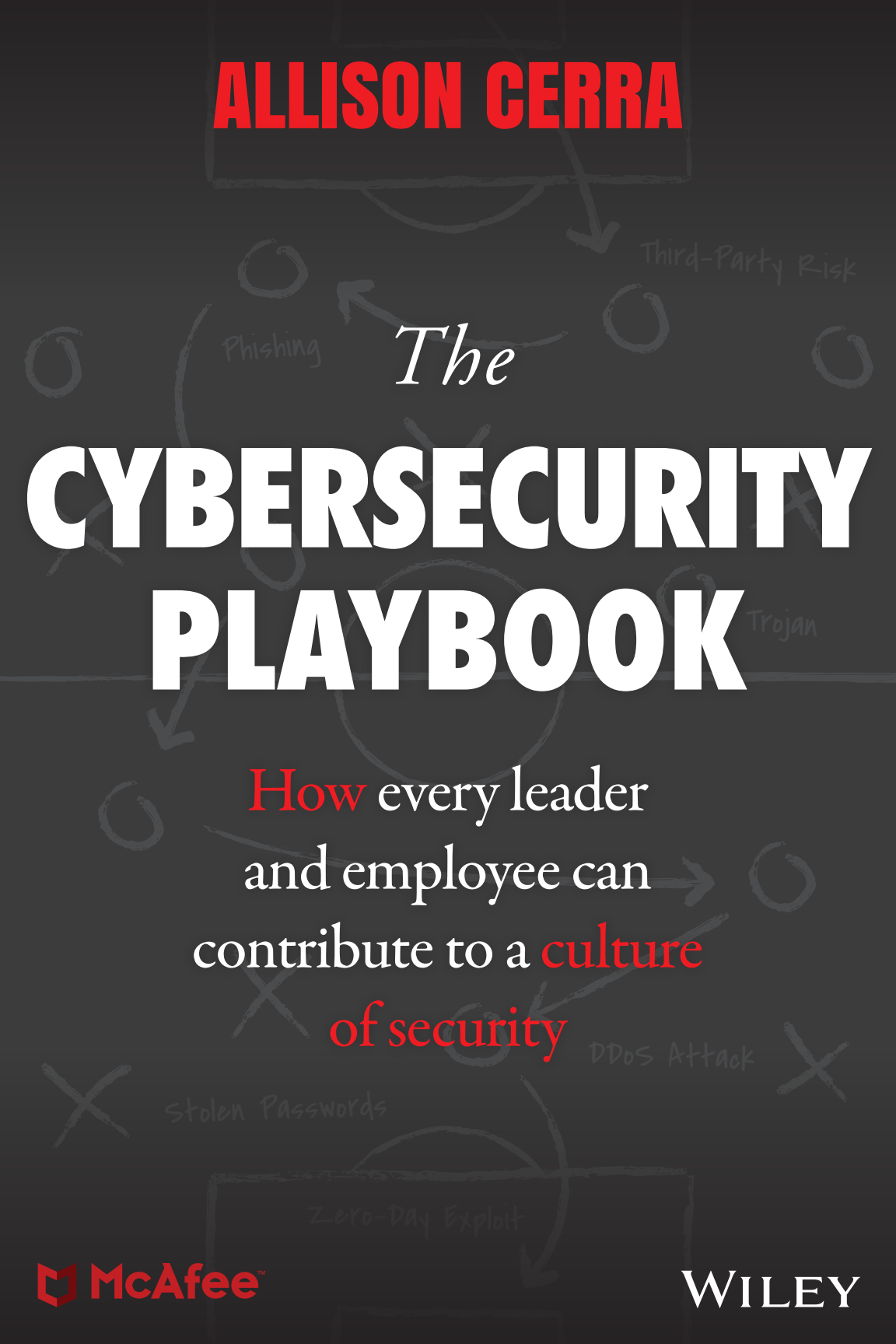
ALLISON CERRA



The CYBERSECURITY PLAYBOOK

How every leader and employee can contribute to a culture of security

McAfee
WILEY

The

CYBERSECURITY PLAYBOOK

ALLISON CERRA

The CYBERSECURITY PLAYBOOK

How every leader
and employee can
contribute to a culture
of security

McAfee™

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:
ISBN 9781119442196 (Hardcover)
ISBN 9781119442165 (ePDF)
ISBN 9781119442134 (ePub)

Cover image: © MicroOne/Shutterstock
Cover design: Wiley

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

For Frank, the love of my life, who has yet to read a single page of anything I've written, including this one. Thank you for loving me and keeping me grounded.

Contents

CHAPTER

1

The Time I Ruined Easter

I've had better Sundays.

It was Easter, April 16, 2017. I had just finished a homemade dinner with my husband. It was time to chill and finally enjoy a few hours of downtime, compliments of the latest binge-worthy craze on Netflix. Little did I know, I was about to star in my own real-life drama that was much more cringe-worthy instead.

My cell lit up and I looked down at the display. It was a text from Chatelle, our chief human resources officer (CHRO). Chatelle and I were close. We had just teamed up to help McAfee's spinout from Intel as one of the world's largest independent cybersecurity companies 12 days prior. Seeing a text from her on Easter wasn't unusual, assuming it

was the type of well-wishing that happens between friends on a holiday. This was not that type of text.

You need to check out our social media page. It's bad.

I immediately felt my blood pressure surge as I opened McAfee's company page on a very prominent social media platform, the name of which I have redacted from this true story. I was horrified.

Someone had deliberately defaced the social profile of our newly minted, 12-day-old company with the most obscene and offensive language directed at nearly every walk of life. This would be bad for any company. But let me try to express how desperately bad this was for us.

The offensive epithets were in stark contradiction to everything our company represented. We had just relaunched our brand with a new tagline, "Together is power," reflecting our belief that it takes *all* kinds to protect our world from cyber threats. We had just unveiled new values to all employees upon our company's launch, one of which espoused *inclusive* candor and transparency. And we were a leader in *cybersecurity*. How would customers feel about our ability to safeguard their most precious digital assets if we couldn't even protect our own company's profile on one of the largest social media platforms? And, to top it off, my team—the marketing organization—was responsible for managing our company profile across all social channels, including the debased one staring me in the face.

I jumped into action. I had to get to the leader of our digital team to figure out what was going on. I reached her immediately and didn't even have to explain that the call wasn't to wish her a Happy Easter.

"I know why you're calling. We're on it. Our account was hacked. We're talking to the [social media platform company] to get it resolved."

I started to think the worst. A hacked social media profile was one thing. What if this was a coordinated attack against McAfee with a much bigger prize at stake, with hackers diverting our attention to this fire drill while they seeped in through our company's systems?

She immediately reassured me that our chief information security officer (CISO) was already on the case, confirming our systems were good. Relief washed over me for a moment—until I realized I needed to make another call. Our CEO needed to know what was going on. And I preferred he hear the news from me. I was about to ruin his Easter Sunday. He picked up the phone almost instantly:

"Chris, one of our social media accounts has been hacked."

His response was measured. "How bad is it?"

"Our corporate servers are fine, Chris. It's our corporate page on a social media site that's been hacked."

I explained to him just what had happened. Our social media manager, Gavin, was the first to discover the attack. Gavin had been at home, doing what social media geeks do on holidays—he was online. Around 5 p.m. he saw a status update on the social media platform with a bunch of random letters in it. He figured someone on his team had butt-dialed the update. Gavin deleted the random post.

He then pinged his team to see who might have accidentally created that post. No one knew anything about it.

Soon, another meaningless post showed up. This was now not random.

Gavin logged into the social media platform and went to the account settings area. All the names were familiar of the people who had administrative privileges for the account. Even so, to be on the safe side, Gavin started to delete all other admins.

As he was doing that, his page refreshed, and Gavin was locked out.

There was now no doubt that this was malicious. In a moment, Gavin realized that his deleting the weird posts had alerted the hacker that McAfee was aware of the defacement. It was like the classic race in tech crime dramas with fingers flying on keyboards, spinning icons as processes complete and messages flashing as only Hollywood can bring to the screen. Gavin and our hacker were racing online to do the same thing. Even without the pulsing soundtrack, the tension was every bit as fraught with drama. Gavin said, "I was trying to delete all the other admins, and the hacker was doing the same thing. He beat me."

Before I hung up with our CEO, I had one more piece of disappointing news to share.

> "Oh and Chris, when you go to our social profile page, you'll now see not just the offensive posts, but also our company logo has been replaced with an image that looks like a bird. Look closer. It's not a bird at all. It's. Um. It's body parts."

It's common in the hacker community to deface sites with obscene drawings to indicate that someone got "pwned,"

hacker slang for being defeated in a humiliating way—for being "owned." Now that the hacker knew we were locked out and he was in control for the time being, he added an obscene image to replace our new company logo, just for good measure.

My team frantically engaged the social media platform company to remediate the issue. But…things don't happen quickly on holidays. And since this was now later in the evening, we were relegated to working with the company's Asia-Pacific (APAC) group, making it seem as if time itself had to physically cross the ocean separating us and the support team. Minutes slowed to a crawl.

We waited for what seemed like an eternity. Because it was not our servers that were hacked, there was no big team from McAfee I could put on the third-party problem to fix it. We could only check in with the company's support team every few minutes, only to be told they were "on it."

After about 30 minutes, we received news that the social media company had locked out *all* admins from our company page, and only they had access now. That was the good news—at least no more damage would be done.

The bad news? They did not have a means to simply roll back the page to what was there 30 minutes before. Their procedure was to lock the page, so no further changes could be made, and then to follow a validation and analysis procedure: For validation, they wanted to make sure that we were who we said we were, and not a hacker calling up pretending to be McAfee (How ironic!). Then the analysis part kicked in, where they wanted to study the extent of the hack before taking any further action.

But what about the obscene image? It was still up on our corporate page. To make matters worse, the way this social

media provider worked was that all employees who had personal pages on this platform and who said they worked for McAfee—their personal pages now sported the obscene image in place of our logo, too!

Including mine.

On the next update I received, the support team said they weren't yet done with their "procedures." They said the only way to roll back the page was first to reactivate the account—unlock it—and they were not going to do that until they finished their security review.

Seriously? How was this happening? *Nothing* could be done about our company page until they were done with their review. We were at their mercy. The most our employees could do was to delete any mention of McAfee on their own personal pages, which some who were aware of the event did.

But that wasn't sufficient. I continued to ruin Easter Sunday for others as I alerted our executive team of the event. We had ensured our company's servers were safe, but that didn't mean McAfee wasn't under attack through other social channels. And we certainly didn't know whether our own executive members—and their social profile personas—weren't the next target.

I took to email and group texts to sound the alarm, instructing our executive team to enable multifactor authentication on their personal profiles immediately on all social networking sites (more on multifactor authentication in a moment).

I followed my own advice and began frantically enabling the security feature on my personal profile pages wherever I could, that is, until I hit a very popular social networking platform where I became stumped. I'm not sure if my

body was in the full throes of fight-or-flight (where the body redirects blood flow to major muscle groups to help one flee a threat or stand ready to combat—in other words, *not* the prefrontal cortex) or if the social media platform could have done a better job of not obscuring the safety capability. It was probably a bit of both. In either case, panic consumed me, and I resorted to a desperate measure: I deleted my personal profile—and all its history—on the social media platform altogether.

An hour stretched to two, then three, then four. I was regularly calling our CEO with the requisite, but annoying, status updates about our increasingly embarrassing vandalized company profile page. Calls that went something like:

"Chris, we're still working with them. They haven't finished their security review. We're hoping it will be resolved in 30 minutes."

Lather, rinse, repeat—every 30 minutes.

It was on one of these calls that our CEO pulled a rabbit out of his hat.

"Allison, I know of someone at the company and I'm tired of waiting on them to take action. I'm calling him."
"Excellent, Chris. We'll keep the heat on the APAC team in the meantime."

Chris made the connection and pleaded our case. Within 30 minutes of the call, the page was restored to its original state. I don't know whether Chris's call mattered, or whether the investigation simply had run its course and was completed. I just knew that the situation was now contained.

On Monday morning, we posted an article on our intranet site, letting every employee know what happened over the weekend. Remember that McAfee value I mentioned about practicing inclusive candor and transparency? We owed it to our employees to explain what happened, especially given their social media pages were defaced over those tense few hours when the heinous image replaced our company logo. Being candid and transparent is difficult when dealing with an uncomfortable topic. But it's also necessary to truly live the value.

* * *

I tell you this story not just because it's interesting, and not just so you feel "Hey, better her than me!" I began with this story because it's a microcosm of what we're going to be talking about for the rest of the book.

Just so you get your money's worth from this book—in the very first chapter—I'll now break down how the hack happened, and what we did afterward. Most importantly I will lay out the steps that you can take *tomorrow morning* at work to see that this does not happen to you.

Lessons Learned the Hard Way

When we regained control of the account, we asked the social media company to tell us whose admin account in our dashboard had been responsible for the changes.

Turns out it was an employee with one of our media placement agencies, who was no longer doing work for

us—let's call her Julie. Her credentials were stolen by a teenager connected to a larger cybercrime syndicate. Julie made the mistake so many others make: She didn't practice good password hygiene. She used the same password to access multiple accounts, including her profile on this social media platform. And, since she was an authorized administrator for McAfee's corporate page on the same site, her personal credentials gave her access to not only her profile, but ours as well. When one of her accounts was compromised and her credentials traded on the Dark Web, hackers simply tried the password across her other online accounts. That's when they struck pay dirt in breaking Julie's administrative access to McAfee's company profile on the social media platform. The rest was child's play.

Hindsight is 20/20 and this case was no exception. Vulnerability number one: ***Julie used the same password for access*** to her social media account (and our corporate page on the same social media platform as one of our authorized administrators) as she used for other accounts. If she had used unique passwords, then the credentials that bad actors bought on the Dark Web would have been worthless. What's worse? When alerted to the hack on her personal account, Julie quickly changed her password. But she failed to change it across her other accounts, including the one in this story. That's on her.

Vulnerability number two: ***We should have required multifactor authentication for all admins*** on that social media site. What this means is you can gain access to a system not only if you have the correct password, but you must also be able to enter a one-time code that's generated

and sent to, say, your phone. If you don't have the code within a few seconds or minutes of being asked for it, you're not getting in. There are several versions of this type of authentication and I'm simplifying it here, but you get the idea. That's on us.

Vulnerability number three: ***We did not do a review frequently enough to see who no longer needed access*** to our account. Julie helped us a while ago, but we should have removed her from being an admin after her activity had ended**.** We still could have been hacked while she was actively working with us, but our lack of access hygiene just made it worse. That's definitely on us.

All of these actions would have vastly reduced the chances of the hack occurring. But let's say for some crazy reason a hacker with enough motivation, skill, and luck was able to get into our social media account. Let's look at what could have helped us after a hack was discovered, had we put certain things into place beforehand.

We should have had a ***procedure where we lock out all admins without letting on that we are aware of the attack***. By our deleting the nonsense posts, we alerted the hacker. Then when the hacker saw we were deleting permissions, he acted more quickly than we did.

It was fortunate that Gavin was on the defaced page on Easter Sunday. Otherwise we may not have known as quickly about the defacement. Now we have a tool that uses machine learning to detect unusual images, profanity, slurs, and other anomalous material on social media sites. It *immediately alerts* several members of our team in the event it detects such unusual activity.

Note: I'm not going to name the tools we use for two reasons: First, tools come and go, and they also tend to have different effectiveness at different times. In other words, when a tool is first launched, it may be highly effective—until hackers figure a way around it. Because I don't know when you're reading this book, I don't want to praise something that I may no longer be using when you're actually reading these words.

The second reason for not mentioning the tool is McAfee already is a huge bullseye for hackers around the world. By keeping them guessing what exact tools we use, we help to lessen that threat. If you search for some of the descriptions I use for tools, you'll quickly find current ones you can try.

Back to the story of lessons we learned:

At the time we alerted the social media company of the hack, we did not know their procedures for dealing with it. Mistake. We found out only then that their policy was to freeze the account for many hours, regardless of how defaced our page was. ***We now ask about these procedures in advance*** of creating corporate pages on other sites.

We learned the hard way that money talks. Because we were spending a decent amount of money on advertising on this social media site via agencies, we looked like a smaller account to the company than we were; that might have affected response levels. Today, ***we spend directly with social media platforms*** to accurately reflect our investment and receive the commensurate service levels we deserve.

And, we learned that ***third-party companies with which we do business may not have strong security*** practices. This is especially important to remember for companies that have access to your systems or appear as an extension of your organization. In particular, smaller third-party companies with which you have a relationship may not have formal IT and security teams, let alone practice rigorous cybersecurity hygiene.

Finally, the postmortem of that Easter's unfortunate events delivered one final punch in the gut. McAfee wasn't even a deliberate target in the hack. The hacker didn't realize Julie was an administrator for McAfee when he broke her credentials. He didn't know (or care) who Julie was. He was on the hunt for passwords. His reward would come only after he determined what the password unlocked—be it a personal banking account, a company's network, or something else. Once he found one that just so happened to unlock the keys to McAfee's company page on that social network, he unleashed his rants of abuse on it, offending everyone he could and humiliating us in the process. *Even for hackers, sometimes it's better to be lucky than good.*

Additional Lessons for You

Have lists of people you can call and people to whom you can escalate. Have them where you and your team can access them anytime. Also, the lists must not only be for people on your team but also for people at the vendors for your website, social media, cloud storage, etc.

It needs to be in someone's job description to regularly review who has access to an account and clean up the list to remove people who no longer work on those projects.

Use multifactor authentication. For some systems we can automatically detect if one of our users has it turned on, and the system will tell us if a user turns it off, even for a few minutes as she switches to a new computer, for example. With systems over which we have less direct control, like a cloud-based service, we require that users send us screenshots of the multifactor authentication being enabled.

You can imagine that we scrutinize social media outlets now before we put a page up. In addition to the measures I described above, we ask the following:

- How do you handle any personally identifiable information?
- What technology are you using? (We take the answers and do a vulnerability assessment.)
- How does your access management system work?
- What third-party tools are allowed to connect to your platform to automate any rollback of content that is necessary after a hack?
- What is your escalation process if an account is taken over?
- What's your service level agreement for responding to a hack and for getting a customer back to the pre-hack content?

Who Was at Fault?

Certainly, the social media provider can make the case that we didn't do some obvious things like keeping admins to a minimum by reviewing them often, insisting upon unique, strong passwords, and so forth. But it didn't help that they had such a rigid policy that even an obvious, egregious hack to a site had to remain in place until "analysis" was complete. And of course, the agency person should have not reused the same password across multiple accounts.

But notice that I titled this chapter "The Time *I* Ruined Easter." No, I didn't hack McAfee's corporate social page. I didn't knowingly leave the door open for a bad actor to do the same. And there was nothing I wanted *less* on that Easter Sunday than to be dealing with a situation that resulted from a comedy and confluence of errors across multiple fronts. All that said, I can only take responsibility for its occurrence. Because, at the end of the day, that corporate social page was under my team's watch. And we failed to take reasonable measures to uphold our duty in safeguarding it.

Personal responsibility is an uncomfortable thing. Very few of us relish the thought of examining what we could have done better or differently to prevent an unfortunate event. Deflection is a much more human response. Yet, it's our very tendency to abdicate personal responsibility that remains a key weapon in the hacker community's arsenal.

For too long, cybersecurity has been "someone else's" problem. For too many, cybersecurity is an opaque topic undeserving of their time, let alone personal responsibility. This book seeks to change that narrative, even if only by

taking a humbling step in acknowledging the responsibility we all share as employees—and ultimately defenders—of our organizations. If our company can't trust us to take reasonable precautions in protecting its most sacred digital assets, whom can it trust?

Let me step off my soapbox to acknowledge the real problem. It isn't that employees, generally speaking, don't *want* to do the right thing. It's much more often the case that they simply don't know *how* to do it.

Cybersecurity is a team sport with everyone needing to play her or his position for every minute of the game. Tools can be tremendously helpful, but it's only when people, tools, procedures, regular reviews, and other factors work together that they form an effective defense.

Remember This Crucial Element

There's another crucial element to minimizing cyber threats, and that's honesty. I'm certainly outside my comfort zone starting off a book with my name on it by describing an embarrassing security failure on my watch. Could it have been far worse? Absolutely. Should it never have happened? Absolutely.

And could it have been you, instead of me? Again, absolutely.

By telling you this story, I want to set a tone of honesty that's also needed in your business when you work to repel the bad guys: you need to develop a culture of security that allows people not only to help each other, but also to be honest with each other when they see unsafe practices. It's

honesty without anger or blame or retribution, and it's crucial to making the culture work.

The second reason for describing our social media hack is so you can take these lessons and immediately apply them to where you see chinks in your own security armor.

Why Me?

There is no shortage of cybersecurity books available for your consumption from reputable, talented authors with a variety of experiences. You'll find some from journalists, who have dissected some of the most legendary breaches in history. You'll find others from luminaries, who speak with authority as being venerable forefathers of the industry. And you'll find more still from technical experts, who decipher the intricate elements of cybersecurity in significant detail.

But, as I type this, you won't find many cybersecurity books authored by marketers. And probably fewer still from marketers with just a few years in the industry. So why trust this author with a topic of such gravity?

Think of me as a hybrid between marketing and technology. I've spent my career translating technical concepts into everyday language. I've studied the intersection of work and technology to understand how corporate culture is shifting.

So if you're a generally nontechnical person, rest assured that I strive to give you sufficient education to understand the nuances of this thorny subject, without overwhelming you with technical details. If you're more technical than I am, while I won't dumb down this topic, I will provide

prescriptions that every employee—technical or otherwise—can practice to protect her organization. Finally, if you are one of my cybersecurity brethren, I hope you read and enjoy this book as a glimpse into our world. Then, I want you to pass it along to your non-cybersecurity colleagues to recruit them in our fight.

Why You?

You may consider yourself someone who doesn't have much to offer in the realm of cybersecurity. After all, how could employees, managers, executives, and board members who are not within cybersecurity's corridors really play a meaningful role in a game they may not even understand?

This is where I turn to the world of professional sports for inspiration, as it often reveals many lessons we can all learn about the power of teamwork. While I'm no sports junkie, I do have a soft spot in my heart for American football. That's because I have fond memories from my earliest years in grade school of sitting on my family room couch, next to my dad, watching his favorite team, the Dallas Cowboys, play.

Like millions of us who tune in to watch our favorite teams, I'm a spectator in the world of professional sports. Watching the game is about as close as the majority of us will ever come to playing it. Spectators hardly influence the outcome of a game. That's a role left to the far more important athletes and coaches on the field or on the court who, by their talent, tenacity, and teamwork, ultimately determine whether a game is won or lost.

I used to believe that. And then I was introduced to the Seattle Seahawks' 12th Man. The Seattle Seahawks are a professional U.S. football team. In football, there are 11 active players allowed on the field, per team, for any play. But the Seahawks recognize 12 active teammates—represented by 11 players and the equally important spectator crowd.

I eventually came to realize that Dad and I did not want our Cowboys facing the Seahawks on the latter's home turf. That's because the Seahawks' stadium is not one that favors opponents. Its noise level, created by the 12th Man, has been measured at only a couple of decibels below that of an aircraft carrier flight deck. As it turns out, these spectators have played quite a meaningful role in influencing the outcome of more than a few games. In three seasons, the Seahawks scored 26 wins against two losses on their home field. The 12th Man has twice set the world record for crowd noise and is even to blame for at least one minor earthquake.

Their revered football team knows just how important these "spectators" are. The Seahawks retired the number 12 jersey on December 15, 1984, in honor of their fans. You'll find a giant flagpole with the number 12 blazoned across it flying proudly in their stadium. When the team took the field for one of their Super Bowl appearances, they were led by someone carrying the 12 flag.

Are the 12s (as the Seahawks fans are called) really that loud? Mostly, yes. But it turns out their stadium was also specially designed to retain noise. Unlike other open-air stadiums where noise naturally escapes into the ether, the Seahawks' stadium has a second deck and canopy that bounces noise downward, creating a cacophony when the 12s roar.[1] The Seahawk organization has taken great measure to enlist the 12s as part of

the team—ensuring these fans can bring their collective might to the game and virtually play alongside those on the field.

The 12th Man teaches us that spectators can influence outcomes. But they must be engaged. They must be enlisted. That's where you come in. I've written this book to engage every layperson on your importance in a cybersecurity game that is always in play. No one can blame you for not taking up the mantle sooner. But after reading this book, no one can excuse you for abdicating your responsibility either.

This book seeks to advance the dialogue by picking up where so many other worthy titles end: giving the business layperson an action plan he or she can execute immediately to be part of an organization's cybersecurity agenda. If you still question whether it's an agenda that should include you, realize it already does. Cybercriminals are counting on employee apathy or disengagement to unleash havoc on their targets. If you are not actively playing on the side of your company, you are likely unknowingly a pawn on the side of your enemy. If you value online freedom, if you care to know that the data you use to make decisions isn't corrupted, if you insist that your connected devices are used for good and not harm, then you already share a mission with the cybersecurity professionals in your workplace. You have more in common with those of us in cybersecurity than you may realize.

W.I.S.D.O.M.

At McAfee, the executive team takes development seriously. We meet quarterly to put the "work" back into "teamwork." We coach one another, share intimate stories about

our professional journeys, and recommit ourselves to being more authentic toward one another and our employees. At the end of those development sessions, we practice something we learned from the AIP Group, our partner in leadership development, called W.I.S.D.O.M. It stands for **W**hat **I**'ll **S**ay (and do) **D**ifferently **O**n **M**onday. Each of us makes our W.I.S.D.O.M. commitment to hold ourselves and each other accountable to practicing one key developmental area we have learned.

In the same way, I want to equip you with W.I.S.D.O.M. for this journey. That's why, after each chapter, I'll give you a practical prescription for what you can do on Monday to improve your organization's cybersecurity posture. Some of the tips are banal on the surface but can have significant impact for your success. Others require more work, but the view is worth the climb. In every case, I'll limit the prescription to no more than five pieces of W.I.S.D.O.M. in any given chapter, since I want to focus on the 20 percent of efforts that will yield 80 percent of results.

The advice you'll find in these pages is applicable to a very wide spectrum of businesses. McAfee protects hundreds of millions of consumers around the world. We also protect the largest government and enterprise environments. Our solutions go from the backyard to the boardroom. We understand you.

The W.I.S.D.O.M. is also applicable to a very broad range of roles in the business—from the board member to the individual contributor. Cybersecurity is a mission too important to be left in its siloed technical domain. Each employee or stakeholder plays a part. This book covers a lot of ground to apply discipline across the organization.

In fact, to prepare for this book, in 2017, McAfee interviewed 50 chief officers across a variety of functions (including CEOs, CFOs, CIOs, CMOs, and more) to take their pulse on their firms' cybersecurity readiness. We also conducted an online ethnographic study among 69 employees for the same reason (think of this methodology as an online focus group, of sorts, in which we gave respondents questions and exercises in which to participate and collaborate over several days). At the beginning of each chapter, you'll see a direct quote from one of these research subjects to help further frame the discussion and prescription.

We need you, the 12th Man, in the fight with us. You can determine the outcome of this battle. This book seeks to teach you about the game in play, while giving you tools and tips to know when to cheer even louder. When you do, the enemy will know he has entered a house that will not succumb easily. We will ultimately persevere in a fight that we simply can't afford to lose.

Now, let's get you enlisted.

Note

1. Louise Bien, "What Makes Seattle's 12th Man So Special?," SB Nation, January 22, 2015, https://www.sbnation.com/nfl/2015/1/22/7871519/seattle-seahawks-12th-man-super-bowl-patriots.

CHAPTER

2

Mr./Ms. Cellophane

A very simple analogy that I use with the boardroom when you're talking about cybersecurity and defense is a baseball game. I've got to pitch a perfect game every time. [Adversaries] only have to get one single. It doesn't even need to be a bad apple that gets in. It can simply be somebody set up a server and missed a step. The reality in cybersecurity, if you're on the defense, you have to pitch a perfect game every time. That's not going to happen.

SVP/EVP, Professional Services Company

Poor Amos. His wife murders her lover in cold blood and claims doing so in self-defense against the man she says is an "unknown" intruder. Amos dutifully stands by her side, even after discovering the ugly truth of the affair. Everywhere Amos

goes, he is a shadow in the background of his wife's lurid story, practically invisible to all around him.

I'm speaking of the character Amos in the award-winning musical *Chicago*. His character laments just how overlooked he is in his solo number of the production aptly titled, "Mister Cellophane":

And even without clucking like a hen,
ev'ryone gets noticed now and then,
Unless, of course, that personage should be
invisible inconsequential me.
Cellophane, Mister Cellophane
should have been my name, Mister Cellophane,
'cause you can look right thru me,
walk right by me and never know I'm there.

Many of us can relate to Amos in sometimes feeling like we are invisible. It's usually not a great feeling, typically accompanied by that of being underestimated or underappreciated. And it's no fun being outright misunderstood.

For too long, chief information security officers (CISOs) have been the metaphorical Mr./Ms. Cellophanes of our organizations, destined to toil in virtual anonymity as they relentlessly focus on the yeoman's work of security. They've lived in the shadows of those they protect. Indeed, if they emerge from their cloak of invisibility, there's bound to be trouble on all sides.

As employees, we don't want to be bothered with CISOs or their department. We simply expect them to keep us safe. And we want them to do it while staying out of our way. In fact, CISOs got their start in the back office of our organizations,

literally out of sight and out of mind. If they dare hit our radar and become visible with annoying security patches that slow our performance, we vent. Worse yet, if they attempt to block us outright from accessing our favorite service or device, we'll simply bypass them.

