. If you cannot describe the purpose of each of your metrics in business-consumable terms, you will not be able to communicate with people outside of your security organization. For example, let's look at the count of unencrypted outbound emails. A business purpose definition might be able to provide visibility to email activity where sensitive information is leaving the company.

- **Determine data source:** As stated previously, there are hundreds, if not thousands, of technical measures and data variations that can be generated to display security controls. Designating the specific source of raw data that will be used to generate each of the metrics within your program is important for continuity of your metrics program. Using the same example as above—unencrypted outbound emails—your data source might be your data loss prevention system. We will talk more specifically about the data sources on the next page.

- **Decide publication frequency:** For each metrics, you'll want to indicate on your measurement plan what the publication frequency is (e.g., weekly, monthly, quarterly, etc.). This will set expectations for all consumers.

- **Build operational definitions:** This section is another critical component of your metrics program and your measurement plan. Security, in general, is very technical, complex, and difficult to understand for non-security professionals, let alone, one team's definition of process, procedure, or technology usage might vary slightly or significantly from another team. It's important that you define operational and technical terms, acronyms, and anything else that might be useful to your audience and help them to better understand the story you are trying to tell with your metrics. As an example, Severity 1 might mean something entirely different from team to team. It's important to define what Severity 1 means related to that specific metric.

- **Establish review process:** It's important to determine what the review process will be in order to ensure the success of your program. For instance, you wouldn't want metrics going to your customers or stakeholders without your leadership review. Or, if by chance the metrics you are producing are intended for consumers outside of your organization, you would likely need your leadership review and possibly legal and/or your communications team.

- **Metrics hierarchy classification:** We are going to talk more about metrics hierarchy in the coming slides, but for the purposes of understanding this measurement plan requirement, you will need to know that each metrics should be classified based on your reporting output (for example, Executive Balanced Scorecards, Operational Dashboard, or Technical Charts and Graphs).

Metric Selection Is Important

- Metrics should answer the "so what" for your organization
  - They need to be transformed into more meaningful data through analysis
    - Many data sources you can use (e.g., antivirus, antimalware systems, SPAM filters, etc.)
  - Financial metrics should be considered in two ways
    - How much does it cost to operate security (e.g., % of security budget compared to IT)
    - How security incidents impact your company financially (e.g., direct loss of intellectual property or cost of downtime)
  - Customer/stakeholder satisfaction and business process should measure what's important to the organization
    - Value: For example, reliability, responsiveness, and assurance of service
    - Invisible value: For example, activities and controls that are our corporate responsibility but have little to no impact on what the customer perceives as value

Your metrics program should be inclusive of various types of metrics such as security, financial, customer satisfaction, and business process. Including these categories of metrics will provide your leadership, stakeholders, and executives a strategic and holistic view of your efforts.

Security Metrics
As stated previously, there are hundreds, if not thousands, of technical security metrics that you can generate based on the data that can be gathered from your environment. The following is a list of some of the potential sources you can collect raw data from in support of your security metrics. As a reminder, these data sources are a good starting point. However, the data from these tools often have to be transformed into more meaningful information through analysis in order to provide intelligence that enables key decisions to be made.

- Antivirus, antimalware, systems
- Spam filters
- Firewalls
- Vendors or managed security services
- Weblogs
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Patch logs
- Vulnerability scans
- Penetration tests
- Databases
- Network access control
- Data loss prevention systems
- Access logs
- Server logs
- VPN
- Configuration hardening

- Secure web gateways
- Web application firewalls
- Mobile data protection
- Governance, risk, and compliance management
- Storage encryption
- SIEM

Financial Metrics
For financial metrics, you might want to consider looking at this from two angles. First, how much does it cost to operate security? Some examples of this might be "Security budget as a % of overall IT." You might want to further group by business unit, or specific to application development or some other important category, or categories your company will find useful. You might also want to show a % of change in security budget from previous fiscal year, % of security budget dedicated to contractors, outsourcing, and/or training. You will also want to provide information on operational budget (OPEX), which lays out ongoing spending on routine daily operations. You will also want to include capital expenditures or (CAPEX), which refers to a one-time investment on hardware, software, and in some instances project-related resources.

Secondly, you'll want to show how security incidents, or the lack thereof, either positively or negatively impact your company financially such as the cost of incidents. This could include:

- Direct loss might include the value of intellectual property, customer lists, trade secrets, or assets that are destroyed.
- Cost of business system downtime would include the cost of refunds for failed transactions, or the cost of lost business directly attributed to the incident.
- Cost of containment includes efforts and the cost of existing security resources and assets, and potentially, consulting services.
- Cost of recovery could include the cost of incident investigation and analysis, efforts required to repair and/or replace systems, consulting services for repairs and/or investigations, and additional costs not covered by an insurance policy.
- Cost of restitution could include penalties and other funds paid out due to breach of contracts or SLAs resulting from the incident, and cost of services provided to your customers as a direct result of the incident such as ID theft insurance and/or credit monitoring. This could also include public relations costs, and cost of disclosures and notifications, and legal costs, fines, and settlements.[1]

Customer/Stakeholder Satisfaction and Business Processes
Customer and stakeholder satisfaction is another way a security organization can evaluate its goals and measure progress. In order to develop metrics for this, a security organization must understand who its customers and stakeholders are, and what's important to them. We covered stakeholder management in Section 1: Strategic Planning Foundations.

It's important to note that customer satisfaction might be the result of the metrics you capture and report on in your business processes. The efficiency of your business process often influences and/or has direct correlation to your customer's satisfaction.

The first thing you must do to determine what customer/stakeholder satisfaction metrics you can produce is understand what types of services or business processes your security organization provides to your customers and stakeholders. More importantly, you need to know what your customers and stakeholders "value" versus the "invisible value" we "think" is important to organizations because of our roles, responsibilities, and due diligence we must perform as a security organization.

Value: A customer or stakeholder might value reliability, which is your team's dependable and accurate performance against what was promised. A customer might also value responsiveness, which is your team's willingness to provide prompt service for client needs. A customer and stakeholder might also value assurance that your team has knowledge and competence in the services performed.

- **Invisible Value:** As security professionals, we perform many tasks to secure an environment and meet regulatory and contractual compliance. Many of these tasks go unseen or unnoticed and are, in essence, invisible to our customers and stakeholders. If we as security professionals measure what we "think" is important to our customers and stakeholders—the invisible value—we will miss the mark every time.
    - An example of this would be endpoint protection. We might have several layers of controls for our endpoint protection. The majority of our customers do not care about all of these layers of control. It's invisible to them. What will be of concern is if all these layers are causing performance latency issues that impact their ability to perform their job.
    - For another example, if you are performing a security assessment for a new application that will be deployed to the environment, a customer generally won't care about all the specific tasks that you performed through the assessment. What will be of value to them is that you completed the assessment on time and on budget, and you helped them get through any remediation of findings with ease so they can meet their deadlines.

To summarize, you must select metrics that are important to your customers and stakeholders, and remember, they may come from various groups within your organization such as Finance, Sales and Marketing, Legal, and Compliance to list a few. Your metrics need to be customized for what's important for each respective group. Below are a few examples for consideration:

- Percentage of security projects delivered on-time and on-budget
- Customer facing (such as e-commerce sites) incidents and time to remediate
- Productivity incidents and time to remediate
- SLAs on various security capabilities (for example, delivery of evidence to Legal and/or HR on investigations)

Reference:

[1] https://www.cisecurity.org/cis-benchmarks

Metrics Programs Should Be Prioritized

- Metrics programs should provide useful and actionable information on performance and progress against goals such as:
  - Program priorities (including the business)
  - Compliance and/or behavior change
  - Corrective actions and process improvement
- Like any other program, metrics have to be:
  - Properly designed: Visually appealing and easy to understand
  - Economical to collect: Automatic to the extent possible
  - High leverage: Don't collect metrics just because you can
  - Encompass a feedback mechanism in two ways
    - Technical and operational (e.g., tuning and/or corrective actions)
    - Feedback from your consumer (e.g., clarification or additional information requested)

As stated previously, as a security professional, it's your job to understand the quality and progress of your "business of security" as well as communicate value and risks to your leadership in a manner that is easy to consume and relevant enough to make well-informed decisions.

There is not a better, more effective way to understand and communicate all aspects of business than metrics. It's a common language that all leaders understand and has been used for decades. Considering these factors, your metrics program should be a priority.

Your metrics program doesn't need to be all-inclusive out of the gate. Your program can mature over time. However, even in program infancy, your metrics have to be:

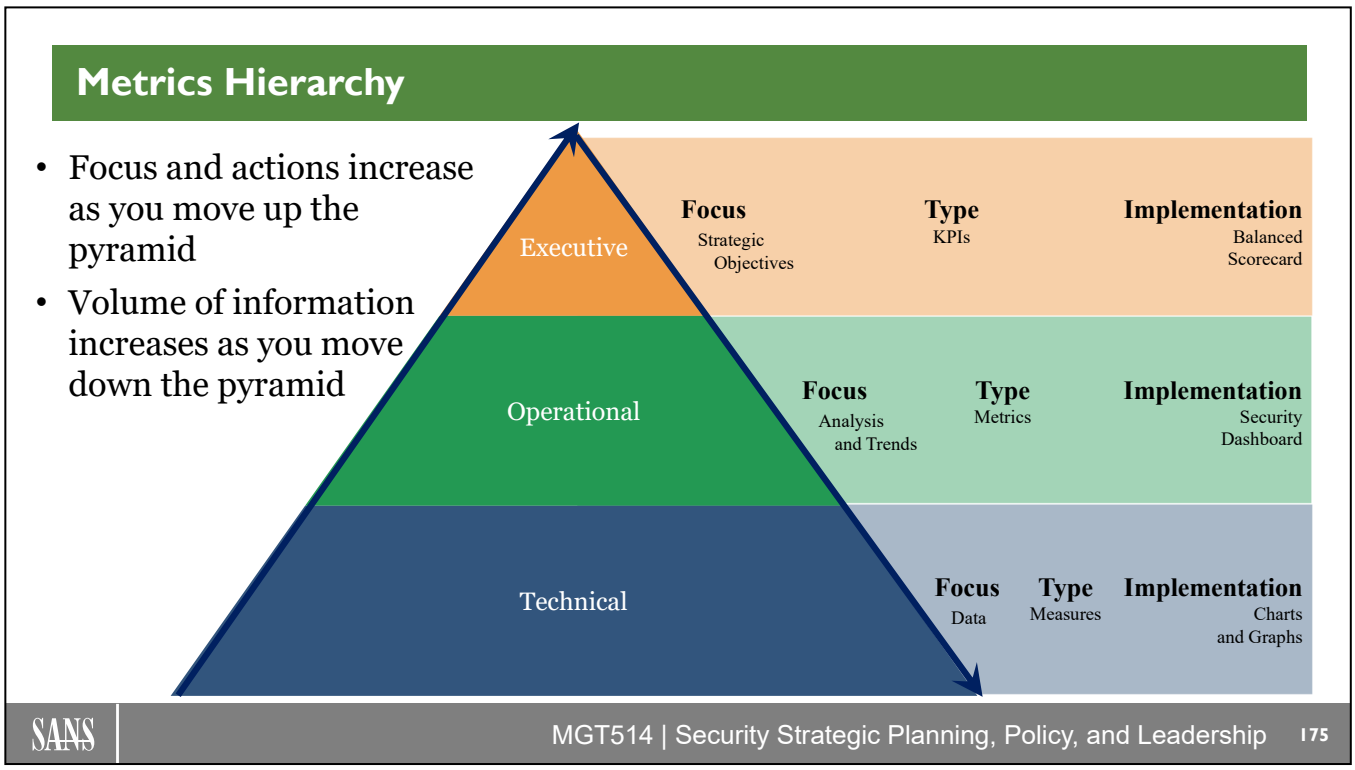
- **Properly designed:** Metrics need to be properly designed in a manner that is visually appealing and easy to understand. If you are the only one who can understand the data or read the story the data is telling, then this information is useless to anyone besides you. As Albert Einstein once said, "If you can't explain it simply, you don't understand it well enough."

- **Economical to collect**: As you develop your program, this should be a prime consideration. With all the metrics options, your program could easily get bogged down in heavy administrative costs to produce. You'll want to automate as many metrics as possible, create a repeatable process to eliminate variation, and rework.

- **High leverage**: Don't collect metrics just because you can. As we mentioned previously, there are numerous metrics that can be collected for a security organization. You want your resources focused on collecting, analyzing, and producing the most valuable metrics to you, your leadership, and the organization as a whole.

- **Encompass a feedback mechanism:** There are two angles to consider as feedback mechanisms:
  - First, from a technical and operational perspective, when the results are produced and analyzed, are there any process and technology considerations that need to change as a result of the results (e.g., policy tuning on network firewalls, corrective actions on processes, etc.)?

- Second, you'll want to work with your leadership, customers, and stakeholders to include any feedback they might have. This feedback might come in the form of questions they have because your metrics were not clear, or items you didn't consider. It might also come in the form of wanting a deeper dive into the root cause of the results.



