

## 514.1

# Strategic Planning Foundations



PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With this CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, USER AGREES TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, USER AGREES THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If User does not agree, User may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP® and PMBOK® are registered trademarks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

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



# Strategic Planning Foundations

© 2023 Frank Kim | All Rights Reserved | Version I01\_02

Welcome to SANS MGT514: Security Strategic Planning, Policy, and Leadership!

## **A Note about URLs**

Sometimes, this courseware cites URLs, which were valid at the time they were originally cited. URLs change all the time. This courseware does not necessarily update all URLs. Out-of-date URLs have several values. They show that a statement is based on scholarship. They can give hints about how to find source material, even if it is no longer at the original URL. They can also be used to find material at the Wayback Machine maintained by the Internet Archive.

<b>MGT 512</b>	<b>Security Leadership Essentials for Managers</b> Leading Security Initiatives to Manage Information Risk		<b>MGT 414</b>	<b>SANS Training Program for the CISSP® Certification</b> Need Training for the CISSP® Exam?	
<b>MGT 514</b>	<b>Security Strategic Planning, Policy, and Leadership</b> Aligning Security Initiatives with Strategy		<b>MGT 433</b>	<b>Managing Human Risk</b> People are the Primary Attack Vector. Manage Your Human Risk.	
<b>MGT 516</b>	<b>Managing Security Vulnerabilities: Enterprise and Cloud</b> Stop Treating Symptoms – Cure the Disease		<b>MGT 520</b>	<b>Leading Cloud Security Design and Implementation</b> Building and Leading a Cloud Security Program	
<b>MGT 521</b>	<b>Leading Cybersecurity Change: Building a Security-Based Culture</b> Build and Measure a Strong Security Culture to Secure Your Workforce		<b>MGT 525</b>	<b>Managing Cybersecurity Initiatives &amp; Effective Communication</b> Meet and Exceed Your Security Program's Goals	
<b>MGT 551</b>	<b>Building and Leading Security Operations Centers</b> Prevent – Detect – Respond   People – Process – Technology		<b>MGT 415</b>	<b>A Practical Introduction to Cyber Security Risk Management</b> Cutting Through Academics: Practical Risk management for Cybersecurity	
<b>SEC 566</b>	<b>Implementing and Auditing Security Frameworks and Controls</b> Building and Auditing Critical Security Controls		<b>MGT 553</b>	<b>Cyber Incident Management</b> Open in Case of Emergency	
<b>AUD 507</b>	<b>Auditing &amp; Monitoring Networks, Perimeters, and Systems</b> Controls That Matter – Controls That Work		<b>SEC 440</b>	<b>CIS Critical Controls: A Practical Introduction</b> Introduction to Critical Security Controls	
<b>LEG 523</b>	<b>Law of Data Security and Investigations</b> Bridging the Gap Between Legal and Cybersecurity				

The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world.

SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center.

SANS offers a number of courses that prepare cyber leaders and managers for building and leading world-class security teams. As security becomes more relevant to the business, we need to develop business, leadership, and technical skills to effectively interact with business leaders as well as lead and inspire our technical teams. The following courses give you the necessary skills to navigate in the new world of security:

### **MGT512: Security Leadership Essentials for Managers | GSLC | 5 Sections**

Get up to speed on information security issues and terminology. You don't just learn security; you learn how to manage security.

### **MGT514: IT Security Strategic Planning, Policy, & Leadership | GSTRT | 5 Sections**

Learn to build and execute strategic plans, develop and assess policy, and utilize management tools to lead, inspire, and motivate your teams.

### **MGT516: Managing Security Vulnerabilities: Enterprise and Cloud | 5 Sections**

Learn to build and manage a vulnerability management program for your enterprise and cloud systems.



**MGT521: Leading Cybersecurity Change: Building A Security-Based Culture | 5 Sections**

Apply the concepts of change management to embed a strong security culture in specific security initiatives or organization wide.

**MGT551: Building and Leading Security Operations Centers | GSOM | 5 Sections**

Learn how to build, operate, and continuously improve your Security Operations Center (SOC).

**SEC566: Implementing and Auditing Security Frameworks and Controls | GCCC | 5 Sections**

Students learn how to merge security control requirements into a cohesive strategy to defend their organization while complying with industry standards.

**AUD507: Auditing & Monitoring Networks, Perimeters, and Systems | GSNA | 6 Sections**

Learn how to audit and monitor your key controls.

**LEG523: Law of Data Security and Investigations | GLEG | 5 Sections**

Understand key lessons on the law of data security and investigations that all managers, leaders, & executives should know.

**MGT414: SANS Training Program for the CISSP® Certification| GISP | 6 Sections**

Need to pass the CISSP® exam? Here's how.

**MGT433: Managing Human Risk | 3 Sections**

Learn how to manage and measure your human risk through a mature security awareness and engagement program.

**MGT520: Leading Cloud Security Design & Implementation | 3 Sections**

Learn how to build and lead a cloud security program

**MGT525: Managing Cybersecurity Initiatives and Effective Communication | GCPM | 5 Sections**

Learn how to effectively drive and manage projects and key initiatives.

**MGT415: A Practical Introduction to Cyber Security Risk Management | SSAP | 2 Sections**

Understand how to assess and manage cyber security risk.

**MGT553: Cyber Incident Management | 2 Sections**

Creating and empowering effective cyber incident managers

**SEC440: CIS Critical Controls: A Practical Introduction | 2 Sections**

Introduction to proven techniques and tools needed to implement and audit CIS Critical Controls v8 as documented by the Center for Internet Security (CIS).

# 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 I

### • Overview

- Need for Strategic Planning
- 30-60-90 Day Plan
  - Lab #1: CISO First Impression
- Decipher the Business
  - Historical Analysis
  - Values and Culture
  - Stakeholder Management
    - Lab #2: Relationship Management
- Asset Analysis
- Business Strategy
  - Lab #3: Strategy Map
- Decipher the Threats
  - Threat Actors
  - PEST Analysis
  - Threat Analysis

The goal of this course is to give you the knowledge to go beyond technical information security work and become a security business leader who can not only build effective security plans and programs but can also make information security relevant and understandable to key stakeholders across your organizations. To develop these skills, the course covers the following topics:

### **Section 1**

Use tools to understand the business and, given this understanding of key business drivers, understand the threats so that we can better protect the organization.

### **Section 2**

With an understanding of the business and the threat landscape, we can analyze the current state of our security program and develop a roadmap to accomplish our goals. Once we have a strategic plan in place, we can use tools to build and maintain our security program.

### **Section 3**

Security policy is one of the key tools we can use to influence and guide the organization.

### **Section 4**

Leadership competencies are developed to lead, motivate, and inspire our team as we work to implement the strategic plan.

### **Section 5**

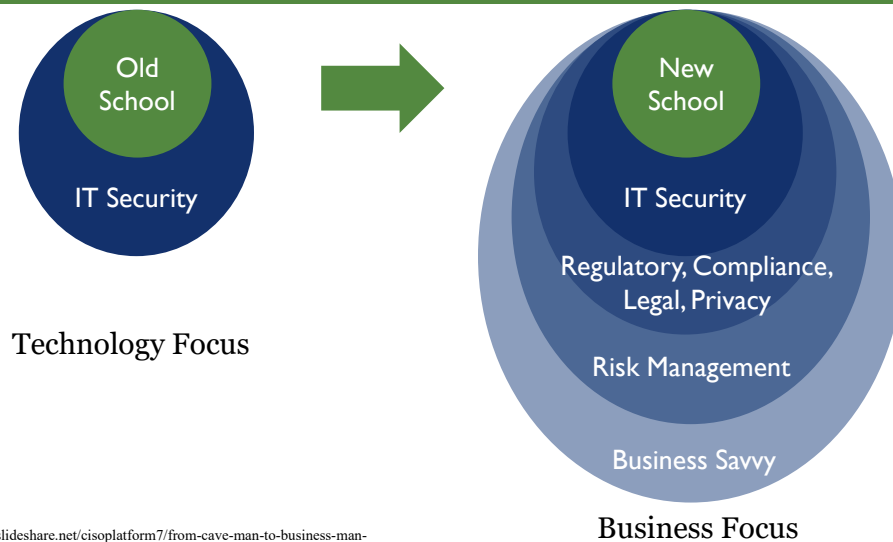
Case studies and group discussions teach you to apply the tools from class to real-world scenarios.

## Background

- Focus on cybersecurity is at an all-time high
  - Increasing number of breaches
  - Visibility at the Board and CEO levels
- Information security teams have
  - More budget and more opportunity
  - Increased responsibility and scrutiny
- Security is not just an IT concern
  - It's a vital part of the growth of your business
  - Security business leaders must learn how to navigate in this new world

As security professionals, we have seen the landscape change. Information security is now more vital, crucial, relevant, and important to the growth of your organization than ever before. As a result, information security teams have more budget, more opportunity, and more visibility to the Board and executives. With increased opportunity comes increased responsibility and scrutiny. Security business leaders must learn how to navigate in this new world.

## Evolution of Security Leadership



Graphic credit: <https://www.slideshare.net/cisoplatfrom7/from-cave-man-to-business-man-the-evolution-of-the-ciso-to-ciro>

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

6

It used to be that information security was largely the domain of IT security with a focus on technical work, technical projects, and therefore technical leadership. That technical expertise is, of course, still extremely important. But, the modern world of cybersecurity requires a more business-focused approach to security. This "New School" approach requires that security leaders and managers understand not just IT security but also risk management and various regulatory, compliance, legal, and privacy drivers. Ultimately, the success of a modern security leader depends upon the extent of their business savvy and just how much they can relate, communicate, and build relationships with the rest of the organization. This is why strategic planning is vitally important and why the tools discussed so far in class are vitally important to your success, the success of your teams, and the success of your organization.

### Graphic credit:

<https://www.slideshare.net/cisoplatfrom7/from-cave-man-to-business-man-the-evolution-of-the-ciso-to-ciro>

## About This Course

- This course teaches you how to
  - Build and execute strategic plans
    - That resonate with other IT and business leaders
  - Develop and assess security policy
    - To help steer your organization
  - Utilize management tools and frameworks
    - To better lead, inspire, and motivate your teams
- The goal is to teach you
  - What to do to become a security business leader
    - Not only an information security specialist

This course covers the skills and tools that managers and leaders need to effectively build, lead, and motivate security teams. As a first step, security leaders must get buy-in for their security initiatives. This means that you need to know how to build strategic plans that not only make technical sense, but you also need plans that resonate with other IT and business leaders. Moreover, you have to effectively steer the organization toward these strategic goals. Effective development of security policies and effective assessment of security policies are key skills that security managers and leaders need to possess. Finally, effective security leaders know what motivates and drives their teams and how to inspire and motivate people to achieve a larger goal.

## Strategic Planning Process

### Decipher

- Historical Analysis
- Values and Culture
- Stakeholder Management
- Asset Analysis
- Business Strategy
- PEST Analysis
- Threat Analysis

### Develop

- Vision and Mission
- SWOT Analysis
- Visioning and Innovation
- Security Framework
- Gap Analysis
- Security Roadmap
- Business Case
- Policy Development

### Deliver

- Security Metrics
- Marketing Plan
- Executive Communications
- Policy Assessment
- Policy Management

Lead, Motivate, and Inspire

People may think about "strategic planning" as simply coming up with a roadmap that contains a number of projects to implement. That is an important part of the process, but it is much more than that. Strategic planning starts with a deep analysis and understanding of the state of the business and the threats faced by the organization. Based on this analysis, you can then start to develop your objectives based on the organization's vision and mission, stakeholder risk appetite, and opportunities. This is key to determining how you will provide *value* to the organization. With this as the foundation, you can start to create the actual plan. This includes identifying opportunities for innovation, selecting a security framework, performing gap analysis, and then developing a roadmap. But, the work is just beginning.

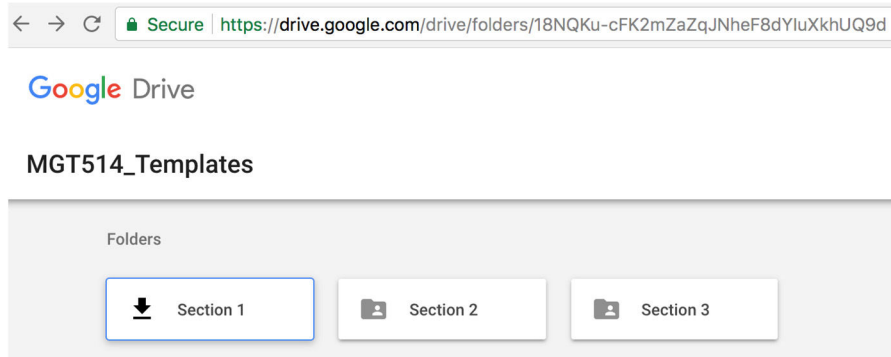
A plan is not worth much if it can't actually be implemented. This means we have to figure out how to execute the plan by navigating the internal values and culture, developing a business case to get support and funding, and promoting your activities through effective marketing and communications. This is key to driving *engagement* throughout the organization. As you execute and develop policy to effectively steer the organization, you need to monitor progress. Metrics are extremely important as is effective policy management and assessment, so you can understand what is working and what is not. Throughout this entire journey as a leader and manager, you must continuously strive to lead, motivate, and inspire your team members and colleagues to accomplish the goals of the overall strategic planning process that ultimately results in organizational *transformation*.

In Section 1, we start by covering the topics in the Decipher phase.

Ready to begin?

## Digital Download Package

- Templates, tools, and documents from class
  - Available on Google Drive via **mgt514.com**



Throughout the class, we cover a number of strategic planning tools that can be used throughout your strategic planning process. To help you get started quickly when you return to work, we provide a number of templates, tools, and documents from class that you can use as a starting point.

These templates are available as a course Digital Download Package online in Google Drive via this URL: **mgt514.com**

## Who Should Take This Course?

- **Intended audience:**
  - Senior security and IT leaders (for example, CISO and CIO)
  - Directors and managers of IT security teams
  - Team leads responsible for security operations
- **Anyone interested in**
  - Going beyond technical skills
  - Learning how to communicate with senior leaders
  - Talking about security in ways business leadership can understand

This course is for anyone interested in going beyond technical skills and learning how to communicate with senior leaders who may not have much experience in information security or even Information Technology (IT). Anyone in a leadership position, including senior staff, team leads, managers, directors, and senior leaders (such as the CISO and CIO) will benefit from taking this course. The point of the course is to make you more effective as a security professional and leader in managing your team, your business, and your relationships with other leaders across the organization.



## How the Course Works

- **Expectations**
  - Managers and leaders are expected to voice opinions
  - This class will give you opportunities to practice
- **Intensive management level labs**
  - Case studies, case scenarios, and group discussions
  - Cyber42 Leadership Simulation game



People in leadership positions are expected to voice their opinions. If leaders do not speak up, what is the perception? The perception is they don't have the appropriate knowledge, savvy, or confidence to be in a senior leadership position!

Because this is a management class, we will model that expectation by providing you the opportunity to practice in class. As a result, the success of this class depends largely on you. To put you in real-world situations the course labs utilize a variety of case studies and scenarios. Throughout the class you will read and analyze 3 business case studies, respond to situations faced by 4 fictional companies, discuss 15 case scenarios, and play 15 Cyber42 Events. It's going to be a ton of fun!

If you are taking this class live (online or in-person) we will have group discussions that require you to break into teams of 4-5 people to discuss the exercises. You will come up with solutions as a team and, based on the group discussion, team members will report to the rest of the class. Please be prepared for this opportunity!

## Fictional Companies in the Course



Throughout the course you will respond to scenarios faced by four different fictional companies:

- HealthHound is a maker of wearable activity trackers
- Thunderbolt is a global logistics and shipping company
- PharmaCo is a large pharmaceutical company
- iPremier is a high-end online retailer

Different companies and industries are used so you can see how various business objectives inform security strategic planning.

## Background and Need for Strategic Planning

- Security and business goals must be aligned
  - Security is just one type of risk that needs to be addressed
  - Security budgets need to be balanced with other business investments
  - Strategic planning is needed to ensure that all business goals are considered

Strategic planning enables us to align security with business goals. Successful security planning requires an understanding of not only security threats and capabilities but also a deep understanding of the business environment and organizational goals. An organization faces many risks in the course of doing business, and security is just one of the risks that needs to be addressed. By balancing security needs with those of other business investments, security can be seen as a business partner and not just a cost of doing business.

## Technology and the Threat Landscape

- Dependence on technology
  - Transformative effect
  - Global connectivity
  - Opens the doors equally to benefits and harm
- Security breaches are on the rise
  - Geographic limitations do not exist
  - Crimes can be committed anonymously around the world
  - There is very little risk of being caught
- Cyber challenges are emerging as fast as we can combat them
  - Information as a commodity has become highly profitable

Business leaders understand that technology and the dependence on technology have had a transformative effect on our society. We have entered an era of global connectivity that opens the doors equally to benefits and harm. Almost weekly, there are new reports in the media of data breaches that range from Personally Identifiable Information (PII) to sensitive government documents to credit card data. Security breaches are on the rise and new cybersecurity challenges are emerging as fast as experts can combat them.

Cyber criminals have taken full advantage of global connectivity in that geographic limitations do not exist, meaning crimes can be committed anonymously across the country with very little risk of being caught. This advantage has also created a market demand that is driven by the need for more raw information that is then used to generate intelligence. Information and intelligence as a commodity have become highly profitable.

As an example, Shawn Henry, previously FBI's executive assistant director, stated in an article published in *The New Yorker*.<sup>[1]</sup> "When I started in my career, in the late 80s, if there was a bank robbery, the pool of suspects was limited to the people who were in the vicinity at the time. Now when a bank is robbed, the pool of suspects is limited to the number of people in the world with access to a \$500 laptop and internet connection. Today, that number is 2.5 billion people. Instead of stealing just one person's credit card, you can steal from millions of people at the same time."

Reference:

[1] <http://www.newyorker.com/magazine/2013/05/20/network-insecurity>

## Security Is No Longer Just an IT Issue

- Security must work across the entire organization:
  - HR, Legal department, and Compliance department
    - Investigations, eDiscovery, Forensics, DLP
  - Business support:
    - Cloud, mobile, BYOD
    - Security architecture, data classification
    - Risk assessment of new initiatives
- Security now impacts others outside of IT:
  - Board of Directors
  - CEO, CFO, etc.

Security is moving beyond being just an IT issue. For security teams to be successful, they have to work effectively across the entire organization. This includes HR, legal, and compliance to support necessary functions such as investigations, eDiscovery, forensics, and data loss prevention. But this also includes new technology areas such as the cloud, mobile, Bring Your Own Device (BYOD), and any other new business initiatives.

One organization has placed an extreme focus on information security. Commonly, the Chief Information Security Officer (CISO) reports to the Chief Information Officer (CIO). However, at one organization, the roles are reversed. At Booz Allen Hamilton, a large U.S.-based government, military, and business consultancy, the CIO reports to the CISO because "the nature of Booz Allen's business—advising businesses, the military and government clients on matters regarding national and information security—requires it to demonstrate the importance of security in its operations."<sup>[1]</sup>

Reference:

[1] <https://www.bankinfosecurity.com/blogs/role-reversal-cio-reports-to-ciso-p-1648>

## Security Investment Prioritization Challenges

- As the threat landscape continues to evolve, it's difficult to determine what security controls should be put in place
- How can security investments be rationalized?
  - Are we spending too much on security?
  - Are we spending too little?
  - Are we spending effectively?
  - How do we decide where to invest?
  - How much should we spend?

Even with a deep understanding of the importance of security, it is still a challenge to prioritize the security controls that should be in place and the amount of investment required. Business leaders want to know that security spending is appropriate and effective.

## Risk-Based Decision Making

- Security business leaders know how to frame decisions around business risk
  - Risk-based decisions must be agreed to by business leaders
- "How much" potential loss is acceptable?
  - What do business leaders believe is an acceptable level of risk to carry?
- Strategic planning is required to:
  - Better address the evolving threat landscape
  - Align and partner with the business
  - Design the most advantageous approach to combat cyber threats

One thing is certain: It's not a matter of "if" an information system will be compromised. It's more about "when" and "how much" information will be lost once it does occur. How can we manage risk to an acceptable level?

Effective strategic planning is required to appropriately address the evolving threat landscape, align security with key business initiatives and stakeholders, and ultimately design the most advantageous approach to combat cyber threats.

## Building a 30-60-90 Day Plan

- Helps set concrete goals
- Manage expectations
  - For leadership, your team, & yourself
- Improves transition process
  - When moving to a new role or org
- Follows a typical process
  - Decipher -> Develop -> Deliver
  - Evaluate -> Optimize -> Strategize
  - Learn -> Contribute -> Lead

30 Days <i>Decipher</i>	60 Days <i>Develop</i>	90 Days <i>Deliver</i>
<input type="checkbox"/> Action #1	<input type="checkbox"/> Action #4	<input type="checkbox"/> Action #7
<input type="checkbox"/> Action #2	<input type="checkbox"/> Action #5	<input type="checkbox"/> Action #8
<input type="checkbox"/> Action #3	<input type="checkbox"/> Action #6	<input type="checkbox"/> Action #9

The 30-60-90 plan is a tool to set concrete goals when someone starts a new job or joins a new team. It is used to define what will be accomplished in the first 30, 60, and 90 days in a new role. Setting clear goals helps ensure that transitions will be smooth and expectations are not only set but also mutually agreed upon.

As a leader you want to make a good first impression. Coming in prepared with a 30-60-90 day plan will give your leadership confidence that you are the right person for the role. In fact, in some cases a potential employer might ask for such a plan as part of the interview process. Even in times of transition when an existing team member takes on an interim leadership position the creation of such a plan may be used to test your strategic planning capabilities.

As a manager you not only want to make a plan for leadership but you also want to have a plan for your immediate team as well as yourself personally. This allows you to reflect on how you and your team are currently positioned and where you want things to go.

The use of specific time frames is a bit of a misnomer. In smaller, faster moving organizations you may want to accomplish certain tasks much sooner than 90 days. In larger, slower moving enterprises it may take much longer than 90 days to achieve certain goals. So why use a 30-60-90 day planning tool at all? It helps focus your thinking in three different buckets.

Typically, the first "30 days" is used to understand your environment. The next month is used to show that you bring some value by contributing some improvement or optimizing an existing approach. This helps you gain traction more quickly. The last month is then used to focus on more strategic goals that will be carried forward past the first 90 days.

In short the first "90 days" are critical to developing your plan and getting buy-in as a security leader.



---

## Case Scenario

---

This page intentionally left blank.

## HealthHound Case Scenario

- Dennis Scott just started a job as Director of Security at HealthHound this week
  - He has a three-person team: Two operations people and one compliance person
- His boss, the VP of IT Operations, unexpectedly left the company
- Now the CEO wants to meet with Dennis
  - Says he has heard that Dennis "knows his stuff"
  - Asked to see his 30-60-90 day plan in two days



It's Tuesday at 7 p.m. You just got home from a long day at work and are making dinner when you get a call from a good friend whose name is Dennis.

You and Dennis go way back. In fact, you first worked together as penetration testers at a big bank many years ago. Dennis just started a new job this week as Director of Security at HealthHound, where he is the highest-ranking information security person in the organization.

Truth be told, you are a little surprised that he got the job. The only management experience Dennis has is as a team lead of some penetration testers at his previous job. But Dennis was always great at interviews, and HealthHound is looking for a technically savvy individual who really understands security threats.

You pause your dinner preparation (that is, opening the takeout) and answer the phone. Right away, you can tell that Dennis is in a little bit of a panic. He's not his usual cool self. It turns out that his boss, the VP of IT Operations, has just left the company for greener pastures. Now the CEO wants to meet with Dennis. In an email, the CEO says that he is looking forward to the meeting because he has heard that Dennis "knows his stuff." The email concludes by asking Dennis to bring his 30-60-90 day plan to the meeting. Dennis has never done such a plan and doesn't know where to start.

## HealthHound Background

- **Maker of wellness products**
  - Wearable activity trackers to measure steps taken, quality of sleep, and other personal metrics
  - Sell to self-insured employers to make employees healthier and lower healthcare costs
- **In an emerging but competitive market**
  - Apple, Fitbit, and other competitors
- **Technology-driven company**
  - 1,500 employees with \$2B revenue
  - Custom hardware
  - Mobile apps, website, cloud accessible via API



HealthHound is one of the leading makers of wellness products, including activity trackers. Their goal is to empower and inspire you to live a healthier, more active life and achieve your health and fitness goals, whatever they may be. The company is in an emerging but extremely competitive market, and it is an incredibly technology-driven organization with a focus on custom hardware and software that enables its wellness tracking platform.

## Lab 1.1: HealthHound Case Discussion

Estimated Time: 15 Minutes

- Goal of this exercise
  - Understand how to frame the work of the security team so that it makes sense to business leaders
- Write down three things that:
  - You think the CEO cares about
  - Dennis should plan to get out of the meeting
- Don't turn the page
  - Potential answers are on the next slide

### NOTE

Don't read the next section

It contains a debrief and potential lab answers

The HealthHound CEO wants to meet with Dennis Scott, the Director of Security, for the first time in just two days. This is Dennis's first week on the job. He is not sure what to expect from the meeting, but he has to come up to speed quickly. He knows that he will have to convey the work of the security team to the CEO in a way that makes sense.

What are three things that you think the CEO cares about?

- 1)
- 2)
- 3)

What are three things you think Dennis should plan to get out of the meeting?

- 1)
- 2)
- 3)

---

## Lab Debrief

---

*Note that this section contains a debrief  
and potential lab answers*

This page intentionally left blank.

## Lab 1.1 Solution: HealthHound Case Debrief

- What does the CEO care about?
  - Getting new products to market
  - Ensuring that customers trust HealthHound's products and services
  - Knowing that you have a plan for security
- What are Dennis's goals for the meeting?
  - Show that he understands HealthHound's business
  - Show that security will be built into HealthHound's products
  - Demonstrate a plan for the security program



The first step in any meeting with one of your key stakeholders is to ensure that you understand their top priorities, interests, and concerns. HealthHound is in an extremely competitive market and the goal of the organization is to empower people to lead healthier lives. This is, of course, done by developing new products that customers will find useful. This product focus is the CEO's top priority. A big component of this is ensuring that customers trust HealthHound's products and services. Without that trust, which is underpinned by a rigorous information security program, customers may not be as willing to invest in the company's products. So, the CEO wants to know what Dennis Scott has planned for security.

If you understand the top priorities, interests, and concerns of your key stakeholders, it is relatively straightforward to map those items to your top action items. As a result, Dennis's goals for the meeting should be to show that:

- 1) He is not just a technical security expert but someone who understands the business and can help the organization grow.
- 2) Security will be built into HealthHound's products, and that the security team will not simply be a reactive organization.
- 3) He has a plan for the organization of the security program.

<b>Audience</b>	<b>30 Days Decipher</b>	<b>60 Days Develop</b>	<b>90 Days Deliver</b>
<b>Executive</b>	<input type="checkbox"/> Meet with key stakeholders <input type="checkbox"/> Understand the culture <input type="checkbox"/> Identify crown jewels <input type="checkbox"/> Analyze control gaps	<input type="checkbox"/> Develop security vision <input type="checkbox"/> Select security frameworks <input type="checkbox"/> Create security roadmap <input type="checkbox"/> Develop business case	<input type="checkbox"/> Establish metrics program <input type="checkbox"/> Develop marketing/comm plan <input type="checkbox"/> Create board presentation <input type="checkbox"/> Develop policy library
<b>Team</b>	<input type="checkbox"/> Understand team member goals <input type="checkbox"/> Analyze team's strengths and weaknesses	<input type="checkbox"/> Define team values <input type="checkbox"/> Develop performance goals	<input type="checkbox"/> Create training plan <input type="checkbox"/> Develop hiring plan
<b>You</b>	<input type="checkbox"/> Define goals for this job <input type="checkbox"/> Define your career goals	<input type="checkbox"/> Find someone to mentor	<input type="checkbox"/> Find a sponsor for yourself
<div> <div>SANS</div> <div>MGT514   Security Strategic Planning, Policy, and Leadership 25</div> </div>			

How can you demonstrate to senior leadership that you have a plan for security?

Framing these items around a 30-60-90 day plan makes it clear what you plan to accomplish.

In the table above the “Executive” row highlights various management and leadership tools used in the course to analyze and better understand the business environment. However, senior leadership quite often will not care about the output of these tools themselves. They care about the outcomes that the analysis will drive. Specifically, the more tangible outcomes of the strategic planning process include leveraging industry standard frameworks, developing a security roadmap, assessing maturity, creating a business case, and establishing a metrics program. These specific outcomes provide tangible evidence that you, as a security leader, have a plan in place to improve the effectiveness of the security program and drive continuous improvement.

It’s not just about what senior leadership wants to see. The “Team” row above highlights that you also need to take time to understand your team members’ goals and corresponding strengths and weaknesses. This will help you develop appropriate performance goals, identify gaps, create a training plan, and onboard new talent.

Finally, you have to remind yourself to be intentional about your career. As no single job is necessarily the destination you want to define your goals for your current job. What do you want to get out of it and what transferable skills do you want to develop? While you may not know early on in your career journey, this process can help you figure it out. Being a mentor to others also aids in this area and helps, not only the other person, but you to develop as well. Finally, to be as successful as possible, especially in the senior executive ranks, you also have to find a sponsor, someone that is willing to connect you with key opportunities and help you achieve your goals.



## Security Leadership Simulation

Let's get familiar with the Cyber42 security leadership simulation, the web application, game mechanics, and scoring.



## Cyber42 – Overview

- Leadership simulation game
  - Puts you and/or your team in real-life situations
  - You choose to take actions that have uncertain outcomes
- Improve your strategic planning capabilities
  - Decipher, Develop, Deliver, and Lead
- Manage your resources



Cyber42 is a leadership simulation game used in a number of SANS Leadership classes. The goal is to put you and your team in real-life situations that security managers and leaders encounter on a regular basis. Of course, your goal is to improve the state of security for your organization and more effectively manage risk. However, the actions that you choose to take can have uncertain outcomes and even unintended consequences.

As you try to improve the security capabilities of the various organizations you encounter you must manage your limited resources effectively. Just like your real-world job you must carefully utilize your available budget and time to deliver projects that are ideally on time and under budget. However, in some cases it may pay off to be more aggressive and proactively build your capabilities. Sometimes fortune does favor the bold. But, just like in real life, you will have to understand when to make those more aggressive moves.

## Cyber42 – How to Win

- Winning the game
  - The team with the highest Security Culture Score wins the game

Score	Emoji
100+	😄😄😄
90 – 99	😊😊😊
80 – 89	🙂🙂🙂
70 – 79	😐😐😐
60 – 69	😞😞😞

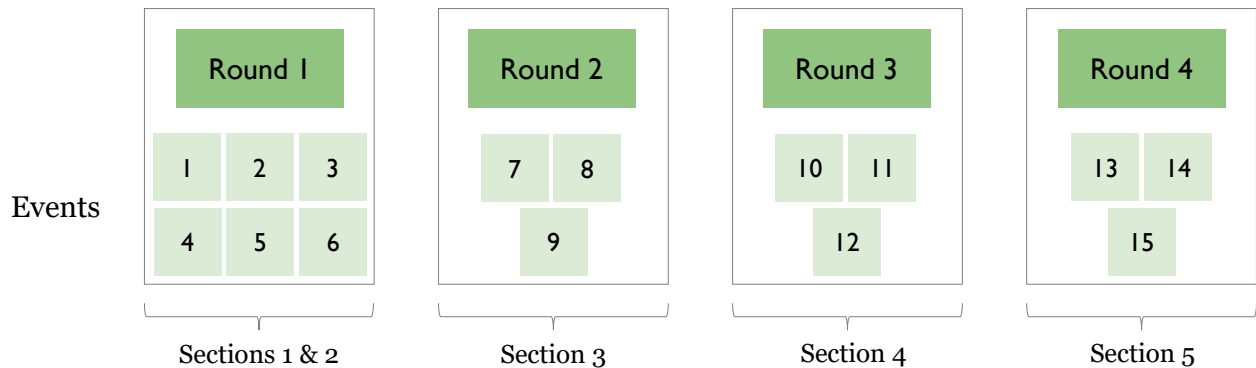
The goal of the game is to get the most Security Culture points. To gain culture points, you build your security capabilities which are tracked based on how much you are able to improve your Decipher, Develop, Deliver, and Lead functions. While you are doing this, just like in the real world, you have to manage your budget and time effectively.

As an indicator of how well you are doing in the game we have a range of scores on a “happiness” scale as represented by various emoji. At the end of the game if you have a score of 100 or more you did amazing (starry eyed grin). A score of 90-99 is great (big smile). Between 80-89 is very strong (smiley face). A little lower between 70-79 there was room for improvement (neutral face). At 60-69 you probably need to revisit your strategy (sad face).

For live classes (in-person or online) the team with the highest Security Culture score will be crowned the winner. If there is a tie, then budget, time, and total of security capabilities (Decipher, Develop, Deliver, Lead) will be used as tie breakers in that order. For example, if two teams have the exact same Security Culture score, then the team with the most budget remaining wins. If those teams have the exact same budget remaining, then the team with the most time points remaining wins. If those teams have the exact same time remaining, then the team with the highest total security capability score wins.

## Cyber42 – Game Structure

### CYBER42



The Cyber42 game in this class is divided into four Rounds. Each round is comprised of a number of different Events. Each Event has different Options (where you choose A, B, C, etc. for your response).

Round 1 has six events. This is done purposely so that you can make more progress building your capabilities before the end of round scoring adjustments occur for the first time. This Round is played over the first two sections of the course.

Round 2 and 3 both have three Events and are played over sections 3 and 4 of the course, respectively. Remember that scoring adjustments (accelerators and penalties) occur at the end of each of these Rounds as well. More about the scoring on the next slide.

Round 4 is the last round of the game and has three total Events. This final Round is played during the last section of the course.

## Cyber42 – Game Scoring

- Game has four rounds
  - You respond to 3-6 Events per round
- Scoring adjustments at the end of each round
  - For every \$250k spent beyond your budget
    - Decrease Security Culture by 1 points
  - For every 1 time unit spent beyond your plan
    - Decrease Security Culture by 1 point
  - For every 1 point greater than 2 for each security capability
    - Increase Security Culture by 2 points

The game is played in four Rounds. At the end of each Round of play, your Security Culture score is adjusted as follows:

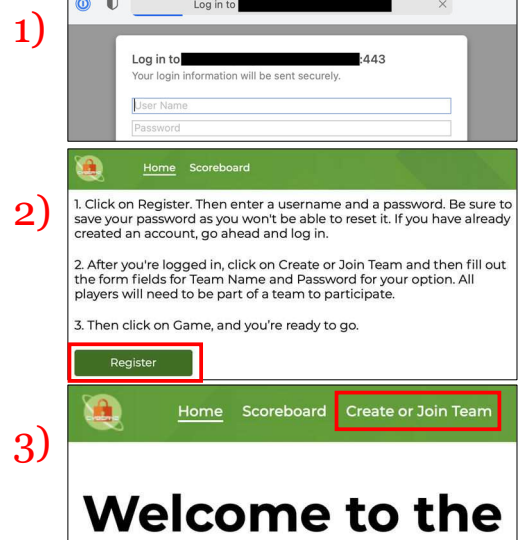
For every \$250k spent beyond your budget, decrease your Security Culture score by 1 point. For example, if you have a -\$500k budget, then decrease Security Culture by 2 points.

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 2 for each security capability, 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 – Game Setup

- 1) Access the Cyber42 web app
  - Link will be provided
  - Enter the basic authentication credentials
- 2) Create your personal account
  - Click the “Register” tab
  - Choose a username and password
  - Include your first name in your username
- 3) Join your team
  - Click “Create or Join Team”



Before you can play the Cyber42 game, you must access the Cyber42 web app. The link will be provided as part of your class. You must do the following three steps:

- 1) Access the Cyber42 web app using the provided HTTP basic authentication credentials. This simply allows you to view the web application.
- 2) Create your personal account in the web application. Click the “Register” tab and choose your username and password. Please select a username that includes your first name so that your team members will know who you are. Once you submit the form, you will be automatically logged in.
- 3) Join a team by clicking “Create or Join Team.” This is explained further on the next slide.

## Cyber42 – Joining or Creating a Team

- For live classes

- Online or in-person
- Enter the “Team Name” and “Password” provided by the instructor
- Events are “unlocked” by the instructor



Home Scoreboard Create or Join Team Hello, frank-instructor

### Join Team

Join

Don't have a team to join? Create one. All players need to be in a team, even if it's a team of one.

- For OnDemand classes

- Create your own team
- You will play as an individual on your own personal team
- Complete Events as they are presented in the class material



### Create Team

Create

If you are playing the game in a live class (online or in-person) you will form teams of 4-5 people. The instructor will help you form teams. Once your team has met and you have introduced yourselves, join your team in the Cyber42 web app. Your instructor will provide your team name and password. All team members must join with the provided password.

If you are taking this class online in OnDemand, you will play on your own as an individual. To get the most out of the game, we recommend pausing the recording when prompted and taking time to play the game. You can then listen to the debrief for each game event and see how other choices would have led to alternate outcomes. With your OnDemand access, you will receive a link to the the Cyber42 web application that is specifically for OnDemand students.

When playing in OnDemand, you must create your own personal team that only has you as a member. Even though you are playing as an individual, you still need to create and join a team. This way the other OnDemand students will only see your team name and not your user id (which may include your actual name). As you play, you will be shown new Events immediately after completing your current selections. To get the most out of the game, we suggest only proceeding to the next Event as the game is presented within the class material.

## Cyber42 – Warning on Using the Cyber42 App

- Choose one person to submit answers for your team

### **WARNING**

- Anyone on the team can make a selection
- Do not finalize a selection until your team agrees
- Choices cannot be reversed

If you are playing the Cyber42 game at a live event (online or in-person), and you are part of a team, you **MUST BE CAREFUL**.

Anyone on the team can make a selection. If they do, it becomes final.

**DO NOT** finalize a selection until your team agrees. **DO NOT** share the team password with anyone else.

Your selections **CANNOT** be reversed.

# 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 I

- Overview
  - Need for Strategic Planning
  - 30-60-90 Day Plan
    - Lab #1: CISO First Impression
- **Decipher the Business**
  - Historical Analysis
  - Values and Culture
  - Stakeholder Management
    - Lab #2: Relationship Management
  - Asset Analysis
  - Business Strategy
    - Lab #3: Strategy Map
- Decipher the Threats
  - Threat Actors
  - PEST Analysis
  - Threat Analysis

This page intentionally left blank.



## Why Security Must Decipher the Business

- Many technical security professionals do not have an understanding of business goals
  - There is a disconnect between security and business leaders
  - There is an inability to identify which security projects are important to the organization
- Elevator pitch
  - You're in the elevator with the CEO and get asked, "What are you working on?"
  - How do you answer?

Many technical security professionals do not have a good understanding of business goals. This creates a disconnect between security and business leaders. One way to help bridge this disconnect is by working on your elevator pitch for security using the "30/60/90" approach for communications. Assume that you have 30 seconds with the CEO, 60 minutes with a business partner, and 90 minutes to do a presentation. Have talking points and presentations prepared in advance so that you can seamlessly communicate how security is able to understand and meet business goals. However, building up to these short talking points and presentations is not easy. They require a deep understanding of your organization and the business.