Case in point: McAfee reports the average organization has around 2,000 cloud services in use at any given time. What does its IT team *think* it has? Closer to 30.[1] That chasm between perception and reality can at least partly be blamed on shadow IT—a phenomenon where employees go rogue and use cloud services without the knowledge of, let alone authorization from, their IT department.

What's worse than a CISO becoming visible to employees? Becoming visible to the board. Historically, boards have wanted as little to do with cybersecurity as employees. If the board called a CISO into a meeting, it typically wasn't to give a strategic update on the state of cybersecurity in the company or to receive a heartfelt "thanks" for his work. It was more than likely to answer tough questions about a breach.

Deloitte,[2] the global professional services network, does a regular study of boards of directors, in which it surveys hundreds of public companies. As recently as 2014, a mere 5 percent of the *very largest* companies had standing committees of the board relating to the combined topic of "cybersecurity and IT."[3]

So the CISO has largely accepted the role of Amos in our metaphorical musical—devoted to offering protection for those who don't appreciate it and destined to remain in the shadows.

But bad actors intent on inflicting harm are rewriting this musical. Hardly a day passes without a headline

(or company) announcing the next breach. The mood of the board is changing. Many are realizing that relegating the CISO to the shadows is at their own risk. When Deloitte repeated its board study in 2016, cybersecurity had risen to the number one risk earning board focus, with 25 percent of companies experiencing a breach in the past two years.[4] Mr. and Ms. Cellophane are finding themselves freed from the back corner of the back office, and even seeing an occasional invitation to board meetings as a result.

However, just because hackers have put the limelight on CISOs doesn't solve the cybersecurity challenge. It's heartening that boards are taking notice of the problem, but simply acknowledging it is only the first step. Improving a company's cybersecurity posture requires these parties—the technical CISO and the strategic board executive—to learn each other's language.

Let's start by attempting to relate to what I submit is the most misunderstood role of the C-suite, the CISO. The edification benefits not only board members, but all employees alike. CISOs profit by finally emerging from the shadows.

The New Kid on the Block

Corporations, and the functional disciplines that comprise them, have been around over hundreds of years. Banks and manufacturing firms were among the earliest corporations, so it should come as no surprise that many major public companies today have deep competency in finance or operations—the initial disciplines that served as the foundation for our corporate ancestors.

Indeed, according to Deloitte's 2016 Board Practices Report, other than the CEO and general counsel, the members of management most likely to regularly attend board meetings are the CFO (chief financial officer) (cited by up to 99 percent of companies surveyed) and the head of a business unit (cited by up to 47 percent). What about the CISO? He only makes a regular appearance in board meetings for up to 11 percent of companies, by comparison.[5]

It should come as no surprise that CISOs are still clawing their way into these closed-door sessions. After all, with other functional disciplines spanning centuries, if not millennia (lawyers can claim their functional roots all the way back to ancient Egypt), the CISO's role goes back only decades. Back then, we didn't even call it "cybersecurity." These early pioneers claimed their profession as "Information Security," consistent with their field's beginnings in "Information Technology."

It's critical we take a brief, but important, journey into the origins of cybersecurity for us to understand the relatively new role of the CISO. Back in the day, physical security and information security were largely one and the same. I remember, not that long ago, if I wanted to access my company's network, I did so through a stationary desktop, connected to a physical Ethernet cable that took me to a local area network. The desktop and the Ethernet technology connecting it resided on my company's premises. So the only way to access the corporate network was to physically enter the company itself—and that required a tangible security clearance, like my employee badge. I connected physical and information security inextricably in mindset and in practice.

I'm amazed at how much work has changed in just my lifetime. Work is no longer a place I go; it's a thing I do. I increasingly work outside the safe, physical perimeters of my employer. I blend my professional and personal lives seamlessly—responding to email over my mobile device, connecting just about anywhere I can find WiFi, and accessing myriad cloud services that make my life easier.

I'm not the only one embracing work as a tetherless experience. Let's consider how our relatively new work behaviors pose exponentially greater pressure on the CISOs who must defend us and our companies. At any given time, our CISO is balancing one or more of three strategic efforts:

1. Transformation

Every adoption of a technology, be it mobility, cloud, or the Internet of Things (IoT) subjects a company to greater risk. That's because the safe perimeter of the enterprise continues to erode in the process.

Case in point: Who "owns" the Internet? That's a byzantine maze of complexity that would make the heads of the most technical among us spin.

Who "owns" the infrastructure of public clouds, like those provided by Amazon, Google, and Microsoft? That's at least an easier question to answer—those companies are responsible for the physical security of those cloud environments. But that's the equivalent of saying they own securing the physical access to those massive data centers, much the same way our companies own protecting the buildings in which we work. Cloud theft isn't typically the result of resourceful thieves breaking into the physical data centers

of major web companies. It's the outcome of cybercriminals finding a way to hack the data residing in or traversing through said data centers.

Who ultimately "owns" responsibility for that data? That's the easiest and clearest answer of all: your company—and your company alone—is responsible for securing its own data, regardless of where it resides—be it on servers located on your employer's premises or those rented through a public cloud marketplace.

The cloud is just one example of the CISO's receding control over the infrastructure used to store or transmit her company's data. The bring-your-own-device (BYOD) movement is here to stay, meaning company-issued mobile devices may soon be relics of the past. There's a good reason so many companies are rushing headlong to allow their employees to work on whatever mobile device(s) they choose. According to Frost & Sullivan, using smartphones for work saves employees close to an hour per day, while increasing productivity by 34 percent.[6]

To make the goal of transformation even more difficult to accomplish, old technologies have a very long shelf life. Even with business units rushing to deploy cloud services (with or without the formalized consent of IT), there's still a long tail of on-premises infrastructure that must be maintained. Consider USB thumb drives as one example. In 2017, researchers at Ben-Gurion University documented 29 known attack vectors to compromise USBs.[7] And Apricorn, a manufacturer of software-free, hardware-encrypted USB drives, reported in 2017 that while 90 percent of employees used USBs, only 20 percent did so with encryption.[8]

Since long-tail legacy technology infrastructure rarely goes away and never does so quickly, these transformation pursuits entail risky expansions of scope and responsibility.

What's our CISO to do? Frivolously support an all-access, anything-goes environment and he leaves his organization open to increasing risk. Become the department of "no" to contain the potential threat and he'll likely be disintermediated by the very employees he must protect (remember those nearly 2,000 cloud services in use unbeknownst to IT professionals in the average company?).

The CISO is in an unenviable position. He must simultaneously protect his company's most precious digital assets while advancing its transformation agenda. Unfortunately, those imperatives couldn't be at greater odds with one another.

2. Risk Management

Cybercrime is big business—to be exact, a $600 billion business in 2017, up $100 billion from 2014.[9] In terms of global impact, cybercrime ranks third as an economic scourge, behind government corruption and narcotics.

How did we get here? There was a time when cybersecurity was relatively "simple." Not only was security contained to the physical, as already mentioned, but addressing a threat was significantly easier. In 2006, McAfee detected 25 new threats per day. Ten years later, that figure had jumped to 500,000—more than five new threats per second!

Volume is only part of the challenge. Spotting a threat used to be straightforward. Threats came in the form of malware—software designed by bad guys to wreak havoc on their

victims. The cybersecurity industry talks of "traditional" malware, including those pesky viruses you've come to know and hate. Malware once only came with a static string of code that allowed the industry to identify it as such. Think of it as a software fingerprint of sorts—what the cybersecurity industry calls a signature. Much like law enforcement relies on a national registry to identify criminals based on fingerprints, the cybersecurity industry looks for software signatures to load known malware into its own database. If the signature is found on a file, the file is blocked and the threat contained.

How times have changed. The most insidious threats no longer come conspicuously donning a known and readily identifiable fingerprint. Bad actors have grown much smarter. When you read this, the latest cybersecurity threat is almost certainly not listed here, but as I write this, my industry is fixated on "fileless" attacks. These threats surreptitiously exploit trusted technology within your organization, like sanctioned tools and applications. Then they do their damage, typically by gaining access to your company's larger network and pilfering its data.

I say "typically" because data exfiltration is no longer the only tactic online adversaries execute. Ransomware is another topic du jour of cybersecurity, where adversaries won't bother exfiltrating data to sell it on the Dark Web. They'll shortcut their path to profit by locking (or encrypting) their victim's files and demanding ransom for the key (or decryption) before permanently destroying them.

Or perhaps data and money aren't the end pursuits at all. An adversary may be more inclined to wreak havoc by

shutting down access to a victim's critical systems, bringing the company to its knees in the process. Or hackers may practice information warfare, where data itself is weaponized to create chaos (just think of the volumes of data your company generates each day and how the tiniest manipulations to it could cause your employer considerable harm and confusion). Or perhaps it's your company's reputation the hacker is after, as McAfee learned the hard way with our social media exploit.

You get the picture. Not only are threats exponentially greater, but they're significantly more complex and insidious. And the volume, variety, and vigor of threats translate to more risk.

How can CISOs be expected to explain this convoluted reality to their boards, many of which meet less than six times per year for four hours, on average, according to Deloitte? That's 24 hours per year for the average board to cover topics ranging from company strategy to financial performance to sensitive M&A activities and everything in between. Is it any wonder that cybersecurity as a topic, with its highly technical and complex nature, gets short shrift by most boards?

But it doesn't have to be this way. Cybersecurity is indeed highly technical. But it's also very straightforward at its core. It's fundamentally about risk management—a language in which most board members are naturally fluent.

CISOs are continually walking a tightrope in mitigating risk. They must strike the right balance between addressing high-volume threats that likely won't cause catastrophic impact and low-volume, highly targeted attacks that can take a company down.

All of us, board members or otherwise, can relate to the CISO on the challenge of risk management, since we walk the same fine line in our own lives. We have bathmats in our bathrooms to prevent the risk of falls (a relatively minor risk for most under a certain age). We use smoke alarms in our homes and purchase insurance policies to mitigate more catastrophic risks, like fire. And while other truly cataclysmic risks, such as being struck by a meteorite can happen (and, yes, this really *did* happen for one poor unfortunate soul in 1954[10]), we safely ignore these risks given their infinitesimal probability.

CISOs must categorize risks in much the same way for their companies. The challenge for our CISO is to simplify the topic of cybersecurity, without making it simplistic in the process. The onus for board members? Leaning in to the discussion, realizing the morass of complexity beneath the surface will rarely, if ever, yield a clear-cut decision. War doesn't lend itself to clarity. Neither does cybersecurity.

3. Automation and Efficacy

"Doing more with less" is an annoying cliché of the modern enterprise. It's also the CISO's unfortunate mandate. Not only does the volume of threats show no sign of abating, but the demand for cybersecurity professionals far exceeds the supply of talent in the labor market. According to Cybersecurity Ventures, more than 3.5 million cybersecurity jobs will be unfilled by 2021[11]—that's enough to fill 50 NFL stadiums!

And the problem is only growing worse. In 2014, the cybersecurity industry estimated it would be short one million professionals worldwide. By 2015, the gap had crept up to 1.5 million openings. In 2016, forecasters thought the

cybersecurity talent shortage would be 2 million professionals in 2019.[12] Just as threats continue to increase, so does the gap for qualified cybersecurity professionals.

Given there aren't enough people to throw at the problem, CISOs have resorted to a cavalcade of products from a vast battalion of cybersecurity vendors vying for cybersecurity dollars to fill the void. In stark contrast to the shortage in the labor market, there's an overwhelming surplus of cybersecurity products vying for the CISO's limited dollar. As of this writing, there are 3,500 cybersecurity vendors[13] courting CISOs. Each vendor offers one or more defensive technologies, many promising to solve a small (if not large) portion of the cybersecurity challenge.

There can be too much of a good thing. And the abundance of cybersecurity technologies available to the CISO is illustrative of this axiom. CISOs, attempting to demonstrate value and anticipate the next threat, have historically rushed to adopt the latest defensive technology for their arsenal against the adversary.

But they've gotten the short end of the stick in executing this strategy. That's because the fragmented vendor landscape that competes for every dollar is itself a complex quagmire of technologies that, for the most part, don't work well together. Too often, this technology is promoted, purchased, and put on the shelf. Budgets are spent, "shelfware" grows, and organizations are no more secure for the innovations, intentions, or investment. Even if the technology makes its way off the shelf and into deployment, chances are it's not integrated with the rest of the organization's defenses.

Imagine going to war with a cluttered mess of artillery in your inventory. Picture being inconsistent in deploying

this weaponry to cover your bases against your enemy sufficiently. Now envision your fighters not being able to communicate with one another to share information about the threats they encounter to collectively bolster your coordinated defense.

You likely don't have to imagine it. If your company has one, just visit its security operations center (SOC), the nerve center where your cybersecurity colleagues stand as first responders between your company and unending attacks. These front-line cybersecurity professionals have often inherited a patchwork of technologies and tools acquired over the years, usually adopted over multiple CISO regimes in their companies. Many of these products do not share threat intelligence, let alone make the jobs of cybersecurity professionals any easier. All too often, you'll find your cybersecurity colleagues working for their tools, rather than their tools working for them.

Enterprise Strategy Group (ESG), an independent industry analyst that studies the cybersecurity market, reports that 40 percent of organizations have more than 25 cybersecurity tools deployed. Roughly the same percent admit to manually collecting intelligence feeds. And 27 percent believe the security team spends *most* of its time fighting fires, rather than working on strategic projects,[14] leading to staff burnout and turnover—disastrous consequences for a CISO confronting a global talent shortage crisis.

As if that weren't enough, there's a dirty, unavoidable secret inherent in the cybersecurity industry. It's this: no one product can defeat cybercrime. You may not find this surprising. After all, it would be the equivalent of going into

a sustained war with just one weapon in your arsenal. You wouldn't do it and expect to last long.

But there's more to this reality. It's not just that there isn't a proverbial silver-bullet defense that inoculates all threats. It's that *every* defensive technology is most effective when it is *first* deployed in the market. This is completely opposite from what we've learned as conventional wisdom in IT.

Think about it. When a new IT technology comes to market, most companies are reluctant to be an early adopter. After all, why be a guinea pig for an unproven technology? Let other companies go first, work out the bugs, and make the technology better (and cheaper). Then, follow fast in deploying it. That seems like a much smarter playbook for deploying your garden-variety IT technology.

But cybersecurity technology is fundamentally different. When an IT organization is deploying the latest fill-in-the-blank IT technology, there isn't an adversary on the other side actively working against its success. Not so with cybersecurity. When enough of the market deploys a defensive technology that is highly effective against a threat, adversaries go back to their own product labs to develop countermeasures against it. They ultimately find a way to circumvent the defensive technology, if not make it less effective over time. (It's at that time that cybersecurity vendors, like McAfee, return to our labs and develop countermeasures against the countermeasures, and the race continues.)

Time matters in cybersecurity. Being early to market with a new defensive technology especially matters. That's because said technology will deliver maximum efficacy for the earliest of its adopters.

So let's try to square this circle by thinking like a CISO:

1. There's no single defensive technology that defeats all varieties of cyberattacks—there are simply too many of them, and the adversary continues innovating every day. You'll need to deploy lots of products, from multiple vendors, to put forward your best unified defense.
2. Every defensive technology is most effective when it's first deployed in the market. In short, you want to be an early adopter of the latest cybersecurity technology. That's because adversaries have not had sufficient incentive or time to develop countermeasures against it. When they do, the cat-and-mouse game between cybersecurity vendors and adversaries ensues, with each side developing countermeasures against the other.
3. So being first to deploy matters. But you (and the rest of the industry) suffer a talent shortage. There just aren't enough people on your team to implement defensive technologies quickly. Even if you can, chances are you're not deploying these defenses in a coordinated way, such that all technologies in your environment work synergistically to share threat intelligence and operate with consistent tools.
4. And since your defensive technologies don't share threat intelligence seamlessly, your limited cybersecurity staff is left to fill in the gaps. Given that both the volume and complexity of threats are exponentially increasing, your team must separate the signal from the noise in detecting and remediating the most insidious threats in your environment—before your adversaries get the upper hand and inflict harm on your company.

Who wants that challenge? Not many. It's why cybersecurity professionals truly are the unsung heroes of our companies. They stand in the fight for us. They sit in the shadows, invisible and largely unappreciated for their efforts.

Bringing us back to our CISO, "doing more than less" is so much more than a trope. It's essential. She must find a way to automate as much of her environment as possible, to allow her scarcest asset, her employees, to hunt for the most sophisticated attacks. And she must aggressively deploy new cybersecurity technologies while not compromising her overall cybersecurity posture with nonintegrated defenses.

You now understand what your CISO is up against and can put yourself in her shoes:

- Help your company transform, while protecting an expanding attack surface of cloud, mobile, and IoT technologies.
- Manage your company's risk, all while the volume and sophistication of threats escalate exponentially.
- Maximize efficacy by adopting products early and integrating them into a unified defense. And automate workflows to free up capacity for your scarcest resource—your talented employees—to hunt the most sophisticated and menacing threats.

W.I.S.D.O.M. for the Board and CEO

Everyone reading this book is either part of the cybersecurity problem or part of its solution for his company. The CEO and board member are no exceptions. There are multiple ways to finally notice the Mr./Ms. Cellophanes among us and give

them the credit and support of which they are so rightfully deserving.

First, cybersecurity should not be a random or sporadic topic to board agendas. Even more, it's not a topic that can be outright ignored until the inevitable breach occurs. Boards must make cybersecurity a regular topic. I'm not so naïve as to believe that cybersecurity will ever earn the same amount of time or attention as financial performance, for example. But if boards are at all concerned about mitigating risk (and I'm confident most are), then give cybersecurity reasonable time on your agenda.

How much time should you allocate? It depends on how well your board already understands this topic. If you haven't started by having your CISO give a meaningful view of your current cybersecurity posture, *allocate at least 90 minutes to the topic.* In that time, your CISO should cover the assets that are most critical to the overall company.

This requires significant consultation with business unit leaders. The right answer may not be so obvious. Customer data, for example, may not be your organization's most prized asset (although it will likely rank very high on the list). If you're in the business of running major manufacturing facilities, these sites may be your most strategic asset (and, yes, with connected devices permeating just about every facet of business, motivated hackers can, more often than not, compromise [if not shut down] these facilities).

Your CISO should provide the current vulnerability state for each asset, listed in priority order of the asset's strategic value. Without oversimplifying the task, you can imagine a 2x2 quadrant, with vulnerability state and strategic priority plotted on each axis. *Those assets that are both highly strategic and highly vulnerable deserve immediate budget reallocation.*

On the point of budget allocation, while that may seem like an obvious output of this exercise, most boards are inclined to loosen purse strings only in the event of a breach—and even that's a tall ask. In 2017, EY's Global Information Security Survey found 76 percent of executives admitting that the allocation of additional cybersecurity resources would only be triggered in the case of a breach that did actual damage. A breach with no damage? Nearly two-thirds said it would not compel additional spending.[15]

Having sufficient cybersecurity knowledge to provide effective oversight of cyber risks is essential. And yet, less than 40 percent of boards have it.[16]

Once your board and CISO have aligned, make your CISO a regular attendee at board meetings. Cybersecurity changes at a dizzying pace. Your adversaries are highly motivated to do you harm. They don't take a day off. You shouldn't either.

Spend at least 30 minutes in each board meeting discussing the topic of cybersecurity. If the average board meets six times a year for four hours each time, I'm asking for less than 15 percent of your time on this important topic. Deloitte reports that less than 20 percent of boards feature cybersecurity as a regular board agenda.[17] If Deloitte has it right, and cybersecurity is also the top risk for most boards, spending three hours per year regularly discussing it seems more than reasonable.

Have the CISO update your risk assessment in these sessions. He should be prepared to discuss how the vulnerability landscape of your assets has shifted. *He will know this information based on giving you output from what the cybersecurity industry calls red-teaming exercises or penetration testing. Insist on these exercises as a discipline.* These are simulated attacks your CISO

will coordinate against your company to test its defenses. He'll organize two teams—a red team (the attackers) and a blue team (the defenders). The red team, typically comprised of experts from external entities, tries to breach the blue team (the company). Through this exercise, the company is finding where it had previously unknown vulnerabilities.

Know this: The red team *always* wins. And that's a *good* thing. You want to discover your company's vulnerabilities before hackers do. Compensating external agencies to discover your cybersecurity weaknesses is a lot more cost-effective than paying off adversaries (and regulators) in the event of an actual breach.

Finally, *consider appointing a board member with cybersecurity expertise.* This individual will bring a unique perspective to the table. As a steward for cybersecurity, he will ensure your board doesn't regress in putting the function back in the shadows. It seems we have work to do on this front. Deloitte reports that more than 80 percent of companies have not added anyone to their boards with cybersecurity expertise in the past two years.[18]

Making Mr./Ms. Cellophane Visible

The CISO is an indispensable, often underestimated, member of the executive team. While cybersecurity is everyone's responsibility, boards and the CEO must set the right tone from the top of the organization. You must play your part in elevating cybersecurity to the role it has earned at your table.

One of my favorite movie quotes comes from *The Usual Suspects*: "The greatest trick the devil ever pulled was

convincing the world he didn't exist." Your adversaries want nothing more than for you to keep your Mr./Ms. Cellophane neatly tucked away in the shadows. They're hoping that, if you do, you'll also ignore them—the increasing legion of hackers seeking to do your organization harm. These bad actors want you to deprioritize cybersecurity as a nonstrategic investment. Don't give them that power.

If you fail on this point, you risk losing one of the most valuable members of your executive team: Mr./Ms. Cellophane. And that cybersecurity talent shortage I mentioned will prove very difficult for you to hire a replacement anytime soon.

CISOs have a relatively short tenure at their companies, as low as 24 months by some industry benchmarks. ESG sought to find out why the life expectancy of a CISO is so short. The cybersecurity labor market is a seller's market for now and the foreseeable future (thanks to that talent shortage). But ESG found that there's far more than compensation in play when a CISO hangs it up and joins another company:

- 36 percent leave when their current employer doesn't have a corporate culture that emphasizes cybersecurity (good thing you're reading this book!);
- 34 percent exit when they are not active participants with executive management and the board of directors; and
- 30 percent bolt when cybersecurity budgets are not commensurate with the organization's size or industry.[19]

There's a lot the CEO and board can do to be a part of the cybersecurity solution, including giving your CISO a voice. Beyond giving her access to the conversation, offer her a forum to argue her case for more resources (given what

I've shared with you, her case for more dollars is likely more legitimate than not). All that said, treat her as an executive member and inspect her arguments by asking salient questions. To do this, you must first enrich your understanding of the cybersecurity problem—a pursuit I hope this chapter supported.

The true stuff of a CISO is made of anything but fragile cellophane. She has a backbone of steel in the stiff winds of transformation; iron fists to pound through an unending onslaught of attacks; and a jaw of concrete to take the blows of blame that would incapacitate otherwise weaker individuals. When you finally recognize and appreciate the grit and determination that make up the most misunderstood member of the executive team, you bring cybersecurity out of the shadows, along with adversaries who would love nothing more than to remain there.

Notes

1. McAfee, "Cloud Adoption and Risk Report," 2019.
2. I'm sharing the smart work insights of many others who are steeped in the cybersecurity challenge and in the best practices of successful enterprises. I'll share McAfee's proprietary insights along the way, but I'm proud to introduce you to a growing body of research and fresh thinking by organizations like Deloitte, Ernst &Young (EY), ESG, and others. You're not alone in this fight. The number of savvy analysts and consultants focused on this space proves it.
3. Deloitte, "2014 Board Practices Report—Perspectives from the Boardroom," https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-2014-board-practices-report-final-9274051-12122014.pdf.
4. Deloitte, "2016 Board Practices Report—a Transparent Look at the Work of the Board," https://www2.deloitte.com/content/dam/Deloitte/us/Documents/center-for-board-effectiveness/us-cbe-2016-board-practices-report-a-transparent-look-at-the-work-of-the-board.pdf.

5. Ibid.
6. Melanie Turek, "Employees Say Smartphones Boost Productivity by 34 Percent: Frost & Sullivan Research," Samsung Insights, August 3, 2016, https://insights.samsung.com/2016/08/03/employees-say-smartphones-boost-productivity-by-34-percent-frost-sullivan-research/.
7. Nir Nissim, Ran Yahalom, and Yuval Elovici, "USB-Based Attacks," *Computers & Security*, Elsevier, September 2017, https://www.sciencedirect.com/science/article/pii/S0167404817301578.
8. Apricorn press release, "Apricorn USB Data Protection Survey: Majority of Enterprise USB Security Is Outdated, Inadequate; Nine Out of 10 Employees Use USB Devices, But Only 20 Percent of Them Are Leveraging Encryption," December 12, 2017, https://markets.businessinsider.com/news/stocks/apricorn-usb-data-protection-survey-majority-of-enterprise-usb-security-is-outdated-inadequate-nine-out-of-10-employees-use-usb-devices-but-only-20-percent-of-them-are-leveraging-encryption-1011079268.
9. McAfee, "The Economic Impact of Cybercrime—No Slowing Down," https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf.
10. Justin Nobel, "The True Story of History's Only Known Meteorite Victim," *National Geographic News*, February 20, 2013, https://news.nationalgeographic.com/news/2013/02/130220-russia-meteorite-ann-hodges-science-space-hit/.
11. Cybersecurity Ventures, "Cybersecurity Jobs Report 2018-2021," May 31, 2017, https://cybersecurityventures.com/jobs/.
12. Ibid.
13. Leslie Scism, "Insurers Creating a Consumer Ratings Service for Cybersecurity Industry," *The Wall Street Journal*, March 26, 2019, https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600?mod=hp_lista_pos5.
14. Jon Olstik and Jack Poller, "Automation and Analytics versus the Chaos of Cybersecurity Operations," Enterprise Strategy Group, September 2017.
15. EY, Global Information Security Survey 2017–18, https://www.ey.com/gl/en/issues/governance-and-reporting/center-for-board-matters/the-cost-of-cybersecurity-on-the-board-agenda-ey.
16. Ibid.

17. Deloitte, "2016 Board Practices Report."
18. Ibid.
19. Jon Oltsik, "Why Do CISOs Change Jobs So Frequently?," CSO, January 2, 2018, https://www.csoonline.com/article/3245170/why-do-cisos-change-jobs-so-frequently.html.

CHAPTER

3

"Good Morning, This Is Your Wakeup Call."

I would say I have never knowingly violated my company's cybersecurity policy. And yet, I feel that the larger problem overall is that there's not always clear communication about what the policies are. These things tend to be glossed over by managers all the time because they themselves are not always savvy as to what all the rules are. I think the reason for this is the majority of people do not understand all the implications of their actions when it comes to cybersecurity and protecting company information. And many people within organizations do their best in terms of trying to be safe using technology. But that is a constant battle being waged by IT groups within almost every company.

Respondent, McAfee Online Ethnographic Study

I grew up with a healthy respect for authority. My mom and dad were on the stricter side. They expected me to comply with reasonable rules. Do your homework. Be home by curfew. Clean your room. Respect your elders. The stuff of building a responsible and contributing member of society.

So when I got a voicemail from my mom early one weekend morning telling me someone from law enforcement was looking for me, I couldn't reach for my phone fast enough.

"Allie, there's a sheriff in Nashville who just called here looking for you. He says there's a warrant out for you for a missed court appearance in Davidson County."

My heart started racing as I listened to my mom frantically giving me this sheriff's information.

"Mom, this doesn't make sense. I haven't lived in Nashville for 20 years! I never was told I needed to be in court."
"Babe, I told him the same thing. I told him I'd have you call him."

I'm a much earlier riser than my husband. I figured I'd quickly take care of the phone call before he woke.

I dialed the digits with the (615) Nashville area code.

"Sheriff Johnson speaking."

Have you ever been caught off guard when the person you're calling answers the phone? It's a weird feeling. You expect an answer. Yet, you don't. That's the kind of feeling I had when I heard his voice. I found myself searching for my words.

"Uh, hello, Sheriff Johnson. This is Allison Cerra calling. I understand you spoke with my mom this morning."

He wasn't at the same loss for words.

"Yes, Ms. Cerra. I called your mother since we've been trying to reach you. I have an outstanding warrant for you to appear before Judge [name withheld] in Davidson County, Tennessee, for a missed court appearance in August.
"I show that you resided in Nashville in the past, is that correct?"

Authority is a powerful force, especially for someone who has respected it for a lifetime. I had learned from an early age that, when someone in authority asks you a question, you don't answer with a question. You simply answer.

"Yes, that's correct."
"Well, we're showing you have a warrant for a missed court appearance on August 15."

Authority also compels you to correct the record. This guy couldn't be right. But instead of my fight-or-flight trigger kicking in, raising red flags of suspicion (and questions), my overwhelming deference to authority had me explaining.

"Sir, I'm sorry. That doesn't sound right. I only lived in Nashville a few months back in 1995. I wasn't even in Nashville in August."
"Ms. Cerra, I don't know what to tell you. The judge issues the warrants. You'll have to take care of it with her."

Now here's where the story veers into the unexpected. Because you would expect that, if this guy was a scammer, he would immediately launch into his "but if you give me your credit card number, I'll be sure to clear this up for you" pitch that would have undoubtedly sent my red flags flying.

He did no such thing. He just kept asking me questions to verify my background.

And I just kept answering.

"I show that you lived at this address, is that right?"
"Yes, sir. That's correct."
"And I show that you now reside in Denton County. Correct?"
"Yes, with my husband."

Notice how I was in the full grips of authority, answering questions with even more information than required. This guy had me.

It's around this time that my husband emerged from the bedroom, wiping the sleep from his eyes, yet alert enough to realize I was on a serious phone call—and it didn't sound like work.