The metrics hierarchy is an illustrative arrangement or classification diagram designed to help you identify the functional relationships among technical, operational, and executive design elements related to your metrics program. The key thing to remember is focus, actions, and simplicity increase as you move up the pyramid, and volume of information also increases as you move down the pyramid.

Technical
At the base of the pyramid is Technical. The focus here is on data that typically provides a snapshot in time view of specific discrete factors. The example used previously to describe a measurement was 29% (2,574) unauthorized devices on the network. This is the area where you might also include project-level details to include on time and on budget. You might want to evaluate resource allocation or customer satisfaction by team. This is the area you will have detailed data—and lots of it. The implementation or output in this area is typically charts and graphs.

Operational
Moving up the pyramid to Operational, your focus and action increase as described in the first paragraph. In this section, the focus is more on analysis and trends, where you will typically use metrics to describe the results. As a reminder, metrics compare a baseline with two or more measurements such as February, number of unauthorized devices increase by 1,995, and Q1, we had an overall increase of 1,207 (using January as our baseline) as we described in the previous section. The implementation or output in this area is typically a dashboard and for a security organization, this would be a Security Dashboard. We will share attributes of a dashboard coming up later in the section.

Executive
At the top of the pyramid is Executive. Again, your focus and action increase even more. The specific focus in this section is around strategic objectives with results of progress illustrated through Key Performance

Indicators (KPIs). KPIs are performance metrics that illustrate progress toward a stated outcome (e.g., on Wed, Sat, and Sun, we exceeded our target SLAs). Implementation of this section is generally displayed through a tool like the Balanced Scorecard. We will share attributes of a Balanced Scorecard later in this section.

The key takeaway from this slide is to remember as you are designing your metrics program, you wouldn’t likely share "all" technical measures with executives for a couple of reasons. You wouldn’t want to inundate them with data, just because you can, and you want your story to come through loud and clear. You can do this by selecting the high-value KPIs that align with strategic objectives of the organization. At the same time, you wouldn’t want to run your business of security on only KPIs. You need to have more information. You need analysis and trending on your security controls and processes to be well informed as a security leader, and you have to have enough information to make a decision and/or take corrective actions.

Using the Metrics Hierarchy

	Technical	Operational	Executive
Identify	1. # of unauthorized devices on the network 2. Avg. time to detect new devices on network 3. Avg. time to isolate/remove unauthorized devices 4. # of devices blocked by network authorization 5. % of systems not utilizing network authorization 6. # of unauthorized software applications 7. Avg. time to remove unauthorized applications 8. % of systems not running app allowlisting 9. # of software apps blocked by allowlisting 10. Avg. time to detect new software installed 11. Avg. time to remove unauthorized software 13. % of systems that have not been scanned 14. Avg. vulnerability score for systems 15. Total vulnerability score for systems 16. Avg. time to deploy OS software updates 17. % of custom apps that have not been scanned 18. % of database systems that have not been scanned 19. Aggregate vulnerability rating for all apps 20. Avg. time for alerts to be generated and sent to system admin that a vulnerability scan has or has not completed 21. Aggregate score of all penetration tests	1. #, % of authorized vs. unauthorized devices on the network 2. #, % of authorized vs. unauthorized applications 3. Avg. time to remove unauthorized with trend over time on metrics 4. Vulnerability scanning coverage with # of known vulnerability instances with trend over time 5. Avg. time to deploy updates (OS/application) with trend over time	1. % increase in unauthorized devices by business unit Describe risk and any variance or significant drivers to metric.

This table further illustrates how focus and actions increase as you move toward the Executive section, and how volume and information increase as you move toward the Technical section.

In this example, we've elected to use the NIST function "Identify" to illustrate what we've been discussing about the various levels of the metrics hierarchy. We've listed some measurements, metrics, and KPIs to share with you as examples that are likely to appear in each of the respective sections of the pyramid.

Again, you wouldn't want to take 21 measures to your CEO to describe your security controls. Besides the fact that there is too much information, and the information is not sufficient for them to make important decisions, it doesn't answer the "so what?" At the same time, you wouldn't expect your security operations team to manage its business of security with one metric such as that found in the Executive section.

Security Dashboards

- Security Dashboards should:
  - Focus on analysis and trends that impact the overall health of your security organization, which includes:
    - Financial
    - Customer and stakeholder satisfaction
    - Business processes
    - Security metrics
  - Be designed with a security leader in mind
    - High level, multi-dimensional summary showing:
      - Analysis and trends
      - Highlighting anomalies and variations
      - Illustrating progress toward goals

A successful security leader wants to know all aspects of running the business of security. This includes more than just security metrics.

Dashboards are an ideal format to provide the results of your analysis and trends related to operations and security leadership. Carefully selected metrics will provide a good indication of the overall health of the security organization. The key to remember when designing your dashboard is that you need to have an inclusive set of metric categories such as:

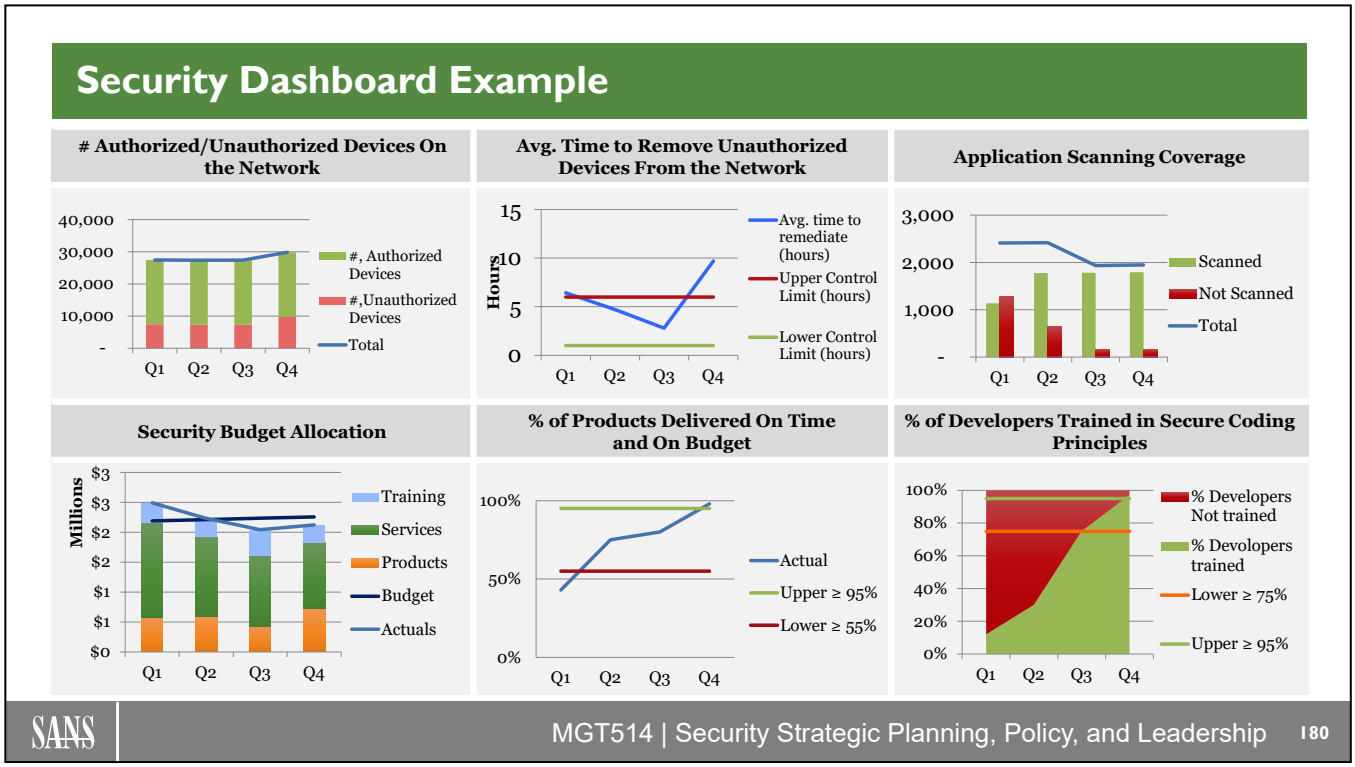
- **Financial:** Metrics that indicate the financial health of your security organization. This might include metrics such as:
  - Security budget allocation, trending, and year-over-year comparison. You might also include categories such as OPEX and CAPEX
  - % of security budget compared to overall IT
  - Run rate on high-priority initiatives

- **Customer and stakeholder satisfaction**: Metrics that measure what's important to your customers and stakeholders. This might also include regulatory agencies or contractual obligations. This might include metrics such as:
  - Percent of security projects delivered on time and on budget with outliers explained
  - Incident and downtime on customer-facing applications such as e-commerce with trend analysis and variation and outliers explained
  - Productivity incidents and time to remediate, with a trend analysis and variation and outliers explained

- **Business processes**: Metrics that communicate how effective and efficient business processes are, and how you are improving over time. This might include metrics such as:
  - Avg. time to deploy updates (O/S and application) against SLA, with trend over time analysis, and variation and outliers explained
  - Avg. time to detect, respond, and remediate an incident against SLA, with trend analysis
  - Avg. time to remove unauthorized devices from the network against SLA, with trend over time

- **Security metrics:** Metrics that indicate how effective and efficient your security controls are, and should illustrate how your security controls are improving. This might include metrics such as:
  - Number of encrypted/unencrypted outbound email containing sensitive information; include false positive, true positive analysis, and trend over time
  - Number of authorized/unauthorized devices on the network including false positive, true positive analysis, and trend over time
  - Number of dangerous websites blocked, with classification analysis and trend over time

Your security dashboard should be designed with the security leader in mind. You need to provide a high-level, multi-dimensional summary of activity across the security organization. Your metrics should clearly show your analysis and trends highlighting any anomalies and variations. You should also be prepared when presenting your dashboard to security leaders, to speak in detail to these anomalies and variations if asked. Lastly, your security dashboard should illustrate your progress toward the goal.



This is an illustrative sample of metrics that would be appropriate to display in a security dashboard, the Operational section of the pyramid. As a reminder, your focus is more on analysis and trends when you are describing your results, and metrics compare a baseline with two or more measurements.

An important thing to remember when you are preparing your security dashboard is that you should be prepared to provide additional details on the trend and any anomalies and/or variances. We will describe two of the metrics illustrated on this page for discussion.

- **Number of authorized/unauthorized devices on the network**: Q1, Q2, and Q3 remain steady. In Q4, the number of unauthorized devices increased by 34% (2,458) over Q3. Further investigation will lead you to determine this increase is the result of a BYOD pilot program your IT department implemented.
- **Avg. time to remove unauthorized devices from the network**: Will tell the story that in Q1, your response time exceeded your upper control limit. This means you have work to do in improving your response time. In Q2 and Q3, you make tremendous improvements toward your goal (lower control limit), but in Q4 your response time rockets past the upper control limit, which indicates this process is in trouble. Do you think this has any correlation to the first metric we discussed, and the root cause could be the BYOD pilot? You need to be prepared to explain this to your leadership.

Below is a reference list of Business Intelligence (BI) solutions that can help you automate the output for your dashboard. They are not in any particular order of preference.

- Microsoft BI using SharePoint and SQL Server Reporting Services (SSRS): https://docs.microsoft.com/en-us/sql/reporting-services/create-deploy-and-manage-mobile-and-paginated-reports
- Pentaho: https://www.hitachivantara.com/en-us/products/data-management-analytics/pentaho-platform.html

- Tableau: http://www.tableau.com
- Domo for BI: https://www.domo.com/roles/bi
- QlikView: http://www.qlik.com
- Birst: https://www.birst.com
- Board: http://www.board.com/

Additional information about other BI solutions and processes can be found at http://thebusinessintelligenceguide.com.

Gemba Board at a Glance (1)

A Gemba board can be an effective place to start for your security reporting efforts.

Jack Nichelson, who was recognized by SANS as one of the "People Who Made a Difference in Security in 2013," provided the Gemba board image above. Paraphrasing, he describes Gemba as the Japanese expression, identifying the location where value is created. Jack's Gemba board is located on a prominent wall near his office that includes security components for five distinct areas of the security department:

- **Security**: Data capturing the risk assessments, attacks, incidents, and other important threat or business metrics
- **Quality**: Performance metrics such as the SLAs delivered by the security team and customer feedback data
- **Delivery**: Metrics about the roadmaps, milestones, and completion schedule for security initiatives
- **Cost**: Information about the budget, costs, and life cycle of security projects being used at the company
- **People**: Training schedule, on-call contact information, and other relevant security team staffing and organizational data

The public nature of the board generates discussions during scheduled stand-up meetings as well as with executives who walk by and stop when something catches their attention. Building a Gemba board can effectively get the security conversation started. What you show and how you display your data will keep the discussion going.

