514.5

Strategic Planning Workshop

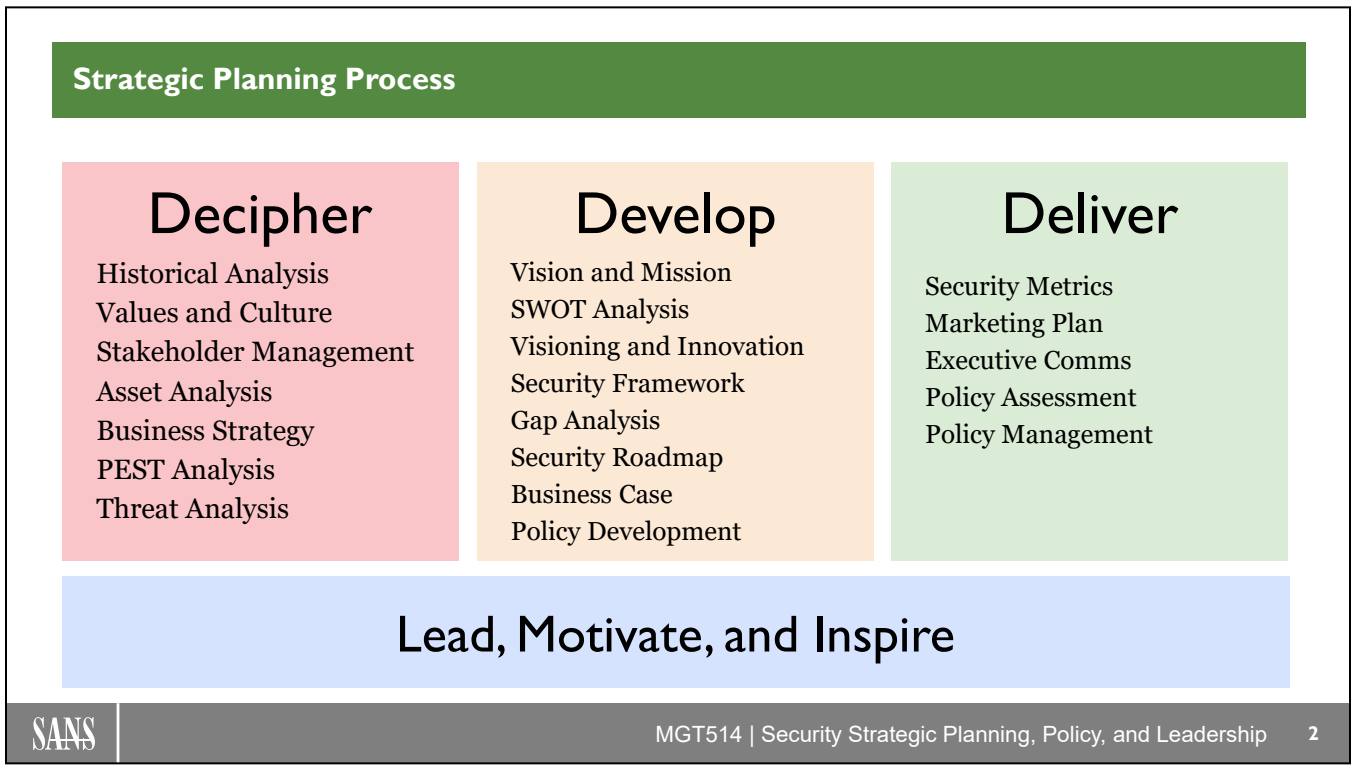
All reference links are operational in the browser-based delivery of the electronic workbook.

MGT514.5 | Security Strategic Planning, Policy, and Leadership

SANS

Strategic Planning Workshop

This page intentionally left blank.



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 5

- ***Background***
  - Case Study Method
- Case Studies
  - iPremier Case (A)
  - iPremier Case (B)
  - iPremier Case (C)
  - PharmaCo Case (A)
  - PharmaCo Case (B)
  - PharmaCo Case (C)
  - HealthHound Case
- Summary
  - Course Summary
  - Resources

This page intentionally left blank.

Strategic Planning Workshop

- Managers and leaders
  - Expected to voice opinions
  - Analyze and react to uncertain scenarios
  - This section gives you opportunities to practice
- Success of this section depends on you
  - Highly interactive
    - Work in groups to discuss and analyze real-world cases
    - Share the results of group discussions with the larger class
  - Using the case study method
    - Apply the tools from class to evaluate and refine analysis

This section of the course consists of a series of case studies. By analyzing these case studies, you have the opportunity to apply the skills you have gained this week. We will use the case study approach to place you into real-world situations. By interacting with one another and the information, you will be able to share your insights as they apply to the cases at hand. You will be expected to answer or develop several points for presentation and to be prepared to share them with the rest of the class.

Case Study Method

- The case studies are from leading educational institutions
  - Harvard Business School
  - Ivey School of Business
  - SANS Institute
- They touch on real-world issues
  - Allow us to practice
- We will debrief with each other to learn

As we learned through the previous sections of the course, we can use a number of tools to analyze and create strategic plans. We will use these tools in a safe, productive environment, which is this class.

Our first goal is to evaluate the information that will be provided in the cases. It is sometimes difficult to know what is immediately important to a case and what might be important later, so it is important to analyze all of the information provided in the case. You can draw false conclusions from misleading information in the case. Stay away from wishful thinking related to security events presented in the case studies. Understand that people will gravitate to "group think" very readily, and will also develop hypotheses to fit their own stereotypes. Be aware that some of the information provided may be nothing more than a distraction to get you off the correct track.

Teamwork is the order of the day. We will work as teams, and we encourage everyone to use the tools from class to get clarity on what the case represents and what is important. Remember, you likely will never act as a solo agent in a situation like this. Be prepared to discuss, defend, and defer to others during all discussions.

We will also debrief others on the findings and conclusions we have reached. The presentation may be only a sentence or two or a few points, but remember that in your real job, you may get only five minutes in front of the board to state your case.

Notes on the Case Studies

- Case study analysis is focused on
  - Core principles and lessons learned
  - Situational analysis
- Use tools from earlier sections of the course
  - Constantly think about tools to apply
- Older case studies may be used as they
  - Contain timeless scenarios
  - Are useful for teaching and learning
  - Place you in interesting decision-making situations

Case studies are intended to place you in situations similar to ones that you might encounter in the real world at work. As a result, case study analysis is focused on core principles and learning from the scenarios described in the case. A key component will also be thinking about and applying the tools, tips, and techniques you learned in earlier sections of the course to bring that thinking to bear on the case at hand. It will be helpful to repeatedly think back to earlier sections of the course and consider the tools that can be applied to the case under discussion. In analyzing the case, you can decide which tools to use and how to best deal with the situation at hand. Because the focus is on using these tools, we offer case studies that, although they may have been written some time ago, contain timeless scenarios that place you in real-world decision-making situations.

Case Study Discussion

1) Case Overview
   - Key points to consider as you read the case
2) Read the case
   - On your own
3) Case Analysis
   - Analyze and Discuss options and associated pros/cons
4) Class Debrief
   - Share how you would handle the situation
5) Case Summary

1) **Case Overview:**
The case will be described and outlined prior to reading the prepared text. The instructor will use this time to prepare students for the types of topics to focus on while reading and assimilating the case.

2) **Read the Case:**
Students are given time to read the case quietly to themselves for comprehension and assessment of the actions or events described. This is done individually.

3) **Case Analysis:**
The class will break into groups for more detailed dissection and discussion of the events and actions identified in the case. During this time, each member of the team will be asked to contribute his or her assessment of the events and to provide thoughtful points either pro, con, or both for the participants and their actions during the case events.

4) **Class Debrief:**
To view the differences in perception, we will debrief the class. Instructors will ask for each team to summarize the key points that they recognized and have a presenter or representative to itemize these points for the class. This step helps highlight differences in perception of the same events among the various teams.

5) **Case Summary:**
After we have reviewed all of the debrief notes, the instructor will lead a summary of the case. This step should enable the student to recognize the tools and techniques that were used during the case study. In turn, this helps to internalize the learning steps taken.

Tips for Reading Case Studies

- First, read the case
  - Get a sense of the overall event
  - Don't try to second-guess the characters
  - Immerse yourself for a few minutes in the drama
- Gather as much initial information as you can
  - Look for what is there
  - Look for what is NOT there

Begin with a first reading of the case. This should be a high level or cursory review of the provided information. Enjoy the read. Suspend disbelief. For example, don't condemn the characters in the case by thinking, "He or she would never say something like that," "That's crazy," and so on.

Gather as much information as you can with a quick read. Look for the highlights and lowlights that jump out at you. Don't worry about dissecting every word.

Try to summarize the key points presented to you. These points will be useful later if you are able to remember key elements from the initial reading.

Also, look for what is not said. Often, the space between the words can say as much as the words themselves.

Some of the questions to ask yourself might include:

- Does it feel as though I am being given all of the information?
- Are there any obvious gaps or mistakes visible at first read?
- What is the management style of the organization being studied?
- Can I spot any special agendas from any of the characters?
- What are some of the questions we are left without answers to, and how will that affect the case?
- What areas or items must we ignore due to a lack of information made available?

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 5

- Background
  - Case Study Method
- Case Studies
  - ***iPremier Case (A)***
  - iPremier Case (B)
  - iPremier Case (C)
  - PharmaCo Case (A)
  - PharmaCo Case (B)
  - PharmaCo Case (C)
  - HealthHound Case
- Summary
  - Course Summary
  - Resources

This page intentionally left blank.

iPremier Case Overview

- Web-based retailer in Washington state
  - Survived the dot-com crash to become one of the major players in high-end retail online
- Bob Turley, the CIO, is in New York
  - Called and told a DoS attack may be underway
  - Has to deal with this crisis from afar
- The time frame is short, but intense
  - This can make for interesting decisions

iPremier is a web retailer that caters to higher-end clients. It was started by a couple of college students in 1996. Today, it is one of the two larger web retailers still in existence and operating at a profit. Sales have increased by 20% or more in each of the last three years. Although sales are going up, profits are spotty or thin.

The clientele expects upscale service and is ready to pay upscale prices for the goods they purchase.

Bob Turley is relatively new to the company, and this is his first CIO gig. Lately, the management team has been moving from a "bred here" cadre of original players to more outsiders with specific business skill sets. Turley is one of these recent hires.

Other than that, not much detail is given regarding Turley, although from the description of the hiring process, it would seem that he looked as if he had the experience necessary for this job. However, being new means there are likely lots of skeletons he is not aware of. For instance, we do not know what the policy and procedure repository looks like and if it will help.

Because Turley is in New York City to meet with Wall Street analysts, he is not even able to put hands on the situation and must manage it remotely. Often, making important decisions from afar can be difficult. Note how or if he deals with the frustration of not being on the scene.

The case happens very quickly and over a short period of time, or so it appears. Decisions must be made split second, and any decisions made may affect the organization for a long time to come.

Note that some attitudes may be reinforced or modified due to the short, but intense, timeline. Watch for people using this situation to reach false conclusions, or to see what they want to see.

iPremier Read Case (A)

- On your own
  - Take 30 minutes to read the entire case
- As you read the case, think about these questions:
  - What did iPremier do well?
  - What could it do better?
  - What is its security posture?
- If you finish reading the case early
  - Start noting key points for further thought and discussion

Take 30 minutes to read the entire case. Read for comprehension and not necessarily for total detail. Get a sense of the key events in addition to iPremier's culture and management style.

As you read the case, think about the questions below. You may want to highlight or underline key items that stand out to you. If you finish reading the case early, start noting key points for further thought and discussion.

What did iPremier do well?

- Did it do anything well? Although it may not seem like it, there is always a silver lining. See if you can identify one.

What could iPremier do better?

- What do you see as structural issues to iPremier?

What is their security posture?

- What clues are given in the case about iPremier's security posture?
- What is the management philosophy of the organization?
- How mature are their operations?

HARVARD | BUSINESS | SCHOOL

9-601-114
REV: FEBRUARY 28, 2018

ROBERT D. AUSTIN

The iPremier Company (A): Distributed Denial of Service Attack

January 12, 2018, 4:31 AM

Somewhere a phone was chirping. Bob Turley, CIO of the iPremier Company, turned beneath the bed sheets, wishing the sound would go away. Lifting his head, he tried to make sense of his surroundings. Where was he?

The Westin in Times Square. New York City. That's right. He was there to meet with Wall Street analysts. He'd gotten in late. By the time his head had hit the pillow it was nearly 1:30 AM. Now the digital display on the nearby clock made no sense. Who would be calling at this hour? Why would the hotel operator put a call through?

He reached for the phone at his bedside and held it to his ear. Nothing. The chirping was coming from his mobile. Staggering out of bed, he located the noisy phone and opened the call.

"This is Bob Turley."

"Mr. Turley?" There was panic in the voice. "I'm sorry to wake you, Joanne told me to call you."

"Who is this?"

"It's Leon. Ledbetter. I'm in Ops. We met last week. I'm new. I mean, I was new, last month."

"Why are you calling me at 4:30 in the morning, Leon?"

"I'm really sorry about that Mr. Turley, but Joanne said—"

"No, Leon, I mean tell me what's wrong."

"It's our website, sir. It's locked up. I've tried accessing it from three different computers and nothing's happening. Our customers can't access it either; the help desk is getting calls."

"What's causing it?"

Professor Robert D. Austin, Dr. Larry Leibrock (Chief Technology Officer, McCombs School of Business, University of Texas at Austin), and Alan Murray (Chief Scientist, Novell Service Provider Network) prepared this case. This revised version was prepared by HBS Emeritus Professor Richard L. Nolan, Professor Robert D. Austin (Ivey Business School), and Professor Michael Parent (Beedie School of Business, Simon Fraser University). HBS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management. The situation described in this case is based on real accounts of denial of service attacks directed against several companies during 2000 and 2001. Company names, product/service offerings, and the names of all individuals in the case are fictional, however. Any resemblance to actual companies, offerings, or individuals is accidental.

"Joanne thinks—if we could only—well, someone might have hacked us. Someone else might be controlling our site. Support has been getting these e-mails—we thought it was just the web server, but I can't access anything over there. Joanne is on her way to the data center. She said to call you. These weird e-mails, they're coming in about one per second."

"What do the e-mails say?"

"They say 'ha.'"

"Ha?"

"Yes, sir. Each one of them has one word in the subject line, 'ha.' It's like 'ha, ha, ha, ha.' Coming from an anonymous source. That's why we're thinking—."

"When you say they might have hacked us—could they be stealing customer information? Credit cards?"

"Well, I guess no firewall[1]—Joanne says—actually we're using a firewall service we purchase from the hosting company, so—."

"Can you call someone over there? We pay for monitoring 24/7, don't we?"

"Joanne is calling them. I'm pretty sure. Is there anything you want me to do?"

"Have we set our emergency procedures in motion?

"Joanne says we have a binder, but I can't find it. I don't think I've ever seen it. I'm new—"

"Yes, I got that. Does Joanne have her cell?"

"Yes sir, she's on her way to the data center. I just talked to her."

"Call me back if anything else happens."

"Yes sir."

Turley stood up, realizing only then that he had been sitting on the floor. His eyes were bleary but adrenaline was now pumping in his bloodstream. Steadying himself against a chair, he felt a wave of nausea. This was no way to wake up.

He made his way to the bathroom and splashed water on his face. This trip to New York was an important assignment for someone who had been with the company such a short time. It demonstrated the confidence CEO Jack Samuelson had in him as the new CIO. For a moment, Turley savored the memory of the meeting in which Samuelson had told him he would be the one to go to New York. As that memory passed another emerged, this one from an earlier session with the CEO. Samuelson was worried that the company might eventually suffer from "a deficit in operating procedures." "Make it one of your top priorities," he had said. "We need to run things professionally. I've hired you to take us to the next level."

[1] A "firewall" is a combination hardware/software platform that is designed to protect a local network and the computers that reside on it against unauthorized access.

Looking himself over in the mirror, seeing his hair tussled and face wet, Turley lodged a protest with no one in particular: "I've barely been here three months!"

The iPremier Company

Founded in 1996 by two students at Swarthmore College, the iPremier Company had evolved into a web-based commerce success story. From its humble beginnings, it had risen to become one of the top two retail businesses selling luxury, rare, and vintage goods on the web. Based in Seattle, Washington, the firm had grown and held off incursions into its space from a number of well-funded challengers. For the fiscal year 2017, profits were $20.1 million on sales of $320 million. Sales had grown at more than 20% annually for the last three years, and profits, though thin, had an overall favorable trend.

Immediately following its IPO in late 1998, the company's stock price had nearly tripled. It had continued up from there amid the euphoria of the 1999 markets, eventually tripling again. A follow-on offering had left the company in a strong cash position. During the NASDAQ bloodbath of 2000, the stock had fallen dramatically but had eventually stabilized and even climbed again, although not to pre-2000 levels. In the decade plus since, the company had held its own and consolidated its leading market position, enjoying better-than-average returns by streamlining and focusing its business to achieve profitability.

Most of the company's products were priced at a few hundred dollars, but there were a small number of items priced in the thousands and tens of thousands of dollars. Customers paid for items using their credit cards. The company had flexible return policies, which were intended to allow customers to thoroughly examine products before deciding whether to keep them. The iPremier customer base was high-end—so much so that credit limits on charge cards were rarely an issue, even for the highest-priced products. Trust was critical to this relationship. Customers had to believe and trust that the goods sold by iPremier were genuine. Otherwise, they could easily purchase the same sorts of goods from a number of other websites, including iPremier's fiercest competitor, MarketTop. iPremier's competitive advantage lay not necessarily in its array of goods, but more in its responsive and attractive website, order fulfillment, and after-sales service. iPremier led its industry segment in the quality of the "user experience" and constantly innovated to provide the best, and most seamless service. As a result, the company had over one million regular customers in its database, and another few hundred thousand casual buyers.

Management and Culture

The management team at iPremier was a mix of talented younger people who had been with the company for a long time, and more experienced managers who had been gradually hired as the firm grew. Recruitment had focused on well-educated technical and business professionals with reputations for high performance. Getting hired into a senior management position required excelling in an intense series of three-on-one interviews. The CEO interviewed every prospective manager at the director level and above. The reward, for those who made the grade, was base compensation above the average of managers at similar firms, and variable compensation, mainly in the form of stock options, that could be a significant multiple of the base. All employees were subject to quarterly performance reviews that were tied directly to their compensation. Unsuccessful managers did not last long. Most managers at iPremier described the environment as "intense."

Throughout the company, there was a strong commitment to doing "whatever it takes" to get projects done on schedule and on budget, especially when it came to system features that would benefit

customers. The software development team was proud of its record of consistently launching new features and programs a few months ahead of MarketTop. Senior managers understood that their compensation and prospects with the company depended on executing to plan. They pursued "the numbers" with obsessive zeal.

Technical Architecture

The company had historically outsourced management of its technical architecture and had a long-standing relationship with Qdata, a company that hosted most of iPremier's computer equipment and databases, and provided connectivity to the Internet. Qdata was an early entrant into the Internet hosting business, but it had been battered by the contraction of the Internet bubble and lost any prospect of market leadership. Its data center was physically proximate to the corporate offices of iPremier; some felt there was little else to recommend it. The company had not been quick to invest in advanced technology and had had trouble retaining staff.

The iPremier Company had a long-standing initiative aimed at eventually moving its computing to an internal facility, but several factors had kept this from happening. First, and most significant, iPremier had been very busy growing, protecting its profits, and delivering new features to benefit customers; hence the move to a better facility had never quite made it to the top of the priority list. Second, the cost of more modern facilities was considerably higher—two to three times as expensive on a per-square-foot basis. Third, there was a perception that a move might risk service interruption to customers. Finally, one of the founders of iPremier felt a personal commitment to the owners of Qdata because they had been willing to renegotiate their contract at a particularly difficult time in iPremier's very early days.

4:39 AM

Sitting at the hotel room desk, Turley began scrolling through the phonebook on his phone. Before he could find the number for Joanne Ripley—his technical operations team leader—she called him.

"Well, Joanne. How are you this morning?"

A cautious laugh came from the other end of the call. "About the same as you, I'm guessing. I assume Leon reached you."

"He did, but he doesn't know anything. What's going on?"

"I don't know much either, yet. I'm in the car, on my way to the data center. I ought to be there in five minutes."

"How long after that until we are back up and running?"

"That depends on what's wrong. I'll try restarting the web server as soon as I get there, but if someone has penetrated our databases and stolen customer data, getting the server running will be the least of our worries. Did Leon tell you about the e-mails?"

"The 'ha, ha' e-mails? Yeah. Makes it sound like something deliberate."

"I'd have to agree."

"No chance it's a simple DDoS attack?"

"I doubt it's a *simple* DDoS attack; we've got software to deal with those."