"What's going on?"

The sheriff was still confirming information with me. I hurriedly put him on mute to bring my hubby up to speed on the morning's events.

"Mom called. She got a call from a sheriff in Nashville who says there's a warrant out for me for a missed court appearance. I'm on with him now trying to clear it up."
"How is that possible? You haven't lived there in forever."

(Now I was getting irritated with my husband for stating the obvious.)

[Through clenched teeth] "I know that. That's why I'm trying to clear this up."

And then my husband, barely awake, asked me the question that I should have asked myself before ever dialing the number:

"Are you sure this guy isn't scamming you?"

You know when thoughts come rushing into your head so fast that you can play back the last few moments of your life in what is no more than nanoseconds? In my case, it was the past 30 minutes since I first picked up the message from my mom that I was now reliving in my head. For the first time in those 30 minutes, I had unmistakable clarity.

My mind was blown and my heart now racing for an entirely different reason. "Sheriff So-and-So" was still blabbering as my fight-or-flight response finally kicked in. I attempted to gather my thoughts and reengage the brain that had failed me.

"Sheriff, I'm sure this is a mix-up. Thank you for alerting me to it. I'm going to call you back to resolve it."

I wanted off that phone call. He was surprisingly accommodating. No last-ditch hard push for a credit card number. No threatening that police would be on my doorstep to collect me in minutes.

"Sure, Ms. Cerra. I understand. You can reach me back on this number."

Click.

Before I had even hung up, my husband was already on his cell phone, calling the Davidson County Sheriff's Office.

You can likely guess the rest of the story. There was no Sheriff Johnson employed there. Just as there was no outstanding warrant for me for a missed court appearance—or anything else, for that matter. Apparently, this type of scam was quite popular as confirmed by the real policeman on the other end of my husband's line.

"We get at least one of these a week. It's a scam. Tell your wife that we don't call people like that when there's a warrant out. We just show up on your doorstep." (Duh. I felt like an idiot.)

But, just for good measure, I went to my own local precinct to confirm there was no blemish on this responsible-and-contributing-member-of-society's record. I took that well-measured respect for authority, deeply ingrained in me, and asked the officer behind the desk if he was planning to arrest me. Relief finally washed over me when he looked at me as if I had just landed from Mars, but answered with the only word I wanted to hear, "No."

* * *

You might be questioning your own judgment in buying a book about protecting your company from cyber threats

from an author who just admitted to such a stupid mistake. You wouldn't be off the mark. After all, I've already told you I felt like an idiot after the episode unfolded.

But before we both judge my actions too harshly, let's consider that my story is just one example of what is happening literally thousands of times a day to unsuspecting victims like me. The cybersecurity industry describes such scams as "social engineering."

You know one variety of this as "phishing," which is when cybercriminals send malicious emails, pretending to be a trusted authority in their victims' circles, asking they give up sensitive information or click on a link. We've come to somewhat underestimate phishing or the ingenuity of its creators. Phishing has come a long way from the "Help, I'm a Nigerian prince and I need money" days. McAfee detected more than a million new phishing URLs in 2018 alone.[1] These are the URLs attached to those malicious emails to get you to take the bait.

And social engineering moves beyond the digital realm, as my situation proves. I work in the industry, so I've learned to look for those phishing emails. But I wasn't expecting an old-school attempt over the telephone.

Criminals needn't be sophisticated to be effective. They know that trust is an essential ingredient in our society. They also know that I'm not alone in my upbringing. Many of us are responsible, contributing members of society. We learned to be that way through old-fashioned values of respect and trust.

The last thing I want is for any of us to succumb to fear-mongering that has become too commonplace in our world. Trust is essential for progress. And, yet, without being too

trusting, we can also avoid being too fearful. It's a fine line to walk, not unlike all the others you're finding as we unwrap the complex topic that is cybersecurity.

Without rushing headlong into some end-of-times prophecy where hackers take everything we've got, there is a sobering reality that I can't hyperbolize and it's this: for any individual contributor reading this book, *you* are among your company's strongest or weakest links in its fight against cybercrime.

Consider the power of that statement. Industry analyst Gartner predicted that companies spent more than $114 billion worldwide in cybersecurity products and services in 2018.[2] That puts cybersecurity in the same zip code as other $100 billion-plus industries, like digital television and video, digital marketing and gaming.

Yet, that investment is no substitute for employees doing the right things and doing things right.

The Best Defense

Military history across millennia records that the best defense is a good offense. Which explains why George Washington included this time-tested military advice in his writings even in retirement, nearly a quarter century after he led a fledgling nation to victory in its War of Independence. It serves as sound instruction when competing against an opponent. Draw first blood, and your rival will be more distracted defending himself than attacking you. In sports, teams try to put the first points on the scoreboard to earn initial momentum in a game. In business, companies seek first-mover advantage in launching a new product or service to capture early market share.

In cybersecurity, there's no such thing as a "good offense" for a company. That's because, by definition, companies aren't the ones striking first. That would be the job of the adversary. Adversaries *always* get first-mover advantage. They apply the axiom that has served reputable categories so well. Our companies are destined to playing defense forever. In cybersecurity, the best defense is a good (if not great) *defense*.

I mentioned earlier that I believe most employees want to help defend their organizations. They just don't know how to play their role effectively.

But let's just say I'm wrong. Let's assume, for a moment, you don't have any altruistic motives toward your company. That's not to say you wish your company harm. You wouldn't intentionally throw your employer under a bus, for example. But maybe you're the type who wouldn't stand in front of a moving vehicle for your company either.

That would put you in a category of apathetic bystander. You figure your company spends enough money on cybersecurity. They hire people to do the job of defense. If you aspired to do that line of work, you would have sought the degree and the job to do so. You didn't. You're working in another area of your company and you expect that the work of cybersecurity is (and should be) handled elsewhere. If your company does suffer a breach, assuming you're not ultimately the one found responsible for it, then it really isn't your problem. They'll pay the fines and maybe lose some customers. But life and work will go on.

If you find yourself in this category, you're not alone. In fact, in McAfee's online ethnography study of employees just like you, we heard similar sentiments offered when we asked the question:

What role do front-line workers play in maintaining cybersecurity in your organization? Do you think you play a key role or a background role?

Respondent 1: *I think I play a very small role in the cybersecurity of my company. I think it's important for me to be aware of how I can help protect the company's information, but the overall high-level security should be addressed by the higher-level employees in the company.*

Respondent 2: *More of a background role, as our IT department handles all the behind-the-scenes cybersecurity.*

Respondent 3: *I think I play a background role. The first line being the technology from our IT team, then our IT team themselves, and then the average worker.*

It seems that at least some employees think cybersecurity is better left to the tools or teams within IT, if not escalated to the higher-ups at the company. Here's the problem with both points of view.

First, there aren't enough cybersecurity personnel to throw at the problem (back to the cybersecurity talent shortage I mentioned in the previous chapter). Cybersecurity demands all hands on deck.

And second, if you think the muckety-mucks at your company are the best suited to tackle the problem, don't be so sure. Yes, the CEO and board have a responsibility to set a tone from the top that encompasses cybersecurity. But 60 percent of C-suite leaders and IT executives say the person directly responsible for information security is not a board member.[3]

It's understandable that a pass-the-buck mentality for cybersecurity is so rampant in organizations. The cybersecurity industry has coined a condition known as

"breach fatigue." It's what happens when we allow the noise of breaches in our environment to deaden our sense of urgency to respond. We either believe someone else will eventually pay the price on our behalf (even though consumers ultimately bear the brunt of breaches through higher prices) or we surrender the control we truly have over our own destiny by assuming there's nothing we can personally do about breaches to prevent them.

This book attempts to resolve the latter perspective by giving you practical steps you can take to help your company prevent a breach. That's about giving you *what* you can *do*. But if you find yourself in the former camp, let me take a moment to offer *why* you should *care*.

A few weeks ago, I received an email from someone in our HR department. She forwarded an email she had received sent to her personal email account. It appeared to come from me. It asked that she reply with instructions on how to change my automatic payroll deposit. The sender's email address came from a personal email account, presumably mine.

Luckily, her spider senses kicked in, and she forwarded the email to my work address with a simple question:

Allison, I got this email today. Can you confirm you sent it?

It didn't take me long to respond with an emphatic no. We reported the incident to our Security Operations Center (SOC). They traced the email and found that a hacker had compromised her personal email account.

I'm certain that, if I were to look up the job description of that HR employee, it wouldn't mention "cybersecurity" as

a requirement or expectation. I'm willing to bet it wouldn't contain language that demanded she be vigilant against cyber threats to employee identity as a core responsibility. Reaching out to me directly to confirm the email she received was legit wouldn't have been in this individual's "job description." Yet, that's exactly what she did, and I'm better for her sound judgment and concern. Her training stopped her from responding with copy-and-paste instructions from our intranet site explaining just how easy it is to change one's direct deposit. I marvel at my fortune that her instincts made the job of that hacker a lot harder. And she saved me indeterminate hours of frustration in attempting to reverse a bad outcome. Crisis, for me, averted.

Sometimes hackers are after more than our companies. Sometimes, they're after *us*. Our employers have a wealth of information about each of us, including our social security numbers, our bank account details (as my direct-deposit example proves), and more. The most notable breach in recent history that targeted employee records happened to the U.S. government, when its Office of Personnel Management (OPM) was compromised in a breach of more than 21.5 million records. Among the plunder collected by adversaries? Extensive background information of individuals who may not even have been current or former employees.[4]

If that's still an insufficient argument to convince you to care, how about this: the stakes of a data breach for your company have never been higher. That's thanks to regulators that are piling on to help motivate companies to protect customer data. The General Data Protection Regulation (GDPR) applies to all companies doing business or monitoring the activities of subjects in the European Union (EU).

Companies can lose up to 4 percent of annualized global revenues if found to be noncompliant with GDPR's standards for collecting and protecting customer data. In 2018, Ponemon reported the average cost of a data breach was $3.86 million—and that was largely before GDPR's enactment.[5] Any company with more than $100 million in annualized global revenues that does business in the EU can already expect to pay more—potentially considerably more, depending on its revenues—for a breach that violates GDPR.

The risks of a data breach are significant. The costs for a data breach are higher still. Don't assume your company will survive the next breach just because it may have done so in the past. Even if it does, the financial pressures may lead to other consequences, up to and including layoffs. If you're inclined to retain your existing job and see your company continue as a going concern, you must assume cybersecurity as part of your job description. Enemies love abject apathy on your part.

W.I.S.D.O.M. for the Employee

According to Verizon's 2018 Data Breach Investigations Report (DBIR), employees are directly or indirectly responsible for over a quarter of all breaches. In more than 60 percent of these cases, a careless employee is to blame. That means nearly 20 percent of all breaches are at the hands of negligent employees.[6] It's the reason employees remain among the strongest or weakest links in their company's cybersecurity defenses.

Thankfully, employees can take many steps to be a part of cybersecurity's solution, rather than its problem. First, be

alert to social engineering scams. Cybercriminals know how to exploit the trust of employees. And their methods are getting better. Spear phishing is the tactic of specifically targeting certain individuals or companies through a malicious communication, such as an email. As opposed to traditional phishing, which is more of a spray-and-pray tactic used by cybercriminals (in other words, very little, if any, targeting is in play), spear-phishing campaigns are much more effective since the criminal goes to great lengths to personalize the message.

Whaling is one such variety of spear phishing, where the adversary impersonates a high-profile executive of the company, such as the CEO or CFO, and requests action from an unsuspecting employee. For instance, a criminal masquerading as the CFO could target a rank-and-file employee in the finance department and request that he transfer company funds to an account.

Social engineering is one of the adversary's clearest weapons against naïve employees. According to Verizon's DBIR, 4 percent of people will click on any given phishing campaign. Perhaps most surprisingly, these victims aren't prone to learning from their mistakes. The more phishing emails someone has clicked, the more likely he is to do so again.[7]

Social engineering is highly effective at multiple levels of the organization. Yes, even against executives. In 2018, *Forbes* reported that nearly 80,000 firms across the U.S., UK, and Europe sent more than $12 billion to adversaries launching a highly targeted, five-year whaling campaign. Who were the employees duped into helping the adversaries fleece their companies? The companies' own CFOs. It turns out the adversaries had a targeted database of more

than 50,000 CFOs to use as their "marks" in the scam.[8] In this case, the cybercriminals used highly personalized emails, seemingly sent by the CEO, to compel the CFO to immediately complete a wire transfer. We all can learn from this expensive lesson. *Any one of us can be conned.*

So the first piece of W.I.S.D.O.M. for employees is **do not fall for the phish**. Look for the telltale signs of a malicious email such as the sender's email address. Don't click on a link from an unknown source. Instead, search for the company or go to the domain directly. But beware. Pharming sites are also popular, where cybercriminals stand up malicious websites to lure victims, then harvest their bounty be it financial or other personally identifiable information. Even by typing the domain directly, you may still land on a site with malicious intent and/or content.

Beyond not falling for the phish, **be proactive and report it to your IT or security team immediately**. According to Verizon's report, companies have 16 minutes until someone takes the bait with the first click to a phishing campaign. When does the first report come in to the security team? After 28 minutes.[9] During those mere 12 minutes, time is on the side of the adversary, and in their hands, time becomes yet another weapon through which they can inflict significant harm.

As my confession at the beginning of the chapter illustrates, social engineering doesn't have to be high-tech to be effective. Phone scams and good old-fashioned theft of carelessly unattended laptops, USBs, and mobile devices can also do the trick.

But, while old-school tactics could fit the bill, know that adversaries continue to get smarter and better through

technology to make social engineering even more effective. Artificial intelligence (AI), the stuff that makes our lives easier in so many ways (such as by our favorite search engine completing our term or phrase before we've even finished typing it), is the latest weapon in the arsenals of adversaries and defenders alike. AI promises to give adversaries even more precision in executing their phishing campaigns. They can target unsuspecting victims with more accuracy. And they can use AI to craft very personalized messages in large volumes.

The new breed of social engineering that results combines the targeted effectiveness of spear phishing with the scale of traditional phishing. In other words, phishes will be harder to spot in the future. The online world is increasingly a masquerade ball, with all the magic of wonder and dazzle the Internet promises. But the party is more crowded every hour with threats like phishing in ever craftier disguises. Your vigilance in being aware of this threat must increase over time as well.

Since adversaries are becoming more sophisticated, companies are spending more on cybersecurity than ever before. But those defenses are only useful if consistently applied and updated. You may think that the responsibility largely falls in the lap of the CISO and his department. You'd be right—up to a point. **Employees are equally responsible in ensuring those patches to laptops, mobile devices, and other personal technologies remain current.**

If your IT department pushes a patch during regular business hours that impacts your productivity for a few moments, please don't complain. Remember, cybersecurity doesn't follow the traditional rules of IT, where software patches can come and go at the leisure of the business. If

an adversary is assaulting your organization with the latest online scourge, your cybersecurity team doesn't have the luxury of sitting and waiting for a "convenient" time to push a security update to employees' devices. Time is the most coveted weapon in the adversary's arsenal. Time is certainly not on the side of your company. A little understanding and a lot of compliance on your part in accepting these security updates are most welcomed by the cybersecurity team doing its job to protect you.

Finally, there's no substitute for strong hygiene when it comes to cybersecurity defense. Sometimes the most effective measures are also the easiest to take. There's probably no better example of this than one from the healthcare industry. In the nineteenth century, Hungarian doctor Ignaz Semmelweis sought to solve a mystery. He wanted to know why so many women in maternity wards were dying of fever after childbirth. In particular, he noticed the death rate was significantly higher in wards tended by all-male doctors versus those served by all-female midwives. After lots of experimentation, including changing the position of the women during childbirth and even asking priests to avoid walking past survivors in the ward when paying respect to a recently deceased mother (lest these priests actually frighten the other mothers into a fatal fever with their very presence!), Semmelweis had his answer.

It turns out that the male doctors performed autopsies. The female midwives did not. Following an autopsy, the same male doctor may deliver a baby, in the process infecting the mother with cadaverous particles from the corpse he had dissected. Semmelweis insisted these male doctors cleanse their hands and instruments with a chlorine solution, beyond

simple soap-and-water, to completely remove any cadaver particles from their hands. He didn't have any knowledge of chlorine as a disinfectant. He just knew it would be highly effective at removing the objectionable odor associated with remnants of cadavers on physicians' hands and their instruments. While the discovery of germs was still several decades away, Semmelweis's new protocol was smart medicine, nonetheless. The death rate from childbed fever among women in the male-attended ward subsided as a result. Lucky for us, his accidental discovery paved the way for decreased mortality rates in medicine.

Even today, hand washing remains one of the most powerful tools in public health—from preventing infections in surgery to avoiding the flu. It requires discipline, for sure. But it takes only a few seconds (for the bathroom visitor) to a few minutes (for the surgical professional) to effectively inoculate ourselves from a host of bacterial and viral enemies in our environments.

Taking a page from our healthcare professionals, employees can practice commonsense hygiene to protect their companies from a wide variety of adversarial threats. Ever allow a website to automatically save passwords or use your mobile or laptop device to store them? Don't. In just one case I can give you, an employee was using her mobile device to store all her passwords, including the one for her O365 email account. A cybercriminal hacked her mobile device and stole the O365 credentials. The now-compromised credentials were used to access her O365 account, with the hacker sending phishing emails, appearing to come as legitimate emails from this employee, to a host of executives and other employees in her O365 address book. Credential

theft is particularly difficult to detect by an organization. After all, the access to the employee's O365 account looked legitimate, for all intents and purposes. It wasn't until diligent employees—the recipients of the attacker's email campaign—sounded the alarm that the threat was detected and contained.

I understand password management is difficult. Our brains weren't wired to remember hundreds of passwords across various devices, sites, and applications. To make matters worse, proper cybersecurity hygiene requires that you change those passwords regularly, making retention of them all the more difficult.

There are tools on the market such as password managers to help you generate and retrieve complex passwords. If a tool isn't desirable, you'll need to use mnemonic tricks to help your memory. Things like finding a memorable phrase (Jack and Jill went up the hill to fetch a pail of water), using the first letter of each (JaJwuthtfapow), using a combination of uppercase and lowercase letters and symbols (J@Jwuthtf@pow) and adding a number for good measure (J@Jwuth2f@pow). According to site HowSecureIsMyPassword.net, the password I just created would take a computer about *three million years* to crack.

Password management is essential to sound cybersecurity hygiene. Unfortunately, it's not practiced nearly as much as it should be. As recently as 2018 in one state, the number of government officials using "Password123" as their password was nearly 1,500.[10] Talk about making the job of a hacker even easier!

Next, be as mindful of your physical security as you are about online security. As I mentioned in the last chapter, the

worlds of physical and cyber security are increasingly converging. Not only are cybercriminals targeting physical infrastructure in their attacks (including power grids and manufacturing facilities), but compromised employee devices are an on-ramp to company systems for cybercriminals.

One of the most notable nation-state attacks in history, Stuxnet, occurred through a compromised USB device. A USB device allowed the U.S. government to stall the nuclearization of Iran by giving the former access to Iranian nuclear centrifuges. As I continue to say, a cyberattack doesn't have to rely on next-generation technologies to be effective.

So you're not the type to work in a nuclear facility? Chances are you at least have a computer you use for work. If you're like 25 percent of U.S. employees, you leave that computer on and unlocked when you go home at the end of the day.[11] That's tantamount to not washing your hands after using the restroom!

Last, but not least, use your company's virtual private network (VPN) whenever accessing or transmitting sensitive data. Public WiFi networks are cesspools for enterprising criminals. Cybersecurity hygiene in this area is weak—even among cybersecurity professionals! At the industry's largest annual event, RSA, which draws more than 40,000 cybersecurity professionals each year, self-professed hacker @Grifter801 tweeted that he had collected more than 33,500 non-encrypted passwords in roughly 26 hours of the show's debut in 2019.[12] The seductive siren song of public WiFi is a powerful force, irresistible to even the most trained cybersecurity professionals among us.

* * *

The match-up simply isn't fair. Not only is your company destined to play defense against cybercriminals, but it must do so with near-perfect precision. Attackers need only score *one* time to inflict considerable, if not irreparable harm. No investment in cybersecurity technology is any match against a combination of willful adversaries and apathetic, if not ignorant, employees co-opted to their side of the battle.

But here's the good news. A cybersecurity protocol that harnesses the power of technology, tools, and *people* working in harmony can provide an impressive defense against adversaries. That doesn't mean adversaries won't score points. In fact, it's not a matter of *if* your company has been breached, but rather if it *knows* it has. While breaches are inevitable, their damage needn't be catastrophic. When companies enlist a formidable force of educated, vigilant, and determined employees committed to their successful defense, the fight against the adversary gets that much fairer.

Notes

1. McAfee Labs Threats Report, December 2018, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf.
2. Gartner press release, "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019," August 15, 2018, https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.
3. EY Global Information Security Survey, 2018–2019, https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf.

4. Patricia Zengerle, "Millions More Americans Hit by Government Personnel Data Hack," Reuters, July 9, 2015, https://www.reuters.com/article/us-cybersecurity-usa/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M420150709.
5. Ponemon, "2018 Cost of a Data Breach Study: Global Overview," July 2018.
6. Verizon, "2018 Data Breach Investigations Report," https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf.
7. Verizon, "2018 Data Breach Investigations Report."
8. Dante Disparte, "Whaling Wars: A $12 Billion Financial Dragnet Targeting CFOs," *Forbes*, December 6, 2018, https://www.forbes.com/sites/dantedisparte/2018/12/06/whaling-wars-a-12-billion-financial-dragnet-targeting-cfos/#59a7bc3b7e52.
9. Verizon, "2018 Data Breach Investigations Report."
10. Taylor Telford, "1,464 Western Australian Government Officials Used 'Password123' as Their Password. Cool, Cool.," *The Washington Post*, August 22, 2018, https://www.washingtonpost.com/technology/2018/08/22/western-australian-government-officials-used-password-their-password-cool-cool/?utm_term=.d28180e988e7.
11. https://www.techrepublic.com/article/over-40-of-reported-security-breaches-are-caused-by-employee-negligence/
12. https://twitter.com/Grifter801/status/1103007628244869121.

CHAPTER

4

Stop the Line

Cybersecurity is viewed as a critical defensive effort for our business. If you think about what we do and what we provide—water—in the event of something compromising our systems and if our customers lose faith in our ability to provide good, clean, safe drinking water, it's catastrophic.

CEO, Utilities Company

The year was 2017. We saw the beginnings of an investigation of suspected tampering by Russians in the U.S. presidential election. We witnessed the rise of the #MeToo movement and the subsequent fall of entertainment and business tycoons crushed under its weight. We endured catastrophic losses,

courtesy of Mother Nature's wrath, with some of the most devastating hurricanes in recent history, including Harvey, Irma, and Maria.

Amid all this turmoil that seemed to characterize 2017, we lost a luminary whose contributions to business will remain with us long into the foreseeable future. Tatsuro Toyoda, son of the founder of the Japanese automotive company Toyota, passed away quietly and without much media fanfare on December 30. He was 88 years old.

You're more than likely familiar with auto giant Toyota. But you may not realize how profoundly one of its forefathers, Toyoda-san, influenced the way you and I do business today.

To understand Toyoda's impact, we must go back to a different era—the early 1980s—when he took the reins of his company's first American factory. At the time, American auto manufacturers dominated in market share. General Motors (GM) was far and away the world's largest car company. Despite its success, it had a challenge: the U.S. government's emission guidelines forced auto companies to produce small, fuel-efficient cars, and GM had historically struggled in doing so. At the same time, there was a disturbing trend emerging in the U.S. auto market overall. Japanese car companies were starting to grab market share fast—so much so that the U.S. Congress was threatening to restrict auto imports.

This strange confluence of real and potential U.S. regulations—one that forced GM to produce small, fuel-efficient cars and another that threatened to limit Toyota's car imports—created the unlikeliest of unions. Toyota and GM, fierce competitors in the market, became partners of sorts.

The two companies teamed up to open a joint plant in Fremont, CA, home to a former GM production facility.

Each competitor got value from the interesting arrangement. Toyota would build GM a quality fuel-efficient small car that would finally turn a profit. In the process, GM would gain access to Toyota's manufacturing principles—literally peeking in the cupboard to discover its competitor's secret sauce. In turn, Toyota would learn to build cars in the United States and mitigate the risk of future car import restrictions.

Now, about that former GM plant in Fremont. If this "partnership" between two rivals wasn't weird enough, the location they chose to set up shop bordered on the bizarre. The former GM plant in Fremont was an unmitigated disaster. Bruce Lee, who ran the western region for the United Auto Workers union at the time, called the Fremont employees "the worst workforce in the automobile industry in the United States."[1] Their behavior was infamous in the industry—from record absenteeism to lewd acts on the factory floor to sabotaging cars for the chance to earn overtime to fix them. If conduct was any indicator, these employees hated their jobs and their employer.

You may not find GM and Toyota's decision to establish their new joint operation in a manufacturing facility that had bad history as unusual. After all, why throw a baby out with the bathwater? The physical plant may have been completely acceptable. But the labor force needed changing—badly.

But GM and Toyota didn't change the employees. In fact, they hired 85 percent of that former Fremont workforce (described as the worst in America by one of their

own union leaders) to tackle the challenge of producing a profitable and high-quality fuel-efficient automobile—something GM hadn't accomplished in the *best* of its U.S. plants.

Perhaps even more surprising, they flew some of those former Fremont employees to Japan to learn how to build cars the Japanese way. The first car, a yellow Chevrolet Nova, rolled off the assembly line in December of 1984. Almost right away, the Fremont plant was producing cars at the same speed and with as few defects per 100 vehicles as those produced in Japan.

What exactly was it that allowed Toyota to produce the first quality small car for GM using virtually the same workforce that was so subpar under the GM regime? It wasn't a secret sauce as much as it was a secret ingredient: continuous improvement.

GM adopted its philosophy from Henry Ford. Factories were highly departmentalized, division of labor was the standard, and efficiency was king. If we had to sum up the GM culture with a bumper sticker slogan, it might be simply "Never stop the line." In fact, those four words were a cardinal rule in the former GM plant. No matter what, the assembly line could never stop.

An interesting mandate, since so few workers showed up on some mornings that the production line couldn't even *start*. On those days, GM would bring in people off the street to fill the void. And when the production line finally started, it didn't stop.

Billy Haggerty worked in hood and fender assembly. Rick Madrid built Chevy trucks for the plant. Along with Bruce Lee, they were interviewed by NPR to give the rest of

us a glimpse into just how strictly that golden rule was practiced at the former GM Fremont plant.

> Haggerty: *The line could never stop, never stop the line.*
> Madrid: *You just don't see the line stop. I saw a guy fall in the pit and they didn't stop the line.*
> Lee: *You saw a problem, you stop the line, you are fired.*[2]

Workers would deal with defects after the fact. For GM, it was about quantity over quality.

Toyota built its philosophy on continuous improvement. Not only were employees *allowed* to stop the line, but Toyota *encouraged* them to do so. The "andon cord" was within reach above the head of every worker on the line. (Andon comes from the Japanese word for paper lantern. Accordingly, workers could visually signal whether things on the line were just fine—green light; whether production quality was at risk—yellow; or whether a decline in quality meant it was imperative to stop the line—a red light.)

Toyota wasn't just building cars; they were building a process—one that welcomed good ideas from any level of the company. One that relentlessly pursued and obliterated every inefficiency. One that persisted to set the bar higher and higher.

This "Stop the Line" philosophy empowered every employee to be a plant manager of sorts and made quality an inherent part of everyone's job responsibility. Toyoda brought the Japanese philosophy to U.S. auto workers. When the White House Automotive Task Force assessed GM decades later in 2009 during the latter's Chapter 11 bankruptcy, it

publicly acknowledged GM's global production and procurement system, modeled on Toyota's, as world-class and every bit as efficient as its Japanese teacher's.[3] As Toyoda was the leader of Toyota's venture into Fremont, GM owes much of their tutelage to the late visionary himself.

But Toyoda's impacts extend far beyond GM or even to the automotive industry. At around the same time as the Fremont plant's success in the 1980s, the Total Quality Management (TQM) movement gained traction across multiple industries—where continuous improvement was the new face of management and quality the prize.

TQM eventually gave way to other movements like ISO 9000, Six Sigma, and lean manufacturing. While the standards and the names may have changed, the guiding principle didn't. Quality was no longer a *nice-to-have*; it was *essential* to a company's long-term success.

Security, as an endeavor, is similar to where quality was before we all caught TQM fever. When designing products and processes, we tend to think of security as tomorrow's problem. It's something we'll get around to after a product exits the line. We'll fix it after the fact. In many ways, security is an aftermarket afterthought. And that thinking must change if we are to embed security in everything we deliver.

If not, the results could be catastrophic.

The Internet of Terrorism

The year was 2016. You may not realize it, but a war occurred on October 21 of that year. It lasted only a day, but it will go down in infamy in the annals of cybersecurity. Because that's

when the Internet's ramparts were breached by marauders intent on chaos at a scale not previously seen. It was the day the Internet broke.

The events of October 21, 2016, prove that truth can be stranger than fiction. What was unusual about that day was not that hackers deliberately set their sights on a company to inflict damage. That kind of headline news has become all too commonplace in our digital world. What was unique about the attack was the company that found itself in hackers' crosshairs: Dyn.

While you may not have heard of Dyn in 2016, you undoubtedly used the services they enabled: Twitter, Netflix, Spotify, and Etsy, to name just a few. Among other things, Dyn was a domain name system (DNS) provider. When you entered a website address for one of these popular services, Dyn mapped it to its corresponding IP location.