## How to Develop an Understanding of the Business

- 1) Understand where you've been
  - Analyze your organization's history
- 2) Understand how you operate
  - Determine your values and organizational culture
- 3) Learn who the major players and leaders are
  - Develop a Stakeholder Management plan
- 4) Understand key business assets
  - What is important to the business?
- 5) Learn how business strategy works
  - Create a strategy map to link projects to strategic objectives

This understanding of the business comes from:

- 1) Understanding where you've been  
By analyzing your organization's history, you can better plan for the future.
- 2) Understanding how you operate  
It's not just about *what* has been done in the past. Understanding *how* this was accomplished is key to understanding acceptable working norms. This is done by understanding the organization's values and culture.
- 3) Understanding and developing relationships with key stakeholders  
Learning about the major players and leaders in the organization to develop a Stakeholder Management plan.
- 4) Understanding business assets  
With your knowledge of the business from the previous sections, you should have a sense of what the organization considers to be critical business assets. If you think these assets are important, then it is possible that your adversaries may consider them to be valuable, too.
- 5) Understanding business strategy  
Analyzing business models and strategic objectives and utilizing strategy maps and Porter's Five Forces to analyze corporate direction.

# 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 I

- Overview
  - Need for Strategic Planning
  - 30-60-90 Day Plan
    - Lab #1: CISO First Impression
- Decipher the Business
  - **Historical Analysis**
    - Values and Culture
    - Stakeholder Management
      - Lab #2: Relationship Management
  - Asset Analysis
  - Business Strategy
    - Lab #3: Strategy Map
- Decipher the Threats
  - Threat Actors
  - PEST Analysis
  - Threat Analysis

This page intentionally left blank.

## Historical Analysis

- Learn your organization's history to better:
  - Communicate with business leaders
  - Understand the probable future
  - Align security team activities with business goals

"Those who cannot remember the past  
are condemned to repeat it."  
- George Santayana

George Santayana was a philosopher, essayist, poet, and novelist who was born in Spain, and raised and educated in the United States. He famously said, "Those who cannot remember the past are condemned to repeat it." This is especially important for strategic planning. Business leaders are aware of an organization's history. If we don't have that same understanding, we will not be able to communicate effectively with those business leaders. Moreover, the past helps us understand the probable future. Instead of being condemned to repeat the past by remembering what has previously occurred, we will be better prepared to align security team activities with business goals.

## What Are the Major Periods of Change?

- Identify periods of major change
  - Use archives and interviews
  - Are there things you used to do that you should consider doing again?
  - Are there things you are doing that you should consider NOT doing again?
- Lessons from history
  - Mistakes you do not want to repeat
  - Events that helped shape the culture

To better understand your organization's history, it is useful to identify the major periods of change.

In 1993, Apple introduced the Newton, which was the first Personal Digital Assistant (PDA). It was intended to be a portable computer that would reinvent personal computing. However, it was not commercially successful and was discontinued in 1998. Despite its commercial failure, Apple learned from the Newton and went on to develop the iPhone and iPad. This is an example of a product that was ahead of its time and was worth considering again once technology matured.

It was under the leadership of then Apple CEO John Sculley that the Newton was introduced. Sculley famously ousted Apple founder Steve Jobs from the company and went on to increase profits from \$800 million to \$8 billion.<sup>[1]</sup> He was CEO from 1983 to 1993 and, many argue that by the time of his departure, had shifted the company away from its product-centric culture and focus on "making the best products in the world." This lesson of staying true to the company culture is with Apple to the present day. In 2012, Apple hired John Browett to head the retail business. He was fired after only nine months on the job. Apple and Browett realized very quickly that it wasn't a cultural fit with Browett saying, "The issue is I just didn't fit with the way they ran the business."<sup>[2]</sup>

### References:

[1] [https://en.wikipedia.org/wiki/John\\_Sculley](https://en.wikipedia.org/wiki/John_Sculley)

[2] <https://gigaom.com/2013/03/15/former-apple-retail-chief-john-browett-admits-he-was-a-bad-fit-at-the-company/>

## Phases of Computing

Era	Dates (approximate)	Computers (approximate)	Users (approximate)
<b>Mainframe</b>	1950-1965	~100,000	Millions
<b>Mini-computing</b>	1965-1980	~10M	Tens of millions
<b>PC and Client/Server</b>	1980-1995	~100M	Hundreds of millions
<b>Internet</b>	1995-2007	~1B	Billions
<b>Mobile</b>	2007-present	Billions	Billions
<b>Internet of Things (IoT)</b>	Present-?	Tens of billions	Billions

IBM, as a company, largely parallels the history of computing. In the mainframe era, the cost of computing was high. Only large enterprises could afford the investment, which limited the number of computers and corresponding users. With the mini-computer, costs decreased, and more companies could invest in computing resources. However, it wasn't until the PC era ushered in by IBM and Microsoft that the cost of computing decreased enough to reach larger numbers of users. Now, everyone could have a PC on their desk and eventually have access to the internet. With the introduction of mobile devices, computing access has now increased to billions of people. It is estimated that there will soon be almost as many smartphones as there are literate adults in the world. With the Internet of Things (IoT), there is an opportunity to connect even more devices.

Looking back in time, the height of each phase of computing lasted approximately 15 years. Certainly, the older technologies still persist. Mainframes are still widely used today. But each wave of computing allowed technology to reach more and more people. Recently, starting with the internet era, the length of time between new technologies seems to be shortening. With the internet era starting in roughly 1995, it was overtaken by the mobile era starting in 2007. Has the Internet of Things already started its rise?

## Security History

- 1972: Buffer overflow first described
- 1988: Morris Worm exploits buffer overflow
- 1996: Step-by-step guide for exploiting buffer overflow
  - "Smashing the Stack for Fun and Profit" by Aleph One
- 1998: SQL Injection described
  - Article by Rain Forest Puppy in *Phrack* magazine
- 2005: Samy MySpace Worm
- 2006: XSS goes mainstream
  - "Hacking Intranet Websites from the Outside" by Jeremiah Grossman
- 2010: Stuxnet discovered
  - "The World's First Digital Weapon"

The history of security closely maps to the various phases of computing. The buffer overflow vulnerability was first described in 1972.<sup>[1]</sup> However, it wasn't until 1988, in the PC era, that the first large-scale exploit of a buffer overflow occurred. This was the Morris Worm created by Robert Tappan Morris, who was a grad student at Cornell University. It exploited known vulnerabilities in UNIX services, including sendmail, finger, and rsh/exec, and it was the first work to gain significant media attention. *The Cuckoo's Egg* by Cliff Stoll also described the author's efforts at combating the worm.<sup>[2]</sup> Buffer overflow vulnerabilities still plague many systems today. This is partly due to Aleph One's 1996 paper, "Smashing the Stack for Fun and Profit," which provided step-by-step instructions for exploiting buffer overflows.<sup>[3]</sup>

As the web rose in prominence, so did web application security vulnerabilities. In 1998, Rain Forest Puppy described SQL Injection in *Phrack* magazine.<sup>[4]</sup> It is still one of the most impactful vulnerabilities that you can have in your application because it allows an attacker to potentially execute any database command. In 2005, Samy Kamkar created the Samy MySpace Worm, which was the first Cross-Site Scripting (XSS) worm.<sup>[5]</sup> Just one year later in 2006, Jeremiah Grossman gave a talk at BlackHat called "Hacking Intranet Websites from the Outside."<sup>[6]</sup> This talk helped take knowledge about XSS mainstream and resulted in increased focus on web application security issues.

The Internet of Things (IoT) is about connecting increasing numbers of physical objects such as cars, homes, thermostats, and even people to the internet. The Stuxnet Worm showed how security issues could have a huge impact on connected devices.<sup>[7]</sup> By targeting the Siemens Programmable Logic Controllers (PLC) used in Iranian nuclear facilities, the Stuxnet Worm changed the speed at which centrifuges used to process nuclear materials would spin. This resulted in damage to the nuclear facilities and a delay in Iran's nuclear capabilities.

### References:

- [1] <https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande72.pdf>
- [2] [https://en.wikipedia.org/wiki/The\\_Cuckoo%27s\\_Egg\\_\(book\)](https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg_(book))
- [3] <http://phrack.org/issues/49/14.html>
- [4] <http://phrack.org/issues/54/8.html>
- [5] <https://samy.pl/myspace>
- [6] <https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Grossman.pdf>
- [7] <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

## Your Security Team History – Example

### 2017

- + Network Security
- + Intrusion Prevention Systems
- + Antivirus
- + Remote Access VPN
- + Security Monitoring
- + Incident Response
- + Endpoint Encryption

### 2019

- + Application Security
- + Data Loss Prevention
- + File Integrity Monitoring
- + Web Application Firewall
- + Forensics

### 2021

- + First CISO Hired
- + Metrics Program
- + Next Generation Firewall
- + Wireless Intrusion Detection
- + Security Monitoring Expansion

### 2023

- + Data Science
- + Advanced Analytics
- + Cloud Security
- + Cyber Threat Intelligence

### 2018

- + PCI Support
- + SOX Support
- + Network Segmentation
- + Web Content Filtering
- + Vulnerability Management
- + Security Event Management

### 2020

- + Product Security Team
- + Host Intrusion Prevention
- + Removable Media Encryption
- + Security Operations Center
- + Application Security
- + eDiscovery

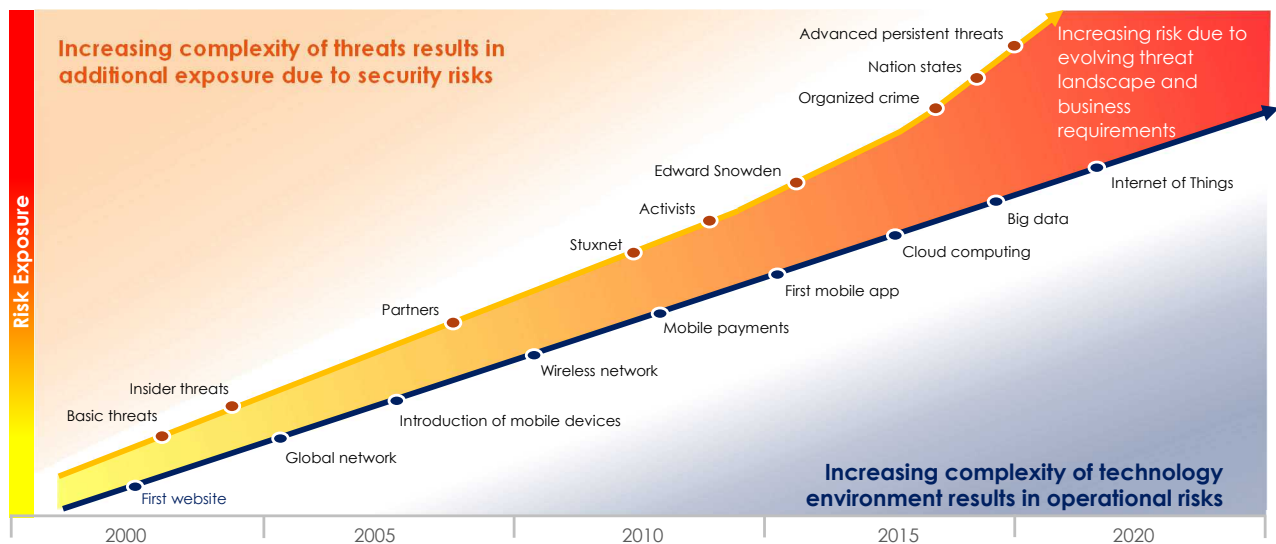
### 2022

- + Security Team Centralized
- + Awareness Training
- + Mobile Security
- + Penetration Testing Program

Just as it's useful to track the history of your company or industry, it is also useful to track the history of your security team. This example shows how the security team improved capabilities over years by focusing on network, host, compliance, incident response, application security, data security, mobile, and many other capabilities. If your team has undertaken major initiatives or projects, it is useful to create a timeline like this to remind management of all the work that has been done and celebrate the team for their accomplishments to date.



## Technology Risk Graph



This graph shows another way you can visually represent the history of your organization. The lower part of the graph represents the evolution of technology that is used in your company to support various business initiatives. This example has been made generic to include things like "First website," "First mobile app," and "Cloud computing." For your company, you can put even more specific items and systems. This highlights the fact that, over time, the company makes increasing investments in technology to support business goals. This increasing complexity of the technology environment results in increased operational risks. These technology investments, coupled with the increasing complexity of the threat landscape as shown in the upper part of the graph, result in increasing risk that the organization has to choose how to handle.

## In Summary

- Business leaders
  - Understand the history of the organization
  - Where it's been and where it's going
- Security team must:
  - Frame our work within the larger business and technology context
  - Highlight the accomplishments of the team
- Allows us to better:
  - Communicate with business leaders
  - Understand the probable future
  - Align security team activities to business goals

By understanding the history of your industry, company, and department, you can better understand where you've been and where you might want to go. Framing the work of the security team within these larger contexts allows us to better communicate with business leaders. By framing the conversation around risk associated with various business decisions, we can better align security activities with business goals.

## Thunderbolt Shipping Case Study

- Shipping and logistics company
  - “What you need when you need it!”
  - Grew from a family-owned business
- Publicly traded
  - Competes with FedEx, UPS, and DHL
  - 500K employees around the world
- Considering a cloud migration strategy
  - Focus on activities that drive revenue and profit
  - Need to retrain existing staff

### READ

Read the 1.5 pages of the case study below

It takes approximately 10 minutes to read the case



### Thunderbolt Shipping Case Study

*What You Need When You Need It!*

#### Overview

Just as Leslie Franks, Chief Information Security Officer (CISO) of Thunderbolt Shipping, was about to close up for the day, she received a calendar hold from Chief Executive Officer (CEO) Barbara Hamer. The executive offsite, which had not been held in person for years due to the COVID pandemic, would be hosted in person. As Franks quickly reviewed the agenda, her shoulders fell. Most of the session would be facilitated by Hani Selah, the recently hired Chief Digital & Technology Officer (CDTO), and the focus was titled “Thunderbolt’s Cloud Migration Strategy.” For years, Franks had pushed back against the idea of moving data to the cloud, but she knew the tide was turning. Despite previous security issues and a longstanding philosophy of information control, a new CEO and a new CDTO were confident that moving data to one or more cloud providers would benefit the company in the long run.

Still, Franks loved Thunderbolt, and she always preferred to be part of the solution, not part of the problem. She knew that cloud migration strategies take various forms, and there was plenty of middle ground between 100% cloud data storage and zero cloud data storage. Admittedly, a few applications already resided in the cloud and there had been no security issues thus far. There was also pressure from the board as competitors announced bold cloud migration strategies. Additionally, an increasing talent shortage fueled the desire to outsource non-critical information technology (IT) functions and free up resources for more valuable work. But members of her own team were very set in their ways and fearful of any change disrupting the status quo. If cloud migration was truly inevitable, how could Franks support the transition of the right technology to the cloud without losing key talent and keep critical data secure?

#### Company History

Thunderbolt Shipping was founded in 1949 by Frederick A. Casey. Casey fought on the European front in WWII and was inspired by the ability of the allied forces to deliver what was needed when it was needed to overseas troops as well as the Republic R-47 Thunderbolt fighter jet. Shortly after naming his new company,

Casey added the tagline, “What you need when you need it!” Casey predicted that consumer demand for goods would one day require military level logistics, and he was not wrong. Despite being raised near Chicago, Casey opted to start the company in Minneapolis, Minnesota. Aside from proximity to corporations that would eventually become household names (e.g., General Mills, Target, 3M), Casey’s bet on the Twin Cities paid off with the construction of Interstates 35 and 94 in 1956 as well as the expansion of the MSP airport in 1962. Casey’s military service and subsequent connections as well as a strong focus on information protection provided an “in” to government shipping contracts, which helped the business survive several economic downturns.

In 1990, Casey Sr. retired and handed the company to his son, Frederick A. Casey Jr. Although Casey Jr. believed in his father’s philosophy of information protection as a strategic advantage, he moved the company to a more business-forward strategy. While moving away from government business, he embraced technology and fully utilized internet-enabled services such as real-time tracking and delivery notification. He also spearheaded the creation of two homegrown systems: Bolt and Hermes. Bolt optimizes delivery routes based upon geographic distance and contracted delivery time. Hermes began as a basic customer notification system that grew into an effort to make shipping “fun” by inserting positive messages and stories for customers as packages passed key transit points. The explosion of consumer demand helped Thunderbolt grow exponentially, and the company was routinely listed as one of the top 10 privately held companies. Casey Jr. remained steadfast, however, that information should be kept in-house whenever possible for the safety of the company, its customers, and its employees.

Casey Jr. resisted pressure to take the company public but could no longer hold off the board of directors upon his father’s death in 2004. The company began trading on the New York Stock Exchange (NYSE) in 2005. In 2009, Thunderbolt acquired Orage, a European shipping business, solidifying the company’s ability to ship globally. The integration of the two companies was not without its challenges, and European operations were the victims of a ransomware attack in 2014. The attack resulted in a loss of over \$250 million, and the board blamed Casey Jr. for allowing the European division to maintain its own IT operations and not adopt Bolt. The blame increased with the discovery of a memo from Franks, then a security manager, highlighting several vulnerabilities in Orage’s technology. These observations gained her significant recognition, and Casey Jr. eventually appointed her Chief Information Security Officer (CISO), which was a newly created position. This was not enough to satisfy the board. Casey Jr. was replaced with Hamer, former Chief Revenue Officer (CRO) of a major big box retailer. Her first order of business was to hire Peter Yang as Chief Information Officer (CIO) and charge him with converting European operations to the Bolt system in 2016. The move was successful, but Yang felt strongly that Thunderbolt’s core competency was not in building and managing its own internal data centers. He began suggesting cloud data solutions as an alternative. Franks, still concerned about data control and visibility, disagreed.

Hamer’s first big move was to acquire Plinky Printing & Copying in 2018, which was renamed ThunderPrint. Plinky/ThunderPrint was led by Praful Daskika, and he joined Thunderbolt with the acquisition. The concept of “print and ship” had already been pursued by direct competitors for decades, and Hamer argued this was simply what needed to be done to match the competition. Franks voiced strong opposition to keeping ThunderPrint data in the cloud in contrast to Yang’s position that their operations were more efficient and technology resources should be used for more valuable activities. The debate increased the visibility of the cloud computing and it rose to the top of the priority list during the COVID pandemic years of 2020 and 2021. Thunderbolt and its competition found themselves in an “all hands” situation with resources working overtime to get an increased number of packages to customers during lockdowns. Franks continued to raise concerns while Yang continued to maneuver for technology resources to be diverted from internal systems, data management, and storage to work that could improve operations, enhance the customer experience, and lighten the burden placed on the technology team. Seeing the need for a more holistic technology strategy, Hamer created the position of Chief Digital & Technology Officer (CDTO), which was filled by Selah in 2022. Selah came to Thunderbolt with over a decade of experience with a direct competitor in a similar position, which convinced a reluctant C-Suite that the position was indeed necessary. Hamer asked Selah for an assessment of cloud computing versus on-premises systems, and he recommended the company pursue a comprehensive cloud strategy. Franks was concerned.

# CYBER42

## Round 1 Event #1

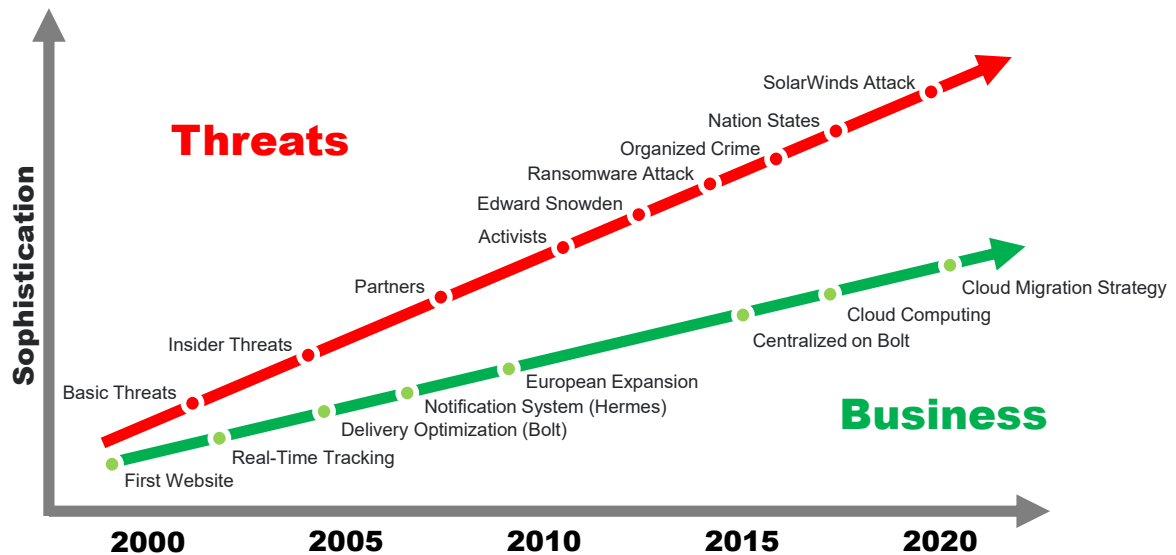
Now that you are self-registered in the Cyber42 web app, it's time to start Event #1. Let's begin!

# CYBER42

## Event #1 *Debrief*

This page intentionally left blank.

## Thunderbolt Business Risk Graph



SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

49

Based on what we have now learned about Thunderbolt the diagram above highlights the business technology investments that the company has made over the years. It's important to couch these items in terms that senior leadership can understand. For example, all business leaders will know that improvements have been made over the years to the delivery and notification systems, European expansion occurred, and that now there is a push to move to the cloud.

These business investments have increased operational risk to the organization in the context of a changing threat landscape. Thunderbolt suffered the ransomware attack that was, notably, during a period when there were few if any technology investments (between European expansion and the centralization on Bolt). These facts can be used to highlight a larger story of the need to keep up with business, technology, and threat landscape changes that impact 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 I

- Overview
  - Need for Strategic Planning
  - 30-60-90 Day Plan
    - Lab #1: CISO First Impression
- Decipher the Business
  - Historical Analysis
  - **Values and Culture**
  - Stakeholder Management
    - Lab #2: Relationship Management
  - Asset Analysis
  - Business Strategy
    - Lab #3: Strategy Map
- Decipher the Threats
  - Threat Actors
  - PEST Analysis
  - Threat Analysis

This page intentionally left blank.



## Values and Culture

- Learn about core values to:
  - Better understand the culture of your organization
    - What is it like to "live" here?
    - Will I like it here? Will they like me here?
  - Establish acceptable working norms
  - Align security to corporate culture

**"Culture eats strategy for breakfast."  
- Peter Drucker**

The quote, "Culture eats strategy for breakfast," is attributed to famed management guru Peter Drucker. On one hand, it can refer to the fact that a winning culture, one focused on teamwork and delivery, can accomplish anything. On the other hand, it can refer to the fact that every organization has a certain way of doing things and, if you don't conform to those working norms, the culture will eat you alive. As a leader and manager, you have to understand the culture of your organization so that you can establish acceptable working norms. By aligning security to the corporate culture, you can position your team for success.

## Purpose of a Value Statement

- Values
  - Help you understand the culture of your org
  - Critical to current state analysis
  - Guiding principles to help you achieve your vision
  - Foundation of organizational culture
- Why are values important for strategic planning?
  - Establish stability and long-term continuity
  - Provide guidance for how to act
  - Describe "how" the work will get done
  - Provides a decision-making framework

Organizations are living organisms, and, like individuals, they have a personality and organizational culture that are unique. A large part of being a successful executive is understanding your people and then using that knowledge to build both high-performance teams and superior working relationships. Organizational culture and personality are built on a foundation of values that define the organization.

To establish this understanding and then get people to buy into the fact that you have their best interest at heart, all while still accomplishing the organizational mission, require the executive to demonstrate the values of trust and integrity each and every minute of each and every day. Values must be shown by example and driven top down in alignment with overall corporate direction.

You can also encourage employees to create a personal value statement that aligns with the departmental and corporate values. This might add more meaning to the company's value statement for the employee.

Employees will pay more attention to what you *do* instead of what you *say*. Executives must "walk the talk." Too often in the business environment, managers will say the right thing, and then turn around and by their actions demonstrate that they didn't mean what they said. This type of behavior will lead to an environment that lacks trust, and it shows employees the manager is lacking in integrity. Employees will often put up with a lack of competence in some areas—lack of time management skills, etc.—but very few will put up with a lack of trust and integrity for an extended period of time.

Initially designing organizational values is important, but it is just as important for senior management to show—preferably by example—that it embraces and lives the values that have been determined to be of importance to the organization. It is not sufficient to establish values and a value statement, and then take a look at it only every couple of years in order to dust it off and say, "Hey, look what we have." The established organizational values, as defined in the value statement, must be lived by all employees each and every day.

The consumer product giant Procter & Gamble has as one of its values that it will not provide bribes to local, state, or government officials in any country—even if that is the norm for the country in which it is trying to establish a business foothold. This value is "lived" by every employee so there is never any confusion as to what the right thing to do is when establishing a factory in a third-world country. Conversely, Enron had a fantastic value statement, and the results speak for themselves. Enron management clearly did not "walk the talk."

The SEC, in its final definition of "Code of Ethics," states, "We continue to believe that ethics codes do, and should, vary from company to company and that decisions as to the specific provisions of the code, compliance procedures, and disciplinary measures for ethical breaches are best left for the company. We strongly encourage companies to adopt codes that are broader and more comprehensive than necessary."<sup>[1]</sup>

The primary reason to create a value statement is to assist each and every employee in regard to knowing how to act and what decisions to make when they are confronted with a question that requires clarification. For example, I need to build this factory in China and the local mayor is asking for a \$10,000 contract kickback. Is this okay for me to do? What if the employee of a competitor calls me and wants to sell me its new secret product formula? Can I buy it and use it to improve our competitive advantage?

It is vital to an organization that the executives believe in and promote the value statement as a core part of the organization's ethical culture. They must ensure the organization applies resources to provide employee training on the key concepts covered by the value statement and communicate expectations about adhering to these values in all situations.

Consider the famous quote attributed to Machiavelli, "The end justifies the means." Do we want to live like that and work in an organization that thinks like that? Probably not. Value statements balance the mission and vision. We define what we want to achieve and how we want to act in pursuit of those achievements. Both are important.

Reference:

[1] <https://www.sec.gov/rules/final/33-8177.htm>

## Values At General Electric

"Develop an atmosphere  
where people will dare to try new things  
where people feel assured in knowing  
that the only limits of their creativity and  
drive will be the feeling on how  
far and fast they move."

Jack Welch of General Electric made this value statement, and then went on to make internal changes showing that he was serious about having this value embraced.

At GE's training center, procedures on what made a good senior manager had been enshrined in Blue Books. When Welch made his new value statement on creativity, he then had a symbolic Blue Book burning ceremony. This was his way of saying that the old values were not enough and that new values were needed.

In a culture such as this that values innovation, the security team cannot be seen as the team that blocks creativity. In fact, security can thrive in this environment by pushing the envelope on security capabilities and enhancing product security features.

## Federal Reserve Bank of Atlanta Values

- Integrity
  - We do the right thing
- Excellence
  - We do things right
- Respect
  - We treat people right
- Institutionalized using the six-word story
  - Six-word statements written by employees
  - Demonstrate how bank values resonate
  - Based on the Ernest Hemingway challenge of writing a six-word story
    - "For sale: Baby shoes, never worn."
- Example stories:
  - "Be the person my dog sees."
  - "Wrinkles and eye circles. Worth it."
  - "Being different's hard, until you accept."



The Federal Reserve Bank of Atlanta has a novel approach to socializing the values of their organization. They started an initiative called the Six-Word Story Project where they asked employees to create a six-word story that demonstrated how the Bank's values resonated with them on a personal basis. These stories were published on television screens throughout the organization and in printed materials along with the photo of the person who submitted the story. These stories were also used in a commemorative art project that traveled to various bank locations. What a great way to get people engaged and thinking about the organization's values!

Information about the values at the Federal Reserve Bank of Atlanta courtesy of their CISO, Russell Eubanks.  
Twitter: @russelleubanks

## Tips for Creating Value Statements

- As a manager and leader, you are expected to:
  - Understand the vision and values of the company
  - Define "how" the work of the team gets done
  - Express the "how" by the values you create and espouse
- Pick a small number of core values around which you can build the team culture and personality
  - Do they provide guidance to employees?
  - Can they be measured and prioritized?
  - Are they stable? They should not change frequently
- Security team culture must align with:
  - Values of stakeholders
  - Culture of the overall organization

As a manager and leader, you are expected to understand the vision and values of the company. These values define how the work gets done in the organization. By defining and living these core values, you create a team culture and personality that help guide employees in the work that they do.

Once you determine a core value, you need to also figure out how you are going to measure the adoption and adherence to that value. For example, if we want to be a people-oriented organization, we can measure employee turnover. Why? So we can compare retention with our peers. Can we put periodic annual checks in place to see how well we are adhering to this value? How are we going to enforce or discipline an employee who is behaving counter to this value?

Values should be stable and tied closely to the vision of the organization. The mission might change due to the changing demands of the market, and the vision might be altered based on the results of strategic planning, but the values, culture, and ethics of your organization should be long-lasting.

Security should not try to change the corporate culture. Security must align with the values and culture of key stakeholders and the overall organization.

## Whose Values Are These?

"Respect, Integrity, Communications, and Excellence.  
We do not tolerate abusive or disrespectful treatment.  
Ruthlessness, callousness and arrogance  
don't belong here."

This is Enron's value statement. It has common values like respect, integrity, communications, and excellence. However, it then specifically calls out ruthlessness, callousness, and arrogance as not being acceptable to the organization. It is very strange to have such items called out in a value statement. Maybe the leaders at Enron knew something about the culture of their organization and wanted to pay attention to what employees *do* instead of what they *say*.

Reference:

<http://www.nytimes.com/2002/01/19/opinion/enron-s-vision-and-values-thing.html>

## What Values Should Your Security Department Have?

- Accountability
- Automation
- Business Supporting
- Collaboration
- Customer focus
- Efficiency
- Entrepreneurial
- Ethical behavior
- Excellence
- Expertise
- Innovation
- Integrity
- Leadership
- Partnership
- Professionalism
- Quality
- Respect
- Transparency
- Trustworthiness
- Vulnerability

No matter what the overall values of your larger company are, you might want to instill a set of values specifically for the security team. Some example values are listed here on this slide for reference.



## Thunderbolt Values Discussion

- Read the case study below
  - Thunderbolt's corporate structure and executive team priorities drive the values of the organization
- Group discussion
  - How would you describe Thunderbolt's culture?
  - Who would be satisfied saying "no" to cloud?
  - Who would be satisfied saying "yes" to cloud?
- Prepare your thoughts for a class debrief
  - Write down your key points

### READ

Read the 1-page case study below

It takes 5-10 minutes to read the case



### Thunderbolt Corporate Structure

Thunderbolt operates via three distinct departments: Consumer, Small & Medium Business (SMB), and Corporate. ThunderPrint reports to the consumer division, despite serving both consumer and business clients. Within each department, logistics are managed by the air, rail, ship, truck, and "first/last mile" teams. All sales and customer service teams report to Sandra Lopez, Chief Revenue Officer (CRO). Lopez joined Thunderbolt in 2012 from a direct competitor. Operations are overseen by Chief Operating Officer (COO), Enola Benally, who was referred by Lopez and hired in 2013. Operations mirrors sales in its structure and consists of separate divisions supporting Consumer, SMB, and Corporate.

Talent management of Thunderbolt's 500K+ team members is led by Adam Samuelson, Chief Human Resources Officer (CHRO). The average employee has higher-than-average tenure with Thunderbolt due to its superior wages and benefits as well as a strong familial culture. Recent labor market challenges and an overworked staff have made recruiting and retention more difficult, particularly within the IT department and the customer-facing retail teams. Higher-than-average tenure also means a higher-than-average age for the employee population, and younger workers tend to be more attracted to technology companies working on "cooler stuff."

Finance and Accounting report to the Chief Financial Officer (CFO), Damien Biggs. Biggs joined Thunderbolt in 2003 after several years with a US Big Four auditing firm. He rose through the ranks and was appointed CFO in 2013. He saw the company through several downturns, and his aversion to risk avoided many financial traps pursued by competitors who were eventually acquired by others or went bankrupt. Despite his low tolerance for risk, Barbara Hamer (CEO) recognized Biggs as a good balance for her own risk-loving personality and often consulted him privately about big decisions before bringing in the rest of the C-Suite.

The technology team is overseen by Hani Selah, the Chief Digital and Technology Officer (CDTO), and is divided into two divisions. The first is the IT Department, overseen by CIO Peter Yang. Yang's department is charged with the creation, acquisition, and maintenance of all Thunderbolt technology systems and numbers close to 5,000 team members (over 1,000 of whom are developers). The IT team spends the bulk of its time

maintaining and upgrading its two homegrown systems, Bolt and Hermes. The second is the Security Department, which counts nearly 150 team members and is run by CISO Leslie Franks. Franks joined Thunderbolt in 2010 and became CISO after the European cyber-attack scandal when the board discovered she had pushed for Bolt technology to be adopted in the European acquisition. Most believe the financial losses of the breach would have been avoided if her advice had been followed. Because of this foresight, her word now carries extra weight with the board. Franks has a loyal following, and her team consistently exceeds retention averages of both the company and the industry.

## Thunderbolt Values Discussion

Response to Cloud	What values would be conveyed?	Who might be satisfied with this response and why?
No		
Ignore		
Yes		

There is a saying that actions speak louder than words. Every security team, knowingly or inadvertently, conveys certain values depending on the actions they take.

**1) What values would be conveyed if Thunderbolt said *no* to the use of cloud computing? Who would be satisfied with this response?**

**2) What values would be conveyed if Thunderbolt *ignored* the use of cloud computing? Who would be satisfied with this response?**

**3) What values would be conveyed if Thunderbolt said *yes* to the use of cloud computing? Who would be satisfied with this response?**

---

## Discussion Debrief

---

*Note that this section contains a debrief  
and potential answers*

This page intentionally left blank.

## Thunderbolt Values Discussion

Response to Cloud	What values would be conveyed?	Who might be satisfied with this response and why?
<b>No</b>	Conservative Dictatorial	<b>CISO</b> - historically resisted cloud and wants to maintain control and visibility of data <b>CFO</b> - naturally risk averse
<b>Ignore</b>	Complacency Unsupportive	Other stakeholders may be indifferent as long as their business needs are met
<b>Yes</b>	Innovation Partnership	<b>CDTO</b> and <b>CIO</b> - they are charged with getting features to market faster and recruiting/retaining talent

Thunderbolt has an overall family and people-focused culture as evidenced by the above average wages and higher than average tenures. These factors have created strong company loyalty along with a workforce that has a higher-than-average age. There is a realization that younger workers are attracted to working with modern technologies. Cloud is a big driver of modern technology trends. In response to the current reality, Thunderbolt has three high level options:

### 1) Say "No" to cloud

Preventing technology teams from utilizing cloud services can create more uniform technology deployments and ensure standard controls are utilized. However, this approach could alienate teams that are already utilizing cloud computing. Moreover, it would mean falling behind on current technology trends. More traditional and risk averse leaders like the CISO and CFO might be okay with this approach.

### 2) Ignore cloud by doing nothing

Given that various teams are already using cloud services, Thunderbolt could simply ignore the situation. However, this would further push people to find unsupported mechanisms to process and store data, resulting in shadow IT deployments and increased risk. While other leaders in the company may simply be focused on meeting their business needs, they should also be informed of the ongoing operational risk of these unsupported technology activities.

### 3) Embrace cloud and officially support it

Given the current situation, Thunderbolt can realize that the adoption of cloud computing is inevitable. As a result, Thunderbolt's leadership can make the strategic decision to implement cloud computing across the organization as a whole. This is why the Chief Digital and Technology Officer (CDTO) was hired and what the CIO wants to help recruit and retain new talent.

## Core Values Summary

- Core values are key to:
  - The culture of the organization
  - Establishing acceptable working norms
- Culture is very unlikely to change
  - Must determine how to adapt the security team to the culture of the organization

Remember that "culture eats strategy for breakfast." In other words, culture is very unlikely to change. As a manager and leader, you must determine how to adapt the security team to the culture of the larger organization so that it can be successful. This is done by understanding the values of the larger organization and establishing acceptable working norms. This helps guide the team and provides guidelines for *how* the work should get done.

# 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 I

- Overview
  - Need for Strategic Planning
  - 30-60-90 Day Plan
    - Lab #1: CISO First Impression
- Decipher the Business
  - Historical Analysis
  - Values and Culture
  - **Stakeholder Management**
    - Lab #2: Relationship Management
  - Asset Analysis
  - Business Strategy
    - Lab #3: Strategy Map
- Decipher the Threats
  - Threat Actors
  - PEST Analysis
  - Threat Analysis

This page intentionally left blank.

## Stakeholder Management Strategy

- By the end of this section, you will understand:
  - The importance of stakeholders
    - Common stakeholders
  - Stakeholder management
    - How to identify stakeholders
    - How to map their interests and influence
    - How to develop and drive your relationship plan
  - Common communication methods
    - Managing resistance to your project

In this section, we cover the importance of stakeholders and stakeholder management. It may not be apparent initially, but even a simple technology deployment as part of your strategy could impact not only your security organization but also the overall enterprise. As a result, all stakeholders and associated impact need to be identified and managed through a Stakeholder Management Strategy.

As an example: As part of your data encryption strategy, you'd like to force encrypt all outbound email messages containing sensitive data. The technology deployment is straightforward and can be done in a couple of weeks. At first glance, it is just that—"a technology deployment"—but the organizational impact that may not be factored into this effort could indeed have a high impact on your team. You will need to consider all areas, such as Legal or Compliance for review of the messaging that end users will receive to ensure your company is held harmless of any legal and/or regulatory risks. You may also want to consider your sales team, if applicable, to help you determine if the user interface to unencrypt the message is acceptable for customers. You may also need to consider your help desk or call center teams to make certain they have up-to-date information on your go-live date. You will also need to provide these teams with appropriate user guides so they can help end users who call in and need help unencrypting the messages they receive.

For the success of any effort you undertake, it's important to understand the process of how to identify all of your stakeholders and reach beyond the people and groups that are typically involved in security initiatives—those who may have an indirect impact or where the impact is currently unknown. These types of stakeholders may be a bit more difficult to identify, but they need to be factored into your Stakeholder Management Strategy.

It's equally as important to understand how to map your stakeholders' interest and influence and to drive your relationship plan so that you can get the support you need to successfully manage the deployment of your strategy and/or initiatives.



## Why We Need a Stakeholder Management Strategy (I)

- Understanding the business is not just about understanding the goals of the company
  - It's also about understanding key stakeholders, their motivations, interests, and power
- As you become more successful in your career, the initiatives you run will affect more people
  - It's likely your work will impact people who have power and influence over your projects
  - These people can support or block you

Stakeholder management has always been important, but arguably it is more important now than ever before. This is due in large part to our increasing dependency on technology and interconnectivity that's at the core of nearly all personal and business usage. It's equally as important to know that understanding the business is not just about understanding the goals of the company; it's also about understanding key stakeholders, their motivations, interests, and power.