"Can we track the e-mails?"

"Not soon enough. They're coming through an anonymizer that's probably in Europe or Asia. If we're lucky we'll find out sometime in the next decade who sent them. Then we'll discover they're originating from some laptop or smart thermometer in Podunk, Idaho, and their owner has no idea they've been compromised by hackers."

"What are the chances they're stealing credit cards? I know we don't keep credit card numbers on our database, but they could be stealing other sensitive information, right?"

Ripley paused before answering: "There's really no way of knowing."

"Should we pull the plug? Physically disconnect the communications lines?"

"If we start pulling cables out of the wall it may take us a while to put things back together."

"Joanne, don't we have emergency procedures for times like this? I don't think I've seen it but it comes up when people mention our business continuity plan (BCP)."

"We've got a BCP binder," said Ripley. "I've got a copy with me. Keep it in my car. There's one at the office too, and we store it electronically on our shared drive. But to be honest, well—it's out of date, and we don't really train people with it because of that. Lots of people on the call lists don't work here anymore. I don't think we can trust the phone numbers and I *know* some of the technology has changed since it was written. We've talked about practicing incident response but we've never made time for it."

"A Disaster Recovery Plan (DRP)? An Incident Response Plan (IRP)?" Turley was incredulous. It boggled his mind, and created more than a little career-anxiety that he hadn't thought to check these since his arrival. He'd assumed that, as a publicly-listed company, iPremier had to have such plans.

But now was not the time, he decided, to grill Ripley about it. So he changed the subject: "What's the plan when you reach the data center?"

"Let me restart the web server and see what happens. Maybe we can get out of this without too much customer impact."

Turley thought about it for a moment. "Okay. But if you see something that makes you think customer records or other information are being stolen, I want to know that immediately. We may have to take drastic action."

"Understood. I'll call you back as soon as I know anything."

"Good. One more thing: Who else knows this is going on?"

"I haven't called anyone else. Leon might have. I'll call him and call you right back."

"Thanks."

Turley disconnected. Just as he did so, his phone rang again.

"Damn." It was Warren Spangler, VP of business development. Turley recalled vaguely that Warren and Leon's father were college buddies or something. Ledbetter had almost certainly called Spangler.

"Hi, Warren," said Turley.

"Hi, Bob. I hear we've got some kind of incident going on. What's the story?"

"Something's definitely going on, but we're not sure what yet. We're trying to minimize customer impact. Fortunately for us, it's the middle of the night."

"Wow. So is it just a technical problem or is somebody actually doing it to us?"

Turley was eager to call the chief technology officer (CTO), so he didn't really have time for this discussion. But he didn't want to be abrupt. He was still getting to know his colleagues.

"We don't know. Look, I've got to—"

"Leon said something about e-mails—"

"Yes, there are suspicious e-mails coming in so it could be someone doing it."

"Oh, man. I bet the stock takes a hit tomorrow. Just when I was going to exercise some options. Shouldn't we call the police?"

"Sure, why don't you see what you can do there, that'd be a big help. Look, I've got to—"

"Seattle police? Do we know where the e-mails are coming from? Maybe we should call the FBI? No. Wait. If we call the police, the press might hear about this from them. Whoa. Then our stock would really take a hit."

"I've really got to go, Warren."

"Sure thing. I'll start thinking about PR. We got you covered here, bro. Keep the faith."

"Will do, Warren. Thanks."

Turley ended that call and began searching through his cell phone's memory to find the number for Tim Mandel, one of iPremier's co-Founders and now the company's CTO. He and Mandel had already cemented a great working relationship. Turley wanted his opinion. Just as Turley was about to initiate the call, though, another call came in from Ripley.

Turley answered the phone and said: "Leon called Spangler, I know. Anything else?"

"Ah, no. That's it for now. Bye."

Turley dialed Mandel. At first the call switched over to voicemail, but he retried immediately. This time Mandel answered sleepily. It took five full minutes to wake Mandel and tell him what was happening.

"So what do you think, should we just pull the plug?" Turley asked.

"I wouldn't. You might lose some logging data that would help us figure out what happened.

"I'm not sure knowing exactly what's happening is the most important thing to me right now."

"I suggest you change your mind about that. If you don't know what happened this time, it can happen again. And, if you don't know what happened, you won't know what, if anything, you need to disclose publicly. We might also need to preserve evidence of what has happened. A DDoS attack is a federal crime, and we might eventually need to involve the FBI."

Turley heard a thumping sound, as if Mandel had fallen getting out of bed; his phone clattered as it impacted something, the floor perhaps. A scant moment later, Mandel came back on the line and continued: "Come to think of it, Bob, preserving the logs is irrelevant because I'm pretty sure detailed logging is not enabled. Detailed logging adds a performance penalty of about 20%. Someone somewhere at some point decided that unacceptably impacts the customer experience."

"So we aren't going to have evidence of what happened anyway."

"There'll be some, but not as much as we, or the FBI, will want."

Another call was coming in.

"Hold on, Tim." Turley kicked the phone over to the waiting call. It was Peter Stewart, the company's legal counsel. What was he doing awake?

"This is Turley."

"Hey, Bob, it's Pete. Pull the plug, Bob. Shut off the power, pull the cords out of their sockets, go dark, kill it…everything. We can't risk having PII (Personally Identifiable Information) stolen."

"Spangler call you?"

"Huh? No, Jack. Samuelson. He called three minutes ago, said hackers had control of our web site and were stealing information. Told me in no uncertain terms to call you and 'provide a legal perspective.' That's exactly what he said: 'provide a legal perspective.'"

So the CEO was awake. The result, no doubt, of Spangler's "helping" from that end. Stewart continued to speak legalese at him for what seemed like an eternity. By this time, Turley was incapable of paying attention to him.

"Thanks for your thoughts, Pete. I've got to go, I've got Tim on the other line."

"Okay. For the record, though, I say pull the plug. I'll let Jack know you and I spoke, and will write a memo to file reflecting this conversation and my advice."

"Thanks, Pete," said Turley, acerbically.

Turley switched back over to the call with Mandel.

"Spangler's got bloody everybody awake, including Jack. I recommend you get dressed and head into the office, my friend."

"Is Joanne on this?"

"Yes, she's at Qdata by now." Turley's phone rang. "Got a call coming in from her now."

He switched the phone.

"What's up Joanne?"

"They won't let me into the NOC2," she said angrily. There's no one here who knows anything about the network monitoring and that's what I need to use to see the traffic coming into our site. The Qdata guy who can do it is vacationing in Aruba. I tried rebooting the web server, but we've still got a problem. My current theory is an attack directed at our firewall, but to be sure I've got to see the packets coming in, and the firewall is their equipment. You got an escalation contact to get these dudes off their butts?"

"I'm in New York, Joanne. I've got no Qdata contact information with me. But let me see what I can do."

"Okay. I'll keep working it from this end. The security guard doesn't look too fierce. I think I could take him."

"Do what you can."

Turley hung up. He noticed that Mandel had disconnected also. For a moment, Turley sat back in the chair, not sure what to do next.

5:27 AM

The phone rang again, and Turley could see from Caller ID that it was the call he had been dreading: Jack Samuelson, the CEO.

"Hi Jack."

"Bob. Exciting morning?"

"More than I like it."

"Are we working a plan?"

"Yes, sir. Not everything is going according to plan, but we are working a plan."

"Bob, the stock is probably going to be impacted and we'll have to put a solid PR face on this, but that's not your concern right now. You focus on getting us back up and running. Understand?"

"I do."

Samuelson hung up abruptly.

That had gone better than Turley had feared. He avoided the temptation to analyze Samuelson's every word for clues to his innermost thoughts. Instead, he called Ripley.

"Hi, Bob," she said, sounding mildly cheerful. "They let me in. I'm sitting in front of the console right now. It looks like a SYN flood from multiple sites directed at the router that runs our firewall service. So it *is* a DDoS attack. By the way, this is not a proper firewall, Bob; we need to work on something better." (**Exhibit 1 explains the different types of Denial of Service attacks).**

"Fine, but what can we do right now?"

---

[2] The "Network Operations Center" is the control room from which production computer operations and networks are monitored and operated.

"Well, looks like the attack is coming from about 3000 sites. If the guys here will let me, I'm going to start shutting down traffic from those sites. I'll have to set the phone down for a minute."

There was a pause of a couple of minutes. Turley heard some muffled conversation in the background, rapid keyboard clicks, then several epithets. Ripley came back on the line.

"Damn it, Bob, they're spawning zombies. It's Dawn of the Dead out there."

"You're going to have to translate that one for me, Ripley."

"Every time we shut down traffic from one address, the zombie we've shut off automatically triggers attacks from two other sites. I'll try it a few more times, but right now it looks like that's just going to make things worse. My guess is the hackers are using a 'bot net of enslaved machines."

"If it's a DDoS, they haven't hacked us, right? It means it's not an intrusion. They haven't gained entry to our system. So customer data are safe. Can we say that?" Turley was especially worried in light of recent, gigantic data breaches, and the ensuing class-action lawsuits they provoked (see **Exhibit 2**).

"There's nothing that makes a DDoS attack and an intrusion mutually exclusive, Bob."

Turley knew this, but had hoped otherwise in a moment of wishful weakness. Hearing Ripley remind him of the facts strengthened a growing, nauseating storm in his stomach. "I'll let you get back to it. Call me with regular updates."

Turley hung up and thought about whether to call Samuelson and what to tell him. He could say that it was a DDoS attack. He could say that the attack, by itself, was not evidence that customer information was at risk. But Turley wanted to think some more before he went on record.

Before he could do anything else, his cell phone rang again. It was Ripley.

"It stopped," she said excitedly. "The attack is over."

"What did you do?"

"Nothing. It just stopped. The attack just stopped at 5:46 AM."

"So—what now?"

"The website is running. A customer who visits our site now wouldn't know anything had ever been wrong. We can resume business as usual."

"Business as usual?"

"I'd recommend that we shut down, or at least disconnect from the public Internet, and give everything a proper going-over. In the longer run, we'll need to conduct a thorough forensic audit to ensure nothing else bad has happened. I've been thinking about how they targeted the firewall, and I don't think it sounds like script kiddies. With your approval, I'd like to reach out to some cybersecurity consultants and get them in ASAP."

What to Recommend

Post attack, Turley realized that he immediately faced a new decision: Whether to recommend shutting down – or, at least, disconnecting from the Internet as a precaution – while they figured out what had happened. Doing either would shut down normal business operations.

Shutting down to conduct a thorough forensic audit seemed like a prudent course, but it was unclear how long that would take. In such time, iPremier's customers could flee to a competitor. iPremier would have to explain a shutdown, and, for legal reasons, they'd probably have to admit that such a precaution was motivated by concerns about a data breach.

Shutting down, then, could freak out customers, sink the stock, even kill the company. And, Stewart's memo notwithstanding, there were plenty of good arguments to keep the business up and running. iPremier had done nothing to provoke the attack, and there was – as of this moment anyway – no actual evidence of an intrusion or breach. Turley knew that DDoS attacks were a daily occurrence, and that the bigger players like Amazon, Apple, Google, Yahoo and Microsoft were being attacked constantly. It was usually just a cost of doing business in this space, not a material event.

But – Ripley had observed that this seemed like a particularly sophisticated DDoS attack. And he realized, now, that the company had been lax in deploying and protecting its systems – the very thing he'd been hired to do. His new job honeymoon was over – he'd have to obtain the resources to secure company operations.

On the one hand, there was no *evidence-ba*sed reason to shut down. Indeed, doing so could be considered an irresponsible overreaction. After all, iPremier's corporate officers were first and foremost responsible to iPremier shareholders.

On the other hand, if customer data *had* been stolen, and if the site *was* insecure, keeping the site running could lead to more mischief by hackers – and kill the company in a different way, by exposing it to reputation damage, liability, and lawsuits.

Turley knew that the company's senior management team would be conflicted and angry about all this, and that he would have to make a recommendation soon. He guessed that Peter Stewart (Legal) and, probably, Joanne Ripley (Tech Ops) would want to shut the site down for an indefinite period, until such time as they would be reasonably assured that no data had been taken, or no ticking time bomb had been planted within iPremier systems. But he could easily imagine that some members of the senior management team would object to a shutdown; they would argue that until demonstrated otherwise, it should be assumed that nothing bad had happened beyond what they already knew – that iPremier had 'dodged a bullet'.

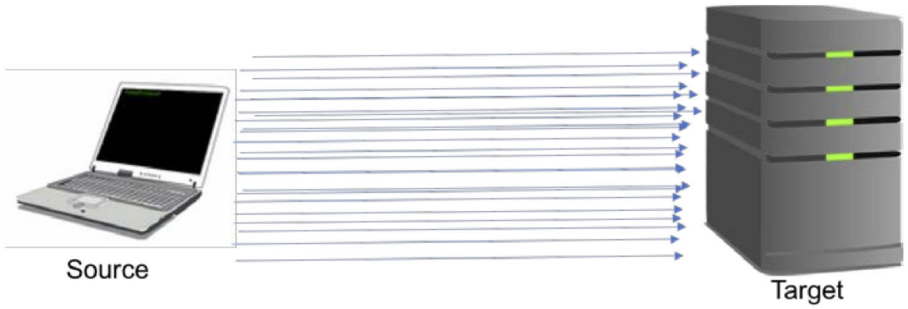
Samuelson and the Board of Directors would be looking to Turley for guidance, and his recommendation would have a profound impact on the future of the company.

Exhibit 1 Denial of Service Attacks Explained

Keying-in a website's URL (Uniform Resource Locator), or web address on a web browser or search engine's input line begins a conversation with the web server that will eventually return, or send the requestor the web page requested.

Each such "conversation" with a web server begins with a sequence of "handshake" interactions. The initiating computer first sends a "SYNCHRONIZE" or "SYN." The contacted web server responds with a "SYNCHRONIZE-ACKNOWLEDGE" or "SYN-ACK." The initiating computer then completes the handshake with an "ACKNOWLEDGE" or "ACK." A "SYN flood" is an attack on a web server intended to make it think a very large number of "conversations" are being initiated in rapid succession. Because each interaction looks like real traffic to the website, the web server expends resources dealing with each one. By flooding the site, an attacker can effectively paralyze the web server by trying to start too many conversations with it. This is the essence of a Denial of Service, or DoS attack.

In its simplest form, an attacker uses a single computer to send many requests in rapid succession. Because these types of attacks (single source) can be more easily traced, they are seldom used, except for the most unskilled of script kiddies.



More sophisticated hackers engage in Distributed denial-of-service (DDoS) attacks, such as described in the case, where many requests come in rapid succession from many computers. This might include the use of "Botnets", large clusters of Internet-enabled devices such as cellphones, computers, and even smart devices like thermometers, that have been infected with malware, allowing hackers to control these devices – sometimes called "zombies" – remotely. In one recent example, the Mirai Botnet was used to attack Internet service company Dyn in October 2016.

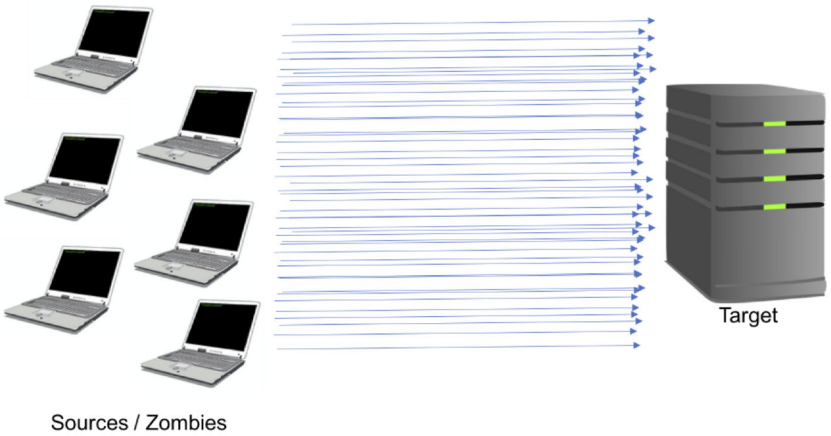
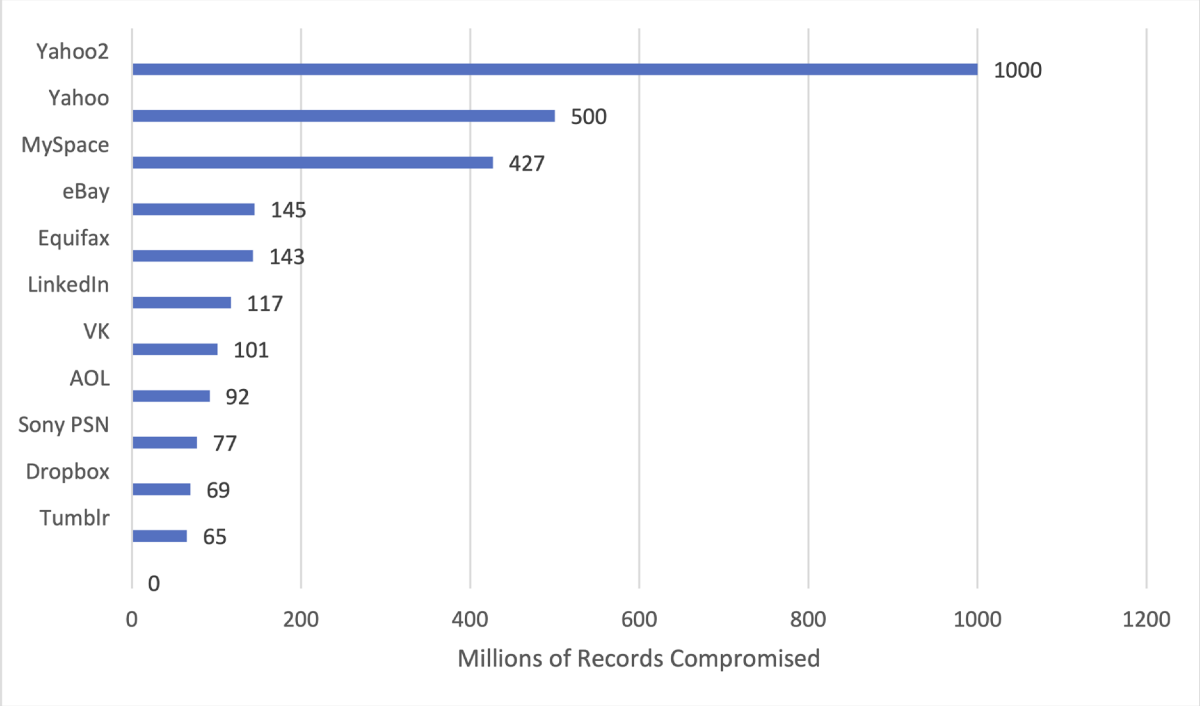


Exhibit 1 Denial of Service Attacks Explained (continued)

The most sophisticated denial-of-service attacks target other parts of source codes used by companies' websites. In one advanced case, many computers send requests to many *other* computers. However, by using IP (Internet Protocol) spoofing, the source address of these many other computers is set to the *target's* address, causing replies to go to the target address and flood it. This is called a Distributed *Reflected* denial-of-service, or DrDoS, attack.

Source: Casewriters.

Exhibit 2 A History of Large Data Breaches



Source: Casewriters.

iPremier Case (A) Case Analysis

- Analyze the company
  - How would you describe iPremier's culture?
  - What did iPremier do well?
- Develop recommendations
  - What are three things iPremier should do immediately?
  - What are three things it should do in the longer term?
- Identify tools to use
  - What tools from previous sections can be applied?
- 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 case answers.

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

1) How would you describe iPremier's culture?

2) What did iPremier do well?

Imagine that you have been hired to help iPremier in the aftermath of this incident. Develop recommendations to improve its security posture by answering these two questions:

3) What are three things iPremier should do in the short term?

4) What are three things iPremier should do in the long term?

In this class, you have learned about a number of tools that can aid in the strategic planning process. Think about what you have learned this week to answer the following question:

5) What tools or management techniques are helpful in understanding the organization and providing direction on next steps?

iPremier Case (A) Debrief

Note that this section contains a debrief and potential case answers

Please note that this section contains a debrief and potential case answers. The instructor will walk through this section with the class after you have analyzed the case.

iPremier Company Culture

- Strengths
  - Senior leadership and employee engagement
- Intense focus on financial performance
  - "Managers pursued 'the numbers' with obsessive zeal"
  - "The stock is probably going to be impacted"
- Management concerned about perceptions
  - "For the record, though, I say pull the plug"
  - "We'll have to put a solid PR face on this"
- Security is not a priority
  - "We've talked about practicing incident response but we've never made time for it"
  - "Not been quick to invest in advanced technology and had trouble retaining staff"

The preamble of the case delivers a picture of the management style of iPremier that sets the tone for the case. The company has been fighting its way up in the economy from a rough start and likely many close calls. This fact is borne out in the comment about some management having a soft spot for the hosting service because of their willingness to renegotiate the firm's contract in the early days when things were tough. These comments are not throw-away statements but rather serve to color the overall tendencies of the management team during a crisis.