On that fateful October day, hackers crippled Dyn with a distributed denial of service (DDoS) attack. DDoS attacks are a perennial favorite scourge among hackers. They occur when hackers flood a website with excessive traffic to effectively bring it to its knees. Our Internet is comprised of multiple routes and destinations, not unlike an intricate highway system. When enemies target a website, they can launch a DDoS attack to congest it to the point of failure. While DDoS assaults are among hackers' more popular threat varieties, there were two notable exceptions to the Dyn attack that made it categorically special.

First, most DDoS threats target a particular company. In fact, there are companies in certain industries more susceptible to these pernicious launches than others. Take online gaming, one of the more popular industries targeted for

DDoS assaults. If you're an online gamer, you likely know why. Many online games are of the "high-twitch" variety, meaning they rely on a player's fast reaction time for victory to ensue. If a hacker can congest the virtual highways that connect online players to their shared experience, response times slow to a grinding halt, making it impossible for you to shoot your opponent before he can fire a bullet in your direction, as an example. Though uniquely harmful to online gaming outfits, DDoS attacks can wreak havoc for any company with a digital presence. By flooding a website with garbage traffic, hackers can deny legitimate visitors access.

But the Dyn attack was distinct. It took out multiple websites with one hit. By congesting Dyn's DNS service—the metaphorical equivalent of the postal address system on the web—hackers blocked entry to several popular sites. In one fell swoop, an entire region of the United States found some of the most popular web services unavailable as the Internet backbone itself gave way. If you imagine our nation's participation on the Internet as a nighttime view from space, on that fateful October day, the Eastern seaboard simply disappeared. In our hypothetical view from on high, tens of millions of people and the digital infrastructure they rely on was swallowed up by darkness to apparently join the Atlantic Ocean's vast expanse. Hackers effectively erased the digital existence of one of the most powerful corridors of power on our planet.

The Dyn attack was unique in another way. DDoS attacks require enormous scale to execute. The typical website won't be buckled by a few hundred or even a thousand motivated hackers each pinging it at the same time. It would require millions of attempts to deliver a crushing blow.

This is where another cybersecurity term that has made its way into the lexicon—a botnet—comes into play. In laymen's terms, a botnet is comprised of a network of devices enslaved by a hacker. The zombie army that results is under the command and control of one or more bad actors, who commandeer the drones to do any number of actions, including launching a distributed denial of service attack by flooding a website with requests. How do these botnets come under the control of their evil overlords? It happens through malicious software deposited on computers when users visit an infected site or download a contaminated message. In many cases, users are unaware their device has even been seized.

You might wonder how exactly the DDoS attack on Dyn was so different. The botnet employed was not an army of computers, or even mobile devices, which as you might expect are common soldiers for a hacker's zombie legion. Instead, cybercriminals compromised ordinary connected household devices. Baby monitors, security cameras, and digital video recorders (DVRs) were among the recruits in the botnet that took down Dyn. Hackers exploited weak factory-default passwords in these connected devices to seize control. No user had to first unknowingly download malicious software. In this case, consumers did nothing to compromise their own devices. As it turns out, nothing is exactly what fit the bill, since users also didn't think to change their devices' default passwords, assuming the average user would know how to do so in the first place.

Within a moment of the Dyn network's collapse, the Internet of Things (IoT) became the Internet of Terrorism. And, lest you believe that the Dyn attack was a fluke, contemplate

one more frightening reality: The botnet that disabled Dyn was actively recruiting enrollees for its next attack several months *after* the incident. In an always-on world, hackers have billions of connected devices at their mercy, simply awaiting their next command from their new leader.

The Dyn DDoS attack opened our eyes to a new reality: *The targets have become the weapons.* What we used to protect, we must now be protected against. Just as data can be manipulated to deceive us, those harmless connected devices that make our lives convenient in so many ways at home and work can be turned against us to cripple the digital infrastructure upon which we (and they) rely. Cyber threats are now so pervasive that they lurk around every connected device, every bit of data we take for granted.

The Dyn attack proved that innovative hackers can exploit any connected product or service in their next attack. When cybercriminals slithered in through ordinary household appliances, cybersecurity slipped into the mainstream of product development.

Take connected cars, as just one example. In 2017, Toyota, Intel, and others formed the Automotive Edge Computing Consortium. The group estimated that the data volume between vehicles and the cloud will reach 10 exabytes per month around 2025—a projected 10,000-fold increase from 2017's baseline. That's the equivalent to *twice* the volume of all words ever spoken by humans since the dawn of time.[4]

Weaponizing the IoT to take down the Internet is one thing. Weaponizing the eight million autonomous cars expected to be on roads by 2025[5] makes the Internet of Terrorism that much scarier. Those connected vehicles will depend on accurate, real-time data to assess their

surroundings and navigate accordingly. They will rely on the 10 exabytes of data per month flowing between them and the cloud—data that will be a veritable treasure trove for hackers less motivated by profit than terror.

If you think your company doesn't have to worry about such concerns since it's not in the business of Internet backbones or connected cars, adversaries welcome your indifference on this topic. But Dyn shows that your company can simply be caught in a hacker's crossfire. Dyn wasn't the target of the attack. The Internet services they supported were.

If that still doesn't compel you to think differently of the brave new world in which we find ourselves, consider this: How many of your employees work from home on an occasional basis? Now consider that the average home had 10 connected devices in 2016, the year of the Dyn attack, per Intel. The semiconductor giant predicted at the time that figure would rise to 50 connected devices per household by 2020.[6] If left unsecure, those devices can serve as the potential onramp for hackers to compromise your employees while working from their home offices—and potentially seep into your company as a result. The edge of the corporate network is now in the home.

Lines are blurring. Home and work are colliding. The products and services we use as consumers, we use as employees. The IoT is just one example of how cybersecurity permeates more than what meets the eye. For any employee charged with product or service development, *you are key to stopping the line* whenever cybersecurity is conspicuous by its absence.

In this case, it's not just your company depending on you for the same. It's *every user* directly or indirectly touched by your creation.

W.I.S.D.O.M. for the Product Developer

Product developers are the first line of defense in embedding cybersecurity requirements in every product or service a company offers. There's no need to reinvent the wheel on sound product development principles and checklists (of which there is no shortage in the market). By integrating cybersecurity concepts into tried-and-true design methodologies, developers play an essential role in hardening their companies'—and even their users'—cybersecurity defenses.

First, in the initial phases of design, customer input is imperative. Many companies actively solicit this feedback from customers through quantitative research, one-on-one interviews, customer advisory councils, and/or other methods. A simple, but profound, way to ensure cybersecurity is not an aftermarket afterthought is to straightforwardly **ask customers about their cybersecurity requirements as part of this discovery phase**.

Let's say you're in the business of manufacturing a [fill-in-the-blank] connected household device (like the kind used in the drone army to take down Dyn). Discovering when consumers would be more likely to take action in changing a factory-default password would be an important element in the design phase. Better yet, eliminating procrastination from the consumer during this phase by, say, requiring a password change through an intuitive application when the connected device is installed removes a key security vulnerability right out of the box.

Now let's imagine you're in software development. And let's assume that consumers aren't your target. You market to businesses. The same principle applies. In this case, finding out exactly how your customer will use your application securely prevents the need for bug-fixing down the road.

Will your clients rely on the cloud, or do they prohibit the cloud for data upon which your application depends? On the flip side, have you designed a product to live within a firewall only to find your customer prefers a software-as-a-service (SaaS) consumption model? These and many other qualifying questions during the discovery stage are invaluable to implanting security in the foundation of your product.

Since we're on the topic of software developers, here's another one for you. Make sure security is part of any minimum viable product (MVP). When Eric Ries, author of *The Lean Startup*, popularized MVP, he captured the essence of what any startup endeavors to do: launch a new product that allows a development team to collect the maximum information on customer usage and acceptance with the least amount of effort. The process lends itself well to cloud-based applications that have very few upfront capital requirements (since many leverage public cloud infrastructure offered by AWS, Azure, and Google). Essentially, it allows for quick learning, fast iterations in product development, and a continuous feedback loop with customers. All good stuff—especially if it lets a start-up (or any company) avoid the costly mistake of launching a software product that fizzles in the market.

Here's the thing: Do not focus your attention so much on the word "minimum" in the moniker that you ignore the one right after it, "viable." **Security must be built in, not bolted on**, whether for a product intended only for the early adopter or for the mass market. Security *must* be part of your minimum viable product requirements.

Next, when designing the product, be deliberate about how, where, and for what amount of time your company will use customer data. There are regulations that will force your company to care about such matters, assuming it needs the

extra motivation. So what I'm talking about here are not the mandated requirements issued by regulatory authorities. Instead, I'm referring to the ethical standards to which your company will hold itself accountable. To be clear, the higher of the two bars—the legal requirement or your company's ethical principle—is the waterline on this test.

For example, in the first chapter, I discussed a hacker's defacement to McAfee's company page on a popular social media platform. While there was no customer data in play with our event, it will help me paint the picture of what I mean on this point. Since there was no data stolen or any McAfee system compromised, McAfee was under no legal obligation to report the hack at all, let alone alert the media.

But McAfee holds itself to a higher standard than the legal requirement. In this case, the social media pages of our employees were also defaced, along with McAfee's company profile page, when the hacker exchanged our logo for a graphic image. That image showed up for several hours on the personal page for any employee who had McAfee listed on his profile. McAfee has a company value we uphold with employees: *We practice inclusive candor and transparency*. While the legal limit did not require any reporting on our part, our own company value demanded more.

So the day after the hack occurred, we published a front-page intranet story admitting the same to all employees. We knew the risk was that a story that had not received any real media attention (given the attack occurred on an otherwise quiet Easter Sunday) could ignite on a Monday morning should *just one* employee send it to the media. Thankfully, that didn't happen. In the end, it was a risk we had to take if we were to uphold a company value that exceeded our legal requirement.

So **define your data requirements clearly and consciously in the design of any new product or service**—upholding the higher of either legal requirement or ethical standard. I'll give you one more example to put a finer point on it. To date, one of the only U.S. regulators to issue explicit guidance on reporting a ransomware attack is the Department of Health and Human Services (this instance of regulatory guidance is an important step forward, especially considering that healthcare is a frequent target of ransomware; but, given that it stands in exceptional company, it's also representative of why ransomware is likely much worse than the actual reported industry figures would have you believe). If your company has a similar value of transparency with customers and would require disclosure of a ransomware attack, then you will likely have a different point of view on how much risk you want to take in storing customer data, even if the law may be more permissive in this regard (that is, until the U.S. and other countries take the EU's lead and revisit guidance associated with customer privacy).

Next, build security ownership into each phase of the product lifecycle. How will your product or service be upgraded to address the next threat vector? What department is accountable for ongoing maintenance and patching? Who is accountable for handling incidents after a breach occurs? Where will budgets sit? You get the idea. Be explicit about swim lanes across the company and where and when security decisions must be made and resources allocated.

The effort required to introduce a product can be simple when compared against that needed to maintain it. It's only after the first customers adopt your creation that the inevitable issues of support, scalability, and—yes—security rear their ugly heads. By then, the warm-and-fuzzy feelings

of your triumphant launch will be distant memories. Having clear ownership for these certainties established upfront, before your product ever reaches its first customer or user, will save time and mitigate risk down the road.

It's no different from the discipline you likely already practice when contemplating other key issues in the product lifecycle. In addition to signing off that support and scalability concerns have been planned for, the highest functional leader in the company for each department (such as customer support, engineering, or marketing) should also explicitly review and approve that the security requirements for her function have been sufficiently built into the product before it is introduced to market.

Last, but certainly not least, you must **stop the line** should security be lacking or missing at any part of the product launch process. More importantly, you should actively encourage this stop-the-line philosophy for *any* employee engaged directly or indirectly in the development process. This is never easy to execute since time is money in business. But it's harder still for companies that don't have all workers concentrated in one physical location (like that Toyota plant in Fremont, with tangible cues in its environment, including the universal colors of red, yellow, or green that immediately and unmistakably communicated the current state of quality to all plant employees). Likewise, many companies don't have a pull cord or button that employees can activate to immediately stop a line. There's no physical production line where software is concerned, for example.

In fact, if you're like me, you work for an employer with a hybrid and distributed environment of company locations and remote employees. So you'll need to be resourceful in

using the virtual tools at your disposal to communicate when an employee has stopped the line. Companies are accustomed to lots of fanfare upon a product's successful launch. It's only natural to applaud such a milestone. While not losing a celebratory culture upon a product's release, consider practicing the same level of recognition when an employee stops the production line due to a security flaw.

Employees notice reward and recognition in companies. It's one part of the culture that is highly visible and clearly communicates what is (and is not) important to senior leadership. When an employee stops the line, find a way to reward her. Then publicly recognize her through any communication vehicle most leveraged by your company (here's where your HR and marketing colleagues can help you). The point is that you want employees to know that your company takes security as seriously as it does quality. When they see for themselves how you've changed your reward-and-recognition system acknowledging that, you'll find more diligent employees speaking up when security is falling down. And you'll save your company from potential financial, reputational, or intellectual property losses down the road.

* * *

Companies have come a long way from the cavalier, haphazard mentality once given to product quality. Educated buyers can easily check a company's quality track record before making a commitment they may regret. Today, companies know the value of a quality experience. They measure it in customer satisfaction, net promoter scores, and retention. They compete for it in customer awards. And they see the value of it in their financial results.

Cybersecurity is the quality of our generation. Like quality before it, it's underestimated, underappreciated, or simply unmeasured. A good friend of mine often says, "What's bred in the bones will come out in the flesh." A company with strong cybersecurity marrow in its bones stands to benefit in less risk, fewer financial losses, more customer trust, and, yes, higher quality thanks to products inherently designed and built with *both* cybersecurity and quality in mind. As the dreamers and designers of tomorrow's products, developers have an essential role to play in embedding cybersecurity in everything we consume.

Notes

1. NPR, "The End of the Line for GM-Toyota Joint Venture," March 26, 2010, https://www.npr.org/templates/transcript/transcript.php?storyId=125229157.
2. Ibid.
3. David Kiley, "Goodbye, NUMMI: How a Plant Changed the Culture of Car-Making," *Popular Mechanics*, April 2, 2010, https://www.popularmechanics.com/cars/a5514/4350856/.
4. Verlyn Klinkenborg, "Editorial Observer; Trying to Measure the Amount of Information That Humans Create," *The New York Times*, November 12, 2003, https://www.nytimes.com/2003/11/12/opinion/editorial-observer-trying-measure-amount-information-that-humans-create.html.
5. Bret Kenwell, "This Is How Many Autonomous Cars Will Be on the Road in 2025," TheStreet.com, April 23, 2018, https://www.thestreet.com/technology/this-many-autonomous-cars-will-be-on-the-road-in-2025-14564388.
6. Shilipa Phadnis, "Households Have 10 Connected Devices Now, Will Rise to 50 by 2020," ETCIO.com, August 19, 2016, https://cio.economictimes.indiatimes.com/news/internet-of-things/households-have-10-connected-devices-now-will-rise-to-50-by-2020/53765773.

CHAPTER

5

Bridging the Gap

I think the risks are really attracting the top talent, retaining the top talent, making sure that there is continued funding to invest in cybersecurity on the programs where we will need to prioritize and then processes that need to be improved. Overall, you can't stop what's going on outside of your organization. You can't stop the bad things. You have to just prepare how to respond to them so the biggest risk is not doing anything. That would be detrimental. But, as long as you have a good security program, you're able to retain the talent and work towards fulfilling some of the gaps and holes that you have, you should be okay.

CIO, Healthcare Provider

Walk into any major McAfee campus around the world and you'll see a common fixture. It's not the usual

amenity you might expect to find in modernized workplaces, like a gym or friendly dogs at work (though we also have plenty of those!). It's a…wall.

Since the public discourse is replete with talks of walls at the moment, let me explain. Like many companies, McAfee has a vision, mission, and values. Our vision reflects our aspiration for our industry and world. Our mission guides strategy. Our values express behaviors for the company we are. Those important cultural pillars are likely not that different from what your employer espouses.

But what sets us apart from many companies is that we also have a pledge. While our vision, mission, and values reflect our ambition, thinking, and conduct, respectively, our pledge reminds us of our calling:

> We dedicate ourselves to keeping the world safe from cyber threats.
>
> Threats that are no longer limited to the confines of our computers, but are prevalent in every aspect of our connected world.
>
> We will not rest in our quest to protect the safety of our families, our communities, and our nations.

You'll find these words prominently displayed on pledge walls in every major McAfee location around the world. In addition to the pledge, our walls commemorate the signatures from thousands of McAfee employees volunteering themselves to uphold that pledge. For the rest of employees in more remote facilities, including our work-at-home population, chances are they electronically signed this pledge upon joining our company.

The pledge is central to why McAfee does what we do. We're in the business of cybersecurity. So it's only natural that security is the lifeblood of our company. Even so, we're not immune from adversaries intent on doing us harm. No company is.

But how does your company, one that is likely not in the core business of cybersecurity, develop a culture that embeds security into the fabric of your organization? While I don't envision pledge walls featuring employees committed to keeping the world safe in your future, there are plenty of areas where your company can focus to make cybersecurity a meaningful component of your culture.

Chances are your company and culture could benefit from a healthy dose of cybersecurity. There's no doubt that the ongoing cybersecurity battle between the good guys and bad guys can tilt in favor of the former when more companies adopt cultures of security.

Since our HR professionals are the experts among us who have devoted their careers to organizational health and are the champions behind the cultures sustaining it, I'm dedicating this chapter to them. While they are not exclusively responsible for company culture, they have more sway over it than just about any other party, except for the CEO. They inspire the rest of us by creating environments that attract and retain exceptional talent, something I've witnessed firsthand at McAfee in how a visionary CHRO can spread influence and impact far beyond her reach. And they have much more to offer in being part of the cybersecurity solution than they might think.

When Too Much of a Good Thing Is Bad

Before I joined the ranks of cybersecurity, I spent much of my career in telecommunications. I was part of the wild ride that was the dot-com boom of the late nineties. I remember when just about everyone I knew was off to found or join the next dot-com start-up. It seemed that all were destined for success. I remember those of us fortunate enough to work in the industry at the time gloating that we were part of the modern-day gold rush. I was in the right place, at the right time. There were more job offers coming my way than I could shake a stick at. Life was good.

Until it wasn't. The dot-com bust at the turn of the century shattered dreams and careers. Unemployment soared overnight. The struggle was very real for many of my friends who traded their equity that wasn't worth the paper on which it was printed for a pink slip worth even less.

It took several years and multiple rounds of layoffs for a tumultuous telecom industry to eventually equilibrate. But equilibrate it slowly did. And the virtually nonexistent telecom unemployment rate at the dawn of the millennium is now a reminder to those of us who endured that journey and have the scars to show for it, of how too much of a good thing can be very bad indeed.

Fast-forward in my career nearly 15 years later when I entered McAfee and the cybersecurity industry. Of course, I knew that McAfee was in the business of security. It was a calling I shared. I wanted to do something meaningful with the 60-plus hours per week I invest in my career. Saving lives seemed about as good as it got.

So good, in fact, that I soon learned that we couldn't hire people fast enough. The global talent shortage in the industry took me back to the days of that practically nonexistent unemployment rate from an era gone by. While candidates in cybersecurity roles may relish the idea of perpetual job security, the reality is that the consequences of a zero-percent unemployment rate in this industry are even worse than what I experienced so long ago.

The reason is that there is so much more at stake. Back in the day, filling jobs for the latest dot-com boom wasn't likely a matter of life or death. Some enterprising start-ups may have found it more difficult to attract and retain talent for their latest ventures, but let's be real. What was really at stake?

Perhaps we'd have to wait a few more years for the Internet's potential to catch up to its hype; for the app economy we know and love today to materialize. Those early grocery or pet supply delivery services would see a few false starts. Lucky for us, there were plenty of viable options through which to procure such goods, even while we waited for e-commerce at our fingertips to deliver virtually anything to us in days (if not hours). The dot-com boom and subsequent bust are now but distant memories for most of us. We survived to tell the tale.

Cybersecurity is different. There's more than network bandwidth or cool applications at stake. A lot more. We have national security to consider. Companies have intellectual property, finances, reputation, and more to protect. All the while, we struggle to fill jobs for those who defend us.

Unlike in the telecom industry, this talent shortage isn't likely to be solved by some industry bust. We're not likely to see

unemployment rates skyrocket with a glut of talented cybersecurity professionals entering the market. That's because our enemy won't have it that way. Adversaries continue to recruit to their ranks. As long as there is no shortage of bad actors, there will be no surplus of cybersecurity professionals.

This is the nature of our beast. Cybersecurity vendors poach talent from one another, since it's easier to pay more for someone already schooled in the industry than to attempt to recruit from a virtually bankrupt pipeline of candidates. The private sector finds itself in the same revolving door of talent. And the public sector, typically with the most to defend (our national security!) is left to compete in this hotly contested labor market with the toughest constraints on compensation.

The demand for cybersecurity professionals far exceeds its supply. And that gap affects all of us.

To make matters worse, we have a dearth of diversity in the talent pool. Women and minorities are woefully underrepresented. Even if you're not one who sees the goodness in having a diverse workforce, this problem transcends political or ideological principles. The unfortunate reality is that we don't have enough qualified candidates in the labor market or pipeline, and that's a problem that requires *all* the help we can get. A gender or minority gap works against all of us by greatly diminishing our addressable market for cybersecurity talent.

It Wasn't Always This Way

It's tempting to think this problem is too big to solve. It's easier to kick the can down the road than put the work in today to address the cybersecurity talent shortage. It's particularly understandable when considering what we're up against:

- Millions of cybersecurity jobs globally will go unfilled over the next several years.
- Depending on the source, women make up anywhere from 11 to 20 percent of the cybersecurity workforce.[1] Even if we take the higher percentage, it's a representation far lower than in the general labor market, where women represent half the workforce.
- For minorities, the statistics are even worse. They make up only 5 percent of cybersecurity professionals[2] compared with approximately one-third of employed Americans overall.

Perhaps the problem isn't solvable? Maybe women and minorities simply aren't inclined to pursue jobs in cybersecurity? Or perhaps they're just not cut out to do the work? Could it be that the cybersecurity industry is doomed to lack diversity and its inherent benefits?

Not if its origins are any indicator of its destiny. The original software programmer was a woman. Ada Lovelace is widely credited with writing the first computer program in history—an algorithm that would calculate the Bernoulli sequence, which, among other things, explains why an airplane's wings take flight.

In the mainframe era that dawned in the 1940s, it was women, once again, who programmed the machines. Men were more interested in building these behemoth computers, leaving the meticulous coding to their female counterparts.

During World War II, women comprised 75 percent of the Bletchley Park code-breaking operation[3] that helped break the Enigma code of the Germans.

After the war, women remained foundational to coding in the private sector. A woman, Grace Hopper, created the

first compiler, something that translated English-friendly code into the bits and bytes understandable by a computer.

As programming jobs exploded in the 1950s and 1960s, women were a mainstay in the labor force. The field was a meritocracy, based on aptitude and achievement. Companies often selected programmers based on an admissions test, one that typically involved pattern recognition. Women and men were on an equal playing field.

What changed?

Perhaps the more important question is: What *didn't* change? Women didn't suddenly lose their propensity to apply math or science skills to their work. And companies didn't decide overnight that men were more capable than women of fulfilling the responsibilities required of a programmer.

As this history lesson would reveal, sometimes technology can impede progress on one front to accelerate it on another. Specifically, when the first personal computers entered households in 1984, we could hardly have imagined their impact decades later. On one end, personal computing made possible the digital age in which we find ourselves today. On the other, it unintentionally disenfranchised women and minorities from the pursuit of programming roles, including cybersecurity jobs, that are in such high demand.[4]

You see, when personal computers entered the market, their price points favored more affluent households, as is the case with many new technologies. That reality disadvantaged minority households, which earned, on average, less than their nonminority counterparts.

Within a few years, universities began to be flooded with applicants who wanted to pursue a career in programming—now a hot market with a bright future thanks, in large part, to the

advent of personal computing. Economic powers of supply and demand took hold. Universities couldn't fulfill the demand for all candidates wanting a career in computer sciences, including women and minorities. They began ratcheting up the requirements for such degrees, particularly in the crucial first year of study, to weed out candidates without a perceived penchant for the skills required (typically by accelerating the curriculum that would otherwise be found later in a candidate's studies).

The fast-tracked curriculum favored those with the prior experience of banging on a keyboard, learning the inner workings of a computer. In other words, candidates coming from PC households—white males.

But what about white females within these households? Why would a little girl's interest in computers be less than her brother's when she had access to the same technology?

Think back to the mid-to-late 1980s and the teenage culture splashed on Hollywood's big screen. You'll remember pop-culture classics like *Revenge of the Nerds*, *Weird Science*, and *WarGames*. The protagonists that emerged from these box-office hits? Hollywood's stereotype of a lovable nerd—a white male nerd, to be exact.

Computers, and the programming language that controlled them, became a guy's trade.[5] Teenage girls, like me at the time, no longer visualized ourselves in these careers since it seemed they were tailor-made for males. There's a saying that strikes a chord with me as a woman, "If she can't *see* her, she can't *be* her." And the female archetype who happened to kick butt in programming—one resembling Ada Lovelace, Grace Hopper, and the Bletchley Park women—was conspicuous by her absence in just about every blockbuster movie that glorified computing at the time.

I give you that brief history lesson not to assign blame in any one direction. To be clear, I couldn't be more grateful that I have a computer through which to write this book. I couldn't be more appreciative that we have talented programmers—both male and female—who make possible many of the innovations I enjoy today. I happen to be a fan of those 1980s movies that moved computers into our pop culture. And I take absolutely nothing away from the countless innovators—men and women alike—who paved the way for the future we have seized.

I simply want to expand our addressable market for cybersecurity talent because the cybersecurity talent shortage is yet one more threat we face. Another menace to our digital freedom is certainly something we can all do without.

Those who do not learn from history are doomed to repeat it. There is much we can glean from this history lesson to change our trajectory going forward and move above a zero-percent cybersecurity unemployment rate (a strange ambition to *want* unemployment in cybersecurity, I realize, but I hope I've made the point that a bit of a labor surplus beats the seemingly endless talent shortage in which we find ourselves). As the recruiters for our companies, HR professionals have a significant role to play in helping their companies—and the cybersecurity industry—bridge the gap.

W.I.S.D.O.M. for HR Professionals

We must accept two realities. First, our pipeline of existing cybersecurity talent is desperately lacking, and that problem isn't going to change anytime soon. Second, because there aren't

enough candidates in the pipeline to fill the cybersecurity jobs we currently have, we need every employee to take up arms in the battle, doing her part to strengthen her company's defenses.

The two-sided coin—recruitment and enlistment—becomes a call-to-arms for HR professionals. On the recruitment front, HR can help their organizations **expand the aperture for cybersecurity talent**. This isn't a case where bias can win. We need all talent helping in the fight—men and women, minorities and non-minorities, arts and sciences. To this last point, our industry has been so focused on STEM (science, technology, engineering, and math) that we've lost STEAM (science, technology, engineering, arts, and math). Cybersecurity is as much a psychological battle as it is a technical one (combat lends itself to both). It entails both soft and hard skills. It exercises creativity as much as it does problem solving.

Review your cybersecurity job postings and look for a balance of skills that widen the market of applicants. Doing so will not compromise the quality of candidates (this isn't about lowering standards). Look to the history of women in this field, back when complex math was computed in a human's brain, not a machine, and you'll realize that women are equally as capable of fulfilling the roles as men. You may simply need to look for the same unconscious bias that had universities weeding out diverse talent in the late 1980s in your company's own cybersecurity job descriptions. When you find it, *weed it out* relentlessly.

But that's still not sufficient. You'll need to do the same throughout your recruitment process. That includes the interview. Unfortunately, questions that are everyday fare in many interviews are also a source of unconscious bias. For

instance, behavioral interview questions that are commonplace (such as, "Tell me about a time when…") naturally favor candidates with more history. However, that history may or may not be relevant to today's challenges. In fact, research suggests such questions predict success only 12 percent better than a coin flip.[6]

Instead, give the candidate a problem and ask her how she would solve it. You may ask the candidate to walk you through her plan for acclimating herself to your culture and company upon hire. You might show her a flowchart of your current process and ask her to make suggestions for improvement. The point is that you want to see how a candidate thinks, not simply have her regurgitate her past.

In the interview process, use panels of interviewers to identify the most qualified candidates. Here is another case where too much of a good thing can be bad. For example, Google has its Rule of Four, in which they have successfully modeled that four interviews are sufficient to predict a new Googler's success with 86 percent confidence.[7] Any more is overkill. Any less, insufficient.

No matter your company's ideal number, make sure at least one interviewer on your panel is a diverse leader. Men and women answer questions differently. Having both on your interview panel will account for these differences.

Taking another lesson from Google, they also have an interesting interview question for which they grade men and women differently. It's this: "On a scale of 1 to 5, rate yourself as a software engineer."

Their evidence suggests the most successful male Googlers answered "4" when asked this interview question. Google finds that men tend to inflate their experience or

qualifications. The score most likely to predict success for female candidates? A perfect 5, as Google finds women are more likely to be reserved and humble.[8] (Of course, Google will now have to come up with additional interview questions to determine success, given their secret is out!)

For all these reasons, McAfee uses a panel interview approach for most positions. And we place at least one female or minority on every interview panel to represent the same diversity we aspire to recruit.

