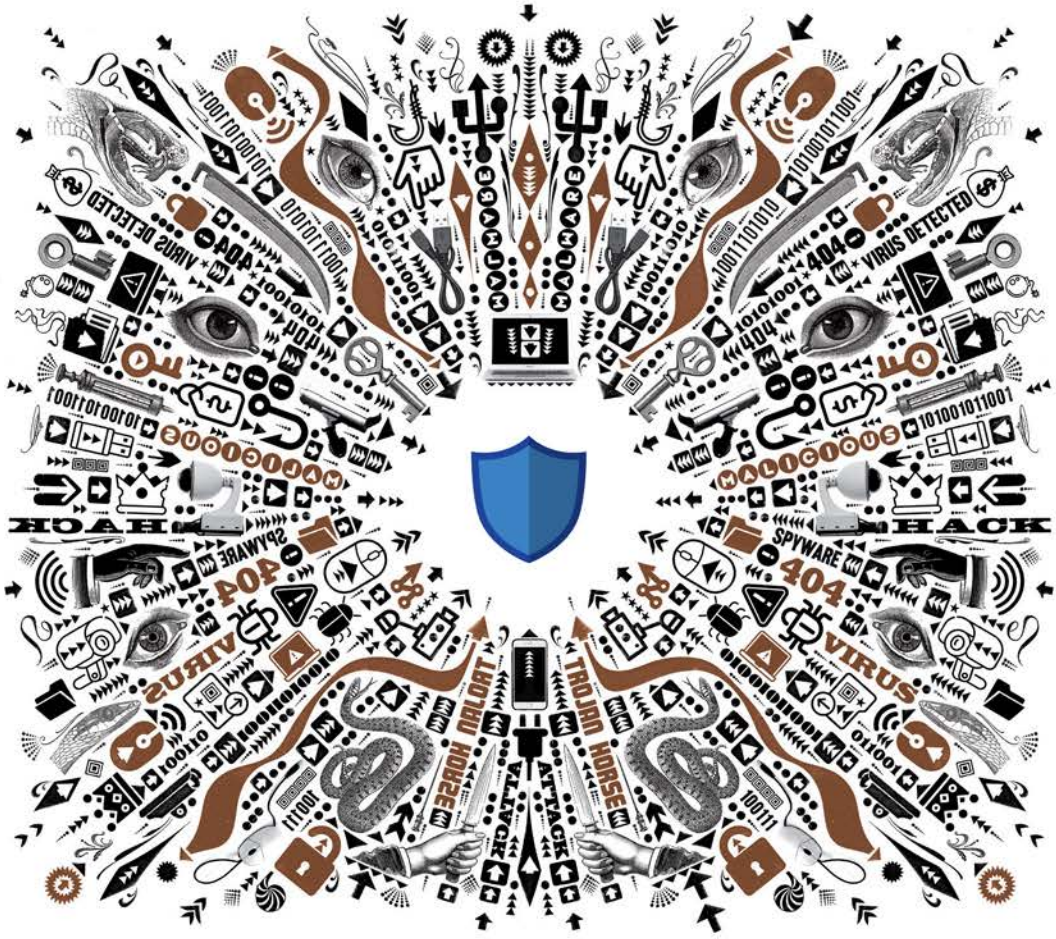
HARVARD BUSINESS REVIEW PRESS

A Leader's Guide to Cybersecurity



WHY BOARDS NEED TO LEAD—AND HOW TO DO IT

Thomas J. Parenty | Jack J. Domet

Introduction

Digital Stewardship

Over the past decade, as the world has become more digital, companies, governments, and organizations have spent billions of dollars on cybersecurity. Yet, as their investments have grown, the financial consequences of cyber breaches have increased, seemingly in lockstep.