Note that a number of calls early in the event seems to predispose the line of thinking that will be used later after the smoke starts to clear. The technical architecture of the company is also a clue as to how it really views information security. In addition to the infrastructure, no Chief Information Security Officer (CISO) is mentioned, which must be a clue as the value placed on security. No mention is made of requirements for credit card security and Payment Card Industry (PCI) compliance. Given that it's an online business, iPremier is likely required to comply with the PCI-DSS (Data Security Standard).

The company is described as having a "make the numbers" mentality. This is a major red flag for any information security incident:

- Security is not revenue generating for the organization.
- When a company decides it needs to "make the numbers" above all else, we can see that planning would tend to receive less than sufficient funding.
- It is very apparent from the beginning of the call that the company has very little process or practice around incident response.
- Turley does not take any immediate action on the phone with the first reporter. This is a very good move because the situation is still very fluid, and no answers are being given by the participant (Leon) that are truly actionable.

The General Counsel also voices his "legal opinion," albeit unasked for. This is clearly a political move intended to cover his own liability and serves to further complicate and muddle the picture. Things get even more complicated when he actually speaks with the CEO. This type of behavior is clearly designed to distance himself from any blowback and perhaps to throw the CIO, Turley, under the proverbial bus.

With a management style that can be best described as "disorganized," it is not surprising that these calls are flying, and no one seems to have a clear vision as to either what exactly has happened or as to what the next step should be. This is further evidenced by the fact that there is a binder of procedures, but it has not been updated or practiced for some time.

The technical architecture description is instructive. The company does very little of its own work and outsources most IT. Along with this is the interesting fact that there is knowledge that the technical infrastructure is old and needs a refresh. Although there is a project, it keeps getting pushed back. This, in turn, is a red flag because the company's biggest asset and its sole source of revenues are its online customer base. Rather than protecting profits and growth, perhaps it should be concentrating on protecting its customers.

As the incident progresses, it is very quickly apparent that some of the players are reluctant to take any responsibility for what is happening. This, together with a natural inclination to look back and say, "We have never had a major incident that adversely affected us, so how bad could this be," sets that company up to draw false conclusions and downplay what could be a very substantial incident. We are shown that certain players are far more interested in protecting their own position or currying favor with the CEO than in really helping cure the situation.

The introduction of the CEO in the middle of the incident is potentially a game changer. Can the CIO keep his head on straight after comments from the CEO amounting to "get us back up and running, no matter what"?

Each of the executive members offering their take on the incident actually makes this situation more unclear. Bob Turley suddenly needs to consider comments like, "I was about to exercise some stock options," with the need to preserve and protect the environment. This type of influence is totally normal and human in nature. The issue is how Turley manages to keep it out of the situation if he can.

iPremier Immature Operations

- Poor change management
  - Procedures
    - "I'll try restarting the web server as soon as I get there"
  - Version control of systems
    - "Move might risk service interruption to customers"
  - Technology refresh
- Lack of crisis management
  - No crisis leader or single point of contact
    - Security is left to the CIO
  - Lack of defined roles and responsibilities
    - "Shouldn't we call the police?"
  - Outdated procedures and policy for crisis management
    - "We've got a binder…well it's out of date"

Change management is clearly lacking. This is evidenced in several ways:

- There are no clear version control and recovery point for the systems needing to be rebuilt.
- There is a lack of consistent and current documentation of processes and procedures.
- The technology refresh has been on the books but, clearly, has a very low priority.

These basic elements of organizational and change management leave iPremier open to disaster.

Crisis management is clearly not a priority:

- Because there has never been a crisis before this point, planning is a low priority.
- Further to that, there is a false sense of security because the company has not had any major issues.
- One of the keys to an effective security program is assessment of potential threats.
- In any event, iPremier had no leader defined for crisis management.
- It has no clear procedures for communication and no single point of contact.
- All of the policies and procedures it did have are outdated and have not been practiced.

One of the most glaring omissions was a lack of stakeholder management:

- Out of band and inappropriate communications were made repeatedly during the crisis (discussions with the CEO, for example).
- Clear and comprehensive responses were not being given because there was a lack of stakeholder responsibility and understanding.
- This lack of clear roles and responsibilities made decision making much harder than it should have been.

Potential Short-Term Action Items

- Conduct a risk assessment
  - Identify key business assets and systems
- Perform a technical security review
  - Investigate denial of service protection service
  - Review critical systems
- Implement incident response improvements
  - Define incident response plan and procedures
  - Consider retaining an incident response firm
- Assign security responsibility to one person

In the immediate aftermath of the attack, it's clear that iPremier has a number of areas in which it can improve.

What acts or processes prior to the attack could have been better managed?
In the beginning, the company was completely unprepared for an incident of this type. The CEO had expressed to the CIO that he feared there might be a "procedure deficit." Certainly, this could and probably should have been one of the first steps undertaken by any new CIO: Itemize and perform a gap analysis of existing procedures and policies.

Had Bob Turley been able to rely on a strong structure of policy and procedures, he would not have needed to rely so heavily on human reaction. Additionally, it would have helped greatly if clear practice and remediation of procedures and processes had taken place.

What was done during the event that could have been done better?
During the actual event, a number of very human reactions took place, including emotional rather than practical responses, negatively contributing behavior such as group thinking, political maneuvering (on behalf of at least some of the senior management team), leaping to unsupported conclusions, and perceptive bias in favor of evidence supporting a current hypothesis. All of these human traits are normal, but we need to watch for them leaking into our decision-making process. Although it is easy to say that decisions must be made without emotion during a crisis, for example, it is pretty hard to do so when everyone is piling on emotional elements.

To have done a better job during the actual event, the company would have needed to be very strong and take definitive steps, and Bob Turley would have had to be a very pragmatic and unflinching leader. Instead, he did not get the support he needed to do whatever was necessary; and at the same time, his technical folks were not of one opinion on how to proceed. In addition, items like having a single point of communication for all messages and decision points would have improved handling and reduced erroneous or unhelpful communications.

The lack of clearly defined operating procedures and isolation of key technical resources was also important. For example, Ripley made a rushed, personal trip to the hosting site when her expertise might have been more helpful in another capacity.

What was done post event that could have been done better?
In the aftermath of the event, the iPremier team jumped to some additional conclusions. To suppose that the attack was over and was the "entire story" was wishful thinking.

Most security professionals recognize in this day and age that DoS attacks generally are used to mask other activities. This fact was recognized, yet not acted upon, largely due to push-back from a series of nontechnical people. Although management cannot rely totally on its technical resources to make decisions at times like this, taking close notice of the counsel they offer is appropriate. In this case, it was not listened to.

One action that seems to have been missed was to get a proactive start on mitigating the risk presented. So, much discussion regarding potential courses of inaction may have led to "analysis paralysis," resulting in inaction at a critical moment.

iPremier Tools for Success

- What should iPremier do in the longer term?
  - How could Bob Turley answer this question?
- Build a strategic plan that includes an understanding of business and current state
  - Mission and vision
  - Values and culture
  - Stakeholder management
    - SIPOC and Power/Interest Grid
  - PEST analysis

It's clear that, in the long term, iPremier has some serious work to do in improving information security and its operational capabilities. There are a number of things that iPremier can do, but in terms of long-term planning, iPremier will be best served by building a strategic plan that includes a deep understanding of its business and current state. This is exactly what we discussed in earlier sections of the course.

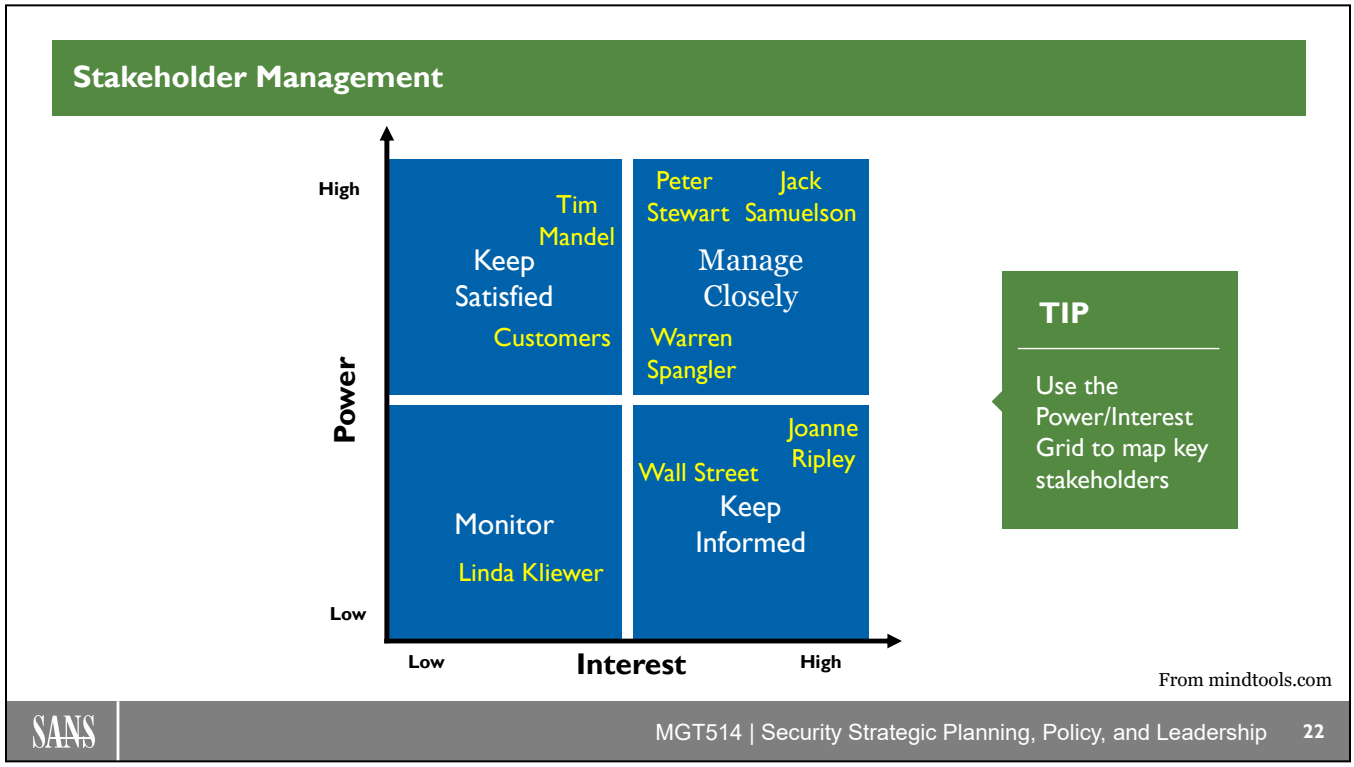
Some key tools to do this include mission and vision analysis, understanding values and culture, stakeholder management by using the SIPOC and power/interest grid, and PEST analysis to highlight the macro factors affecting the organization. We'll discuss these more over the next few slides.

What Is Important to iPremier's Business?

- Without an understanding of the organization's:
  - Mission and vision
    - Security will not be able to identify which projects are important to the organization
  - Values and culture
    - Security will not understand *how* to get work done and the pace the organization wants to go
- What is iPremier's mission?
  - It's not explicitly stated in the case but can infer that it's related to quality
  - Customer base is high-end and they "had to believe and trust that the goods sold by iPremier were genuine"
  - Focus on "quality of user experience" and providing the "most seamless customer service"

When we read the case, it's not exactly clear what iPremier's Mission actually is. We know that it is in high-end retail and is extremely focused on financial results. However, this does not give us a true sense of why iPremier exists and what problem it is solving for its customers. Given its high-end clientele, iPremier is concerned about high quality (or the perception of high quality) and providing full service and high-end customer service. If that is actually the case, then security and IT leaders would be wise to tie security investments back to availability, usability, and key projects that support high-end customer delivery. However, because we don't necessarily know what iPremier's mission is, it is much more difficult to determine which projects security should pursue. The point is, successful security leaders know exactly what is most important to the business.

In addition to knowing what is most important to the business, the most successful security leaders also know how to navigate the organization based on their knowledge of the company's values and culture. Earlier, we discussed iPremier's culture of tight spending and financial focus. In this type of environment, it's important for security activities to be tied to cost-saving measures with strong justification for any security spend.



When discussing stakeholder management earlier in the course, we learned about the power/interest grid and how it can be used to prioritize stakeholders and gauge their impact on any changes to your strategic plan.

iPremier really had no idea of the key stakeholders, their relationship to the crisis at hand, or how they wanted to be involved. By not having this information at hand, Bob Turley was less than convinced about who required his attention most.

The chart above shows our idea of how the stakeholders break out both in terms of interest and in terms of their impact on this particular incident, but also on the overall effect each might have on information security.

As an example, Warren Spangler, the VP of Business Development, has a fairly high level of both interest and power just behind the corporate council and the CEO.

On the other hand, one of the finance people, Linda Kliewer, tries to argue that they should not worry about intrusions because they cannot "prove" that anything was taken. This particular individual has little power and really should have little interest in the overall incident. You will see Linda in Case (C).

Joanne Ripley, on the other hand, is very invested in the incident but has relatively little power, even if she is the SME.

For many reasons, each of these constituents is in need of specific "handling" (style and frequency of communication, for example). Knowing what each requires is very important in making proper decisions regarding the distribution of information during an event like this.

Some of the decisions made would likely have been quite different if there had been a mature stakeholder management and assessment program in place.

Name	**Role**
Jack Samuelson	CEO
Peter Stewart	General Counsel
Tim Mandel	CTO
Warren Spangler	VP, Business Development
Linda Kliewer	CFO
Bob Turley	CIO
Joanne Ripley	Technical Operations Lead

Reference:
https://www.mindtools.com/pages/article/newPPM_07.htm

iPremier PEST Analysis

Political	Economic
• Regulatory obligations (PCI, SOX, etc.) • Investors' reaction and understanding of issues • Insider politics	• Cost of rebuilding network and effect on share price • Potential decrease in profits and cash position as a result of dealing with this crisis • As one of two leaders in this market, niche competition is a macro force
Social	**Technological**
• Employee confidence in company and management • Investor confidence • Consumer confidence • Crisis communications • Company reputation/goodwill	• Issues regarding the age of network equipment • Lack of up-to-date security capabilities • Inability to failover to a clean system • Inventory of software and current patch levels

The chart above shows some of the entries for a PEST analysis form for iPremier. PEST looks at macro forces and, in this case, several forces are close to but external to the incident.

Political:
Regulatory and contractual obligations must be considered regarding reporting and disclosure, for example. Although PCI is not identified in this case, it undoubtedly would be considered a macro force or influencer. Although "soft" is political by nature, the reaction of investors is undoubtedly a "political" type of pressure in this incident. Investors vote with their wallets, and any changes or corrections made will have to satisfy these investors. There is also the case of "insider" politics. Some of the players, in this case, are perhaps looking to make things better for themselves and trying to manipulate the event to their advantage.

Economic:
Rebuilding costs for the network are not strictly external. However, iPremier may find itself at the mercy of the vendors if it is known that it needs to rebuild quickly. There are not likely to be many discounts offered. Pressure in the form of a potential decrease in profits and cash position is also a factor. It may mean less operating capital at a critical time, or it may even make the organization a target for a takeover. The competition also becomes a macro force in this instance. The competition may be likely to seek advantage because of iPremier's position.

Technical:
External or macro forces at play in the technology space include the aging equipment and network structure. If iPremier needs to update and rebuild right now, it likely needs to use the latest version of equipment, which may be costly, have a high learning curve, or be unavailable in a tight time frame. With older technology, there is pressure to make the existing firewalls more secure. This may mean updating firmware or software, and looking to replace the technology itself. There is no evidence of a high availability network, putting pressure on the existing network infrastructure. Further pressure is exerted because there is no clear inventory of software and patch levels, or of fingerprints for existing systems to find good recovery point objectives, or even decide what needs to be rebuilt.

Social:
Employee morale is definitely a pressure point that needs to be considered. Additionally, how will the employees talk about the company and the incident outside the organization?

Shareholders and regulators will likely scrutinize iPremier more carefully going forward. Likewise, consumer confidence in the online retailing capability of the organization will increase external pressure. Pressure will also surely work to force a change in the company's goodwill and reputation.

In reviewing the case, we see that most if not all of these elements were not included in the evaluation. In the event that they were considered, it seems that the correct weighting may not have been applied to each.

This list is not exhaustive. Think of other elements that might influence or should be taken into consideration in this case.

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 5

- Background
  - Case Study Method
- Case Studies
  - iPremier Case (A)
  - ***iPremier Case (B)***
  - iPremier Case (C)
  - PharmaCo Case (A)
  - PharmaCo Case (B)
  - PharmaCo Case (C)
  - HealthHound Case
- Summary
  - Course Summary
  - Resources

This page intentionally left blank.

iPremier Read Case (B)

- On your own
  - Take 5–10 minutes to read the entire case
- As you read the case, think about these questions:
  - Should iPremier shut down and rebuild?
  - Were the security measures iPremier instituted after the attack reasonable?
  - What is missing from its actions to date?
- If you finish reading the case early
  - Start noting key points for further thought and discussion

Take 5–10 minutes to read the case on your own. As you read the case, think about the questions below:

1) Should iPremier shut down and rebuild?

2) Were the security measures (described in Exhibit 1) that iPremier instituted after the attack reasonable?

3) What is missing from what the company has done so far?

HARVARD | BUSINESS | SCHOOL

9-601-115

REV: FEBRUARY 28, 2018

ROBERT D. AUSTIN

The iPremier Company (B): Distributed Denial of Service Attack

A few hours after the attack, iPremier disclosed publicly that it had been the victim of a distributed denial of service attack. A company spokesperson emphasized that the event had lasted only 75 minutes during the middle of night, and that only a few customers had been inconvenienced. Nevertheless, the company stated that it would revisit its already solid computer-security measures. The stock price was not discernibly affected and the event was not a major topic at that afternoon's analyst meeting.

After the attack, the company instituted new security measures, which are listed in **Exhibit 1**. The company was not, however, able to determine whether the firewall had been penetrated. There was no conclusive evidence that intruders had succeeded in tampering with the company's production computer equipment. But there was no conclusive evidence that intruders had *not* compromised the firewall, either. Every file on every production computer was examined for identity and size, but the company's "fingerprint" that told which files should be on production machines had not been kept up-to-date. So there was no guarantee that the file-by-file check of every file would detect, for example, a file that had been replaced by an altered file of the same name.

It was this uncertainty about what had actually happened that led Joanne Ripley to offer a refined recommendation that some still regarded as extreme: disconnect all production computers from the Internet and rebuild the software systems on all of them from development files (which were presumed much less likely to have been tampered with, if there had been intruders). Operations staff estimated that the company would need to completely shut down its business for 24 to 36 hours to complete such a comprehensive rebuild. Although the rebuild processes were theoretically well-documented, some people in operations were concerned that there might be hiccups during the rebuilds that could delay getting everything back online.

Whether to implement Ripley's recommendation was the subject of heated debate among senior managers. Ripley stuck to her guns, noting that the attack had been quite a bit more sophisticated than a routine DDoS attack and that a complete rebuild was "the only way to be sure." Warren Spangler vehemently opposed the plan. "It would be irresponsible of us to take such action," he argued, "knowing that it was certain to significantly degrade customer satisfaction at a time when we are trying

---

Professor Robert D. Austin, Dr. Larry Leibrock (Chief Technology Officer, McCombs School of Business, University of Texas at Austin), and Alan Murray (Chief Scientist, Novell Service Provider Network) prepared this case. This revised version was prepared by HBS Emeritus Professor Richard L. Nolan, Professor Robert D. Austin (Ivey Business School), and Professor Michael Parent (Beedie School of Business, Simon Fraser University). HBS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management. The situation described in this case is based on real accounts of denial of service attacks directed against several companies during 2000 and 2001. Company names, product/service offerings, and the names of all individuals in the case are fictional, however. Any resemblance to actual companies, offerings, or individuals is accidental.

to maintain sales and profit growth in the face of fierce competition." He pointed out that iPremier's situation was pretty much the same as it had been before the attack. Neither before nor after the attack was there evidence that production equipment had been compromised.

Resistance to Ripley's plan led to discussion of another option: They could build a new site in a new facility from development files, then switch the old site off only after the new site was up and running. The company would not have to be shut down and the new site would (probably) be free of any nasty surprises that an intruder might have introduced. This accomplished, argued some, the same thing as Ripley's recommendation, without disruption to the business.