Gemba is often used in lean manufacturing and the "Gemba Walk" is the process of visually identifying areas of improvement by viewing the front lines of a manufacturing floor, workers, and technologies.[1]

Often, Gemba is used to reduce the effects of the seven wastes.[2] These include:

- Defects
- Overproduction
- Stagnate inventory
- Over-processing
- Inefficient employee motion
- Transportation and handling waste
- Waiting or idleness

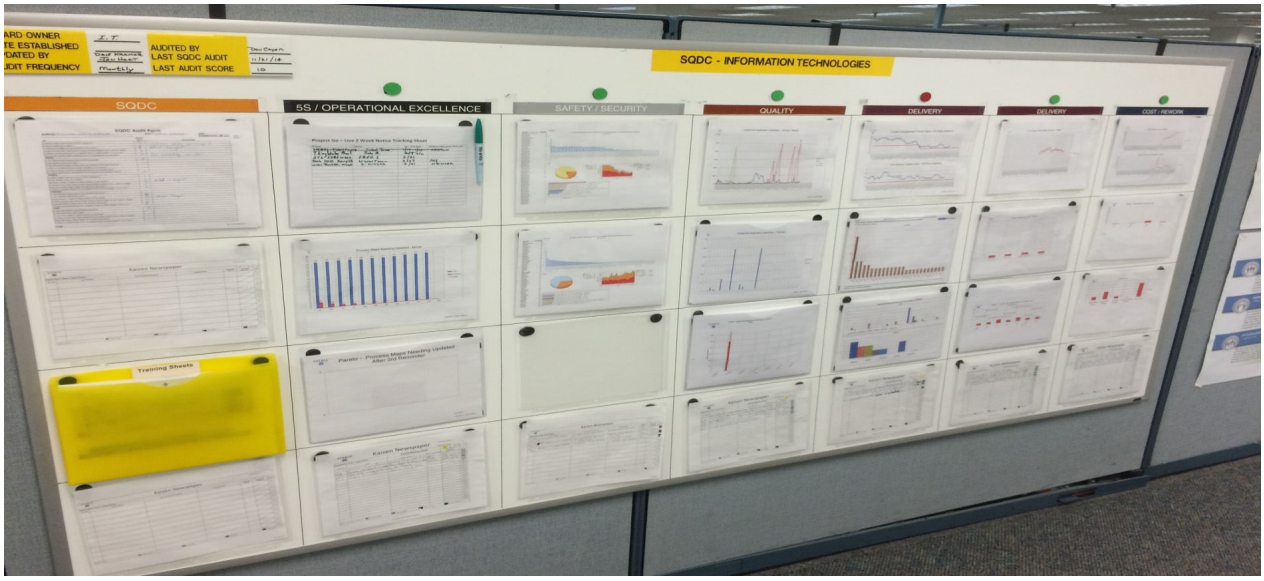
These same principles can be applied to information security.

"The most dangerous kind of waste is the waste we do not recognize." – Shigeo Shingo

References:

[1] http://www.lean.org/WhatsLean/
[2] https://www.systems2win.com/LK/lean/7wastes.htm

Gemba Board at a Glace (2)



In information security, the Gemba board can be a highly effective tool to gather IT and security teams together to review the most relevant metrics or areas where improvement is needed. Socializing and discussing the areas needed for improvement in a regularly occurring discussion can greatly improve the visibility and provide greater accountability for those involved. Gemba boards are also very useful when executives attend the stand-up discussions, and they can be highly effective change agents in organizations that are struggling to get traction with security initiatives.

The Gemba board above was provided by Ed Pollack and is a recent example of an approach that has worked to change culture.

Dr. H. James Harrington on Improvement

"Measurement is the first step that leads
to control and eventually to improvement.
If you can't measure something, you can't understand it.
If you can't understand it, you can't control it.
If you can't control it, you can't improve it."
– H. James Harrington

IBM quality expert Dr. H. James Harrington is credited with developing the cost of poor quality (COPQ) concept.

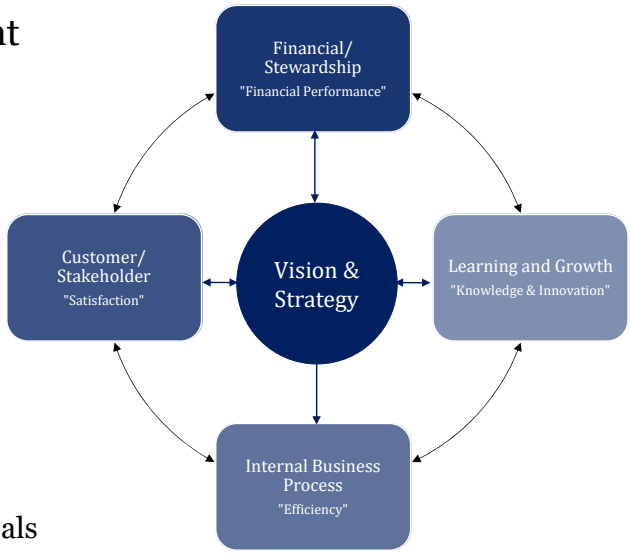
Dr. Harrington defined COPQ in his 1987 book *Poor-Quality Cost*. COPQ is a refinement of the concept of quality costs, or the total costs of related problems associated with creating a quality product or service. IBM undertook an effort in the 1960s to study its internal quality process, and Harrington helped identify process improvement steps and quality measures that made IBM a technology leader.

Dr. Harrington also went on to write other books such as the *Business Process Improvement Workbook: Documentation, Analysis, Design, and Management of Business Process Improvement* and *Statistical Analysis Simplified: The Easy-to-Understand Guide to SPC and Data Analysis.* He also wrote or co-authored dozens of other books including Six Sigma and process improvement handbooks and *The Complete Benchmarking Implementation Guide: Total Benchmarking Management.*

These concepts apply to information security efforts as well. It is critical for security practitioners to provide accurate benchmarking, statistical measurement, and Key Performance Indicators (KPIs) to executives so they can understand current threats, the controls already implemented to mitigate those threats, and the gaps that exist in security controls or policies that are needed to manage the residual risk.

Balanced Scorecard

- Strategic planning and management
  - Executive metrics
  - Focus on strategic objectives
  - Using KPIs
- Used across all industries
  - Including security
  - Align business activities to vision and strategy
  - Improve communications
    - Internal
    - External
  - Monitor performance against strategic goals



As a reminder, at the top of the pyramid is the Executive layer where the focus is on strategic objectives with results of progress illustrated through KPIs (performance metrics that illustrate progress toward a stated outcome). Implementation for this top of the metrics hierarchy pyramid can be displayed through a Balanced Scorecard.

As you design a Balanced Scorecard, don't inundate executives with data. Select high-value information that will tell your story in the most compelling manner. This information should always be aligned with the strategic objectives of your organization.

Balanced Scorecards are used across all industries, including security. If designed well, they can improve communications internally and externally. A Balanced Scorecard generally views an organization from four perspectives to tell a holistic story: 1) financial, 2) capability, 3) process, and 4) customers and stakeholders.

Focusing on all four areas helps keep the vision and strategy aligned.

Financial Stewardship: "Financial Performance"
From a financial perspective, the Balanced Scorecard will measure the financial capabilities of a company, or in the case that we are describing here, for your security organization. It will describe the capability to spend, and/or gain money through profit streams, and very importantly, how you are sustaining your business with existing funds. As we discussed previously, you'll want to look at the Financial Performance on the Balanced Scorecard from two angles. First, how much does it cost to operate Security? This is directly related to your security budget. Secondly, you'll want to include the cost of incidents to your company overall. This would include direct loss, downtime, cost of containment, recovery, and restitution. For metric examples, please refer to the "Metric Selection Is Important" slide.

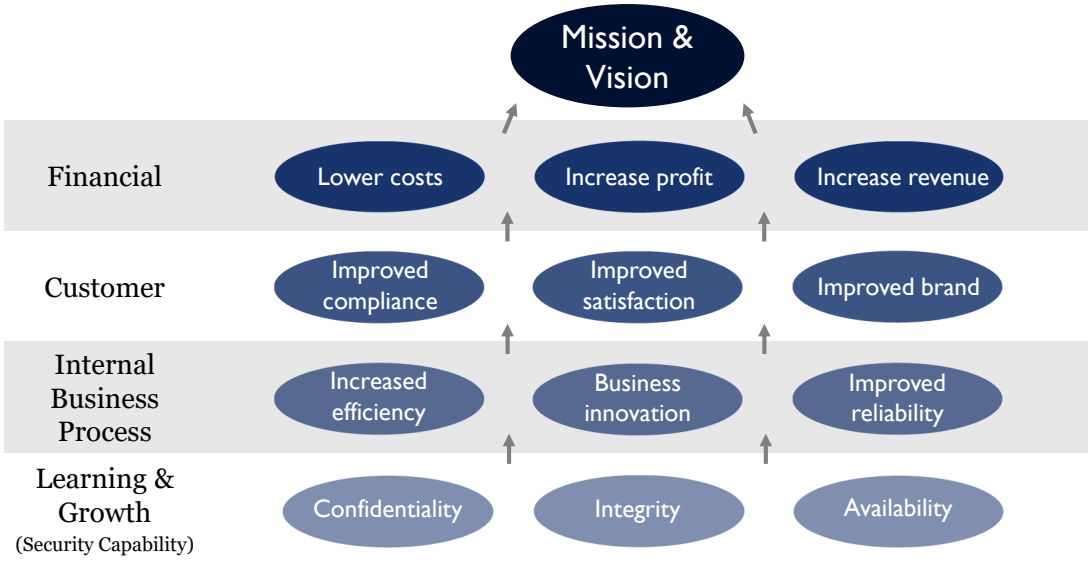
Customer/Stakeholder: "Satisfaction"
Select KPIs for this section that are important to your customers and stakeholders. You must understand what types of services or business processes your security organization provides and what they value. For instance, Finance and IT might value the percent of security projects delivered on time and on budget, whereas Sales and Marketing might value customer-facing incident time to remediate from their customer-facing e-commerce sites, and Legal and HR might value meeting SLAs to produce electronic evidence files involved in investigations.

Internal Business Process: "Efficiency"
In this section, the KPIs communicate how effective and efficient your business processes are, and how you are improving over time. As a reminder, the results in business processes often influence how satisfied our customers are, and it's equally, if not more important, to select KPIs for this section that our customers will value.

Learning and Growth: "Knowledge and Innovation"
In this section of the Balanced Scorecard, you want to include indicators that illustrate your security organization is improving from a capability and capacity standpoint, such as improving tools and technology, and how you are improving knowledge and skill sets, such as strategic security awareness training for the organization or how you are developing and retaining top talent. You might want to "customize" this category for security by naming it "Security Capability" to make it more meaningful for your team.

Reference:
http://www.balancedscorecard.org/BSC-Basics/About-the-Balanced-Scorecard

Mapping to Strategic Objectives



In Section 1, we introduced "Mapping to Strategic Objectives." As a reminder, we as security professionals often focus on the bottom row of this diagram; improving our security capabilities by increasing our knowledge and skills or improving our tools and technology. It's critical that we expand our line of sight and align our activities and efforts to the overall strategic objectives for the organization as a whole, which includes Internal Business Process, Customer/Stakeholder, and Financial/Stewardship.

Mapping your organization's strategic objectives to the Balanced Scorecard quadrants will help you tell the story of how value is created by your security organization. A diagram such as this will highlight the cause and effect of your security initiatives and activities that will make sense to the business as a whole. As an example, if you were to have a strategic initiative to support business innovation/new product support, that would, in turn, improve customer/stakeholder satisfaction and likely increase revenue. This is something the business understands and appreciates.

Reference:
http://www.balancedscorecard.org/BSC-Basics/About-the-Balanced-Scorecard

Translating Security Vision & Strategy

Financial/ Stewardship	**How much does security cost to operate?** • Security budget as a % of IT • Budget including CAPEX, OPEX • Lower costs, increased revenue, increased profitability	**How incidents financially impact your company** • Direct loss (e.g., IP, customer lists, trade secrets, loss or destruction of assets) • Cost of downtime (e.g., refunds, or failed transactions) • Cost of containment, recovery, and restitution
Customer / Stakeholder	• Improved compliance & regulatory (e.g., security controls of impacted systems and reporting capability) • Lower wait times (e.g., meeting SLAs on evidence to HR/Legal, and on-time, on-budget delivery of projects) • Improved satisfaction (e.g., responsiveness in time to remediate incidents on customer facing sites)	
Internal Business Process	• Improved availability & resiliency (e.g., time to detect, respond, remediate outages caused by incidents) • Increased process efficiency (e.g., time to remove unauthorized devices from the network) • Lower cycle times (e.g., response time for customer facing security activities) • Business innovation/new product support (e.g., response time for security assessments)	
Security Capability	• Improved knowledge & skills (e.g., security awareness training completion rate and/or phishing results) • Improved tools & technology (e.g., false positive trends on customer visible security controls such as encryption)	

Now that you've mapped your organization's strategic objectives and you have a better understanding of what is important for your organization, you will need to translate this information to your Security Vision and Strategy in order to ensure the output of your Balanced Scorecard has meaningful information that you can share with executives. As a reminder, you don't want to inundate executives with data just because you can.