Open a newspaper, anywhere in the world, and you'll probably find a story of a cyberattack that had devastating consequences. Recent examples include a 2016 cyber heist at Bangladesh Bank (the central bank of Bangladesh) that resulted in a US$81 million loss—a sizable portion of the country's foreign reserves.[1] In 2017, the Shadow Brokers, an appropriately named individual or organization, stole hundreds of megabytes of tools developed by the National Security Agency.[2] Included in the haul was one tool, EternalBlue, that hackers subsequently used in the WannaCry attack that had an impact on over 230,000 computer systems in 150 countries, with costs estimated to be near $4 billion.[3] In 2018, Marriott announced the compromise of its Starwood reservation system, exposing personal and financial information on up to 500 million guests, and India's national ID database Aadhaar (English: Foundation) was hacked, exposing personal, financial, and biometric information for virtually all 1.1 billion citizens in the country.[4]

Obviously, things need to change.

In our experience in consulting with clients across the globe, the core reason why the billions and billions of dollars spent on cybersecurity haven't made a difference to date is that the central focus of cybersecurity has been, and continues to be, on technology—mainly, computers and infrastructure, and their vulnerabilities—instead of the business risks to a company's operations and strategic direction.

Admittedly, there are both historical and logical reasons for why technology has been and continues to be at the center. Computer scientists were the first to look at cybersecurity. They focused on the specific details of attack and defense and how to build the core, or kernel, of the operating systems running computers so they could withstand attack. Of course, without digital technology, cyber risks wouldn't exist, and cybersecurity technologies and the activities surrounding them are important. The focus on fixing computer vulnerabilities is in fact seductively dangerous because there is value involved.

But there are a couple of reasons why this very focus on cybersecurity technology ends up undercutting its capacity to protect. No company has the resources to fix every cybersecurity problem, and not all fixes are equally important. Only by starting with your company's most critical business activities, and how cyberattacks could disrupt them, can you know how to prioritize mitigation of the cyberattacks that can cause them the most harm. Additionally, only when cybersecurity technologists understand how your company conducts business can they avoid making decisions and undertaking activities that, however well intended, don't reduce cyber risks. And, in some cases, they increase the risks while simultaneously interfering with business operations.

Further, the specialized nature of cybersecurity technology, and the jargon-filled language used in describing it, means that nontechnical stakeholders, including boards of directors, don't have a meaningful

voice in discussions of how to protect their company from cyber threats. This situation changes when discussions of cyber risk start with protecting both current and strategic activities that generate the most value for your company. This small change in approach puts you and your fellow board members in the right position to oversee the management of cyber risks.

Only by starting with critical business activities, not cybersecurity technologies, will your company know which cybersecurity products to buy and which activities to undertake. The narrow focus on technology also deflects attention from nontechnical dynamics that have much more influence in the effectiveness of the technical cybersecurity products than the sophistication of their features. These dynamics include the motivations, incentives, and priorities of the individuals who maintain and use cybersecurity products or otherwise play a role in your company's cyber defenses. We have encountered many situations, for example, in which employees have deliberately bypassed cybersecurity controls because they interfered with their number-one priority, getting their work done. In other cases, we've seen cybersecurity staff lower cybersecurity product protection levels because of the additional work and pressure if a higher level caused a false alarm or disrupted some aspect of business operations. The effectiveness of the cybersecurity group is influenced by its place within the company structure. If the head of the parent organization has different priorities, the cybersecurity group may not get the funding and visibility it needs.

If your company is ever going to materially improve its cyber defenses, it needs the right catalyst—you and your fellow board members. We view cybersecurity as fundamentally a governance problem and see corporate governance as the most effective approach companies can adopt to address their cybersecurity requirements.

Cybersecurity governance starts at the top, with board of directors' oversight and executives setting management direction. From here, it

flows through the rest of the organization, entailing both a shift in responsibility and a shift in focus. Ultimate responsibility for cybersecurity and the management of cyber risk shifts from technology specialists to corporate leadership. Focus shifts from cybersecurity technologies to the business, its operations, strategies, and big bets—and the business risks brought about by cyberattacks that could disrupt or destroy them.

Since you represent the fiduciary interests of your company's owners and are charged with adopting a long-term view of the company's health, profitability, and growth, you have the authority to instigate improvements to overall cybersecurity strategy and cyber defenses. You can step in where market forces have faltered and government regulations won't help.