The level of stakeholder engagement in any project will be a direct result of the Stakeholder Management Strategy. Excellent stakeholder management results in good stakeholder engagement and entails the recognition, acknowledgment, and management of stakeholder needs, concerns, wants, authority, common relationships, and interfaces, and the realization that any changes in business processes increase the impact to the organization and could potentially cause reputational risks that come from poor stakeholder relations. In this context, good stakeholder relations are a prerequisite for good risk management.

As you become more successful in your career, the initiatives you run will affect more people who have power and influence over your projects. These same people can support or block you. It's important you realize that relationship building takes time. Many of the hallmarks of a good relationship—trust, mutual respect, understanding—are intangibles that develop and evolve over time, based on individual and collective experiences and interactions.

## Why We Need a Stakeholder Management Strategy (2)

- Proactive management and engagement of key stakeholders
  - A critical success factor during the creation and implementation of your efforts
- Involving stakeholders early helps positively shape the project, which can help with:
  - Higher quality
  - Additional resources
  - Capability to avoid roadblocks

Proactive management and engagement of key stakeholders during the creation and throughout the implementation of your efforts are crucial. Often, stakeholders are engaged right before go-live, and at this point, you have little to no time to consider what needs to be done to gain support and/or reduce opposition to your efforts.

In Paul Nutt's *Why Decisions Fail*, he conducted an analysis of 400 strategic decisions and found that half of these decisions failed—that is, they were not implemented, only partially implemented, or otherwise produced poor results—in large part because decision makers failed to attend to the interest and information held by key stakeholders.

A Stakeholders Management Strategy provides a mechanism to socialize vital information with your stakeholders and those people and/or groups that influence them. It will also give you the opportunity to address important areas such as what type of information your stakeholders need to make a better decision and how you can best address questions and mitigate concerns that will ultimately help in avoiding roadblocks.

Involving stakeholders early enables you to positively shape your project with higher-quality results and possibly gain additional resources in support of your effort.

Some stakeholders are more obvious than others, and some stakeholders are more challenging to win over. Your Stakeholder Management Strategy will help you identify key people you have to win over in support of your efforts from either a financial standpoint or resource allocation, assist you in influencing other stakeholders, or simply provide support and buy-in for your efforts.

Considering the specific interests your stakeholders may have with your initiatives will help you prioritize. You will also need to consider the benefits your stakeholders might anticipate, plus activities that might cause a sense of loss or power by your stakeholders, and those activities that could create a potential conflict. You will need to consider changes that your initiative might require from your stakeholders, such as business processes. The way they operate today will not be the same as the way they operate after your initiative is launched, and that may be problematic in the eyes of your stakeholders.

Stakeholders play an important role in making your initiative successful, and managing supportive stakeholders and potential negative responses, whether real or perceived, early on will help you develop and drive your relationship plan.

## What Are Stakeholders and Why Are They Important to Me?

- A stakeholder may be a person or a group
  - Who will affect or be affected by your work
  - Who may be internal, external, or both
  - Who can be divergent and vocal with differing expectations about outcome needs
- Stakeholders have a vested interest in your work
  - Unaddressed concerns from stakeholder may undermine your efforts
  - Buy-in is necessary for your success

The term *stakeholder* has become well-known terminology in management theory and practice over the last decade. There are many variants to the definition, but they can all be summarized as the following: Stakeholders are people or groups with a vested interest in the success of your strategy and who will affect or be affected by your team's work. In other words, anyone impacted by the project, or its outcome is a stakeholder. These people or groups may be internal or external to your organization or both, and their support, cooperation, and buy-in are necessary for you to succeed.

Stakeholder groups can be divergent and vocal with differing expectations about outcomes and the need for change. Unaddressed stakeholder concerns can undermine your efforts and result in a lack of strategy and goal buy-in.

Here is a story about a missed stakeholder opportunity:

Robert Taylor, a senior security professional who had been at his company for over five years, was given the opportunity to take the lead on a network blocking security initiative that had the potential for organization-wide visibility. Robert, or Bob as he prefers to be called, knew that this would be a great promotional opportunity in his career. After all, he was the subject matter expert in this domain and was a seasoned network security professional of over 20 years. He knew this technology inside out. Bob quickly and eagerly assembled a project team with the typical folks that he'd previously worked with on numerous other security initiatives. Everyone was on board to make this happen.

The plan progressed flawlessly. The project was on-time and on-budget, all the equipment arrived as scheduled, and network blocking was implemented four days ahead of schedule. Bob knew this would make his boss and the leaders of the organization happy. Bob was at home enjoying his success when he got an urgent call from his boss less than 24 hours after go-live. Bob's boss relayed to him that he had received several calls and emails from key people and groups within the organization, and they were complaining they didn't have access to internet sites they needed to access to get their job done. Bob's boss also received a call from the help desk

director stating that her team had received over a hundred calls concerning end users' inability to access internet sites, and she was concerned there may be a network connectivity problem.

Bob missed the opportunity to engage all of his stakeholders. For Bob, this was a straightforward technology deployment, and he didn't think about the impact to users and how they use the internet to do their job. There could be a number of impacts in a scenario such as this. The sales team or a research and development team may need access to various sites throughout the world to access vital information for their jobs.

The help desk is the first line of defense to field end-user support questions, and Bob's effort was not on the team's radar, nor were they involved. In addition, he didn't engage Communications, a prominent stakeholder to help him get out the message regarding impact to the organization beforehand. This would have given him the opportunity to know the challenges before go-live and work through any obstacles.

It is important you and your team know who your stakeholders are and fully understand their needs and expectations. Stakeholders should be proactively included in your efforts to develop your overall strategy, as the process of overcoming stakeholder resistance after initial implementation is complex and time-consuming. It often involves trust and credibility issues that may or may not be overcome at that point.

## Stakeholder Management Key Components

- Stakeholder management is composed of three phases:
  - Phase 1: Identify stakeholders
  - Phase 2: Understand stakeholders
  - Phase 3: Manage relationships

Stakeholder Management is composed of three key phases:

- **Phase 1:** Identify stakeholders
- **Phase 2:** Understand stakeholders
- **Phase 3:** Manage relationships

We will talk about each of these phases in more detail on the subsequent slides.

- Can be a complicated process
- A single initiative can impact many people throughout your organization
- It is important to identify those who can impact or will be impacted by your strategy

Identifying stakeholders can be a complicated process. As we alluded to previously, a single security strategy or initiative, large or small, can produce numerous impacts not only to your security organization but also the overall enterprise. Because this is an important component of your strategy, you'll want to get this right by identifying all appropriate stakeholders.

To identify your stakeholders, you could hold a meeting with your team of managers and staff to brainstorm who your key stakeholders might be. You realize that with the limited resources you have, you can't possibly do everything for everyone. Your team has taken your beliefs and this assignment to heart. They have submitted numerous names and groups, and in no time at all, you have a large list with some potential problems because your team generally interacts only with the security teams and those teams outside of security that directly work with them on technology deployments. You know this will limit your influence in the organization and possibly the success of your effort. You know it's important to identify those who can impact or will be impacted by your strategy in any way.

## Example: Stakeholders

Phase I

### • Security department stakeholders

Your boss	Lines of business	Customers	Prospective customers
Senior Executives/Board	IT	Finance	Suppliers
Colleagues	Help Desk	HR	Vendors
Your team	Operations	Legal	Shareholders
Your family	Procurement	Compliance	Government
Your peers	Communications	Facilities	Regulators

Listed here are some examples of security department stakeholders. Some are obvious and would likely appear on the results of your team's stakeholder brainstorming. Less-than-obvious stakeholder examples might be:

- **Procurement:** Procurement will be responsible for negotiating pricing terms and conditions for hardware, software, and services for all of your efforts. They may also provide vendor management to ensure your vendors are performing as stated in the contract and deliver exactly what you need.
- **Finances:** The Finance team is responsible for monitoring budget and will typically require business justification or a business case before you can receive funding for your projects. Finance can be a strong ally in helping you get your business case approved through the proper channels, such as business partners and executives. Without Finance, you will likely not receive funding.
- **Facilities:** You may engage Facilities for asset tracking or the convergence of IT and physical security systems. You may also need their assistance in building out specialized rooms for security usage, such as labs, security operations centers, and/or team rooms.
- **Compliance:** Complying with government and industry regulations is a major concern for security departments because many organizations in the public and regulated industries such as utilities, finance, and health care are required to demonstrate adequate security policies are in place and prove compliance such as PCI, HIPAA, and so on. Compliance can help you interpret regulations, and often this team will lead and/or participate in audits to ensure your organization meets compliance requirements.
- **Legal Counsel:** Because regulatory compliance is part of greater information management and governance control, many organizations have started seeking the advice of legal counsel to help them make the right business decisions.



- **Human Resources:** You may need to engage Human Resources (HR) for identity and access-management-related efforts because most databases often obtain information from the employment or HR systems. After an employee is activated, he or she has access, but access is terminated when the employee is deactivated. HR will also be instrumental in interpreting employment law and employee enforcement against security policies.
- **Help Desk:** We talked about engaging the Help Desk or Call Center as part of your data encryption strategy and the roll-out of forced encryption on all outbound email containing sensitive data. Most security efforts that affect or could potentially affect users will need to partner with the Help Desk because this team is generally the first line of defense to support for end users.
- **Communications:** It's always a good idea to get this team involved to help you craft messages about your security initiatives. This team can partner with you and help you sell the value of your initiatives to your stakeholders. They are also likely to understand how to effectively distribute your messaging so that you get the highest degree of penetration throughout the organization.

- SIPOC stands for
  - (S) Suppliers
  - (I) Inputs
  - (P) Processes
  - (O) Outputs
  - (C) Customers
- SIPOC provides a template
  - For defining and mapping a process and allows for identification of end-to-end process touch points
  - Will ensure greater success in identifying all stakeholders that could be impacted or have a vested interest in your efforts

The acronym SIPOC (Suppliers, Inputs, Processes, Outputs, and Customers) is pronounced "sigh-pock." A SIPOC is a high-caliber method of showing how current processes actually work. It breaks down exactly what needs to be done and how it needs to be done. Teams use it to identify all relevant elements of a project before work begins, and it helps to visualize a complex project in a simple table format. This model is particularly useful in helping you identify stakeholders that may not have been previously visible and/or considered.

The SIPOC model can be traced to the teaching of W. Edwards Deming and his lectures to postwar Japanese business leaders in 1950. He introduced Japan and ultimately the world to the idea of systems thinking. In Deming's lectures, he used simple line flow diagrams to illustrate his ideas regarding the need for taking a systems perspective. It was that diagram that later influenced Peter R. Scholtes (a Deming protégé) to create what has become known as the SIPOC model and is now widely known and used throughout the business process community. Scholtes fully describes this in his book *The Leader's Handbook: Making Things Happen, Getting Things Done*, a guide to inspiring your people and managing the daily workflow.

For your security team, using the SIPOC template for defining and mapping a process allows for identification of end-to-end process touch points. This method will ensure greater success in identifying all stakeholders that would be affected by a proposed change and will often help you identify those that would not have been typically considered.

## SIPOC Matrix

## Phase I

- Enables you to comprehensively identify and document all stakeholders for your initiative
  - By considering Inputs, Processes, and Outputs
  - Which are provided by Suppliers to Customers

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers

A SIPOC may also be used as a collaboration tool with your stakeholders to arrive at a consensus on the process and requirements before progressing further in your strategy. It can enhance communication cross-functionally, and it helps your organization and the company as a whole better understand what you are implementing.

- **Suppliers (S)** are those people and/or groups who provide inputs; *they are regarded as stakeholders*. Please note: These are not "suppliers," as in vendors, but those who provide input into your process. They may be internal and/or external to your organization.
- **Inputs (I)** are the key requirements needed for the process to work. The inputs should represent information and/or materials the suppliers provide to you.
- **The Processes (P)** are defined series of activities. Keep this high level and simple. Ideally, this should contain between five and eight steps.
- **The Outputs (O)** are tangible results of the process steps. The outputs can be used as discussion points with customers to validate and ensure your delivery is in alignment with your customers' expectations.
- **Customers (C)** receive or use the outputs. Your customers are recipients or users of the outputs produced at every step in the process. *They are regarded as stakeholders* and may be internal and/or external to your organization.

There are some potential challenges to keep in mind: Processes may not be adequately or completely documented, and/or you may have several processes that need to be factored into your overall strategy.

If this is a challenge you are facing, remember to keep this activity high level and include between five and eight steps of the process. Documenting this process will be a team activity and should involve brainstorming to find and/or determine the hard-to-see details. Doing research on best practices and using these as your guidelines, in addition to brainstorming, will be tremendously helpful. Remember, this method is used to comprehensively identify and document all stakeholders for your initiatives.

## Step 1: Identify Key Process Steps

Phase I

- List high-level process steps
  - Which are required for your project

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
		Define requirements		
		Design		
		Procure		
		Build and Deploy		
		Manage the solution		

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

78

We will walk you through the steps to complete a SIPOC over the next few slides.

The first step in completing your SIPOC is to list high-level process steps that are required to deploy your product. As a reminder, Processes (P) are defined series of activities. Keep this description high level and simple. Ideally, it should contain between five and eight steps. In the case scenario of Office365, we have provided the following as an example:

- **Define requirements:** To successfully deploy a Software as a Service (SaaS) offering, you must have clearly defined business requirements, objectives, and timelines. You need to address the questions of how the application should be designed to run, how it will be accessed, where the users of the application are located when accessing, and whether the SaaS offering will meet your company's scalability needs.
- **Design:** You will need to design the solution with a clear understanding of the application and the service offering. The next step for the team is to ensure the design integrates with the organization's existing infrastructure. For traditional projects, this can include creating physical and logical solution designs for infrastructure components, including things like network components and connectivity; security; hardware such as system hardware; storage and backup; monitoring tools; and system management tools.
- **Procure:** After the solution has been designed, you will need to procure the solution components that meet scalability and business requirements, in addition to services to meet uptime commitments.
- **Build and Deploy:** Normally, network equipment is racked, configured, and tested in this phase. For a SaaS-based deployment of Office365, this will include configurations to the central Active Directory (AD) infrastructure, for example.
- **Manage the solution:** When your infrastructure is in place and all components are working together, ongoing success will result from diligent management. Maintenance tasks should be produced for every device in the infrastructure, and system logs should be reviewed for error and warning messages. Response scenarios are created and updated as needed.

As you can see, each process is complex by nature, but for the purposes of the SIPOC, you want to keep it high level and simple.

## Step 2: Identify the Outputs

Phase I

- For each Process step, identify the Outputs

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
		Define requirements	Use cases Project plans	
		Design	Technical architecture Technical reqs	
		Procure	Executed contracts	
		Build and Deploy	Migration plan Running system	
		Manage the solution	Maintenance plan	

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

80

As a reminder, the Outputs (O) are tangible results of the process steps. The outputs can be used as discussion points with customers to validate and ensure your delivery is in alignment with your customers' expectations.

The output to the process step "Define requirements" is generally use cases and project plans. A use case is a list of steps that describe the interactions between a role/actor and a system and how it will work to achieve a goal—more specifically, your stakeholders' goals. Use cases are an important requirement technique widely used in modern software engineering since their formal introduction by Ivar Jacobson in 1992 through his book *Object-Oriented Software Engineering: A Use Case Driven Approach*. You can read more about it by visiting his website at <http://www.ivarjacobson.com/default.aspx>. A project plan is used to document project scope, schedules, and tasks. Among other things, a project plan can be used to facilitate communication with your stakeholders. Project Management Institute (PMI) is a globally recognized organization that has a wealth of information on project management expertise, resources, and so on. You can read more about this organization at [pmi.org](http://pmi.org).

The output to the process step "Design" is the technical architecture that defines and specifies the interfaces, parameters, and protocols used by product architecture and system architecture layers. The output also includes the technical requirements, which are a set of statements that identify a system's functions, characteristics, and/or constraints. These outputs are generated from physical and logical solution designs to accommodate scalable architecture for hosting the SaaS platform and are based on the applications.

The output to the process step "Procure" is an executed contract(s) signed by all parties that includes various components stipulating what products and/or services you require to meet your commitments. The terms and conditions of the contract will specify scalability and business requirements for uptime commitments and include various terms and conditions for hardware, software, and service specifications, and legal terms and conditions to protect your company.

The output to the process step "Build and Deploy" is the Migration plan, which maps existing capabilities to a new infrastructure; it is also the process by which you will assess the current state and architected state of your infrastructure. It will address how it will happen for tasks such as moving information and/or functionality and

consolidating information and/or functionality. Your company's technology and information life cycles need to be factored into this plan. The other output for this process step is a "Running system." Obviously, many additional steps need to occur between the Migration plan and deploying a running system, such as QA and User Acceptance testing.

The output to the process step "Manage the solution" is a documented Maintenance plan that includes maintenance schedules, system logs that can be reviewed and completed, and response scenarios that can be tested and updated as necessary.

## Step 3: Identify the Customers

Phase I

- Identify the Customers that will receive the Outputs

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
		Define requirements	Use cases Project plans	Business owner Technical teams Project managers Finance, Comms
		Design	Technical architecture Technical reqs	Engineering team Security team Operations team
		Procure	Executed contracts	Business owner Legal and Vendor
		Build and Deploy	Migration plan Running system	Business owner Technical teams Vendor, Leadership Help Desk
		Manage the solution	Maintenance plan	Business owner Leadership

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

82

As a reminder, Customers (C) receive or use the outputs. Your customers are recipients or users of the outputs produced at every step in the process. They are *regarded as stakeholders* and may be internal and/or external to your organization.

The customers that will receive the outputs of the use cases and project plans will be the following: The business owners, who will need to sign off on the use cases to ensure requirements are met; technical teams that will be building, deploying, and running your SaaS; project managers; and Finance. Please note: Finance may be interested in only some aspects of both of these outputs and generally for purposes of helping to build your business case. You will also want to engage the Communications team at this point to begin building your communication plan to adequately socialize with your stakeholders as your effort progresses.

The customers that will receive the outputs of the technical architecture and technical requirements are the Engineering team, which is accountable for the build function; the Security team; and the Operations team, which is responsible for the overall deployment effort.

The customers that will receive the outputs of the executed contract will be the business owners, who will keep records and manage the contract; the Legal team, which generally will maintain original contracts on file; and the vendors with whom the contract is signed, who will need a copy of the fully executed agreement.

The customers that will receive the outputs of the migration plan and a running system will be the business owners, who will be receiving the benefit of the SaaS; and technical teams and vendors, because they are responsible for migration. Leadership will need to be advised of your migration plan and when the system is fully deployed, and you will want to communicate success stories. You will also want to get the Help Desk team involved and provide them with any artifacts and/or training they will need to support end users.

The customers that will receive the maintenance plan output will be business owners and leaders such as the CEO, CFO, CIO, and CISO. Performance metrics to track progress against the maintenance plan will also be included.



## Step 4: Identify the Inputs

Phase I

- Identify the required Inputs for each Process step

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
	Requirements	Define requirements	Business case Use cases Project plans	Business owner Technical teams Project managers Finance, Comms
	Approved use cases Approved project plans	Design	Technical architecture Technical reqs	Engineering team Security team Operations team
	SLAs, Budget, HW & SW reqs	Procure	Executed contracts	Business owner Legal and Vendor
	Technical reqs System configuration	Build and Deploy	Migration plan Running system	Business owner Technical teams Vendor, Leadership Help Desk
	SLAs Business uptime reqs	Manage the solution	Maintenance plan	Business owner Leadership

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

83

As a reminder, Inputs (I) are the key requirements needed for the process to work. The inputs should represent information and/or materials the suppliers provide to you.

For the process step "Define Requirements," the supplier must provide you with requirements as inputs. Requirements are a statement or a list of statements that a product or service must do or a quality it must have. You may have multiple types of requirements, including but not limited to business, security, legal, and/or regulatory.

For the process step "Design," the supplier must provide you with the approved use cases and approved project plans as inputs. These items as inputs will ensure everyone is on the same page and expectations are in alignment.

For the process step "Procure," the supplier must provide you with desired Service Level Agreements (SLAs), budget information, and hardware and software requirements. The contract must include numerous terms and conditions to be in compliance with your organization and groups, such as security that may have the right to audit and test security controls in a vendor environment, and legal terms and conditions such as the right to terminate agreement with or without cause, and remediation terms if a vendor is found in default of agreement and procurement, which may include payment and receiving terms.

For the process step "Build and Deploy," the supplier must provide you with technical requirements and system configuration parameters.

For the process step "Manage the solution," the supplier must provide you with the desired SLAs and business uptime requirements so you can build these expectations into the maintenance plan.

## Step 5: Identify the Suppliers

Phase I

### • Identify the Suppliers of the Inputs

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
Business owner, Legal, Security, Regulators	Requirements	Define requirements	Business case Use cases Project plans	Business owner Technical teams Project managers Finance, Comms
Business Operations team	Approved use cases Approved project plans	Design	Technical architecture Technical reqs	Engineering team Security team Operations team
Business owner, Legal, Security, Vendors	SLAs, Budget HW & SW reqs	Procure	Executed contracts	Business owner Legal and Vendor
Vendors, Architects, Engineers	Technical reqs System configuration	Build and Deploy	Migration plan Running system	Business owner Technical teams Vendor, Leadership Help Desk
Technical teams, Vendors	SLAs Business uptime reqs	Manage the solution	Maintenance plan	Business owner Leadership

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

84

As a reminder, Suppliers (S) are those people and/or groups who provide inputs; *they are regarded as Stakeholders*. Please note: These are not "suppliers" as in vendors, but those who provide input into your process, and they may be internal and/or external to your organization.

Suppliers to the process step "Define requirements" are generally the business owner and Legal, Security, and Regulators who will provide their requirements. Regulators will often be a big influence in what can and cannot be done and/or what controls need to be considered, especially in heavily regulated environments such as Finance, Health Care, Transportation, Power, and so on.

Suppliers to the process step "Design" are generally the business and Operations team, which will provide approved use cases and approved project plans. Teams often go wrong and projects fail when considering the business for input. The product and/or services have to meet business expectations, so it's imperative they are factored into this process step. This step is necessary to ensure that all parties approved, and by doing this, you will ensure that what is delivered is what was agreed to.

Suppliers to the process step "Procure" are generally the business owner, Legal and Security departments, vendors, and the technical teams, which will provide SLAs, budget, hardware, and software requirements.

Suppliers to the process step "Build and Deploy" are generally vendors, architects, and engineers, who deliver technical requirements and system configuration inputs to the process.

Suppliers to the process step "Manage Solutions" are generally the technical teams and vendors, who will provide the SLAs and business requirement uptimes as input to this process.

## Stakeholder Identification Complete

Phase I

- These stakeholders will need to be managed throughout your project

(S) Suppliers	(I) Inputs	(P) Processes	(O) Outputs	(C) Customers
Business owner, Legal, Security, Regulators	Requirements	Define requirements	Business case Use cases Project plans	Business owner Technical teams Project managers Finance, Comms
Business Operations team	Approved use cases Approved project plans	Design	Technical architecture Technical reqs	Engineering team Security team Operations team
Business owner, Legal, Security, Vendors	SLAs, Budget HW & SW reqs	Procure	Executed contracts	Business owner Legal and Vendor
Vendors, Architects, Engineers	Technical reqs System configuration	Build and Deploy	Migration plan Running system	Business owner Technical teams Vendor, Leadership Help Desk
Technical teams, Vendors	SLAs Business uptime reqs	Manage the solution	Maintenance plan	Business owner Leadership

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

85

Now that we have the SIPOC completed for the CIO-sponsored Office365 migration effort, you can see that key stakeholders have been identified in the (S) Suppliers and the (C) Customers columns.

Many of these stakeholders reach well beyond those people and/or groups that would typically be considered for a standard technology deployment. By using the SIPOC template for identification of end-to-end process touch points, you have greater visibility into the overall impact your efforts will have on the organization. By having greater visibility, you will be better positioned to proactively address your stakeholders' motivations and concerns, which we will discuss in more detail in the upcoming slides.

- Stakeholders are both organizations and people
  - Identify the specific individuals within each group
  - They may have different views of your project
  - So, you need to tailor your approach
- Follow a three-step process to manage stakeholders:
  - Understand motivations
  - Map power and interest
  - Prioritize relationships

Now that you have identified your stakeholders, and you know that stakeholders are both organizations and people, you need to understand their motivations. A mistake that teams often make is ignoring the motivations of their stakeholders or making assumptions about what we believe their motives are. It is more than likely your stakeholders will have a different view of your project than you do.

Let's think for a moment about the stakeholders identified in the Office365 migration effort. How would motives vary between business owners, Legal, Security, Regulators, the Operations team, vendors, technical teams, architects, engineers, project managers, help desk, communication team, and leadership?

It is highly likely that your stakeholders will have different views of your project. In addition, office politics and/or personal interests will likely be key factors in distilling true stakeholder motivation; therefore, the approach for each group and/or individual will need to be tailored to support the varying motivations of each of your stakeholders because they can and will affect your efforts. Many of them will have the power to veto your project. Some of your stakeholders will voice their opinions, and as you well know, some people have very strong voices in an organization, so your project may be delayed and/or derailed.

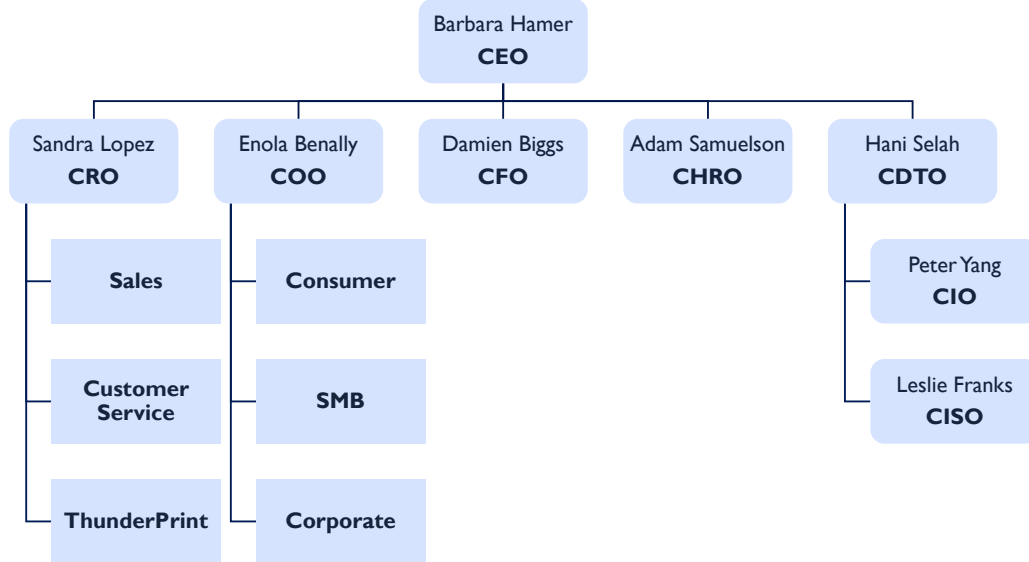
- Meet with them and others who know them to understand:
  - What motivates them?
  - What do they want from you?
  - What interest do they have in your work?
  - What can you provide to them?
  - Whom do they trust? Who advises them?

Step 1 is about understanding stakeholders, and there's no better or faster way to understand stakeholders than by meeting with them and with others who know them. Meeting directly with your stakeholders or the people who know them will help you better understand what motivates them, what they want and need from you, and what interest they have in your work. This step is critically important to understanding and avoiding mishaps and misunderstandings as your projects progress.

Knowing whom your stakeholders trust and who advises them is simply a smart, strategic approach you should leverage to better understand your stakeholders. Let's look further at the case management example that we've been discussing related to the Legal and Finance department's perceptions of the security team's attempt to deploy a new case management system. If security had identified these two groups as key stakeholders and put some effort into understanding whom these groups trust and who advises them, a veto could have been avoided. For example, security may have been able to determine that the Procurement team had great influence into both of the Legal and Finance teams. When you further uncover information, you may determine that Procurement has been working with Legal for some time on a cost-saving strategy for the organization, which is their particular motive, and the team has been advising Legal to consider outsourcing these services. And, Procurement generally partners well with Finance because both teams have the same motives of saving money.

Knowing whom your stakeholders trust and who is advising them will give you an advantage and the opportunity to work with the influencers to develop a win-win situation for the organization. In the preceding scenario, security could have formed an alliance with Procurement to understand competitive pricing models and best-in-class technologies and services, and Procurement may have been an ally in selling the effort to Legal and Finance.

## Thunderbolt Org Chart



So far you have been introduced to the key stakeholders at Thunderbolt and the overall corporate structure. The org chart above summarizes the key players for your reference.

Chief Executive Office (CEO): Barbara Hamer  
 Chief Revenue Office (CRO): Sandra Lopez  
 Chief Operating Officer (COO): Enola Benally  
 Chief Financial Officer (CFO): Damien Biggs  
 Chief Human Resources Officer (CHRO): Adam Samuelson  
 Chief Digital and Technology Officer (CDTO): Hani Selah  
 Chief Information Officer (CIO): Peter Yang  
 Chief Information Security Officer (CISO): Leslie Franks

Business operations are divided into Consumer, Small & Medium Business (SMB), and Corporate divisions. While ThunderPrint is technically a consumer-focused division, it reports to the CRO for historical reasons along with Sales and Customer Service.

An org chart can be one important indicator of what a company deems to be important. For example, it's clear that revenue and operations are business critical areas for achieving Thunderbolt's mission of helping customers get what they need when they need it.

## Step 2: Mapping Power and Interest

### Phase 2

- Full understanding of stakeholder power and interest can be achieved through stakeholder mapping
- Stakeholders have
  - Three levels of power:
    - Those with a “veto”
    - Those with a “vote”
    - Those with a “voice”
  - Three levels of interest:
    - High
    - Medium
    - Low

Step 2 is about mapping your stakeholders' power and interests. We briefly touched on this point in previous slides: The power to "veto" and the power of stakeholders' "voice." Stakeholders also have the power to "vote." Understanding how your stakeholders will want to exert their power will help you minimize and manage issues that are traditional barriers to change.

Stakeholders also have three levels of interest that are important to you. They will have a high, medium, or low level of interest in your project. Understanding this will help you determine how you will need to manage each of your stakeholders and the various views each of them hold regarding your project. You can then tailor your approach to win their support.

## Step 2: Mapping Power and Interest Example

### Phase 2

- Each stakeholder may have different views on your project
- It's important to tailor your approach

Stakeholder	Power	Interest	Views/Interest in project
CDTO/ CIO	Veto	High	Innovation, productivity, attracting top talent
CFO	Veto	Medium	Costs, business risk
CRO / COO	Veto	Low	Business growth, continuity, and operations
CISO	Vote	High	Security, risk, compliance
CHRO	Vote	Medium	Recruiting, retention, development, reskilling
Developers	Voice	High	Working with new technologies, transferable skills

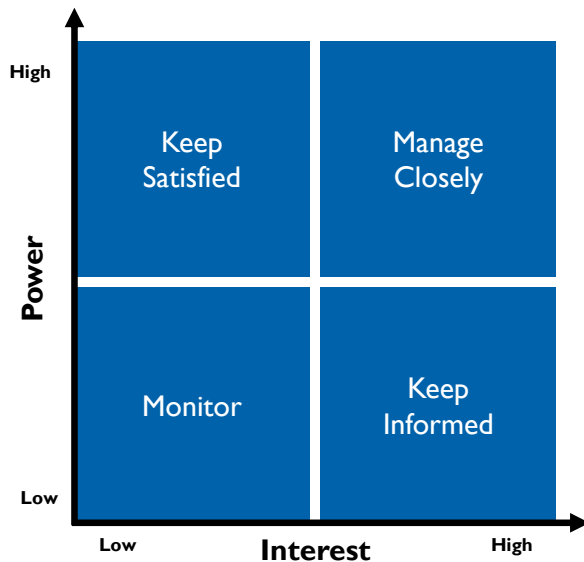
Continuing in Step 2, we provide an example to map power and interest. The varying degrees of power and interest become evident by capturing the information in a grid such as this. By listing additional details in the "Views/Interest in project" column, you can clearly see the need to tailor your approach and degrees of information for each of your various stakeholders.

You wouldn't want to take the same approach at soliciting buy-in and support from someone with veto power and high interest as you would with low/medium interest. Likewise, you wouldn't want to take cost and risk information that you would typically provide to the CFO to the head of HR, whose interests lie in the impact on employee policies. And, you wouldn't want to take the same information to the end users that you would take to legal, whose interests lie in the impact of laws, terms, and conditions of contracts.



### Step 3: Prioritize Stakeholders

Phase 2



- Power/Interest Grid
- Used to prioritize stakeholders

From mindtools.com

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

91

In Step 3, we prioritize stakeholders.

As we've seen in previous slides, the list of people and/or groups affected by your work is long and, over the course of your project, may grow substantially. Prioritizing your stakeholders will help you appropriately and effectively manage them. You can use this 4x4 power/interest grid to help yourself prioritize and see how you can most effectively influence your stakeholders.

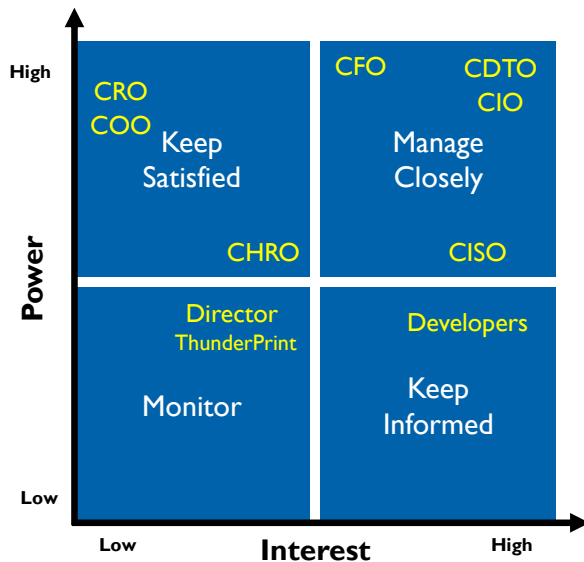
- **High power, interested people:** These are the people you must fully engage and make the greatest efforts to satisfy.
- **High power, less interested people:** Put enough work in with these people to keep them satisfied, but not so much that they become bored with your message.
- **Low power, interested people:** Keep these people adequately informed and talk to them to ensure that no major issues are arising. These people can often be very helpful with the details of your project.
- **Low power, less interested people:** Again, monitor these people, but do not bore them with excessive communication.

For more information on this tool, and to use an interactive screen app, please visit:

[https://www.mindtools.com/pages/article/newPPM\\_07.htm](https://www.mindtools.com/pages/article/newPPM_07.htm)

## Step 3: Prioritization Example

Phase 2



### • Power/Interest Grid

From mindtools.com

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

92

On this slide, we've prioritized our stakeholders based on what we know so far about our stakeholders at Thunderbolt.

In the upper-right quadrant, you can see that we need to manage the CDTO, CIO, and CFO closely. They hold a lot of power within the organization and have vested interest in seeing the cloud migration succeed.

In the upper-left quadrant, you can see that we must keep the CRO, COO, and CHRO satisfied. We must be fully engaged with them to ensure that they don't become dissatisfied with how cloud and security are impacting their operations or perceived to be impacting their operations.

In the bottom-right quadrant, we need to keep our developers adequately informed. They are most directly impacted on a day-to-day basis by cloud security policies and have a vested interest in leveraging leading technologies. As a result, we need to maintain open lines of communication and partner with them to ensure they don't see security as a blocker.

In the bottom-left quadrant, we need to monitor the ThunderPrint team. Specifically, the Director has been deploying to the cloud for years and doesn't see why the organization needs to take it slow. This quadrant usually requires the least amount of effort, but we must continue to monitor these stakeholders in case they require our attention.

- Develop a relationship plan to
  - Proactively manage relationships
  - Answer these questions about your stakeholders:
    - How do they view your work?
    - How can you win their support or manage their opposition?
    - How do they want to receive information from you?
    - What can you provide to them?
      - What's their preferred method of getting information?
    - Whom do they trust? Who advises them?

Managing relationships is critical to the success of every project in every organization, so developing a relationship plan can help you proactively manage your relationships and put you at a strategic advantage. There are several factors that need to be thought through as we've discussed, such as how stakeholders view your work. As an example, if your stakeholder is Finance, the team may view your work as a never-ending request for more funding, and your end users may view your work as an impediment and just another change that makes life more difficult.

You also want to think through ideas on how you can win support or manage opposition to change, and how your stakeholders want to receive information from you. Some people like in-person meetings, some people like formal presentations with a lot of details and numbers, whereas others want summary information and the assurance that you've done your due diligence. Some people like weekly reports, and others just want to know when a problem occurs or your project is in jeopardy.

You need to know how, what, and when to engage your stakeholders and the optimal method of delivery to ensure your greatest chances of success in managing change.

## Lab 1.2: Relationship Management

Estimated Time: 20 Minutes

- Goal of this exercise
  - Understand how to engage larger stakeholder groups when rolling out a new security initiative
- On your own
  - Take 10 minutes to read the case study below

### READ

Read the 2 pages of the case study below

It takes approximately 10 minutes to read the case



### Thunderbolt Stakeholder Feedback

Selah (CDTO) began the process of conducting a cloud migration assessment through a series of surveys and focus groups. He knew from experience that understanding the culture and gaining buy-in of key players across the value chain is critical to the success of any change management strategy. Results of these efforts revealed varying appetites for cloud computing with most reactions firmly rooted in previous experience with security issues, cloud technology headlines, and company culture.