It would, however, be costly to obtain space in a hosting facility and new equipment for a new site. Also, if the production equipment and files had indeed been compromised, keeping the old system live could exacerbate any negative situation. The time it took to create the new site was time when further nastiness might materialize from intruders – if there had been intruders.

"Bad things can happen in three weeks," said Ripley.

Exhibit 1 Security Measures Instituted by the iPremier Company Following January 2018 Attack

- Restarted all production computer equipment (not at the same time—no customer interruptions).
- Conducted a file-by-file examination of every file on every production computer to look for evidence of files or parts of files that should not be present.
- Began a study of technology solutions that might be used to assure that files on production computers were the same files initially installed there.
- Expedited a project aimed at moving to a more modern hosting facility.
- Modernized computing infrastructure to include a more sophisticated firewall.
- Bought additional disk space and enabled high levels of logging so there would be more diagnostic information available after any future attacks.
- Trained more staff in the use of monitoring software; educated all about security threats.
- Created an incident-response team and practiced a simulated attack.
- Began an executive search for a Chief Security Officer.
- Retained a cybersecurity consulting firm.
- Instituted monthly third-party security audits.

Source: Casewriter.

iPremier Case (B) Case Analysis

- Analyze iPremier actions
  - Should iPremier shut down and rebuild?
  - Were the security measures iPremier instituted after the attack reasonable?
  - What else do you recommend?
- Identify tools to use
  - What tools from previous sections can be applied?
- 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 case answers

iPremier

After you have finished reading the case write down answers the questions below:

1) Should iPremier shut down and rebuild?

2) Were the security measures (described in Exhibit 1) that iPremier instituted after the attack reasonable?

3) What else do you recommend? What is missing from what the company has done so far?

4) What tools or management techniques should be used to improve iPremier's security program?

iPremier Case (B) Debrief

Note that this section contains a debrief and potential case answers

Please note that this section contains a debrief and potential case answers. The instructor will walk through this section with the class after you have analyzed the case.

Security Measures Implemented by iPremier

- Reasonable
  - Enabled high levels of logging and trained staff to use monitoring software
  - Created incident response team and practiced a simulated attack
  - Investigated additional technical solutions and modern hosting facility
  - Instituted third-party audits
  - Began search for Chief Security Officer
- Unreasonable
  - Suggestion of shutting down the site to rebuild
  - Reasoning that it's "the only way to be sure"
  - Strict technical recommendation does not factor in the risk of losing business
- Questionable
  - Restarting all production systems
  - Conducting file-by-file examination of every file, despite out-of-date fingerprints

Now that the attack is over, iPremier has implemented a number of action items and publicly announced it would "revisit its already solid computer security measures." There are certainly initial elements of an information security program that should be put into place. However, we know that iPremier is far from having everything under control. The security measures described in Exhibit 1 indicate a lack of understanding about information security.

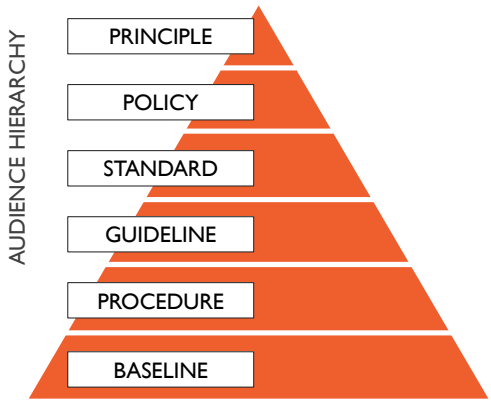
Some of the measures implemented by iPremier are reasonable, including starting additional logging and monitoring, creating an incident response team, instituting third-party audits, and starting a search for a Chief Security Officer (CSO). However, from what we know about iPremier's culture, the CSO may simply be a scapegoat who does not actually have the ability to make meaningful improvements.

The lack of understanding of information security is highlighted by some questionable actions, including restarting all production systems, which could result in the loss of valuable evidence of intrusions, and conducting file-by-file examinations of key system files using unreliable fingerprints.

In addition to technical issues, there is the unreasonable suggestion that the site be brought down to do a complete rebuild. The reason that it is "the only way to be sure" that the attackers are no longer in the environment reflects a complete disconnect on how to manage risk and align with business goals.

iPremier Gaps

- Need to think more strategically about the security program
  - Security program development
    - Framework, maturity model, gap analysis, roadmap
  - Policy, standards, guidelines, baselines
  - Processes and procedures
  - Data classification
  - Governance



For iPremier, a lack of planning has resulted in an incomplete analysis in the best case and detrimental decision making in the worst case. The company needs to regroup and think about developing its security program based on a strategic plan that includes a framework, maturity model, gap analysis, and roadmap all tied to clear business goals, which are socialized with key stakeholders.

Part of the strategic plan must address iPremier's gap in policies, standards, guidelines, and procedures.

Policies define what we should be doing. iPremier had few if any security policies. It is not entirely surprising given that many significantly sized companies have very little in the way of security policy, in some cases having only a very infrequently reviewed and updated document.

Standards define how we should be applying controls across the organization. iPremier does not appear to have a set of standards for incident response or information security.

Guidelines are in some cases less dogmatic, but they tell us what "best practice" is for our organization to achieve control targets. iPremier again does not appear to have a set of guidelines for information security.

Procedures tell us how the individual should go about implementing controls to meet higher policy objectives. iPremier has some procedures. However, they appear to be outdated and potentially untested.

iPremier, like many organizations to this day, was a victim of its own lack of understanding of security risks and how they translate to business risk. By understanding business risks and the importance of key assets and data, iPremier will be much better positioned to effectively manage and govern security risks.

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 5

- Background
  - Case Study Method
- Case Studies
  - iPremier Case (A)
  - iPremier Case (B)
  - ***iPremier Case (C)***
  - PharmaCo Case (A)
  - PharmaCo Case (B)
  - PharmaCo Case (C)
  - HealthHound Case
- Summary
  - Course Summary
  - Resources

This page intentionally left blank.

iPremier Read Case (C)

- On your own
  - Take 5-10 minutes to read the entire case
- As you read the case, think about these questions:
  - How should iPremier handle breach communications?
  - What else does it need to do from a governance perspective?
- If you finish reading the case early
  - Start noting key points for further thought and discussion

Take 5-10 minutes to read the case on your own. As you read the case, think about the questions below:

1) How should iPremier now handle breach communications?

2) What else does it need to do from a governance perspective?

HARVARD | BUSINESS | SCHOOL

9-601-116

REV: FEBRUARY 28, 2018

ROBERT D. AUSTIN

The iPremier Company (C): Distributed Denial of Service Attack

The iPremier Company's senior management decided not to shut down the business for a comprehensive rebuild of all production platforms. Using whatever equipment they could scrounge from other uses (to reduce cost and impact on profits), they *did* embark upon an accelerated plan to create an iPremier site in a more up-to-date hosting facility.

Two weeks later, on January 26, a call from FBI Special Agent Donald Reedy in Washington, D.C., was routed to Bob Turley's desk. Reedy informed Turley that for the past two hours the iPremier Company's biggest competitor, MarketTop, had been experiencing a distributed denial of service attack. The source of the attack, Reedy explained, was inside iPremier's production computing installation.

The iPremier operations staff quickly located and killed computer processes that were the sources of the attack. A file that had spawned some of the processes resided on a database server. This proved that the firewall had been penetrated. Computer security experts whom Ripley and Mandel consulted speculated that the January 12 distributed denial of service attack against iPremier might have been a misdirection tactic, to divert attention from hacking. This sort of "suppressing fire during retreat" was a common tactic used by sophisticated hackers, according to these experts.

The senior team now faced three difficult issues.

The first was familiar: whether to immediately implement Ripley's rebuild recommendation. Some still resisted this idea, arguing that the MarketTop attack might be the full extent of the nastiness the intruders had intended and that the other site would be up soon (although it was now looking more like four to six weeks to get it up and running). Moreover, Legal Counsel Peter Stewart pointed out that the issue was now more complicated. Since iPremier computers had been the source of an illegal attack, the FBI might well consider a rebuild to be destruction of evidence of a crime.

The second issue was also legal in nature: how to handle the situation between iPremier and competitor MarketTop. Stewart suggested that MarketTop could probably mount a lawsuit against iPremier for its apparent role in the January 26 attack. It was not certain that they would do it, though,

---

Professor Robert D. Austin, Dr. Larry Leibrock (Chief Technology Officer, McCombs School of Business, University of Texas at Austin), and Alan Murray (Chief Scientist, Novell Service Provider Network) prepared this case. This revised version was prepared by HBS Emeritus Professor Richard L. Nolan, Professor Robert D. Austin (Ivey Business School), and Professor Michael Parent (Beedie School of Business, Simon Fraser University). HBS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management. The situation described in this case is based on real accounts of denial of service attacks directed against several companies during 2000 and 2001. Company names, product/service offerings, and the names of all individuals in the case are fictional, however. Any resemblance to actual companies, offerings, or individuals is accidental.

because the suit would become public and bring attention to both companies that neither wanted. There was no agreement on whether or how to approach MarketTop.

The third issue was also familiar: What to say publicly. The database server that had been compromised contained credit card numbers. This meant that someone *could have* stolen credit card numbers. But it did not prove that anyone had *actually* stolen credit card numbers. iPremier could not identify individual customers who had been affected. The issue that was discussed heatedly by the senior team was what the company should disclose publicly. Stewart also suggested that iPremier could be in violation of its credit card processing agreement covenants, and if so, lose the ability to process credit card payments.

Turley argued in favor of disclosing what might have happened. Linda Kliewer, iPremier's Chief Financial Officer (CFO), offered a different view:

> "Suppose someone broke into our offices and I'd left some customer information in one of my unlocked desk drawers. Sure, they could have gone into my desk and made copies. But did they? There are many things pranksters might have done. Suppose my desk drawer is just as I left it, to the best of my ability to confirm. I don't have any evidence that they actually did go into my desk. In a case like that, would we go public to say that it is within the realm of possibility that the burglars took some customer information?"

This page intentionally left blank.

This page intentionally left blank.

iPremier Case (C) Debrief

Note that this section contains a debrief and potential case answers

Please note that this section contains a debrief and potential case answers. The instructor will walk through this section with the class after you have analyzed the case.

Approach to Breach Communications

- Certain disclosures are mandatory
  - PCI, SOX, HIPAA, SEC, etc.
- But the approach depends on organizational culture
  - Open versus closed
  - Liberal versus conservative
  - Transparent versus secret
- No question that the "right" thing to do is notify customers and competitors
  - Should law enforcement be engaged?

iPremier finds itself in the difficult situation of dealing with a crisis and having to determine how to handle not only the breach but crisis communications in a very short amount of time. With appropriate planning, the company should already know that certain disclosures are mandatory. For example, the U.S. Securities and Exchange Commission (SEC) requires public companies to disclose cybersecurity risks and incidents on a regular basis. It has time to conduct those disclosures in addition to those required by PCI, SOX, HIPAA, and other regulatory requirements.

The question of how to handle crisis communications will depend largely on the organizational culture. A more conservative or secretive organization may err on the side of disclosing less information to the public. An organization with a more transparent culture may be more apt to "lay its cards on the table" and share details more willingly. In this case, the "right" thing to do is to notify customers and its competitor, MarketTop, which was affected. Legal and compliance will, of course, have to be involved also.

In addition to the approach for handling crisis communications, organizations must plan ahead on how they want to engage law enforcement. In some cases, law enforcement must be engaged based on the type of case. Some organizations, like government entities, may have predefined criteria for engaging law enforcement. For other organizations, security leaders should socialize with other business leaders on the approach to bringing law enforcement into a case. In some cases, law enforcement may have different incentives from the organization as a whole. In any case, it will be important to define the scope of any law enforcement engagement.

Security Governance

- Cybersecurity is an enterprise risk management issue
  - Not just an IT issue
- Responses to risk
  - Avoid, Mitigate, Transfer, Accept
- Number of items to consider to improve risk management
  - Risk Steering Committee
  - Business Continuity Planning (BCP)
  - Disaster Recovery (DR)
  - Cyber insurance

The iPremier case highlights that effectively governing cybersecurity requires that we no longer treat it as just an IT issue. Cybersecurity is an enterprise-wide risk management issue and must be treated with as much care as other critical business risks. This is exactly why C-level executives and boards of directors have security as one of their top priorities.

A key for security business leaders is to go beyond technical details and understand that there are no security risks. There are only business risks. The primary ways that an organization can respond to risk:

- Avoid the risk
- Mitigate the risk
- Transfer the risk
- Accept the risk

Organizations make risk management decisions all the time. Ultimately, this is a business decision that should be addressed by executives and business owners. As security business leaders, we have a duty to frame the discussion in a way that resonates with key stakeholders, provide appropriate governance, and ensure that risks are managed in a conscious manner. In many organizations, this effort often involves something like a Risk Steering Committee in which security risks can be managed and actively decided upon. The way that the business decides to manage risk naturally has ties to Business Continuity Planning (BCP), Disaster Recovery (DR), and even cyber insurance decisions because these are all ways to mitigate or transfer risk.

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 5

- Background
  - Case Study Method
- Case Studies
  - iPremier Case (A)
  - iPremier Case (B)
  - iPremier Case (C)
  - ***PharmaCo Case (A)***
  - PharmaCo Case (B)
  - PharmaCo Case (C)
  - HealthHound Case
- Summary
  - Course Summary
  - Resources

This page intentionally left blank.

PharmaCo Case Overview

- Publicly traded pharmaceutical company
  - Family owned with consistent growth over decades
  - Considering a merger with another company
- Security is getting more visibility
  - Hired first CISO one year ago
  - Having first board level security briefing

PHARMACO

PharmaCo is a large, publicly traded pharmaceutical company with a long history. It was started as a small, family run business and remains, to this day, 30% owned by the family. The company has been led for multiple generations by CEOs from the same family and has had steady growth for decades. Recently, another pharmaceutical company reached out to a board member to start a conversation around a potential merger.

It is against this backdrop that PharmaCo hired their first CISO, Paul Williams, a little over a year ago. Paul reports directly to the CFO along with his peer the CIO. In his time at the company Paul has been improving the security capabilities of the organization and is presenting to the board for the first time.

PharmaCo Read the Case

- On your own
  - Take 30 minutes to read the entire case
- As you read the case, think about:
  - What strategic planning tools are covered in the case?
  - What are PharmaCo's crown jewels?
- If you finish reading the case early
  - Start noting key points for further thought and discussion

PHARMAC

Take 30 minutes to read the entire case. If you finish reading the case early, start noting key points for further thought and discussion.

As you read the case, ask yourself:
- What strategic planning tools are covered in the case?
- What are PharmaCo's crown jewels?

IVEY | Publishing

SFU BEEDIE SCHOOL OF BUSINESS
SIMON FRASER UNIVERSITY

W20218

PHARMACO

It was a crisp September day—one of those days that sticks in your memory, when the oppressive heat and humidity of summer have finally given way to the cool breezes and colours of fall. So, it was with good humour that PharmaCo's board of directors gathered to discuss second-quarter results and strategic plans for the year end.

PharmaCo was on track for record-breaking performance. The company had been approached a month earlier by a competitor who proposed merging the companies. An initial approach had been made, along with a veiled suggestion that should the merger not go through, the competitor might decide to acquire PharmaCo anyway. Management had begun putting a deal book together and had included basic early analyses in the board package prior to beginning negotiations. News of the approach was being guarded closely, limited to the executive leadership team (ELT) and the board.

In some ways, the board was relieved that the meeting seemed otherwise routine. They expected that a lot of time would be spent discussing the proposed merger, reviewing management's initial analyses and recommendations in detail, and deciding on a strategy to either proceed with negotiations, reject and repel the acquirer, or even acquire the competitor, in turn.

It promised to be an interesting discussion.

PHARMACO

Early Days

PharmaCo, as it eventually became known, was founded by Robert "Bob" Kingsley in 1923 as The Compound Pharmacy, a local business in Kingsley's medium-sized hometown. Kingsley, whose family had deep, multi-generational roots in the community, was born in 1887. He followed his physician-father into health care and trained as a pharmacist. Kingsley served in World War I as a pharmacist in a military hospital overseas and never forgot the casualties he had helped treat. He returned from the war a changed man, determined to make a change in the way patients were treated, especially for pain and pain management. The Compound Pharmacy was founded as both a retail and research operation. Kingsley and his assistant pharmacist (a former military pharmacist's assistant who had served with Kingsley) attended

to customers at the front of the store, while in the back, Kingsley ran a research laboratory that focused mainly on innovative compounds and analgesic (pain-relieving) medicines.

At the time, pain relievers ranged from mild, non-narcotic medicines such as acetylsalicylic acid (ASA) to more powerful, potentially addictive narcotics such as codeine and morphine. ASA, more commonly known by its trade name, Aspirin, had been developed by chemist Felix Hoffman at Bayer in Germany in the 1890s. It became one of the first "blockbuster" multimillion-dollar drugs, moving from having to be prescribed to becoming a commonly available, over-the-counter (OTC) drug. In fact, this was largely how the pharmaceutical industry divided itself: into prescription drugs (commonly referred to as "Rx," the short form for the Latin word *recipe*, which translated literally as "take this") and OTC drugs.

Kingsley's breakthrough came when he was able to marry ASA with a small amount of mild narcotics into a time-release, slow-dissolving capsule that allowed for the long-term management of chronic pain without the more addictive side-effects of strong narcotics. He patented the formulation, branded it, aggressively marketed it, and soon built a sizable business that included production and distribution regionally and, eventually, nation-wide. Kingsley's medications were being prescribed in growing numbers by physicians in hospitals as well as in private practices.

Growth

The Compound Pharmacy became PharmaCo, a privately-held family enterprise, in 1935. Expansions in production and distribution led the business to grow. Kingsley also saw the world inevitably moving toward another war in Europe, so he decided to expand his business with a view to supply not only national prescribers and pharmacies but also, potentially, the allied armed forces that he expected would soon be fighting in Europe.

World War II, as this devastating conflict eventually became known, was nonetheless good for business, and PharmaCo thrived on producing and delivering much-needed medication to troops abroad and convalescing soldiers at home. By the war's end in 1945, PharmaCo had grown, mainly through the strategic acquisition of regional and national competitors, into a medium-sized, diversified, integrated pharmaceutical company with a wide portfolio of branded Rx and OTC therapeutics. With sales in excess of $250 million and healthy earnings before interest, taxes, depreciation, and amortization of 12 per cent, PharmaCo was a strong competitor, even if large, integrated pharmaceutical companies had revenues three to five times that of PharmaCo.

Kingsley remained chief executive officer (CEO) until his death in 1962. At that time, his son, Robert Kingsley Jr. (aged 35), assumed the CEO's duties. Robert, as he was known, was also a pharmacist. However, unlike his father, he had never practised. After finishing his pharmaceutical studies, he completed an MBA at Harvard Business School. He worked in investment banking for a few years, then joined the family firm, rising through the ranks in a series of appointments that spanned the gamut of the organization's operations. His last posting was as chief financial officer (CFO) and his father's second-in-command. There was no doubt that he would succeed Kingsley. Kingsley and Robert had shepherded the company through a series of successful acquisitions, progressively growing the business and its profitability.

Going Public

Robert Kingsley's biggest initiative was taking the company public in 1965. At the time, PharmaCo had sales operations in Canada, the United States, Mexico, South America, the United Kingdom, and France.

In later years, the company also expanded into Ukraine and China (the latter mainly due to strategic acquisitions of intellectual property and manufacturing). Manufacturing operations, along with research and development (R&D) labs, were mainly in North America (the United States, Canada, and Mexico), the United Kingdom, and China. By the end of the millennium, PharmaCo was a billion-dollar conglomerate with over 10,000 employees.

The family still retained significant control of the company with a 30 per cent block of shares. As such, it was a straightforward process when, in 1999, Robert ceded the CEO's job to his eldest son, Robert Kingsley III (Trey), then 37 years old. Like his father and grandfather before him, Trey had completed a health science undergraduate degree in pharmacology and followed his father to Harvard for an MBA.

For the most recent nearly two decades, PharmaCo had seen steady, if not spectacular growth, and a return to shareholders that exceeded the average. As a result, the stock market and analysts had been kind to the firm, and it enjoyed a healthy share price. Its shares were not widely traded; they were narrowly held by the family (30 per cent), institutional investors (30 per cent), and both individual and corporate investors, including the company's employees, who could take advantage of a generous stock ownership plan.