Digital Stewardship

Many directors have told us that cybersecurity is daunting, if not overwhelming. They feel as if they're making investment decisions without reliable data and don't fully understand the capabilities of cybersecurity technologies. Further, many think that the learning curve is too steep. Others say they don't know what questions to ask about cybersecurity and cyber risk—or what constitutes a good answer. Often, they are left to rely on broad statements from cybersecurity or IT management along the lines of "We're OK over here, but need work over there." Technology-knowledgeable management might have cybersecurity covered, but the suspicion lingers that they may not.

It doesn't have to be this way. You can make improvements simply by fulfilling your governance and oversight duties. Cybersecurity oversight is similar in concept to the "observer effect" in quantum physics, where the observation of an event changes its outcome. Your requests for

information motivate your company to pay attention to relevant dynamics and perform necessary analyses that it would not have done otherwise.

Your assumption of cybersecurity responsibility need not be an arduous burden. In spite of the general perception that cybersecurity is complex and impenetrable, our experience shows that its governance and oversight do not require an extensive technical background. While an increased understanding of cybersecurity issues is clearly important, you don't need a deep understanding of cybersecurity to lead your company. Pursuing a formal cybersecurity education would provide limited benefits, and be time-consuming and impractical. In the natural course of your board activities, you will gain the needed familiarity with cybersecurity issues.

To assist you, we have developed a framework called "digital stewardship," which comprises four principles, three responsibilities, and a collection of aide-mémoires. The principles provide concise points of reference to guide you in your cybersecurity deliberation and decision making. The three responsibilities address your company's most important cybersecurity undertakings and give you the foundation for oversight. The aide-mémoires contain a series of inquiries you can use immediately to guide your oversight of these responsibilities. By adopting the digital stewardship framework, you will know how to be a cybersecurity leader, what you should ask of your company, and how to understand and interpret the information it provides you.

The Principles

- *If you don't understand it, they didn't explain it.* Cybersecurity management and staff within a company *are responsible for providing* their board of directors with materials and briefings that nonspecialists can understand.

- *It is the business at risk.* All discussions and actions relating to cybersecurity and cyber risks start and end with the business and the risks to its operations and strategic direction, not with computers and their vulnerabilities.
- *Make cybersecurity mainstream.* In both corporate organization and activities, take cybersecurity from siloed functions and incorporate it into mainstream operations.
- *Engage motivation.* Understand and align the interests and motivations of staff and departments to incentivize behavior that leads to accomplishing cybersecurity goals.

The Responsibilities

Manage Cyber Risks

The most significant cybersecurity responsibility is the management of cyber risk. All other responsibilities both support cyber risk management and depend on a clear understanding of the business impact of cyber incidents. Effectively managing cyber risks requires that you clearly understand the relationships among the most significant business risks a company faces, the types of cyberattacks that could cause these risks, and the mitigating controls to prevent or minimize their impact. Ensuring the effectiveness of the controls includes recognizing and accounting for the nontechnical dynamics that can negate even the most powerful technologies.

Fortify the Company

Companies can substantially improve the overall effectiveness of their cybersecurity activities by utilizing the tools of organizational structure, processes, and culture, while accounting for employee motivations

and incentives. The process of discovering new cyber risks will answer the questions, "How secure are we now?" and "How secure will we be tomorrow?" The placement of the cybersecurity group and an understanding of the cyber expertise that boards need—and don't need—can improve the effectiveness of both. Further, a shift in thinking about accountability can unlock valuable information that is essential for informed board and executive decision making.

Lead in Crisis

While a company should not neglect preventative and defensive measures, it needs to be ready for a cyberattack-induced crisis. This readiness entails prior planning, preparation, and coordination in two distinct but related areas. First, a company needs the capacity to recognize and respond to cyberattacks, which includes a skilled cyber response team and the procedures it should follow. Second, the executive team must prepare to lead the company during a cyber crisis, which includes how to treat the situations it will face and what decisions it will make during a crisis. By using information and materials already developed in the process of cyber risk mitigation, executives can think about their course of action before a cyber crisis hits.