Dashboard Example

Financial/ Stewardship	Customer/ Stakeholder	Internal Business Process
Q4 % Product Development Budget Allocated to Security	**Q4 % of Products Delivered On Time and On Budget**	**Q4 % of Developers Training in Secure Coding Principles**
Target 5% ✓ **Trend** → **5%**	**Target 95%** ✓ **Trend** ↑ **95%**	**Target 95%** ✓ **Trend** ↑ **97%**
• Increased support for legal as they piloted their case management system	• 18% increase over Q3 in on-time and on budget delivery. Security staffed temporary PMO team to meet goal	• 100% of flagship application developers completed training reducing overall risk to organization
Q4 & YTD Security Budget Allocation	**Customer Satisfaction**	**Q4 % of Developers Attaining Certification**
	Target 90% ✗ **Trend** ↑ **85%**	**Target 95%** ✗ **Trend** ↑ **42%**
	• 8% increase over Q3 in customer satisfaction rating of 4 or higher out of 5 possible	• Mitigation plan: Follow-up with developers after training is complete for certification

	Q1	Q2	Q3	Q4	YTD
Products	$575,000	$597,000	$425,000	$732,000	
Services	$1,590,000	$1,320,000	$1,190,000	$1,090,000	
Training	$326,000	$315,000	$427,000	$301,000	
Actuals	$2,491,000	$2,232,000	$2,042,000	$2,123,000	
Budget	$2,190,000	$2,211,900	$2,234,019	$2,256,359	
$ Variance	-$301,000	-$20,100	$192,019	$133,359	

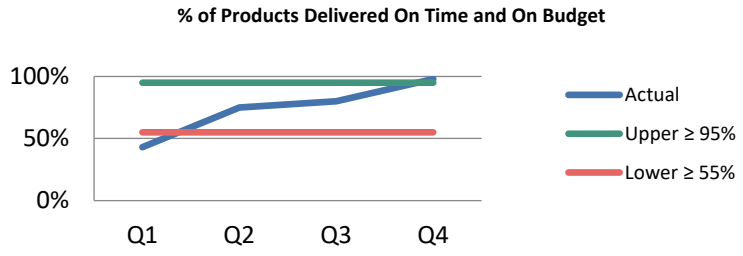
SANS | MGT514 | Security Strategic Planning, Policy, and Leadership 190

Earlier in this section, we talked about the shift we are seeing in Security where more and more security professionals are being brought before executives and asked to demonstrate the effectiveness of their security program. Executives and board members want to quickly understand whether the decisions they made to fund security has helped achieve a competitive advance or will help keep them out of the news.

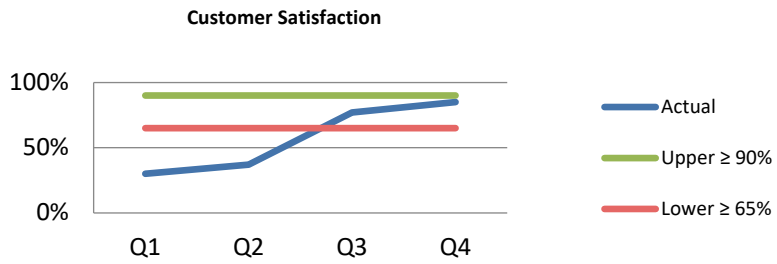
It's important to remember that executives are tasked with making many decisions in a day across multiple lines of business. The more relevant, useful informative information you provide to them, the more confidence they have in you and your security capabilities, and the easier it is for them to come to an informed conclusion and make decisions.

It's critical that you find the right KPIs that are of value. It's equally as important to provide a multi-dimensional view so they have a complete understanding of targets and trends, and very high-level summary of trend drivers. You will see we elect to display a much different view for our executives than the charts and graphs we use on a security dashboard.

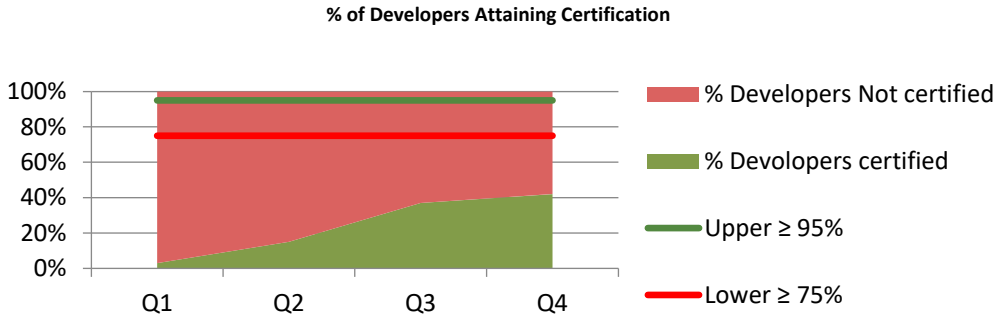
As an example, look at the middle top tile—Q4% of products delivered on time and on budget. We have met our target of 95%. Our trend indicates a positive increase, so we describe the driver behind this; for example, 18% increase over Q3, because we staffed a temporary PMO team to meet goals.



Another example is in the middle bottom tile—Customer satisfaction. Our trend over time is increasing, showing an 8% increase over Q3 results. We have not met our target of ≥ 90%, but we are within the control limits we established.



One last example is in the right bottom tile—Q4% of Developers Attaining Certification. We have a target of ≥ 95% and our trend is increasing over Q3 results, but we are still well below our lower control threshold of ≥ 75%. You will want to let executives know what you are doing to turn this KPI around to reflect positive results as in this example—you will do an immediate follow-up with developers right after training to encourage certification completion.



Security Capability Dashboard Example

Security Capability	Status	Trend	Highlights

Identify: Manage risk to systems, assets, data, and capabilities	Yellow	↑	• 32% increase in unauthorized devices
			  • 29% IT
			  • 3 % HR
			• 27% increase in unauthorized software
			• Attributed to Q4 BYOD pilot

Protect: Ensure delivery of critical infrastructure services	Green	→	• 12% of users failed sponsored email phishing tests • 15% of employees have not passed security awareness assessments
Detect: Identify occurrence of a cybersecurity event	Green	↓	• 27% decrease in elevated access accounts • 275 total elevated access accounts
Respond: Take action regarding a detected cybersecurity event	Green	→	• 5% of database systems with sensitive information have not been scanned by vulnerability scanners
Recover: Maintain plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity events	Red	↑	• 34% of systems not enabled with up-to-date anti-malware • Attributed to Q4 BYOD pilot

In this example, we are using the NIST Cybersecurity Framework functions as technology categories and have selected KPIs that align to security related projects and capabilities.

As a reminder, you want to be very selective with what you choose to display on your Balanced Scorecard in this section. You have to provide just the right amount of information to answer the "so what" and allow them to make important decisions in a very short amount of time.

Balanced Scorecard Example

Financial Objectives		G
Help grow the business		A
Deliver projects on time and on budget		G
Manage suppliers cost effectively		G

Stakeholder Objectives		A
Help get drugs to market faster		A
Build trust with customers		R
Maintain availability of key systems		G

Business Process Objectives		R
Comply with appropriate regulations		R
Embed automation into security processes		A
Manage risk within defined risk appetite		R

Security Capability Objectives		A
Provide safe spaces for drug research		G
Provide the right access at the right time		A
Build a security and risk aware culture		A

Selection of objectives for the Balanced Scorecard is very important. The Financial, Stakeholder, Business Process, and Security objectives should align with what's important to the organization. We've established that there are many metrics you could use to describe your security controls but, for this section, you really want to select metrics that will be meaningful to executives and what they need to know versus what you want to tell them.

What executives need to know is how is security improving the risk posture of the organization, how is security supporting strategic imperatives, what business units should they be concerned with, and how you are going to keep your executive team out of the news. You'll want to do this through displaying improved knowledge and skills, and improved tools and techniques.

Metrics Visualization Considerations

- When you build your metrics program:
  - Discuss visualization strategy with your Marketing team
    - They are experts in message management
    - Will help you follow branding and style guides for your organization
  - Avoid busy-looking charts and graphs that appear cramped or confusing
    - Test your message on subject matter experts
      - To ensure the message you're trying to convey is the message that will be received
        - Balanced scorecards: Test on someone who is non-technical
        - Security dashboards, charts, and graphs: Test with your security peers
  - Remember there is an element of art and design in this work
    - Use colors in a familiar way (e.g., green = good, and red = bad)

You've gone to great lengths to build your metrics program from gathering raw data and turning this into valuable information for you and your teams, leadership, customers and stakeholders, and the executives of your organization. It's vital that your reports—whether they are charts and graphs, a security dashboard, or a Balanced Scorecard—are relevant and, most importantly, persuasive. But that's not enough. The data must be portrayed in a manner that is visually appealing, logical and tells the story you are intending.

You can avoid confusion regarding the meaning of your information if you are mindful of your audience. Take your security hat off and put your business hat on and view it through the lens of your audience.

In addition to this, you'll want to discuss your visualization strategy with the Marketing team or an employee that has experience in design. Your marketing department has experts in product design and can help you manage your message effectively and help you follow branding and style guides for your organization.

Avoid busy-looking charts and graphs that appear cramped or confusing. You might want to test your message on subject matter experts to ensure the message you're trying to convey is the message. You might also want to test on someone who is non-technical to ensure your information is business consumable. For the security dashboard and associated charts and graphs, you might want to test on your peers to ensure alignment with your message.

There is an element of art and design in this work. You will want to use colors in familiar ways (e.g., green = good, and red = bad). When using colors, you also need to factor in the chance that your report might be printed out in black and white or a member of your audience might be color-blind. It's always good practice when using colors to accompany the color with its designated work.

Metrics Communication Guidelines

- Executive/Balanced Scorecards
  - Focus on strategic objectives (high level and business consumable)
  - Monthly review with executives and key stakeholders
  - Monthly or quarterly review with Board of Directors
- Operational/Security Dashboards
  - Focus on analysis and trends
  - Monthly review with security leadership and metrics owners
  - Real-time alerts when process and/or technology deviates outside control limits
- Technical/Charts and graphs
  - Focus on data and measurements
  - Daily, weekly, monthly review as appropriate
  - Staff meetings and/or direct report meetings (1:1's), cross-functional team meetings

Security is not exempt from demonstrating value, and your metrics program is an ideal way to communicate and socialize your efforts whether it's across your teams, to your peers, for your leadership and executives, and to your customers and stakeholders.

We've provided a basic set of guidelines on this slide for each of the sections we've covered: Technical, Operational, and Executive. It's understood that you might have additional communication requirements and you might need to customize your communications methods and cadence to meet the needs of your organization.

Metrics: Pitfalls To Avoid

- Not getting leadership support
  - Show how your efforts can better demonstrate Security's commitment and value
- Too much information, too soon
  - Be selective
  - Collect feedback and incorporate it
- Wrong information
  - Select information appropriate for your audience (e.g., leadership, executives versus operations)
- Inaccurate, misleading, and/or incomplete information
  - Check and recheck your information for errors
  - Define confusing terms and all acronyms

Get leadership support
You need to gain support before you begin to develop your metrics program. The best way to do this is by showing them how your efforts can better demonstrate Security's commitment to supporting organizational strategic imperatives and better indicate the overall health of the security organization.

Too much information, too soon
We have established that there is an abundance of data related to security that can be translated into valuable information, but just because it's there doesn't mean you need to use it all. Be selective on what you display, solicit feedback to ensure value, and build on your program and collect only data that is used. There is nothing more frustrating to teams that generate an output that goes into a black box and nobody sees it.

Wrong information
This has been a historic problem not only in Security and across all industries. People want to display what's important to them in an effort to describe how busy they are, and how much value they bring to the organization. What is important to a security operations analyst might not be what a CEO needs to know. This is not meant to diminish what's important to security operations analysts—they are very valuable and that's why they were hired to do the job, but the information analysts need to do their jobs more effectively and more efficiently might not be the same information a CEO needs to know to make a decision to fund security initiatives. Make sure you select the right things to share, and they are addressing the questions people are asking.

Inaccurate, misleading, and/or incomplete information
A good practice is to always validate and revalidate your information. There is nothing that will take your credibility away faster than if you have reporting errors or misleading information. Make sure you clarify the intent of your information with others to ensure the same message received is the same message you intended to deliver. It's always a good idea to define any terms and acronyms that might be confusing to your audience.

Metrics Planning Worksheet

PHARMACO

Strategic Objective	Security Initiatives	Metric (over time)
Get drugs to market faster	• Secure mobile apps for clinical trials	
	• Provide security assessments for research systems	
	• Ensure availability of key research systems	
Provide safe spaces for drug research	• Decrease patch deployment time on research systems	
	• Implement DLP to monitor for IP loss	
	• Create 24x7 SOC to quickly respond and recover	

PharmaCo has two important strategic objectives:

1) Get drugs to market faster.
2) Provide safe spaces for drug research.