Unsurprisingly, Franks (CISO) and most of her team had strong reservations about moving to the cloud. In one of the interviews, Franks stated,

*"Security is never at the front of anyone's mind...until it fails. I am seen as the naysayer of Thunderbolt, but it is my job to make sure our customer and business data is secure. Yes, these big cloud companies have great reputations now, but that also means they have giant targets on their backs. If we do this, we need to do it slowly, and I want final say on the backup/recovery plan in case of an attack. I also don't want us to use only one cloud provider. We need to diversify the risk and make sure one of these big companies doesn't hold our data hostage."*

Anonymous survey responses revealed hesitation and even fear from team members currently operating and managing Thunderbolt's thousands of servers. One respondent stated,

*"I have been with this company for 20+ years. What happens to me when my job is outsourced? Where is that amazing familial culture everyone talks about?"*

Another focused on the increased value of customer intelligence data and the associated risk:

*"I am certain a hacker could make good money holding our Bolt system hostage, but the real risk is how much our customer intelligence is worth these days. Hermes holds loads of PII and many other things that would fetch a good price. I appreciate the steps cloud companies take to protect data, but it only takes one breach to wreak havoc."*

Yang (CIO) and the IT Department communicated a nearly opposite view. Yang stated,

*“Cloud migration is essential for my department. Right now, managing and maintaining data and servers takes up at least 25% of my team’s time. The more tenured group is resistant to it, I think because they fear for their jobs. But the newer developers are churning out quickly because they don’t want to work on legacy systems. Just last week, we lost a developer who had a great idea for an app that would improve the ability to read customer handwriting, but it was blocked by the security team because it was cloud based. Not only was it demoralizing, but this was something that could have really helped our retail staff. We shouldn’t use valuable resources for basic tasks like data storage and server maintenance. We need to move to the cloud, retrain tenured folks, and spend time on things that drive revenue and profit for the business.”*

A senior manager on Yang’s team added,

*“I get the fear of putting all our eggs in one basket and that these big providers have targets on their backs. But looking at it a different way, they are so much more focused on security than we could ever be. They know the consequences of security breaches to their reputations and income streams. They have some of the best security people on the planet keeping their clients’ data safe. I think we’re more vulnerable if we don’t store data in the cloud.”*

Survey responses indicated that many on the team were ready to leave if not given “cooler” work to do. One developer summarized,

*“I was proud to support Thunderbolt and its customers during the pandemic, but I’m tired. I need more space to think and develop things that actually matter. We need more resources, and if that doesn’t change soon, I’m moving on.”*

Even the neutral party, the HR team saw both sides. Samuelson (CHRO) commented,

*“While I understand and support the cloud migration, we cannot lose sight of how our people respond to this change. There are senior people whose jobs will no longer be relevant. Yes, we need to retrain them, but if they decide to leave, we will have a big gap of company knowledge to fill. Right now, it takes at least three months to hire someone, and they are not effective for another six months at a minimum. I do think this migration will slow attrition if we can redirect work to more of what team members want to do. It’s not just about getting the top people on board; we need to carefully consider how to bring people along across all ranks of the organization.”*

One hiring manager added,

*“It takes two weeks or less for someone to walk out the door, but it takes almost a year to effectively replace them. You don’t have to be great at math to see the negative consequences of lots of people leaving at once.”*

Both the Sales and Operations teams reacted with a hands-off approach—so long as their departments and teams are not impacted. Lopez [CRO] commented,

*“I realize I’m supposed to have an opinion on this, but if my team isn’t impacted, I really don’t care either way. That said, when we went from Lotus Notes to Outlook several years ago, email was unexpectedly down for almost three days. It really hurt our operations and our relationships to key customers. So, if we do go to the cloud, I want to make sure the plan doesn’t put my sales and relationship management teams at risk of a technology outage. No matter who is responsible for a tech issue, my sales team gets a call about it.”*

When asked for the operations perspective, Benally (COO) backed up her long-time colleague.

*“On this question, I defer to Sandra [CRO]. Sales and operations will face the most pressure if the deployment causes issues or downtime. I need my team to be able to operate effectively without losing hours and minutes we simply do not have. That email outage several years ago was only a few days, but it took us months to catch back up. I am primarily concerned with our homegrown systems, Bolt & Hermes. Cloud providers likely have experience with off-the-shelf data from Salesforce or Oracle, but who knows what it will take to make sure the data is safe and useful for a unique system? Obviously, Peter and Leslie would know more about the specifics, but I have heard that homegrown systems are harder to migrate than off-the-shelf systems.”*

Dasika (Director, ThunderPrint) highlighted an example of the benefits of data in the cloud. Openly sharing his frustration, he stated,

*"I realize there's a lot of fear when it comes to letting go of data control. But cloud storage has come a long way, and there are so many advantages, especially freeing up resources to focus on actual business issues."*

Team members backed up his view. One stated,

*"I really don't know what the big deal is. We've been operating Plinky and then ThunderPrint in the cloud for almost ten years, four of which are after the merger. The sky has not fallen. Yes, I read the headlines, but headlines aren't always reality."*

And within the finance department, Biggs (CFO) sided with the status quo:

*"Any time we move information or change technology direction, we open ourselves up to risk. I see headlines almost daily about security breaches and data leakages. I've even heard that short sellers target companies undergoing major transformation like this one. Oracle with PeopleSoft has performed just fine off the cloud; I don't know why we want to fix something that isn't broken. And by the way, how much will this really cost? Every cloud firm touts savings, but what I hear in the CFO community doesn't match that. A cloud provider always starts with a low price and then ratchets it up once they have your data."*

His team, however, had a different perspective. Many noted features and functionality available on cloud versions of Oracle with PeopleSoft as well as the pain of software upgrades. One financial analyst noted,

*"In my previous job, I could do a lot more a lot faster with Oracle. When I came here, many of the features I used didn't exist in the local version, and I had to relearn everything. I still think there are ways I can be more efficient with my job if I had the version I used to use. And every time there is an update, it is such a process! Whenever there was an update to the cloud version, I barely noticed it. But now, I have to plan for the system potentially being down for several hours. I get that they do it on the weekends, but I often use that time to catch up."*

## Lab 1.2: Relationship Management Group Discussion

- **Group Discussion**

- What are the CIO's concerns and how can you get his buy-in to implement security controls?
- What can you do to get developers to understand the importance of security?
- What are the CFO's concerns and how can you get him more comfortable with the cloud?

- **Prepare your thoughts for a class debrief**

- Write down your key points

### NOTE

Don't read the next section

It contains a debrief and potential lab answers



After you have finished reading the case answer the questions below:

**1) What are the CIO's concerns and how can you get his buy-in to implement security controls?**

**2) What can you do to get developers to understand the importance of security?**

**3) What are the CFO's concerns and how can you get him more comfortable with the cloud?**

---

## Lab Debrief

---

*Note that this section contains a debrief  
and potential lab answers*

This page intentionally left blank.



## Thunderbolt Stakeholder Management

Stakeholder	Motivation	Concerns with Cloud	What to provide to mitigate concerns
CDTO / CIO	Innovation	Security and compliance risks	Cloud strategy with risk-based controls
CFO	Cost savings Risk mgt	Actually saving money Effectively using org resources	Detailed business case showing cost savings and rollout plan
CRO / COO	Revenue Continuity	Potential disruption to business operations	Business continuity and resiliency plans Understanding of key business processes
CHRO	Talent management	Change management Cloud upskilling	Training for team members to take other roles in the organization
Developers	Technology	Not doing the "right" thing from a technical perspective	Inclusion from the start in design and architecture decisions Sessions to show cloud security support and expertise

Let's understand what might be driving our key stakeholders. You might have encountered similar situations and personalities in your career. Based on the motivations of each of these stakeholders, the slide above summarizes their concerns and identifies actions that you can take to mitigate these concerns. Use this an example to analyze and manage your relationships.

### CDTO and CIO

Hani and Peter were brought in with a mandate to provide technology innovation to better enable the business. As it relates to security, they want to make sure there is a plan in place to mitigate any potential issues but it's not a matter of whether or not the company will move to the cloud, it's a matter of how. As a result, their focus on innovation is driving the path forward and the CISO will have to get on board or be left behind.

### CFO

Damien is a trusted advisor to the CEO and, as a result, is involved in all key strategic decisions for the organization. Like others on the senior leadership team, he is laser-focused on Thunderbolt's strategic objectives and reviews new initiatives to make sure they are achievable and will be an effective use of the organization's limited resources. As a result, he wants to know if moving to the cloud will actually save the company money and if how corresponding risk can be mitigated.

### CRO and COO

Both Sandra and Enola are focused on running the business. They don't specifically care what technologies may be in use as long as there is not disruption to the business operations and customer needs. As a result, security can show partnership by developing a deeper understanding of key business processes and ensuring associated business continuity and resiliency plans are in place.

### CHRO

Adam has seen large technology shifts impact the workforce before and he knows how disruptive it can be. As a result, he's most concerned about upskilling the existing workforce given Thunderbolt's familial culture and desire to do the right thing for their employees. Part of the change management plan can include training options

for team members to take on other responsibilities related to cloud administration, support, or other work.

**Developers**

The IT and development teams are most concerned with their ability to use modern technologies and taking the appropriate technology direction. Security can partner with this influential group by including them in design and architecture decisions from the start and providing dedicated cloud security support.

## Managing and Leading Change

- Stakeholder management is critical to the success of your work
  - May be a person or groups who will be affected by your initiatives
- Prioritize stakeholders based on Power and Interest
- Provide value
  - Be in tune with the motivations of your stakeholders
- Schedule recurring meetings with stakeholder groups
  - Staff
  - Senior leadership
  - Skip levels (up and down)

In summary, stakeholder management is critical to the success of your work. The level of stakeholder engagement will be a direct result of your Stakeholder Management Strategy. Even simple technology deployments can yield a variety of stakeholders with various levels of power, interests, and influence, and the methods by which you identify, prioritize, and manage your relationships may be the differentiating factor between success and failure. Excellent stakeholder management results in good stakeholder engagement and good stakeholder relations are a prerequisite for good risk management.

A stakeholder may be a person or group who will be affected by your initiative, and stakeholder groups can be divergent with differing expectations about outcomes and the need for change. By understanding who stakeholders are and what they need, you can proactively provide the information they require. This can often diffuse opposition and, in the end, help you navigate your stakeholders through the change cycle.

Even with a thorough understanding of the benefits and buy-in from key stakeholders, implementing a broad initiative like cloud migration can still be very difficult. Some people in the organization might even resist the change entirely. For example, some of your security staff may have a more traditional approach to security and be reluctant participants in moving to the cloud.

As a result, it is extremely important to engage stakeholders regularly throughout the process of developing and implementing a new initiative. Get employee feedback by conducting surveys and interviews as we saw with the various quotes from Thunderbolt employees. Understand their concerns and see what options you have for mitigating those concerns.

# 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 I

- Overview
  - Need for Strategic Planning
  - 30-60-90 Day Plan
    - Lab #1: CISO First Impression
- Decipher the Business
  - Historical Analysis
  - Values and Culture
  - Stakeholder Management
    - Lab #2: Relationship Management
- **Asset Analysis**
  - Business Strategy
    - Lab #3: Strategy Map
- Decipher the Threats
  - Threat Actors
  - PEST Analysis
  - Threat Analysis

This page intentionally left blank.

## Goals of This Section

- Discuss different types of assets
  - What is most valuable to your organization?
    - What is most critical to the mission?
  - What is most valuable to the attacker?
    - What does the attacker want to accomplish?

A key first step of any security program is to identify your key business assets. It's no accident that the first two Critical Security Controls are conducting an inventory of authorized and unauthorized devices and software.

In this section, we will discuss different types of assets and what may be most valuable to your organization. This is informed by an understanding of what is most important to the mission and vision of the organization. By extension, if something is valuable to you, it will likely also be valuable to attackers. Depending on the attackers' motivation and what they want to accomplish, they may want to target different assets.

Reference:

<https://www.sans.org/critical-security-controls/>

## Tangible Assets

- Cyber action can have significant kinetic impact in the physical world
  - Must understand key physical assets of the org
- Critical infrastructure is connected to all aspects of society:
  - Power plants
  - Hospitals
  - Transportation
  - Water treatment facilities
  - Financial
  - Retail
  - Residential

As information security professionals, we are primarily focused on protecting digital assets. However, it is important to keep in mind that cyber action can have significant kinetic impact in the physical world. The Stuxnet worm is a prime example of this.<sup>[1]</sup> It was designed to attack the programmable logic controllers (PLCs) used in Iranian nuclear facilities. By changing the speeds of centrifuges used to process uranium, Stuxnet reportedly damaged one-fifth of Iran's nuclear centrifuges. Similarly, cyber attacks against Industrial Control Systems (ICS) and SCADA systems used to manage power plants could have large impacts on the physical world.

If your organization has important tangible assets such as buildings, data centers, hospitals, transportation infrastructure, water treatment facilities, or even residential centers, it is important to consider how cyber attacks could disrupt your business. As the virtual and physical worlds converge with the Internet of Things (IoT), this becomes even more relevant. It will be important to consider the security implications of such systems as IoT continues to be more widely adopted.

Additionally, incorporating alerts from physical security systems into your information security monitoring capability will help identify anomalous activities.

There are a number of reasons that information security has to stay abreast of the key tangible assets of an organization.

Reference:

[1] <https://en.wikipedia.org/wiki/Stuxnet>

## Example Intangible Assets

Examples				
Critical intellectual property			Top secret plans and formulas	
Acquisition/divestiture plans			Executive/board deliberations	
PII	PHI	PCI	SOX	ITAR
Alliance and joint venture data		Business strategy	External audit results	
Design documents	R&D results	Customer records	Pricing data	Security data
Project plans	Contracts	Accounts receivable	HR, payroll, and benefit data	
List of partners	Revenue growth	Market intelligence	Pay comparison data	

Table credit: <https://www.slideshare.net/ibmsecurity/securing-your-crown-jewels-do-you-have-what-it-takes>

Organizations have many different types of intangible assets:

- **Customer data:** Includes personally identifiable information (PII), credit cards, and contact information. This contact information can be one of the most valuable assets that an organization has. Mailing lists are still one of the most effective ways to inform customers of new products or services. Competitors would love to get access to current and potential customer lists.
- **Employee data:** Includes personal information, human resource data such as salary and benefits, and even internal email communications.
- **Intellectual property:** Includes any "creation of the mind," such as music, literature, source code, and courseware. These inventions are protected by intellectual property laws and include patents, trademarks, copyrights, and trade secrets.
- **Business proprietary information:** Includes business processes, contracts, mergers and acquisitions activity, and even general business know-how.

Reference:

<https://www.slideshare.net/ibmsecurity/securing-your-crown-jewels-do-you-have-what-it-takes>

## Most Critical Assets

- **Crown Jewels**
  - Information that is critical, unique, or irreplaceable
  - Provides a competitive and strategic advantage
  - Can be data, systems, and processes
- **Changes based on**
  - Industry
  - Business model and strategy
  - Time horizon


Given the large amounts of data that is managed, processed, and controlled by many companies, it is extremely difficult to identify what actually constitutes as the crown jewels of an organization. Crown jewels are data, systems, and even processes that are critical to an organization's competitive and strategic advantage. What resources, if lost, would be irreplaceable for an organization? By answering this question, you can start to get an idea of what you should ultimately focus on from a security and risk perspective.

It is difficult to identify crown jewels because it changes across industries and companies. A hospital might consider patient records to be their top asset. However, a pharmaceutical company, which also has patient records, might consider their top asset to be their drug research and manufacturing processes. Protected health information is still important but not necessarily their top crown jewels.

Crown jewels can also change over time. For example, sensitive financial disclosures or merger announcements are extremely confidential until the point at which they are announced.



## Crown Jewels: Example Hierarchy



Data Category	Examples				
<b>Enterprise Critical</b>	Critical intellectual property		Top secret plans and formulas		
<b>Executive</b>	Acquisition/divestiture plans		Executive/board deliberations		
<b>Regulated</b>	PII	PHI	PCI	SOX	ITAR
<b>Business Strategic</b>	Alliance and joint venture data		Business strategy	External audit results	
<b>Business Unit Critical</b>	Design documents	R&D results	Customer records	Pricing data	Security data
<b>Operational</b>	Project plans	Contracts	Accounts receivable	HR, payroll, and benefit data	
<b>Near Public</b>	List of partners	Revenue growth	Market intelligence	Pay comparison data	

Crown Jewels

Table credit: <https://www.slideshare.net/ibmsecurity/securing-your-crown-jewels-do-you-have-what-it-takes>

Crown jewels make up a relatively small percentage of the overall data footprint of an organization. This example lays out a number of categories like "Enterprise Critical" and "Executive" to notionally highlight a possible data classification. It is easy to jump to the conclusion that "Regulated" data such as PII, PHI, and PCI related information is the most important asset for an organization. Depending on the company and industry, that might actually be true. However, truly identifying an organization's crown jewels requires us to think much more deeply about our business goals.

Reference:

<https://www.slideshare.net/ibmsecurity/securing-your-crown-jewels-do-you-have-what-it-takes>

## Challenges Identifying Crown Jewels

- Why do we spend so much time and energy protecting assets that are not the crown jewels?
  - We don't know what constitutes the crown jewels
  - Compliance requirements dictate disclosure of PII, credit card data, etc. but not disclosure of intellectual property loss
  - When security is part of IT, the team tends to start with a focus on applications, databases, technology, etc.
  - Baseline security controls are not in place to protect data in general

Many security teams spend a lot of time and energy protecting assets that are not the crown jewels. Why is this the case?

Oftentimes, we don't actually know what the crown jewels are. If you asked a group of executives, they would all agree that the organization has crown jewels but they likely would not be able to come up with a common definition. Sometimes, they might say that the data in their area is the most important. That is until it becomes obvious that crown jewels will require additional monitoring, effort, and cost to secure. Then they point in another direction.

Compliance requirements dictate that loss of PII or cardholder information be disclosed to the public and the affected individuals. However, there are no regulations that dictate that loss of intellectual property must be disclosed. Disclosing loss of intellectual property can actually be a competitive detriment.

When security reports to IT, the team tends to have a focus on technology. When cataloging key assets, the conversation starts with applications, databases, and systems instead of starting with key business goals and processes.

Sometimes, the team does not even have time to protect data in general, let alone find and protect the crown jewels themselves. When an organization is struggling to achieve even a baseline level of security maturity, it can be difficult to find and secure the crown jewels.

## Tips for Identifying Crown Jewels

- Start with the business problem
- Take an enterprise-wide view
- Engage stakeholders from business units, product development, and risk along with security and IT
- Don't treat it as only a compliance exercise

To identify your crown jewels, start with the business problem, not the technology problem. This requires taking an enterprise-level view by engaging stakeholders from various business units, product development, and risk along with security and IT. Think about the organization's vision/mission, business strategy, and macro forces that can get in the way of achieving business goals. And remember not to treat this as just a compliance exercise. It is commonly stated that compliance does not equate to security. In most organizations, compliance is not the ultimate goal. Providing value to stakeholders is the ultimate goal. Identifying that business problem and how your organization provides the corresponding business solution will help you identify the crown jewels.

## Identify Crown Jewels Discussion

	Crown Jewels	Attacker Goal / Motivation
Financial Services		
Retail		
Government		
Technology		
Your Org / Industry		

Use this worksheet to write down the crown jewels and attacker goals/motivations for the financial services, retail, government, technology industries, and your own organization/industry.

## Identify Crown Jewels – Example

	Crown Jewels	Attacker Goal / Motivation
<b>Financial Services</b>	Funds transfer processes Mergers and acquisitions database	Fraudulent funds transfers Corporate espionage
<b>Retail</b>	Customer and cardholder data (PII & PCI) Supply chain processes	Financial gain Espionage and competitive advantage
<b>Government</b>	Military intelligence Foreign policy and defense network data	Influence diplomatic negotiations and territorial disputes
<b>Technology</b>	Software and hardware design documents	Advance capabilities of competitors Outsource R&D
<b>Your Org / Industry</b>		

Financial services organizations process and manage large amounts of sensitive data. It would be easy to assume that their crown jewels are customer information and associated information such as online banking credentials that, if compromised, could lead to financial loss. And that may actually be the case for a number of financial organizations. However, it's important to identify what is unique to financial organizations. How do they make money? This might mean that the funds transfer processes and backend systems are the most important because a compromise of this system over which billions of dollars flows is the biggest asset for a company. Similarly, how does the company continue to maintain its competitive advantage? They might engage in M&A activity to broaden their portfolio. Depending on the company, this might be the organization's most important asset.

Retail companies also process and manage large amounts of sensitive data. They have been the target of a number of high-profile credit card breaches. Organized crime seeks this data for financial gain. But, that data is common to all retail companies. Is there something else that is unique to retail? This could be the unique supply chain processes and relationships that a company has to deliver just in time inventory. A disruption to this system could cause operating margin to deteriorate and profit to fall.

Governments have large amounts of sensitive information. Data about government employees and taxpayers is, of course, extremely valuable. But, even more critical and unique is information related to military intelligence, foreign policy, and defense networks. The loss of such information could have serious global effects and impact diplomatic negotiations and territorial disputes.

Technology companies have highly valuable intellectual property in the form of software and/or hardware designs. The loss of such information could advance the capabilities of competitors by effectively allowing them to outsource their R&D. As a related example, imagine a pharmaceutical company that loses its brand-new drug recipe. The criminal underground could distribute their own version of the drug and undercut the original drug maker.

What is critical, unique, and irreplaceable for your organization?

## Thunderbolt Crown Jewels

- Understanding critical business assets
  - Enables you to have meaningful conversations with business leaders
  - Creates an understanding of attacker motives
  - Helps determine how assets should be protected
- On your own
  - Take 5 minutes to read the case study below

### READ

Read the ½-page case study below

It takes approximately 5 minutes to read the case



### Thunderbolt Key Systems

Thunderbolt has two homegrown systems that run much of the business, Hermes and Bolt. Hermes interacts directly with customers and provides colorful updates to the customer as the package progresses to its destination. It gathers the information from Bolt as each package is scanned. Customers can choose to receive email or text updates, or they can enter the tracking number into Thunderbolt's website to see progress. In the past five years, Hermes has been using customer intelligence to include tailored messages with mostly positive results. For example, a delivery note to a destination in Phoenix might include a message saying, "It's hot in Phoenix—hope what you're receiving keeps you cool!" Aside from endearing notes, Hermes provides suggestions to SMB clients that help business operations. An SMB client in a small town may receive information such as, "We've seen an increased number of packages going to Florida—we may be able to help with bulk, timed shipping." Marketing and advertising rely heavily on the data provided by Hermes. While marketing content is created by an external firm, digital targeting, SEO, and other marketing technology is developed and managed in-house.

The Sales Department uses Salesforce.com for SMB and corporate clients. As a Software as a Service (SaaS) provider, all associated data is stored in the cloud. The Thunderbolt website is managed in-house by the IT Department using various applications that reside on local servers except for some cloud-based informational and marketing apps. Accounting and Talent Management is run through Oracle/PeopleSoft, and data for this system is stored locally. Email and internal communications switched from Lotus Notes to Microsoft Outlook in 2014 and then to Office 365. The first migration did not go smoothly and resulted in almost 48 hours of email outage from a Monday afternoon to a Wednesday morning. Newer team members successfully lobbied for the use of Slack (partially due to a discount from its parent company, Salesforce), which is cloud based. ThunderPrint still operates a separate technology system that allows customers to create and send documents to Thunderbolt stores. This system is 100% cloud based and is deployed in Microsoft Azure. After the acquisition, there was a suggestion from Franks and the security team to move the system to existing on-premise data centers. Their idea was rejected, and no security issues have arisen since the acquisition.

# CYBER42

## Round 1 Event #2

This page intentionally left blank.

# CYBER42

## Event #2 *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 I

- Overview
  - Need for Strategic Planning
  - 30-60-90 Day Plan
    - Lab #1: CISO First Impression
- Decipher the Business
  - Historical Analysis
  - Values and Culture
  - Stakeholder Management
    - Lab #2: Relationship Management
  - Asset Analysis
- **Business Strategy**
  - Lab #3: Strategy Map
- Decipher the Threats
  - Threat Actors
  - PEST Analysis
  - Threat Analysis

This page intentionally left blank.

## What Is a Business Model?

- **Business model**
  - Description of what your organization does
  - How you make money
  - How you deliver value at a reasonable cost
- **Example business models**
  - Direct sales
  - Franchise
  - Freemium
  - Subscription

A business model describes how your company or organization operates. It is the plan for how you will generate revenue and actually make a profit from that revenue. This is, of course, done by delivering something of value to your customers. When someone asks, "What is your business model?" he or she is really asking a combination of questions that encompass the following:

- Who are your customers?
- What problem do they have?
- How are you solving that problem?
- How will you find and retain customers?
- How do you generate revenue?
- What is your cost structure?
- What is your profit margin?

There are many ways that a business can potentially generate revenue and make a profit. One of the most straightforward ways is to simply make a product and sell it directly to customers. This approach requires you to control some sort of distribution channel. If direct sales is difficult, you could instead sell your product wholesale to distributors or retailers. Another approach may be to franchise your business model to others, similar to what many fast-food chains have done. You can also license your product for sale by others. The freemium approach can include advertising, like many social networks, or be based on paid upgrades, which is an approach taken by many mobile games. Many Software as a Server (SaaS) companies utilize a subscription approach that helps ensure a continuous source of revenue over time.

Whatever the business model may be, the point is that, as a security leader and manager, you must have some understanding of how your company actually generates revenue and makes a profit.

## Bundling Versus Unbundling

"There's only two ways I know of to make money – bundling and unbundling."

- Jim Barksdale

- Examples
  - Music album -> MP3 -> Streaming services
  - Network TV -> Cable TV -> Netflix/Apps
  - Newspapers -> Blogs -> Google/Facebook

Jim Barksdale was the CEO of Netscape Communications, the creator of the first widely popular web browser, when he found himself at the end of a very long road show as the company was taking Netscape public. Just as he was about to leave the meeting, he was asked, "How do you know that Microsoft isn't just going to bundle a web browser into their product?" To end the conversation, he replied, "Gentlemen, there's only two ways I know of to make money – bundling and unbundling" and immediately left the room.<sup>[1]</sup>

This now-famous quote not only served as a nice ending to the meeting but has also proven to be very true.

In the music industry, songs were bundled together into albums, records, and CDs. Then, along came the MP3 format, and songs were subsequently unbundled and distributed via file-sharing services like Napster and BitTorrent. This unbundling was then legitimized by Apple's iTunes music store. Now, we see songs being bundled together again in the form of streaming services like Pandora and Spotify.

In the television industry, shows were bundled together by the TV and cable companies. You could only get certain shows and channels if you subscribed to cable TV and purchased select packages. Now, we see shows being unbundled by new streaming players like Netflix and even stand-alone apps like HBO, which was previously available only as part of a cable TV package.

In terms of news articles, they were bundled together and aggregated by newspaper companies. Large national publications like the *New York Times* served as the curators of content while regional newspapers served the same role on a local scale. Because of this bundling of information, newspapers had tremendous power and reaped the corresponding financial benefits from advertisers. With the rise of the internet, effectively reducing the cost of distribution to zero, anyone with good ideas could now become a publisher. Blogs and easy access to online articles unbundled the news. This unbundling, however, created a discovery problem. How could someone searching for interesting news find it online in a vast sea of information? So, now we see news articles getting bundled by Google, which provides an easy way to search for meaningful content, and Facebook, which is often the "front door of the internet" for many people based on their personal interests and the interests of their connections. This rebundling of online content has, of course, driven large amounts of revenue for these new aggregators.

Reference:

[1] <https://hbr.org/2014/06/how-to-succeed-in-business-by-bundling-and-unbundling/>

## Unbundling Example



Source: SupplyDetermined.com

Craigslist, founded in the early days of the internet, is an online advertisement website with sections for jobs, housing, personal ads, items for sale, and more. It is one of the most successful classified advertisement websites, and its user interface remains largely unchanged from its inception. It is a good example of bundling multiple types of ads into one website.

Over time, many start-ups and entrepreneurs have tried, to varying degrees of success, to unbundle various portions of the craigslist.org website into stand-alone web or mobile applications. Venture capitalist Andrew Parker first created a graphic to illustrate how different companies have attempted to carve out niches from Craigslist.<sup>[1]</sup> Since then, David Haber has created the updated graphic shown on this slide.<sup>[2]</sup>

This graphic nicely illustrates how various portions of Craigslist have been unbundled by various other services:

- Uber and Lyft for rideshares and transportation
- Airbnb for sublets and temporary rentals
- Zillow and Trulia for real estate and apartment rentals (not shown on this slide)
- GitHub and StackExchange for software-related work
- Coursera and edX for educational lessons
- Match.com and others for online dating
- Quora for online discussion forums
- Gazelle for used cell phones
- StubHub for tickets

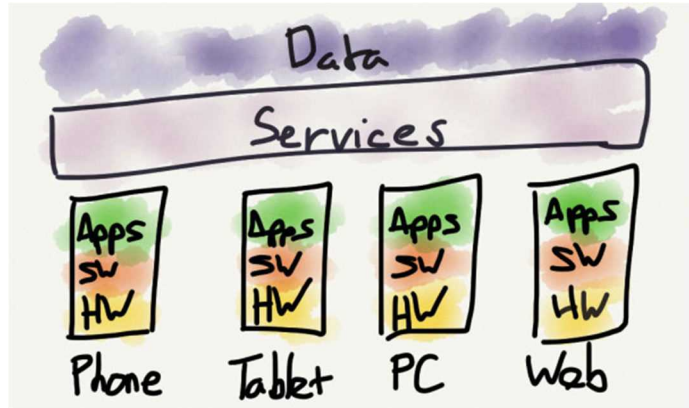
References:

[1] <http://thegongshow.tumblr.com/post/345941486/the-spawn-of-craigslist-like-most-vcs-that-focus>

[2] <http://techcrunch.com/2012/12/01/the-future-of-online-marketplaces/>

## Vertical Versus Horizontal Business Models

- Vertical business model
  - Consolidate multiple steps in the value chain
  - Example: Manufacturing, distribution, retail in one org
- Horizontal business model
  - Focus on one area in the value chain



Source: stratechery.com

It is also useful to consider whether your company employs a vertical or a horizontal business model. Vertical business models consolidate multiple steps in the value chain into one organization. For example, a shoe company may decide to integrate vertically by owning design, manufacturing, distribution channels, and retail stores to control all aspects of the business. On the other hand, a company with a horizontal business model may decide simply to focus on one layer of the value chain. For a shoe company, this may mean controlling just the design or retail distribution of shoes.

In the technology industry, Apple is a good example of a company with a vertical business model. Apple not only designs the overall device but also manufactures its own custom ARM chips, creates the operating system, and develops apps that run on the device. On the other hand, companies like Google, Facebook, and Dropbox have a horizontal business model. They provide services to customers that they want to make as broadly available across as many device types as possible. Apple wants its proprietary services, like iCloud, to run only on Apple devices (that is, vertical). Dropbox, however, wants its apps and services on as many devices as possible to ensure ubiquitous access to data (that is, horizontal).<sup>[1]</sup>

Ben Thompson of Stratechery nicely summarizes this concept: "Vertical players typically monetize through hardware, only serve a subset of users, and any services they provide are exclusive to their devices. Horizontal players, on the other hand, monetize through subscriptions or ads, and seek to serve all users across all devices."<sup>[2]</sup>

The type of business model your company uses informs a number of decisions that drive the organization's overall strategy.

### References:

[1] <https://stratechery.com/2013/the-dropbox-opportunity/>

[2] <https://stratechery.com/2013/understanding-google/>

## Business Strategy

- **Business model**
  - Describes what your company does to generate revenue and profit
- **Business strategy**
  - How you build competitive advantage
  - How you will do better than your rivals
  - Actions to implement your business model

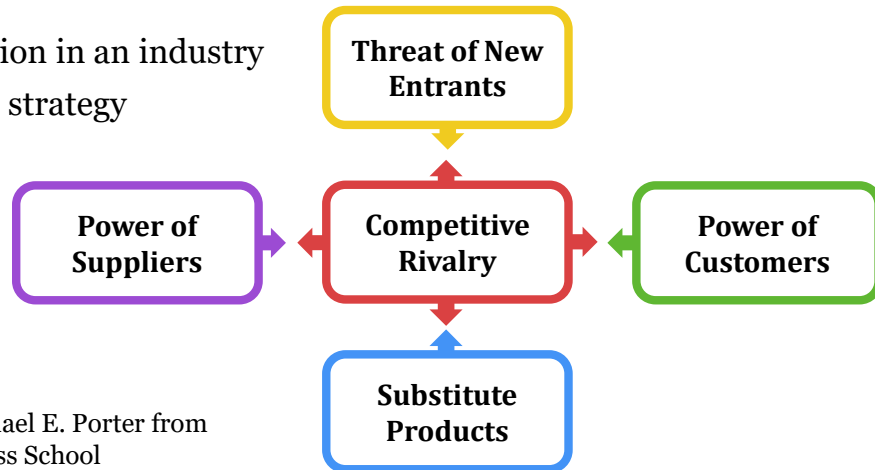
If a business model describes what your company does to generate revenue and profit, then what describes *how* your company accomplishes this feat?

Many companies have similar business models, but only some survive and thrive. Why did Microsoft dominate the PC market where other operating system vendors failed? Why did Google come to dominate search in the face of many competing search engines like Yahoo!, Bing, and countless others? Why has Facebook become the king of social networking despite the large head start that MySpace enjoyed?

Having a solid business model alone is not enough. How did organizations like the ones mentioned above build competitive advantage and do better than their rivals? This is where an understanding of business strategy, actions that can be taken to implement your business model, come into play.

## Porter's Five Forces

- Framework to
  - Analyze competition in an industry
  - Develop business strategy



Created by Michael E. Porter from  
Harvard Business School

Porter's Five Forces is a powerful method used to develop business strategy by understanding where power lies in a business situation. By looking at the internal and external pressures that exist within an industry sector, you can determine whether or not an industry is attractive and if you will have a defensible niche. It's a checklist of sorts that leads you through the identification and consideration of five forces that determine competitive intensity and, ultimately, how you can make a profit.

Porter's Five Forces also aids in the understanding of how markets may change and narrows the factors that could bring about change. A change in any of the forces normally requires a business unit to re-assess the market. The balance or net effect of these five forces determines your relative strength in the marketplace.

Porter's Five Forces was developed in 1979 by Michael E. Porter, who is a leading authority on competitive strategy and economic development. Porter has authored 18 books and numerous articles and is one of the most-cited authors in business and economics. Porter's Five Forces method has been applied to a diverse range of problems from helping businesses become more profitable to helping governments stabilize industries. You can learn more about Porter's research and other business tools in his book, *Competitive Strategy: Techniques for Analyzing Industries and Competitors*.<sup>[1]</sup>

Below is a summary of each of the five forces:

- **Power of Customers:** Here, you look at the impact your customers have on your business. As an example, this force is driven by the number of customers you have, the importance of each individual customer to your business, and the cost involved for them to switch from your products and services to another company or organization. In other words, you are looking at the ability your customers have to put your firm under pressure.
- **Substitute Products:** Here, you look at the ability of your customers to find substitute products or alternative ways of doing what you, your team, or your company does. If substitution is easy and viable, this weakens your power.



- **Power of Suppliers:** Here, you look at how easy it is for suppliers to influence and drive up prices; the uniqueness of their product or service; their strength and control over you, your organization, and/or your company; and the cost of switching from one supplier to another. The fewer suppliers you have, and the more you need suppliers, the more powerful the suppliers are.
- **Threat of New Entrants:** Here, you look at how easy it is for people to enter your market. New competitors can easily become a threat if it costs little time and money to enter your market and effectively compete with your company. If there are few economies of scale in place, or if you have little protection for your key technologies, new competitors can quickly enter your market and weaken your position. If you have strong barriers to entry, you can maintain leverage and maintain a favorable position. The thing you have to remember in this area is profitable markets will always attract new firms.
- **Competitive Rivalry:** Here, you will look at the number of competitors and their capabilities. You will have less power in the market if you have many capable competitors that have equally attractive products and/or services. On the other hand, if no one else can do what you do, or provide the services you can provide, you will have tremendous strength.

Reference:

[1] <http://www.amazon.com/Competitive-Strategy-Techniques-Industries-Competitors/dp/0684841487>

## Porter's Five Forces – Characteristics



### Power of Customers

This force looks at the impact your customers have on your business. It is driven by the number of customers you have, the importance of each individual customer to your business, and the cost involved for them to switch from your products and services to another company or organization. In other words, you are looking at the ability your customers have to put your firm under pressure.

Customers have the power to demand lower-priced or higher-quality products when their bargaining power is strong. Lower price means lower revenue for the company, while higher quality typically raises production costs. Customers have strong bargaining power when they buy in large quantities, control access points to the final customer, or where only a few buyers exist. They also have power when the switching costs to other suppliers are low, or there are many options for products and/or service, or finally, if customers are price sensitive.

### Substitute Products

Here, you look at the ability of your customers to find substitute products or alternative ways of doing what you, your team, or your company does. If substitution is easy and viable, this weakens your power. This force typically impacts an industry through price competition; as more substitutes become available, the demand becomes more elastic because customers now have more alternatives to choose from.

This force is especially threatening when customers can easily find alternatives or substitutes for their desired products and/or services with attractive pricing and/or better quality and when customers can easily switch from one product and/or service to another with little to no cost. As an example, switching from coffee to tea costs you little to nothing, whereas switching from a bicycle to a car for transportation will cost more.

### Power of Suppliers

Here, you look at how easy it is for suppliers to influence and drive up prices, the uniqueness of their product or service, their strength and control over you, your organization and/or your company, and the cost of switching from one supplier to another. The fewer suppliers you have, and the more you need suppliers, the more powerful the suppliers are. The more potential but realistic sources of supply, the stronger the bargaining power your company will have.

**Threat of New Entrants**

Here, you look at how easy it is for people to enter your market. New competitors can easily become a threat if it takes relatively little time and money to enter your market, if there are few economies of scale in place, or if you have little protection for your key technologies. If you have strong barriers to entry, then you can leverage and maintain a favorable position. Remember that profitable markets will always attract new firms.

It is difficult to enter a market if your products are patented, proprietary know-how is required, you have a strong brand, or there are restricted distribution channels or economies of scales are difficult to achieve.

**Competitive Rivalry**

With this force, you must consider the number and capabilities of your competitors. You will have less power in the market if you have many capable competitors that have attractive products and/or services. If more companies are competing with each other, the resulting competitive pressures will mean that prices, profits, and strategy will be driven by it. Competitive rivalry might be higher when similar-sized companies operate in one market, when companies have similar strategies, when products offered have similar features and offer the same benefit, when the growth in the industry is slow, or there are high exit barriers or low entry barriers.

## Porter's Five Forces – Antivirus Example

Force	Antivirus
Customers	<ul style="list-style-type: none"> <li>• Customers have no choice except to purchase but can switch whom they purchase from</li> <li>• High-volume customers can negotiate more favorable terms and pricing</li> </ul>
Substitute Products	<ul style="list-style-type: none"> <li>• No acceptable substitutes seen by most of market, though allowlisting solutions may help</li> <li>• High barrier to switching</li> </ul>
Suppliers	<ul style="list-style-type: none"> <li>• Product is dependent on intellectual capital, not material inputs, so suppliers have little power</li> <li>• Employees have some power collectively, but not individually</li> </ul>
New Entrants	<ul style="list-style-type: none"> <li>• High costs to develop and market a new competitive product</li> <li>• Strong brand loyalty</li> <li>• Customers resistant to switching</li> </ul>
Competitors	<ul style="list-style-type: none"> <li>• Market dominated by a few large competitors, very fragmented remainder of market</li> <li>• Customers see little differentiation in core product, just in support and ease of use</li> </ul>

Let's take a summary view of how we would apply Porter's Five Forces analysis to a security vendor for antivirus. Performing this method of analysis should be a prerequisite to establishing the right components for your strategy because it will enable more informed decisions about your security investments—such as security products and or services purchases.

### Power of Customers

When you are looking at current or potential suppliers of your security products, you may want to consider additional questions with a slight twist. In relation to suppliers in the marketplace, as a customer, what does our spending represent as an overall percentage of their turnover? Are we a large or small buyer of their security products and/or services? Could we send a typical supplier in the marketplace into liquidation if we moved our business from one supplier to another? In the antivirus example, customers have no choice but to purchase, but they can switch which supplier they purchase their product from. High-volume customers can negotiate more favorable terms and pricing.

The higher your spend is against the spend of other customers in the marketplace, the stronger bargaining power you have for your security products and/or services. You may want to consider procurement auctions for categories in which your business is significant enough to be attractive, you have clearly defined requirements, and there are ample suppliers attracted to your business to ensure competition.

### Substitute Products

You'll want to determine if other products are available that could fulfill the same purpose or if technology advancements provide an alternative way of fulfilling the same need and how likely new inventions are to get to market and lastly, whether new products are delayed in getting to the market for fear of disrupting the market. In the antivirus example, there are not acceptable substitutes seen by most of the market, although allowlisting solutions may help, and there is a high barrier to switching.