Finally, eliminate the bias that may have your company seeking only professionals with prior cybersecurity experience. There aren't enough of them in the market. We can't keep poaching from one another, driving up wages, and churning talent in the process. So eliminate questions that bias your company against candidates with different backgrounds. For instance, asking a candidate to tell you about the latest hot innovation he finds interesting in cybersecurity disadvantages those with less hands-on experience (as we learned from the history lesson of the PC). Ensure your questions pick up STEAM—pun intended—when looking for qualified candidates.

I walked into McAfee without having a lick of cybersecurity experience in my background. Within six months, I had co-authored a book on the topic. I'm not minimizing the complexity of the industry. But I am suggesting that skills are transferable. Look for candidates with technical skills in other fields. You'll find technical industries, like telecom, that aren't in the same zero-percent unemployment state. Technology lends itself to ebbs and flows in different labor markets. Expand your aperture for qualified talent with transferable skills, whether candidates have prior cybersecurity experience or not.

On the enlistment side of the coin, you can pull multiple levers to embed cybersecurity in the day-to-day jobs of employees, without overwhelming them in the process. First, **search your company values**—those standards for conduct or guiding principles that you expect employees to uphold—**and see where you can add one word to change their meaning in a profound way: *security***.

For example, in exploring my former stomping grounds at a prior employer, Verizon, I found the company has an impressive credo featured on their website at the time of this writing. Let's take a look at how inserting just one word can expand meaning without compromising intent (italics mine, to suggest the addition):

> We have work because our customers value our high-quality communications services.
>
> We deliver superior customer experiences through our products and our actions. Everything we do we build on a strong network, systems and process foundation. The quality, reliability *and security* of the products we deliver are paramount. Customers pay us to provide them with services that they can rely on.

One word can change scope without altering purpose.

Now this isn't a game of Cybersecurity Bingo. There are values or guiding principles where security just doesn't fit. Don't force a square peg in a round hole. Case in point from Verizon's example:

> We know teamwork enables us to serve our customers better and faster.

> We embrace diversity and personal development not only because it's the right thing to do, but also because it's smart business. We are driven not by ego but by accomplishments. We keep our commitments to each other and our customers. Our word is our contract. We respect and trust one another, communicating openly, candidly and directly since any other way is unfair and a waste of time. We voice our opinion and exercise constructive dissent, and then rally around the agreed-upon action with our full support. Any one of us can deliver a view or idea to anyone else, and listen to and value another's view regardless of title or level. Ideas live and die on their merits rather than where they were invented.

I happen to love that excerpt from Verizon's credo. But, try as I might, I couldn't find a way to naturally insert "security" in what is already stated beautifully.

That's okay. While you won't contrive a home for security in a company value where it doesn't belong, you'll likely find at least one where it easily does. Assuming your values are more than fancy copy on the back of an employee's badge, you'll begin to seed security into your company's foundation by rooting out non-secure behaviors and implanting secure ones in their place.

Next, let's look at your **rewards and recognition programs** to find a natural home for cybersecurity achievements. The first is clear and easy. Show some love to your cybersecurity team. As mentioned in Chapter 2, they've been relegated to the backstage of your company for too long. Bring them out from behind the curtain.

How? Give your CISO a voice in some company all-hands meetings. She doesn't need to be a perennial fixture in

every company event. But you can certainly expose her and her team's accomplishments for the broader employee population to understand the attack landscape and the importance of cybersecurity defense. Beyond enlisting more recruits to the fight, a little appreciation goes a long way and may help stymie high turnover rates (thanks to that nonexistent unemployment rate) in your cybersecurity ranks.

Next, expand your rewards and recognition programs to include cybersecurity. I mentioned in the last chapter about the importance of stopping the line for a new product or service release whenever security is subpar. Use your company's recognition platform to publicly credit employees—whether in cybersecurity or not—for raising valid security concerns that stop any such product or service from ever reaching the market.

Now it's time to address the elephant in the room where this book is concerned. Up until this point, we've been talking about employees as generally well-intentioned subjects seeking to do right by their companies in the way of cybersecurity, but perhaps lacking the education or prescription to do so. That's largely the reality.

But there is a subset of employees who have no desire to do right by your company. These aren't simply apathetic bystanders in the cybersecurity fight. These are malicious insiders seeking to do your organization harm and/or personally profit at your company's expense. According to Verizon's DBIR report, malicious insiders account for over 10 percent of all company breaches.[9]

Malicious insiders are the most insidious enemies for companies to address. For one, companies are reluctant to impose a Big Brother state of monitoring on employees—and for good reason. Privacy concerns notwithstanding,

employers may be unwilling to treat every employee as a potential bad actor, favoring instead a workplace culture in which trust is freely offered, not arduously earned over time.

Yet, bad actors who work for your company are a reality. What's an organization to do to weed out the threat from within? Your cybersecurity organization has technologies it can deploy to identify anomalous behavior. But technology, on its own, is a much weaker defense than the combination of technology, tools, and people working together. This is where HR professionals can assist in creating people controls to identify malicious insiders.

First, work with the CISO to identify the employees with the greatest access to the company's most valuable assets. Your CISO should already have a taxonomy of risk, mapped against value, for your organization's most prized possessions, whether intellectual property, manufacturing facilities, sensitive databases, or something else entirely. Define the perimeter of employees with privileged access to these valuables. Establish with the hiring manager and your security organization what level of access is required for these employees to do their jobs effectively. Periodically review the list of employees to ensure no job changes warrant an adjustment to privileges. Come performance review time, create a list of employees who may pose a flight risk and compare it against those who have privileged access, ensuring Legal is in the process to respect employee privacy concerns. By establishing and monitoring employee access privileges regularly, you protect your company from those who no longer require enhanced privileges (or may never have required them in the first place).

Note that access hygiene not only protects your company against malicious insiders but malevolent outsiders as well. Had McAfee applied this prescription, we would have removed an agency employee (essentially an extended insider to our team) from having administrative privileges to our social media page when she was no longer doing work for us. By doing so, we would have averted the hack I covered in the first chapter.

Next, within your reward-and-recognition program, carve out a place for whistleblowers. This goes beyond government programs that protect and incentivize these people. Establish a confidential program whereby employees can report suspicious behavior. Clearly, this is a fine line to walk, as you don't want to create a company culture of distrust among employees. But if you allow employees to speak up when they see something that doesn't sit right with them, you can marshal one of your most powerful weapons—your own workforce—in identifying rogue employees.

Case in point: A while back, McAfee reprioritized our investment areas to more closely align with our customers' needs and the marketplace. These decisions never come easy for a company, especially when they impact employees, which was the case in this example.

I received an email from a manager on my team, who forwarded one he had received from one of his employees. In it, the employee asked the manager for help. One of our impacted employees was overheard on what seemed to be a suspicious phone call. In it, the employee in question stated that, now that they had been "let go," they could reveal exactly what McAfee had been working on in recent months.

(I should mention that this employee had knowledge of an upcoming product rollout.)

Upon hearing the conversation, our concerned employee decided it best to send an email to a manager reciting exactly what was said. Because of this, we were able to intervene with a reminder to the exiting employee of confidentiality requirements (without exposing the whistleblower in the process). And we were able to make other decisions to accelerate or otherwise alter the original rollout schedule for the product in question.

Since the exiting employee wasn't using company systems to relay or exfiltrate the information, this threat would have gone undetected by McAfee's cybersecurity team. Only one employee overheard the phone conversation and was under no obligation to report it. But the person did. I couldn't have expressed my gratitude more for one of our own looking out for the company. **Find a confidential, nonthreatening way for conscientious employees to blow a whistle or raise a flag when they see something dubious. When they do, reward them appropriately.**

Finally, examine your company's key performance indicators (KPIs) to find those related to cybersecurity. At a minimum, **every member of the executive team should have at least one cybersecurity KPI**.

This shouldn't be hard. After all, this book reveals how cybersecurity permeates multiple functional areas of the company and where every employee can play his part. Find a few examples and embed at least one meaningful cybersecurity KPI for every chief officer. He will in turn cascade the appropriate cybersecurity metrics to those on his team with

responsibility for the same. Those leaders will, in turn, distribute responsibility to the individual contributors on their teams. This waterfall effect eventually soaks cybersecurity into all functions and all levels of your company.

* * *

This book is about instilling a cybersecurity culture at all levels and layers of organizations. Culture isn't pushed down. It spreads laterally and organically. The best management can do is provide the optimal soil for great cultures to flourish. That entails ensuring employees are mindful of the vision, mission, and values guiding your company forward. It requires recruiting the right talent, aligned to those company values, and committed to mutual success. And it entails having reward-and-recognition programs and clearly aligned metrics to ensure everyone is moving in the same direction.

As those who most tend to a company's culture, HR professionals have a significant role to play in depositing cybersecurity seeds. You are instrumental in helping the industry's, let alone your company's, cybersecurity talent shortage. By removing the unconscious bias that limits our collective ability to find and recruit exceptional cybersecurity talent and creating a climate that enlists every employee in the battle, HR can bridge the cybersecurity gap for all of us.

Notes

1. Steve Morgan, "Women Represent 20 Percent of the Global Cybersecurity Workforce in 2019," Cybersecurity Ventures, March 13, 2019, https://cybersecurityventures.com/women-in-cybersecurity/.

2. Jane LeClair, "Why There Are So Few Women and Minorities in Cybersecurity," Thomas Edison State University, September 7, 2018, https://blog.tesu.edu/why-there-are-so-few-women-and-minorities-in-cybersecurity.
3. Bletchley Park Research, https://www.bletchleyparkresearch.co.uk/research-notes/women-codebreakers/.
4. Clive Thompson, "The Secret History of Women in Coding," *The New York Times*, Feb. 13, 2019, https://www.nytimes.com/2019/02/13/magazine/women-coding-computer-programming.html.
5. Ibid.
6. John Sullivan, "7 Rules for Job Interview Questions That Result in Great Hires," *Harvard Business Review*, February 10, 2016, https://hbr.org/2016/02/7-rules-for-job-interview-questions-that-result-in-great-hires.
7. Shannon Shaper, "How Many Interviews Does It Take to Hire a Googler?" re:Work, April 4, 2017, https://rework.withgoogle.com/blog/google-rule-of-four/.
8. Shankar Vedantam, and Maggie Penman, "How Google's Laszlo Bock Is Making Work Better," National Public Radio Hidden Brain Podcast, June 7, 2016, https://www.npr.org/2016/06/07/480976042/how-googles-laszlo-bock-is-making-work-better.
9. Verizon, "2018 Data Breach Investigations Report," https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf.

CHAPTER

6

Luck Favors the Prepared

We have a team process that gets triggered if a cyberattack happens and so we wouldn't directly go out and let the press know until we figured out certainly what it was and where it came from and what we planned to do about it. We haven't been that far yet. It all depends on what the data flow is and how severe of a problem it is.

Chief Marketing and Sales Officer, Hospitality Company

A friend of a friend of mine knows a guy who was traveling on business in Las Vegas. He went to a bar one night and had a few drinks with a friendly stranger. The next morning, he awoke to excruciating pain in his lower back, submerged in a bathtub of ice. He noticed a phone next to the tub with a note that said something to the effect of, "Call 911. Your kidney has been surgically

removed." He lived to tell the tale but has one less kidney to show for it. Be careful—there's an underground market harvesting organs from unsuspecting business travelers and tourists.

I bet you've heard a similar story from a friend of a friend. But perhaps the victim in question wasn't in Las Vegas. He might have been in Europe. Or South America. Who knew the underground market for stolen organs was so vast?

Of course, it isn't. This urban legend started in the late 1990s and, while we can roll our eyes at its absurdity today, I remember it sending shivers down my spine (right down to my kidneys!) when I first heard of this horror. I wasn't the only one who fell for it.

On January 30, 1997, after being inundated with phone calls from wary travelers rethinking their plans to party at Mardi Gras, the New Orleans Police Department issued the following statement:

> Over the past six months the New Orleans Police Department has received numerous inquiries from corporations and organizations around the United States warning travelers about a well-organized crime ring operating in New Orleans. This information alleges that this ring steals kidneys from travelers, after they have been provided alcohol to the point of unconsciousness.
>
> After an investigation into these allegations, the New Orleans Police Department has found them to be **COMPLETELY WITHOUT MERIT AND WITHOUT FOUNDATION**. The warnings that are being disseminated through the Internet are **FICTITIOUS** and may be in violation of criminal statutes

concerning the issuance of erroneous and misleading information.[1]

I'm fascinated by urban legends. As a marketer, one of the hats I wear is that of storyteller. Urban legends are unique stories in that they catch fire fast. Turns out the most legendary among them share certain characteristics.

They tend to have a moral, such as, "Look out for approachable strangers offering you alcohol in a bar." They prey on societal fears of the moment. And they usually come by way of "a friend of a friend." In other words, tracking down the source or veracity of the information is impossible, leaving people to fill in details of the story as it spreads.

I'm struck by the similarities between a successful urban legend and a breach that makes its way to the headlines. Like urban legends, the news of a public breach tends to spread quickly. The details of a breach, such as how it happened and who was to blame, are typically slow to come, leaving individuals to fill in the gaps of the story with their own assumptions, the way "friends of friends" do for folklore tales.

Breaches and urban legends have one more thing in common: They tap into a powerful emotion—fear. Why is fear so powerful? It's deeply rooted in our survival instinct. Fear and anger, known as "hot" emotions, are two emotions we feel intensely. Our bodies have been programmed through the millennia to respond quickly to preserve our existence when these emotional chords are triggered. In contrast, it takes us longer to feel "cool" emotions, like joy and love, since our immediate survival depends on feeling neither as intensely.[2]

In fact, the one notable difference between urban legends and breaches is that the latter are real. For marketers and communications professionals, regaining control of your company's narrative, while remaining transparent and authentic throughout the process, is a daunting challenge at best. The public relations battleground is littered with more bad examples than good of companies that mis-stepped in a communications outreach following a breach.

As the ultimate stewards of brand reputation, my marketing and communications colleagues must be ready to respond—and respond quickly—when the next breach occurs.

BREACH!

In 2014, when Frank Blake announced he was stepping down as CEO of The Home Depot, he was leaving behind a seven-year legacy of strong business performance and compassionate leadership. Like many CEOs, Blake saw his fair share of challenges over his tenure. When he first took the reins in 2007, the looming housing crisis was just starting to smolder. In addition to stock price, morale was also on the decline thanks to a top-down managerial style that had overstayed its welcome with employees.

Blake went to work focusing on the basics. He paused on opening new stores and started opening fulfillment centers instead, moving merchandise closer to existing locations. He focused on profitability and merchandising mix. He closed unprofitable divisions and markets.

At the same time, he brought southern charm back to the giant retailer's culture. On a typical Sunday, Blake would

handwrite hundreds of personalized thank-you notes to worthy employees—a courtesy he picked up from then–Vice President George H. W. Bush, when he served as his deputy general counsel.

A few years of tenacious focus turned The Home Depot around. Under Blake's tenure, the stock price had doubled from the time he took office in 2007 to when he announced his intent to step down in August of 2014.

So in the final months of his tenure, Blake was taking some well-deserved time off on Labor Day weekend—just 12 days after announcing his departure as CEO. Ever the workaholic, Blake was writing his handwritten thank-you notes to employees that Sunday afternoon. As he would say, "You get what you measure. You get what you celebrate."[3]

The weekend celebrating wouldn't last. The next morning, Blake got a call from his company's general counsel. It looked as though their computer systems had been infiltrated.

While Blake didn't have all the details yet, his company's financial health and reputation were at risk. In his last few months on the job, Blake was staring down the barrel of a crisis that not only endangered his company but threatened to tarnish the CEO's unblemished record as well.

We know the end of this story. The Home Depot had 56 million debit and credit cards breached. But what makes this story unique is not the hack itself but the way the company responded. Indeed, the general consensus from critics and opinion leaders alike is that we can all learn something from their example.

During a time when big-company hacks were making headlines regularly, The Home Depot stood out—in a *good* way. Blake didn't run for cover. He didn't deny responsibility.

He didn't withhold information until he had all the details. And he didn't pass the buck to his recently named successor to let the new guy sink or swim. (And, to be clear, any of these options would have been taken by someone with a weaker constitution.)

Instead, Blake did the most unnatural thing of all. He reported the breach publicly before his company even knew definitively what was happening. He apologized for the incident before fully understanding who was to blame. He let all customers know that his company would be responsible for any fraudulent charges and offered free credit monitoring before knowing the full extent of the damage.

While the company wasn't spared from a class-action lawsuit, it avoided the full wrath of potential punitive damages, largely because of how Blake and the executive team rallied. As the judge explained as part of his decision:

> The real villains in the piece were the computer hackers who stole the data. After the data breach was discovered, there was no cover up, and Home Depot responded as a good corporate citizen to remedy the data breach. There is no reason to think that it needed or was deserving of behavior modification. Home Depot's voluntarily-offered package of benefits to its customers is superior to the package of benefits achieved in the class actions.[4]

In the end, while other companies that suffered major breaches of the time were derided in the court of public opinion for executing their communications strategies so ineptly, The Home Depot was lauded for its integrity.

What of Blake's sterling legacy? Incredibly, the hack may have helped polish it even more. After all, how often is it that a company is publicly *praised* after a breach?

And the hackers didn't manage to steal The Home Depot's reputation either. In the company's "voice of the customer" surveys, the net percentage of customers who would strongly recommend The Home Depot to others increased 44 percent under Blake.[5]

The Home Depot avoided being the punchline of their breach. They controlled their message, leaving little chance for "friends of friends" to fill in the details for them. They traded on empowerment, instead of fear. Years later, we're still admiring how not to let a crisis go to waste.

Preparing for Battle

While The Home Depot may be legendary in the way it executed its response, it certainly isn't unique in suffering a breach in the first place. Since the time you started reading this chapter, more than 30,000 data records have been lost or stolen globally. That's according to the Breach Level Index, which reports 72 records are compromised each second.

Time is never on the side of a responder, no matter the crisis. But in a breach, time works against your company in two ways. First, there's the time required to discover the breach, what's known as "dwell time" in the industry. Per Ponemon, the average dwell time was 197 days in 2018,[6] more than six months of cybercriminals rummaging through a breached company's systems before being detected.

(Once identified, it takes companies, on average, an additional 69 days to contain the breach.[7])

Then, there's the time required to notify constituents of the breach. Companies typically struggle on this front as well, since the forensic details of a cyberattack rarely come easy. The International Association of Privacy Professionals conducted a study for 18 months of cybersecurity incidents from 2016–2017. They found the average time from discovery of a breach to its notification to be 29 days.[8] As a comparison, the GDPR requires notification in 72 *hours*.

The bar is undoubtedly high. But if we as storytellers have learned but one thing over a career of experience and training, it's this: Luck favors the prepared.

There are scores of valuable research studies on effective crisis communications, compiled over decades. Distilling it down, effective companies take two common approaches.[9] It's as though Blake and his team enacted the playbook that scholars have researched for decades:

1. *Successful companies communicate early and often*. When bad news breaks, your company is on trial in the court of public opinion. It should come as no surprise that the first tenet of effective crisis communications comes from those who defend others in a court of law. "Stealing thunder" originated in the legal field and pertains to revealing one's mistakes before someone else does so (in a court of law, it's the defendant doing so before the prosecution; in a court of public opinion, it's the company doing so before the media). Stealing thunder is presumed to work since being first to break your own bad-news story instills

credibility in your message and makes your revelation look less incriminating. To this latter point, your audience interprets the severity of your transgression based on who is sending the message—you or someone else. Specifically, they are more likely to assume your offense is *less* significant, precisely because you're the one bringing it to light.[10] Transparency is highly treasured in the courts of law and public opinion.

Finally, it pays to be aggressive. Keeping stakeholders regularly informed is better than quietly retreating, hoping the problem will simply go away. While an aggressive communication approach initially caused a sharper drop in both stock prices and reputation scores for organizations suffering a crisis, those companies' stock prices and reputations also rebounded faster than their counterparts that chose a passive style.[11]

2. *Successful companies focus on the victim, not themselves.* This one is tougher than it may seem since it requires companies to express empathy for victims. Because companies are often reluctant to extend social graces, like public apologies, due to legal concerns, they can fall short on the victim-centered litmus test. Note that victim-centricity is necessary, but not always sufficient, in effective crisis communications. If victims believe the company could have done more to prevent the crisis or view the firm's reputation poorly, more may be required, like victim compensation.[12]

Many companies resist victim-centricity in their communications strategy and opt to deny responsibility

instead. On this point, the research is clear. Denying a crisis for which the company is responsible results in a double-whammy. Not only is denial initially less effective but, when the facts later expose the company's culpability, *another* crisis ensues. The only approach where denial is effective is when it is *known* that the company has no culpability.[13]

Even though denial is a selective approach, communicators would be wise to bake several strategies with it at the core. In particular, there may be cases where a company is not directly responsible for a breach. For example, your customer may reuse the same password across multiple services, including one provided by your company. Say hackers compromised one of those other services and your customer's password is sold on the Dark Web. Even though your company wasn't responsible, how would you handle such notifications where something or someone else is to blame?

Breach-by-association is one thing. Data weaponization is another. As organizations are learning, it's no longer what cybercriminals can *take*, but what they can *fake*. Maybe it's your reputation that bad actors most want. One threat vector could be to hack into your corporate email servers and expose sensitive or otherwise unflattering emails senders and recipients never intended for a public audience.

But why stop there? Adversaries are beginning to mess with their victims' minds, just as they've historically done with their money. Perhaps they'll put some fake emails in the mix when the "leak" is exposed. When sprinkled in with their authentic counterparts, these

> counterfeit messages are hard to identify and even harder to explain. Communications experts must anticipate how they would effectively deny culpability for blatantly falsified emails (or other documents) that impugn their brand's reputation lest they find their company starring in its own urban legend of their enemy's making.

While cybersecurity attacks are a relatively new phenomenon for communications experts, crises are not. We can apply the wisdom from this canon of research to our own blueprint for action.

W.I.S.D.O.M. for the Marketer/Communicator

If luck favors the prepared, you need a plan well before the breach. Time isn't on your side otherwise. When precious minutes are ticking by, the last thing you want is for your executive team to be ruled by their own hot emotions of fear or anger that can cloud rational thinking.

Build a multifaceted communications plan with explicit executive buy-in. Think like a CISO in this exercise. CISOs must provide the board with a view of asset risk. All assets are not created equal in this exercise. You'll need to do the same as it pertains to what your company should do, depending on the type and severity of attack. Not all attacks are created equal.

Work with your CISO to identify popular threats your company faces, things like web defacement, ransomware, data breach of customer records, data breach of employee records, and the like. From there, be very prescriptive about your notification principles in each case.

- Even if the law didn't require it, would you notify?
- What if your company wasn't responsible for the attack? How would that change the tone and content of your message? (Think of the breach-by-association or data weaponization examples mentioned earlier.)
- When would you notify? Realize that earlier is better to shape public opinion. In fact, the body of research on crisis communications suggests the best timing is within one hour of the incident.
- Whom would you notify?
- What would you say if you didn't have all information right away (which is more than likely to be the case with a breach)?
- What would you be willing to offer customers as compensation or as a show of victim-centered empathy (such as free identity protection or offering to cover customer losses from a credit card breach, for example)?

Have your CEO and the executive leadership team participate in this exercise and agree to the guiding principles that govern how, when, and what you communicate based on the severity of the attack.

This exercise will take weeks, if not months, to complete sufficiently. Since chances are your company is already under attack and just doesn't know it yet, formalizing a consensus-built plan is your first priority.

Create the communications templates for each scenario identified in your plan. Team up with Legal to frame each message. Write emails, web copy, blogs, telephone scripts, press releases, media statements, and other assets, leaving placeholders for details that you'll fill in when the attack

occurs. Stage websites (internal and external) that can go live quickly to communicate details of the breach when it occurs.

Messages must strike the right balance of instruction and tone. When a crisis happens, customers want to know that your company has their best interests in mind and the situation under control. Unfortunately, breaches are rarely so cooperative in giving your company flexibility on both points.

In the way of demonstrating your company is in control of the situation, stick to the following blueprint for your templates:

- Who was impacted?
- What data and/or systems were lost, stolen, and/or otherwise compromised?
- Over what period did the breach occur?
- What precautionary action do stakeholders need to take?
- What actions is your company taking to correct the problem and mitigate the risk of it happening again?

Even if your company does not yet have all the information, being early and accurate in communicating the details you do have allows you to steal thunder.

Next, in the way of tone, show empathy in these messages while protecting your legal interests—a key reason to get Legal involved early in the exercise. On that point, have Legal review all templated messages so, when the breach occurs, you're that much closer to securing final approval once you've inserted any remaining details.

We've discussed the importance of empathy. This tried-and-true crisis communications tenet proves true in the

world of data breaches. Ponemon surveyed consumers who terminated their relationships with a company following a data breach in 2014. When asked what these companies could have done to preserve the relationship, more consumers wanted a sincere apology (43 percent) than wanted free identify theft and credit monitoring services (41 percent).[14]

Match your language to the tone. Empathy doesn't lend itself to technical jargon or legalese. Consumers can spot a fake apology a mile away. Another Ponemon study in 2012 found approximately one-third of consumers complaining about the length or legalese in the post-breach communications they received.[15]

Design the tick-tock schedule for every attack scenario. Cybersecurity's currency is time. Design your plans accordingly. Have minute-by-minute schedules for each attack vector. You likely won't have all the information in the early minutes of finding out your company has been breached.

Lucky for you, your communications plan will guide you on what your executive team is comfortable releasing, and when. Because you will have built this plan while not under the duress of the clock, you can be more persuasive in submitting evidence that shows early-and-often communication pays (remember The Home Depot as a sterling example)—even when not all facts are readily available.

Your tick-tock schedule should identify who is responsible for distributing messages and/or assets to key stakeholders at every phase of the plan. More than 60 percent of consumers say that their satisfaction with a breached company's response would greatly improve if the organization notified them immediately.[16]

Be sure your plan includes employees, whether employee records are breached or not. During crises, employees (perhaps even more so than customers) need reassurance that their employer is in control. Employees are the best brand ambassadors for a company. If you keep them in the dark on the details of the situation, they can't help you spread your message, leaving you once again a potential victim to the "friend-of-a-friend" grapevine. Actively engage your employees to enlist their support and calm any anxieties. In terms of tactics, consider going beyond email and intranet updates. Have at least one town hall meeting to explain the situation. Additionally, open a conference hotline each day for a scheduled period (say, 30 minutes), where you can update interested employees on the latest and answer any questions.

Practice, practice, practice. CISOs run red-teaming exercises, where they simulate attacks on their organization to identify vulnerabilities and shore up defenses. In the same way, CMOs should practice crisis drills to test their team's effectiveness in responding according to plan. Crisis management experts recommend doing so at least once a year to build the muscle memory of your organization.

As part of the practice drills, simulate media interviews with your designated company spokespeople. You will need multiple spokespeople trained and ready to engage the media when a breach happens. Ensure they are prepared with the talking points and answers to the tough questions to retain control of the message. In this case, practice makes nearly perfect.

Run your overall crisis plan and the results of your drill by the executive team to confirm nothing has changed in your guiding principles for communication. Take time to

review what other companies have done in the timeframe from your last exercise to learn best practices and adapt your own plan in the process continuously.

* * *

Maya Angelou once said, "I've learned that people will forget what you said, people will forget what you did, but people will never forget how you made them feel." The reason we're still talking about Frank Blake's enduring legacy in cybersecurity is because his swift actions and accommodating response left all of us (victims or not) *feeling* better that companies still do the right thing. What Blake revealed through his actions is that his company cared about its customers. And that feeling prevailed long after Blake resigned his post as CEO.

When a breach happens, luck favors the prepared. Your company won't be able to prevent all breaches. Determined cybercriminals only need to score once. When they do, the marketing and communications teams will need to strike back quickly with a coordinated, choreographed communications plan that engages all relevant stakeholders with clear instructions and sincere empathy. Your customers and employees will measure your company based on its response. When the smoke clears, they may not recall everything you said or did, but they'll certainly remember how you made them feel.

My marketing and communications comrades, *you* stand between hackers and your brand's reputation. Lucky for you, there's plenty of preparing you can do to be ready.

Notes

1. https://web.archive.org/web/19980506013419/http://mardigrasday.com/police1.html.
2. Jim Taylor, "Is Our Survival Instinct Failing Us?" *Psychology Today*, June 12, 2012, https://www.psychologytoday.com/us/blog/the-power-prime/201206/is-our-survival-instinct-failing-us.
3. Maria Saporta, "UPDATE: Retired Home Depot CEO Frank Blake: 'I Really Don't Like Amazon,'" *Atlanta Business Chronicle*, August 15, 2017, https://www.bizjournals.com/atlanta/news/2017/08/15/retired-home-depot-ceo-frank-blake-i-really-dont.html.
4. Lozanski v The Home Depot, Inc., 2016 ONSC 5447 (CanLII), <http://canlii.ca/t/gt65j>, retrieved on 2019-03-11.
5. Jennifer Reingold, "How Home Depot CEO Frank Blake Kept His Legacy from Being Hacked," *Fortune*, October 29, 2014, http://fortune.com/2014/10/29/home-depot-cybersecurity-reputation-frank-blake/.
6. Ponemon, "2018 Cost of a Data Breach Study: Global Overview," July 2018.
7. Ibid.
8. Mahmood Sher-Jan, "From Incident to Discovery to Breach Notification: Average Time Frames," https://iapp.org/news/a/from-incident-to-discovery-to-breach-notification-average-timeframes/.
9. W. Timothy Coombs, "State of Crisis Communication: Evidence and the Bleeding Edge," *Research Journal of the Institute for Public Relations* 1, no. 1 (Summer 2014).
10. Lara Dolnik, Trevor I. Case, and Kipling D. Williams, "Stealing Thunder as a Courtroom Tactic Revisited: Processes and Boundaries," *Law and Human Behavior* 27, no. 3 (June 2003).
11. R. Moran, and J. R. Gregory, "Post Crisis: Engage—or Fly Low?" *Brunswick Review* 6 (2014): 32–34.
12. W. T. Coombs, "Impact of Past Crises on Current Crisis Communications: Insights from Situational Crisis Communication Theory." *Journal of Business Communication* 41, no. 3 (2004): 265–289.
13. W. Timothy Coombs, Sherry Jean Holladay, and An-Sofie Claeys, "Debunking the Myth of Denial's Effectiveness in Crisis Communication: Context Matters." *Journal of Communication Management* 20, no. 4 (2016): 381–395, https://doi.org/10.1108/JCOM-06-2016-0042.