Management and Governance

PharmaCo's management team was the usual mix of talent seen in an integrated pharmaceutical company (see Exhibit 1). The ELT consisted of Trey Kingsley and his seven direct reports: Pat Provost, CFO and chief risk officer (CRO); Leslie Jones, chief marketing officer; Jack Paulson, senior vice-president responsible for all operations, including production and distribution; Claude Chastain, chief human resources officer; Dr. Evelyn Rutledge (Ph.D. in biochemistry), vice-president, regulatory affairs; Dr. Elizabeth Bowen (MD, Ph.D.), the chief scientist and vice-president, R&D; and Frank Maneri, the firm's general counsel (chief lawyer) and corporate secretary.

One level down in the company's structure, two executives reported directly to Provost: Amrit Pal Singh, PharmaCo's chief information officer, and Paul Williams, the company's chief information security officer (CISO). Three divisional vice-presidents responsible for all operations in each of the firm's geographical markets reported to Paulson.

The group was notably cohesive and worked well together. Interactions were not without tension, but it was the healthy kind of tension that characterized high-performing groups. Each executive had been carefully recruited through an extensive process that involved multiple interviews and both formal and informal meetings with Trey Kingsley, the board of directors, and other executives. In some cases, it took over six months to hire.

The most recent addition to the team had been Williams as CISO, one year ago. The company had recognized the need to protect its considerable data assets and had hired Williams to develop and implement a more sophisticated approach, along with policies and procedures for data and information protection in the organization, including a cyber-breach playbook.

Executives at PharmaCo were well compensated, with a compensation target set at 125 per cent of the industry average, including salary, bonuses, and stock options.

PharmaCo's board of directors was equally impressive (see Exhibit 2). The firm had 11 directors, including Trey Kingsley as its chair and Provost as the second executive director. The nine additional, non-executive directors were all independents, with Arthur Schulz, a lawyer and long-time Kingsley family friend and advisor, as the

vice-chair and lead director.[1] Collectively, the board had a good mix of industry experience, strategic ability and experience, and specific skills. All members were successful, proven leaders who had excelled professionally. They were all committed directors and actively engaged in overseeing PharmaCo's business.

There were four committees: audit; risk; governance and nomination; and human resources and compensation. Each committee was chaired by an independent director and had three members. The committees met regularly, at least quarterly and sometimes monthly, well in advance of board meetings. Directors were required to own shares in the company equivalent to one year's compensation (having four years after their initial appointment to meet this requirement). They were well compensated in cash and options at 125 per cent of their pay comparator group. Directorship had both term and age limits. Directors were allowed to serve no more than three five-year terms and aged out at 78 years old.

Information and Information Management

Like most integrated pharmaceutical companies, PharmaCo had in its possession large amounts of sensitive data. In addition to the plethora of information found in most large companies (financial information, cost structures, production information, employee information, sales and marketing data, customer information, etc.), PharmaCo had a large amount of highly sensitive health information (measured in terabytes of data space). This included patient information from clinical trials, R&D, clinical results, hospital and health insurance data, and all data that covered the company's many drug and processing patents, patented processes, and other valuable intellectual property.

The firm considered its information technology (IT) infrastructure to be sophisticated and mature. Data were physically and logically separated on encrypted on-site servers as well as at three separate and distinct encrypted backup sites. The company adhered to the NIST Cybersecurity Framework,[2] and Williams had developed and implemented a number of policies and procedures in his first year on the job that had led to the development of a sophisticated information management approach. Part of the process included a plan for regular reports to be given to the executive team and the board. The first such report was on the agenda for the Q2 board meeting (see Exhibit 3).

PharmaCo had never been hacked but was ready for the eventuality with draft business continuity, incident response, and disaster recovery plans. Williams had not yet managed to create a cyber-breach playbook, but he had this on his work plan for the coming year, along with more thorough testing of the response plans.

THE PROPOSED MERGER

At a highly confidential meeting, the chair of one of PharmaCo's competitors, a company roughly the same size and in similar markets but with complementary branded drugs and therapeutics, approached Schulz with the idea of merging the two companies. The competitor's chair argued that their respective companies were more co-operators than competitors; that is, they had a suite of complementary products. Her firm focused mainly on OTC products, with a limited suite of branded Rx products. Moreover, the competitor's Rx products were injectables—a product category that PharmaCo had, up until that time, avoided, owing

[1] It was common in companies where the chair of the board was also the CEO or president of the board to appoint a lead director from among the board's non-executive, independent directors to chair the meetings when discussing matters conflicting with the CEO (for example, when deciding on the CEO's compensation).

[2] The NIST Cybersecurity Framework, published by the US National Institute of Standards and Technology, was a voluntary system of standards, guidelines, and practices recommended to organizations to manage and reduce their cybersecurity risk; "Cybersecurity Framework," NIST, accessed January 10, 2019, www.nist.gov/cyberframework.

to their manufacturing and regulatory complexities. The competitor's chair also asserted that the two companies were in similar markets but that her company had expanded into markets where PharmaCo was not present. In sum, merging the two companies would present a great opportunity for long-term, sustainable value creation for the shareholders. Not only would a bigger and stronger company emerge, but significant cost synergies would also be possible.

Because both firms' share prices and market caps were roughly the same, the competitor's management team and advisers had concluded that a merger made the most sense. That approach would avoid what might evolve into a long, protracted, and expensive takeover. Both chairs knew that most such acquisitions failed, and even when they succeeded, they were much more expensive and time-consuming to conclude. The competitor's chair had approached Schulz with the idea, based partly on their long-standing professional relationship and partly from a desire to discharge their respective duties of care and fiduciary duties to both companies.

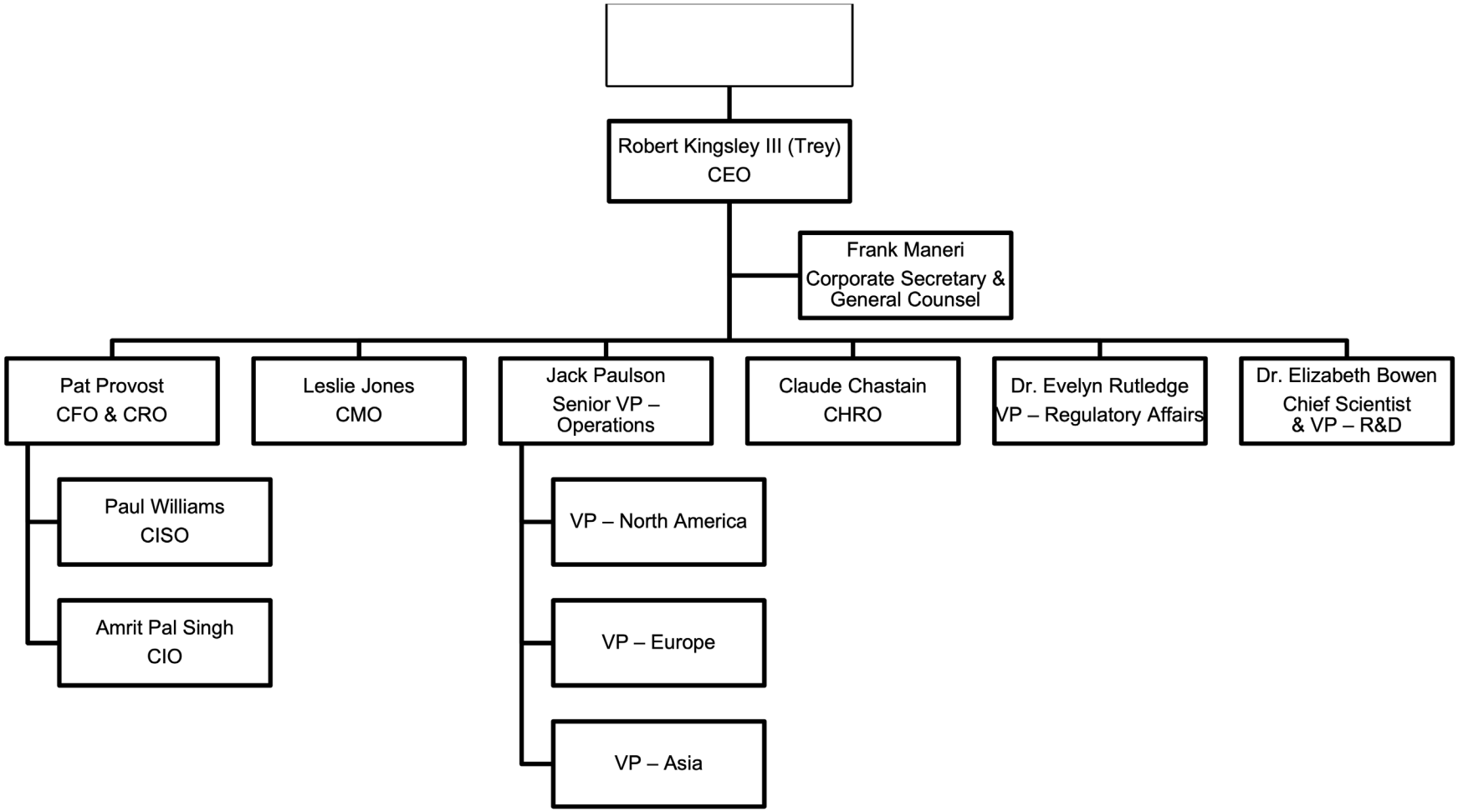
Schulz had quietly and confidentially reported the contact to Trey Kingsley, as was his duty. Schulz approached the issue cautiously, knowing that the Kingsley family's 30 per cent holding of PharmaCo shares inspired confidence in investors. To Schulz's surprise, Trey expressed cautious interest in the deal and told Schulz that he would instruct Provost, the CFO, to assemble a deal team, retain mergers and acquisitions advisors, and begin conducting a preliminary investigation into the merger. Trey shared all of this with the board in a conference call, warning the directors to not repeat it and to communicate only with him, Schulz, or Provost.

The internal PharmaCo deal team had spent the previous month on the project, assessing the pros and cons of the deal. The team would be presenting its findings to the board at the second quarter (Q2) meeting. To maintain secrecy, the team had not included detailed materials in the board package, just a high-level overview, preferring instead to brief the board in person. Management's recommendation, though, was to proceed with the merger and enter into preliminary negotiations with the other company.

THE Q2 BOARD MEETING

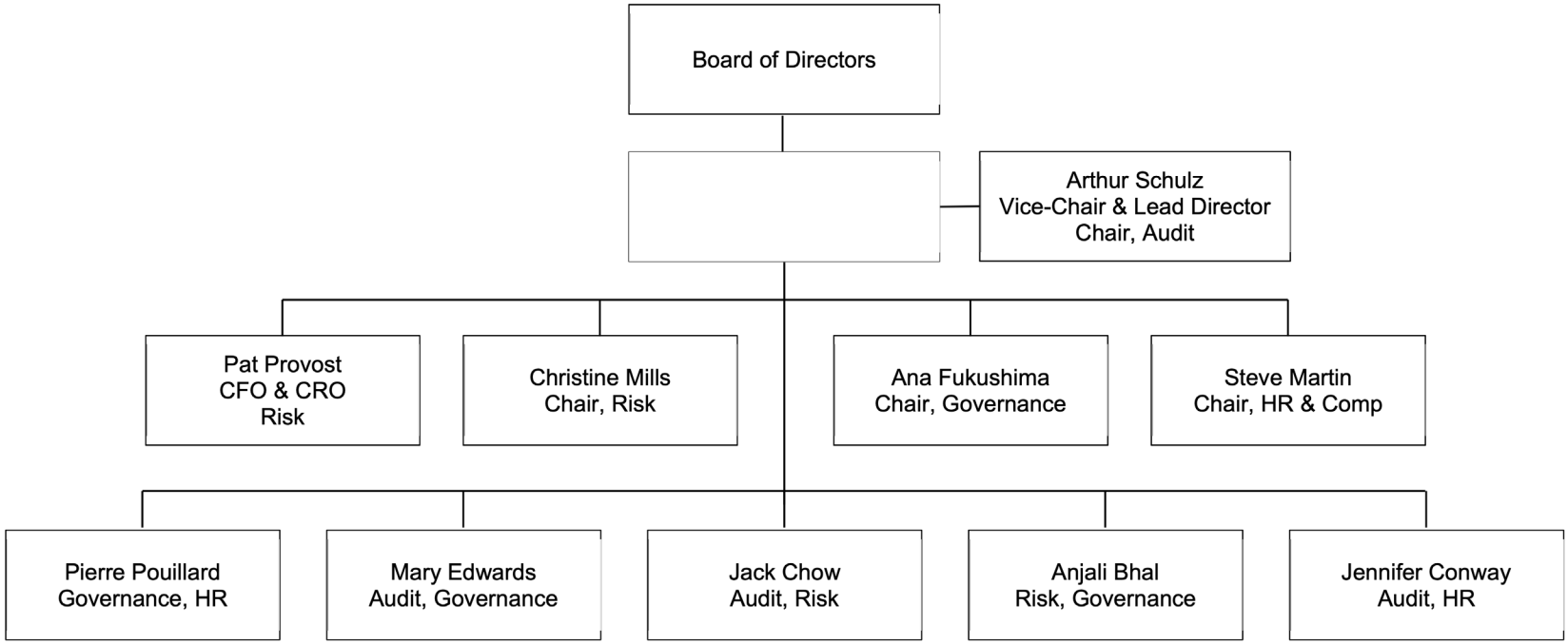
PharmaCo's directors were not unanimous in supporting the merger but were keeping an open mind. This was a potentially billion-dollar-plus deal, and they knew that prudent guidance and oversight would be critical to the company's future. It promised to be an interesting discussion.

EXHIBIT 1: PHARMACO ORGANIZATION CHARTS



Note: CEO = chief executive officer; CFO = chief financial officer; CIO = chief information officer; CISO = chief information security officer; CMO = chief marketing officer; CRO = chief risk officer; R&D = research and development; VP = vice-president.
Source: Company files.

EXHIBIT 2: PHARMACO BOARD OF DIRECTORS & COMMITTEE ASSIGNMENTS



Committee Membership

	Audit	Risk	Governance & Nomination	HR & Compensation
Chair	Arthur Schulz	Christine Mills	Ana Fukushima	Steve Martin
Members	Jack Chow	Anjali Bhal	Anjali Bhal	Jennifer Conway
	Jennifer Conway	Jack Chow	Mary Edwards	Pierre Pouillard
	Mary Edwards	Pat Provost	Pierre Pouillard	Arthur Schulz

Note: CFO = chief financial officer; Comp = compensation; CRO = chief risk officer; HR = human resources.
Source: Company files.

EXHIBIT 3: PHARMACO BOARD CYBER REPORT

PharmaCo: Q2 Cyber Brief

1 of 2

1. External Cyber Incidents

1. According to industry reports there has been a 50% increase in reported phishing campaigns aimed at Pharmaceutical companies. There have been 9 such campaigns reported in the last quarter.

2. Internal Cyber Incidents

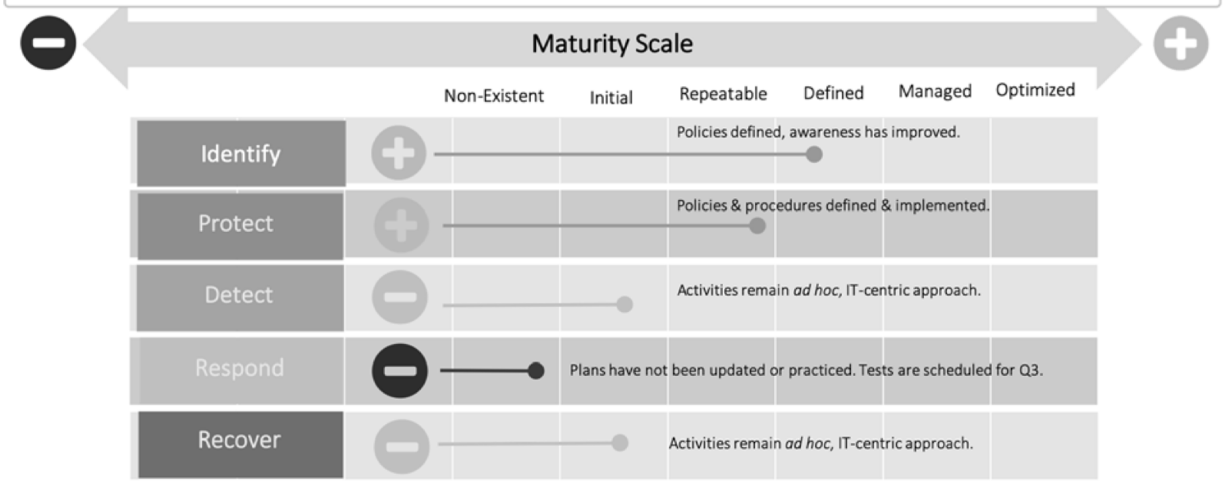
1. There were 25 phishing campaigns aimed at members of the Executive Team, with no business impact.
2. There were 9 phishing campaigns aimed at IP assets, with no business impact. .

3. Narrative

- Industry phishing metrics have increased by 50% & internal phishing campaigns by 300%.
- Cyber teams are puzzled – and are investigating what is the potential root cause and why internal numbers are higher.
- Currently no business impact. We plan to monitor more closely and adjust Operations as necessary, reporting back as needed.
- Upcoming cyber exercises in Q3 and Q4:
  - Red /Blue Team exercise
  - 3rd-party Penetration testing
  - Enterprise Phishing training campaign and test.

PharmaCo: Q2 Cyber Security Maturity Scorecard

2 of 2



*Note: The scorecard is based on the NIST Cyber Security Framework.

Source: Company files.

This page intentionally left blank.

PharmaCo Case (A) Case Analysis

- Analyze PharmaCo actions
  - What strategic planning tools are covered in the case?
  - What are PharmaCo's crown jewels?
- Prepare your thoughts for a class debrief
  - Write down your key points

Decipher | Develop | Deliver

NOTE

Don't read the next section

It contains a debrief and potential case answers

PHARMACO

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

Throughout the class we have been covering various tools used in our strategic planning process. The PharmaCo case gives us an opportunity to analyze which tools were used to Decipher, Develop, and Deliver improvements to the organization. The case study does not explicitly call out these tools. Instead, what we see is the output of these tools. Let's be more explicit and identify what tools were used to get PharmaCo to this point.

1) What **Decipher** tools are covered in the case?

2) What **Develop** tools are covered in the case?

3) What **Deliver** tools are covered in the case?

4) What are PharmaCo's crown jewels?

PharmaCo Case (A) Debrief

Note that this section contains a debrief and potential case answers

Please note that this section contains a debrief and potential case answers. The instructor will walk through this section with the class after you have analyzed the case

PharmaCo Strategic Planning Activities

Phase	*Strategic Planning Tool*	*Example from case study*
Decipher	❑ Historical Analysis	Overview of company history
	❑ Business Strategy	M&A, worldwide production/distribution, new IP
	❑ Asset Analysis	IP, R&D, clinical trials/results, patented processes, PII
	❑ Stakeholder Management	Org chart, background on executives & board members
Develop	❑ Security Framework	Use of NIST CSF
	❑ Gap Analysis	Identification of less mature functions
	❑ Security Roadmap	Maturity scale mapped to CMMI
	❑ Policy Development	Developed and implemented policies & procedures
Deliver	❑ Security Metrics	Phishing metrics
	❑ Executive Communications	Board presentation, reports to executive team

Decipher Tools
The PharmaCo case study, like most business case studies, provides a comprehensive overview of the history of the company from founding to present day. We learn that it is still a family controlled business and they have a long history of innovation. It is clear that the analyst conducted a thorough historical analysis.

It is not always explicitly stated but, by reading between the lines, we can see how PharmaCo has become successful and implemented their business strategy. They have grown over the years via acquisition and have developed production and distribution operations around the world. Underlying this of course, is the consistent investment in the development of new drugs and intellectual property. All these activities have proven to be sustainable business moats, as evidenced by the consistently (if not spectacularly) increasing share price.

The case study also clearly lists out various PharmaCo assets. These are important for security leaders to understand to determine which items are actually the "crown jewels". Certainly, PharmaCo has a large amount of sensitive data about employees, customers, sales/marketing, and financial information. While this data must, of course, be protected and is often required to be protected via regulation, such data are not often actually the crown jewels. The aforementioned worldwide production and distribution systems and processes are likely more important for the business. Additionally, any data related to the business strategy such as drug formulae, clinical trial results, R&D information, and M&A information and more likely to be considered the crown jewels.