Aide-Mémoires

Each of the aide-mémoires in the book has four components. The first part is an inquiry relating to one aspect of your company's cybersecurity responsibilities. We have drafted the inquiries so you can use them directly as written. The second component gives a brief rationale of the inquiry in terms of your company's cyber defenses and cyber risk management activities. The next component gives examples and descriptions of the types of evidence that respond to the inquiry. The final

component describes the actions you should take to fulfill your oversight responsibilities relating to the inquiry. Use of the aide-mémoires does not require that you have any prior cybersecurity or technical experience. Further, the aides are effectively key performance indicators for your company's management of cybersecurity and cyber risk.

Guide to the Book

We have written this book specifically to provide counsel and assistance to you, a board member, in fulfilling your cybersecurity governance oversight responsibilities. Given that fulfilling these responsibilities requires your company's input and action, we provide guidance to executive leadership and cybersecurity management both on the cyber protection of their companies and on fulfilling their own responsibilities to you and the board. While specifically addressing corporate boards of directors, the principles and practical guidance we offer here also apply to other types of organizations, including governmental agencies and nonprofits.

The book is divided into four major parts, each contributing to your understanding of cybersecurity in the context of your board oversight responsibilities.

- The first part, "The Problems," lays bare many of the reasons cybersecurity activities don't deliver on their promises and cybersecurity appears so impenetrable. These insights equip you to critically question the rationales for the cybersecurity decisions your company makes.

- The next part includes the four principles of digital stewardship, which are a shorthand guide for all your cybersecurity decisions, especially as you face new and unexpected issues.
- The third part addresses three foundational cybersecurity responsibilities that your company needs to fulfill and you must oversee. Each responsibility addresses the critical and often overlooked factors necessary for success.
- The final part, the aide-mémoires, includes detailed inquiries you can use to gain the necessary assurance that your company is meeting its responsibilities.

Throughout the book, we use examples from the public domain and our own practice to illustrate the application of digital stewardship principles and practices in real life, and some of the consequences when they were not applied.

PART ONE

The Problems

Let's start with two questions:

- Have you ever felt that some of the information you've been told about cybersecurity and cyber risk didn't ring true, but you weren't sure how to articulate this doubt?
- Have you ever suspected that discussions about cybersecurity are more complicated than they need to be?

If so, your intuition is correct. A significant disparity exists between what appears to be true in the area of cybersecurity and what really is. Before addressing digital stewardship principles and responsibilities, we will pull back the curtain on some of the misleading platitudes, hidden dynamics, and misguided voices that give rise to your suspicions and make addressing cybersecurity harder than it must be.

1

Misleading Platitudes

Cybersecurity discourse is full of platitudes that seem obvious and compelling at first, but more thoughtful consideration shows they are misinformed, ineffectual, or counterproductive. Unfortunately, people repeat these platitudes so frequently they take on the patina of truth and distort perceptions about cybersecurity priorities and courses of action. Three such staples of cybersecurity conventional wisdom—"it's a people problem," "protect the crown jewels," and "cyber threats are new and constantly changing"—are especially troubling.

It's a People Problem

"Cybersecurity is a people problem, not a technology problem." This platitude often takes another form: "People are the weakest link." While people do make mistakes, such as losing USB drives and opening malicious email attachments, we don't believe the problem lies with careless employees; rather, the problem rests on cybersecurity staff who fail to address how people behave in the digital world and whose motivations and incentives poorly influence their approaches to protection.

To provide context, compare how we address the people problem when securing the physical world versus the digital world. In the physical world, we understand that certain environments and situations have a higher level of inherent risk, and that people are not always careful when navigating these risks. To compensate, we build in protections to help mitigate the potential harm. These include, for example, putting guardrails on highways and speed bumps in front of schools. We take human behavior into account and don't blame people for, well, being human. We don't think or expect people will act differently just because we tell them to. The situation is radically different in the digital world, where we seldom protect people from making understandable mistakes. Instead, we blame them when they err and recommend more security awareness training as the solution.