14. Ponemon Institute, "The Aftermath of a Data Breach: Consumer Sentiment," April 2014, https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf.
15. Ponemon Institute, "2012 Consumer Study on Data Breach Notification, June 2012, http://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf.
16. Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*. Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1187.html. Also available in print form.

CHAPTER

7

Interesting Bedfellows

As you move further and further out—our secondary and tertiary relationships—you obviously have greater vulnerability. We have a very robust third-party service policy and network for monitoring and maintaining those relationships. In fact, that's one of the areas that I'm responsible for myself. We have an entire department dedicated to that. We have questionnaires. We have different third parties that will then do audits and examinations of some of our more critical third-party service providers to make sure that they are maintaining appropriate levels of security. We require certain third-party audits of their data security that must be done every year. It's pretty robust.

CFO, Financial Services Company

If you're a CFO for an enterprise, chances are you have something in common with most hackers: You have a healthy profit motive. Many adversaries would agree with a philosophy you likely hold dear: Cash is king.

The cybersecurity industry has done itself no favors with the stereotypical hacker trope of a bad guy in a hoodie lurking behind a green DOS screen that appears to be from the 1980s (coincidentally, the decade when Hollywood gave a face to the hacker community). The shadowy figure of a lone wolf behind a keyboard is no representation for the extensively sophisticated cybercrime syndicates that have very healthy profit motives indeed.

Jonathan Lusthaus never envisioned a career studying cybercriminals. His passion was in researching religious violence. But when his dissertation topic didn't conform to the research areas of the Oxford faculty, he needed to find a new interest.

Quite by accident, he became inspired by a well-known author on cybercrime who was lecturing on the topic at Oxford just as Lusthaus's deadline for choosing a new subject loomed. Almost 250 interviews with law enforcement agents, security professionals, and former cybercriminals later, Lusthaus is an authority on the topic. In his book *Industry of Anonymity: Inside the Business of Cybercrime*, he exposes the real underbelly of this $600 billion industry[1] to the rest of us.

He found that the underground market shares quite a lot in common with the financial markets that underpin healthy—and legitimate—business and industry. Lusthaus points to specialization among cybercriminals. There are very few jacks-of-all-trade in cybercrime. Instead, as Lusthaus uncovered, there are more economic benefits to

investing in a "trade" and relying on others to perform specialized functions. Some are more technical, so they design the online scourge. Others are natural at selling, so they take to the underground commerce markets to promote the value proposition. Still others are strong at implementation. They provide the post-sales support to buyers who need help in getting the weapon to its intended target(s).

The division of labor that propels the world's most sophisticated companies serves the needs of the Dark Web as well. How do cybercriminals with such specializations trust one another to make good on payment when services are rendered? In much the same way online shoppers have learned to trust legitimate online companies seeking their business. They rely on numerical rating scales of other cybercriminals evaluating their experience. They use feedback forums to exchange information about the ne'er-do-wells among them (apparently, there really *is* honor among thieves).

These feedback mechanisms scale the business of cybercrime. Each criminal can spend less time validating the expertise and trustworthiness of potential partners in the chain and more time executing on his craft to commit crime.

Beyond mimicking the services of online exchanges, the cybercrime market imitates rules of legitimate governance as well. Lusthaus found cybercriminals using escrow to entrust a third party with holding payment, if not goods, until everything had been verified. There's even arbitration, where each side can argue its dispute in front of a senior member of the community, appointed to make a ruling. In certain cases, the "judge" may ban the offending party from the marketplace.

McAfee has done our own research[2] on the vast cybercrime market that lurks beneath the surface of the web. Thanks

to law enforcement takedowns of some prominent Dark Web marketplaces, cybercriminals are exercising their entrepreneurial chops. Several individual sellers are trading established marketplaces (which tend to be targets for law enforcement officials) for their own websites to peddle their goods and/or services on the Dark Web. Defiant website designers are accomplices in the pursuit, designing hidden marketplaces for aspiring vendors. Yes, even the Dark Web has layers that allow its participants to fly lower still beneath the radar.

Regardless of a bad actor's intent to open her own click-and-mortar equivalent, there are plenty of helpful underground forums dedicated to the topic of cybercrime to help these criminals hone their craft. The more popular discussions entail leaked user credentials, common vulnerabilities and exposures, and "dump sites" to offer plenty of stolen credit cards, fresh for the taking.

This is the face of cybercrime. This complex labyrinth of entangled services, buyers, sellers and "regulators" is what your company is up against. And your company has the deck stacked against it. This isn't a fair match-up. There are no Sarbanes-Oxley (SOX) requirements on the Dark Web. No GDPR governing privacy and the use of data. No compliance standards dictated by hosts of governing bodies. Hackers can code at 2:00 a.m. and exploit their victims by 4:00 a.m. There's also no need for onerous testing windows to ensure that quality controls are met.

Unlike your competitors, which are governed by the same rules, regulations, and general business ideals as your company, adversaries respect no laws (except those of their established communities). Unlike competitors seeking to take market share, bad actors want to take you for everything they can.

You may be very familiar with the fact that you're dealing with a highly coordinated enemy. But consider how Finance typically doles out budgets to organizations to understand the rub for cybersecurity. Budgets might be allocated based on benchmarking data. While you can find such benchmarks for cybersecurity spend, they're a bit misleading. That's because the *real* benchmarks for cybersecurity must come from adversaries. If you don't know what adversaries are spending in research and development to create their "products," how can you accurately assess the cybersecurity budget required to match it?

If not benchmarking data, budgets are allocated by return on investment (ROI). Again, that's a tricky measure for cybersecurity professionals to prove. Because how can CISOs prove a negative? Even if they tried, wouldn't smart CFOs challenge the argument at face value? Imagine a conversation between a CFO and CISO that goes something like this:

CFO: Why do we need to buy this new security widget?
CISO: Because we're seeing a record number of attacks against the company in this area.
CFO: But what's the return on investment for that spend?
CISO: Well, there's a possibility we could be breached if we don't do something.
CFO: So you're telling me that you can guarantee me we won't have a breach if we buy this technology?
CISO: Not exactly. It's a bit more complicated than that.
CFO: Let's uncomplicate it. What's the return on investment for the spend?

You can see how the circular argument could go on for a while. Short of attempting to shock and awe finance people with convoluted cybersecurity metrics, there's no clever way for a CISO to answer the "What's your ROI?" question.

It's not that CISOs are evading the question—or that they don't comprehend the concept of ROI. To understand why this is such an impossible question to answer, let's look at a few adversarial attacks that put a finer point on it.

The More Things Change . . .

In May of 2017, cybersecurity made its way to the front page of practically every media website and the first segment of virtually every news broadcast worldwide. Those who didn't know about ransomware before would learn it by one name, WannaCry. Unprecedented in scale and velocity, the attack infected more than 200,000 computers worldwide within its first few days—shutting down hospitals, universities, and banks.[3] WannaCry held each victim's computer files for ransom to the tune of up to $300 in bitcoin. The estimated damage of WannaCry's wrath? Well into the billions of dollars globally.

But it would be unfair to call WannaCry ransomware. Sure, ransomware was the visible exploit to victims threatened with unrecoverable file loss. But what made WannaCry so stealthy is the way in which it propagated, using the properties of a worm to contaminate new systems. Without taking a technical detour into the weeds here, the key difference between "traditional" ransomware and WannaCry is that the latter didn't require human intervention to spread. That's

how it proliferated so quickly. It didn't rely on unsuspecting humans taking its bait. Instead, it exploited a vulnerability already resident in a popular operating system.

McAfee's own analysis of WannaCry revealed that it barely qualified as ransomware at all. Its authors left it with rather crude monetization capabilities. They didn't connect a victim's unique identification to his bitcoin payment, making decryption of files extremely difficult. So what was WannaCry really? Ransomware? Worm? Both.

In 2018, hacker ingenuity was again on full display with the release of Zyklon. Zyklon was a fully featured package of threats for enterprising criminals to exploit—it could steal passwords, launch DDoS attacks, mine cryptocurrency, and more. What really was Zyklon? Cryptojacking? DDoS? Keylogging? All of the above.

As WannaCry and Zyklon show, hackers not only cooperate in specialty, but they collaborate to create new concoctions of converged threats. They're mixing old varieties (like worms) with new ones (like ransomware). In McAfee's analysis of underground forums, we see cybercriminals discussing vulnerabilities, both old and new. The results are sophisticated threats capable of contagion much faster than ever before.

Back to our conversation between the CFO and CISO. When the CISO approaches the CFO for more money, it's usually because of this reality. Even mid-cycle, long after budgets have been allocated, the CISO may need more. WannaCry didn't wait for a convenient fiscal period end to wreak its havoc. Bad actors don't care about your budget cycle.

If ROI isn't the right metric for cybersecurity, then what is? Risk management. Cybersecurity professionals are

in the risk management business. Sure, they have technical expertise and scores of products in use to defend their companies against highly organized crime syndicates. But take that technical jargon out of the field and it really comes down to one clear business objective—mitigate the company's risk.

As CFOs know, risk management and its associated metrics fundamentally differ from the more traditional finance measure of ROI. I live in North Texas, part of a region of the country that has earned the unfortunate colloquialism "Tornado Alley." To this day, I have a healthy fear of tornadoes. Blame it on the tornado sirens that are tested the first Wednesday of every month at noon. The chilling sound is straight from a war movie. Or chalk it up to Dorothy and her trip to Oz by conveyance of a tornado, the thought of which freaked me out as a child. Either way, I fear tornadoes. But every spring in North Texas, they are a persistent threat to me and my otherwise peaceful existence.

Until I was educated on just how unfounded my fears are. McAfee's chief technical officer (CTO) relocated to the Dallas area last year. He immediately was schooled on tornadoes by nervous colleagues and long-time Texans like me. However, unlike me, he decided to do his own research rather than succumb to the hype. He discovered that, in 69 years of tracking, there has been only *one* F3 or higher tornado in my county (this is a tornado capable of causing severe to incredible damage).

Now, let's go back to our risk management discussion. Does your finance team inspect the ROI of tornado shelter signs posted clearly on your company's campus, particularly one like mine that happens to reside in "Tornado Alley"? Likely not. Even if you examined the risk of losing these signs altogether, you might find the data supports such reckless

abandon (the tracking our CTO found for my county would suggest a deadly tornado is a very unlikely event indeed).

Even if there is only one catastrophic tornado in 69 years, there's still a risk. Should that risk materialize, foregoing visible and sensible signage to save a few dollars may prove to be a costly decision.

Cybersecurity is in the same boat. While CISOs must address volumes of threats each day (which likely won't cause cataclysmic damage but may disrupt the business nonetheless), they must also consider the catastrophic (albeit far less likely) risk inherent in a major-scale attack that could incapacitate their company for some time. They're walking the risk tightrope every minute of every day.

If CFOs can begin the discourse a bit differently with CISOs, they can help build the bridge from cybersecurity to risk management. Imagine that earlier conversation a bit differently:

CFO: Why do we need to buy this new security widget? What are we attempting to secure?

CISO: It secures our [fill-in-the-blank] asset, which we've identified as a highly strategic resource for the company.

CFO: But how do you know that asset is at risk?

CISO: We know of a vulnerability that attackers could exploit.

CFO: What's our risk if we don't do something?

CISO: Given that it's a high-risk asset, the consequences of a breach would mean [disruption to our business, fines up to $x million, customer safety recalls, shutdown of critical systems or sites, etc.].

> **CFO:** Let's double-click on that consequence a bit more. Tell me what our [financial, legal, intellectual property, and/or reputational] exposure looks like.

Simply by framing the conversation differently, CFOs can assist their CISO partners in translating cybersecurity investments into business outcomes—all while losing the technical jargon and eye charts of cybersecurity metrics that most CFOs likely won't miss. It starts with asking the right questions.

Those same questions prove fruitful for other business decisions governed by Finance's tried-and-true ROI metric. Most profit-seeking companies are in the business of growth. Because of this, there are pressures to enter new markets, expand with new products, enhance productivity with new technologies, and the like. Many of these business cases hold up to the ROI litmus test. But how often are they searched for their impact on the company's risk profile, particularly by expanding the attack surface for adversaries to exploit?

CFOs can help their organizations ask these risk-related questions whenever a new business case crosses their desks:

- How does the new [market, internal technology, customer product, etc.] change the attack surface for the company?
- How does it alter the risk profile of the company's most strategic assets?
- [Assuming risk is increased] What additional investment is required (one-time and recurring) to bring the

risk profile to its acceptable baseline? Is this investment included in the ROI analysis?

By asking these questions of their non-cybersecurity counterparts, CFOs and their teams can ensure cybersecurity is not an aftermarket afterthought of the strategic growth initiatives for their companies.

…the More They Stay the Same

They hide during the day to feed at night. They look for a blood meal to survive, snacking on their victim while he sleeps, since they abhor movement. They are fast movers, generally covering three to four feet per minute–when scaled, the equivalent to an average adult's sprinting pace. Yes, bed bugs are having quite the resurgence around the world.[4]

These miniscule predators were all but vanquished following World War II, thanks to fastidious household hygiene and aggressive pesticides that banished them into virtual extinction. In recent years, they've been making a comeback. It turns out a strain of bed bugs, highly resistant to those initial harsh pesticides, has entered the insect kingdom. Couple that with an influx of global travelers who serve as unwitting carriers for these repulsive hitchhikers and you have a bedbug epidemic once again sweeping the world.

Here's what makes bed bugs so difficult to eradicate. You can have the cleanest house in the world. You could disinfect your bedding religiously. You could do the same for pajamas or any other clothing that should touch your place of slumber. But if you happen to travel to a hotel or in an airplane that is infested, it takes just one pesky bed bug to hitch

its wagon to your star (in this case, your luggage or what's packed inside) and make its way to your domicile.

The problem is even worse if you happen to live in an apartment building or other multi-dwelling unit. Now, it just takes the neighbor with whom you happen to share a wall to be a bit laxer than you are in his standards, and you may find yourself with unwelcome inhabitants in your home (yes, these determined parasites can move along and through wall voids, using plumbing and electrical chaseways as their routes).

If that isn't bad enough, because there is such a stigma associated with bed bugs, most people are loath to admit they cohabitate with these bloodsuckers. By the time they concede they have a problem and seek help, they may be facing an all-out infestation. If you happen to spend the night (as in a hotel) or share a wall (as in neighbor)—you get the idea….

Bed bugs are an unfortunate reminder of how dependent we are on one another. It isn't a matter of leaning on our neighbors for help. It's about trusting them to know their environment (nearly 50 percent of people with bed bugs in one study didn't even know they had them[5]) and to seek professional help to eliminate them.

What a fascinating allegory to cybersecurity. Companies do not operate on islands unto themselves but do so in highly complex, interconnected ecosystems. While a company may practice sound cybersecurity hygiene, it must rely on its neighbors—any third party with whom it does business and has some connection to its systems—to do the same. Otherwise, it leaves itself open to insidious predators using side doors and back doors to infiltrate. (By the way, the "systems" connected in this case need not necessarily be

through extensive networks. Think back to the cybersecurity hygiene practices covered in Chapter 3. All it takes is a careless partner leaving a USB or laptop with your company's sensitive files unattended and unencrypted, and your company is exposed.)

For all the decades we enjoyed living a relatively bed-bug-free existence, we're reminded that what is old can be new again. And the more things change, the more they stay the same. We're once again lamenting bed bugs in spite of all the progress once made against them.

While change is the only constant in business, many CFOs can still rest in one certainty: They manage procurement for their companies. Since this largely remains a finance function, the CFO's kinship with the CISO is about to get a lot closer.

Just as bed bugs remind us of how reliant we are on one another to be vigilant against infiltrators, third-party relationships serve as additional points of exposure adversaries can exploit to inflict harm on our companies. Consider the following points from Ponemon[6] that reflect the sobering reality:

- 59 percent of organizations confirm they experienced a breach due to one of their third parties.
- Only 29 percent state they would learn of such a breach from the third party itself.
- 76 percent say the number of cybersecurity incidents involving vendors is increasing, yet only 46 percent agree that managing outsourced relationship risks is a priority.
- 57 percent don't know whether their organizations' vendor safeguards are sufficient to prevent a breach.

On the positive side, there's plenty of room for improvement in these metrics. Third-party security management is relatively new for many organizations. It's also critically important, as the above numbers show. CFOs carry the flag for their organizations in ensuring the procurement process sufficiently vets third parties' cybersecurity posture. Here's an area where your CISO will help you ask the right questions.

Of course, the ultimate trusted third-party relationship is one in which a company outsources a function, or part of it, entirely. Deloitte conducted a global study in 2016 examining the outsourcing lifecycle and key trends. The top function reported as outsourced? IT, with a whopping 72 percent of organizations outsourcing at least a part of the function and 31 percent planning to increase the same.[7]

It was once absurd to consider outsourcing one's cybersecurity environment. But it appears cybersecurity is following in the footsteps of its IT ancestors, as it's becoming more acceptable to let third parties protect an organization's most prized digital assets. Of course, the global cybersecurity talent shortage just adds more fuel to the fire. Rather than compete vociferously for cybersecurity talent that just isn't in the market, companies are opting to hire third parties with this expertise to at least augment internal staffing capabilities.

In particular, the areas of the security operations center (SOC) most likely to be outsourced include penetration testing (75 percent of organizations outsource), threat intelligence collection and feeds (54 percent), and digital and malware forensics (51 percent).[8]

There are several pros to outsourcing one or more areas of the cybersecurity function. As is the case with most outsourcing, companies stand to save money and minimize upfront

capital expenditures by hiring third parties with comparable cybersecurity infrastructure. Companies may also mitigate the risk of obsolescence by negotiating service level agreements with these managed security service providers (MSSPs) to dictate terms of technology refresh. Finally, MSSPs specialize in cybersecurity. They can focus on this core competency, leaving more time for their customers to focus on theirs.

As with most topics in this book, this one is imbued with several shades of gray. While outsourcing a portion of one's cybersecurity program is perfectly suitable for many companies (particularly those with harsher staffing constraints), cybersecurity is somewhat like charity—it starts at home. Abdicating complete responsibility of one's cybersecurity posture to a third party is risky business indeed. What an MSSP makes up for in cybersecurity experience, it lacks in understanding of your company's unique environment. Because of this, it may miss anomalies in your environment that a dedicated internal team would readily spot. Because an MSSP supports multiple customers (on one hand, a positive benefit since it has perspective on trends across broader markets), you may find less time dedicated to your company's needs—all of which can result in a sub-optimized cybersecurity posture should your company toss the keys over completely to an MSSP.

This is yet another area in which CFOs and their teams should exert considerable influence. Outsourcing is not bad, per se, but the terms of a relationship with a trusted MSSP must be carefully crafted to generate positive outcomes. No company cares more about your organization's cybersecurity posture than you do. This is not a case for complete abdication of cybersecurity. It's an opportunity for mutual

partnership to leverage core competencies and additional staffing for maximum gain.

W.I.S.D.O.M. for the Finance Professional

As the organization's key allocators of resources and budget, finance professionals have much to offer a culture of cybersecurity, specifically, **help CISOs and their teams speak the language of the business**. This requires losing language that doesn't fit cybersecurity—in particular, "return on investment." Once CFOs relieve CISOs of the burden to answer an impossible question, the teams can work together in earnest to define the value of cybersecurity investments to the business.

The goal is mitigating risk as efficiently as possible. There are plenty of questions to get CISOs and CFOs communicating at a different level, such as:

- What asset(s) are at risk?
- What is the strategic value of the asset(s)?
- What is the current level of vulnerability for the asset(s)?
- What are the consequences (financial damages, intellectual property exposure, reputational risk) in the event of a breach?

To ensure cybersecurity is not an aftermarket afterthought, CFOs should ask the following for business cases submitted by other leaders:

- How does the new [market, internal technology, customer product, etc.] change the attack surface for the company?

- How does it alter the risk profile of the company's most strategic assets?
- [Assuming risk is increased] What additional investment is required (one-time and recurring) to bring the risk profile to its acceptable baseline? Is this investment included in the ROI analysis?

In the way of **ensuring resources are spent as efficiently as possible, it's very fair to ask the CISO for her metrics** in the following areas:

- How much investment in cybersecurity has been made in products still sitting on the shelf (shelfware)?
- What is the plan for deploying those products?
- When was the last audit performed to ensure security products are configured properly? What were the results?
- When was the last penetration test performed? What were the results?
- When was the last cybersecurity training conducted for all employees? What were the results?

Next, as the leaders of procurement, **finance professionals lead their organizations in mitigating breach-by-association through third-party exposure**. Start with a comprehensive inventory of all third parties (something only 34 percent of organizations say they have, per Ponemon[9]). From there, conduct an audit of cybersecurity defenses and practices. The bad news is this could take significant time and effort. The good news is that the same

auditing questions can be used to qualify any new third party interested in becoming a vendor.

The questions will focus in multiple areas to assess the aspiring partner's cybersecurity posture, including:

- Looking at how the third party assesses and updates access rights and privileges.
- Understanding their business continuity process and how often they test it.
- Searching their change-control guidelines for new users and/or new software for their systems.
- Clarifying how any data passed between your company and theirs will be used, protected, and disposed of at the appropriate time (upon contract termination and/or in accordance with compliance standards).
- Knowing how they encrypt data at various states (at rest, in use, and in motion).
- Assessing how they train their employees on cybersecurity awareness and hygiene protocol.

For your most strategic suppliers, consider hiring a third party to audit their security practices once a year. Vetting suppliers is a great first step. But ensuring their security practices don't become lax once they've landed you as their customer requires even greater diligence.

Finally, be careful what you allow third parties to promote about your company. It's common practice for partners to issue press releases announcing their business arrangements. It's also normal to see companies splash the logos of all their customers, suppliers, and/or partners across their websites.

I'm a marketer, so I get it. Using the power of the ecosystem to increase brand value for all parties is generally a good thing.

But use caution. Any third party wanting to promote their relationship with your company alerts hackers to the side doors and back doors through which they may penetrate your company. It shows these parasites of the cyber kingdom how to infiltrate your company, once they know the neighbors that share one of your walls. If there is the slightest concern that one of your third parties wanting to promote their relationship with your company does not hold itself to the cybersecurity standards you require, **don't allow them to promote it**.

This is just a subset of an extensive checklist to ensure your third parties are as disciplined about securing your organization from threats as you are. If they're serious about earning your business, shouldn't they be just as inclined to protect it?

* * *

The worlds of finance and cybersecurity may not seem to fit together on the surface. But a deeper look reveals there's more in common than initially meets the eye. At its core, cybercrime is big business—something that a CFO can understand. In turn, cybersecurity is about risk management—another concept very familiar to finance types. CFOs can help CISOs speak the language of the boardroom (risk management) more fluently. In turn, CISOs can help those in procurement speak the language of cybersecurity when vetting third parties. When the two functions come together to admire their similarities and put aside their differences,

both emerge stronger from the collaboration. After all, bad actors already know the value of collaborating. Isn't it time CFOs and CISOs realized the same?

Notes

1. McAfee, "The Economic Impact of Cybercrime—No Slowing Down."
2. McAfee Labs Threat Report, December 2018, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf.
3. Alfred Ng, "WannaCry Ransomware Loses Its kill Switch, So Watch Out," CNET, May 15, 2017, https://www.cnet.com/news/wannacry-ransomware-patched-updated-virus-kill-switch/.
4. Sean Rossman, "Bed Bugs Disappeared for 40 Years, Now They're Back with a Vengeance. Here's What to Know," *USA Today*, June 21, 2017, https://www.usatoday.com/story/news/nation-now/2017/06/21/bed-bugs-disappeared-40-years-now-theyre-back-heres-what-know/399025001/.
5. Korin Miller, "You Can Have Bed Bugs and Not Know It—Here's What to Look Out For," *Self*, April 6, 2016, https://www.self.com/story/you-can-have-bed-bugs-not-know-it-heres-what-to-look-out-for.
6. Ponemon Institute, "Data Risk in the Third-Party Ecosystem—Third Annual Report," November 2018.
7. Deloitte, "Deloitte's 2016 Global Outsourcing Survey," May 2016, https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/operations/deloitte-nl-s&o-global-outsourcing-survey.pdf.
8. EY Global Information Security Survey 2018–19, https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf.
9. Ponemon Institute, "Data Risk in the Third-Party Ecosystem—Third Annual Report," November 2018.

CHAPTER

8

Mr./Ms. Cellophane (Reprise)

A very big problem for any company is that fact that their users, the business people, can just go buy stuff. They have no idea of what they're doing, nor do they really care. They look at a software package and say, "Oh, I want that. That will help me with my job." They don't care—they don't even think about the security aspects of that. And in many cases, they can load it and use it. And that is a huge risk, from a cybersecurity standpoint. And yet, stopping them is impossible.

CTO, Manufacturing Company

Lucky Amos. He may have married a cheating murderess but at least she got her just deserts, rotting the rest of her life away in prison. And as for Amos? He happily remarried. They have a beautiful family together. He found happiness and fulfillment in his career. Although he still encountered life's typical challenges along the way, he managed to emerge stronger and smarter after each one. Surer of his value. More secure in his identity. And no longer satisfied to allow society to look right through him, walk right by him, and never know he was there.

* * *

For my fellow fans of the musical *Chicago*, you know that I made up that storybook ending for Amos. In the musical, the best he can hope for is a fleeting moment of acknowledgment by his wife's seedy lawyer before exiting the stage—and story.

But he doesn't have to exit my imagination. In my ending for Amos, I'm rewriting his future. Why shouldn't he have a great life? In my mind's eye, Amos turns tragedy into triumph and reclaims his destiny. He realizes he's worth a lot more than others would give him credit for. And he compels others to recognize his value, refusing to retreat quietly to the shadows.

In the same way, I want CISOs to rewrite their future. It will require them to learn to speak the language of the boardroom. It will entail that they loosen the reins on employees to gain *more* control over their environments. And it will mandate they take up arms as the culture leaders their companies need.

A Picture Is Worth a Thousand Words

In the book *Brain Rules*, John Medina states the following, "We do not see with our eyes. We see with our brains."[1] He points to a fascinating study where wine connoisseurs were given white wine mixed with red, tasteless, odorless dye. Of course, the subjects had no idea that researchers manipulated the white wine in this way. The latter wanted to measure the power of vision in affecting all other senses. Would the aficionados rely on the combination of their other senses—including taste and smell—to spot the counterfeits right in front of their noses?

Not so much. When the wine tasters encountered the fake reds, they described their experience using vocabulary associated with authentic reds. As Medina notes in his book, "Visual processing doesn't just *assist in* the perception of our world. It *dominates* the perception of our world"[2] [emphasis mine].

Perhaps that's why our business world is brimming with visual cues. We have scorecards that reflect performance, fancy presentations to share information, and real-time dashboards that give us instant feedback on a multitude of metrics across functional areas.

When McAfee spun out from Intel as an independent company in 2017, our CEO Chris Young quickly mobilized to gather and analyze critical metrics across the company to give him complete visibility into the business. I was thrilled to showcase what the marketing and communications team was delivering on behalf of McAfee. I was confident we had at least an interesting story to share—we were gaining momentum in generating viable pipeline and our brand-building efforts were starting to bear fruit.

I dutifully submitted my team's dashboard week in and week out. Chris is a very engaged leader with a studious eye for detail. So I'd get questions from him regularly about the team's performance. Those questions would instruct what additional information we'd include in the next week's submission. And the virtuous circle continued.

Until, one day, I realized something was missing in my team's dashboards. In our case, it wasn't a data point or metric. It was the *signal*. It shouldn't come as a surprise that dashboards can fall victim to providing too much detail such that the noise drowns out the message. But that wasn't so in our case. We had judiciously pruned our metrics to ensure we weren't competing with ourselves with too many distractions.

Instead, we had created too much noise by not serving the most critical sense of all—vision—with the visual graphs included in our dashboards.

The revelation came to me by way of Chris himself. It turns out Chris has an aversion to one of the most popular charts of our time (and on my team's dashboards)—the pie chart. At first, I thought he was just being persnickety. Then I realized he wasn't alone in his derision.

A simple Google search reveals contempt for the pie chart among many. Some agree it's the Nickelback of data visualization[3] (my apologies to any die-hard Nickelback fan reading this!). If that sort of music isn't your thing and you're partial to comic book heroes, critics say it's the Aquaman of charts. As they would argue: Do you really need Aquaman when Superman can do all that he can and then some?[4]

Chris would put it more diplomatically. Pie charts often contain too much information crowded in minuscule slices with no perspective of how data has changed over time.

The pie chart does one thing—and one thing only—represent something as a portion to the whole. Other graphs, such as stacked column charts, do the same—*and* they show perspective of a trend over time.