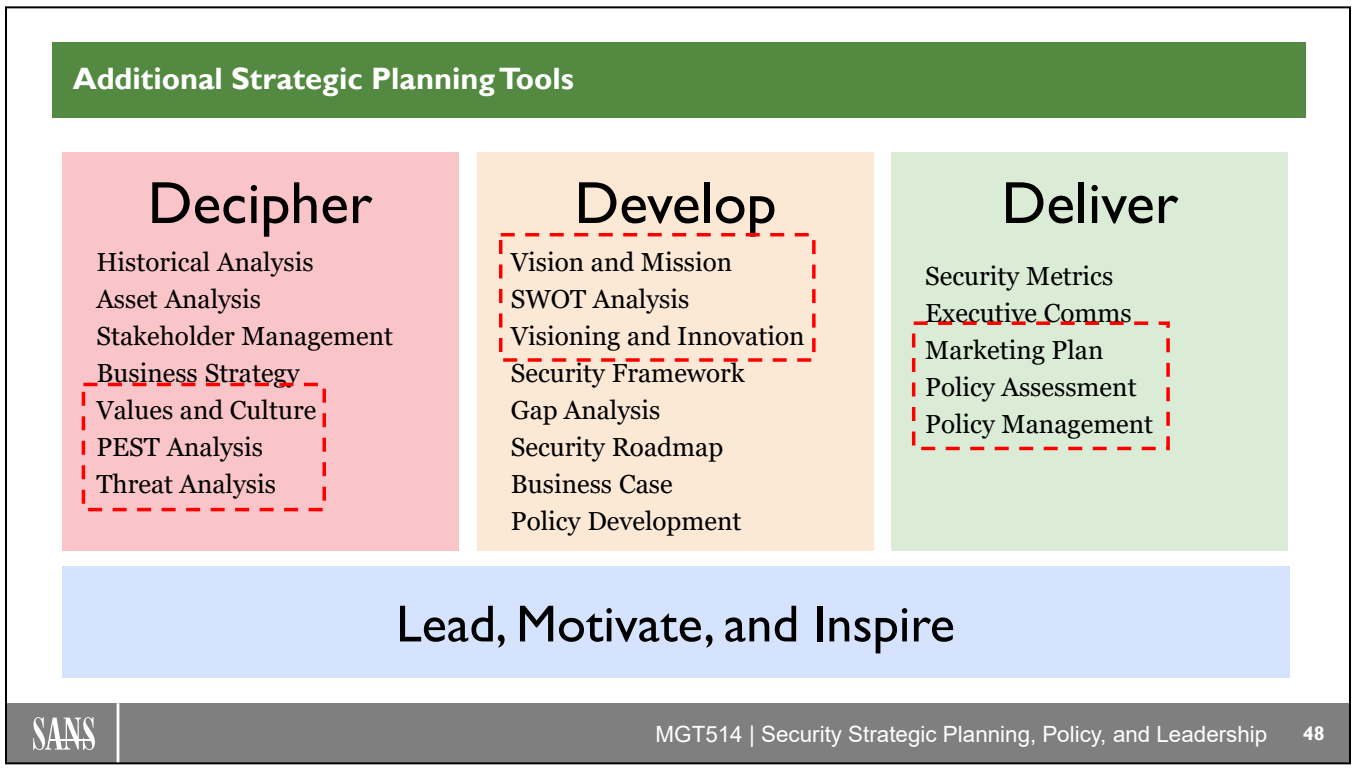
We also see the high-level org charts for PharmaCo. This directly informs where we want to start our stakeholder management activities. The case also gives us good insight on the background of specific leaders along with their history at the company. The structure of the company also informs what is most important. For example, there are dedicated executives for worldwide business operations, regulatory affairs, and R&D.

Develop Tools
One of the first things the new PharmaCo CISO did was to utilize the NIST Cybersecurity Framework (CSF). This is a good first step to provide structure for a gap analysis to identify what was or was not being done.

This gap analysis feeds directly into the creation of a security roadmap, which we see in the form of maturity levels mapped to CMMI in the case document. Finally, the CISO developed and implemented various policies and procedures that “led to the development of a sophisticated information management approach”.

Deliver Tools

It’s in this phase that we see the need for improvement. There are some basic phishing metrics included in the case study along with the information for the first board presentation. Security reports are also given to the executive team on a regular basis but it has taken an entire year to get to the point of doing the first board briefing.



A lot of good work has been done to date at PharmaCo but, by looking at our strategic planning process we see that there is room for continued improvement. The tools highlighted by the dashed boxes above should also be used when conducting comprehensive strategic planning.

Decipher Phase
Due to the fact that the company has been family controlled since its founding we can possibly infer some things about how the organization might be run. However, it is not explicitly stated. As a security leader, this is something you want to understand much sooner than later. Also, there can be a deeper analysis of the threats that the organization is facing. PharmaCo certainly knows that business disruptions such as inability to ship products can lead to not only lost revenue, but more importantly patients not being able to obtain life saving or life sustaining medicines. This can lead to brand damage, lawsuits, and even regulatory actions. A comprehensive PEST analysis will help to structure these threats. Also, deeper threat analysis is necessary to go beyond the simple phishing metrics that are included in the case study.

Develop Phase
The case study does not explicitly state the mission of PharmaCo. As a result, the security team does not have an explicit tie to PharmaCo's guiding light. This can be flushed out for the security team by understanding the cone of plausibility and what sustaining innovations can be developed to enable various business processes. The SWOT analysis will also help to summarize the current state and identify areas of focus.

Deliver Phase
While a comprehensive policy library has been created, continual assessment and policy management is needed in anticipation of changing technology and business requirements. Finally, it is imperative that you take credit for all the hard work you have done building the security program. Make sure you have a marketing plan in place to help spread the word and position your team appropriately.

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 5

- Background
  - Case Study Method
- Case Studies
  - iPremier Case (A)
  - iPremier Case (B)
  - iPremier Case (C)
  - PharmaCo Case (A)
  - ***PharmaCo Case (B)***
  - PharmaCo Case (C)
  - HealthHound Case
- Summary
  - Course Summary
  - Resources

This page intentionally left blank.

PharmaCo Case (B) Case Analysis

- Analyze board material
  - How would you improve the presented security metrics?
  - What is missing from the "Q2 Cyber Brief"?
  - How would you improve the "Q2 Cyber Security Maturity Scorecard"?
  - What do you think the board will ask?
- 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 case answers.

PHARMAC

Paul, the PharmaCo CISO, is nervous about the upcoming board meeting. It will be the first time that he has presented to the board and, while the team has made great progress in his short time at the company, he knows that there is still much to be done. He has spent a lot of time with the team trying to simplify the material for the board but he is now asking you, his good friend and trusted colleague, for your feedback.

1) How would you improve the presented security metrics?

2) What is missing from the "Q2 Cyber Brief"?

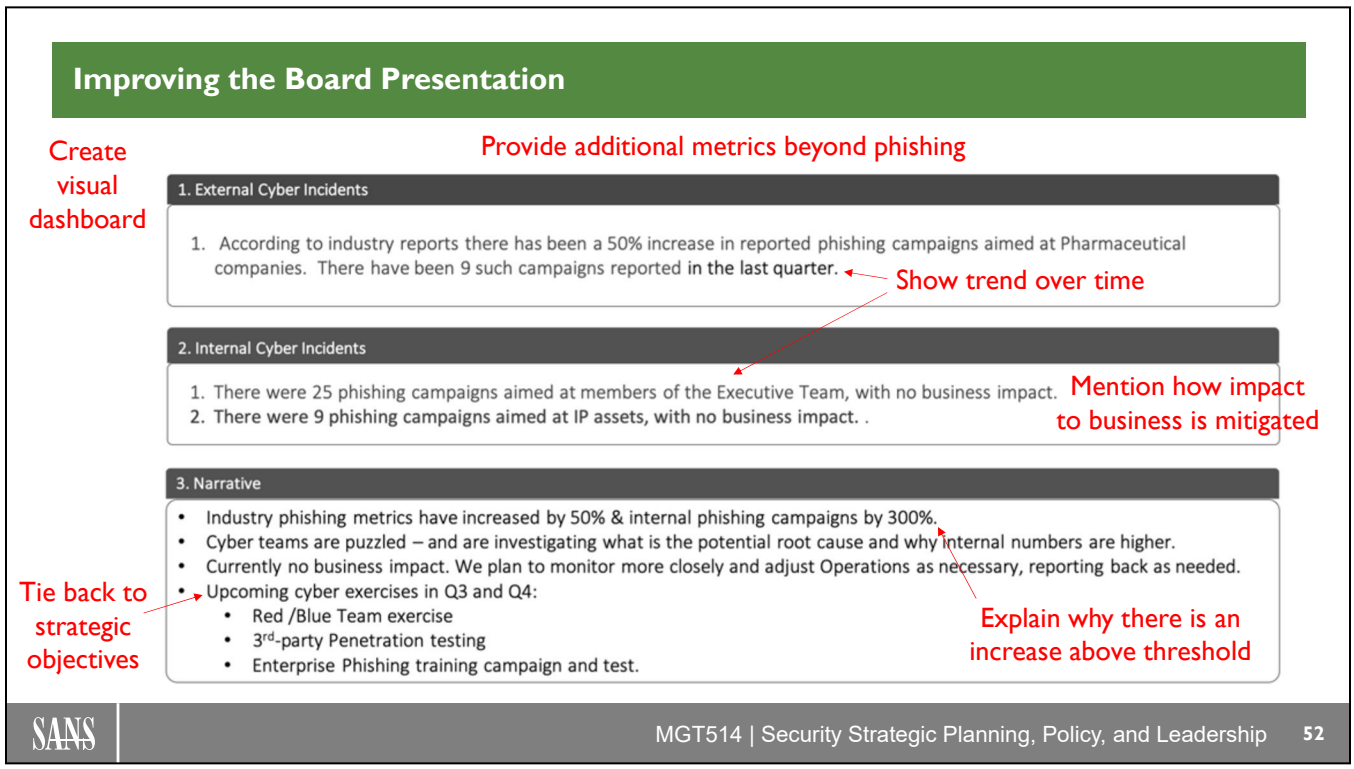
3) How would you improve the "Q2 Cyber Security Maturity Scorecard"?

4) What do you think the board will ask?

PharmaCo Case (B) Debrief

Note that this section contains a debrief and potential case answers

Please note that this section contains a debrief and potential case answers. The instructor will walk through this section with the class after you have analyzed the case



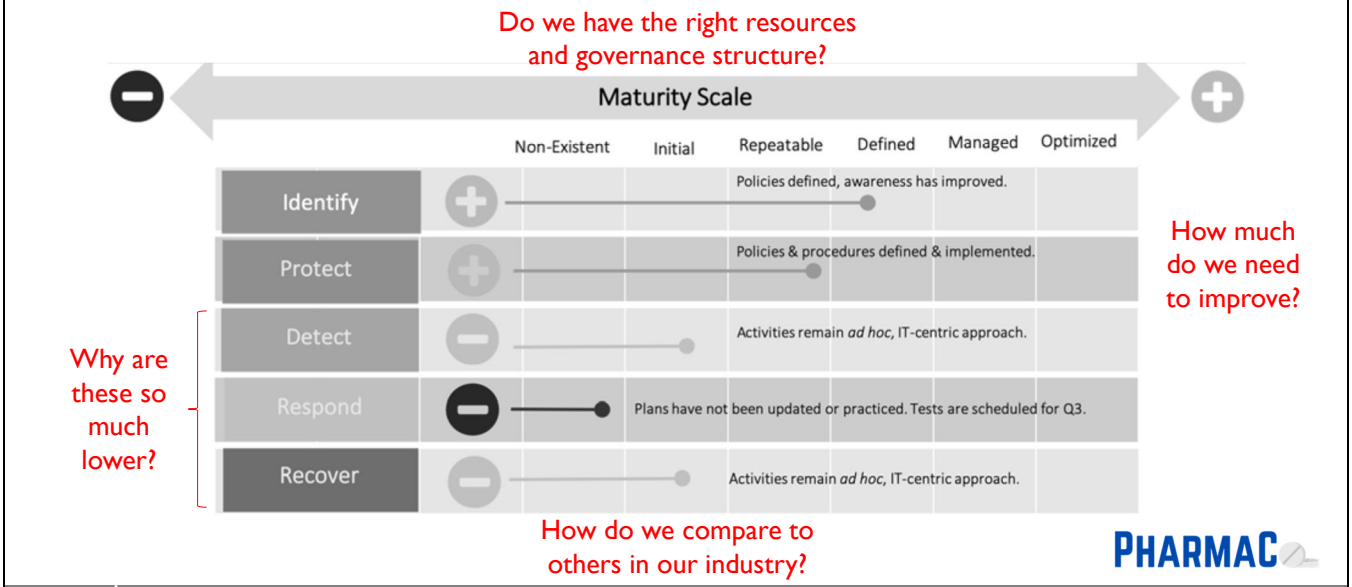
The big thing missing from this portion of the board briefing is context. It is intended to convey important metrics but only focuses on phishing. This can leave the board (who are not security experts) wondering, at best, if that is the only risk to the company or, at worst, you are not comprehensive in your analysis. You need to provide additional information beyond phishing metrics or clearly explain that this just one small element of the items the security team measures on a regular basis.

Additionally, the briefing is too text heavy. There needs to be a visual that shows some sort of trend over time. A 50% increase in reported phishing campaigns sounds bad but notice that there were only 9 such campaigns in the last quarter. Nine does not sound like all that many for a company the size of PharmaCo. You need to show how many campaigns there were in previous periods.

It is also stated that the phishing campaigns had "no business impact". If that is the case, why even mention them to begin with? Instead, you should talk about crown jewels and what types of protections are in place or being put in place. Board members don't understand phishing, but they certainly understand key business assets. If you do talk about technical items like phishing it should be in the context of helping business leaders look to see what is around the proverbial corner. The fact that internal phishing campaigns have increased 300% could be tied to some new business ventures. Highlight to the board that you need to know that business is planning to help mitigate cyber risk.

Finally, the information on "upcoming cyber exercises" is too technical. It would be more appropriate to mention these items as a footnote or in an appendix as, depending on the level of technical knowledge, it is likely that the board doesn't know what these items actually mean. Instead, focus on PharmaCo's strategic objectives and how these activities help manage business risk.

What Will the Board Ask?



The maturity scorecard shown above follows the structure that we have shown earlier in class. It focuses on the five NIST CSF functions and their corresponding maturity from Initial to Optimized. This is a tried-and-true approach and can be easy for non-technical people to understand. The addition of the "+" and "-" icons can also be useful to convey, at a glance, where something needs work.

What is missing from this graphic? There is nothing that conveys the target maturity level. The board will likely want to know how much improvement is actually needed. This is directly related to another missing element. How do we compare to others in the industry? There should be some an analysis and indication of where PharmaCo stands in relations to other pharmaceutical and health care companies.

In terms of other improvements, the "Non-Existent" column should be removed. Is the response capability truly non-existent? Probably not. In fact, the case points out that "draft business continuity, incident response, and disaster recovery plans" had been created with work in progress to do "more thorough testing of the response plans". Saying that something is non-existent is probably inaccurate and could raise a lot more questions than intended.

Finally, you have to be ready to explain why the Detect, Respond, and Recover functions are all so low. The case states that the CISO "had not yet managed to create a cyber-breach playbook" but the board likely doesn't have this background since this is the first cybersecurity briefing to the board. Expect this question to come up.

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 5

- Background
  - Case Study Method
- Case Studies
  - iPremier Case (A)
  - iPremier Case (B)
  - iPremier Case (C)
  - PharmaCo Case (A)
  - PharmaCo Case (B)
  - ***PharmaCo Case (C)***
  - HealthHound Case
- Summary
  - Course Summary
  - Resources

This page intentionally left blank.

This page intentionally left blank.

CYBER42

Event #14

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 5

- Background
  - Case Study Method
- Case Studies
  - iPremier Case (A)
  - iPremier Case (B)
  - iPremier Case (C)
  - PharmaCo Case (A)
  - PharmaCo Case (B)
  - PharmaCo Case (C)
  - ***HealthHound Case***
- Summary
  - Course Summary
  - Resources

This page intentionally left blank.

HealthHound Case Scenario Refresher

- Dennis Scott started job as Director of Security at HealthHound this week
  - He has a three-person team
    - 2 operations people and 1 compliance person
- His boss, the VP of IT Operations, unexpectedly left the company
- Now the CEO wants to meet with Dennis
  - Asked for a security briefing in two days
  - Says he has heard that Dennis "knows his stuff"

We started the course with this HealthHound case, and now we will close the course with the same case so that you can apply what you have learned to this scenario. As a refresher, here is the case scenario:

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, 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 were a little surprised that he got the job. The only management experience Dennis had was effectively as a team lead of some penetration testers at his previous job. But, Dennis was always great at interviews, and HealthHound was looking for a technically savvy individual who really understood 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. 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 and has asked for a security briefing in two days. In an email, the CEO says that he is looking forward to the meeting because he has heard that Dennis "knows his stuff."

This page intentionally left blank.

HealthHound Presentation

- Goal of this exercise
  - Create an outline for an exec presentation to the CEO
- Presentation must show that
  - You understand what the CEO and company value
  - You have a plan for the security team
- Brainstorm with your group
  - Create an outline of no more than five slides
  - Define the topic to be covered in each slide
  - In this scenario Dennis has only been on the job for one week and is briefing the CEO for the first time

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.

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.
2) Security will be built into HealthHound's products, and the security team will not simply be a reactive organization.
3) He has a plan for the organization of the security program.

HealthHound Presentation Scoring

- For live online or in-person classes
  - Team with the "best" presentation decided by vote
  - Each team gets one vote and can't vote for themselves
  - Top three teams awarded 3, 2, and 1 culture point(s), respectively
- For OnDemand classes
  - Students are playing in a separate OnDemand Cyber42 instance with other OnDemand students
  - No points are awarded for the presentation

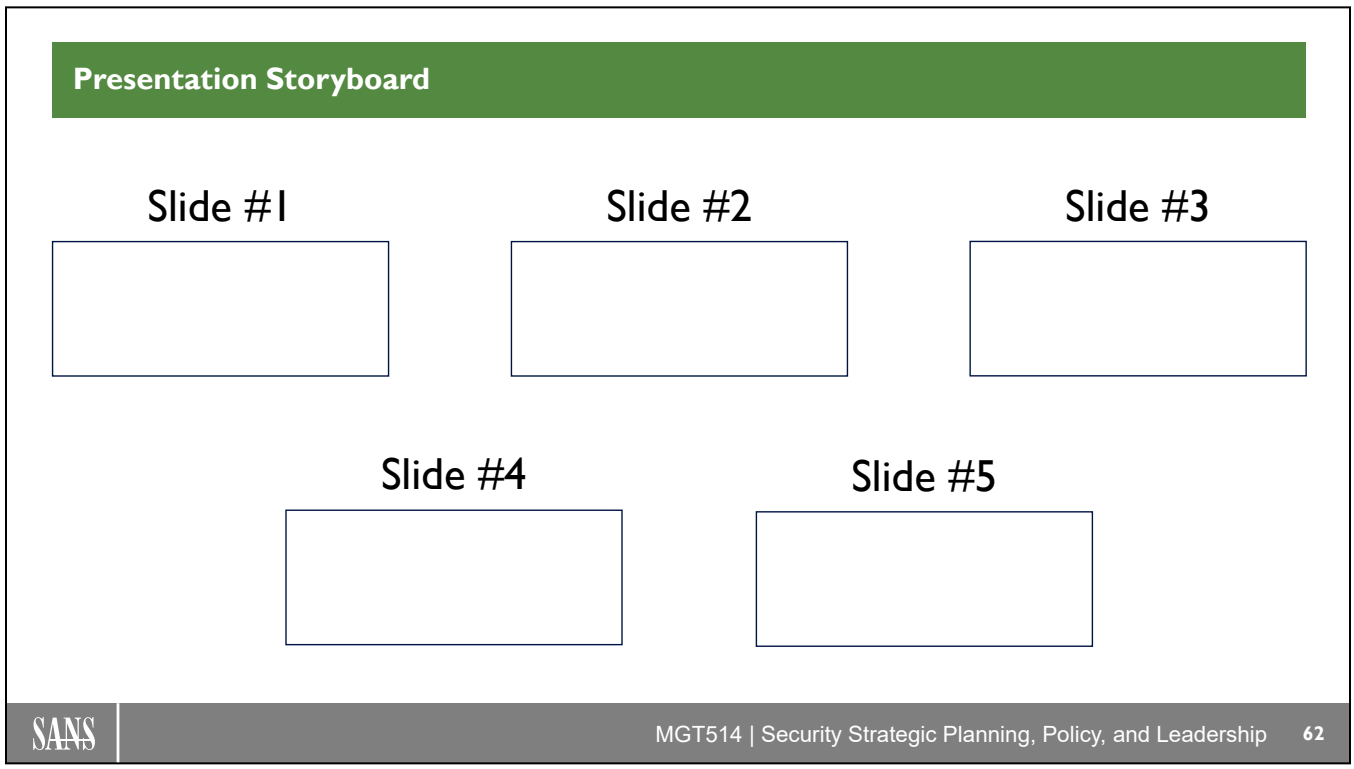
NOTE

Don't turn the page after the blank worksheet.