Every department in the company must support these two objectives because they help drive increased growth and revenue.

In the "Initiative" column, Paul has identified some key actions and proposals from the team's Gap Analysis and mapped them to these strategic objectives. In the "Metric" column, write down at least one metric that can be used to track progress toward supporting the business.

Security Metrics Examples

PHARMACO

Strategic Objective	Initiative	Example Metric (over time)	Example Goal
Get drugs to market faster	• Secure mobile apps for clinical trials	• % of mobile devices using MDM • % of mobile apps built with standard controls	• 100% coverage • 100% coverage
	• Provide security assessments for research systems	• % of systems deployed on time • % of assessments completed w/in SLA	• 95% deployed on time • 95% completed w/in SLA
	• Ensure availability of key research systems	• % of researchers served • % availability of research systems	• 100% researchers served • 99.999% availability
Provide safe spaces for drug research	• Decrease patch deployment time on research systems	• % of systems patched on time	• 90% patched on time
	• Implement DLP to monitor for IP loss	• Amount of revenue lost due to stolen IP	• $100,000 million
	• Create 24x7 SOC to quickly respond and recover	• % of incidents with same root cause	• 0%

A key component of creating meaningful metrics is to ensure that they meet overall business goals. On this slide, we see two of PharmaCo's strategic objectives: 1) Get drugs to market faster and 2) Provide safe spaces for drug research. These goals indicate that PharmaCo is extremely focused on growing revenue by creating new breakthrough drugs. Its scientists and researchers are key to this effort and, as a result, the ability to serve researchers and enable them to do their work effectively and quickly is of extreme business importance.

Getting drugs to market faster requires new mobile apps that support clinical trials as well as access and availability of key research systems. Because these are important business initiatives, it's important that security aligns with them by providing appropriate protections. This includes mobile device management (MDM) software to ensure that mobile devices are encrypted and mobile application development controls like access control (% of mobile devices using MDM and % of mobile apps built with standard controls). However, it's not enough to simply enable these controls. Security needs to provide these tools and assessments as quickly as possible to align with PharmaCo's needs to get to market quickly (e.g., % of systems deployed on time and % assessments completed within SLA). Ultimately, this means happier researchers (% of researchers served).

In addition to enabling key systems, security must also protect the organization's key assets (% of systems patched on time), safeguard intellectual property created by researchers (e.g., revenue lost due to stolen IP), and continuously improve security capabilities (% of incidents with same root cause).

With these metrics in place, Paul can now determine the target state. These are represented in the "Example Goal" column. This takes into account the current state and, by implication, the delta of improvement. This is extremely important to define and might be unique for your own organization, because the threshold that you define as the goal represents your Key Performance Indicators (KPIs) by which you will identify leading or lagging indicators to see whether there is a problem to which management must respond.

Metrics in Summary

- Make sure your metrics program is:
  - A priority for your organization
    - Designed to depict the overall health of your security organization
    - Leveraged to identify improvement opportunities
    - Included in team goals
  - Simple to collect data (preferably automated)
    - Actionable
    - Measured frequently
  - Related to the business
    - Appropriate amount of information for your audience
    - Easy to interpret
    - Evangelized to educate, communicate, and build credibility

When we introduced this metrics section, we stated that paving the road to success depends on you and your leadership team being well informed and having the right information to make the right decision; and, as a security professional, it's your job to do that—understand the quality and progress of your "business of security."

Ensuring your metrics program is a priority for your organization will ensure a greater level of success. Your metrics program should be designed to depict the overall health of your security organization as well as identify improvement opportunities to make your security processes more effective and efficient. One way to ensure your metrics program is a priority is to include this in everyone's goals and make everyone accountable in some manner.

Your metrics program should be simple to collect. Automation is a consideration for addressing this concern. Your metrics program should be actionable and measured frequently depending on the respective needs and demands of your organization.

Most importantly, your metrics program should be integrated with the business and include only information that is relevant to your audience. Your output should be easy to interpret and should certainly be evangelized at every opportunity to educate customers, stakeholders, leadership, executives, and board of directors. Your metrics program is a mechanism for you to build credibility for your security efforts.

This page intentionally left blank.

End of Round 1

- End of Round 1 scoring adjustments
  - For every $250k spent beyond your budget
    - Decrease Security Culture by 1 point
  - For every 1 time unit spent beyond your plan
    - Decrease Security Culture by 1 point
  - For every 1 point greater than three for each Security Function dial
    - Increase Security Culture by 2 points

For each Round of play, the Security Culture score is adjusted.

For every $250k spent beyond your budget, decrease your Security Culture score by 1 point. For example, if you have a -$500k budget, then decrease Security Culture by 2 points.

For every 1 time unit spent beyond your budget, decrease your Security Culture score by 1 point. For example, if you have -4 time points, then decrease Security Culture by 4 points.

For every 1 point greater than three for each Security Function dial increase Security Culture by 2 points. For example, if your Decipher dial is 4 and your Develop dial is 5, then increase Security Culture by 6 points.

CYBER42

Event #6

Debrief

This page intentionally left blank.

Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Define Current State
  - Vision and Mission
    - Lab #1: Mission Statement
  - SWOT Analysis
    - Lab #2: SWOT Exercise
- Develop the Plan
  - Visioning and Innovation
  - Security Framework
  - Security Roadmap
    - Gap Analysis
    - Lab #3: Roadmap Development
  - Business Case Development
- Deliver the Program
  - Security Metrics Program
  - ***Marketing and Exec Communications***

This page intentionally left blank.

Marketing and Executive Communications

- Goals of this section
  - Learn to promote your strategic efforts
  - Understand why marketing is important to security
  - Learn how to develop effective marketing
  - Learn how to effectively communicate with executives

The goals of this "Marketing and Executive Communications" section are for you to learn to promote your strategic efforts and understand why marketing is important to security. A marketing framework is also provided that will take you through the steps of how to develop an effective marketing plan and, most importantly, how to effectively communicate with executives.

What Is Marketing?

- Internal and/or external activities for a security organization that:
  - Builds your brand
  - Promotes your value
    - Products and services
    - Capabilities
    - Skill sets
    - Relationships
      - Stakeholders
      - Customers
      - Employees

Simply stated, marketing for a security organization is all of the activities you can do internally and/or externally, to build or enhance your brand and promote the value of your security organization. You might want to market things such as the products and services your team provides, your capabilities and team skill sets and lastly, you might even want to promote your relationships such as your partnership with key stakeholders or customers, or the top talent of your employees, and the industry expertise they have.

Internally, you might want to market to your own security team (or to other teams within your company) and company executives, or your stakeholders. You may want to market externally to your customers or possibly even outside industry experts.

Your marketing is limited only by the activities you decide to take on in your marketing efforts, and the number of people and/or groups you determine should hear your marketing messages, which we will discuss later on in this section.

Why We Need Marketing

- Security is no longer just an IT issue
- Marketing ensures that you:
  - Stand out from other organizations in your company
    - Gain support for your overall strategic plan
    - Increase funding
    - Improve employee satisfaction and retain top talent
  - Maintain or gain an advantage over your competitors to:
    - Attract and retain top talent
    - Strengthen brand/image
    - Build partnership in the community

Security is no longer just an IT issue. The topic of security has reached the Board of Directors and most Boards have heard the message loud and clear that security is important. This doesn't, however, give you an automatic pass on marketing, and a blank check. Security budgets still need to be balanced with other investments, and as a security leader, you will want to develop a competitive advantage and stand out from other organizations in your company.

In addition to standing out from other organizations in your company, you can gain vital support on your overall strategic plan and/or any initiatives you are taking on. You can use marketing to increase funding for your team and/or initiatives. You can even market to your team to improve employee satisfaction and retain top talent.

Outside of your company, you can use marketing to maintain or gain an advantage over your competitors to attract top talent to your team and strengthen your company and your specific security organization's brand and image. You can use marketing to build partnerships in the community.

For the bottom line as a security organization, people need to hear and understand your value as stated in the previous slide. Through these efforts, you begin to build or enhance your brand and gain a competitive advantage through your marketing efforts.

Marketing is imperative to the successful adoption of your strategy and/or security initiatives, as well as retaining top talent, and all the other benefits we discussed thus far and will continue to expand on as we progress through this section.

Steve Jobs on Marketing

"Marketing is about values.
It's a complicated and noisy world, and
we're not going to get a chance to get people to
remember much about us. No company is.
So we have to be really clear about
what we want them to know about us."
- Steve Jobs

Steve Jobs is quoted as saying, "Marketing is about values. It's a complicated and noisy world, and we're not going to get a chance to get people to remember much about us. No company is. So we have to be really clear about what we want them to know about us."

Jobs was the undisputed king of "wow" marketing. He was also considered one of the most charismatic business leaders in the world. He took every opportunity to market to others, and he made it look effortless. He did this through simplicity, but the truth is, he worked very hard to make it look simple.

Jobs says that marketing is not about touting features and speeds and megabytes or comparing yourself to the other guys; it's about identifying your own story, your own core, and being very clear about what you are all about, and what you stand for … and then being able to communicate that clearly, simply and consistently. Jobs believes that brand should always come back to its core values.

As Apple's CEO, Steve Jobs will be remembered for many things—not just a purveyor of innovative, landscape-changing products. He'll also be remembered as one the most powerful and charismatic orators and marketers of our time.

For additional highlights on Jobs' values and identifying your core, top speeches and marketing lessons Steve Jobs taught us, please see the following URLs:

- http://www.presentationzen.com/presentationzen/2011/10/steve-jobs-on-values-and-identifying-your-core.html
- http://www.pcworld.com/article/238905/top_three_steve_jobs_speeches.html
- http://postcron.com/en/blog/10-amazing-marketing-lessons-steve-jobs-taught-us/

Marketing for Security

"Marketing for a security organization is about making security relevant to the business and the business relevant to security."
- Jaynie Bunnell

"Marketing for a security organization is about making security relevant to the business and the business relevant to security." Security is complex by nature, and not easily understood by people who are not security professionals. Not only that, security has primarily been a back-office function for years and just recently, security leaders have been given the opportunity to sit at the table with business executives and the Board of Directors.

If you can't effectively articulate security relevance to the business, you are seen as just another IT cost, and this is not an ideal perception that will by any means win you support and buy-in for your strategy and/or initiatives. Remember, your security team is competing for funding and support with other organizations, and these organizations are likely to provide distinct value that is generally understood throughout the business, such as your sales and marketing teams who are generating revenue, your accounts receivable teams who are collecting money, research and development teams who are developing products to take to market, etc.

The key to determining how to make security relevant to the business is to think beyond the technology and consider how your team enables the business. We've talked about this concept in nearly all the content we've covered so far. Find stories of interactions and events where the security team has helped the business get its business done. Some examples include:

- Application security team creating secure code development training for the Web Development team, enabling it to develop more secure code for your company's online transactions to protect customer and cardholder data
- Incident response team is on call for executives to address any security-related concerns such as phishing emails by providing immediate support as questions arise

In addition to the stories of interactions, use the content you've generated throughout the strategic planning process. Think back to the PEST and Porter's Five Forces examples that we worked through. In PEST, we determined that security could develop relationships with airline intelligence agencies and monitor potential terrorist activities, as well as provide due diligence before airline consolidation by providing M&A security

technology reviews and monitoring for potential data loss. Lastly, we said that security could provide forensics and eDiscovery services as support for legal cases. These examples illustrate how security can enable the business and go well beyond describing security controls, further enabling you to have a deeper, more meaningful dialogue with your business partners and executives.

Making security relevant to the business is not enough! You must also make the business relevant to security. If security doesn't understand the importance of the business, it might, in fact, hinder instead of enable. Think back to the stakeholder management story of Robert Taylor and his missed opportunity. As you recall, Bob took the lead on a network blocking security initiative, and he didn't engage all of his stakeholders. Bob thought his project was a straightforward security technology deployment, and he didn't take the time to understand the business impact of his efforts. He blocked the network as designed, but as a result, Bob also blocked the sales team and research and development team from access to vital information they needed to do their job. Remember, these two teams generate revenue and develop new products for the company. Bob also caused additional work for the Help Desk because he did not consider business relevance in his technology deployment.

This is not an easy concept, and it takes a lot of consideration and practice, but as security leaders interact with executives, and security teams interact with business partners more and more, you will find it necessary to master this skill for your continued success.

Marketing: It's a SNAP

- Strategic planning work from earlier
  - Can be leveraged to market your organization
- Invest time in creating a solid marketing plan
  - Information can be repurposed
- SNAP marketing has four key components

Specify	Marketing Objectives
Niche	Identify Value Proposition
Audience	Identify Target Market
Promote	Distribution Strategy

The approach outlined in SNAP marketing is fairly straightforward and simple to develop and execute. The SNAP marketing method has four key components that drive your marketing plan through successful execution:

Specify: Marketing objectives. You'll need to determine your marketing goals. As an example, you'll need to decide whether you want to strengthen the stakeholder relationship and gain support, establish brand awareness, retain and/or recruit top talent, increase your revenue, increase funding, etc. Once you determine the goals you want to target in your marketing plan, you'll need to describe some specifics around the goal.