I use this example to put a finer point on the need for CISOs to become fluent in another language—that of the CEO and the board. I certainly am not saying that CISOs are the proverbial Aquamen of Corporate America, just that they can't afford to remain experts in only their domain. To become the Supermen and Superwomen of their companies, they can learn some lessons from the pie chart:

- If vision is the key sense, then the boardroom is a 3-D IMAX® theater. The visuals must stand up. This isn't a book on presentation style. That said, the study of how the delivery of a message affects its impact goes back to the days of Aristotle. If delivering a compelling message that isn't lost in a cacophony of graphics and/or nonverbal distractions isn't your strength, avail yourself of resources to sharpen your axe in this area.[5]
- Next, CISOs are the metaphorical tourists in the boardroom. Speaking in the tongue of the native board members is on the onus of the visiting CISO.
- Besides being fluent in the typical financial metrics (revenue, profit, cash flow, etc.), the board talks in the language of risk. CISOs typically speak in the language of attacks. While the two are related, there are distinct differences, and it's up to the CISO to make the connection.

  Let me explain. CISOs have multiple frameworks for examining the threats in their environment. These models dissect the anatomy of an attack—a critically

important (and challenging) endeavor for CISOs to assess how and where adversaries maneuver. If a CISO understands the enemy's ways across the life of an attack, he can defend his organization with commensurate tactics, techniques, and procedures to evade it. And he can find vulnerabilities in his environment by applying one of several attack frameworks to his company's cybersecurity defenses.

In contrast, boards deal in risk management (e.g., What can go wrong?). They do so as part of a much larger conversation that includes corporate strategy (How will we create value?), business models (How does strategy translate into value?), and key performance indicators (How will we measure our performance?).[6]

Certainly, a cyberattack on the firm poses risk, sometimes significant. But notice that CISOs must make at least two connections to translate their language into that of the board. First, they must string the beads from risk to strategy. A risk out of context of strategic importance, value creation, or corporate measurements is the equivalent of giving the board a pie chart of your results—it only shows one small sliver of the total picture.

Second, CISOs must translate the threat into risk. This requires understanding the board's risk tolerance for high-priority assets, how a potential attack challenges this tolerance, and the consequences (financial or otherwise) that may result.

If this seems like a high bar, it is. Stanford reports that most companies do not integrate risk management and strategy. Further, 50 percent have no enterprise risk management in place.[7] The good news for CISOs? You'll be a pleasant exception to these rules when you

effectively communicate the company's cybersecurity posture in your board's language.

CISOs deserve access to the boardroom, as I argued in Chapter 2. But once a CISO gains entry, the way he crafts and delivers his message will likely determine whether he is invited to the party again. Learn the language and the style of the boardroom to avoid being cast aside, along with those one-dimensional pie charts.

Letting Go to Hold On

In 2014, enterprises were losing control. They were being engulfed by an all-out crusade; IT departments consumed by its fury; Security caught in its crosshairs. At the heart of the frenzy? Well-intentioned employees were requiring the same access to always-on, on-demand technologies in the workplace as they had come to expect at home. By 2014, the verdict was in. The "consumerization of IT" *trend* was anything but. It was here to *stay*.

That same year, IDG Enterprise researched the effect of the phenomenon on organizations. At the time, 40 percent of companies predicted the obsession for consumerized technology in the workplace would inflict negative security outcomes.[8] Their concerns were valid. Consider this slippery slope: 90 percent of organizations in 2014 reported that employees were using consumer or individual services at work—41 percent *without* IT's approval.

Not surprisingly, the organizations in question were committed to action. Over half created policies for accessing

and sharing corporate data on mobile devices and/or through cloud-based services. Roughly one-third had invested in a secure service for file sharing. Still others had implemented a sanctioned enterprise collaboration tool.

Fast-forward a few years to McAfee's 2019 Cloud Adoption and Risk Report. Rather than ask respondents for their opinions or plans for cloud consumption (cloud is a huge component of the consumerization of IT trend), McAfee checks how many files are actually secure in the cloud. (We do this by looking at the enterprise policy set on each file. For example, the enterprise determines the sensitivity of the file and we use anonymized, aggregated data to determine whether usage matches policy.)

The results suggest the runaway train of consumerized IT jumped its track a while back:

- 21 percent of all files in the cloud contain sensitive data. That figure is on the rise—up 17 percent over the past two years.
- The amount of files with sensitive data shared in the cloud has also increased—53 percent in just one year.
- 92 percent of all organizations have stolen cloud credentials for sale on the Dark Web.

In addition to the exploding consumerization of IT movement happening in 2014, there was another race afoot. Developers were using public cloud environments more and more to create applications for their companies.

This is where securing the cloud became even trickier. As CISOs know, their organizations bear more risk as they

move from software-as-a-service (SaaS) to platform-as-a-service (PaaS) to infrastructure-as-a-service (IaaS) cloud varieties. While the protection of data is consistent across all three, CISOs assume greater responsibility for securing the underlying infrastructure components of the cloud as their companies move from one to the next.

For instance, the same 2019 McAfee cloud report reveals that the average enterprise has 14 IaaS or PaaS misconfigurations currently running. What kind of misconfiguration? The kind that leaves the public cloud infrastructure—the same that must be protected to secure the enterprise's data—open for access.

To be clear, these security vulnerabilities are not laid at the feet of the public cloud providers in question. They are the fault of the companies using these services without understanding how to secure them properly. And that buck ultimately stops at the CISO.

Organizations battened down the hatches when confronted with the reality of the consumerization of IT. There's no way to know whether, in doing so, they unintentionally fueled its fire or they were simply outmatched by the genie they attempted to put back in the bottle. Said another way, did employees simply bypass the policies that frustrated their productivity? Or did the policies help curtail bad behavior only to be outstripped by cloud growth on the other side? While the answer is likely a bit of both, our McAfee research suggests organizations are losing more control of securing their data stored in the cloud than what we saw just a couple of years ago.

I've given each organizational stakeholder prescriptive advice for how she can play her part in bolstering her company's overall security. But you won't find me advising

employees to stop using the popular cloud-based services they've come to love. That's because I know that such advice will fall on deaf ears. Until enterprise IT services catch up to providing the experience of alternatives available to Joe Q. Public, employees will continue consuming the latter. They'll simply do so without IT's knowledge, let alone permission, making the challenge even greater (remember the nearly 2,000 cloud services in use unbeknownst to IT teams in the average company I mentioned in Chapter 2—evidence that "shadow IT" can cast a long shadow indeed).

Assuming the Mantle

A few months ago, there was quite a buzz at my office. Someone had posted flyers throughout with the following message, "We're going to need a bigger boat." *Jaws* enthusiasts immediately spotted the reference to the famous line from the movie. But other than that, any explanation as to what it could mean for land-dwelling McAfee employees was nonexistent.

The rumor mill swirled with wild speculation. Were we relocating to a bigger office? Were we merging with or acquiring a company? Was the parking lot expanding? (Yes, parking at the office can be challenging at times.)

Imagine our surprise when we discovered the culprits behind the message—none other than our CISO organization. The teaser campaign kicked off a companywide initiative to refresh cybersecurity awareness at McAfee. Specifically, the "bigger boat" reference was a play on words to phishing (clever!). As the CISO organization sent phishing emails to employees, some took the bait. When they did,

they were alerted to the error and encouraged to report all suspicious emails to the security team (through a convenient "report phishing" plug-in to our email application that also coincided with the launch of the campaign).

Our CISO went even further. Each member of the executive team received monthly reports on his team's performance. What percentage of his team took the phish? Of those who didn't, what percentage went the proactive extra mile and reported the suspiciously planted email to the security team?

As the campaign continued, the signage on campus shifted to reminder messages on how to spot and report phishing. Awareness across the company grew. Leaders (including me) used the reports to give our teams constructive feedback on how we could improve or where to keep up the good work.

I even found myself on more heightened alert, waiting to spot a "phish" from our security team and ready to report it immediately. In leaving my house one morning to go to work, I checked my phone for any emails needing my immediate attention. I saw one from our CEO, Chris. But I could tell immediately it was way off. It asked that I reply to him via email since he couldn't reach me via phone.

As I grabbed my keys and ran out the door, I thought to myself, *That phishing campaign at work started out so cleverly. But this fake phish from Chris really wasn't great. Too easy to spot.*

As soon as I got to the office, I dutifully reported the phish. To my surprise, I didn't get the usual congratulatory message popup from our security team saying I had passed the test. *That's odd. I'll need to let them know that their immediate response is off. Next time I see our CISO, I'll mention it.…*

But I wouldn't have that opportunity. That's because, in less than 10 minutes, I received an email from our security team. But it wasn't the "good on you for spotting the fake phish" email I was expecting. Turns out, it was a real phish I reported. Our cybersecurity team investigated it in minutes and responded with immediate steps to take in case I *had* responded (which I hadn't).

You would expect such a multifaceted campaign from a marketing or HR team. You might not immediately think of your cybersecurity team in the same light. But if our CISOs and their teams don't assume the mantle of evangelizing culture, how can they expect their business counterparts to do the same with cybersecurity? CISOs must meet them more than halfway if a culture of cybersecurity is to take root.

W.I.S.D.O.M. for the Cybersecurity Professional

CISOs have a wealth of resources on best-in-class practices in their trade. This W.I.S.D.O.M. isn't for those looking for deep-dive technical advice. That makes it no less important. This prescription is about connecting your value to that of the business. It requires CISOs to both cover the basics and stretch beyond their departmental walls.

Sound cybersecurity hygiene is nonnegotiable. CISOs must ensure the basics are covered and cybersecurity hygiene is at the top of that list of "things to do." This is a case where common sense isn't always so common. In one of the biggest breaches to date, the failure was due to a known vulnerability that was unpatched. Even more interesting about the postmortem on this attack: The email roster

used to notify security administrators of the vulnerability neglected to include those who "needed to know." So the unpatched vulnerability caused the breach. And an out-of-date email distribution group of security administrators led to the unpatched vulnerability. It's just one notable example of how the devil truly is in the details for cybersecurity professionals.

Because your infrastructure continues to expand both physically and virtually, sound patching requires an inventory of all possible servers in use or otherwise. Zombie servers, those that haven't been used in at least six months, are an example. They can make up a significant percentage of an enterprise's infrastructure. Up to 30 percent of all virtual servers are comatose.[9] Since nobody is using them, it's also likely that nobody is actively securing them.

You can't secure what you can't see. Your people also can't patch what you don't promote. In addition to an inventory of all assets and their patch status, review your internal communications plan for notifying administrators of a vulnerability.

Staying on hygiene, inventory your cybersecurity defenses for shelfware. When you find a defensive technology your company purchased but has not installed, find out why. Is the solution no longer needed? Or has time not been on your organization's side to implement it? If the latter, work the project plan with your own team or with a professional services company to ensure your precious investment is not rotting on the shelf (and leaving you exposed, to boot!).

Next, configurations matter. You could have the best hygiene in patching vulnerabilities. You could be second-to-none in installing all cybersecurity technologies you

purchase. But if you've improperly configured your security products, hackers will crawl through the gaps. While you're inventorying your patch status, your notification lists, and your shelfware, take stock of the configurations on your existing products to ensure nothing has changed since the last time you looked at them (which may go as far back as when your organization first installed them).

Additionally, back up your data. While backed-up data won't protect you against all attack varieties (data exfiltration being a prime example), ransomware is ineffective against organizations with regularly backed-up data and systems. With a *robust* backup system in place, it's possible to ignore ransomware demands and restore all files with relatively low downtime. It's worth evaluating which of your assets you simply cannot do without, and then determining how to back up the data and systems to an acceptable degree.

Of course, backups are useful for other reasons, like being able to restore an earlier configuration or earlier version of a document. This can be particularly helpful in the case of data weaponization, where hackers manipulate data for deception or other reasons. Having regularly archived records allows an organization to retrieve an earlier, accurate version of the data if necessary.

Make sure to test your backup system periodically to ensure the data you've been archiving is, in fact, being stored—yes, this type of backup failure has been known to happen. Use encryption to securely back up all data—yes, at least one company received a black eye for its nonencrypted data logs.

If you find yourself in a cybersecurity department that is not directly aligned with your brethren in IT, maintaining sound hygiene is exponentially more difficult. Unfortunately,

the relationship between CISOs and CIOs sometimes resembles that of feuding family members more than kissing cousins. As cybersecurity has moved into adolescence, it has struggled to create and maintain an independence separate from its IT parent.

Much of the conflict arises from competing objectives between cybersecurity and IT teams. IT is about keeping critical systems running and deploying technology in support of the business. Cybersecurity is about protecting the organization's assets. Sometimes, those outcomes may be at odds with one another. For instance, a CISO may stall or stop a technology that poses a risk to the organization. A CIO may resent this barrier, particularly if his incentives are aligned to a timely deployment schedule.

There has been much debate through the years as to the ideal CIO/CISO relationship. In 40 percent of companies, the CISO reports to the CIO, rather than to the CEO or CFO.[10] Some criticize this relationship, citing organizational conflict as a key concern. Still others have argued that such a structure statistically results in more downtime and higher financial losses due to cybersecurity incidents.[11]

What this age-old debate reveals is that CISOs and CIOs must be aligned within the spirit, not simply the letter, of the law. **This requires CISOs to engage CIOs on metrics and goals**, regardless of whether the former reports to the latter or the two are peers sitting around the same table. In particular, the roles and responsibilities for proper cybersecurity hygiene—including patching, backups, multifactor authentication, and the like—must be established and agreed upon at the beginning of each planning cycle. If the two functions share a budget, the leaders must identify and

allocate what portion will serve IT versus cybersecurity. In addition to run-rate budget carveouts for each, perhaps any new IT project is ascribed a cybersecurity tax to fund and protect new technologies. As discussed for other functions, CISOs and CIOs should agree to key performance indicators (KPIs) and service level agreements (SLAs) to prioritize efforts and resolve disputes when they arise.

Finally, managing this list alone is challenging work (it's one of the reasons cybersecurity hygiene is so difficult to practice). Conduct regular penetration testing on your environment, preferably using third parties. These companies will help you find unknown vulnerabilities (in your cybersecurity hygiene or in otherwise lacking defenses) before bad actors do.

Next, **invest in technologies that drive your business value up and that of your adversaries down**. Specifically, businesses are moving to the cloud. More importantly, employees are moving to the cloud. So unless your organization is completely restricted (and some, such as large government agencies, are), chances are you won't be able to stop employees from accessing potentially dangerous applications or services in the workplace.

If you can't beat them, join them. Rather than resist the move to cloud, embrace it. Consider Cloud Access Security Brokers (CASB) as one potential solution. Essentially, CASB technologies give security organizations visibility of and control over cloud services in use by their organizations (sanctioned or otherwise). They can detect security configuration errors in cloud controls (such as a publicly readable and/or writeable storage bucket). They may allow organizations to set consistent security policies

across any cloud environment. In short, they allow organizations to secure the popular cloud services employees are using. And they allow CISOs to support their companies' transformation agendas while ensuring security remains at their center.

Now, about impacting your adversary's value negatively. I said earlier that there's no such thing as playing offense in cybersecurity. That's true. Defenders, by their very definition, don't strike first. But they can still confuse their enemies.

The art of deception in war goes all the way back to Sun Tzu. In cybersecurity, carefully disguised decoys that appear to be treasure troves planted in your infrastructure do a few things. First, they give you additional data points through which to track your enemy's patterns. Second, they distract your enemy from the real treasure you are interested in protecting. Finally, they waste your enemy's time and resources on wild goose chases. This last point is really about as close to playing offense as cybersecurity teams can get.

Use artificial intelligence (AI) capabilities to identify the most advanced threats and address the talent shortage—but know its limitations. AI is the latest buzzword technology in cybersecurity. To be sure, it promises to help cyber defenders find the most sophisticated threats in their environment quickly, pairing the scale of machines with the problem-solving capabilities of humans. But beware of cybersecurity marketers disguised in sheep's clothing. While AI promises to help strapped CISOs do more with less, it comes at a cost—false positives. Given AI uses sophisticated analytics to determine the likelihood of a threat, it renders a probability, not certainty, that one in fact exists. That means AI will be wrong at least some of the time.

On the flip side, those tried-and-true signature-based detection models I mentioned in Chapter 2 can also be wrong. A zero-day threat that has not yet been identified has no signature in a threat database. If your organization is unfortunate enough to be Patient Zero, that false negative can cause real harm. While AI may find the zero-day threat overlooked by signature detection, it does so by also capturing false positives (there's no such thing as a perfect detection model).

You may think that false positives are a lot less harmful than false negatives. It depends on how you look at it. False positives divert a security organization's limited time and attention away from true positives. Much like the deception technology I mentioned earlier distracts adversaries, false positives are a considerable drain on an organization's cybersecurity resources.

A Ponemon study[12] explored how insidious false positives can be. The average organization faces 17,000 threat alerts weekly. Of those, a mere 19 percent were deemed worthy for action. Ponemon concluded the average large company spends $1.3 million chasing false positives—equivalent to almost 21,000 hours of wasted time.

Adding to the complexity of this topic is a new threat category called adversarial machine learning (AML). Bad actors are at it once again, innovating in ways to create chaos or harm for their victims. With AML, adversaries manipulate inputs to otherwise sound machine learning models. The "garbage-in, garbage-out" premise applies as much in the realm of cybersecurity as in any other realm of IT. A machine learning model is only as good as its inputs. If the inputs are faulty (or tampered with), the model's accuracy suffers.

At a recent tradeshow, McAfee showed how the slightest changes to pixels in an image, imperceptible to a human eye, could confuse a machine learning model into classifying a picture of a penguin as…a frying pan! Frying pans and penguins may be harmless in the real world. But imagine the same poisoning of pixels in a digital stop sign that an autonomous car now registers as a speed limit sign, and you can imagine how dark the use cases in this area can get.

Enemies can potentially inflict the same confusion to malware classification engines. By introducing slight variants to highly sensitive machine-learning models, adversaries can disorient cybersecurity professionals. They can slam these first responders with a rash of false positives, perhaps deadening their sense of urgency to respond in the process (in much the same way nuisance fire alarms have been shown to do in multi-tenant buildings[13]). Then, when the adversary is confident her victim's shields have been lowered, she wages her real assault.

AI, like any technology, is a weapon in both your company's cybersecurity arsenal and your enemies' arsenals. It doesn't mean we should avoid AI. Rather, we need to understand its potential and limitations.

For example, there's no avoiding the talent shortage. On one hand, AI allows cybersecurity defenders to address more threats by delegating to machines tasks that would otherwise require human intervention. That said, AI will also increase false positives and is subject to adversarial poisoning. If either of these possibilities is left unattended, AI will sap some of the productivity gains it created in the first place. Threats come in all varieties. Defenses must do the same. This problem requires teaming humans with machines.

It also requires pairing various threat detection models—artificial intelligence and signature-based—to maximize efficacy and minimize the occurrence of false positives.

Finally, **carry the culture flag for cybersecurity** at your company. This requires two efforts. First, a CISO has to be able to speak the language of the board. Boardrooms speak the language of risk—and it's always connected to company strategy. Work with business unit leaders, your CFO, and CEO to identify and prioritize the most strategic assets in the company. For each, identify the consequences of a breach. Finally, provide its current vulnerability. Immediately prioritize the high-priority/high-vulnerability assets for get-well plans. When invited to the boardroom, use this framework as your guide to define how your cybersecurity strategy maps to that of the broader company.

In addition to spreading a culture of security vertically, do so horizontally through the organization's employees. Take up arms with your HR counterparts in delivering effective training to raise employee awareness in their roles (just like McAfee's CISO did with his phishing campaign). Find a way to make cybersecurity more than just an annual training event or a checklist of questions employees answer upon joining the company. Hire a communications expert on your team, working with your marketing department to define the role and skill set for the position. Have your communication ambassador work with Marketing and HR to develop effective internal campaigns that make cybersecurity part of everyone's day job.

* * *

It's time for CISOs to embrace their role at the executive table. It's time they nurture a cybersecurity culture that extends far beyond IT. It's time for new partnerships with key stakeholders—namely HR and Marketing—to drive cybersecurity awareness up and security vulnerability down. It's time to rewrite the end of the CISO's story. Thanks to many progressive CISOs already leading the way, the rest of the cast need not imagine their storybook ending. It's already becoming a reality.

Notes

1. John Medina, *Brain Rules: 12 Principles for Surviving and Thriving at Work, Home and School* (Seattle, WA: Pear Press, 2014).
2. Ibid.
3. https://twitter.com/WaltHickey/status/345646754089291777.
4. Walt Hickey, "The Worst Chart in the World," *Business Insider*, June 17, 2013, https://www.businessinsider.com/pie-charts-are-the-worst-2013-6.
5. One of my favorite presentation books of all time is *Presenting to Win: The Art of Telling Your Story* by Jerry Weissman. If you don't have time or budget for professional coaching, the book is an invaluable resource in providing tricks of the trade for telling an effective story.
6. David F. Larcker and Brian Tayan, Corporate Governance Research Initiative, "Strategy & Risk Oversight," Stanford Business Corporate Governance Research Initiative, https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/cgri-quick-guide-06-strategy-risk-oversight.pdf.
7. Ibid.
8. IDG Enterprise, "2014 Consumerization of IT in the Enterprise," https://www.scribd.com/presentation/212942014/IDGE-CITE-2014.
9. Patrick Thibodeau, "A Third of Virtual Servers Are Zombies," *Computerworld*, May 12, 2017, https://www.computerworld.com/article/3196355/a-third-of-virtual-servers-are-zombies.html.

10. Jody R. Westby, "Governance of Cybersecurity: 2015 Report," Georgia Tech Information Security Center, October 2, 2015, https://globalcyberrisk.com/wp-content/uploads/2012/08/GTISC-GOVERNANCE-RPT-2015-v15.pdf.
11. Bob Bragdon, "Maybe It Really Does Matter Who the CISO Reports To," *CSO*, June 20, 2014, https://www.csoonline.com/article/2365827/maybe-it-really-does-matter-who-the-ciso-reports-to.html.
12. Rishi Bhargava, "False Positives Have Real Consequences," *Light-Reading* SecurityNow, June 22, 2017, https://www.securitynow.com/author.asp?section_id=613&doc_id=733939.
13. G. Proulx, J. C. Latour, and J. W. MacLaurin, "Housing Evacuation of Mixed Abilities Occupants," IRC-IR-661, Internal Report, Institute for Research in Construction, National Research Council of Canada, 1994.

CHAPTER

9

Experiencing a Culture of Security

I think that my office is too soft with cybersecurity. If someone really wanted to, I think they could obtain sensitive information easily by tricking unaware employees or through unprotected company networks.

Respondent, McAfee Online Ethnographic Study

As I begin writing this chapter, I do so from the most unnatural of places that has become strangely familiar to me—roughly 35,000 feet above the earth's surface in a tube weighing more than 50 tons and traveling nearly 450 miles per hour. I'm en route from Tampa to Dallas after a long weekend of visiting family. Travel for me has become ordinary. I'm not

one to consider myself a road warrior by most definitions of the phrase, but I still easily log more than 100,000 miles in a year—worthy enough to earn elite traveler status from my preferred airline to make the routine a bit more bearable.

Even though I'm struck by just how mundane travel has become in my life, I still consider myself a bit of a nervous traveler. For instance, leading up to a trip, I fixate on what I'll pack for the visit (whatever it is and for however long the trip, it must fit in an airline-approved carry-on suitcase, since checking baggage is simply out of the question). On the day of travel, I check for my identification, wallet, and cell phone several times before I leave for the airport. (I have a healthy dose of anxiety that I'll arrive at the security checkpoint only to find I've left one of these essentials behind.) I give myself plenty of time to make it to the airport since sprinting through a terminal, breathlessly dragging myself and my carry-on luggage through crowds of fellow passengers to make my flight *just in time* is simply not my idea of a *good time*. Then, when I do get to my gate, I wonder if the flight will be on schedule given I'm usually rushing to a meeting as soon as I'm supposed to arrive.

These thoughts are like a perennial playlist of worrisome possibilities I set to repeat in my brain every time I travel. But notice what track isn't on the list. For all my fretting, there's one concern conspicuous by its absence. That is, I don't worry about my safety. I don't actively think about whether getting in a 50-plus ton tube hurling itself roughly seven miles above the earth is a good idea. I assume that it is. And I join the ranks of four billion passengers worldwide who do the same each year.[1]

How far I've come from my very first flight. I was a 20-year-old intern with INROADS, a nonprofit organization that gave me my start in Corporate America. I was on my way from Tampa to Atlanta for a special INROADS retreat with my friends and fellow interns. I boarded the plane and took my seat *way* in the back—next to the lavatories, which I thought was great luck since I'd be extra close to the restroom should nature call. How convenient!

As the flight attendants were giving safety instructions that my ears were hearing for the first time, I dutifully began to comply with buckling my seatbelt. Only it didn't buckle. After a few failed attempts and asking the passenger next to me for assistance, it was clear: My seatbelt was broken. I remember thinking to myself, *Oh well. I guess seatbelts are sort of optional, kind of like they are on a school bus.* I didn't think twice to mention it. And the flight attendants didn't look twice to confirm I had securely fastened it.

Of course, after logging millions of miles in the air, I know how egregious a broken seatbelt is. Today, I wouldn't consider taxiing the runway, let alone leaving the ground, without a properly fitting belt secured firmly about my waist. (As an aside, that airline I took on my maiden voyage eventually went out of business. At the heart of its ultimate derailment? Serious safety concerns.)

I now know what safety looks and feels like on a plane and in an airport. And I'm well aware of the behemoth infrastructure that assures me one primary right as a passenger: a safe experience. That's not to say that airplanes don't crash. But, at the same time, I needn't settle for anything less than a safety standard rigorously upheld in air travel—and, yes, an effective seatbelt certainly qualifies on the list.

There's a reason that air travel remains the safest mode of transportation—more than 100 times safer than the automobile.[2] There's a culture of security that permeates every facet of the airline industry.

That statement may not strike you as extraordinary. You might think that safety should be at the heart of air travel. After all, the industry exists to transport precious cargo—in this case, human lives—from one place to another. You'd only be partially right. In fact, the commonplace nature of security that has become so threaded into the very fabric of air travel belies its virtually nonexistent beginnings in the industry.

When we think of the good ol' days of flight, our minds conjure up images of fashionably attired passengers, doted on by service-conscious flight attendants, on luxury liners with legroom to spare and haute cuisine served in the friendly skies. What that nostalgic image lacks is any reality to the dangers of flying back in those days. Passengers suffered a fatality rate nearly four times today's average[3] given a "culture of security" that was anything but. Consider this punch list of safety concerns passengers faced at one time or another during the history of commercial airline travel:

1. Mid-air collisions and deadly landings were far more common thanks to technology that left much to be desired for flying or landing an aircraft in inclement weather.
2. Engines dropped out of planes so often that the incidents weren't even recorded as accidents, provided the other engine could land the plane in a clutch.

3. Inferior seatbelt designs and lower cabin ceilings meant a healthy dose of turbulence could result in more than a tossed lunch—it could lead to a snapped neck.
4. About that turbulence. It was much more common on planes of yesteryear that lacked pressurized air cabins to allow flight at higher, safer, and more comfortable altitudes.
5. Trips to the airplane lavatory were perilous for the less-than-sure-footed passenger. Stumble and you might find yourself landing on the sharp edge of a chair or table, yet another dangerous element in the environment contributing to injury or death.
6. Glass dividers separating first-class and coach passengers were lovely to admire. They could also shatter and spray customers in an accident or turbulence.
7. You could light up on a plane. Secondhand smoke added to the in-flight ambience.
8. If cigarettes, faulty wiring, or unapproved cargo (such as chemical oxygen generators—yes, this really did happen) resulted in fire, no smoke detectors or fire extinguishers on board would give warning or resolution, respectively.
9. Forgot your identification at home? No worries. It wasn't needed to board a flight.
10. Even when identification became a requirement, there was no need for the name on the ticket and identification to match.
11. Carrying a weapon onboard? Flight attendants might have even helped you stow it away for safekeeping in an overhead bin.[4]

12. There was no security check of checked bags on domestic flights.
13. There was a security check of checked bags on international flights—*sometimes.*
14. Box cutters, knitting needles, scissors, and baseball bats? Welcomed accoutrements on a plane.
15. The more, the merrier. Passengers could (and regularly did) bring loved ones all the way to the gate to say their farewells.
16. Visiting the cockpit was a treat for the lucky passenger. You might have even earned your "wings" in doing so.
17. While visiting that cockpit, you would meet a pilot with one-sixth the flying experience[5] required of those who inhabit it today.
18. That pilot would also likely be more fatigued, compliments of more lenient rules on minimum mandatory rest requirements for aviators.
19. Those safety instructions we now take for granted? Much less stringent in the early days of flight. Things like dimming the cabin and raising the window shades upon takeoff and landing are relatively recent additions to passenger welfare, given both allow air travelers to adjust their sight to the ambient conditions they may encounter in a crash.
20. The Transportation Security Administration (TSA) that screens more than two million passengers and crew daily? It didn't exist before 2001.

Those are just 20 examples of how far the safety of air travel has come through the decades. And I haven't even scratched

the surface of all the changes made in a post-9/11 world that forever altered the complexion of commercial flight.

These changes didn't happen overnight. They are the result of an industry, under siege by adversaries (environmental and human alike), pressured to steadily raise the bar on security over time. While we may be nostalgic for simpler times, when airport security was virtually nonexistent, many of us will also never know the terror that once threatened the freedom of flight. If you're like me, you can't imagine boarding a flight with a perpetual fear that it could be diverted or doomed, not by turbulence or inclement weather, but by a hijacker bent on personal or political gain.