It contains a debrief and potential case answers.

If you are taking this class live, either online or in-person, a member of your team will give the presentation to the rest of the class. After hearing all the other presentations, the winner will be decided by vote. Each team gets one vote and can't vote for themselves. Once the votes are tallied, the top three teams are awarded 3, 2, and 1 culture point(s), respectively.

If you are taking this class in OnDemand, you have been using an instance of the Cyber42 web app specifically for all OnDemand students. You should still create your presentation storyboard, but no extra points are awarded to anyone playing in OnDemand.



The goal of this lab is to create an outline for a five-slide presentation. You can simply write your topics for each slide into the boxes 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 slide above.

Additionally, space is provided below to write down ideas for your slides.

Topic

Slide 1: _____

Slide 2: _____

Slide 3: _____

Slide 4: _____

Slide 5: _____

This page intentionally left blank.

Cyber42 – End of Game

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

This is the last time that the Security Culture score will be adjusted.

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

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

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

And the winner is the team that has the highest Security Culture score.

If there is a tie then budget, time, and total of security functions (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 function scores wins.

Cyber42 – How Did You Do?

Score	Emoji
100+	🤩🤩🤩
90 – 99	😃😃😃
80 – 89	🙂🙂🙂
70 – 79	😐😐😐
60 – 69	😕😕😕

Great job on completing the class and the Cyber42 Security Leadership Simulation game!

As an indicator of how well you did 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).

HealthHound Case
Example Executive Presentation

Note that this section contains a debrief and potential case answers

Please note that this section contains a debrief and potential case answers. The instructor will walk through this section with the class after you have created your presentation outline.

Before We Begin

- These slides are examples
  - Every organization is different
  - Every CEO and leader has different preferences that inform your presentation
  - They are not intended to cover all potential scenarios
  - We will walk through this example and discuss what you would change
- Based on the case scenario, the goals are to
  - Inform the CEO that there is a plan for security as it relates to the business
  - Solicit input and feedback from the CEO

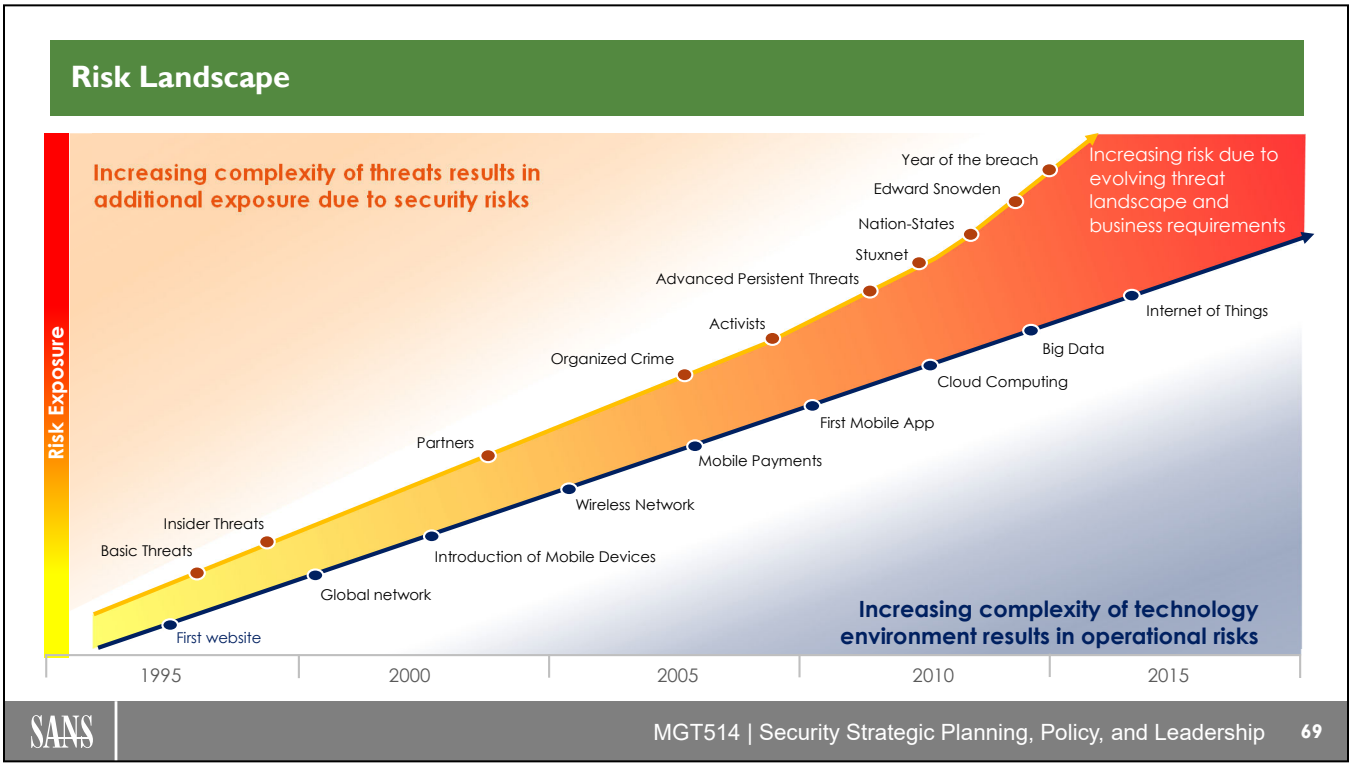
Before we look at the example executive presentation, it is important to note that it is just that—an example. Every organization and every leader is different. There will likely be different preferences in addition to organizational and cultural norms in your company that will inform your presentation. This example is not intended to cover every potential scenario. However, it does include key elements and artifacts from various phases of the strategic planning process that you can include in your slide deck. As you go through the strategic planning process at your organization, you are doing a lot of good thinking and laying the foundation for exactly these types of presentations and conversations.

In this specific exercise, the case scenario highlights that Dennis is new to the company (only one week in) and has to put together a presentation for the CEO in a very short period of time. Given these constraints, Dennis's primary goal is to convey to the CEO that he has a plan for the security team as it relates to the important business priorities. He should explicitly state that certain elements like finance are not included and take this opportunity to solicit input and feedback from the CEO directly.

Organization Mission

"Empower and inspire you to live a healthier, more active life and achieve your health and fitness goals."

Even though this is information the CEO already knows, Dennis has included this slide here to show that, although he is new to the company, he also understands the mission of the organization. This is the point in the presentation where he could briefly share a personal story about his fitness goals and why joining the company was important to him.



This slide is not specific to HealthHound but is an example of a slide that Dennis might use to highlight the fact that both the increasing complexity of threats and the complexity of technology combine to result in increased risk to the organization.

Threat Actors and Motivations

Threat Actor	Description	Motivation
Hacktivist	Activist groups target organizations because of real or perceived slights. Their goal is to damage the brand and embarrass the organization.	• Ideology or protest • Fun, curiosity, or pride • Grudge or personal offense
Organized Crime	Criminals want to make money using stolen data and access to systems. They use malware, phishing, and application attacks to steal data.	• Financial gain
Nation-State	Countries attempting to gain economic or military advantage over their adversaries and economic competitors by stealing data and sabotaging equipment.	• Espionage • Competitive advantage • Fear or duress
Competitor	Other organizations in the same or similar industries seeking proprietary information.	• Espionage • Competitive advantage
Insider	Employees who put data at risk by violating policies and standards or through negligence.	• Espionage • Grudge or personal offense • Convenience or expediency
Partner	Vendors that are relied upon to store and process sensitive information. Partners may have elevated levels of access to sensitive data or systems.	• Espionage • Convenience or expediency

On this slide, Dennis could highlight recent attacks and security events at HealthHound or similar companies. By highlighting real-world attacks and attacker motivations, Dennis makes the threat landscape realistic for the CEO.

Crown Jewels and Business Assets

Asset	Description	Business Importance Impact	Attacker Motivation Likelihood
PHI (Protected Health Information)	Organized crime uses PHI to commit healthcare fraud Nation states target sensitive personal data to profile targets Insiders may leak or mistakenly use sensitive data	High	Financial Espionage Grudge Convenience
PII (Personally Identifiable Info)	Organized crime uses PII to commit healthcare fraud Nation states target sensitive personal data to profile targets Insiders may leak or mistakenly use sensitive data	High	Financial Espionage Convenience
PCI (Cardholder data)	Organized crime easily monetizes stolen cardholder information	High	Financial
Research data	Competitors and nation states utilize intellectual property to advance their own programs	High	Espionage
Key systems	Attackers target key systems like the Member Portal, Health Information Exchange (HIE), Health Insurance Exchange (HIX), Claims Systems for political/economic advantage or to cause business disruption	High	Financial Espionage Ideology, Fun

With an overview of the threats, the next step is to discuss key business assets that are valuable to the organization and, by extension, attackers.

This slide lists key assets that are utilized by the organization, including:

Protected Health Information (PHI)
PHI is extremely valuable because it offers many opportunities for financial, credit, and medical fraud. The black-market value of stolen healthcare credentials is reported to be 10 times more than a stolen credit card,[1] while a stolen medical record is reported to be worth up to $50.[2] It shouldn't be a surprise that organized crime is becoming more interested in the theft of electronic health records. Additionally, nation-states are reportedly targeting healthcare records to steal the personal information of military and government workers to profile targets.[3] Also, employees and other insiders have accidentally disclosed sensitive health records.

Personally Identifiable Information (PII)
HealthHound holds a wealth of personal information about its customers. In addition to names and contact information, HealthHound also stores unique information about a person's health, diet, and exercise.

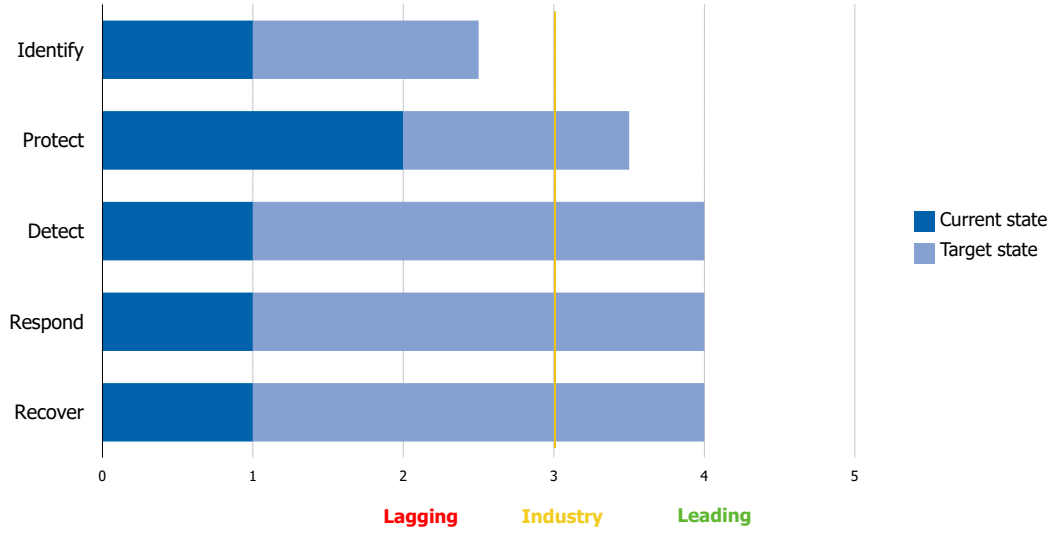
Payment Card Industry (PCI)
This is a big target for organized crime groups that want to monetize large amounts of stolen cardholder data.

Intellectual Property
HealthHound develops proprietary software and hardware that would be extremely valuable to competitors. Information about potential mergers and acquisitions and product development plans must also be safeguarded.

Key Systems
Attackers may target internet sites, the customer portal, or the public API to steal data or cause business disruption.

References:
[1] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924
[2] http://hipaahealthlaw.foxrothschild.com/2015/03/articles/privacy/hacked-health-records-prized-for-their-black-market-value/
[3] http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/

Security Maturity



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

Audience	30 Days *Decipher*	60 Days *Develop*	90 Days *Deliver*
Executive	❑ Meet with key stakeholders ❑ Understand the culture ❑ Identify crown jewels ❑ Analyze control gaps	❑ Develop security vision ❑ Select security frameworks ❑ Create security roadmap ❑ Develop business case	❑ Establish metrics program ❑ Develop marketing/comm plan ❑ Create board presentation ❑ Develop policy library
Team	❑ Understand team member goals ❑ Analyze team's strengths and weaknesses	❑ Define team values ❑ Develop performance goals	❑ Create training plan ❑ Develop hiring plan
You	❑ Define goals for this job ❑ Define your career goals	❑ Find someone to mentor	❑ Find a sponsor for yourself

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.

HealthHound Case In Six Months

This section contains information that you should develop when you have more time to flush out the details. Remember that in the scenario we just discussed, Dennis had only been on the job for one week. In that short time, the best he can do is describe a "plan for a plan." Based on that plan, he can use the available time to do deeper analysis.

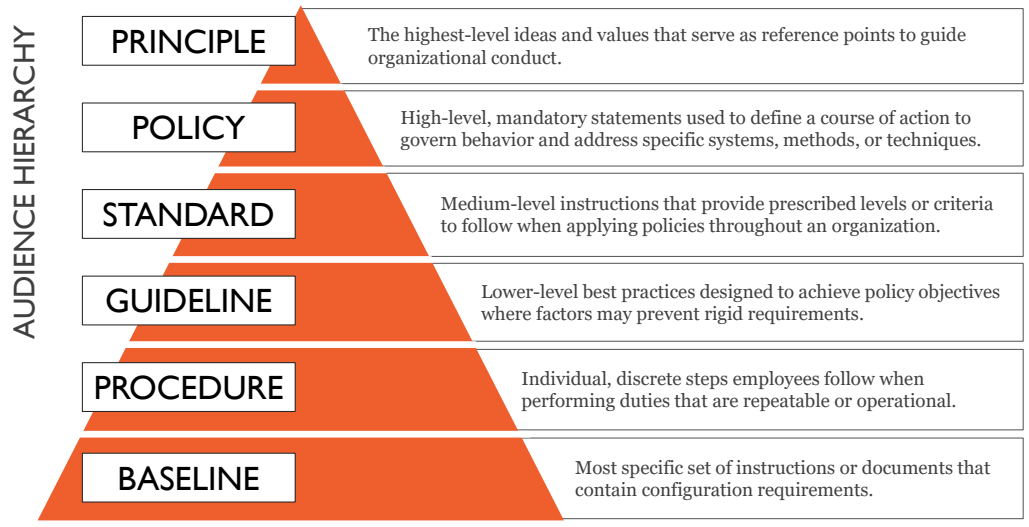
Strategic Planning Outcomes

- How to demonstrate that you have a plan for security
  - Implement an industry standard security framework and approach
  - Develop a multi-phase security roadmap
  - Assess maturity in comparison to industry peers
  - Establish a metrics program for continuous improvement
  - Create a security business case

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

Throughout this course, we utilize numerous management and leadership tools to analyze and better understand the business and threat 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.

Policy Pyramid



This slide is intended to highlight the fact that Dennis is leveraging an industry accepted approach for structuring security policy and associated standards, guidelines, procedures, and baselines. Moreover, these documents are informed by requirements from industry frameworks like the NIST Cybersecurity Framework, ISO 27001, and various compliance and regulatory requirements with which the organization must comply.

Detailed Roadmap – Protect Function Example

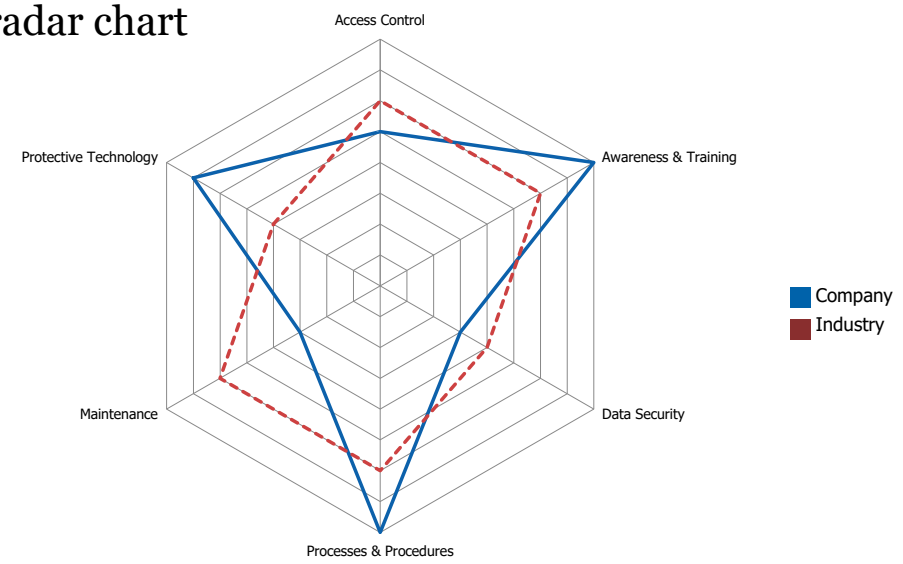
Function	Category	Level 1	Level 2	Level 3	Level 4	Level 5
Protect	Access Control	VPN Firewall Segmentation	Web SSO	Federated SSO	***Risk-based authentication***	*Network Access Control*
	Awareness and Training	Basic awareness training	Phishing exercises	***Role-based training***	*Executive education*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

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

Depending on the interest of the audience, this slide may be placed into the appendix. The main point of this slide is to show that (1) a roadmap guides the work of the team, (2) a number of security controls are in place, and (3) a number of items still need to be started.

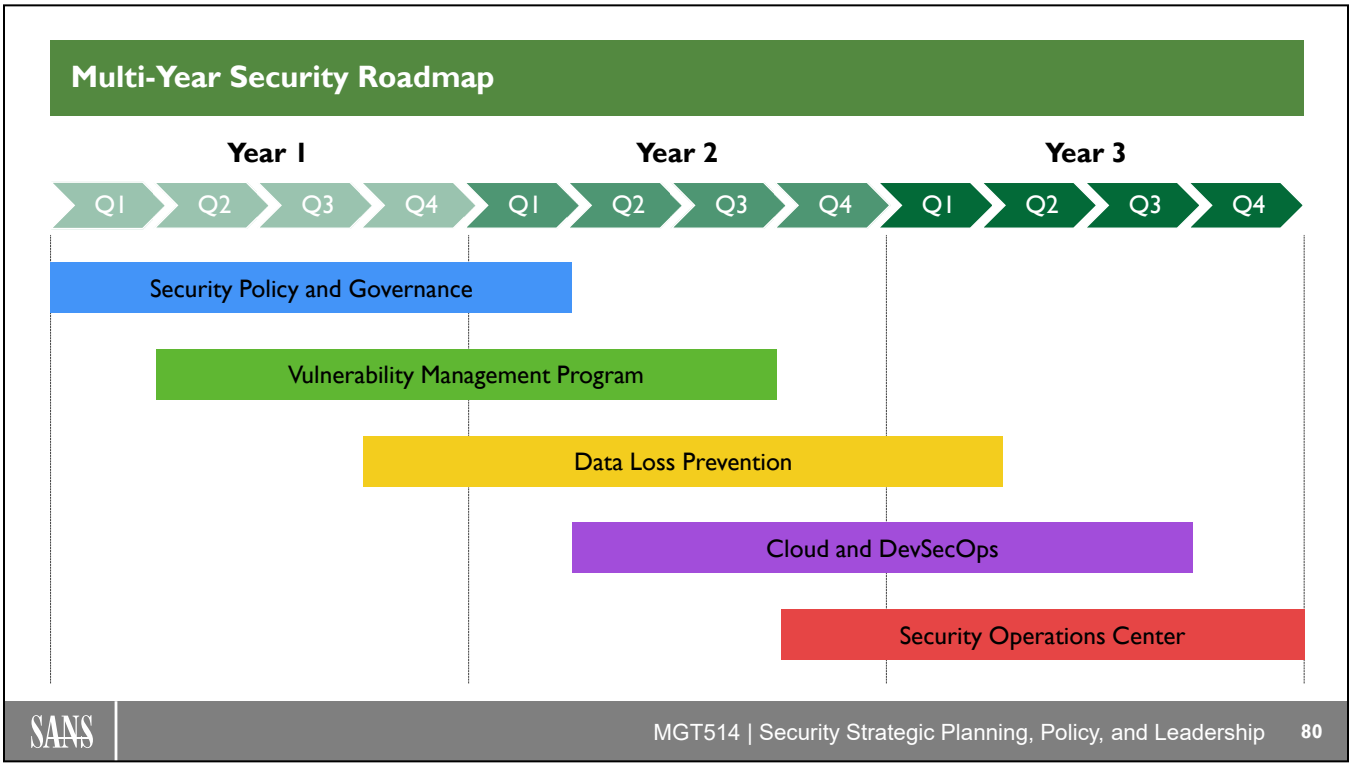
Detailed Industry Comparison – Example

- Sample radar chart



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

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



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

Security Capability Dashboard

Security Capability	Status	Trend	Highlights

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

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

Metrics should align with what's important to the organization. We've established that there are many metrics you could use to describe your security controls. You want to select metrics that will be meaningful to executives and what they need to know versus what you want to tell them.