### Power of Suppliers

You'll want to determine how many sources of supply there are in the market for a particular product,

how stable the market is, and if the same suppliers have dominated the market for years. You'll also want to consider if there is supplier consolidation taking place or if current suppliers are enjoying high profits or if they are going out of business. In the antivirus example, products are dependent on intellectual capital, not material inputs, so suppliers have little power, and employees have some power collectively, but not individually.

### **Threat of New Entrants**

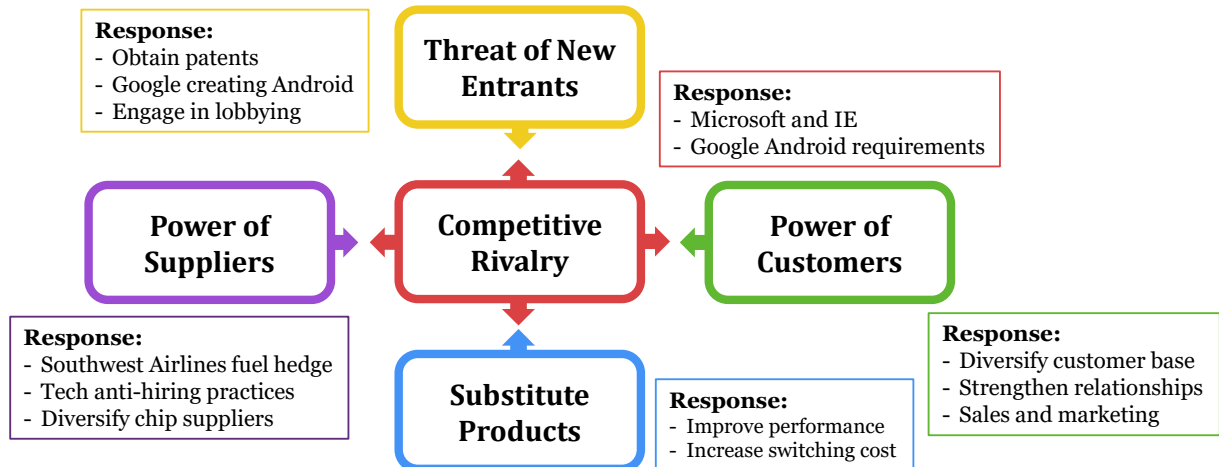
You'll want to determine if the market is profitable for current and potential suppliers, or if there are barriers to entry for a new firm, such as regulation, high fixed cost, or strong brand equity. You'll also want to determine if a new entrant can add value to the product or create a differentiation, and lastly, how quickly new products are introduced. In the antivirus example, there are high costs to develop and market a new competitive product, and there is a strong brand loyalty; therefore, customers are resistant to switching.

### **Competitive Rivalry**

The fiercer the competition between existing firms, and the more firms that reside in the marketplace, the stronger bargaining power you have for your security products and/or service needs. This should be balanced against the number of customers in the marketplace. If there are a lot of customers and a lot of suppliers, then suppliers can change their customers as can customers change their suppliers. In the antivirus example, the market is dominated by a few large competitors, and the remainder of the market is very fragmented. Customers see little differentiation in core products but recognize differentiation in support and ease of use.

## Responding to Competitive Forces – Examples

- Build a moat to protect your business



When you have an understanding of the competitive forces that affect your industry and company, the next step is to translate this understanding into action. The idea is to build a moat that protects your business. By quickly building favorable synergies and rigid consequences, companies can strengthen their own virtuous cycles and block the cycles of others. Ultimately, the goal is to create defensible business positions that enable you to capture more value than competitors.

### Power of Customers

Because customers can potentially walk away from your business at any time, it is important to broaden, diversify, and strengthen your customer base. For example, customers can, in theory, easily switch computing devices—whether it be from a Mac to a PC or from an iPhone to an Android phone. To help combat this, Apple has focused on creating synergies among its various products. After the iTunes Store was made available on PCs, existing iPod customers started buying more Macs. This "halo effect" has since been seen in relation to iPhone customers who also buy Macs and other Apple products. To further strengthen customer relationships, Apple created the Genius Bar in its stores. This customer support desk is not a profit center but is instead designed to engage with customers, provide them needed support, and make them happier about the use of Apple's products. All of this is further strengthened by Apple's marketing, which often focuses on emotional appeals and helps strengthen long-term relationships with customers.

### Substitute Products

Customers can switch away from your product and use something else entirely. In transportation, people can choose to take planes, trains, buses, boats, cars, bicycles, and so on. Each of these options has trade-offs in terms of time, cost, and convenience. To ensure that customers prefer your particular product, you can, of course, continue to improve it over time. A better product often means happier and more loyal customers. One way to engineer "loyalty" is to increase switching costs. If it is extremely expensive or time-consuming to switch products, then you are less likely to do so. This is why technology vendors like Microsoft worked to create dependencies among their various products. To run Exchange, you had to have Windows Server, which includes Active Directory (AD). With large parts of the Microsoft stack in place, it's much more likely that other Microsoft products like SQL Server and SharePoint would be used.

### **Power of Suppliers**

Suppliers have a key role in your value chain. They can determine how quickly you can get the product to market and how profitable you may be. If the costs of your key inputs go up drastically, this will obviously impact your bottom line. In the airline industry, this is exactly why Southwest Airlines enters into fuel hedging contracts. By better controlling the volatility of one of its key inputs, the company is able to keep fares lower than competitors. In the technology industry, skilled labor (for example, developers, security professionals) is a key input for many companies. To keep costs down, a number of technology companies like Adobe, Apple, Google, Intel, Intuit, and others entered into illegal anti-poaching agreements that restricted the recruitment of their high-tech employees. In response, the Department of Justice brought an antitrust action against these companies, resulting in settlement payouts of hundreds of millions of dollars.<sup>[1]</sup> In addition to cost, suppliers can determine whether or not updated products get to market. For many years, the availability of newer Intel chips determined when new, more powerful PCs could be brought to market. In recent years, Apple has tried to diversify supply of its A-Series chips from multiple manufacturers like Samsung and Taiwan Semiconductor Manufacturing Co. (TSMC) to better manage risk from key suppliers.

### **Threat of New Entrants**

It is often beneficial to make it difficult for new entrants to join your market. This can be accomplished by developing new, proprietary technology that others do not have and patenting it. Because creating new inventions and patents is difficult and time-consuming, some organizations have simply bought large patent libraries from other companies. In the competitive mobile space, this is a big reason that Google bought Motorola for \$12.5 billion. This is also why a consortium of Apple, Microsoft, BlackBerry, and others bought Nortel's patents for \$4.5 billion. All this patent acquisition is a hedge against attacks from competitors. In fact, that is why Google originally created Android. It was concerned about Microsoft, with its leading mobility efforts at the time, controlling an operating system that would exclude Google Search. Google didn't know it at the time, but its investment in Android wound up being more of a hedge against Apple's iOS. Many companies also engage in political lobbying to create or update regulations to their benefit. This includes items like patent reform, corporate tax reform, privacy, and cybersecurity.

### **Competitive Rivalry**

To win in the market, companies often try to create barriers for other firms. This is what Microsoft was accused of when it bundled its Internet Explorer (IE) web browser and Windows Media Player with its Windows operating system. Regulators argued that Microsoft used its monopoly power in PC operating systems to unfairly gain an advantage in other markets.<sup>[2]</sup> Shifting from PCs to mobile devices, Google is now accused of anti-trust violations in the European Union (EU) because it required manufacturers to pre-install Google Search and Chrome, provided financial incentives for favoring Google Search, and provided access to the Google Play Store only to manufacturers who agreed to make Google Search the default and agreed not to create forked versions of Android. These tactics helped strengthen Google's dominant position and built barriers that protected its core business.

#### **References:**

[1] [https://en.wikipedia.org/wiki/High-Tech\\_Employee\\_Antitrust\\_Litigation](https://en.wikipedia.org/wiki/High-Tech_Employee_Antitrust_Litigation)

[2] [https://en.wikipedia.org/wiki/United\\_States\\_v.\\_Microsoft\\_Corp](https://en.wikipedia.org/wiki/United_States_v._Microsoft_Corp)

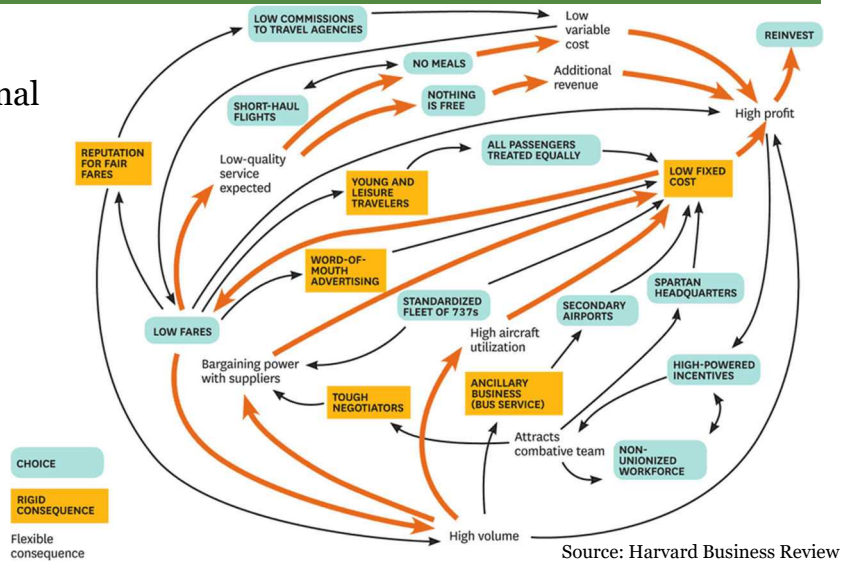
## Strategic Objectives – Ryanair

### • Strategic objectives

- Long-term organizational goals
- Convert vision and mission into more specific plans

### • Ryanair

- Vision to become a low-cost airline
- What are the next steps?



Organizations create strategic objectives to clearly define how they should respond to the competitive forces in the marketplace. These strategic objectives are long-term organizational goals that help turn high-level mission and vision statements into more concrete goals. In other words, strategic objectives are actions you take to implement your business strategy.

Ryanair had a vision to become a low-cost airline. It wanted to move away from its traditional business model, which had become unprofitable. So, Ryanair took steps to implement a number of strategic objectives to help it achieve its plan of becoming a low-cost airline. The company defined the following critical strategic objectives:

- **Maintain Low Fixed Costs:** This included flying out of secondary airports, choosing a nonunionized workforce, operating out of a spartan headquarters, and utilizing a standardized fleet of Boeing 737s.
- **Attract Young and Leisure Travelers:** The company chose to treat all passengers equally. By catering to only one class of passenger, it could charge for all additional services, serve no meals, and focus on short-haul flights. This objective not only reduced costs but also drove additional revenue because now customers had to pay for all checked bags, snacks, and so on.
- **Be Tough Negotiators:** The company decided to hire an aggressive management team by offering high-powered incentives for performance. This enabled the company to more effectively bargain with suppliers and the workforce.
- **Build a Reputation for Fair Fares:** As a result of these strategic objectives, Ryanair reduced variable and fixed costs while driving up volume because of its reputation for reasonable fares. It has created a virtuous cycle in which all the parts of its business help deliver acceptable service at low prices.

Reference:

<https://hbr.org/2011/01/how-to-design-a-winning-business-model>



## Strategy Maps

- Strategic objectives
  - Strategy is often expressed via strategic objectives
  - Based on understanding of the business model, strategy, & competitive forces
  - High-level and sometimes vague
- Strategy map
  - Links high-level strategic objectives to specific projects, initiatives, etc.
  - Shows how to turn strategy into tangible outcomes
  - Highlights gaps in strategy implementation
  - Helps communicate strategy to the entire organization

A strategy map helps you communicate strategy to the entire organization. Some have even called them "a piece of the strategy in everybody's pocket."<sup>[1]</sup>

Oftentimes, we hear organizations say that they want to "increase shareholder value" or "grow profit by 50%." These can be seen as vague proclamations that are hard for many in the organization to turn into concrete action. Strategy maps help link these high-level objectives to specific projects, initiatives, and activities.

Laying out a visual strategy map also highlights gaps or areas where the strategy may not be fully implemented. For example, the strategy map could highlight that one business unit does not have any objectives for compliance. Is this because the unit does not have to comply with various compliance regulations? Do they not process in-scope sensitive data? Did they find another way to process or obfuscate the data? Strategy maps help uncover such situations.<sup>[2]</sup>

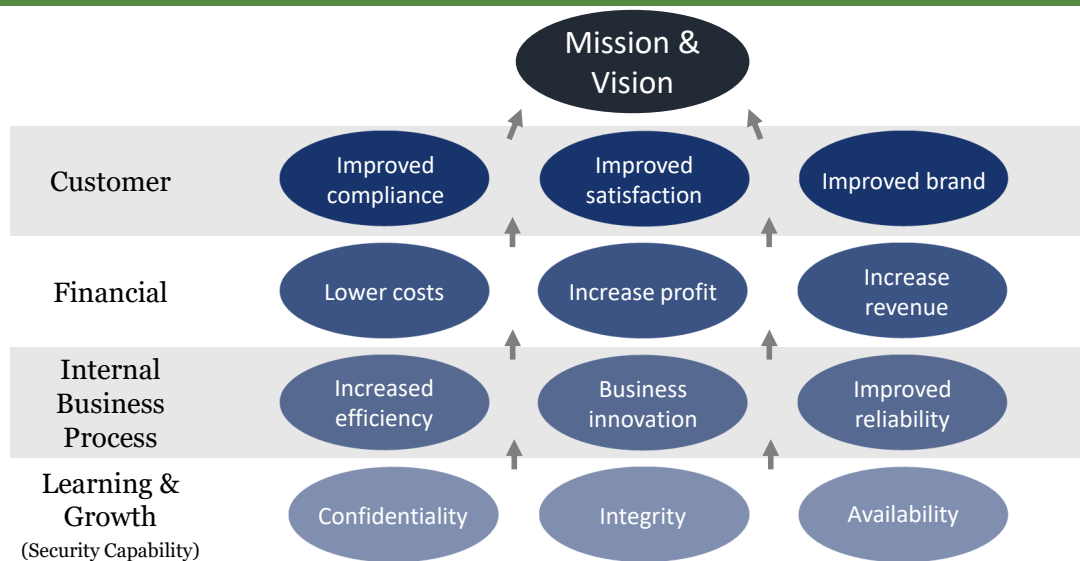
Even nonprofits and government agencies can benefit from strategy maps. Most for-profit organizations will place financial goals at the top of the map. However, non-profits and government agencies often place customers at the top. This highlights the organizations' focus on their mission and serving their constituents. Financial goals are still important and will be included in the strategy map, but these financial goals are just in service of the larger customer goals.

### References:

[1] <https://www.excitant.co.uk/resources/white-papers/strategy-maps-and-strategy-mapping/>

[2] <https://hbr.org/2000/09/having-trouble-with-your-strategy-then-map-it>  
<https://hbr.org/product/strategy-maps-converting-intangible-assets-into-ta/an/1342-HBK-ENG>

## Strategy Map



As security professionals, we are often focused on the bottom row of this diagram – improving our security capabilities by increasing our knowledge and skills or improving our tools and technologies. As security leaders and managers, we have to remember how these security activities support the overall strategic objectives for the organization as a whole. For example, improving security tools and technologies can help support business innovation in the form of new products that the company is trying to bring to market. These may be new mobile apps, websites, or other technology products in which security can contribute new features or capabilities. These new products have a direct correlation to improving customer satisfaction and ultimately increased revenue. Similarly, by improving our security capabilities, we can improve business processes around efficiency and availability, leading to improved compliance and ultimately lower costs.

The goal of any organization is to create value for its key constituents. Usually, this means increasing revenue and overall profitability. Whatever the key strategic objectives are for your organization, a key component to your success as a security business leader will be mapping your security activities to those overall strategic objectives.

## Lab 1.3: Creating a Strategy Map

Estimated Time: 20 Minutes

- Goal of this exercise
  - Fill out a strategy map to show how objectives and activities link together to achieve desired outcomes
- Warning
  - Strategy maps are intended to be a bit ambiguous
  - There are not necessarily clear right/wrong answers
  - Going through the mapping process is most vital
- Lab steps
  - Read the case below then
  - Fill out the blank strategy map on the subsequent page

### READ

Read the 2-page case study below

It takes approximately 10 minutes to read the case



### Thunderbolt Operations

The shipping process begins with a customer request to send a package to a specific destination. Packages may be picked up from an address by a Thunderbolt delivery driver, left at a stand-alone drop box, or dropped off at a Thunderbolt store. The first/last mile team is charged with the beginning and ending of a package journey and serves a critical role in the data integrity of its customers. While customers have the option to print shipping labels, 25% of customers (mostly consumers) still hand-write addresses on packages. Handheld devices carried by drivers and store registers can identify many address errors, but the pace of delivery and pickup hinders employees from doing consistent checks. These errors increased during the pandemic as front-of-house staff grappled with the near doubling of volume of packages and the shift from store and business deliveries to residential deliveries.

Once a package completes its “first mile”, a Thunderbolt employee enters the information into Bolt, which creates the optimal package route. The same data is input into Hermes, and the customer begins to receive notifications. The package is scanned at each transfer point, and data is sent to the main servers with its location and updated delivery date/time if applicable; this information is also sent to customers via Hermes. Packages with a delivery schedule of one, two, and sometimes three days are taken by truck to the nearest airport for prioritization and routing. By optimizing package routes, Bolt allows Thunderbolt to use the most cost-effective delivery strategy and avoid expensive air freight. For example, if a package is needed 200 miles away in two days, Bolt may locate a truck covering that distance in a faster time than sending the package by air. Thunderbolt does not own its own planes but partners with several airlines to execute air shipping. This makes air shipping more expensive than competitors with in-house plane-fleets and makes cost optimization by Bolt even more important.

After the package finishes the bulk of its trip, it is once again in the hands of the first/last mile team for delivery. While Bolt recommends final delivery options, local distribution centers are given leeway in optimizing the last mile route. When the package is delivered, Bolt and Hermes are notified, and Hermes sends a message to the customer with an option to provide feedback.

## **Cloud Technologies and the Competition**

While technology and cloud strategies are not required to be publicly disclosed, several direct competitors have made headlines by announcing digital strategy partnerships with cloud providers. The announcements were largely seen as positive, and each announcement corresponded to a general increase in share price, at least in the short term.

### **UPS**

After a trial relationship with Google Cloud in 2019, UPS announced an expanded partnership with Google Cloud in 2022. Citing the dramatic increase in packages shipped as well as world events such as the COVID-19 pandemic, UPS identified a need to store and analyze more data and use it more quickly to adapt to an ever-changing environment. The UPS/Google Cloud partnership claims more data will be tracked, stored, and analyzed with results rapidly impacting business decisions and operations. UPS also cited the increased use of RFID tracking on each package impacting the amount of data created, and therefore, stored. Chief Information and Engineering Officer Juan Perez stated, "We have to get to a place where we can analyze data much more rapidly."

### **FedEx**

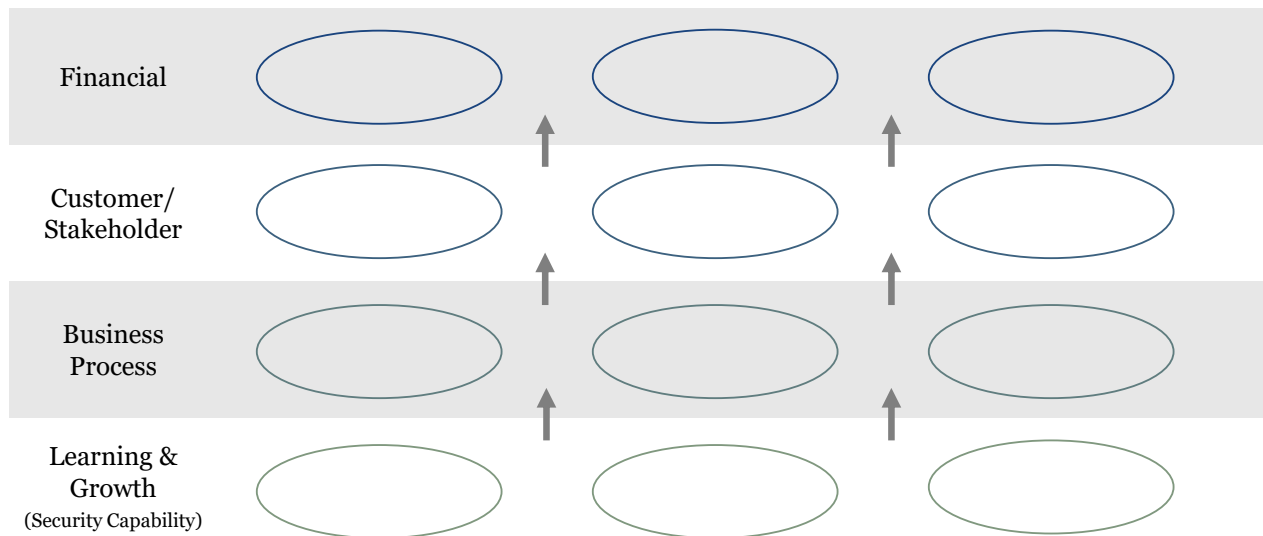
FedEx included a cloud migration announcement during its "investor day" in June of 2022. CIO Rob Carter claimed the move would save over \$400 million annually and that the project would be completed in two years. He went on to say, "We've shifted to cloud...we've been eliminating monolithic applications one after the other after the other...we're moving to a zero data center, zero mainframe environment that's more flexible, secure, and cost-effective." FedEx has partnered with Oracle and Microsoft Azure for the project.

The announcement was not without pushback as some questioned the value of a mature organization like FedEx shifting 100% to the cloud. "Ultimately companies that abdicate their informatics operations like this will give their profits to their data-center operators, who will be empowered to charge them whatever price they want," warned a commentator on Hacker News. "Because what's their BATNA [best alternative to a negotiated agreement]? Migrating from Azure to AWS when Microsoft doesn't want to let them?"

### **DHL**

DHL partnered with Microsoft Azure and AI fulfillment provider Blue Yonder in 2020 to simplify data and analytics around supply chain logistics and integrate warehouse robots. Results of the partnership were positive enough to land DHL as a case study on Microsoft Azure's "Customer Stories" in 2021. DHL consistently mentions Cloud Technology and its advantages in many areas of its website and across several regional hubs and leverages digital operations as a strategic advantage.

## Lab 1.3: Fill in the Strategy Map



There are 12 items below related to Thunderbolt and their cloud migration. The goal of this lab is to show how objectives and activities link together to achieve desired outcomes.

Place the 12 items below into the appropriate bubbles on the slide above. The items below are listed in alphabetical order but must be rearranged on the slide above.

You can simply write the items into the bubbles above or, if you have thin Post-it notes available, you can write the items onto the Post-it notes and move them around on the page in your book.

**Suggestion: Start by filling in the bottom “Learning & Growth” row and then fill out the top “Financial” row. This will make it easier to complete the mapping in the middle.**

- 1) Advance analytics
- 2) Automate operations
- 3) Cloud security architecture
- 4) Cloud security monitoring
- 5) Delivery optimization
- 6) Enhance tracking & notification
- 7) Improve margin
- 8) Improve security governance
- 9) Increase productivity
- 10) Increase revenue
- 11) Reduce costs
- 12) Secure Infrastructure as Code

---

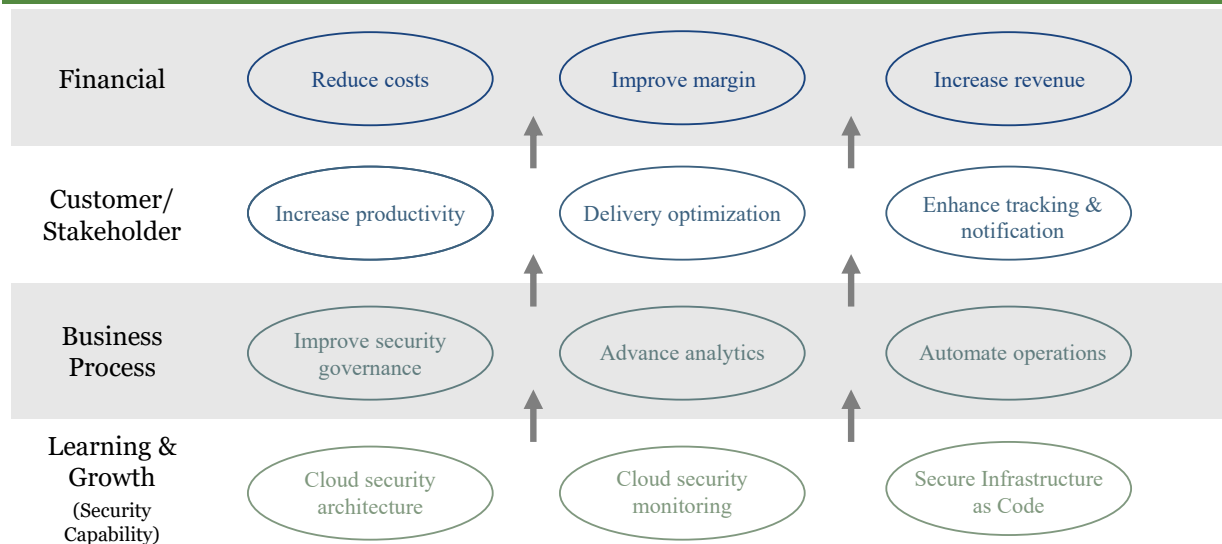
## Lab Debrief

---

*Note that this section contains a debrief  
and potential lab answers*

This page intentionally left blank.

## Lab 1.3 Solution: Fill in the Strategy Map



As a for-profit corporation, Thunderbolt's ultimate goal is to improve margin. This can be done by increasing revenue (i.e., growing the top line) and reducing costs (i.e., managing the bottom line). Oftentimes, this is generically referred to as "increasing shareholder value." However, this broad statement is not always specific enough to drive action within the organization.

In our example above, costs are reduced by increasing productivity (a commonly stated benefit of moving to the cloud). The Thunderbolt case also mentions delivery optimization helps the company manage costs while enhanced notification and tracking can lead to increased customer satisfaction and, therefore, increased usage and revenue.

Productivity can add to the "ease of doing business" which might also be enabled by advanced analytics capabilities and automated operations. Underlying these benefits are appropriate cloud security architecture, cloud security monitoring, and secure infrastructure as code that can be used to ensure appropriate controls are used for all cloud deployments.

## In Summary

- Security leaders and managers must understand
  - Business model
    - What the organization does to create value
  - Business strategy
    - How the organization competes
  - Strategic objectives
    - Specific goals to implement strategy

A business model describes how your company or organization operates. It is the plan for how you will generate revenue and actually make a profit from that revenue. This is, of course, done by delivering something of value to your customers. However, it's not enough to simply have a business model. Successful businesses have a strategy that defines how the organization will respond to the various competitive forces in the marketplace. To win in the market, an organization will define strategic objectives that are specific goals that help the company implement the overall strategy. As security leaders and managers, we must understand how our businesses operate so we can provide services that help drive value for the overall 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 I

- Overview
  - Need for Strategic Planning
  - 30-60-90 Day Plan
    - Lab #1: CISO First Impression
- Decipher the Business
  - Historical Analysis
  - Values and Culture
  - Stakeholder Management
    - Lab #2: Relationship Management
  - Asset Analysis
  - Business Strategy
    - Lab #3: Strategy Map
- **Decipher the Threats**
  - Threat Actors
  - PEST Analysis
  - Threat Analysis

This page intentionally left blank.

## Why We Need to Decipher the Threats

- By understanding the threats and threat landscape, we can
  - Better plan our defenses
  - Learn how we can improve against actual threats
  - Understand where attackers are weak

"If you know the enemy and know yourself  
you need not fear the results  
of a hundred battles."  
- Sun Tzu

Sun Tzu (544–496 BC) was a Chinese military general, strategist, and philosopher who is best known for writing *The Art of War*. It presents a philosophy of war that is widely accepted as a masterpiece of strategy. Its lessons have been applied not only to military affairs, but also to business, politics, and, of course, information security.

In the previous section, we covered topics to help us understand the business ("know yourself"). In this section, we cover topics to help us understand the threats ("know the enemy"). By understanding the threats, we can improve our defenses and understand where attackers are weak. As Sun Tzu notes, it is only by understanding both that we can hope to build a successful information security program.

## How to Develop an Understanding of the Threats

### 1) Understand threat actors

- Their motivations and mindset

### 2) Understand business threats

- Analyze the Political, Economic, Social, and Technological (PEST) factors that affect the organization

### 3) Analyze threats

- Understand tactics, techniques, and procedures using Kill Chain Analysis and MITRE ATT&CK

This understanding of the threats comes from:

#### 1) Understanding threat actors

Being able to think like your adversaries requires an understanding of their motivations and mindset.

#### 2) Understanding the macro factors and business threats that affect the organization

Utilizing PEST to analyze elements that may be of concern to senior leaders.

#### 3) Analyzing threats

If an adversary is attempting to gain access to your critical assets, then it will need to mount an attack. Understanding its tactics, techniques, and procedures will help you better plan your defense and understand where your current defenses may be lacking.

# 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 I

- Overview
  - Need for Strategic Planning
  - 30-60-90 Day Plan
    - Lab #1: CISO First Impression
- Decipher the Business
  - Historical Analysis
  - Values and Culture
  - Stakeholder Management
    - Lab #2: Relationship Management
  - Asset Analysis
  - Business Strategy
    - Lab #3: Strategy Map
- Decipher the Threats
  - **Threat Actors**
  - PEST Analysis
  - Threat Analysis

This page intentionally left blank.

## Understanding Threat Actors

- Goals of this section
  - Learn about the different types of threat actors
  - Understand their motivations
  - Understand the tactics used by common threat actors
    - By walking through two cases of real-world attacks

In this section, we cover the different types of threat actors, their motivations, and the tactics used by common threat actors by walking through two examples of real-world attacks.

## About VERIS

- VERIS
  - Vocabulary for Event Recording and Incident Sharing
  - Schema that describes security incidents in a structured & repeatable manner
    - Available at <http://veriscommunity.net>
- Used by the Verizon DBIR
  - Standard way to analyze incidents
  - Mapped and recoded incidents from other frameworks
- VERIS Community Database (VCDB)
  - Free repository of publicly reported security incidents
    - Available at <http://veriscommunity.net/vcdb.html>

VERIS is the Vocabulary for Event Recording and Incident Sharing.<sup>[1]</sup> It defines a schema and set of metrics to describe security incidents in a structured and repeatable manner. It is most famously used by Verizon as part of its annual Data Breach Investigations Report (DBIR).

The VERIS Community Database (VCDB) is a free repository of publicly reported security incidents. Both the raw incident data and a nice dashboard for searching historical incidents are available online.

By utilizing a standard mechanism for talking about security incidents, the VERIS framework helps us describe threat actors and their motivations.

Reference:

[1] <http://veriscommunity.net>

## VERIS Threat Actors

Category	Description	Actor	
<b>External</b>	Threats from sources outside the organization and its partners. This includes criminal groups, lone hackers, former employees, and government entities, as well as "Mother Nature" and chance.	<ul style="list-style-type: none"> <li>• Acquaintance</li> <li>• Activist</li> <li>• Auditor</li> <li>• Competitor</li> <li>• Customer</li> <li>• Force majeure</li> </ul>	<ul style="list-style-type: none"> <li>• Former employee</li> <li>• Nation-state</li> <li>• Organized crime</li> <li>• State affiliated</li> <li>• Terrorist</li> <li>• Other</li> </ul>
<b>Internal</b>	Threats that arise from within the organization. This includes full-time employees, contractors, interns, and other staff.	<ul style="list-style-type: none"> <li>• Auditor</li> <li>• Call center staff</li> <li>• Cashier</li> <li>• Developer</li> <li>• End-user</li> <li>• Executive</li> <li>• Finance</li> </ul>	<ul style="list-style-type: none"> <li>• Help desk</li> <li>• HR</li> <li>• Maintenance staff</li> <li>• Manager</li> <li>• Security guard</li> <li>• System admin</li> <li>• Other</li> </ul>
<b>Partner</b>	Any third party that has a business relationship with the organization. These business partners usually have some level of trust or privilege.	<ul style="list-style-type: none"> <li>• Supplier</li> <li>• Vendor</li> <li>• Hosting provider</li> <li>• Outsourced IT</li> <li>• Other</li> </ul>	

VERIS has three categories for threat actors:

- **External:** Threats from sources outside the organization and its partners
- **Internal:** Threats that arise from within the organization
- **Partner:** Any third party that has a business relationship with the organization

Each category has a comprehensive list of potential threat actors that an organization may encounter.

## Sample Threat Actors and Motivations

Threat Actor	Description	Motivation
<b>Nation-State</b>	Countries attempting to gain economic or military advantage over their adversaries and economic competitors by stealing data and sabotaging equipment.	<ul style="list-style-type: none"> <li>• Espionage</li> <li>• Competitive advantage</li> <li>• Fear or duress</li> </ul>
<b>Hacktivist</b>	Activist groups target organizations because of real or perceived slights. Their goal is to damage the brand and embarrass the organization.	<ul style="list-style-type: none"> <li>• Ideology or protest</li> <li>• Fun, curiosity, or pride</li> <li>• Grudge or personal offense</li> </ul>
<b>Organized Crime</b>	Criminals want to make money using stolen data and access to systems. They use malware, phishing, and application attacks to steal data.	<ul style="list-style-type: none"> <li>• Financial gain</li> </ul>
<b>Competitor</b>	Other organizations in the same or similar industries seeking proprietary information.	<ul style="list-style-type: none"> <li>• Espionage</li> <li>• Competitive advantage</li> </ul>
<b>Insider</b>	Employees who put data at risk by violating policies and standards or through negligence.	<ul style="list-style-type: none"> <li>• Espionage</li> <li>• Grudge or personal offense</li> <li>• Convenience or expediency</li> </ul>
<b>Partner</b>	Vendors that are relied upon to store and process sensitive information. Partners may have elevated levels of access to sensitive data or systems.	<ul style="list-style-type: none"> <li>• Espionage</li> <li>• Convenience or expediency</li> </ul>

Let's look at some common threat actors and their motivations.

**Nation-State:** Countries that attempt to gain economic or military advantage over their adversaries

**Hacktivists:** Activist groups who target organizations for real or perceived slights

**Organized Crime:** Criminals who want to make money using stolen data and access to systems

**Competitor:** Other organizations that may seek proprietary information for competitive advantage

**Insider:** Employees who put data at risk through malicious or negligent actions

**Partner:** Vendors who knowingly or unknowingly put data and information at risk

Threat actor motivations defined in VERIS:

**Espionage:** Espionage or competitive advantage

**Fear:** Fear or duress

**Financial:** Financial or personal gain

**Fun:** Fun, curiosity, or pride

**Grudge:** Grudge or personal offense

**Ideology:** Ideology or protest

**Convenience:** Convenience or expediency

**Unknown:** Unknown

**Other:** Other



---

## Nation-State Case

---

This page intentionally left blank.

## Nation-States

- Complex set of motivations
  - Espionage
    - Political gain
  - Fear
    - Geo-political destabilization
  - Financial gain
  - Ideology

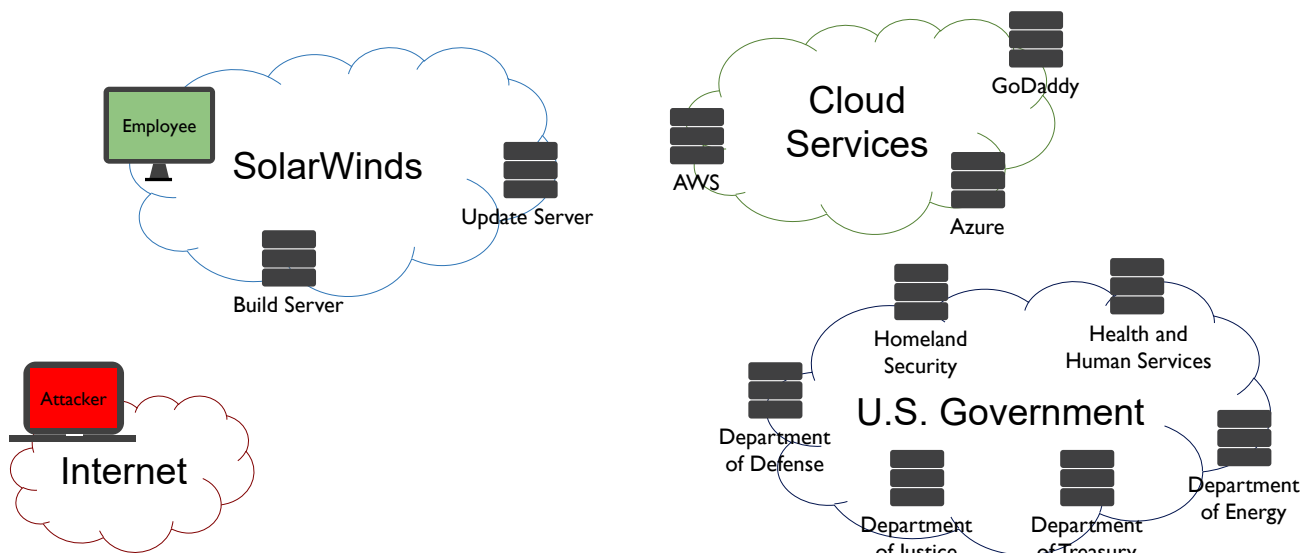
Nation-state actors have a diverse set of motivations. They often focus on espionage to gather information about other countries and adversaries to further their own political goals or ambitions. Even before cybersecurity concerns began making regular headlines, countries around the world have used various intelligence mechanisms to gather information and influence political outcomes in their favor. This influence also extends to disrupting a nation's political activities by causing fear, duress, or panic that can lead to geo-political destabilization. At one point during the Ukrainian power grid attacks, the adversary also launched a telephone denial-of-service attack so that the hundreds of thousands of people without power could not even contact the power company. It has been speculated that this was done to weaken the confidence that citizens have in their government and institutions.