Losing USBs

In 2007 and 2008, there were nine incidents in which personal and medical digital information on sixteen thousand Hong Kong residents was accidentally lost. As a result, the Hong Kong Hospital Authority hired us to be part of a task force on patient data security and privacy. Our goal was to understand the root causes for the breaches and recommend security improvements.[1]

One incident involved a clerical staff member at the Prince of Wales Hospital in Hong Kong's New Territories who lost a USB flash drive in a taxi. It would be easy to jump to the conclusion that the staff member's lack of security awareness was the root cause of the incident, just as, in the beginning of a movie or TV show, we might assume that the gun-wielding person standing over a dead body is the murderer.

But we asked only two questions to find out the real root cause: "What do you do at work?" The clerk prepared spreadsheets for

interhospital, cross-charge billing for pathology tests performed at Prince of Wales Hospital. "Why did you copy this information onto a USB drive?" The reason wasn't sinister but, instead, a practical frustration many people who work at large companies might face. She didn't have Excel installed on her computer, so she used a USB drive to copy the spreadsheets she got from other hospitals to a colleague's computer that did have Excel so she could do her work. To no avail, she had repeatedly asked IT to install Excel on her computer.

So, this incident was the result of a people problem, but not a problem with the clerk. The problem was with the IT staff who didn't install Excel on her computer. When they eventually installed Excel, the risk of her losing patient information on a USB drive disappeared because she no longer had any reason to use one. This example shows that people are motivated to do their jobs, even if it entails undermining cybersecurity. The clerk was not conscious of the fact that her actions could compromise patient information. She just wanted to do her job.

Phishing

People often open attachments and click on links in emails that result in malware being downloaded onto their computers. Attackers have become savvier in using information gleaned from social media and professional networking sites in crafting these phishing emails, so recipients find it increasingly difficult to tell the difference. While a few Nigerian princes still want to give you millions, their emails have largely been replaced by a variety of more-convincing ones. The University of California at Berkeley keeps a database of phishing attack examples, such as one purporting to be from the human resources department (see figure 1-1).[2]

FIGURE 1-1

Example of phishing attack

From: "HR@berkeley.edu" <HR@berkeley.edu>
Subject: Message from human resources
Date: April 13, 2017 at 9:29:54 PM PDT
To: XXXXX@berkeley.edu

Dear XXXXX@berkeley.edu

An information document has been sent to you by the Human Resources Department.

Click here to Login to view the document. Thank you!

Berkeley University Of California HR Department.
@2017 The Regents of the University of California. All rights reserved.

CONFIDENTIALITY NOTICE: This email and any attachments may contain confidential information that is protected by law and is for the sole use of the individuals or entities to which it is addressed. If you are not the intended recipient, please destroying all copies of the communication and attachments. Further use, disclosure, copying, distribution of, or reliance upon the contents of this email and attachments is strictly prohibited.

The email in the figure looks legitimate, and the instruction to log on to your account to view the document isn't suspicious because this is standard practice for many organizations, especially when a document contains sensitive information. The security advice the Berkeley Information Security Office offered for this type of example is that the email recipient should first verify that the link is legitimate before clicking on it. To perform the verification, the email recipient needs first to position his or mouse over "Click here" so that the website's address will appear. Then, most critically, the recipient needs to discern if it is really the address of the HR department website as opposed to one trying to impersonate the website.

This advice, with which most cybersecurity experts would agree, fails to consider two factors. The first is that reading email at work is not a leisure activity; people try to get through it as quickly as possible. Many will find that the time to position a mouse over a link, look at a website address, and decide if it is legitimate or not will take too long.

The other and more important factor is that determining the validity of a website address is not a responsibility that most people can reliably fulfill, so not one that a company should impose on them.

Security Awareness Training

A commonly used control to prevent phishing attacks and, more broadly, the introduction of malicious software into a corporate environment is security awareness training. However, even employees at cybersecurity companies have difficulties internalizing cybersecurity awareness training. Intel Security (formerly McAfee) tested 19,000 people from 140 countries and only 3 percent were able to identify all the phishing emails in a sample of 10, and 80 percent failed to spot any of the phishing emails.[3] No amount of security awareness training can satisfactorily mitigate this risk, as it takes only one person to click on the wrong link or open a tainted attachment in order for this type of attack to succeed.