Niche: Identify Value Proposition. Having a strong value proposition is of critical importance, because it distinguishes your organization from others in your company to your stakeholders and business partners, against competitors, to your employees and future employees, and to your customers.

Audience: Identify Target Market. These are the people and organizations that are key to your continued success, such as executives, business units, employees, and customers.

Promote: Distribution Strategy. You need to determine the most effective method by which you promote your marketing—in other words, how your messages will reach your audience. This is your distribution strategy, and it includes critical components needed to execute a successful marketing effort.

It's necessary to invest appropriate time in creating a solid marketing plan using the SNAP components. The good news, however, is the SNAP method is designed to leverage the output from your strategic planning work you've already completed in this course, such as Threat Analysis, Historical Analysis, Gap Analysis, Security Roadmap, Metrics and Dashboards, SWOT Analysis, Vision and Mission, PEST Analysis, Porter's Five Forces, Values and Cultures, Stakeholder Management Strategy, and project planning.

You will find that once you've created and refined the messages from this framework, you will have a ready portfolio of information available to you for multiple uses, such as meetings with executives, teams, stakeholders, vendors, or the output of this effort can be used for vendors, customers, or potential employees.

References:
http://www.forbes.com/sites/davelavinsky/2013/09/30/marketing-plan-template-exactly-what-to-include/
https://smallbusiness.chron.com/essential-elements-marketing-plan-60625.html
http://www.investopedia.com/terms/m/marketing.asp
https://www.everclearmarketing.com/blog/top-5-cybersecurity-marketing-challenges-and-how-to-overcome-them#.VU5y4Os2JUQ

Specify: Marketing Objectives

- Determine marketing goals
  - Increase funding and/or revenue
  - Build stakeholder relationship and gain support
  - Establish brand awareness
  - Retain and/or recruit top talent
- Specify your objectives as brief descriptions that are business consumable
  - Example goals from PharmaCo

- Attackers don't sleep, so we can't either
  - Fund 24x7 Security Operations Center
- Share intelligence to respond and block attacks
  - Establish Cyber Threat Intelligence function

Every marketing plan needs objectives and a way of measuring success (metrics) to ensure your marketing efforts are not wasted. You'll need to determine your marketing goals. As an example, you'll need to decide whether you want to strengthen stakeholder relationship, and gain support, establish brand awareness, retain and/or recruit top talent, increase your revenue, increase funding, etc. Once you determine the goals you want to achieve, you'll need to describe some specifics around the goal.

Stating that you want to increase stakeholder engagement and buy-in for additional funding isn't specific enough. Think about what actions you want your target audience to take after they are made aware of your campaign or promotional activity. In the example above, Paul Williams is acutely aware that attackers don't sleep, and in order for the security team to defend the company, a 24x7 Security Operations Center must be funded and a Cyber Threat Intelligence function must also be established. Paul is very specific about his marketing objectives and has translated them into business consumable language that non-security professionals can understand.

Paul used outputs from the strategic planning process, such as Threat Analysis, Historical Analysis, Gap Analysis, Security Roadmap, Metrics and Dashboard, and SWOT Analysis to determine where he should focus his marketing objectives.

In the Threat Analysis section, he gained an understanding of how attackers work by applying the Intrusion Kill Chain, and that threat intelligence can create a feedback loop that can be used to disrupt attackers. He also learned that defenders must move detection and analysis up the kill chain, and implement defenses across the entire kill chain, and lastly, the intrusion kill chain provides a structure to analyze intrusions, extract indicators, and drive defensive courses of action.

In the Historical Analysis section, he learned that the company is facing increased risk due to the evolving threat landscape such as organized crime, advanced persistent threats, and increasing business requirements such as Cloud computing, Big Data, and the Internet of Things, which all result in operational risks.

In the Gap Analysis section, it was identified that the current state of defense was limited, due the inability to mitigate attacks and limit the amount of data loss.

The Security Roadmap section identified numerous initiatives, such as Establishing a 24x7 Security Operations Center and Cyber Threat Intelligence capabilities. It was at this point that he realized there weren't enough resources to do everything at once—budget needed to be secured and staff needed to be put in place.

Through the SWOT Analysis (Specifically, the Weaknesses, Opportunities, and Threat quadrants), we learned that PharmaCo has access to talent around the world. It also confirmed that security is decentralized and understaffed. The opportunities also confirmed the need to operationalize around the kill chain and leverage the global presence to build a 24x7 team, and increase staffing levels. Most importantly, this section confirmed there are threats that are cause for alarm. These include insider threats due to a geographically dispersed workforce, competitors seeking intellectual property, and lastly, nation-states seeking to accelerate research and development, which could all potentially result in data loss.

Niche: Identify Value Proposition

- How is your organization, department, or team different?
  - From other organizations in your company
  - For stakeholders and business partners
  - Against competitors
  - To your employees and future employees
  - For your customers
- Specify your value proposition as a brief paragraph
  - Example from Paul Williams who was promoted to PharmaCo CISO

"Help people lead healthier lives by
creating safe spaces for drug research and innovation."

Having a strong value proposition is critically important because it distinguishes your organization from others in your company, to your stakeholders and business partners, against competitors, to your employees and future employees, and for your customers. The hallmark of great companies is their niche or value proposition. For example, FedEx's Unique Selling Proposition (USP) of "When it absolutely, positively has to be there overnight" is well known and resonates strongly with customers who desire reliability and quick delivery.

Paul used the information he had completed to-date, such as his Vision and Mission, PEST Analysis, Porter's Five Forces, Values and Cultures, and SWOT Analysis to identify his value proposition or niche, which is "Help people lead healthier lives by creating safe spaces for drug research and innovation."

Through the Vision and Mission work that was done, the security organization realized that through security and innovation, trust and safety could be promoted.

Through the PEST (specifically, the Economic, Social, and Technological quadrants), it was determined that protecting intellectual property and brand is very important.

Through Porter's Five Forces, it was determined that competitive rivalry was high and protecting drug research and innovation is one way security could enable the business.

Through the Values and Cultures, it was determined that the security team culture must align with the values of stakeholders and the culture of the overall organization.

And through the SWOT Analysis (specifically in the Strengths quadrant), it was determined that the business mission to help people lead healthier lives and the culture was one of innovation and research and development.

Audience: Identify Target Market

- Build a picture of your target market
  - Identify the people and organizations that are key to your continued success
    - Executives
    - Business units
    - Employees
    - Customers
  - Positioning
    - Determine how to best influence your audience
  - Consider what end goal you want to achieve
    - Approve additional funding
    - Buy-in and support your effort
    - Remain committed to the security organization mission

You need to identify your target market—in other words, your audience for your marketing efforts. These are the people and organizations that are key to your continued success, such as executives, business units, employees, and customers. You'll need to build a precise picture of who your audience is. If you are not precise, you run the risk of a scattered approach that will dilute your message and possibly limit your success. The more specific you can be, the easier it will be to craft the right message for the right person and develop the right distribution plan.

You'll need to determine positioning of your marketing efforts. You can achieve this only through understanding how to best influence your audience. A common mistake is to latch onto an idea without first understanding your prospective audience, and what they want to hear and, more importantly, what motives them. If you try selling something that people don't want or don't understand why they need it, they won't buy into it and by that way, that also includes the request for additional funding from your company's top executives. "Because security is important" is not an ideal motivator and will not likely get you where you need to go.

You need to consider what actions you want your audience to take such as approving additional funding, gaining buy-in, and supporting your efforts, or remaining committed to the security mission.

The information that you previously developed through your Stakeholder Management Strategy and your Visioning and Innovation will help you identify your target market, position you for a successful outcome, and clarify what actions you want your audience to take. As an example, through your stakeholder management strategy, you learned your stakeholders will have different views on your project. You also learned that office politics and/or personal interests will likely be key factors in distilling true stakeholder motivations. You also know that the approach for each group and/or individual will need to be tailored to support the varying motivations of each of your stakeholders. For example, you wouldn't want to take cost, risk information that you would typically provide to the CFO to the head of HR who is interested in the impacts on employee policies.

From your Visioning and Innovation, you also learned tips for your security team. Never ask for the money; instead, articulate the vision and describe how you will solve a problem being faced by your key stakeholders. By stating the problem and aspiration, you can increase commitment and turn stakeholders into partners.

Three Things That Make Executives Unique

1) Executives are extremely busy
   - Want solutions, not more problems
   - Looking to you for answers
2) They are required to make rapid decisions with limited information
   - Want assurance you have comprehensiveness of thought
   - Everything we have done in these two sections leads to this
3) They have a complex enterprise to run
   - Security is only one component of the overall organization
   - Help them tie all the pieces together with security
   - Communicate in business consumable language

Executives are important to you because they impact or provide oversight and are accountable for nearly every aspect of the work that you do. They generally make decisions on initiatives and/or strategic direction, they are likely the individuals who stand between you and appropriate funding that is needed for your security organization, and more often than not, they have a lot of questions that likely require rapid response from you. It's important to understand what makes executives unique and the importance of positioning yourself appropriately when you interact with them so you can do so effectively.

The first thing you need to understand is, executives are extremely busy. You might be thinking to yourself right now, "Well I'm busy, too." But the fact of the matter is, as stated above, executives are the individuals who hold the keys to get you what you need to do your job. You have an accountability to them to appropriately interact with them, and provide them information they need in a manner in which they can consume it and can make decisions on behalf of the company. Executives want solutions, not more problems, and they are looking to you for the answers, not more questions.

Secondly, executives are required to make rapid decisions with limited information, and they want assurance that you have comprehensiveness of thought. The good news is everything we have done in these two sections leads up to this and will provide you all the factors you will likely need to establish yourself in this area.

Lastly, executives have a complex enterprise to run, and security is only one component of the overall organization. Oftentimes, we get so focused on our own organization, and what we are expected to deliver, we forget this. It's up to you as a security leader to help them tie all the pieces together with security in mind. They are not the security experts—you are; and you need to understand what business factors your executives are concerned with and tie it back to security in a business consumable language that is easy for them to understand.

Board of Directors Concerns

- Focused on business strategy
  - Not technology oriented
- Want measurable results
  - Related to people and data
    - Profit and loss in for-profit companies
    - Mission-driven focus, especially in government or not-for-profit organizations
- Key questions:
  - How do we compare to others?
  - Have we improved our efficiency?
  - What is our cybersecurity succession plan?
  - What is the cyber risk impact & mitigation plan for our new strategic initiative?

When interacting with the Board of Directors, we must understand their role in the organization. They are there to provide oversight and governance, not make day-to-day tactical decisions. As a result, the Board is focused on overall business strategy. Typically, they are not technology or security experts who know and understand technical jargon. They are very smart, just not knowledgeable about security.

Given their focus, the Board wants measurable results related to people, data, and key drivers for the organization. In for-profit companies, this is typically related to profit and loss. In organizations with a mission-driven focus, this will be related to how effectively the mission is being achieved. It's important to note that for-profit companies can also have a mission-driven focus as well.

John Pescatore and Lance Spitzner from SANS gave a webcast called "Talking Cybersecurity to the Board" where, among many other topics, they laid out four key questions the Board will ask you as a security leader:[1]

- **How do we compare to others?** This is related to profit/loss as well as mission-driven goals because an over or underinvestment in security can, as we know, have adverse consequences.
- **Have we improved our efficiency?** This also ties into profit/loss because an ineffective security team is an unnecessary drag coefficient on the business.
- **What is our cybersecurity succession plan?** Effective governance involves understanding the long-term viability of key capabilities like security.
- **What is the cyber risk impact and mitigation plan for our new strategic initiative?** It's imperative for the Board to understand inhibitors and risks to achieving business goals.

Reference:
[1] https://www.sans.org/webcasts/security-awareness-board-directors-105920

Goal for Your Board Meeting

- Ask yourself
  - What do you want them to do, feel, or say after the meeting?
- Board feels confident that
  - You know what you're doing
  - The organization is in good hands
- How do you accomplish this?
  - What should you leave out?

When presenting to the Board about your security program, make sure to ask yourself, "What do I want them to do, feel, or say after the meeting?" Technical security professionals may overwhelm the board with security jargon, leaving them confused. How the Board *feels* about you is the most important takeaway from your Board meeting. They want to feel confident that you know what you're doing and that the organization is in good hands. Accomplishing this often requires you to leave out much of the detail you might normally use when to presenting to more technical audiences.

Effective Communications

"Security people don't speak our language. In fact, at each briefing, they seem to speak a different language."