Nation-states have also undertaken campaigns to steal intellectual property from countries and companies to gain a financial advantage by "outsourcing the research and development" of key products. Some have speculated that North Korea has even undertaken hacking campaigns to raise money to fund their military as a way to offset their overall weak economy. They have even conducted attacks driven by ideology when they attacked Sony Pictures in retaliation for creating the movie *The Interview* that portrayed the North Korean leader in a negative light.<sup>[1]</sup>

Reference:

[1] <https://deadline.com/2017/04/as-north-korea-rumbles-insiders-tell-how-small-players-stood-tall-helping-sonys-the-interview-1202069868>

## Overview

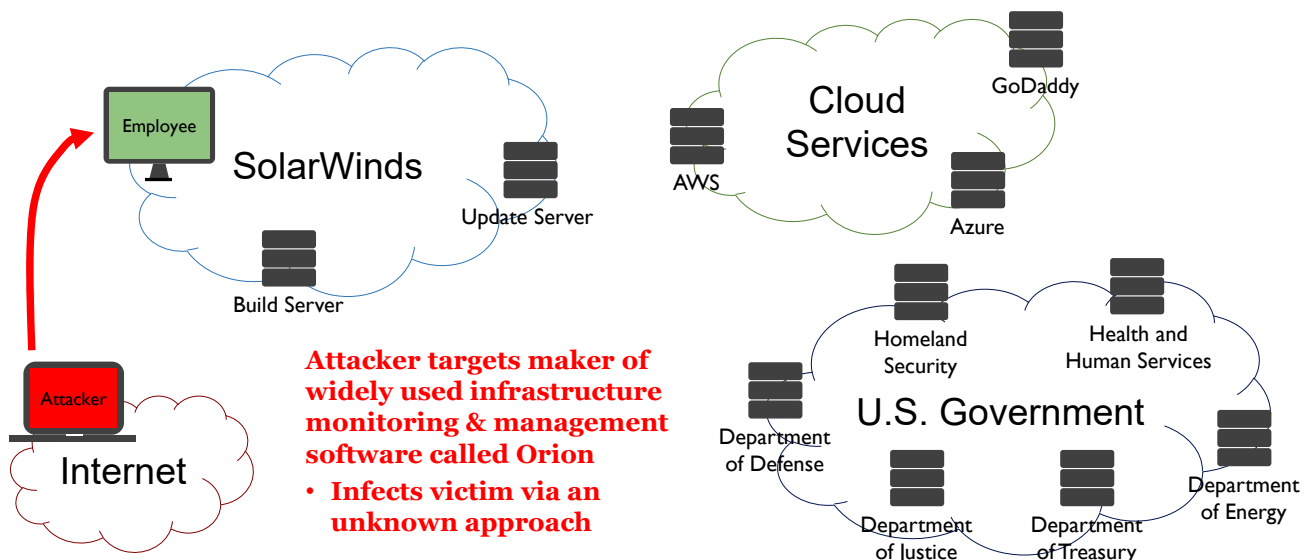


Before talking about how the SolarWinds attack was conducted, let's start by providing an overview of the different players and systems. In the lower left-hand corner, we have the attacker lurking somewhere on the internet. As a first step, the attacker identified SolarWinds as the maker of popular enterprise software used by thousands of organizations around the world (approximately 300,000 customers at the time of the attack). Specifically, SolarWinds makes the Orion infrastructure monitoring and management software. Given the functionality of this software it is often required to have elevated or administrative access with the organizations where it is deployed.

In the upper right-hand corner, we have various cloud services that the attacker leveraged to aid in their attack.

In the lower right-hand corner, we have different departments and agencies of the U.S. government that were affected by the attack. There were many other groups and companies that were impacted but for the purposes of our overview we are highlighting just some areas of the U.S. government.

## Overview



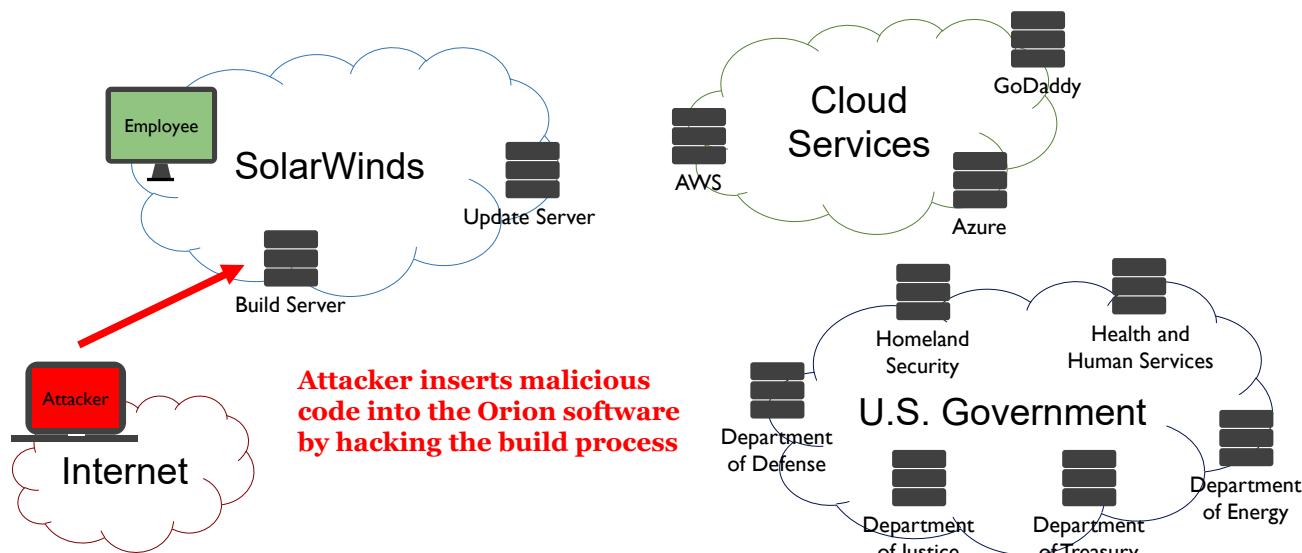
SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

150

At the time of this writing how the attacker first gained entry to SolarWinds was not publicly disclosed. The compromise could have occurred in a number of ways. This could have been accomplished via a watering hole attack where the attackers compromised a web application that is frequently visited by employees at the company. Alternatively, the attacker could have used a targeted spear phishing attack to install malware on the victim's machine and get access to the SolarWinds network. Some initial reports even mentioned the possibility of an accidentally disclosed password leading to initial access. No matter the specific technique, the mischief truly started once the attackers had access.

## Hacking the Supply Chain



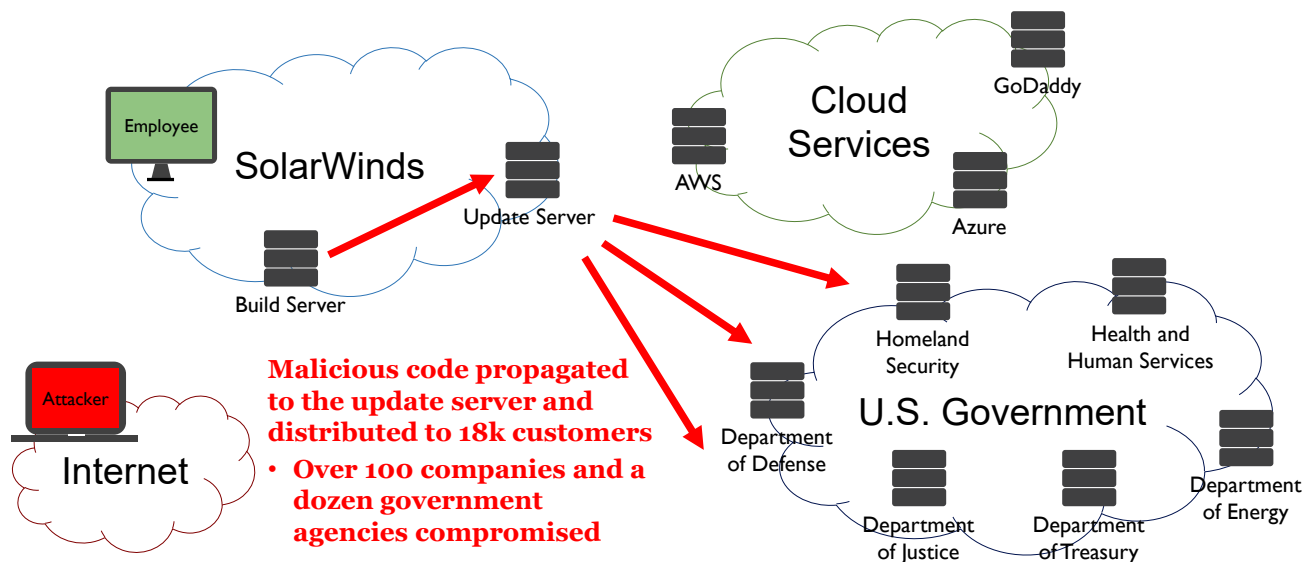
SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

151

With access to SolarWinds environment attackers turned their attention to the internal build server used to package the Orion infrastructure software sold to customers around the world. This is where the attackers revealed their craftiness. Instead of modifying the source code for Orion they made changes to the executable code that is the output of the build process. Why this approach? Most organizations have some sort of code review process that also leverages various automated code scanning tools. However, by compromising the build process itself the attackers reduced the chance of detection and ensured that their changes would be included in the validly signed software. This is a key control used in the software supply chain that was entirely bypassed. Anyone downloading the malicious software would now wrongly assume that it was trustworthy.

## Abusing the Supply Chain



SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

152

Once the malicious software was created the attackers just had to wait for unsuspecting victims to download it. SolarWinds had approximately 33,000 Orion software customers who would periodically check for updates. According to Sudhakar Ramakrishna, SolarWinds president and CEO, "Eighteen thousand was our best estimate of who may have downloaded the code."<sup>[1]</sup> Once it was download victims still had to install and deploy it.

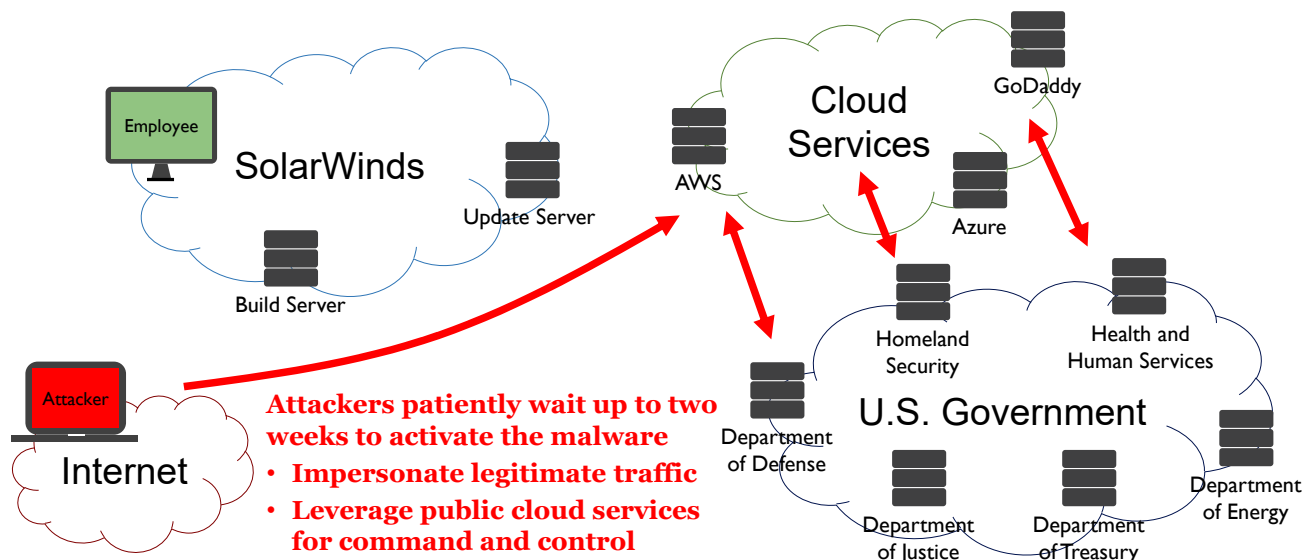
SolarWinds estimated that approximately 100 companies and about a dozen government agencies<sup>[1]</sup> installed the malicious update and were compromised. In the U.S. government alone, this encompasses high profile departments such as the Department of Defense which includes the Pentagon, National Security Agency (NSA), and Defense Information Systems Agency (DISA); Departments of Justice, Treasury, and Energy; Homeland Security; Health and Human Services (HHS); and numerous others. Numerous high-profile companies were also compromised including Microsoft, FireEye, and Palo Alto Networks.

Attackers were able to gain access to emails of top officials, sensitive communications and documents, court documents, sealed case files as well as source code and red team's tools.

Reference:

[1] <https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack>

## Cyber Espionage



SANS

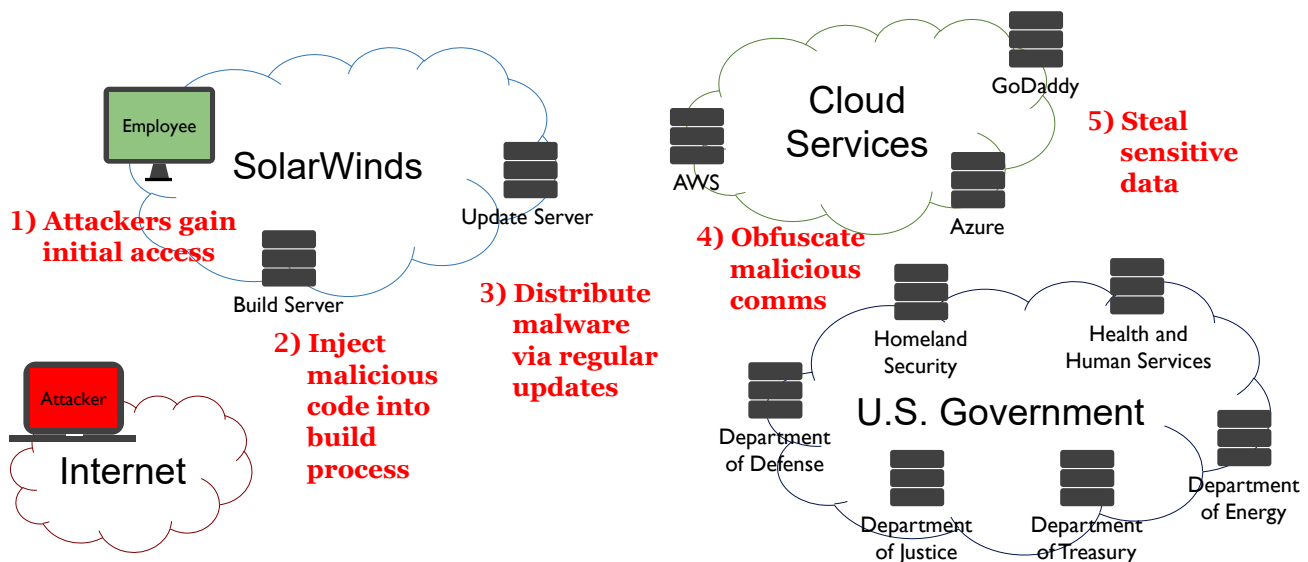
MGT514 | Security Strategic Planning, Policy, and Leadership

153

The malware used in this attack has been given different names. FireEye called it SUNBURST, Microsoft named it Solorigate, and CrowdStrike called it SUNSPOT. But this malware, no matter the name, was very ingenious. Once installed the creators set it to wait for up to two weeks before it was activated. They also had the malware communicate in a format that was based on legitimate Orion syntax and message formats to make their command and controls instructions blend into normal traffic. They also hosted their command-and-control servers in commonly used cloud providers leverage services from Amazon Web Services (AWS), Microsoft Azure, and GoDaddy. The attackers were very patient, thorough, and skillful.

Once command and control was established the attackers pivoted inside of the compromised networks. Since Orion, by definition, had elevated visibility to various systems the attackers were able to connect to victim Office 365 accounts as a trusted third-party application and gain access to emails and other sensitive communications. They were also able to steal certificates that would allow them to impersonate legitimate users and services further elevating their access along the way. Data was, of course, accessed and exfiltrated on a wide scale.

## Attack Summary



SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

154

The SolarWinds<sup>[1]</sup> hack resulted in one of the worst cyber-espionage incidents to ever hit the United States. According to Alex Stamos, former CSO at Facebook and now professor at Stanford University, "It's one of the most effective cyber-espionage campaigns of all time."

The U.S. Government attributed the attack to the Russian Foreign Intelligence Service (SVR)<sup>[2]</sup> with affiliated hacking groups known as Cozy Bear, UNC2452, and Nobelium. These attackers ultimately broke into the networks of at least 100 organizations<sup>[3]</sup> and caused a massive amount of work for security teams around the world.

The SolarWinds hack significantly highlighted both the skill, tactics, and techniques of modern adversaries as well as the need to understand and defend against software supply chain attacks.

### References:

[1] <https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack>

[2] <https://www.cisa.gov/emergency-directive-21-01>

[3] <https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements>



---

## Financial Information Case

---

This page intentionally left blank.

## Equifax Case

- **Equifax Breach**
  - 148 million personal records stolen
  - 400k personal records of UK residents
  - 8k personal records of Canadian residents
- **Equifax Data Breach Report**
  - Published by U.S. House of Representatives Committee on Oversight and Government Reform
  - Information in this section is from this publicly available report



Equifax is one of the three major credit reporting agencies in the United States. The company collects and manages a large amount of personal and financial information, primarily for US residents, but also for a sizeable number of residents of other countries.

In September 2017, Equifax announced that they had suffered a major data breach. The breach eventually grew to encompass 148 million personal records. The vast majority of these records were of US residents along with 400,000 and 8,000 personal records of UK and Canadian residents, respectively.

The breach is a reminder to all organizations about the need for appropriate security controls and post-breach response and communications processes. Within days of the breach, three executives sold \$2 million worth of stock, raising subsequent questions about insider trading. Equifax asked people to go to the website, [equifaxsecurity2017.com](http://equifaxsecurity2017.com), and enter their personal information to find out if they were affected. However, the site asked for exactly the same information that was stolen. The Equifax Twitter account accidentally directed people to [securityequifax2017.com](http://securityequifax2017.com), which was a spoof website at a different URL. Controversially, the initial terms of free credit monitoring for impacted individuals stated that by signing up for the service, they would waive their right to participate in future class action lawsuits. Both the CIO and CSO "retired" shortly after the breach was announced.

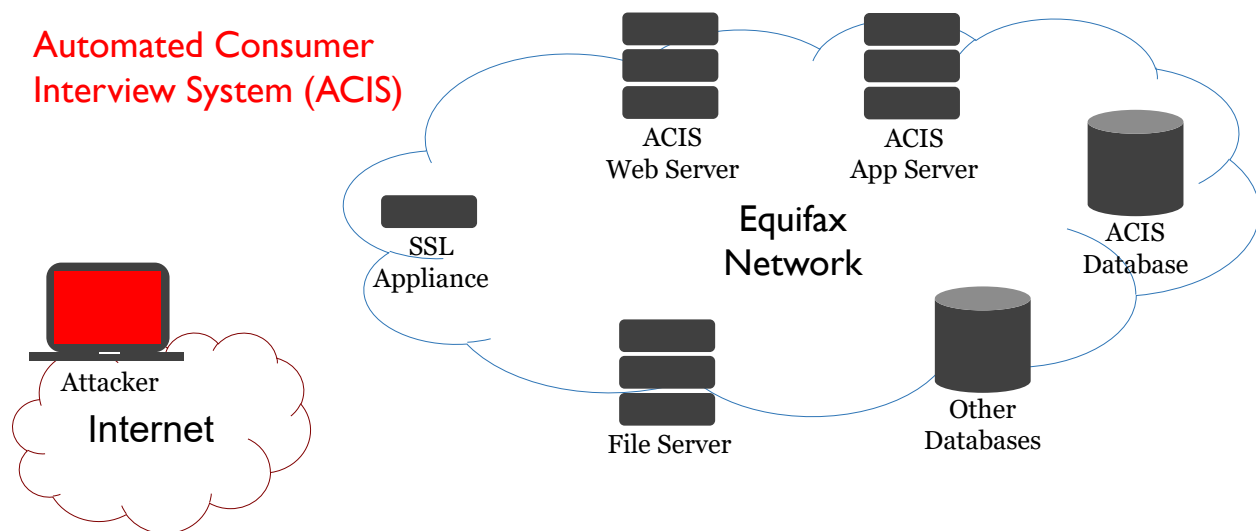
There was so much publicity about the Equifax breach that the US House of Representatives eventually published a detailed report on the breach.<sup>[1]</sup> The upcoming slides are based on information from this publicly available report.

Reference:

[1] <https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf>

## Overview

### Automated Consumer Interview System (ACIS)



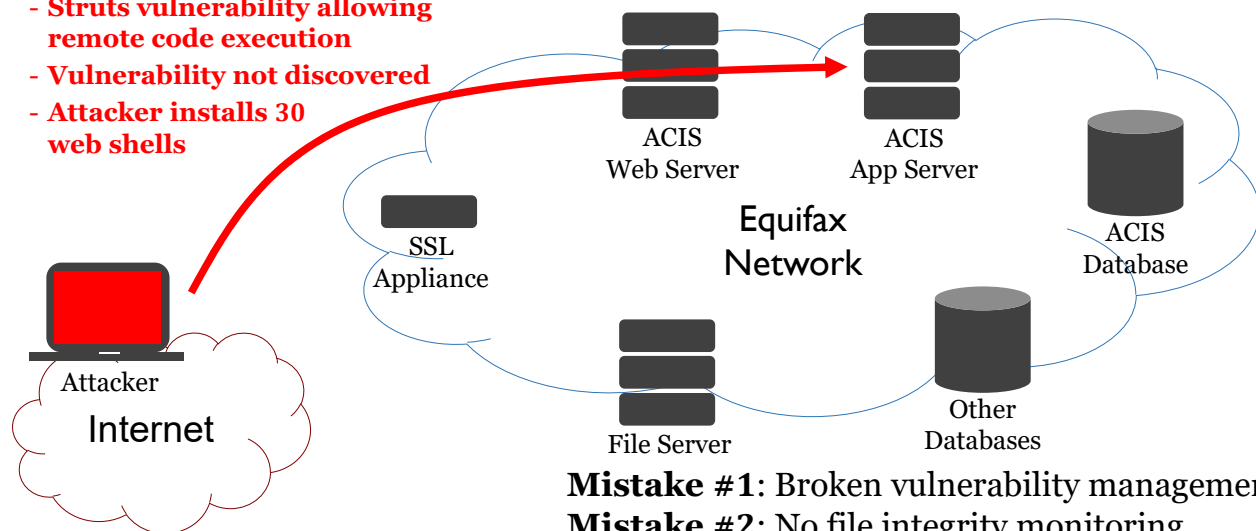
Before talking about how the breach occurred, let's start by providing an overview of the systems that were involved.

In the lower left-hand corner, we have the attacker lurking somewhere on the internet. The attacker discovered the Automated Consumer Interview System (ACIS), which is a web-based application used by individuals to dispute incorrect information found in their credit reports. This application consisted of two web servers, two application servers, and three backend databases.

Additional databases, a file server, and a SSL appliance were also involved in the breach.

## Initial Compromise

- Struts vulnerability allowing remote code execution
- Vulnerability not discovered
- Attacker installs 30 web shells



**Mistake #1: Broken vulnerability management**

**Mistake #2: No file integrity monitoring**

In March 2017, the Apache Software Foundation disclosed a vulnerability in Apache Struts<sup>[1]</sup>, which is a popular framework used for web application development. This vulnerability was given the highest severity rating possible (CVSS base score of 10 out of 10) because it was easy to exploit, allowed arbitrary remote code, and could lead to total compromise of the target system.

The U.S. Computer Emergency Response Team (US-CERT) sent a notice to Equifax about the need to patch the Struts vulnerability. This notification was distributed to the Global Threat and Vulnerability Management (GTVM) team mailing list of approximately 430 people. The email instructed responsible personnel to upgrade Struts: “As exploits are available for this vulnerability and it is currently being exploited, it is rated at a critical risk and requires patching within 48 hours as per the security policy.”<sup>[2]</sup>

The Equifax security team conducted an open-source component scan to look for vulnerable versions of Apache Struts. This scan, however, did not identify any vulnerable versions “because the scan was run on the root directory, not the subdirectory where the Apache Struts was listed.”<sup>[2]</sup> The security team also deployed a new signature for their vulnerability scanner to scan externally facing systems but did not find any vulnerable instances in 958 externally facing IP addresses. Despite the fact that the tools and process failed to identify vulnerable systems, the GTVM team reminded responsible parties to upgrade their Struts libraries.

Attackers discover that the ACIS web application is using a vulnerable version of Apache Struts. Forensic analysis revealed that attackers likely discovered the vulnerability in March 2017 after it was publicly disclosed. However, it was not exploited until May 2017 when attackers executed remote code to upload approximately 30 web shells. A web shell is a malicious script that provides a backdoor for continued and convenient access to the compromised system. In addition to failing to identify the Struts vulnerability, the compromise was not detected. File integrity monitoring software could have detected the installation of 30 web shells.

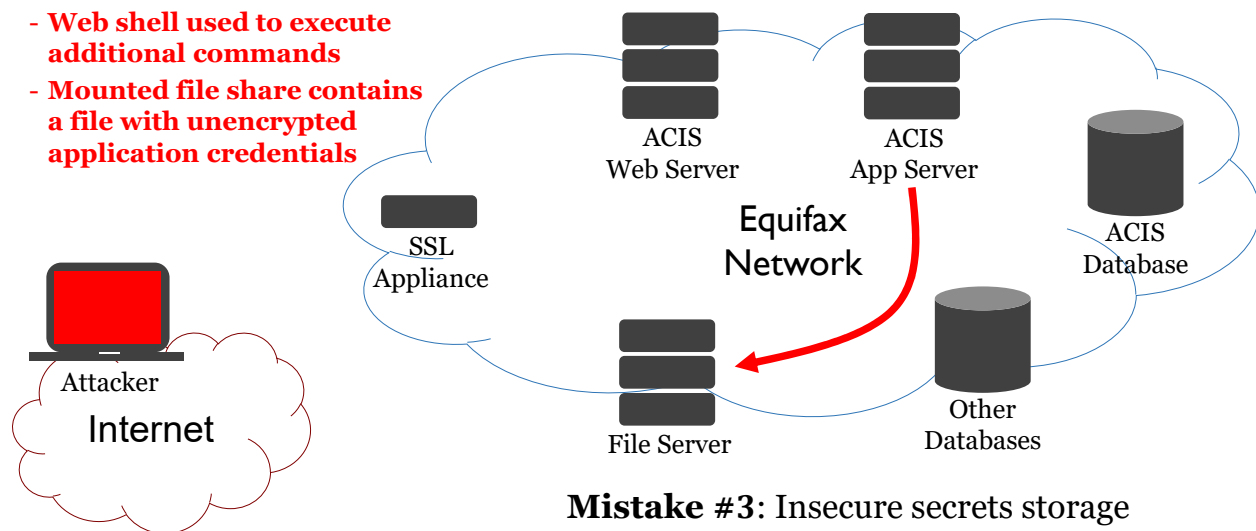
### References:

[1] <https://nvd.nist.gov/vuln/detail/CVE-2017-5638>

[2] <https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf>

## Credentials Discovered

- Web shell used to execute additional commands
- Mounted file share contains a file with unencrypted application credentials



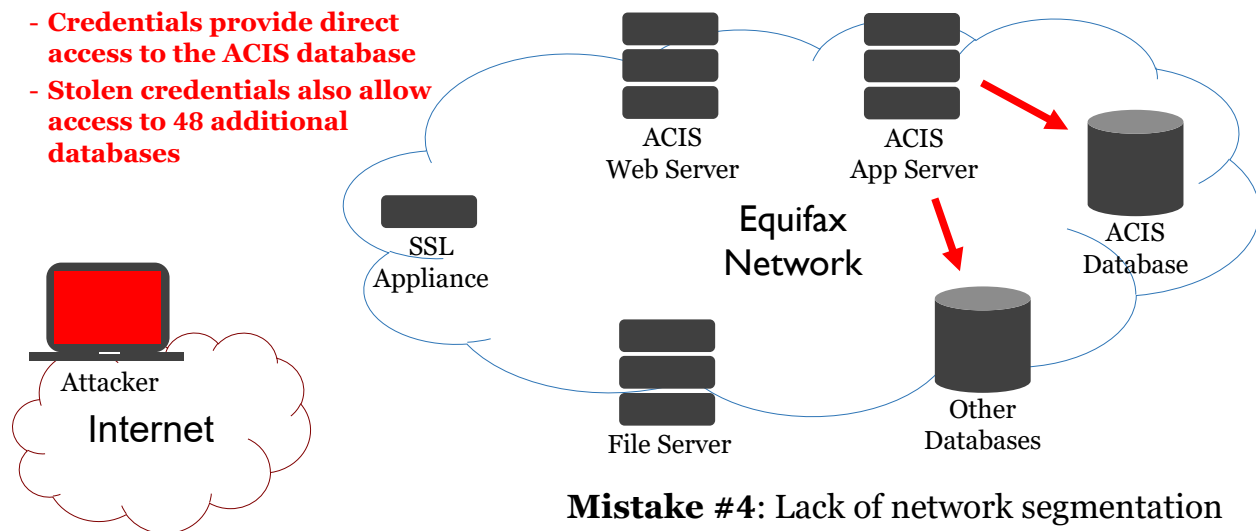
### Mistake #3: Insecure secrets storage

Using the web shell, the attacker maintains persistence and can conveniently execute additional commands to scan the system. The attacker identifies mounted file share on a remote file server. This share contained a configuration file containing unencrypted application credentials. Gold mine!

Storing sensitive secrets in this manner is a basic security mistake that leads to additional access.

## Data Access

- Credentials provide direct access to the ACIS database
- Stolen credentials also allow access to 48 additional databases



### Mistake #4: Lack of network segmentation

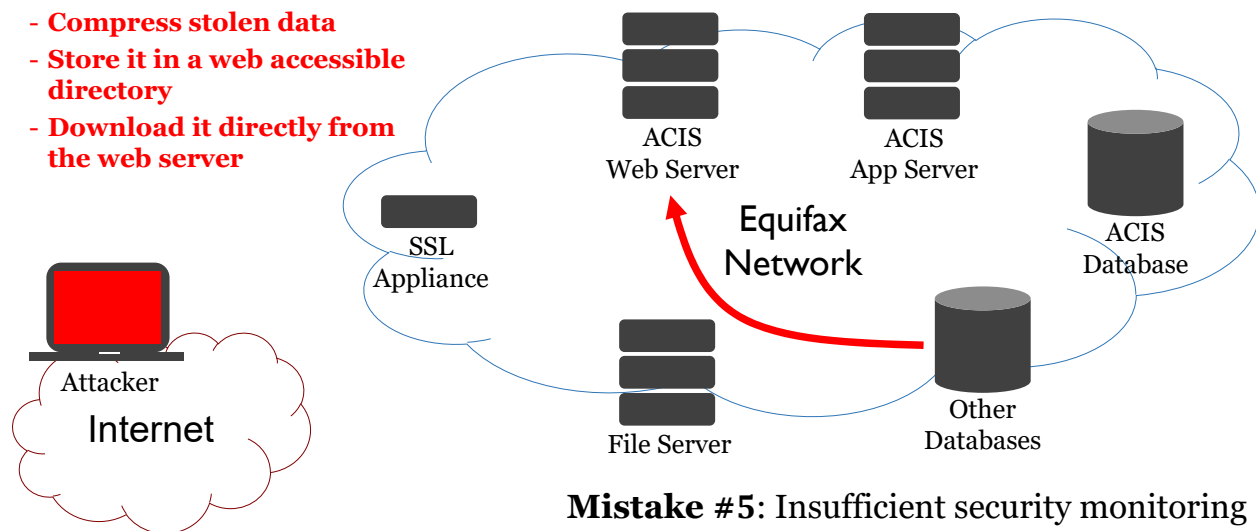
Using the newfound application credentials, the attacker accesses the three underlying databases associated with the ACIS application.

The attackers discovered that they were not only able to access the three ACIS databases but 48 additional databases that were not part of the ACIS system. Attackers ran 9,000 queries to discover tables with personally identifiable information (PII) and then ran additional queries to retrieve sensitive data.

The fact that the attackers were able to access 48 additional databases is an indication that there was a lack of network segmentation. The ability to run thousands of queries and retrieve large amounts of data also indicates there was insufficient security monitoring in place.

## Data Exfiltration

- Compress stolen data
- Store it in a web accessible directory
- Download it directly from the web server



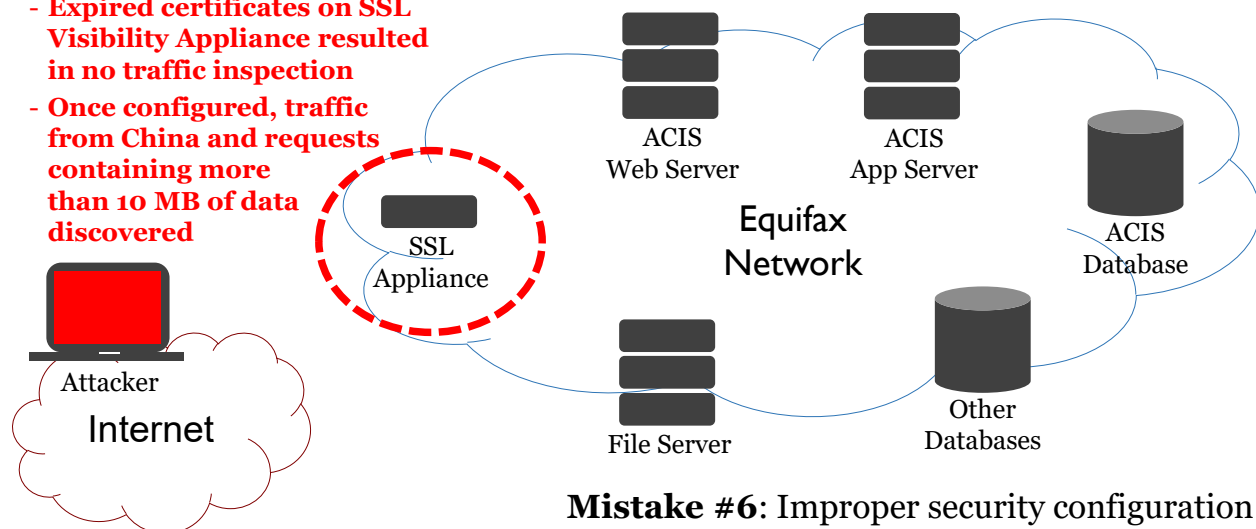
### Mistake #5: Insufficient security monitoring

The attackers stored sensitive data from the database into compressed files. These files were then placed in a web accessible directory for exfiltration. By using the `wget` tool, a simple utility to retrieve content from web servers, the attackers successfully transferred the files out of the Equifax network using an estimated 35 different IP addresses.

In total, attackers were in the Equifax network for 76 days conducting the attack. There was clearly insufficient security monitoring and an inability to detect malicious activity.

## Security Misconfiguration

- Expired certificates on SSL Visibility Appliance resulted in no traffic inspection
- Once configured, traffic from China and requests containing more than 10 MB of data discovered



### Mistake #6: Improper security configuration

Best practice is to utilize Secure Sockets Layer (SSL) / Transport Layer Security (TLS) to encrypt data in transit, especially for web applications such as ACIS. However, when data is encrypted in this manner, it cannot be analyzed for malicious activity. As a result, organizations often use a “SSL Visibility Appliance” to decrypt SSL/TLS traffic and send the traffic to security monitoring devices such as an Intrusion Detection System (IDS). For the SSL Appliance to function properly, it needs the SSL certificate for the specific application. In this case, the appliance was configured to let traffic continue to pass through even if the SSL certificate was expired. This prevented the malicious traffic from being inspected. According to the Congressional report, this misconfiguration existed for 19 months.<sup>[1]</sup>

In July 2017, the SSL Appliance was updated with 67 new SSL certificates, which allowed traffic to be properly inspected. Almost immediately, suspicious traffic was identified from China, along with requests containing more than 10 megabytes of data and image files associated with credit investigations. Further testing identified serious issues in the ACIS application, including SQL Injection and Insecure Direct Object Reference vulnerabilities that could be used to steal data from the database and bypass access controls.

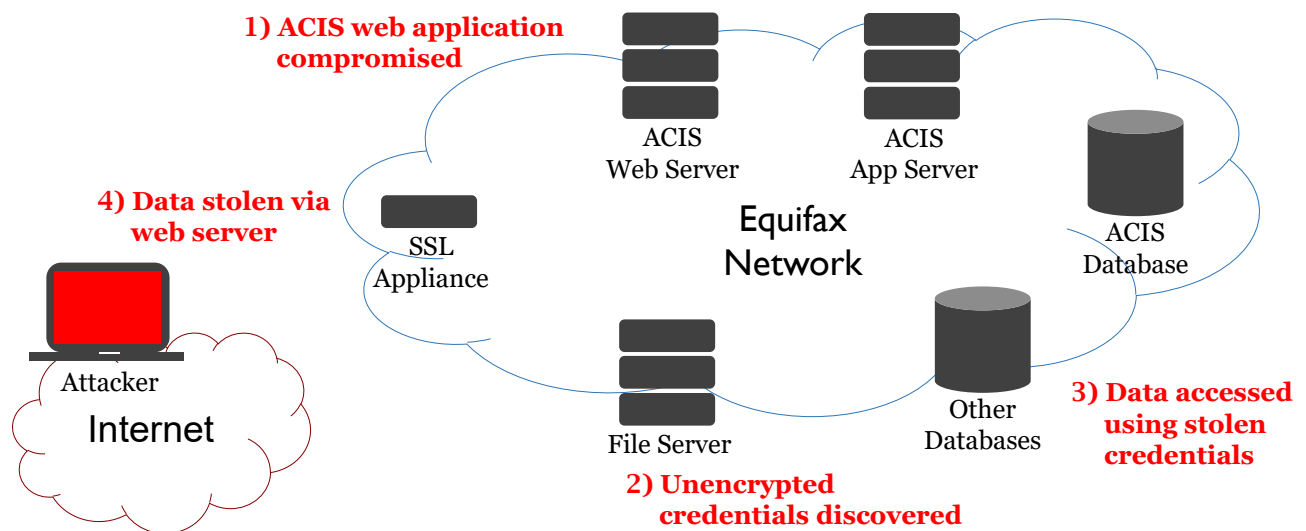
Further forensic analysis confirmed that stolen data likely contained PII. The ACIS application was subsequently shut down.

#### Reference:

[1] <https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf>



## Attack Summary



The attacker used knowledge of a remote code execution vulnerability in the Apache Struts framework to compromise the ACIS application. With access to the ACIS server, the attacker installed various web shells to maintain persistence and execute further commands. This led to the discovery of a mounted file share that contained a file with unencrypted application credentials. These credentials allow the attacker to access both the ACIS database as well as 48 additional databases that were not directly related to the application. After running various queries to retrieve data from the databases, the attacker compressed the information and stored it in a publicly accessible web directory. From there, the attacker retrieved the data from various systems around the world.

## Attacker Motivations

Motivation	Description
<b>Espionage</b>	State spying or industrial espionage for competitive advantage
<b>Fear</b>	Use of fear or duress
<b>Financial</b>	Theft of sensitive data for financial or personal gain
<b>Fun</b>	Activities conducted for fun, curiosity, or pride
<b>Grudge</b>	Retaliation based on a grudge or personal offense
<b>Ideology</b>	Actions based on ideology or in protest of a cause
<b>Convenience</b>	Actions conducted out of convenience or expediency
<b>Other</b>	"Some men just want to watch the world burn."