Yet, that image—which has become the fare of big box-office action movies—was once a sobering reality for travelers during what has been dubbed the Golden Age of Hijacking. Skyjackers commandeered over 130 planes in American airspace between 1968 and 1972, often at a pace of one or more per week.[6] The hijacking "virus" was a raging epidemic. Media covered this dark reality of air travel with equal fervor. As psychiatrists interviewed hijackers, they discovered a mentality of one-upmanship. Would-be skyjackers, enamored with widespread news coverage of the latest airplane seizure, would think to themselves, "I can do better than that; I can improve upon that."[7] So the contagion spread.

It's hard to believe, but hijacking became such a common occurrence during those years that passengers simply accepted it as part of the air travel experience. In 1968, *Time* somewhat poked fun at the hijacking plague with an article aptly titled, "What to Do When the Hijacker Comes." In it, the journalist reports of more than 1,000 Americans diverted to Cuba over the previous eleven months. While

"pilots carry maps of Havana's Jose Marti Airport just in case, and stewardesses are instructed not to argue with would-be hijackers—simply to obey their orders…nobody has yet thought to brief the poor passengers."[8]

The author graciously obliges with some dos and don'ts should one find herself an unwitting passenger on a hijacked plane—like don't be aggressive, don't panic, don't push the call button (lest the ding startle the hijacker causing him to unintentionally discharge his weapon), and don't call aloud for the "stewardess." When the flight arrives in Cuba, the journalist suggests two dos: Do stay calm and do enjoy the stay (the article even offers some helpful details on comfortable overnight accommodations in the area).

How did airlines handle the persistent threat? They complied with the hijackers. If a skyjacker wanted to land in Cuba (or anywhere else), pilots would divert the flight. All cockpits were equipped with maps of the Caribbean Sea, regardless of a flight's intended destination, given the popularity of Cuba as a hijacking destination at the time. Further, pilots were given popular phrase cards in Spanish to help them communicate with Cuba-bound skyjackers (such as learning how to say "I must open my flight bag for maps" or "Aircraft has mechanical problems—can't make Cuba").[9] If the perpetrator wanted money, airlines would pay the ransom and hope for its return upon the subject's arrest. Airlines fought tenaciously to protect their existing lax security controls, outright resisting deterrents like metal detectors that would thwart skyjackers since they didn't want to subject their paying guests to the same scrutiny.

Unbelievably, airlines so refused the concept of imposing security restrictions that they even considered building a

fake airport in southern Florida resembling Cuba's own as an alternative to metal detectors and the like. Under this proposal, pilots would land at the decoyed airport, where federal agents would await the suspect's arrival.

Due to cost, the fake airport idea was jettisoned in favor of behavioral profiling instead. Ticket agents would give passengers a once-over for any one of roughly 20 possible behavioral warning flags of a potential hijacker in disguise. To put passenger convenience above security, the profiling would apply to less than 1 percent of all travelers, leaving more than 99 percent unencumbered.

Airlines didn't readily embrace the culture of security I credit them with today. In fact, they accepted these human adversaries in their environment and developed practices to work with them. The security controls now all too common did not initially conform to the airline industry's paradigm of an optimal customer experience. At the time, the rationale for complying with terrorists rather than securing the airways seemed sound. It was the first time that air travel had moved from the elite upper crust to the mass-market traveler. Security delays that cost travelers as little as 15 minutes in extra time could be sufficient incentive to stimulate alternate modes of transportation. It was a risk the relatively fledgling industry couldn't afford to take.

Until November 10, 1972, when hijacking moved from the realm of minor inconvenience to that of national threat. Three hijackers threatened to crash a plane into an atomic reactor at Oak Ridge National Laboratory in Tennessee. The Federal Aviation Administration (FAA) took the measure that airlines had abdicated. In January of the following year, all passengers would undergo physical

screenings, including passing through metal detectors and having their bags searched.

Adversaries are nothing if not determined and innovative. When hijacking proved more difficult thanks to the imposed airport screening, perpetrators turned their attention to aircraft bombs. When security measures were improved in the 1990s to defend against that threat vector, terrorists topped themselves on September 11, 2001, carrying on permissible box cutters to commandeer and use commercial airliners as self-guided missiles (reminiscent of that failed hijacking in 1972 threatening the same).

At every turn, the airline industry has responded with additional security measures.

- December 22, 2001: Onboard passenger Richard Reid attempts to detonate an explosive in his shoes. Five years later, the TSA mandates removal of shoes at security checkpoints.
- August 9, 2006: Officials bust a conspiracy to bring down airplanes with liquid explosives. On September 26 of the same year, TSA bans carry-on liquids of more than 3.4 ounces that can fit in a quart-size clear plastic bag per passenger (now known as the 3–1–1 requirement).
- December 25, 2009: Onboard passenger Umar Farouk Abdulmutallab stuffs an explosive in the most intimate of areas—his underwear. Passengers are soon treated to controversial virtual strip searches at airports, courtesy of "backscatter" machines.

This cat-and-mouse game will persist. When the next threat emerges, the airline industry will respond with

security controls designed to inoculate it. While passengers may grumble at the inconvenience, they'll also accept a new normal that is, at its heart, designed with security at its core.

It's the reason I point to the airline industry as the poster child for executing a culture of security. That's not to say airlines willingly abided by all the controls that keep us safer, if not somewhat inconvenienced, today. There was plenty of resistance in the earliest days when the industry and its passengers viewed hijacking as a nuisance, not a threat.

But consider the following list as a subset of what must happen today before an airplane is cleared for takeoff. Should any of these items be lacking, passengers can expect a delay, if not cancellation of the flight:

1. A preflight check includes an exterior walkaround and visual inspection of critical components, including sensors, probes, and exposed motors and cables, such as those found in the landing gear.
2. The preflight check also encompasses an interior testing of critical systems, like fire detectors, weather radar, and warning lights.
3. The maintenance crew performs any required maintenance, based on a schedule for the aircraft. The least invasive, and most frequent, of these checks occurs every 500 flying hours. The most extensive of these checks happens approximately every six years and is so expensive that, in many cases, the airline simply retires the aircraft instead.
4. The maintenance staff keeps a detailed inventory of the operational state for all inventory onboard. If there are any concerns, the maintenance team decides whether to

fix or defer the problem. This depends on the minimum equipment list the airplane must have in working order to be airworthy. If the aircraft doesn't meet the requirements, it stays put.

5. The pilot reviews the minimum equipment list and deferred items to be aware of the maintenance state of the aircraft before takeoff.
6. Ground handlers check the plane for damage and the runway for any debris or obstacles that could impede it as it taxis out.
7. Pilots and flight attendants huddle for a pre-departure check, where the flight plan, weather report, expected turbulence, and more are discussed to facilitate a smooth and safe experience for all.
8. Air traffic controllers ready the flight plan, considering weather patterns and airport constraints, among other factors.
9. Passengers arrive at the airport in time for security checks. Those clearances, including verifying the passenger is not on a watch list, start long before the day of flight.
10. Travelers provide a government-issued photo identification with the name matching that of the ticket.
11. Checked baggage is screened—*all the time.*
12. Passengers not enrolled in a special program (such as TSA Pre-Check) remove laptops, shoes, outer jackets, and 3–1–1 compliant liquids from carry-on luggage.
13. All carry-on luggage undergoes an x-ray, if not physical, search.

14. Metal detection, millimeter wave body imaging, and/or a physical pat-down check for contraband is conducted on each passenger.

These safety checks, including security screenings, can be even more extensive for international flights arriving in the United States.

Critics will be quick to point to the shortcomings of these security assessments in safeguarding passengers. They will highlight the TSA's failure rate in its own penetration tests, where at least 70 percent of illegal contraband slipped through its cracks in 2017.[10] Indeed, no security posture is perfect, and the airline industry is no exception to the rule.

Instead of criticizing, let's consider the track record. More specifically, let's look at the critical outcome that many would likely agree is most important—the safe transport of passengers. On this metric, the airline industry has performed quite well indeed.

In 2018, the Aviation Safety Network reported a fatal accident rate for large commercial flights at .36 per million flights. That equates to one fatal accident for every three million flights.[11]

Some countries, like the United States, saw an even lower fatality rate. From 2009–2018, U.S.-operated airlines flew several billion people on almost 100 million flights, with no fatalities.[12]

These results speak for themselves. They give me confidence as a frequent traveler that I'm much more likely to die of cardiovascular disease, in a car accident, from a lightning strike, or even a bee sting,[13] than I am to surrender my life on an airplane. I may have worries about packing the wrong

items or leaving my identification at home, but I don't fret about my safety. That's because I know the airline industry is ensconced in security. The public and private sector have united with one goal in mind: keeping travelers safe.

Perhaps your company isn't in the business of preserving lives. Or perhaps your industry hasn't yet seen its equivalent "Golden Age of Hijacking." Maybe your company hasn't yet experienced its metaphorical 9/11. I'm hoping that it doesn't need to in order for you and every other employee and board member to put security in its proper place.

To move security from the back office to the boardroom.
To equip every employee to play a part in securing his company.
To stop the line on product development when security is lacking.
To bridge the gap of the cybersecurity talent shortage.
To respond immediately and transparently when breaches occur.
To thread security across a vast ecosystem of third parties.
To place a culture of security in every workplace.

Will these prescriptions spare your company from ever suffering a breach? Certainly not. But will they deliver positive outcomes that allow your company to mitigate risk and recover from attacks more effectively? Absolutely.

For all my praise of the airline industry's track record, even it is not immune from a threat-free existence—human or otherwise. Just days before my brief hometown visit to

Tampa, there was devastating news of an Ethiopian Airlines crash that killed all 157 on board. My mom is not a frequent traveler. She is, however, a frequent watcher of cable news networks. She called me in the days leading up to my trip.

> "Allie, I'm worried about your trip out here. What type of aircraft are you on?"
>
> "Mom, I don't know. What are you watching and why are you asking?"
>
> "There's a report that the Ethiopian Airlines crash looks similar to another one from a few months ago. They were both on a 737 MAX plane. Is that your plane?"
>
> "Mom, please stop watching the news. I'm fine. I'm much more likely to die in a car accident than an airplane." (More blah, blah, blah on airline safety records, much of which didn't penetrate my mother's extraordinary defenses against hearing anything that would alleviate her fears.)
>
> "Babe, I just need to know if you're on one of those jets. If so, let's reschedule."

Turns out I didn't need to reschedule. And I also didn't need to check the aircraft of my flight. The day before my scheduled departure, the FAA grounded all Boeing 737 MAX 8 planes. That culture of security that envelops every facet of an airline industry I use regularly once again put my safety first.

While I may not have second-guessed the potential danger, the FAA's actions weren't lost on my mom. The night before my flight, she called me to confirm my arrival details.

"Allie, I'm so glad we didn't need to reschedule your flight. Thank God they grounded all those airplanes."

"Yes, Mom. Thank God, indeed."

And, thank the airline industry for showing us what a culture of security can be—definitely not perfect but certainly strong enough to deter formidable adversaries and allay the concerns of even the most paranoid among us. Including my loving mom.

Notes

1. https://www.statista.com/statistics/564717/airline-industry-passenger-traffic-globally/. To clarify, this statistic refers to the number of airline passengers per year. So a frequent traveler like me would count multiple times in the number.
2. Ian Savage, "Comparing the Fatality Risks in United States Transportation across Modes and over Time," *Research in Transportation Economics* 43 (2013): 9e22.
3. John Brownlee, "What It Was Really Like to Fly During the Golden Age of Travel," *Fast Company*, December 5, 2013, https://www.fastcompany.com/3022215/what-it-was-really-like-to-fly-during-the-golden-age-of-travel.
4. Christopher Balderas, "Welcome to the Future: 20 Ways Air Travel Has Changed Since the 1950's," *The Travel*, June 28, 2018, https://www.thetravel.com/welcome-to-the-future-20-ways-air-travel-has-changed-since-the-1950s/.
5. Leslie Josephs, "The Last Fatal US Airline Crash Was a Decade Ago. Here's Why Our Skies Are Safer," CNBC, February 13, 2019, https://www.cnbc.com/2019/02/13/colgan-air-crash-10-years-ago-reshaped-us-aviation-safety.html.
6. Brendan Koerner, "How Hijackers Commandeered over 130 Planes—in 5 Years," *Wired*, June 18, 2013, https://www.wired.com/2013/06/love-and-terror-in-the-golden-age-of-hijacking/.

7. Libby Nelson, "The US Once Had More Than 130 Hijackings in 4 Years. Here's Why They Finally Stopped.," *Vox*, March 29, 2016, https://www.vox.com/2016/3/29/11326472/hijacking-airplanes-egyptair.
8. "What to Do When the Hijacker Comes," *Time*, December 6, 1968, http://content.time.com/time/subscriber/article/0,33009,844656,00.html.
9. Koerner, "How Hijackers Commandeered over 130 Planes."
10. Summer Meza, "TSA Fails to Spot Weapons More than Half the Time," *Newsweek*, November 9, 2017, https://www.newsweek.com/tsa-fails-half-time-706568.
11. David Shepardson, "Fatalities on Commercial Passenger Aircraft Rise in 2018," Reuters, January 1, 2019, https://www.reuters.com/article/us-airlines-safety-worldwide/fatalities-on-commercial-passenger-aircraft-rise-in-2018-idUSKCN1OW007.
12. Lea Lane, "Reality Check After the Southwest Airlines Fatality: Shocking Stats on Flying, Health and Safety," *Forbes*, April 18, 2018, https://www.forbes.com/sites/lealane/2018/04/18/reality-check-after-the-southwest-airlines-fatality-shocking-stats-on-flying-health-and-safety/#1205e3117a46.
13. Ibid.

CHAPTER

10

A Culture of Security for All

A part of governance, risk, and compliance campaigns is "setting a tone from the top." Executive management should point out different types of cybersecurity threats and how they can be recognized. It should then be clear on what part IT plays in preventing the cyberattacks, and what part everyone else plays. Right now, I don't know where this line is drawn. In the arena of cybersecurity, what should I worry about versus what is IT tasked with preventing?

Respondent, McAfee Online Ethnographic Study

The headline for the short article was barely noticeable, buried at the bottom of the page, along with a feature on

the upcoming high school football game. Those who looked closer may have dismissed it outright as hysterical doomsday prophesy, "Is World Series Quake Coming?" Four days later, the magnitude 6.9 Loma Prieta earthquake struck, killing 63 people in its wake, causing billions of dollars in damage and disrupting Game 3 of the World Series at Candlestick Park.[1]

Earthquakes are terrifying specters of nature. Every day, several hundred occur worldwide, though most of us don't even notice them. They're relatively small in nature—magnitude 2 or less. Major earthquakes, greater than a magnitude 7, happen more than once a month. Great earthquakes of at least a magnitude 8 hit about once a year. Unlike their smaller siblings, we notice these major and great quakes. Even if we're lucky enough to be spared Mother Nature's wrath, the media ensures we recognize her devastation by filling our screens with the images of fallen buildings and victims in her path of destruction.

What makes earthquakes terrifying is their certainty. There's no getting around an earthquake happening. Earth is active. Its plates are shifting. There's no escaping this phenomenon.

And yet, for all their certainty, earthquakes are completely unpredictable. There's no way to forecast an earthquake. That single point of distinction separates earthquakes from other natural disasters, like hurricanes, tornadoes, and floods, where scientific models can help people avoid a deadly strike.

Not so with earthquakes. They hit without warning. The United States Geological Survey (USGS) makes the point unequivocally clear on its website: "Neither the USGS nor any other scientists have ever predicted a major earthquake.

We do not know how, and we do not expect to know how any time in the foreseeable future."[2]

So when Jim Berkland, a county geologist, provided that unbelievably accurate (or extremely lucky) prediction of the mag-6.9 quake that rocked Loma Prieta back in 1989, those who missed the obscure headline days before were certainly taking notice of it after the dust settled.

Berkland used scientific indicators, like the presence of high tides and position of the moon to inform his predictions, of which Loma Prieta was one of 300 he had made in the past 15 years. In addition, one more data point Berkland included in his black box to calculate the probability of the quake was the number of missing animals as reported in local pet classifieds leading up to the event. His theory in including this unconventional metric? Pets run away when sensing an impending earthquake.[3]

This hypothesis isn't new. For centuries, prognosticators have suggested that animals have a veritable sixth sense, capable of feeling vibrations or detecting electrical changes in the air or gas imperceptible to humans.

Science hasn't been able to prove any such sixth sense exists—so far. Studies abound looking for the linkage between strange animal observations and a subsequent quake. Indeed, there are scores of anecdotal data points recording animals retreating, acting frantically, or otherwise exhibiting unusual behavior, though the body of "proof" lacks the rigidity of controlled scientific experimentation to clearly link cause and effect.

But within this research, there does appear to be evidence that animals can, in fact, sense earthquakes before they occur. That's not to say they can predict a quake, but they do

seem to detect foreshocks, mild tremors that precede violent shaking, that are indiscernible by humans.

While the jury may still be out on whether unusual animal behavior can help humans forecast an earthquake, there is at least some evidence to show that animals are more in tune with subtle abnormalities in their environment—even if only by being on heightened alert just before disaster strikes—than humans are. Those few moments, however fleeting, can mean the difference between an animal's life or death.

I believe the same is true for organizations that summon the power of the crowd—the proverbial herd instinct—to acquire and develop a sixth sense for cyber threats that is generally lacking in their counterparts. It happens when every employee hones her capabilities for practicing sound cybersecurity defense. More importantly, it occurs when the role of cybersecurity becomes so inextricably intertwined in the day-to-day job of every employee that the collective sixth sense of the organization amplifies the detection of threats before irreparable damage can ensue.

Let's put a culture of security in place across your entire organization.

There's something every employee can do and every functional leader can adopt to embed cybersecurity in the daily fabric of the workplace, to bring the might of the 12th Man to the cybersecurity field and the sixth sense of the collective herd to the first-order fight of the digital sphere.

To that end, this chapter sums up key questions and actions for every employee, manager, executive, and board member.

You've now been enlisted.

W.I.S.D.O.M. for the CEO/Board Member

- Allocate at least 90 minutes to an upcoming board agenda to have your CISO give a meaningful view into your current cybersecurity posture.
- Immediately reallocate budget to assets that are both highly strategic and highly vulnerable.
- Spend at least 30 minutes in each board meeting discussing the topic of cybersecurity.
- Have your CISO report on the status of red-teaming exercises (also known as penetration testing). Insist on these exercises as a discipline.
- Consider appointing a board member with cybersecurity expertise.

W.I.S.D.O.M. for the Employee

- Do not fall for social engineering campaigns. Be on the lookout for telltale signs of a malicious email, such as a sender's email address. Don't click on a link from an unknown source.
- Be proactive and report any suspicious emails to your cybersecurity team immediately.
- Ensure security patches on laptops, mobile devices, and other personal technologies remain current. Don't delay a security update when it is pushed by your security organization.
- Practice strong cybersecurity hygiene—use strong passwords, don't reuse passwords, and avoid unencrypted USB devices.

W.I.S.D.O.M. for the Product Developer

- Ask customers about their cybersecurity requirements as part of the discovery phase.
- Make security part of any minimum viable product requirements.
- Define your data requirements clearly and consciously in the design of any new product or service.
- Build security ownership into each phase of the product lifecycle.
- Stop the line should security be lacking or missing at any point of the product launch process. Reward and publicly recognize other employees across the company for doing the same.

W.I.S.D.O.M. for the HR Professional

- Expand the aperture for cybersecurity talent—men and women, minorities and non-minorities, arts and sciences (STEAM). Review current cybersecurity job postings to look for diverse skills. Look for interview questions that contain unconscious bias, including popular varieties like, "Tell me about a time when…" or "Tell me about the latest hot innovation in cybersecurity." Place at least one diverse leader on each interview panel.
- Search your company values and see where you can add the word *securely* (or its derivative) to change their scope without altering their purpose.
- Reward and recognize behaviors that bolster your company's cybersecurity defense.

- Work with your CISO to identify and control access privileges for your organization's most valuable assets. Find a confidential, nonthreatening way for conscientious employees to blow a whistle or raise a flag when they see something resembling a malicious insider threat. When they do, reward them appropriately.
- Ensure every member of the executive team has at least one cybersecurity key performance indicator (KPI).

W.I.S.D.O.M. for the Marketer/Communicator

- Build a multifaceted communications plan with explicit executive buy-in. The plan should include answers to the following questions:
  - Even if the law didn't require it, would you notify?
  - What if your company wasn't responsible for the attack? How would that change the tone of your message? (Consider breach-by-association and data weaponization use cases as examples.)
  - When would you notify?
  - Whom would you notify?
  - What would you say if you didn't have all information right away?
  - What would you be willing to offer customers as compensation or as a show of victim-centered empathy (such as free identity protection or offering to cover customer losses from a credit card breach, for example)?
- Create the communications templates for each scenario identified in your plan. Leave placeholders to answer the following questions in your templates:
  - Who was impacted?

  - What data and/or systems were lost, stolen, and/or otherwise compromised?
  - Over what period did the breach occur?
  - What precautionary action do stakeholders need to take?
  - What actions is your company taking to correct the problem and mitigate the risk of it happening again?
- Design the tick-tock schedule for every attack scenario.
- Be sure your plan includes employees, whether employee records are breached or not.
- Practice a communications drill of your plan at least once a year.

W.I.S.D.O.M. for the Finance Professional

- Help CISOs and their teams speak the language of the business—risk management—by asking questions like:
  - What asset(s) are at risk?
  - What is the strategic value of the asset(s)?
  - What is the current level of vulnerability for the asset(s)?
  - What are the consequences (financial damages, intellectual property exposure, reputational risk) in the event of a breach?
- To ensure cybersecurity is not an aftermarket afterthought, CFOs should ask the following for business cases submitted by other leaders:
  - How does the new [market, internal technology, customer product, etc.] change the attack surface for the company?
  - How does it alter the risk profile of the company's most strategic assets?

    - [Assuming risk is increased] What additional investment is required (one-time and recurring) to bring the risk profile to its acceptable baseline? Is this investment included in the ROI analysis?
- Mitigate risk as efficiently as possible by asking CISOs questions like:
    - How much investment in cybersecurity has been made in products still sitting on the shelf (shelfware)?
    - What is the plan for deploying those products?
    - When was the last audit performed to ensure security products are configured properly? What were the results?
    - When was the last penetration testing performed? What were the results? (Penetration testing was covered in Chapter 2 and refers to testing the effectiveness of an organization's cybersecurity posture, typically by paying third parties to attempt to breach the company's defenses.)
    - When was the last cybersecurity training conducted for all employees? What were the results?
- Mitigate third-party risk by vetting vendors with an assessment of their security posture, including:
    - Looking at how the third party assesses and updates access rights and privileges.
        - Do you review user access rights at regular intervals to ensure that access rights are based on least privilege job requirements for their job role?
        - Is timely deprovisioning, revocation, or modification of user access to the organization's systems, information assets, and data implemented upon any change

in status of employees, contractors, customers, business partners, or involved third parties?

- Understanding their business continuity process and how often they test it.
  - Do you have Business Continuity and Disaster Recovery Plans for planned and unplanned outages and do you test the plans at least annually? If yes, please describe the types of tests performed.
  - Do you record backups with regularity so that any corruption of data can be recovered with the backup, resulting in only an acceptable amount of data loss? Is restoration from those backups tested regularly?
- Searching their change control guidelines for new users and/or new software for their systems.
  - Have all default usernames and passwords been changed on all of your systems?
  - Do you have controls in place to monitor and restrict the installation of unauthorized software onto your systems (e.g., uploaded malware, disable autorun, excessive admin privileges)?
- Clarifying how any data passed between your company and theirs will be used, protected, and disposed of at the appropriate time (upon contract termination and/or in accordance with compliance standards).
  - Do you have procedures in place to ensure that production data shall not be replicated or used in non-production environments?
  - Is data destroyed securely from storage when the drives or data are no longer needed? Do you destroy non-functional hard disk drives before disposal or warranty return?

    - Do you ensure destruction of all confidential data within 30 days of termination of contract?
  - Knowing how they encrypt data at various states (at rest, in use, and in motion).
    - Is data encrypted when it moves between nodes, modules, instances, or virtual servers? If not, is there an option to add this capability? Describe the encryption used.
    - Is data encrypted when it is at rest (e.g., stored in a database, stored on a backup tape, etc.). If not, is there an option to add this capability? Describe the encryption used.
  - Assessing how they train their employees on cybersecurity awareness and hygiene protocol.
    - Does your organization have a security awareness and training program?
    - Does the organization ensure that personnel are annually trained in the organization's security policies and required to know changes or updates to these policies?
    - Does the organization ensure that all personnel with access to confidential data have information security training for their respective roles?
    - Does the organization ensure that all personnel with access to personally identifiable information (PII) complete a privacy training class and are knowledgeable of any specific privacy requirements for the data being handled?
  - For your most strategic suppliers, consider hiring a third party to audit their security practices once a year.

- If there is the slightest concern that one of your third parties looking to promote a relationship with your company does not hold itself to the cybersecurity standards you require, don't allow them to promote it.

W.I.S.D.O.M. for the Cybersecurity Professional

- Sound cybersecurity hygiene is nonnegotiable. Keep patches updated—on both physical and virtual infrastructure. Review your internal communications plan for notifying administrators of a vulnerability, including a periodic review of distribution lists to confirm accuracy. Install shelfware. Ensure proper configurations of security defenses. Back up your data (and test the backup system). Conduct regular penetration testing and provide regular readouts on progress to executives and board members.
- CISOs and CIOs must align on metrics and goals. Establish roles and responsibilities for proper cybersecurity hygiene, including patching, backups, multifactor authentication and the like, at the beginning of each planning cycle. Identify and allocate what portion of the budget will serve IT versus cybersecurity. Agree to key performance indicators (KPIs) and service level agreements (SLAs) to prioritize efforts and resolve disputes when they arise.
- Invest in technologies that drive your business value up and that of your adversaries, down.
  - Cloud access security broker (CASB) technologies help secure sanctioned and unsanctioned cloud services.

    - Deception technologies distract and confuse adversaries.
- Use artificial intelligence (AI) capabilities to identify the most advanced threats and address the talent shortage, but know its limitations. AI creates more false positives. Traditional threat intelligence has more false negatives. Both together yield high efficacy with lower false positives.
- Carry the culture flag for cybersecurity at your company.
    - Spread it vertically by speaking the language of the boardroom and its executives (risk management). Partner with the finance organization to translate cyber-speak into metrics and outcomes most understood and valued by the board.
    - Spread it horizontally through culture awareness campaigns. Hire a communications expert to work with HR and Marketing to develop effective campaigns that make cybersecurity part of everyone's day job. Deliver actionable scorecards to functional peers that measure employee understanding of cybersecurity principles and adherence to company policies.

Notes

1. D. Frances, "Ready for the Big One," *Sonoma Index Tribune*, January 30, 2014, https://www.sonomanews.com/csp/mediapool/sites/SIT/News/story.csp?cid=3387701&sid=744&fid=181&sba=AAS.
2. https://www.usgs.gov/faqs/can-you-predict-earthquakes?qt-news_science_products=0#qt-news_science_products, Accessed March 20, 2019.
3. "Quake Predictor Suspended from Job," *San Marino Tribune* (and *San Marino News*), Thursday, November 23, 1989, page 10.

Acknowledgments

I've learned that just about everything in life is a team sport and writing this playbook is no exception. I am grateful to you, the reader, for taking your position on the cybersecurity field. And I am indebted to the following individuals for your selfless contributions in making this book possible:

Steve Grobman for your brilliance in translating complex concepts into practical prescriptions. Your technical genius is rivaled only by your deft ability to communicate.

Chatelle Lynch for being a visionary in your field and cultivating an environment for a world-class culture to thrive. You show me every day what it means to play to win.

Mark Murray for your masterful storytelling skills. It's an honor to partner with you in creating amazing and memorable moments.

Chris Chaffin for giving me invaluable feedback throughout the writing process…and doing so while on vacation, no less!

Giulia Mucciarelli for your incomparable talent in creating beautiful designs, including contributing to a cover I'm proud to display on my bookshelf.

Morgan Bell, **Gavin Donovan**, and **Kevin Easterwood** for meticulously poring over each chapter with an eye for factual and technical accuracy.

Jonathan Rozek for your unwavering tenacity in researching multiple aspects of such a thorny topic.

Robert Green and **Adam Rosenblatt** for designing and executing a brilliant research study that tapped into the cultural pulse of cybersecurity in today's workplace.

Michael Marto for lending your wisdom and connections to help me bring a story to life in the way I first imagined it to be.

And last, but certainly not least, **Chris Young** for being the inspirational leader you are. Thank you for dedicating your career and the work of thousands of McAfee employees to keeping the world safe. Your passion is without equal, your talent is without measure, and your principles are without compromise.

About the Author

Allison Cerra found her life's calling at 18 years of age, when she fortuitously stumbled into a lifelong career of marketing complex technologies. She brings a practical approach to demystifying the confluence of significant technology trends—including mobility, cloud, big data, security, and collaboration—and signaling where these forces could lead cultures in the future. Whether in dissecting how broadband upends traditional economies, how technology influences and reflects company culture, how virtual and physical worlds converge to create a new human psyche, or how bad actors are motivated to challenge our digital freedom, she has explored the intersection of technology, incentives, and behaviors in several books. In 2015, motivated by a desire to stand on the good side of a fight too important to lose, Cerra joined McAfee, where she currently marries her calling for marketing with a cause of educating unwitting participants in a virtual battle that is underestimated, if not ignored, by far too many.

Index

B

C

D

E

F

G

H

I

R

S

T

U

V

W

Y

Z

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.