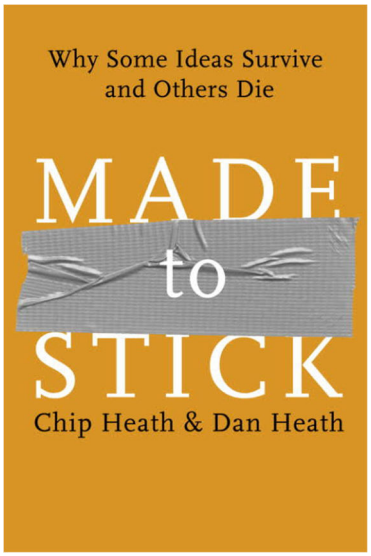
- Board Member

When communicating with senior leaders and board of directors, security professionals must speak in a language that they can understand. Moreover, it's imperative to keep the story not just simple, but consistent. If you attend a board meeting and alter the framework, key metrics, or strategic plan in a substantial way, it will immediately lead to questions about not just why the plan changed, but also lead to questions about your credibility.

Reference:
https://www.sans.org/webcasts/security-awareness-board-directors-105920

Making Ideas Stick

- **S**imple
  - Find the core of any idea
- **U**nexpected
  - Grab attention with surprise
- **C**oncrete
  - Make sure they can be grasped and remembered
- **C**redible
  - Make an idea believable
- **E**motional
  - Help people see the importance
- **S**tories
  - Use narrative



Many technical security professionals suffer from what is known as the "Curse of Knowledge." In short, it occurs when someone is better informed than another person and finds it extremely difficult to think and communicate about topics with people who are less knowledgeable about a subject.

With this in mind, how can you connect with your target audience and create a message that will be memorable? Two brothers, Chip and Dan Heath, have written an excellent book titled, *Made to Stick: Why Some Ideas Survive and Others Die*. They outline six important characteristics that help make an idea sticky. These can be used to market your work with the security team:

- **S**imple: Oftentimes, security professionals default to detailed technical communications and do not focus on the "so what" for the business. By ignoring the impact and resulting risk to the organization, we can inadvertently "bury the lead."
- **U**nexpected: Memorable ideas are ones that are unexpected. People don't expect security to be a business enabler. If you can lead with that story, it will be more likely to resonate with your stakeholders.
- **C**oncrete: Don't focus on technical feeds and speeds, which can be abstract for many people. Instead, focus on how security supports specific business initiatives.
- **C**redible: Develop the credibility of your security team not only by being security experts, obtaining certifications, and speaking at well-known industry events but also by seeking endorsements from key business partners.
- **E**motional: Maya Angelou has a well-known saying, "People will forget what you said, people will forget what you did, but people will never forget how you made them feel." By focusing on the emotional aspect of a situation, you can help people see the importance of your work.
- **S**tories: Stories are one of the most effective teaching tools. They are containers for wisdom and knowledge, and really help drive home the point of a particular idea.

Albert Einstein on Simplicity

"If you can't explain it simply,
you don't understand it well enough."
- Albert Einstein

Albert Einstein said, "If you can't it explain it simply, you don't understand it well enough."

Simplicity is the quality of condition of being easy to understand. Counter to simplicity is our basic human nature to overcomplicate everything we touch, especially when we are trying to convey information or ideas verbally, or in writing such as emails, presentations, and/or meetings. We use words people don't understand such as techno-speak, regulatory jargon, abbreviations, and far too many acronyms. We often document the complexity instead of revealing the simplicity. If people have to decode your complex language, they can't hear or understand what you are intending to say, and it begs the question if you really understand it well enough yourself.

Your message is important and learning to simplify will benefit you in so many ways. We will share some tips, techniques, and examples on the following pages to help you further understand the importance as well as provide guidance on how to simplify your message for marketing.

Example 1: Bad Exec Communication (Log4Shell)

Log4Shell is a **zero-day** vulnerability in Apache's Log4j, a popular Java logging framework, involving **arbitrary code execution**. Log4Shell has a **CVSS severity** rating of 10, the highest available score. The vulnerability takes advantage of the fact that Log4j allows requests to arbitrary **LDAP and JNDI** servers, allowing attackers to execute arbitrary **Java code** on a server or other computer to gain access or steal sensitive information.

https://en.wikipedia.org/wiki/Log4Shell

Your boss, the CISO, is on vacation with no access to email or a cell signal, and he has delegated responsibility for the security organization to you, the Director of Security Operations. Toward the end of the first week of your delegate duties, you receive an email from the CEO who read about Log4Shell in *The New York Times* Twitter feed. He is immediately alarmed your company might be impacted. In his email, he simply asks, "Are we affected by Log4Shell?"

You're excited about the opportunity to finally interact directly with the CEO, and as luck would have it, you've already received threat intelligence from your team, and they are actively assessing the situation. You provide your CEO with the following information: "Log4Shell is a zero-day vulnerability in Apache's Log4j, a popular Java logging framework, involving arbitrary code execution. Log4Shell has a CVSS severity rating of 10, the highest available score. The vulnerability takes advantage of the fact that Log4j allows requests to arbitrary LDAP and JNDI servers, allowing attackers to execute arbitrary Java code on a server or other computer to gain access or steal sensitive information."

You anxiously await a reply from the information that you provided to the CEO and moments later, he responds with a copy to the CIO and your boss, the CISO, and asks, "Are we impacted?" At this point, you know you did not provide your CEO with the information he needed the first time. You take a step back and think to yourself. This was a very short, concise message, and it gives all the technical details about Heartbleed. You're a bit perplexed as to why he doesn't get it.

What do you think was wrong with this message to the CEO?

You are correct that this is a very short, concise technical summary of Log4Shell, but your CEO is not a technologist. Your message was not written in business consumable language so he could understand what this bug is all about and, in reality, he shouldn't have to understand it. That's why he has a security team.

You didn’t provide the direct answer to his question about how the organization is impacted. The message is geared more toward showcasing your technical acumen. There are clearly no solutions provided in your communication, and your message opens up more questions for the CEO than you’ve provided answers. Lastly and most importantly, there is no indication of comprehensiveness of thought. Your message is clearly a reaction to respond expeditiously without thinking through what he really wants and needs to know. You provided what you wanted to tell him.

Reference:
https://en.wikipedia.org/wiki/Heartbleed

Example 1: Better Exec Communication (Log4Shell)

A security vulnerability called “Log4Shell” was disclosed Thursday, which could impact our **websites** and **business processes**. Our investigation to date indicates that **90% of our websites are not at risk**. We are actively investigating the remaining 10% and will provide a daily update until the issue is resolved.

This bug allows anyone with knowledge of the fact that our **house** has an **“open door**” to walk right in. This can result in attackers stealing **sensitive customer data**, **credit card information**, **passwords**, and more from our systems.

The security team continues to scan our systems. If it is discovered the team will immediately remediate by deploying the patches that have been released to address this issue.

Although the previous summary of Log4Shell included some technical jargon, this version is more focused on the impact to the company and what the security team has been able to achieve.

When you are crafting your communications, it's important to consider how you want to be perceived by the receiver. In a more technical company, it might be wholly appropriate to position yourself and the security team as technical subject matter experts. In that type of environment, you might want to focus on technical analysis and technical solutions. However, if your leadership team is not very technically savvy, it might see this type of communication as too detailed and perceive you to be merely a "problem finder." In those cases, you will be better served by positioning the security team as a business leader and solution provider.

The example communication on this slide highlights that Log4Shell impacts "websites" (hopefully something everyone in the company can understand) and that it could result in the theft of sensitive data like customer data, and credit card numbers, and passwords (making the impact very concrete). The statements also highlights how this currently impacts the company. Doing this shows that you have done your due diligence and provides the "so what" that executives are most concerned about. In fact, you might decide to lead with this in the first paragraph to immediately highlight the impact to your company.

Example 2: Bad Exec Communication (DMARC)

DMARC is an email validation system designed to detect **email spoofing** by providing a mechanism to allow receiving **mail exchangers** to check that incoming mail from a domain is authorized by that domain's administrators and that the email (including attachments) has not been modified during transport.

It expands on two existing mechanisms, the well-known Sender Policy Framework (**SPF**) and DomainKeys Identified Mail (**DKIM**), coordinating their results on the alignment of the domain in the **From: header** field, which is often visible to end users. It allows specification of policies (the procedures for handling incoming mail based on the combined results) and provides for reporting of actions performed under those policies.

Source: https://en.wikipedia.org/wiki/DMARC

Imagine that you are preparing for annual budget meetings. There are a number of security initiatives for which you would like to obtain funding, including DMARC to help prevent email spoofing. As part of the business case, you need to provide a justification and decide to supply the project managers with the text above. Although the statement above is technically correct, there is very little in this description that will resonate with non-IT personnel. Terms like "mail exchangers," "SPF," and "DKIM" only add to the confusion. If others have done a better job articulating the business value of their projects, then you might not be very likely to get funding for your important security initiatives.

Example 2: Better Exec Communication (DMARC)

The solution prevents scammers from sending **fraudulent email** to our customers. These fraudulent emails result in **stolen usernames, passwords**, and **fraudulent transactions**. The solution reduces the number of stolen accounts by 20%, **account fraud** by 10%, and the total amount of fraudulent transactions by **$1 million** per year.

This summary of DMARC is much more powerful because it articulates the business value to your organization. Specific terms like "fraudulent email" and "stolen usernames" are much more understandable to non-technical people. Additionally, this version actually quantifies to the impact to the business in terms of reducing the number of stolen accounts, minimizing account fraud, and saving the company $1 million per year. The more you can articulate the value provided by your security projects, the more likely you will be able to succeed and stand out in a competitive market (i.e., the market for limited attention).

Example 3: Bad Exec Communication (DDoS)

DDoS is an attack where multiple **compromised systems**, which are often infected with a **Trojan**, are used to target a single system causing a Distributed Denial of Service (DDoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems **maliciously used** and controlled by the hacker in the distributed attack. The DDoS attack uses multiple computers and internet connections to flood the targeted resource. DDoS attacks are often global attacks, distributed via **botnets**.

Source: http://www.webopedia.com/TERM/D/DDoS_attack.html

Earlier this morning, your company was hit with a distributed denial of service (DDoS) attack. To close out the incident response process, your manager has asked you to draft a summary of what happened. This is the first time you've had to draft such a communication and are not sure how to respond. You decide to start the write-up with some background information about the attack to ensure that everyone understands what a DDoS actually is. And that is where you make your first communications mistake. The write-up above focuses too much on what DDoS is and does not describe at all the impact to the organization. If non-security leadership is not familiar with dealing with denial-of-service attacks, then it will likely be confused by terms such as "Trojan," "maliciously used," and "botnets."

Example 3: Better Exec Communication (DDoS)

On Friday night, our **primary website** was **unavailable** for **two minutes** because it was **flooded** with traffic from the internet by cyber attackers. We immediately instituted our incident response and recovery procedures, and the website was **made available** with **zero customer impact**.

This version is much better because it focuses on the impact to the business. The company's primary website was "unavailable for two minutes" because it was "flooded with traffic." It was quickly made available with "zero customer impact." Senior leaders want to know the "so what" of your security work. They are looking to you for simple answers that describe why something is important and relevant to the complex business that the organization is running.

Leonardo Da Vinci on Simplicity

"Simplicity is the ultimate form of sophistication."
- Leonardo Da Vinci

Leonardo Da Vinci said, "Simplicity is the ultimate form of sophistication."

Ideas are the currency of the 21st century and some people are exceptionally good at presenting their ideas. For these people, this particular skill elevates their stature and increases their influence. There is nothing more inspiring than a bold idea, delivered by a great speaker or easy-to-understand words.

Ideas effectively packaged and delivered can change the world. John F. Kennedy gave a speech at Rice University on September 12, 1962, where he outlined his vision to explore the moon.[1] He captured the collective imaginations of millions of Americans and thousands of top scientists to put their time and energy into this effort. It was one of the most important speeches in American history and it took only 17 minutes and 40 seconds.

There is evidence all around us that illustrates simplicity is the way to go. Ikea provides instructions that are only pictures, no words. Twitter limits its tweets to 280 characters, so they can be easily consumed. There are wildly popular TED talks that cover complex topics like the history of the world, all 13 million years of it, in only 18 minutes. All of these examples are made possible by one concept. Keeping it simple!

Reference:
[1] https://er.jsc.nasa.gov/seh/ricetalk.htm

Promote: Distribution Strategy

- Includes critical components needed to execute successful marketing
- Distribution strategy should include the following:
  - Inbound content marketing
    - Blogs
    - White papers
    - Online talks and videos
    - Internal website
  - Outbound marketing
    - Advertisements
    - Promotional videos

Now that you know who you want to reach, and what actions you want them to take, you need to determine the most effective method by which you promote your marketing—in other words, determine how your message will reach your audience. This is your distribution strategy, and it includes critical components needed to execute a successful marketing effort.

Primary information and/or tools that you can leverage from past work to create your distribution strategy can be found in your project plan or security roadmaps along with other critical pieces of information you've collected as a result of the strategic planning process. The information about the who, what, when, where, and how should be available to you at this point, and the distribution strategy is formalizing the method by which you will deliver the messages for marketing.