This slide lists this attacker's motivations defined in the VERIS framework. It is important to understand why attackers would want to target your organization. In some cases, there may be multiple motivations. In other cases, you may not be able to determine why you were targeted. This conversation between Bruce Wayne and his butler, Alfred Pennyworth, from the movie *The Dark Knight* illustrates this point:

- **Bruce Wayne:** Criminals aren't complicated, Alfred. Just have to figure out what he's after.
- **Alfred Pennyworth:** With respect, Master Wayne, perhaps this is a man that \*you\* don't fully understand, either. A long time ago, I was in Burma. My friends and I were working for the local government. They were trying to buy the loyalty of tribal leaders by bribing them with precious stones. But their caravans were being raided in a forest north of Rangoon by a bandit. So, we went looking for the stones. But in six months, we never met anybody who traded with him. One day, I saw a child playing with a ruby the size of a tangerine. The bandit had been throwing them away.
- **Bruce Wayne:** So why steal them?
- **Alfred Pennyworth:** Well, because he thought it was good sport. Because some men aren't looking for anything logical, like money. They can't be bought, bullied, reasoned, or negotiated with. Some men just want to watch the world burn.

Reference:

<http://m.imdb.com/title/tt0468569/quotes?qt=qt0507146>

## Section Summary

- Reviewed two cases of real-world attacks
  - To understand the tactics and motivations of two common threat actors
- Other threat actors have varied goals and motivations
  - Important to keep them in mind as you plan your defenses
    - Asset analysis
    - Threat analysis

In this section, we reviewed two cases of real-world attacks to understand the tactics and motivations of two common threat actors. It's important to keep these threat actors in mind as you plan your defenses. In the upcoming sections, we will discuss Asset Analysis and Threat Analysis. An understanding of attacker motivations and goals will be important to frame those discussions.

# 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 I

- Overview
  - Need for Strategic Planning
  - 30-60-90 Day Plan
    - Lab #1: CISO First Impression
- Decipher the Business
  - Historical Analysis
  - Values and Culture
  - Stakeholder Management
    - Lab #2: Relationship Management
  - Asset Analysis
  - Business Strategy
    - Lab #3: Strategy Map
- Decipher the Threats
  - Threat Actors
  - **PEST Analysis**
  - Threat Analysis

This page intentionally left blank.

## What Is PEST Analysis?

- Management tool to identify external forces that impact a particular market, industry, or country
- PEST stands for
  - Political: Government regulations and legal forces
  - Economic: Economic issues that have an impact on the organization
  - Social: Social and cultural environment
  - Technological: Impact of technology product or service
- Factors are usually beyond your control
  - Often present as threats
- Many variations of the tool
  - ETPS, STEP, STEEP, STEPE, PESTLE, STEPLE
  - PEST is by far the most widely recognized version

PEST analysis is a widely used management tool that enables identification and analysis of the external forces that are likely to impact your market or industry and therefore your organization. The acronym PEST stands for Political, Economic, Social, and Technological. These four classifications of forces help you understand the big picture of what your company is facing and should be considered when developing your security strategy.

The PEST acronym and forces have been translated into several variations over time, such as ETPS, STEP, STEEP, STEPE, PESTLE, and STEPLE. Despite the variations, the PEST version has proven to be more popular over time, and it's generally agreed that these headings and forces seem to be appropriate for most, if not all, situations.

Harvard professor Francis Aguilar is credited as the creator of PEST analysis. He created an environmental scanning tool called ETPS in his 1965 Harvard dissertation titled, "Formulating Company Strategy: Scanning the Environment," which later was published as *Scanning the Business Environment*. Aguilar discussed ETPS as a mnemonic for the four sectors of his taxonomy of the environment: Economic, Technical, Political, and Social.

A few years later, Arnold Brown, from the Institute of Life Insurance (in the United States), created a variation using the tool name STEP. Building on Aguilar's tool and his four factors, Brown's version stands for Strategic Trend Evaluation Process, which was his way of organizing the results of his environmental scanning. You can read more about this model in his *Supermanaging: How to Harness Change for Personal and Organizational Success* with Edith Weiner (New York: McGraw Hill, 1984).

A number of management philosophers and practitioners created variations as they attempted to add to the original four factors. As environmental issues gained global importance and businesses realized they needed to consider the impact on the environment or ecology, two more PEST variations were created by adding an *E*: STEEP analysis (Social, Technological, Economic, Ecological, and Political) and STEPE analysis (the Social, Technological, Economic, Political, and Ecological taxonomies).

The business world soon realized that legal matters were often derailing strategic plans, so an *L* was later added for Legal environmental scans, creating PESTLE and STEPLE.

One more variation of the PEST analysis encompasses ethical consideration and adds one more *E* to become STEEPLE. STEEPLE seems to be an all-encompassing form of PEST that ensures a thorough scanning of all possible external factors, but as we mentioned earlier, PEST is still by far the most popular and well-accepted form of the environmental analysis tool.

Additional history on PEST and PEST variations can be found here:

<https://www.brighthubpm.com/project-planning/101201-history-of-the-pest-analysis/>

## Why We Need to Do PEST Analysis

- To understand
  - The macro trends that affect the organization
    - How these trends affect the performance and activities of the business
    - Highlights areas of risk and opportunity
  - How security can respond, enable, and support these trends
    - Articulate cyber risk associated with macro forces
    - Understand how security can support business goals

It is important to understand the business goals and the vision and mission of your organization to avoid disconnects between security and business leaders. In this section, we will talk about the importance of understanding the market forces that affect your business, as these factors are driving the strategic decisions of your top leaders. Security leaders must create a broader strategy that will reach well beyond a security organization and traditional security controls. When you have the full picture of what is driving business decisions for your company, you can better understand how security can support business goals and in turn can build a more cohesive, comprehensive strategy with the business in mind.

PEST analysis helps you understand the macro trends of the external environment in which your company operates, and it provides an understanding of risks associated with market growth or decline and your company's position and potential direction. By understanding this environment, you can take advantage of the opportunities, minimize threats, and better understand how security can respond, enable, and support the business in dealing with these trends.

As you work your way through this PEST analysis process and ensure that all relevant and potentially important external forces have been identified, evaluated, and considered, you can easily highlight risks. In turn, you can factor contingency, mitigation, and/or remediation plans into your strategy to address these risks. Opportunities are also highlighted, and you should certainly leverage all opportunities and factor them into your strategy.

Effective use of the PEST analysis tool will ensure you are proactively aligned with the forces of change that impact your business. You will have a greater likelihood of success than if you do nothing and allow these forces to dictate your reactive response.

PEST analysis is often used with other analytical business tools like the SWOT analysis and Porter's Five Forces to give a clear understanding of a situation and related internal and external factors. We will discuss SWOT and Porter's Five Forces later in this course.

## PEST Analysis

- Four factors to consider when developing your strategic plan
- Equal analysis should be applied to each factor
- Revisit over time to ensure changes are captured

<b><u>P</u>olitical</b>	<b><u>E</u>conomic</b>
<b><u>S</u>ocial</b>	<b><u>T</u>echnological</b>

Four factors should be considered in your PEST (Political, Economic, Social, and Technological) analysis.

A couple of noteworthy keys to success: Equal analysis should be applied to each factor. And, during the initial brainstorming on this activity, don't discount any ideas because they may spur thinking that leads to the identification of hidden forces. Lastly, it's important for you to revisit your PEST analysis over time to ensure that all changes in the environment are captured and your strategy can be appropriately updated.

Following is a summary of each of the four factors:

- **Political** factors are government regulation and legal factors that affect the business environment and the trade market and will likely have a trickle-down impact on your company.
- **Economic** factors look at the overall health of the economy and how these factors influence companies, organizations, and decisions.
- **Social** factors look at cultural aspects of the market and how this affects the demand for a company's products and/or services.
- **Technological** factors look at how technology can either positively or negatively impact a business and the products and/or services they provide.



## Political

- Government regulations and legal forces
  - That affect the business environment and trade markets
- Common factors include
  - Political stability
    - War, terrorism, military invasion
    - Inter-country relationships
    - Elections
  - Tax guidelines
    - Tax rates and incentives
  - Trade restrictions
    - Anti-trust laws, tariffs
    - Favored trading partners
  - Legal
    - Intellectual property protection
    - Contract enforcement
    - Employment law
    - Wage legislation
  - Regulations
    - Industrial safety regulations
    - Consumer protection
    - Pricing regulations

Political factors are government regulations and legal factors that affect the business environment and trade market, and they will likely have a trickle-down impact on your company. Regulated companies such as financial, health care, critical infrastructure, and global companies may be more heavily influenced by political factors. Common forces addressed in this section include political stability, tax guidelines, trade restrictions, legal, regulations, and employment laws.

When a company invests money into setting up a facility in a region or country, political stability is obviously favored over instability. Political instability can impact everything from profits to the working conditions of employees. Think for a moment how the risk of a military invasion, war, or terrorism would be detrimental to running a business. Unless you are in the defense industry, the likelihood that your company would benefit from this type of instability is low.

Tax guidelines are another example of political factors that could be considered. In the United States, the federal government often uses tax incentives to partner with the private sector for economic development, such as building a facility in a low-income community or hiring underemployed workers to gain subsidies for investing in such communities. The leaders in your company may have included these forces in their business strategies and decisions.

Different countries react to a variety of factors in an attempt to influence trade; for example, a country may place tariffs on the cost of imported goods in an effort to protect domestic employment, consumers, and industries or national security; or these trade regulations and tariffs may be used as a retaliation. Anti-trust laws prohibit a variety of practices that restrain trade and some business practices, such as price-fixing conspiracies, corporate mergers that are likely to reduce the competitive nature of some markets, and predatory acts designed to achieve or maintain a monopoly. Microsoft, AT&T, and Standard Oil are companies that have been investigated for anti-trust practices.

Let's say your company invests heavily in research and development, where intellectual property protections may just be the difference between success and failure. Intellectual property laws deal with rules for protecting your legal rights to your inventions, designs, artistic work, trademark, and trade secrets. Contract enforcement, mandatory employee benefits, and wage legislation in various states and countries are all likely to impact your company to varying degrees.

Maintaining safe working conditions is a good business practice. It's generally demanded by employees and unions and is required by the government. For instance, the federal Occupational Safety and Health Administration (OSHA) governs workplace safety, no matter what industry you're in, and compliance is not optional. Other regulations that are likely to have government oversight are consumer protection and pricing regulations.

## Political: Examples

- **Estonian cyber attacks**
  - Targeted for relocating the Bronze Soldier statue and a Soviet era tank
  - Risk: Outages, panic, political instability
- **Intellectual property protection**
  - VMware ESX kernel source code leak
  - Risk: Identification of zero-day vulnerabilities, reduced customer trust
- **Federal Trade Commission (FTC)**
  - Settlement with Snapchat over deceptive practices
  - Risk: Increased government scrutiny and monitoring

The following are examples of organizations being affected by political factors.

The northern European country of Estonia was the victim of a cyber attack<sup>[1]</sup> launched in response to the relocation of a statue known as the Bronze Soldier of Tallin. This statue, originally called “The Monument to the Liberators of Tallin”, became a symbol to many in the country of Soviet oppression. As a result, the statue was moved from the center of the capital to the outskirts of the city. This resulted in protests, riots, and looting exacerbated by false Russian news claiming that the statue and Soviet graves were being destroyed. Over the course of two weeks banks, government agencies, and communications networks were taken offline via associated cyber attacks commonly attributed to the Russian government. Similarly, in 2022, Estonia was the target of the biggest cyber attacks<sup>[2]</sup> it had seen since the Bronze Soldier incident, sparked by the relocation of a Soviet era tank from a memorial celebrating the Russian army.

Hackers stole and published source code for the VMware ESX Server kernel online.<sup>[3]</sup> The source code was believed to be from an older version of software, but the risk still remained high because kernel code does not tend to change often. Attackers could use it to discover previously unknown vulnerabilities and potentially identify ways to “escape” from one of the most popular virtual machine technologies to get access to other systems within virtualized environments. This is just one example of the challenges that companies face in keeping some of their most valuable intellectual property secure.

In the United States, the Federal Trade Commission (FTC) investigates organizations that employ unfair or deceptive trade practices. In recent years, the commission's charter has expanded to include companies that fail to provide customers with reasonable security and data protections. For example, Snapchat, makers of a popular ephemeral messaging app, was found to have deceived users because certain “snaps,” or pictures, did not actually disappear as the company claimed.

Additionally, Snapchat failed to secure its Find Friends feature, resulting in a breach of 4.6 million usernames and phone numbers. As part of the settlement, Snapchat agreed to implement a comprehensive privacy program that will be monitored by an independent privacy professional for the next 20 years.<sup>[4]</sup>

References:

- [1] <https://www.bbc.com/news/39655415>
- [2] <https://www.nytimes.com/2022/08/18/world/europe/estonia-cyber-attack-russia.html>
- [3] <https://www.zdnet.com/article/hacker-leaks-vmware-esx-kernel-source-code-online/>
- [4] <https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were>

## Economic

- Examines the economic issues
  - That play a role in the company's success
- Common factors include
  - Consumer confidence
    - Consumer confidence index
    - Inflation rates
    - Unemployment rate
  - Interest and exchange rates
    - Credit rating and availability
  - Policies
    - Taxation and economic policies
    - Government spending
  - Economic stability
    - Economic growth
    - Business cycles
    - Disposable income
    - Commodity shortages
    - Potential for disruption of supply
    - Profit and growth trends
    - Investment levels
    - Market competition

Economic factors look at the overall health of the economy and how these factors influence companies, organizations, and their decisions. These forces include items like inflation, interest and exchange rates; the unemployment rate; economic policies; and economic stability. Economic factors have a high influence on business, regardless of the industry.

Inflation impacts businesses by increasing expenses such as rent or lease, utilities, and cost of materials used in production. A typical response to increased expenses is increased prices on products and services by the business to maintain profits. In addition to inflation, consumer confidence impacts business. Confident consumers have a tendency to spend more money than low-confidence consumers.

Many businesses rely on loans from banks or other financial institutions for financing, and interest rates impact business expense for companies with debt. High interest rates will also reduce consumer spending because people are less willing to take out loans on vehicles and homes, for example. Exchange rates also play an important role for companies that import or export goods because depreciated exchange rates will make export less expensive and appreciated exchange rates will be more expensive. Credit ratings affect debt obligation and security, preferred stock, and insurance companies.

The economy tends to follow a business cycle of economic booms followed by periods of stagnation or decline. During boom periods, jobs tend to be plentiful because companies need workers to keep up with demand. When unemployment is low, consumer spending tends to be high because most people have the income to spend, which helps drive growth. When unemployment is high, consumer spending tends to be low because unemployed people don't have excess income to spend.

Governments spend trillions of dollars per year through direct spending, which will help businesses such as construction companies, which may be contracted to build schools or libraries; engineering companies, which are contracted to build bridges and roads; and defense companies, which specialize in military systems.

Any fluctuation in spending by the government would have an impact in these areas. When tax rates increase for businesses, many companies respond by increasing prices on goods and services. Economic policies also affect wages. For example, an increase in minimum wage would benefit workers by providing them more money, but

it may be challenging for businesses to absorb the increased labor costs.

There are advantages to having a stable economy, such as increased productivity, improved efficiencies, and low unemployment. Common signs of instability in the economy would be recession, rising inflation, and volatile currency exchange rates, and we know this causes a decline in consumer confidence, stunted economic growth, and reduced international investments.

## Economic: Examples

- **Business cycles**
  - Annual tax filing deadline
  - Risk: Tax return fraud
- **Economic downturn**
  - Recession leading to layoffs
  - Risk: Disgruntled employees and corresponding malicious activity
- **Bank of Bangladesh hack**
  - SWIFT operator's credentials stolen and system hacked to steal \$81M
  - Risk: Monetary loss

The following are examples of organizations being affected by economic factors.

Every year, employees receive tax documents (for example, W-2 forms) that they use to file income tax returns. Attackers have started sending targeted spear phishing attacks to HR and payroll administrators while posing as company executives to harvest large numbers of W-2 forms. They may have simple messages such as "I want you to send me the list of W-2 copies of employee wage and tax statements; I need them in PDF file type. You can send it as an attachment. Kindly prepare the lists and email them to me asap."<sup>[1]</sup> By collecting this information, attackers then file fraudulent tax returns with the Internal Revenue Service (IRS) and state governments, requesting tax refunds that are then sent to attacker-controlled mailing addresses or accounts.

In poor economic times, customer confidence can be low. For organizations facing a downturn, layoffs might be necessary. The risk of unemployment is a major stress for many people and can lead to abnormal behavior. In these times, it's important to be cognizant of disgruntled employees conducting malicious activity to harm the organization.

The SWIFT system is used by over 11,000 financial institutions around the world to share data and financial information as well as initiative movement of funds across international borders. Attackers installed malware and obtained credentials of a SWIFT operator at the Bank of Bangladesh<sup>[2]</sup> and issued instructions to fraudulently transfer over \$900M. A large number of the fake payment orders were stopped but \$81M was successfully stolen and sent to accounts in Sri Lanka and the Philippines. This attack has been attributed to North Korea as they need money to support their failed economy.

### References:

[1] <https://www.irs.gov/uac/newsroom/irs-alerts-payroll-and-hr-professionals-to-phishing-scheme-involving-w2s>

[2] <https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know>

## Social

- Demographic and cultural aspects of the company's market
  - Examine consumer needs to determine what motivates them to purchase
- Main issues include
  - Customer demographics
    - Age, gender, race, family size, etc.
    - Population shifts
    - Occupations and earning capacity
    - Diversity
  - Cultural limitations
    - Cultures and religions
  - Lifestyle attitudes
    - Lifestyle changes
    - Living standards
    - Work week
  - Education
    - Education trends and standards
    - Skilled workforce availability
    - Career trends

Social factors look at cultural aspects of the market and how they affect the demand for a company's products and/or services; they also examine consumer needs and determine what incentivizes them to make purchases. Common forces addressed in this section include customer demographics, cultural limitations, lifestyle attitude, and education.

Many companies identify their key customers through various demographic traits such as age, gender, race, family size, and so on, and based on this, build their advertisements and promotions. For example, younger people are more likely to buy high-tech products than an older age group, and certain buying groups have more buying power than other groups. For example, the baby boomers are the single largest population segment. Business needs to be agile and responsive to population shifts and lifestyle changes.

Cultural limitations are important for a company to understand. For instance, when doing business with an affiliate from another country, you must consider the cultural differences such as language, body language, dress, religion, and traditions. You wouldn't want to schedule meetings during religious observations. Political influences past and present can affect the way a person or company does business. Some cultures have a strong sense of nationalism and government pride and may have a preference to doing business with like-minded companies.

Lifestyle attitudes include, for example, lifestyle changes, living standards and work week; quality and availability of employment; class disparity; quality and affordability of housing; hours of work required to purchase necessities; and access to health care. This category is often used to compare between states and countries, such as the lifestyle of the United States versus England or Utah versus New York.

When labor supply increases, there is more pressure on the wage rate. If the demand for labor does not keep up with the supply of labor, the wage rate will be depressed. This is harmful for employees in industries where higher education and training are not required. Industries with higher education and training requirements generally pay higher wages.



## Social: Examples

- COVID pandemic response
  - Shift to remote work
  - Risk: Lack of availability
- Global expansion
  - Hiring in other countries
  - Risk: Onboarding malicious individuals
- Executive peer pressure
  - Latest mobile device support
  - Risk: Unprepared for technology changes, unhappy users

The following are examples of organizations being affected by social factors.

In the early days of the COVID pandemic the world suddenly locked down and many people were told not to come into the office and instead work from home. To get access to work related systems employees would typically connect remotely to corporate infrastructure via VPN. However, these systems were often not provisioned with enough capacity to support 100% of the workforce working remotely and connecting simultaneously. Many organizations had to scramble to ensure that this part of their business continuity plan would actually be achievable by deploying additional capacity.

When a company grows globally, it must carefully consider its hiring practices. Do the same security controls, policies, and procedures afford the same protection in this new environment? Are there different assurances required to verify identity and conduct appropriate background checks? What is the threat level in the country overall? Onboarding a malicious individual that can harm the organization or damage its reputation can have severe consequences when social factors are not appropriately considered.

Another social factor is peer pressure, especially executive peer pressure. In the time that the BlackBerry was still the predominant mobile device used at various enterprises, many organizations struggled with the increasing use of iPhones that did not have equivalent security controls. Often, executives were clamoring for these new devices. This pressure left many organizations scrambling to support this new technology while trying to maintain the same level of control provided by other platforms.

## Technological

- How technology can
  - Impact the introduction of a product or service into a market
- The factors addressed in this section are
  - Technological advancement
    - Rate new discoveries
    - Manufacturing advances
    - New industries
    - Automated processes
  - Life cycle of technology
    - Rate of technology change
    - Rate of obsolescence
    - Waste removal/recycling
  - Technology innovation
    - Internet, cloud, mobile, IoT

Technological factors include how technology can either positively or negatively impact a business and the products and/or services they provide. Common forces addressed in this section include technology advancements, life cycle of technologies, and technology innovation.

The impact technology advancements have over daily life is increasing and expanding. As technology continues to evolve, businesses will also need to evolve to keep a competitive edge.

Technology lowers the cost of production and provides new products; it increases both productivity and efficiencies for businesses. The entire supply chain ecosystem encompassing equipment, manufacturing, distributors, and retailers is undergoing a business transformation in response to changing customer expectations, time-to-market demands, and intense global competition that is being dictated by the internet and mobile economies. Manufacturers must accelerate production cycles, and distributors must shorten delivery times, and much of this is accomplished by automated processes in industry.

Life cycles of technologies in companies generally always have some impact that should be considered. For example, new technology is expected to be integrated with legacy systems. The environmental factor related to waste removal and recycling will also have an impact on companies because there may be regulations and/or company policies that you will need to adhere to. With technology, you always need to consider sensitive data being wiped from things like servers, hard drives, and even printers to ensure your company's sensitive information remains secure.

The internet has allowed companies to find new ways of lowering operational costs on production of goods and services. Some companies may elect to outsource and/or take some of their functions offshore in the hope of driving innovation or lower labor cost. Some of the typical services that are taken offshore or outsourced are customer support, development, programming, manufacturing, data entry, research and development, creative services, and engineering.

## Technological: Examples

- **Connected medical devices**
  - Vice President Cheney disabled wireless capabilities in pacemaker
  - Risk: Death
- **Industrial Control Systems (ICS)**
  - Ukrainian power grid attack
  - Risk: Power outage, decreased confidence in government
- **Food and agriculture**
  - Attacks on smart farming technology
  - Risk: Crop and pricing manipulation, data theft or destruction

The following are examples of people or organizations being affected by technological factors.

Dick Cheney, former U.S. vice president, had the wireless capabilities in his pacemaker disabled due to a concern that it could be hacked in an assassination attempt. His doctor stated, "It seemed to me to be a bad idea for the vice president to have a device that maybe somebody on a rope line or in the next hotel room or downstairs might be able to get into."<sup>[1]</sup>

In December 2015, Ukrainian power distribution centers were hacked, leaving 225,000 Ukrainian residents without power.<sup>[2]</sup> The attack was carefully planned. Once the attack began, backup power supplies were disabled, and operator workstations were wiped using the KillDisk malware, making it harder to respond to the attack. Attackers also overwrote the firmware on substation serial-to-Ethernet converters, making them inoperable and unable to be controlled remotely. This meant that to get power back up, operations had to control breakers manually, reducing response time. Attackers even went so far as to conduct a telephone denial-of-service attack, flooding the call center with thousands of bogus phone calls and preventing legitimate callers from reaching the power companies. The telephone denial-of-service attack, in particular, could be evidence that a key motivation for the attack was to weaken the public's trust in power companies and the Ukrainian government.

Precision agriculture, or smart farming, includes the use of sensors to monitor crop growth to provide insight on how to farm more efficiently. These sensors provide data used to track and anticipate crop availability and pricing. With access to such data, attackers could exploit agriculture resources and market trends, causing farmers to take less optimal actions, such as planting the wrong crops or harvesting at less optimal times. Additionally, hackers could destroy or alter data about the use of pesticides or genetically modified organisms (GMOs) in protest.<sup>[3]</sup>

### References:

[1] <https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheney-s-heart/>

[2] <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

[3] <https://info.publicintelligence.net/FBI-SmartFarmHacking.pdf>

## Equifax PEST Example

### **Political**

- Increased privacy regulations and standards for security
  - GDPR, CCPA, FCRA, GLBA,
  - Data protection authority, FTC, CFPB oversight
- Reporting requirements
  - FTC, SEC, state reporting requirements

### **Economic**

- Increased fines for cybersecurity breaches
  - FTC fine of \$700m
    - Highest ever at time it was announced
    - 20% of prior year's annual revenue
  - UK ICO fine of £500k
    - Highest allowed pre-GDPR

### **Social**

- Cybersecurity seen as a core business functions
  - Need for clear authority and accountability for security
- Boards of Directors and C-Level executives taking more direct interest in security and privacy
- Desire for increased transparency and privacy

### **Technological**

- Industry moving to modern technology environments
  - Cloud infrastructure and software as a service
  - Plan to migrate away from antiquated legacy systems
- Need for foundational security best practices
  - Inventory, segmentation, logging, patching

Let's use the PEST tool to analyze the macro forces effecting Equifax.

### **Political**

From a larger Political perspective there is a global trend of increased privacy regulations such as the General Data Protection Regulation (GDPR) overseen by various data protection authorities and the California Consumer Privacy Act (CCPA). This in on top of existing privacy related requirements like the Fair Credit Reporting Act (FCRA) and Gramm-Leach Bliley Act (GLBA) that are the primary US federal laws regulating credit reporting agencies like Equifax. These laws are enforced by the Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB).

GLBA specifically requires the FTC to establish standards for security and confidentiality of customer information. The "Safeguards Rule" requires credit reporting agencies to maintain a comprehensive information security program that is appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. The FTC in particular has brought over 60 cases against companies for engaging in unfair and deceptive practices that fail to protect consumer data and over 100 actions against companies for violating FCRA. It shouldn't have been a surprise to Equifax that they might come under increased scrutiny given that they manage "1,200 times the data of the Library of Congress."

This oversight also comes with numerous reporting requirements. Equifax must report issues to the FTC, Securities and Exchange Commission (SEC), various state officials, and the Financial Services Information Sharing and Analysis Center (FS-ISAC).

### **Economic**

An obvious economic impact of security breaches to Equifax is the cost of responding and remediating breach related issues. In addition, there is a larger macro trend of increased fines for security and privacy violations. Equifax was fined \$700 million by the FTC for their security breach. This was the highest ever fine at the time it was issued and was the equivalent of 20% of the prior year's revenue. Since Equifax also lost data of UK citizens the Information Commissioner's Office (ICO), which is the UK data protection authority, fined Equifax £500,000. This is a relatively small fine but was the highest allowed since the breach occurred before the new GDPR fines of 4% of global turnover were introduced.

**Social**

There is a trend for more responsible practices related to security and privacy. This is driven by public interest and demands for increased transparency but also by the leaders within organizations after seeing how large breaches impact various organizations. As a result, cybersecurity is now being viewed as a core business function with the need to provide the ultimate security leader with appropriate authority for managing technology related risks. This includes defining clear lines of accountability for developing policy and the ability to execute on these policies.

**Technological**

Equifax, like many large enterprises, has a complex IT environment. Many critical systems are built on legacy technology and they were found to have “antiquated IT” related to various acquisitions. Larger industry trends are to move toward modern technology environments like cloud computing and software as a service platforms. While some of this work was being considered Equifax’s legacy environment was missing numerous foundation security controls like asset inventory, network segmentation, appropriate logging, and patch management.

**Reference:**

<https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf>

## In Summary

- **PEST analysis**
  - Is used to understand
    - What is driving business decisions
    - How market forces can affect business long-term
  - Will help you have more meaningful dialogue with business leaders
    - Articulate cyber risk associated with macro forces
    - How security can support business goals

It is important to understand business goals to avoid disconnects between security and business leaders. In this section, we discussed the importance of understanding the market forces that affect your business, as these are the factors that are driving the strategic decisions.

Security leaders must create broad strategies that reach beyond the security organization and traditional security controls. When you have the full picture of what is driving business decisions for your organization, you can better understand how security can support business goals and, in turn, build a more cohesive, comprehensive strategy with the business in mind. Articulating the cyber risk associated with forces affecting the business and defining potential responses to these risks will enable you to have more meaningful and successful dialog with your business leaders.

# CYBER42

## Round 1 Event #3

This page intentionally left blank.

# CYBER42

## Event #3 *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 I

- Overview
  - Need for Strategic Planning
  - 30-60-90 Day Plan
    - Lab #1: CISO First Impression
- Decipher the Business
  - Historical Analysis
  - Values and Culture
  - Stakeholder Management
    - Lab #2: Relationship Management
  - Asset Analysis
  - Business Strategy
    - Lab #3: Strategy Map
- Decipher the Threats
  - Threat Actors
  - PEST Analysis
  - **Threat Analysis**

This page intentionally left blank.

## Goals of This Section

- Understand how attackers work
  - By applying the Intrusion Kill Chain
- Learn how threat intelligence can
  - Create a feedback loop that can be used to disrupt attackers

In previous sections, we discussed *why* attackers want to target your organization and *what* assets they might be most interested in stealing. In this section, we discuss *how* attackers work and the steps they take to conduct attacks by analyzing the Intrusion Kill Chain. You will also learn how Cyber Threat Intelligence can be used to better understand attackers and disrupt their attacks.

## Risk Analysis

$$\text{Risk} = \text{Impact} \times \text{Likelihood}$$
$$\text{Risk} = \text{Impact} \times (\text{Vulnerability} \times \text{Threat})$$

- Security traditionally focused on vulnerability component of risk
  - Conventional tools like IDS, Antivirus, etc., are focused on vulnerabilities that inform the impact
- To fully understand risk, you must consider threat component
  - Analysis of threat actors and their motivations informs the likelihood of successful attacks

Risk is commonly defined as the combination of the impact and likelihood of an event. Another way to look at risk is to analyze the vulnerability (security vulnerabilities in your systems) and threat (attacker motivations) components.

Security has traditionally focused on the vulnerability component. Because critical vulnerabilities increase risk, much work has been done to mitigate and prevent vulnerabilities using tools like Intrusion Detection and Prevention Systems (IDS/IPS) and Antivirus as well as patching of important issues. This is certainly a good and valuable approach to reduce risk. However, many organizations struggle to keep up with zero-day exploits and unpatched systems.

To reduce risk, we must also focus on the threat component of risk. By analyzing threat actors and their motivations, we can reduce the likelihood of successful attacks.

## Threat Analysis

- To mitigate the threat component of risk, we need to
  - Acknowledge that traditional incident response methodology assumes an intrusion has already occurred
  - Understand the Tactics, Techniques, and Procedures (TTPs) of threat actors
  - Utilize Indicators of Compromise (IOC) to create intelligence-driven computer network defense
- Intrusion Kill Chain described in a seminal paper
  - "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain"
    - By Hutchins, Cloppert, and Amin

Traditional incident response methodology assumes that an intrusion has already occurred. How can the likelihood of successful intrusion be decreased, thereby reducing overall risk?

By understanding the Tactics, Techniques, and Procedures (TTPs) of threat actors, various Indicators of Compromise (IOCs) can be identified to create "intelligence-driven computer network defense." This approach was described in a seminal paper by Hutchins, Cloppert, and Amin and serves as the foundation for much of the modern work on threat analysis.<sup>[1]</sup>

Reference:

[1] <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>

## Intrusion Kill Chain (I)

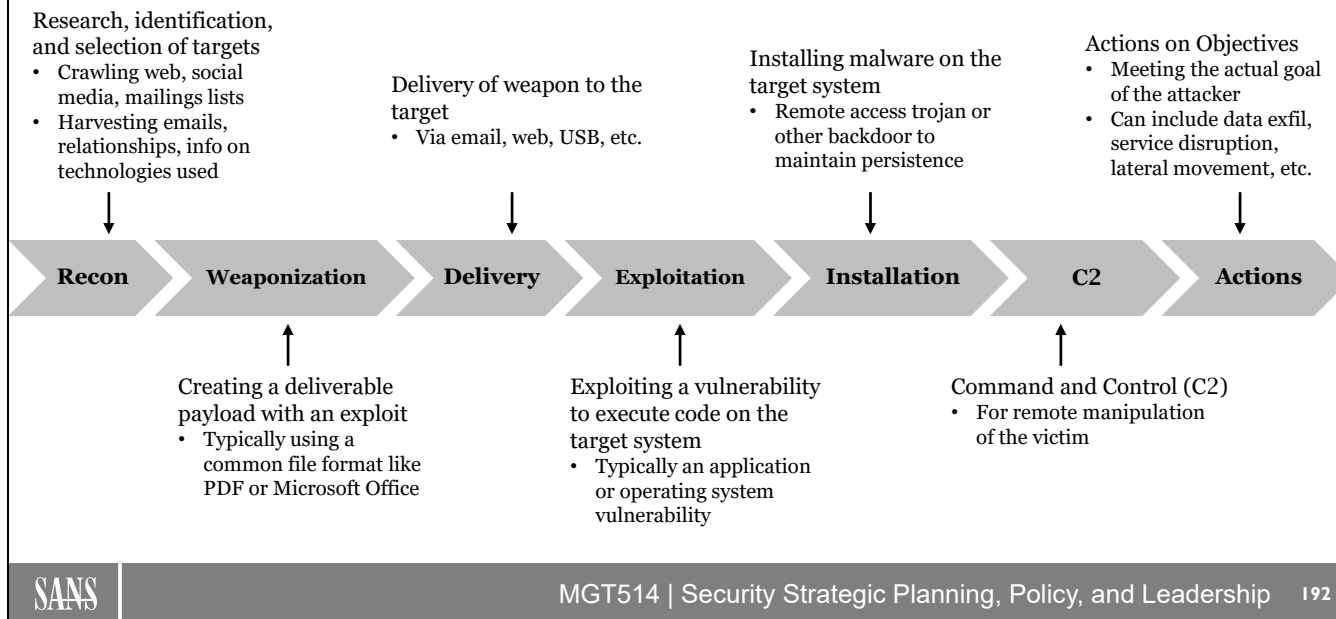
- Attackers must progress through each phase of the chain to achieve their goal
  - Breaking just one link in the chain disrupts the adversary
  - By understanding the attackers' perspective, defenders can gain an edge
    - Against even the most sophisticated attackers
    - Protect against zero-day exploits
      - Which is just one link in the chain



The Intrusion Kill Chain defines a seven-step process that attackers follow to achieve their goal. By breaking just one link in the chain, breaking just one step in the attack process, the defender can disrupt the adversary and stop the attack. Understanding in detail the attackers' perspective and approach enables defenders to gain an advantage against even the most sophisticated attackers. This means that you can more easily protect against zero-day exploits, which are just one phase of the overall Kill Chain (that is, Exploitation), by identifying and blocking attackers before they ever reach their ultimate goal in the final Actions step.

Note that "Intrusion Kill Chain" is also referred to as the "Cyber Kill Chain." However, this second term is trademarked by Lockheed Martin.

## Intrusion Kill Chain (2)



The seven steps of the Intrusion Kill Chain are as follows:

### Reconnaissance

In this phase, the attackers conduct research and identify targets. This can be accomplished by searching websites, social media, and mailing lists to harvest information about relationships and technologies used by the target.

### Weaponization

At this point, the attackers create a payload that can be delivered to the target. This is typically in PDF or Microsoft Office format and will leverage some of the information identified in the previous step to personalize the payload.

### Delivery

In this phase, the attackers deliver the payload to the target typically via email or the web. In some cases, it may also be delivered via USB.

### Exploitation

Once the payload is delivered, it will be executed to exploit a vulnerability on the target system.

### Installation

By gaining access via an exploited vulnerability, the attackers can now install malware on the system to maintain persistence.

### Command and Control (C2)

The backdoor allows for command and control capabilities that enable remote manipulation by the attackers.

### Actions on Objectives

Now, with access to the target system, the attackers can accomplish their ultimate goal. This can include data exfiltration, service disruption, or even lateral movement to other areas of the organization.

## Lockheed Martin Case Study

- Case study is taken from Lockheed Martin paper
  - By Hutchins, Cloppert, and Amin
- Over three weeks, Lockheed Martin detected three similar intrusion attempts
  - Email sent to five users
  - From an individual claiming to be an employee of a well-known aeronautics conference
  - Email contained a malicious PDF with legitimate content
    - First two attempts contained exploits for known but unpatched PDF vulnerabilities
    - The third attempt contained zero-day PowerPoint exploit

To illustrate how the Kill Chain works, we'll review the case study presented in the paper by Hutchins, Cloppert, and Amin.<sup>[1]</sup>

Over three weeks, Lockheed Martin detected three very similar intrusion attempts. All three intrusions attempted to gain access by delivering a malicious email to five different users at the company. The attackers had personalized these emails so that they appeared to contain valid communications in which the targeted users would be interested. For example, one email came from an individual claiming to be an employee of a well-known aeronautics conference in which the targeted user might be interested. These emails contained malicious PDF documents with this legitimate content. However, the malicious PDFs contained exploits for known but unpatched PDF vulnerabilities. A third email even contained a previously unknown zero-day PowerPoint exploit.

By analyzing various Indicators of Compromise (IOC), the Lockheed Martin team was able to successfully repel these attacks.

Reference:

[1] <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>

## Case Study Indicators of Compromise

Phase	Intrusion 1	Intrusion 2	Intrusion 3
<b>Reconnaissance</b>	Recipient List #1 Benign File: tcnom.pdf	Recipient List #2 Benign File: MDA_Prelim_09.pdf	Recipient List #3 Benign File: new.ppt
<b>Weaponization</b>	Trivial encryption algorithm		
	Key #1	Key #2	
<b>Delivery</b>	Subject: AIAA Technical Committees Email Body #1	Subject: 7 <sup>th</sup> Annual U.S. Missile Defense Email Body #2	Subject: Celebrities Without Makeup Email Body #3
	dn...etto@yahoo.com		ginette.c...@yahoo.com
	60.abc.xyz.215	216.abc.xyz.76	
<b>Exploitation</b>	CVE-2009-0658 [shellcode]		[PPT zero-day] [shellcode]
<b>Installation</b>	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEEXPLORE.hlp		
<b>C2</b>	202.abc.xyz.7 [HTTP request]		
<b>Actions</b>	N/A	N/A	N/A

This slide shows the Indicators of Compromise for the three different intrusion attempts against Lockheed Martin mapped to the seven phases of the Intrusion Kill Chain:

### Reconnaissance

In this phase, the attackers gather information about potential targets and search the internet for valid PDF files that can be used in the attack. In all three intrusion attempts, the attackers utilized different recipient lists and originally benign files.

### Weaponization

In this phase, the attackers modify the benign files to create a payload with an exploit. In the first two intrusion attempts, the attackers utilized the same encryption key but changed to a different key in the third attempt. However, an important element noted by the Lockheed Martin team was the repeated use of the same trivial encryption algorithm across all three intrusion attempts. This was one of the valuable Indicators of Compromise that helped the team detect and block the attacks.

### Delivery

In all three intrusions, the attackers attempted to use email to deliver the weaponized PDFs. In all three cases, the attackers utilized different email subject lines and body text. However, in two of the cases, the same target user and source IP addresses were utilized. This information provided some clues that the emails were actually part of an attack.

### Exploitation

In the first two intrusion attempts, the attackers utilized the same known but unpatched PDF vulnerability (CVE-2009-0658). In the third attempt, the attackers utilized a previously unknown zero-day PowerPoint vulnerability.

Normally, this would result in a successful attack. But, because other Indicators of Compromise retrieved from the Weaponization and subsequent Installation and C2 phases helped identify these emails as actual intrusions; even the zero-day vulnerability was successfully blocked.