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

Balanced Scorecard Dashboard

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

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

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

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

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

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

Business Case Options

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

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

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

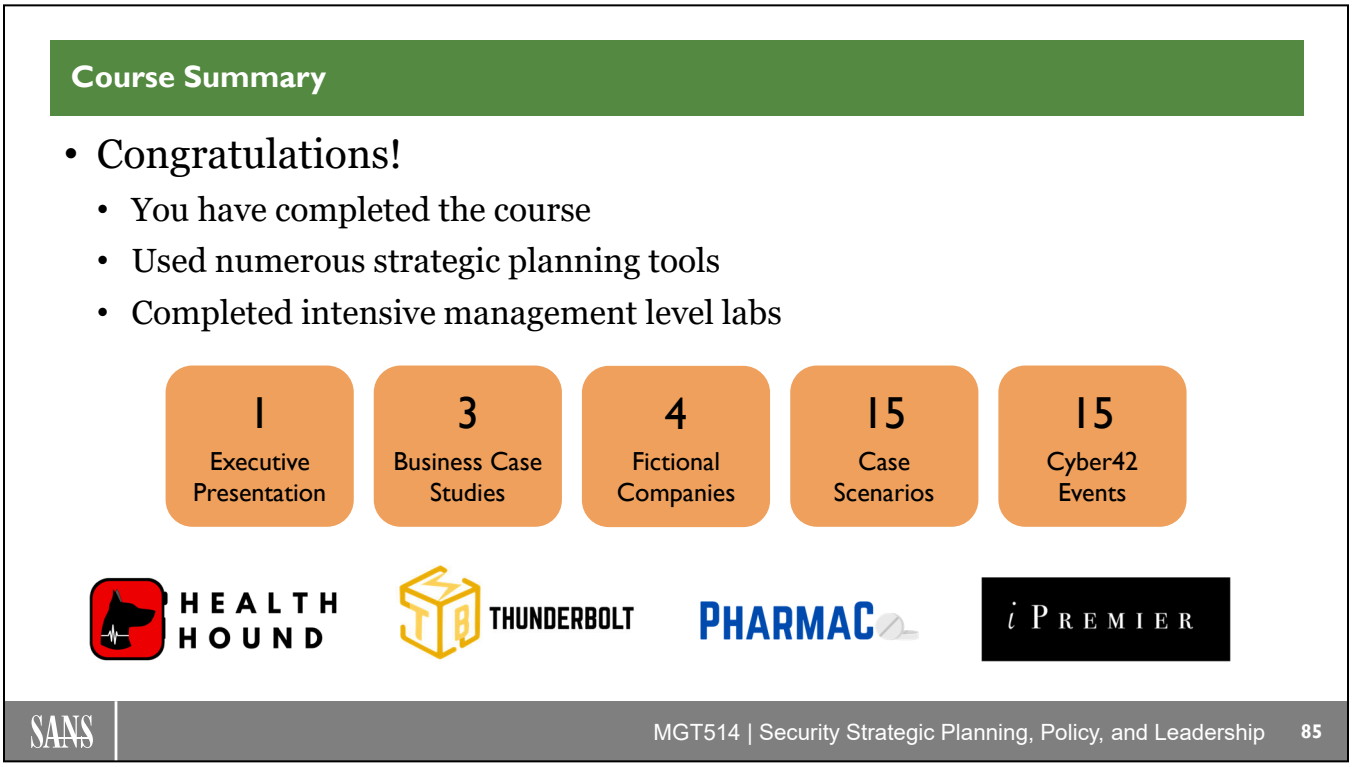
Course Roadmap

- 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 5

- Background
  - Case Study Method
- Case Studies
  - iPremier Case (A)
  - iPremier Case (B)
  - iPremier Case (C)
  - PharmaCo Case (A)
  - PharmaCo Case (B)
  - PharmaCo Case (C)
  - HealthHound Case
- ***Summary***
  - Course Summary
  - Resources

This page intentionally left blank.

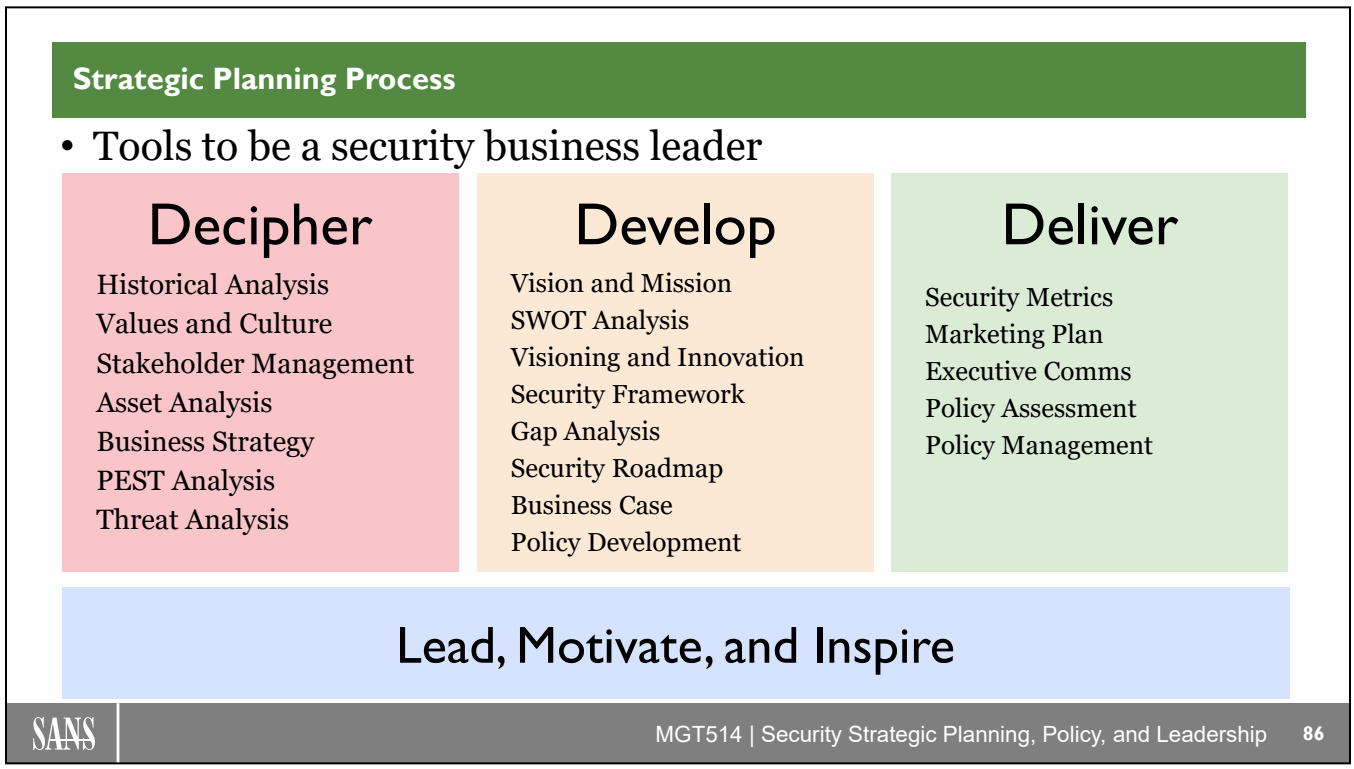


Congratulations! You have completed MGT514: Security Strategic Planning, Policy, and Leadership!

Take a moment to reflect on everything you have accomplished. You have used numerous strategic planning tools throughout the course and completed a large number of intensive management level labs. This includes the executive presentation you just completed along with 15 case scenario labs, and 15 Cyber42 events. These labs were based on three business case studies and four fictional companies. That's quite a lot!

As you go back to work and continue to digest and apply the lessons learned from class try to reflect back upon the scenarios presented here in class. There may be times when you encounter a similar situation at work. We hope that what we covered in class helps you be better prepared for the challenges to come.

Don't forget about our strategic planning process (Decipher, Develop, Deliver, and Lead) and use that as a mental model for building your security program.



This course covered 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 also resonate with other IT and business leaders. Moreover, you have to effectively steer the organization toward these strategic goals. Effective development and assessment of security policies is a key skill 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. 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.

Resources: Strategy

- *Playing to Win: How Strategy Really Works*
  - A.G. Lafley and Roger L. Martin
- *HBR's 10 Must Reads on Strategy*
  - Harvard Business Review
- *Competitive Strategy: Techniques for Analyzing Industries and Competitors*
  - Michael E. Porter
- *Good to Great: Why Some Companies Make the Leap...And Others Don't*
  - Jim Collins
- *The Innovator's Dilemma*
  - Clayton Christensen

This page intentionally left blank.

Resources: Leadership

- *Start with Why: How Great Leaders Inspire Everyone to Take Action*
  - Simon Sinek
- *Leadership and Self-Deception: Getting Out of the Box*
  - Arbinger Institute
- *The Anatomy of Peace: Resolving the Heart of Conflict*
  - Arbinger Institute
- *The Rules of Work: A Definitive Code for Personal Success*
  - Richard Templar
- *Empowering Yourself: The Organizational Game Revealed*
  - Harvey J. Coleman

This page intentionally left blank.

Resources: Leadership and Management

- *How to Win Friends and Influence People*
  - Dale Carnegie
- *Five Dysfunctions of a Team: A Leadership Fable*
  - Patrick Lencioni
- *The 7 Habits of Highly Effective People*
  - Stephen R. Covey
- *The Tipping Point: How Little Things Can Make a Big Difference*
  - Malcolm Gladwell
- *Outliers: The Story of Success*
  - Malcolm Gladwell

This page intentionally left blank.

Resources: Leadership and Change

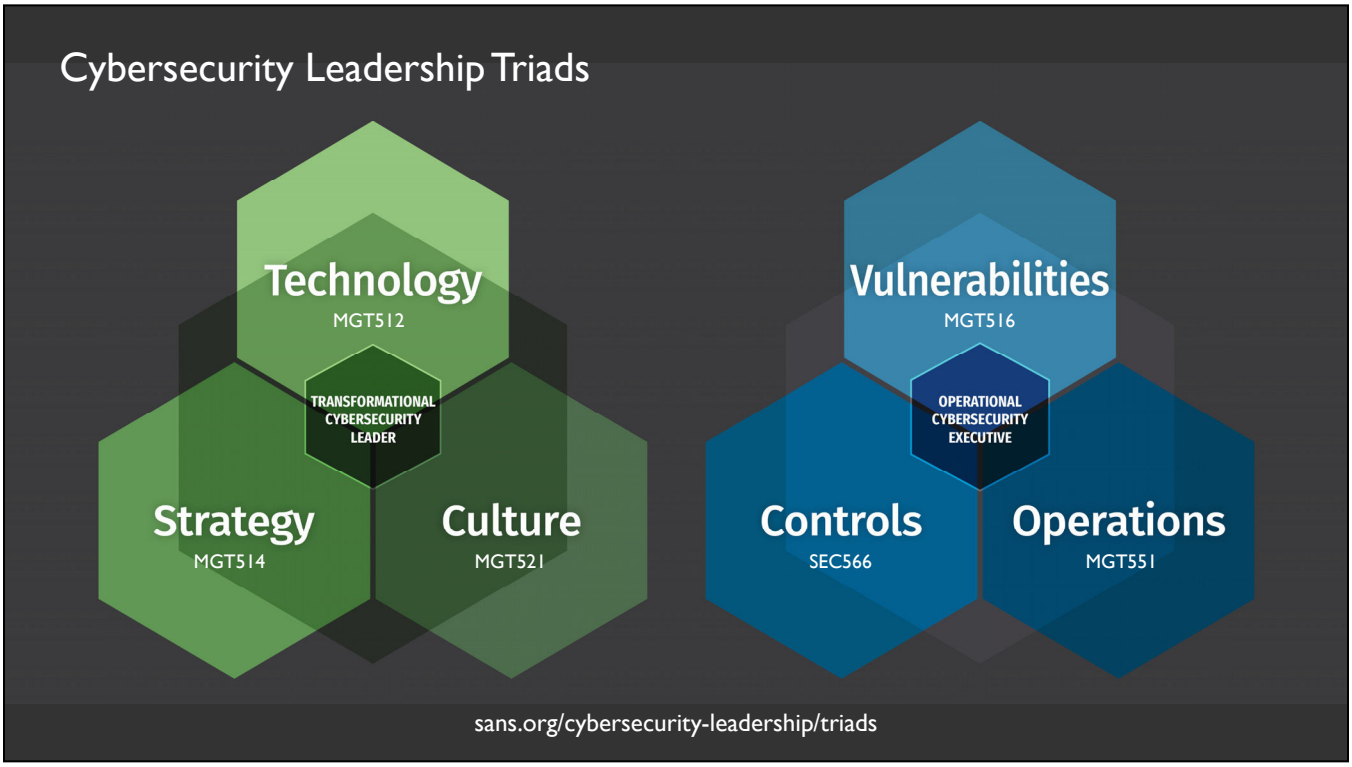
- *Switch: How to Make Change When Change Is Hard*
  - Chip Heath and Dan Heath
- *Made to Stick: Why Some Ideas Survive and Others Die*
  - Chip Heath and Dan Heath
- *Leading Change*
  - John P. Kotter
- *Thinking, Fast and Slow*
  - Daniel Kahneman
- *Mindset: The New Psychology of Success*
  - Carol Dweck

This page intentionally left blank.

Resources: Communications

- *On Writing Well*
  - William Zinsser
- *slide:ology: The Art and Science of Creating Great Presentations*
  - Nancy Duarte
- *Resonate: Present Visual Stories That Transform Audiences*
  - Nancy Duarte
- *Crucial Conversations: Tools for Talking When Stakes Are High*
  - Kerry Patterson
- *Radical Candor: Be a Kick-Ass Boss Without Losing Your Humanity*
  - Kim Scott

This page intentionally left blank.



Transformational Cybersecurity Leader
With organizations in need of protecting against an endless and increasing onslaught of information security threats, technology management skills alone are no longer sufficient. Today it is about technology, business strategy, and people. Cybersecurity leaders need to be up to speed on information security issues from a technical standpoint, understand how to implement security planning into the broader business objectives, and be able to build a longer lasting security and risk-based culture. Adjusting employees' and leadership's way of thinking about security in order to prioritize and act to prevent today's most common cybersecurity attacks requires organizational change that affects the foundational culture of the organization.

A Transformational Cybersecurity Leader will be able to:
- Strategize and apply concepts
- Implement management tools and methodologies
- Critically analyze the current business situation
- Identify target state
- Perform a gap analysis
- Develop a comprehensive cybersecurity roadmap
- Includes employees at all levels of the organization in every type of job role

The following courses can help you on your journey to becoming a Transformational Cybersecurity Leader:
- MGT512 – leading security initiatives to manage information risk
- MGT514 – aligning security initiatives with strategy and business goals
- MGT521 – building a security and risk-based culture

Operational Cybersecurity Executive
As cyber attacks become more common and more expensive, organizations are making a foundational shift to view operations from the point of view of an adversary in order to protect their most sensitive information. Despite vulnerability tools and programs being available for decades, attackers still utilize known vulnerabilities.

With a wide range of technologies in use requiring more time and knowledge to manage, a global shortage of cybersecurity talent, an unprecedented migration to cloud, and legal and regulatory compliance often increasing and complicating the matter more, it’s no wonder we've seen frustration in the eyes of information assurance engineers, auditors, SOC analysts, and cybersecurity managers who are trying to make a difference in their organizations by better defending their data systems.

An Operational Cybersecurity Leader will be able to:
- Understand security controls
- Implement security controls
- Audit security controls
- Create an effective, comprehensive vulnerability management model
- Guide which threats need attention
- Continually mature your security operations, saving time, money, and hours of frustration

The following courses can help you on your journey to becoming an Operational Cybersecurity Leader :
- MGT516 – building and leading a vulnerability management program
- MGT551 – building and leading a security operations center (SOC)
- SEC566 – implementing and auditing critical security controls

Reference:
https://www.sans.org/blog/cybersecurity-leadership-triads

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).

Authors and Contributors

- Authors
  - Frank Kim
    - fkim@sans.org
- Contributors
  - Jaynie Bunnell
    - jayniebunnell2002@yahoo.com
  - Dean Sapp
    - deansapp@hotmail.com
  - Mark Williams
    - 44mdwilliams@gmail.com

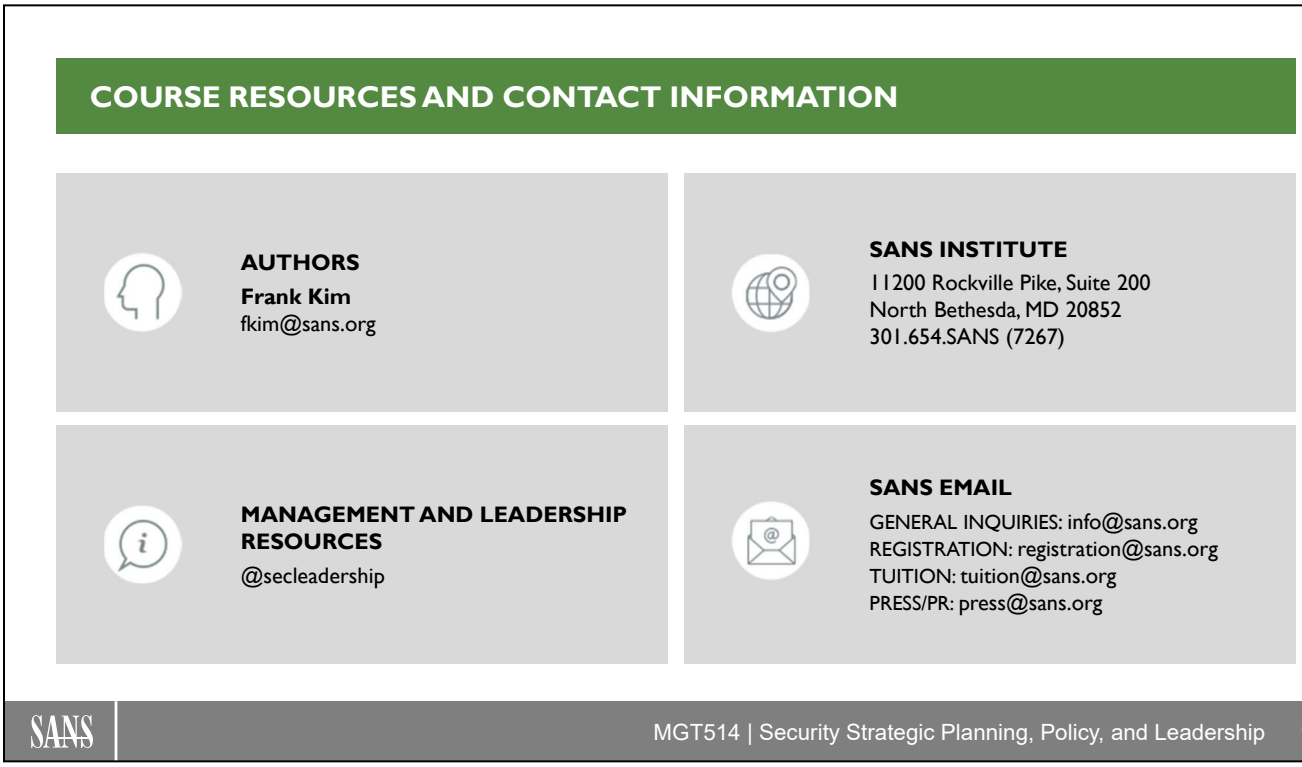
This page intentionally left blank.

This Course is Part of the SANS Technology Institute (STI) Master's Degree Curriculum.
If your brain is hurting from all you've learned in this class, but you still want more, consider applying for a master's degree from STI. We offer two hands-on, intensive master's degree programs:

- Master of Science in Information Security Engineering
- Master of Science in Information Security Management

If you have a bachelor's degree and are ready to pursue a graduate degree in information security, please visit www.sans.edu for more information.

www.sans.edu **855-672-6733** **info@sans.edu**



Contributors:

Jaynie Bunnell
jayniebunnell2002@yahoo.com

Dean Sapp
deansapp@hotmail.com

Mark Williams
44mdwilliams@gmail.com

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W