Inbound content marketing is promoting your efforts through blogs, white papers, videos, and internal websites. The idea is to draw key stakeholders in by providing content that is relevant and useful to them. For example, you might do regular security briefings focused on the threats to a particular line of business. By producing interesting or relevant content, you develop more engaged customers.

Outbound marketing, on the other hand, relies on traditional approaches to buy a customer's attention, such as TV, print, or radio advertisements, flyers, brochures, spam, and promotional videos. These types of activities are associated with traditional brand advertising, which can also be useful for your security team to build awareness of your activities across the larger organization.

Market and Communicate To Employees

- Market to your current employees for retention
  - Lunch and learn
  - Challenge coins
  - Newsletters
  - Specialized security training
  - Highlight innovation and thought leadership
- Market to future employees to attract top talent
  - Recruit at major conferences
  - Speaking engagements from your star performers

Oftentimes, leaders forget that it's important to market and communicate to current employees for retention, and to future employees to attract top talent. As you are aware, the security industry is in high demand and the effort you put into marketing to current and future employees will result in far greater benefits than dealing with vacancy factors. Remember that high-performing team members often know or network with top talent and might become a great partner in your recruiting efforts.

Below are some ideas to market to your current employees:

You can hold brown bag sessions on a variety of topics, such as showcasing great work that various individuals and/or teams are doing. This also provides transparency across your organization. You can also invite key stakeholders to these events, which will also provide insight to all the great work your team is doing. You can bring in non-security related topics that might be of interest to provide insight to your security team, such as someone from your sales and marketing team to talk about how they use technology to generate revenue or have one of your key stakeholders provide information on what his or her organization does. This has the potential to build trust and collaboration and to provide much-needed visibility to both groups. You can even have vendors come and present innovative technology.

Publicly acknowledging the work of your team in brown bag sessions is a great way to increase commitment and morale. Providing special recognition or awards are another great approach. Challenge coins are a great way to do this and serve as a highly visible token of appreciation and achievement.

Newsletters are a great way to communicate a variety of topics to your employees. You can communicate what's top of mind from your leadership team, new security trends, highlight accomplishments, or recognize outstanding performance.

Specialized security training is one area you can invest in and market to your security team. This shows your commitment to developing your team and providing them with the necessary tools and skills to perform their job and stay agile in the industry and illustrate clear paths for promotion.

Innovation and thought leadership will advance your organization's mission and, therefore, you want to market by highlighting those individuals and/or groups that are displaying these attributes. Not only will it reinforce your appreciation to those individuals that you are highlighting, but it will also encourage others to move in that direction by highlighting desired behaviors.

Marketing to future employees to attract top talent is very important for you to build and maintain high-performing teams. You can hold recruiting events at major industry conferences and distribute marketing collateral. Consider holding a specific recruiting event at the location with hiring managers and recruiters on-site to talk with potential candidates. Face time with potential candidates goes a long way.

You might want to encourage your star performers to seek out speaking engagements on topics of interest for the industry or specialized subject matter expertise. For this, it's particularly important that you manage your message. Ensure that your speakers are fully trained for public speaking, and the content and messages in their presentation fully represent your organization and are enticing and engaging to the audience.

Market and Communicate to Customers

- Customer recognition
  - Challenge coins, awards for advocates
- Invite your customers to key conferences
  - That are relevant to the work they do
  - Are innovative and insightful
- Security awareness and training
  - Ask a hacker/security expert series
  - Security booths at corporate events
  - Personalizing security
    - How to keep your kids safe online

Just as employees should be engaged and recognized, your customers should also be formally recognized when they do something notable related to security. This can be for something as simple as fixing all the defects from a recent penetration test to partnering with you to roll out a new enterprise security initiative. When this does occur, make sure to publicly recognize these customers. These success stories and associated awards help highlight the work you are doing and build advocates for future security efforts.

As security professionals, we have a wealth of security events that we can attend. Think about inviting some of your customers to these key conferences to present with you about the work they do and how security plays a part. Oftentimes, security conferences do not have much information about the business reasons for undertaking a particular initiative. As the business continues to innovate, think about how you can share these insights with the rest of the security community to highlight the work that your stakeholders are doing.

Finally, make sure to constantly work on building awareness for your security activities. There are a number of approaches to accomplish this, including conducting regular information sessions about current threats (e.g., "Ask a Hacker Anything"), having booths at company events, and publishing information that can be used at home (e.g., how to keep your kids safe online).

Infographic Example

Infographics are powerful marketing tools. Many people are visual learners and infographics provide a mechanism to transmit complex information that can be quickly consumed in a digestible manner.

According to NeoMam Studios, whose business is to produce exceptional visual content that inspires people to take action, the average person is exposed to 174 newspapers full of information every day and 99% of that information is filtered out through the brain almost immediately, leaving only 1% of the information actually getting to the brain.[1] It also claims that 90% of information transmitted to the brain is visual and half of the brain is dedicated to visual function. It also tells us that 65% of the population are visual learners and images are processed simultaneously at the rate of 60,000 times faster in the brain than text. Text is processed sequentially, and most people retain only about 20% of what they read.

Infographics are an effective way to market information about your security organization. More and more infographics on security topics are showing up in search engines, and based on the above information, it's clear as to why this is happening. Security is a complex topic and not easily communicated to non-security professionals. Take the infographic shown on this page. It illustrates the things that happen in security within 24 hours. It is based on an infographic about what happens on the web in 60 seconds.[2] In a quick easy-to-understand and pleasing view, it gives the audience an idea of how much the security team has to deal with on a daily basis.

How could you take a concept such as this and provide your audience with an indication of all the activities your security team conducts? As an example, I would imagine that your network blocking and/or malicious website blocking numbers are pretty impressive. What about the number of spam emails you block on a daily basis. Think about what meaningful information would be important to your organization. How could you leverage a visual message such as this for your security efforts?

References:
[1] http://neomam.com/blog/infographics-make-great-marketing-tools/
[2] https://www.go-globe.com/blog/things-that-happen-every-60-seconds

SNAP Marketing Tools to Leverage

- Leverage strategic planning work for marketing

Category	Description	Planning Tools	
Specify	Marketing Objectives	Threat Analysis Historical Analysis Gap Analysis	Security Roadmap Metrics Program SWOT analysis
Niche	Identify Value Proposition	Vision and Mission PEST Analysis Porter's Five Forces	Values and Cultures SWOT Analysis
Audience	Identify Target Market	Stakeholder Management	Visioning & Innovation
Promote	Distribution Strategy	Project Plan	Security Roadmap

As stated previously, you can leverage the strategic planning work from earlier in this course to create your marketing plan. Your output for each of these SNAP categories is certainly not limited to the planning tools described in the table. These are simply a good place to begin to collect data points for your marketing efforts.

In the Specify category, where you determine your marketing objectives, you can use output from the Threat Analysis, Historical Analysis, Gap Analysis, Security Roadmap, Metrics and Dashboards, and SWOT Analysis (specifically, Weaknesses and Opportunities and Threats).

In the Niche category, you identify your value proposition. You can utilize output from the Vision and Mission, PEST Analysis (specifically, the Economic, Social, and Technological quadrants), Porter's Five Forces, Values and Cultures, and SWOT Analysis (specifically, strengths).

In the Audience category, where you identify your target market, you can leverage output from the Stakeholders Management and Visioning and Innovation sections.

Finally, for the Promote category, you need to develop your distribution strategy. For that, you can leverage your project plan as well as your Security Roadmap.

In Summary

- Marketing efforts can help increase:
  - Revenue and/or funding
  - Brand recognition
  - Product and/or capability visibility
  - Customer and stakeholder support
  - Aid in employee retention and recruiting efforts
- It's important to evaluate your results and make modifications to your marketing plan as necessary

Marketing your security organization internally and/or externally can help increase revenue and/or funding, brand recognition, product and/or capability visibility, customer and stakeholder support, and aid in employee retention and recruiting efforts.

Investing time into building your marketing plan and perfecting effective messaging techniques is of vital importance and will benefit you tremendously, as security is a complex field and not easily understood by non-security professionals. Security is no longer just an IT issue, and these topics have reached the most senior executives in your company because security breaches are in the media, it seems almost daily. Now is a great time to market your organization and get the best value for your efforts.

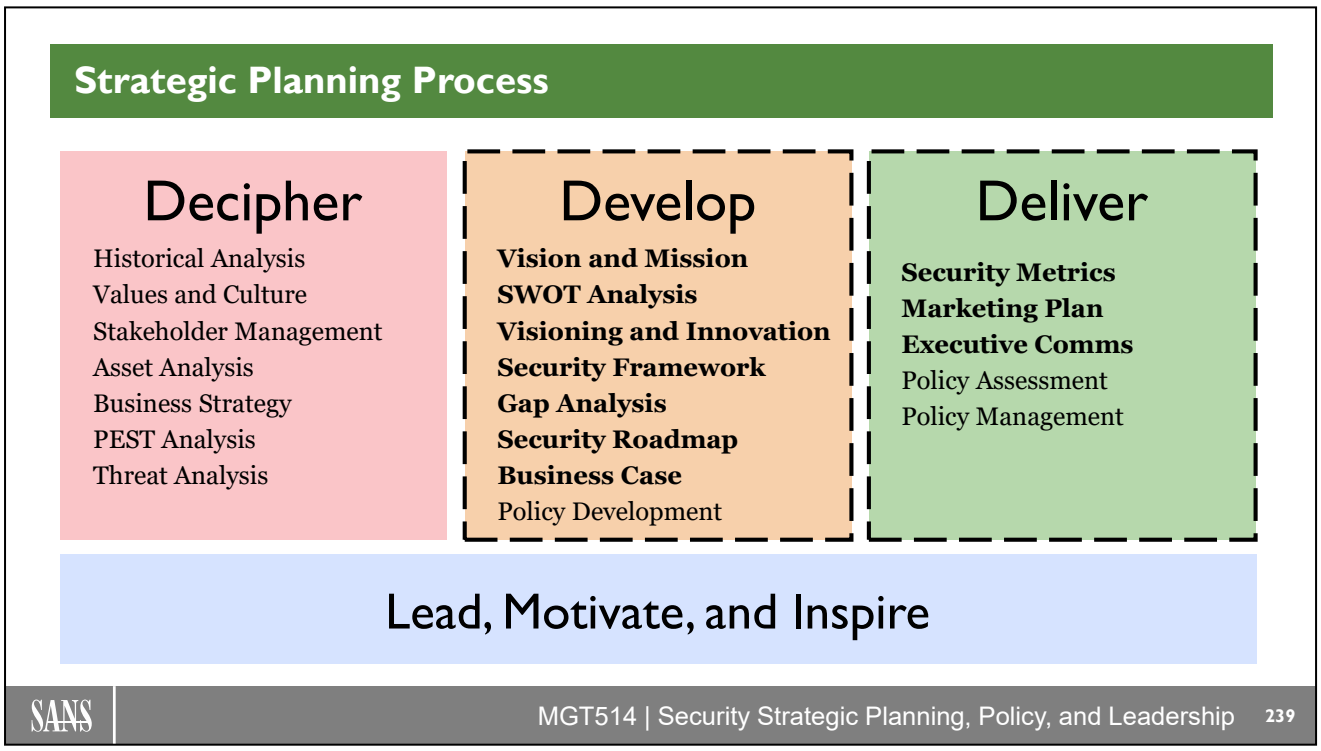
Course Roadmap

- Section 1: Strategic Planning Foundations
- ***Section 2: Strategic Roadmap Development***
- Section 3: Security Policy Development and Assessment
- Section 4: Leadership and Management Competencies
- Section 5: Strategic Planning Workshop

SECTION 2

- Define Current State
  - Vision and Mission
    - Lab #1: Mission Statement
  - SWOT Analysis
    - Lab #2: SWOT Exercise
- Develop the Plan
  - Visioning and Innovation
  - Security Framework
  - Security Roadmap
    - Gap Analysis
    - Lab #3: Roadmap Development
  - Business Case Development
- Deliver the Program
  - Security Metrics Program
  - Marketing and Exec Communications

This page intentionally left blank.



In this section, we expanded our coverage of the various strategic planning phases to include the Develop and Deliver phases, specifically the items in bold on the slide above. By working through the strategic planning process, we can better understand how to drive organizational value, engagement, and transformation.

Strategic Planning Tools: Section 2

Tool	Purpose
Mission Statement	Guides decisions related to business value and purpose
SWOT Analysis	Summarize key analysis results to identify Opportunities and Threats
Visioning and Innovation	Develop stretch goals to inform strategic, not just tactical, planning
Security Framework	Use an industry recognized framework to provide structure to the security program
Maturity Model	Measure maturity based on industry benchmarks
Gap Analysis	Create a menu of options to fill gaps between current and desired future state
Roadmap Development	Prioritize activities based on resource and organizational constraints
Business Case	Describe the business benefits of your security program and initiatives
Metrics and Dashboards	Monitor and measure progress toward goals to identify areas of improvement

This is a summary of the strategic planning tools we covered in this section.