**Installation**

All three intrusions attempted to install the same malware (fssm32.exe, IEUpd.exe, IEXPLORE.hlp) on the target system. This was an obvious Indicator of Compromise that helped detect and block the attack.

**Command and Control (C2)**

All three intrusions also attempted to have the malware connect back to the same command and control server (202.abc.xyz.7) over HTTP. This was another obvious Indicator of Compromise.

**Actions on Objectives**

Because all three intrusion attempts were successfully identified by analyzing reused IOCs, they were all blocked, which prevented the attackers from achieving their ultimate goal (that is, Actions on Objectives).

## Threat Analysis

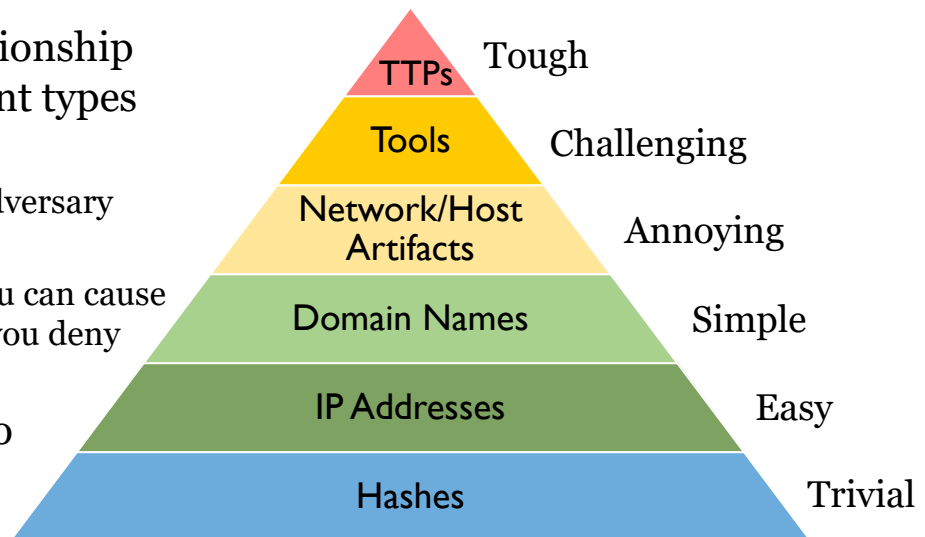
- Threat analysis based on Kill Chain indicators
  - Creates an intelligence feedback loop
    - "Enabling defenders to establish a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt"
  - Forces the attacker to make constant adjustments to Tactics, Techniques, and Procedures (TTPs)
    - Prevents attackers from reusing tools and infrastructure
    - Increases the cost of a successful intrusion by causing attackers to change every phase of the operation
  - Results in an increased level of resilience
    - By utilizing indicators across the entire Kill Chain
    - Instead of focusing only on post-compromise indicators

Analyzing the Lockheed Martin case highlights that threat analysis based on the Kill Chain and corresponding Indicators of Compromise (IOCs) can help defenders create an intelligence feedback loop that establishes "a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt."

This effort forces the attackers to make constant adjustments to their Tactics, Techniques, and Procedures (TTPs) and increases the cost of a successful intrusion. Instead of being able to reuse attack infrastructure and tools, the attackers now have to change every phase of their operation to avoid detection. This drastically increases the effort required by attackers and results in an increased level of resilience. By understanding that attackers leave evidence of an attack even before the compromise itself, defenders can gain an edge against even the most sophisticated adversaries.

## Pyramid of Pain

- Highlights relationship between different types of indicators
  - Used to detect adversary activities
  - Levels of pain you can cause the adversary if you deny indicators
- By David Bianco



The Lockheed Martin case study highlighted how even simple indicators like malware hashes and IP addresses can be useful sources of information. However, David Bianco, in his Pyramid of Pain, points out that those indicators are very trivial and easy for adversaries to alter.<sup>[1]</sup> The Verizon Data Breach Investigations Report (DBIR) states that 99% of malware hashes are seen for just 58 seconds or less. Attackers matured their capabilities as defenders have improved their defenses. The Pyramid of Pain underscores the need to make it more challenging for attackers by identifying harder to change indicators such as network/host artifacts, tools, and detailed tactics and techniques.

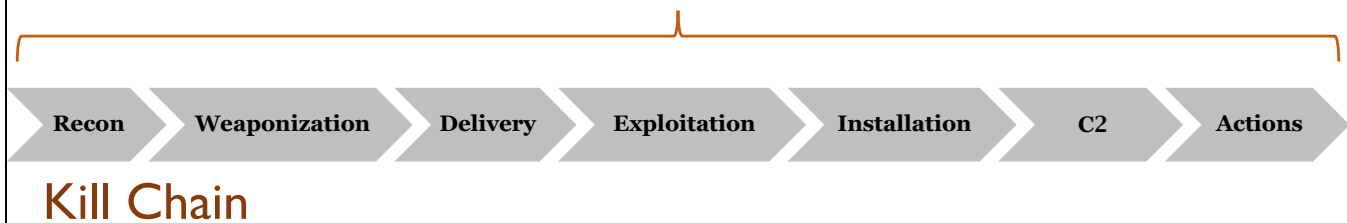
Reference:

[1] <http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

## MITRE ATT&CK Overview

# MITRE ATT&CK™

- **Adversarial Tactics, Techniques, & Common Knowledge**
  - Focus on actionable techniques, detection, and mitigations
  - Provides additional details beyond the traditional Kill Chain



SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

198

MITRE ATT&CK is a “globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.”<sup>[1]</sup> It strives to make threat analysis even more actionable by focusing exactly on how adversaries gain access and what they do once they obtain access.

The Kill Chain provides a high-level view of an attack. MITRE ATT&CK, on the other hand, focuses on how adversaries actually interact with various systems. It was originally created to document TTPs that advanced persistent threats used against Windows enterprise networks. Based on public reporting, it takes the behavior of adversary groups, like APT3, and maps out their specific tactics and techniques.

ATT&CK provides actionable details for every phase of the Kill Chain from Reconnaissance to Actions on Objectives. The original version of ATT&CK only focused on the exploitation phase (Delivery and beyond) while PRE-ATT&CK focused on attacker activities before access was gained (Reconnaissance and Weaponization). However, the latest version of ATT&CK moved the former PRE-ATT&CK domain into ATT&CK proper.

This means that ATT&CK helps you answer the following questions along the entire attack lifecycle:

Are there any signs that we are being targeted?

What are adversaries doing to select a target and gather information?

How are they launching their campaigns?

What are they trying to accomplish?

Reference:

[1] <https://attack.mitre.org>

# ATT&CK Matrix for Enterprise

Tactics	Source Development Techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Gather Victim Host Information (4)	Infrastructure (6)	Compromise Accounts (2)	Scripting Interpreter (8)	Manipulation (4)	Control Mechanism (4)	Mechanism (4)	Credentials from Password Storm (3)	Application Window Discovery	Remote Services	Data (3)	Protocol (4)	Exfiltration (1)	Removal
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Exploitation for Credential Access	Browser Bookmark Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Network Information (6)	Develop Capabilities (4)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Cloud Infrastructure Discovery	Lateral Tool Transfer	Automated Collection	Removable Media	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Org Information (4)	Establish Accounts (2)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (3)	Boot or Logon Initialization Scripts (3)	Desktop/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Encoding (2)	Data Manipulation (3)	Data Manipulation (3)
Phishing for Information (3)	Obtain Capabilities (6)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement (2)
Search Closed Sources (2)	Replication Through Removable Media	Supply Chain Compromise (3)	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (2)	Domain Trust Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Open Technical Databases (5)	Trusted Relationship	System Services (2)	Software Deployment Tools	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Modify Authentication Process (4)	File and Directory Discovery	Software Deployment Tools	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Websites/Domains (2)	Valid Accounts (4)	User Execution (2)	Windows Management Instrumentation	Event Triggered Execution (15)	Group Policy Modification	Group Policy Modification	Network Sniffing	Network Share Discovery	Taint Shared Content	Data from Local System	Fallback Channels	Ingress Tool Transfer	Firmware Corruption
Search Victim-Owned Websites				External Remote Services	Hijack Execution Flow (11)	Impair Defenses (7)	OS Credential Dumping (8)	Network Sniffing	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
				Hijack Execution Flow (11)	Process Injection (11)	Indicator Removal on Host (6)	Steal Application Access Token	Peripheral Device Discovery		Data from Network Shared Drive	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (2)
				Implant Container Image	Scheduled Task/Job (6)	Indirect Command Execution	Steal Web Session Cookie	Permission Groups Discovery (3)		Data Staged (2)	Non-Standard Port	Resource Hijacking	System Shutdown/Reboot
				Office Application Startup (4)	Valid Accounts (4)	Masquerading (6)	Two-Factor Authentication Interception	Process Discovery		Email Collection (3)	Proxy (4)	Service Stop	
				Pre-OS Boot (3)	Modify Authentication Process (4)	Modify Cloud Compute Infrastructure (4)	Unsecured Credentials (8)	Query Registry		Input Capture (4)	Remote Access Software	Traffic Signaling (1)	
				Scheduled Task/Job (6)	Modify System Registry	Modify System Image (2)		Software Discovery (1)		Man-in-the-Browser	Web Service (3)		
				Server Software Component (3)	Modify Network Boundary Bridging (1)			System Information Discovery		Screen Capture			
				Traffic Signaling (1)				System Network Connections Discovery		Video Capture			
				Valid Accounts (4)									

The ATT&CK Matrix for Enterprise is a central repository for TTPs. It seeks to answer, “What does an attacker do to achieve their goals?”

Tactics are the adversary’s technical goals. WHY they engage in a specific activity. At the time of writing, ATT&CK defined 14 Tactics. These items are in the first row of the table above: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact.

Techniques are how the adversary’s technical goals are achieved. WHAT they do. At the time of this writing, ATT&CK defined hundreds of different Techniques. Each technique is associated with one or more Tactics as represented above. Some example techniques include Exploit Public Facing Application, Account Manipulation, Brute Force, and Account Discovery. In the latest version of ATT&CK, MITRE introduced sub-techniques which describe specific implementation of techniques in more detail. Example sub-techniques include Additional Cloud Credentials, Add Office365 Global Administrator Role, and SSH Authorized Keys which are all part of the Account Manipulation technique.

Procedures are specific implementations of various Techniques.

## ATT&CK Technique Example

MITRE | ATT&CK®



### TECHNIQUES

Server Software Component ^

SQL Stored Procedures

Transport Agent

**Web Shell**

IIS Components

Traffic Signaling v

Valid Accounts v

Privilege Escalation v

Defense Evasion v

Credential Access v

Discovery v

Lateral Movement v

## Server Software Component: Web Shell

### Other sub-techniques of Server Software Component (4) ^

ID	Name
T1505.001	SQL Stored Procedures
T1505.002	Transport Agent
<b>T1505.003</b>	<b>Web Shell</b>
T1505.004	IIS Components

Adversaries may backdoor web servers with web shells to establish persistent access to systems. A

ID: T1505.003

Sub-technique of: **T1505**

①Tactic: Persistence

①Platforms: Linux, Windows, macOS

①System Requirements: Adversary access to Web server with vulnerability or account to upload and serve the Web

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership

200

Web Shell is just one example of a sub-technique defined in ATT&CK (part of the Server Software Component technique). Along with a description, the web page also describes the associated Tactics (Persistence).<sup>[1]</sup> Remember that the Tactic is the WHY. The adversary's goal is not to install a Web Shell alone. It is to do things like gain Persistence or conduct Privilege Escalation.

The web page also has detailed references on the Procedures used by various adversary groups related to a particular Technique. Mitigations and Detections are also defined. For strategic planning, we are very interested in the Mitigations and Detections because they inform how we can plan to put appropriate defenses in place based on real-world attacker activity.

Reference:

[1] <https://attack.mitre.org/techniques/T1100>

**ATT&CK Navigator**

Equifax x +

selection controls layer controls technique controls

Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques
Active Scanning (1/2)	Obtain Capabilities (0/6)	Exploit Public-Facing Application (0/1)	Command and Scripting Interpreter (0/18)	Server Software Component (1/3)	Valid Accounts (0/4)	Impair Defenses (1/7)	Unsecured Credentials (1/4)	Network Service Scanning (0/4)	Exploitation of Remote Services (0/2)	Archive Collected Data (0/3)	Application Layer Protocol (1/4)	Exfiltration Over Alternative Protocol (1/3)
Search Victim-Owned Websites (0/4)	Acquire Infrastructure (0/5)	Valid Accounts (0/4)	Exploitation for Client Execution (0/2)	Valid Accounts (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Network Share Discovery (0/3)	Internal Spearphishing (0/2)	Data Staged (0/2)	Communication Through Removable Media (0/2)	Automated Exfiltration (0/1)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Drive-by Compromise (0/2)	Inter-Process Communication (0/2)	Account Manipulation (0/4)	Access Token Manipulation (0/5)	Abuse Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Account Discovery (0/4)	Lateral Tool Transfer (0/2)	Automated Collection (0/2)	Data Encoding (0/2)	Data Transfer Size Limits (0/1)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services (0/2)	Native API (0/2)	BITS Jobs (0/4)	Boot or Logon Autostart Execution (0/12)	Deobfuscate/Decode Files or Information (0/5)	Exploitation for Credential Access (0/3)	Application Window Discovery (0/2)	Remote Service Session Hijacking (0/2)	Clipboard Data (0/2)	Data Obfuscation (0/3)	Exfiltration Over C2 Channel (0/1)
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions (0/2)	Scheduled Task/Job (0/8)	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Direct Volume Access (0/2)	Forced Authentication (0/2)	Browser Bookmark Discovery (0/2)	Remote Services (0/6)	Data from Cloud Storage Object (0/2)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Shared Modules (0/2)	Browser Extensions (0/4)	Create or Modify System Process (0/4)	Execution Guardrails (0/1)	Input Capture (0/4)	Cloud Infrastructure Discovery (0/2)	Replication Through Removable Media (0/2)	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)
Phishing for Information (0/3)	Replication Through Removable Media (0/2)	System Services (0/2)	User Execution (0/2)	Compromise Client Software Binary (0/15)	Event Triggered Execution (0/15)	File and Directory Permissions Modification (0/2)	Man-in-the-Middle (0/2)	Cloud Service Dashboard (0/2)	Software Deployment Tools (0/2)	Data from Information Repositories (0/2)	Fallback Channels (0/2)	Exfiltration Over Web Service (0/2)
Search Closed Sources (0/2)	Supply Chain Compromise (0/3)	Trusted Relationship (0/2)	Windows Management Instrumentation (0/2)	Create Account (0/3)	Exploitation for Privilege Escalation (0/4)	Group Policy Modification (0/2)	Modify Authentication Process (0/4)	Domain Trust Discovery (0/2)	Taint Shared Content (0/2)	Data from Local System (0/2)	Ingress Tool Transfer (0/2)	Exfiltration Over Web Service (0/2)
Search Open Technical Databases (0/5)				Create or Modify System Process (0/4)	Group Policy Modification (0/2)	Hide Artifacts (0/7)	OS Credential Dumping (0/8)	File and Directory Discovery (0/2)	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive (0/2)	Multi-Stage Channels (0/2)	Scheduled Transfer (0/2)
Search Open Websites/Domains (0/2)				Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Indicator Removal on Host (0/6)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing (0/3)	Peripheral Device Discovery (0/3)	Email Collection (0/3)	Non-Application Layer Protocol (0/2)	Transfer Data to Cloud Account (0/1)
				External Remote Services (0/11)	Scheduled Task/Job (0/6)	Indirect Command Execution (0/6)	Steal Web Session Cookie (0/4)	Password Policy Discovery (0/3)	Permission Groups Discovery (0/3)	Input Capture (0/4)	Non-Standard Port (0/2)	
				Hijack Execution Flow (0/11)	Implant (0/11)	Masquerading (0/6)		Process Discovery (0/3)		Man in the Browser (0/4)	Proxy (0/4)	

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership 201

ATT&CK Navigator is a free, open-source tool hosted by MITRE on GitHub<sup>[1]</sup>. It allows you to navigate, visualize, and annotate attack techniques. You can use it online or deploy it locally in your environment. There is functionality to create multiple layers; download data in JSON, Excel, or image format; create various filters; and color code attack techniques. Katie Nickels has a great “Introduction to ATT&CK Navigator” video<sup>[2]</sup> that is only 12 minutes long.

The above highlights the Techniques that were used (or were leveraged) in the Equifax breach that was discussed earlier. In the *Reconnaissance* phase, the attacker *Searched for Victim-Owned Websites* and conducted *Active Vulnerability Scanning* to discover the issues in the ACIS application. Once a vulnerability was discovered, the attacker used a tool that they had previously obtained. Gaining *Initial Access*, the attacker *Exploited a Public Facing Application* with the Apache Struts vulnerability. Based on that initial access, a *Web Shell (Server Software Component)* was installed to maintain *Persistence*. From there, *Privilege Escalation* was conducted by identifying and using *Valid Accounts* discovered on a file share (e.g., *Credentials in Files*). To *Discover* additional databases to access the attack, they likely conducted *Network Service Scanning* and *Moved Laterally* within the environment by performing *Exploitation of Remote Services*. The attacker *Collected* the data by *Archiving* then *Staging* it and, finally, *Exfiltrated it Over an Alternative Protocol*. All of these activities *Evaded Detection* because security tools were inadvertently disabled (note that the attacker in the Equifax attack did not have to *Impair Defenses* or *Disable or Modify Tools* directly as they were already misconfigured).

To get familiar with ATT&CK Navigator, you can upload the Equifax attack file shown above. A sample file called `Navigator Example.json` is online in the course Digital Download Package (available at [mgt514.com](http://mgt514.com)) in the Section 1 -> Threat Analysis -> ATT&CK directory. Once you have the file, go to the online ATT&CK Navigator tool, select “Open Existing Layer”, then “Upload from local”, and choose the JSON file to upload.<sup>[1]</sup> Then you will be able to see the same Techniques highlighted above. Feel free to experiment with the different options in the toolbar.

#### References:

[1] <https://mitre-attack.github.io/attack-navigator>

[2] <https://youtu.be/pcclNdwG8Vs>



## ATT&CK Use Cases

- **Improve Detection**
  - Develop analytics to detect the adversary
- **Leverage Threat Intelligence**
  - Structure, compare, and analyze threat intelligence
- **Emulate Adversaries**
  - Allow red teams to emulate threats and plan operations
- **Prioritize Defenses**
  - Assess capabilities and drive engineering decisions for detection, response, and prevention

ATT&CK has four common use cases or scenarios where it provides benefits to your security team.

### **Detection and Analytics**

Since ATT&CK is based on real-world observations of adversary tactics and techniques, it can be used to develop analytics to detect attackers. By identifying gaps in your detection coverage, you can be better prepared for common attacks. See the post “Getting Started with ATT&CK: Detection and Analytics” for more information.<sup>[1]</sup>

### **Threat Intelligence**

ATT&CK provides a structure to more easily compare, analyze and share threat intelligence to build threat-informed defenses. See the post “Getting Started with ATT&CK: Threat Intelligence” for more information.<sup>[2]</sup>

### **Adversary Emulation and Red Teaming**

ATT&CK provides a valuable way to structure adversary emulation, red team, and purple team activities. Defenders can mimic known adversaries by incorporating threat intelligence to define specific actions, tactics, and techniques that testers should use. See the post titled “Getting Started with ATT&CK: Adversary Emulation and Red Teaming” for more information.<sup>[3]</sup>

### **Prioritize Defenses**

The post titled “Getting Started with ATT&CK: Assessments and Engineering” refers to this use case as “Assessments and Engineering” and states that ATT&CK can help 1) assess how defenses stack up to techniques in ATT&CK; 2) identify high priority gaps; 3) build defenses to fill those gaps.<sup>[4]</sup> As a result, the author prefers to refer to this use case as “prioritizing defenses.” This is exactly what strategic planning helps you prioritize!

#### References:

[1] <https://medium.com/mitre-attack/getting-started-with-attack-detection-a8e49e4960d0>

[2] <https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f>

[3] <https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3>

[4] <https://medium.com/mitre-attack/getting-started-with-attack-assessment-cc0b01769cb4>



## ATT&CK Data Sources

- ATT&CK defines various data sources to improve detection
  - Process monitoring and information
  - File monitoring
  - API monitoring
  - Packet capture
  - Windows logs
  - Authentication logs
  - Netflow
  - Network protocol analysis
  - Binary file metadata
  - Network intrusion detection system
  - Malware reverse engineering
  - Network device logs
  - Antivirus
  - Application logs
  - Data loss prevention
  - Web logs and web proxy
  - Email gateway
  - Web application firewall logs
  - DNS records
  - Detonation chamber

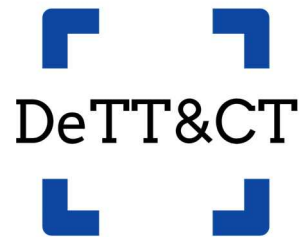
To assess our gaps and prioritize areas of improvement, we first need to understand where data is gathered in our environment. The following is a list of the data sources defined in ATT&CK. The number to the left of each item represents the number of Techniques, at the time of this writing, that can be detected with the corresponding data source. As you can see, some data sources are richer sources of information for the Techniques seen in ATT&CK. For example, process monitoring and associated process information like command-line parameters provide insight into a large number of Techniques.

169	Process monitoring
97	Process command-line parameters
97	File monitoring
43	API monitoring
39	Process use of network
36	Packet capture
36	Windows Registry
28	Authentication logs
27	Netflow/Enclave netflow
22	Network protocol analysis
22	Windows event logs
18	DLL monitoring
18	Binary file metadata
13	Loaded DLLs

9	SSL/TLS inspection
9	Network intrusion detection system
9	System calls
9	Malware reverse engineering
8	Network device logs
7	Kernel drivers
7	Antivirus
6	Application logs
6	Data loss prevention
4	Web logs
4	Services
4	PowerShell logs
4	Email gateway
4	Windows Error Reporting
4	Web proxy
4	User interface
4	Host network interface
3	Web application firewall logs
3	BIOS
3	MBR
3	Third-party application logs
2	Sensor health and status
2	Component firmware
2	DNS records
2	Detonation chamber
2	Mail server
2	Environment variable
1	Asset management
1	Browser extensions
1	Access tokens
1	Digital certificate logs
1	Disk forensics
1	WMI Objects
1	VBR
1	Named Pipes
1	EFI

## DeTT&CT

- **Detect Tactics, Techniques & Combat Threats**
  - Consists of scoring tables, YAML administration files, and a Python tool
  - By Marcus Bakker and Ruben Bouman
- Used to improve detection and response
  - Data log source quality
  - Visibility coverage
  - Detection coverage
  - Coverage prioritization
  - Defense identification



DeTT&CT is a tool created by Marcus Bakker (@bakk3rm) and Ruben Bouman (@rubenb\_2) that builds upon ATT&CK with the goal of providing a useful approach for improving detection and response.<sup>[1]</sup> Specifically, the tool provides a scoring table that helps you analyze the following:

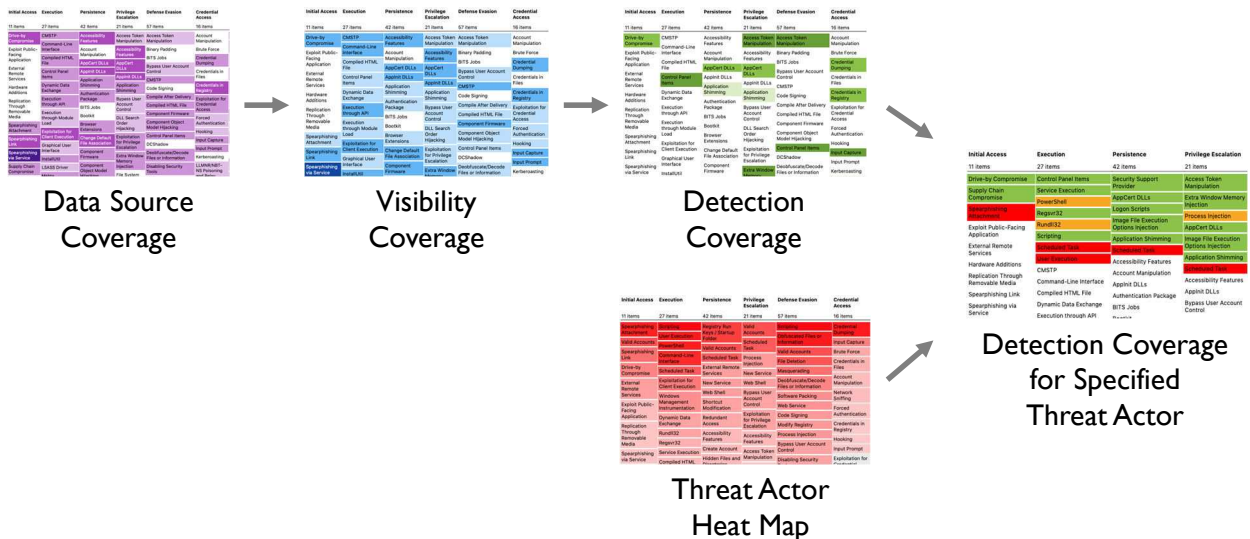
- **Data source quality:** Do I have good data? This is based on device completeness, data field completeness, timeliness, consistency, and retention measures.
- **Visibility coverage:** What percentage of data sources are available? This is based on scoring of no visibility, Minimal visibility (to see one aspect of a technique's procedures), Medium visibility (to see more aspects of a technique's procedures), Good visibility (to see almost all known aspects of a technique's procedures), and Excellent visibility (to see all aspects of a technique's procedures).
- **Detection coverage:** How well are you doing detecting the techniques? This is based on degree of detection, timing, coverage of the technique, opportunities to bypass detection, false negative, and false positive measures.

Based on your scores, you then create YAML administration files that can then be used by the Python tool to generate different outputs that are visualized in ATT&CK Navigator. This helps you prioritize areas where you might want increased coverage as well as providing input to identify defenses. For more information on using DeTT&CT, see the Getting Started guide and the overview article on Mapping Your Blue Team to MITRE ATT&CK.<sup>[2,3]</sup>

### References:

- [1] <https://github.com/rabobank-cdc/DeTTECT>
- [2] <https://github.com/rabobank-cdc/DeTTECT/wiki/Getting-started>
- [3] <https://www.mbsecure.nl/blog/2019/5/dettact-mapping-your-blue-team-to-mitre-attack>

# DeTT&CT Analysis Flow



This is a visual representation of the DeTT&CT analysis flow. First, you define your data source coverage. Based on this information, you can determine your visibility coverage, which informs your detection coverage. With that foundational information in place, you can then decide which threat group activity to analyze. This can be one of the known adversary groups, techniques from your red team, or activity from a specific attack. Then compare the detection coverage with the threat actor heat map to determine how well you can detect actual adversary activity.

To get familiar with these visualizations, you can load DeTT&CT data into ATT&CK Navigator layers. The following sample files are online in the course Digital Download Package (available at [mgt514.com](http://mgt514.com)) in the Section 1 -> Threat Analysis -> DeTT&CT -> output directory.

- 01 data\_sources\_endpoints.json
- 02 visibility\_coverage.json
- 03 detection\_coverage.json
- 04 all\_threat\_actor\_heat\_map.json
- 05 one\_threat\_actor\_heat\_map.json

For each file, go to the online ATT&CK Navigator tool, create a new tab, select “Open Existing Layer”, then “Upload from local”, and choose a JSON file above.

## ATT&CK Enterprise Mitigations

Account Use Policies	Active Directory Configuration	Antivirus/Antimalware	Application Developer Guidance	Application Isolation and Sandboxing	Audit
Behavior Prevention on Endpoint	Boot Integrity	Code Signing	Credential Access Protection	Data Backup	Data Loss Prevention
Disable or Remove Feature or Program	Do Not Mitigate	Encrypt Sensitive Information	Environment Variable Permissions	Execution Prevention	Exploit Protection
Filter Network Traffic	Limit Access to Resource Over Network	Limit Hardware or Software Installation	Multi-factor Authentication	Network Intrusion Prevention	Network Segmentation
Operating System Configuration	Password Policies	Pre-compromise	Privileged Account Management	Privileged Process Integrity	Remote Data Storage
Restrict File and Directory Permissions	Restrict Library Loading	Restrict Registry Permissions	Restrict Web-Based Content	Software Configuration	SSL/TLS Inspection
Threat Intelligence Program	Update Software	User Account Control	User Account Management	User Training	Vulnerability Scanning

In addition to improving detection capabilities, you want to implement mitigations to prevent attacks from occurring in the first place. At the time of writing, ATT&CK defines over 40 Enterprise Mitigations. Each Mitigation on the ATT&CK website lists all the corresponding Techniques that it can mitigate.<sup>[1]</sup> In turn, each Technique lists all the corresponding Mitigations.

Some Mitigations are more specific than others. For example, Restrict Registry Permissions is very specific and restricts the ability for attackers to modify registry hives or keys. Exploit Protection, on the other hand, is broader. It mentions Web Application Firewalls (WAF) along with other defensive mechanisms like Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR).

Reference:

[1] <https://attack.mitre.org/mitigations/enterprise>

## Defense Identification Example

### Tactics

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Exploit Public-Facing Application	Web Shell	Valid Accounts	Disabling Security Tools	Credentials in Files	Network Service Scanning	Exploitation of Remote Services	Data Staged	Exfiltration Over Alternate Protocol

### Mitigations

### Techniques

WAF Update Software Vulnerability Scanning	Privileged Account Management Update Software	Password Policies Privileged Account Management	Restrict Permissions User Account Management	AD Config Audit Password Policies User Training	Disable Program NIPS Network Segmentation	Application Isolation Exploit Protection Network Segmentation	Restrict File and Directory Permissions	Filter Network Traffic DLP, NIPS Network Segmentation
--	--	--	---	--	---	---	---	---

SANS

MGT514 | Security Strategic Planning, Policy, and Leadership 208

The Mitigations section on the slide above contains a partial list of Mitigations for each of the corresponding Techniques. The text below includes all the Mitigations defined in MITRE ATT&CK for each of the Techniques. You will notice that some of the Mitigations apply to multiple Techniques.

This list is a good starting point to identify the security controls that can be implemented or improved to strengthen your security program against attacks.

#### 1) Exploit Public-Facing Application

Application Isolation and Sandboxing  
Exploit Protection with WAF  
Network Segmentation  
Privileged Account Management  
Update Software  
Vulnerability Scanning

#### 2) Web Shell

Privileged Account Management  
Update Software

#### 3) Valid Accounts

Password Policies  
Privileged Account Management

#### 4) Disabling Security Tools

Restrict File and Directory Permissions  
User Account Management

### **5) Credentials in Files**

- Active Directory Configuration
- Audit
- Password Policies
- Restrict File and Directory Permissions
- User Training

### **6) Network Service Scanning**

- Disable or Remove Feature or Program
- Network Intrusion Prevention
- Network Segmentation

### **7) Exploitation of Remote Services**

- Application Isolation and Sandboxing
- Disable or Remove Feature or Program
- Exploit Protection
- Network Segmentation
- Privileged Account Management
- Threat Intelligence Program
- Update Software
- Vulnerability Scanning

### **8) Data Staged**

For this Technique, ATT&CK states that “This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.” For example, simply staging data in a certain location or using a compression algorithm cannot be easily prevented. However, restricting file and directory permissions could minimize the locations where the attacker is able to stage data.

### **9) Exfiltration Over Alternate Protocol**

- Filter Network Traffic
- Network Intrusion Prevention
- Data Loss Prevention
- Network Segmentation

## Cyber Threat Intelligence

- Techniques that collect, classify, and use knowledge about adversaries
- This knowledge can be shared using well-known frameworks
  - **STIX – Structured Threat Information eXpression**
    - Language that describes the full range of cyber threat information including adversary TTPs, campaigns, and courses of action
    - Open community effort sponsored by the U.S. Department of Homeland Security
    - Commonly used in confidential information sharing organizations
  - **TAXII – Trusted Automated eXchange of Indicator Information**
    - Transport mechanism that standardizes automated exchange of cyber threat info
    - Supports a number of sharing models
      - Hub and Spoke
      - Source/Subscriber
      - Peer to Peer

Cyber Threat Intelligence (CTI) is the collection, classification, and exploitation of knowledge about adversaries that helps defenders reduce the adversary's likelihood of success with each subsequent intrusion attempt.<sup>[1]</sup> There are three levels of threat intelligence:

1. **Strategic:** Executives and senior leaders seek to understand the larger threat landscape to identify risks and make investment and strategic decisions.
2. **Operational:** Operational staff look for trends in an adversary's operation or campaign.
3. **Tactical:** This level shows foundational consumption and sharing of Indicators of Compromise (IOCs) and attacker Tactics, Techniques, and Procedures (TTPs).

As the Lockheed Martin case shows, gathering even basic IOCs about adversaries and their TTPs can greatly aid in disrupting intrusion attempts. Building profiles of adversary groups and sharing intelligence with other organizations further enhances an organization's ability to detect and disrupt attacks.

STIX and TAXII are two well-known frameworks used for defining and sharing threat information.

STIX is a language that enables you to specify and communicate standardized cyber threat information. It is a schema sponsored by the U.S. Department of Homeland Security (DHS) as an open community effort. As a result, it is widely used in confidential information sharing organizations such as the Financial Services Information Sharing and Analysis Center and National Health Information Sharing and Analysis Center (FS-ISAC and NH-ISAC).

STIX defines the cyber threat information, whereas TAXII provides a standard way to share that threat information.<sup>[2,3]</sup> It is flexible enough to support a number of sharing models, including these:

- **Hub and Spoke:** One organization serves as the central hub of information while a partner organization can choose to consume and/or provide information.
- **Source/Subscriber:** One organization provides information to the subscribers.
- **Peer to Peer:** Two or more organizations share information directly with each other.



References:

[1] <https://www.sans.org/course/cyber-threat-intelligence>

[2] <http://stixproject.github.io>

[3] <http://taxiipproject.github.io>

## Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
<b>Reconnaissance</b>	Web analytics	Firewall ACL				
<b>Weaponization</b>	NIDS	NIPS				
<b>Delivery</b>	Vigilant user	Proxy filter	In-line AV	Queuing		
<b>Exploitation</b>	HIDS	Patch	DEP			
<b>Installation</b>	HIDS	"chroot" jail	AV			
<b>C2</b>	NIDS	Firewall AV	NIPS	Tarpit	DNS redirect	
<b>Actions on Objectives</b>	Audit log			Quality of Service	Honeypot	

Source: Lockheed Martin paper

From a technical perspective, a number of techniques can be used against attackers across various phases of the Kill Chain. The Lockheed Martin paper lists a number of technical controls that can be used to detect, deny, disrupt, degrade, and deceive attackers.<sup>[1]</sup>

### Detect

Web and audit logs, along with Network Intrusion Detection (NIDS) and Host Intrusion Detection (HIDS) systems, provide a wealth of information about potential attacker activity. Additionally, vigilant users are often the first ones to notice signs of anomalous activity. Training them to report suspicious activity can provide a great early warning sign to potential attacks.

### Deny

Capabilities such as firewalls, access control lists (ACLs), Network Intrusion Prevention (NIPS), proxy filtering, and Antivirus can be effective means of blocking attacks. Patching vulnerabilities and running in a "chroot" jail, which prevents software from accessing files outside of its own root directory, are also effective means of preventing attacks.<sup>[2]</sup>

### Disrupt

Attacks can also be disrupted using a number of techniques such as in-line Antivirus and Network Intrusion Prevention (NIPS). To disrupt the Exploitation phase, software can also be built with the Data Execution Prevention (DEP) feature.<sup>[3]</sup> DEP is a security feature available on modern operating systems that marks certain areas of memory as "nonexecutable." This helps disrupt certain types of malware from executing.

### Degrade

Attackers can also be slowed down to buy defenders more time to respond. This can be accomplished by queuing requests or decreasing the quality of service by using tarpits to purposely delay connections.<sup>[4]</sup>

### Deceive

Attackers can also be deceived by DNS redirects or honeypots that appear to be part of a real system but are actually isolated systems that are specifically monitored to analyze attacks.

References:

- [1] <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>
- [2] <https://en.wikipedia.org/wiki/Chroot>
- [3] [https://en.wikipedia.org/wiki/Executable\\_space\\_protection#Windows](https://en.wikipedia.org/wiki/Executable_space_protection#Windows)
- [4] [https://en.wikipedia.org/wiki/Tarpit\\_\(networking\)](https://en.wikipedia.org/wiki/Tarpit_(networking))

## In Summary

- Defenders must:
  - Move detection and analysis up the Kill Chain
  - Use MITRE ATT&CK to understand adversary TTPs
  - Implement defenses across the entire attacker life cycle
- Use threat analysis to:
  - Determine current state coverage
  - Identify visibility gaps
  - Prioritize defenses

Understanding the Tools, Techniques, and Procedures (TTPs) of adversaries helps defenders improve detection, leverage threat intelligence, emulate adversaries, and prioritize defenses. By using the Kill Chain and MITRE ATT&CK as a structure to analyze intrusions, defenders can drive defenses across the entire attack life cycle. This helps defenders gain an edge against a variety of threats.

Start small with your threat analysis. Scoring data and creating a full heat map can be challenging. You can start by picking just a single technique to determine coverage, visibility, and required enhancements. Look at your existing analytics and tooling to see your current state coverage, identify visibility gaps, and determine future mitigations.

# 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 I

- Overview
  - Need for Strategic Planning
  - 30-60-90 Day Plan
    - Lab #1: CISO First Impression
- Decipher the Business
  - Historical Analysis
  - Values and Culture
  - Stakeholder Management
    - Lab #2: Relationship Management
  - Asset Analysis
  - Business Strategy
    - Lab #3: Strategy Map
- Decipher the Threats
  - Threat Actors
  - PEST Analysis
  - Threat Analysis

This page intentionally left blank.

## Strategic Planning Process

### Decipher

- Historical Analysis
- Values and Culture
- Stakeholder Management
- Asset Analysis
- Business Strategy
- PEST Analysis
- Threat Analysis

### Develop

- Vision and Mission
- SWOT Analysis
- Visioning and Innovation
- Security Framework
- Gap Analysis
- Security Roadmap
- Business Case
- Policy Development

### Deliver

- Security Metrics
- Marketing Plan
- Executive Comms
- Policy Assessment
- Policy Management

Lead, Motivate, and Inspire

In this section, we laid our "Strategic Planning Foundations" by focusing the Decipher phase. By understanding the business and the threat landscape, we gain a better understanding of how we provide *value* to the organization. In the next section, we will cover topics in subsequent phases to drive organizational engagement and transformation.

## Strategic Planning Tools: Section I

Tool	Purpose
Historical Analysis	Analyze the organization's past to inform future development
Values and Culture	Understand how to operate effectively within the organization
Power/Interest Grid	Prioritize stakeholders to develop a relationship plan
SIPOC	Understand key processes to identify stakeholders
Asset Analysis	Identify and classify the "crown jewels" of your organization
Porter's Five Forces	Analyze competition in an industry to understand business strategy
Strategy Map	Link business objectives to security projects and initiatives
PEST Analysis	Analyze external forces that create cyber risk or opportunity
Kill Chain and MITRE ATT&CK	Understand attacker tactics, techniques, procedures (TTPs) to plan defenses

This is a summary of the strategic planning tools we covered in this section.