Identifying Malicious Software

Another tool for foiling phishing attacks, and their associated malware, is anti-malware technologies that work by detecting malicious software before it can establish a beachhead on a computer and start its process of exploitation. Therein lies the problem—how to identify malicious software. Initially, this was done by compiling a list of the signatures, or fingerprints, of known malicious software and comparing it with any new program before allowing the software to run. More-sophisticated anti-malware products look at additional characteristics, including behavior, of potentially malicious software. However, the challenge remains, as defenders constantly try to catch up with the new versions of malicious software that attackers are adept at creating.

In late 2017, the company Malwarebytes, itself a provider of anti-malware solutions, examined malware detection rates from almost 10 million computers and found that even highly ranked anti-malware products failed to detect over 60 percent of the malware it tested.[4] Going back to 2013, the *New York Times* revealed its corporate network had been breached in an attempt to discover reporters' sources.[5] This attack included the use of forty-five different kinds of malicious software, of which only one was detected by its anti-malware solution.

Going further back to the beginnings of computer viruses, the inherent limitations of antivirus solutions were recognized by a founder of the antivirus industry. When the first computer virus appeared in 1986, within two years, there were as many as forty antivirus vendors in this booming market.[6] With this rapid proliferation of vendors, John McAfee, who developed the first successful commercial antivirus program, estimated that "as many as 75% of the products currently being marketed are ineffective in that they do not detect or protect against a significant percent of the viruses."[7] He publicly worried that a "lack of understanding on the part of end users has created an environment conducive to misinformation, emotionalism and fraud."[8] As of 2018, the worldwide annual revenue for these types of products exceeded US$15 billion and was expected to continue to grow at a brisk 10 percent CAGR.[9]

There is an elegant technological solution for addressing phishing attacks and all other types of malicious software that is inherently effective and doesn't require all your employees to make the right decision all the time about what they click on or open. "Application whitelisting" is based on the principle that if malicious software can't run on a computer, it can't harm the computer. It borrows from a practice often used to restrict access to clubs, parties, and other special events—the guest list. Instead of trying to determine if every program or piece of software is malicious, application whitelisting focuses on only allowing

software that is already known to be safe to run on a computer. It doesn't matter what links people click on or what attachments they open. It doesn't matter how many new variants of malicious software are created every day. If the malware isn't on the guest list, it won't be let in.

IT Staff Incentives

The security concepts behind application whitelisting have been known for years. There are commercial whitelisting products, and even the Windows and macOS operating systems contain application whitelisting tools. So, the question remains, why aren't people using application whitelisting more broadly? Further, why is it likely that you have never heard of it, while antivirus or anti-malware products are quite familiar? The answer comes down to motivation and blame.

Since current malware defenses aren't effective, infections are routine and perceived as inevitable. When infections do occur, companies blame neither the providers of security awareness training nor the anti-malware solutions for the failure of the products and services. Nor do they blame the staff people who procured these products and services. There is no motivation for the cybersecurity function within an organization to change from approaches that aren't effective to one that is.

There are, however, distinct disincentives for individuals in cybersecurity or IT departments to adopt application whitelisting in lieu of anti-malware. Within a traditional corporate office environment, the deployment of an anti-malware solution is simple, and ongoing management is largely automated. Again, there is no blame if it doesn't work, so long as it is in place. The deployment of an application whitelisting solution requires more effort and attention on the part of IT staff. They need to make sure that updates to existing applications

remain on the whitelist and that new, authorized business applications are added. If they don't do this work correctly, and someone in the company can't use their computer or an application they need as a result, the IT staff will be blamed and under great pressure to fix the problem immediately.

The fundamental issue boils down to the question of who has responsibility for creating a safe digital environment in which people can work. To date, companies have largely placed this responsibility on individuals who are in no position to protect themselves, and on technologies that can never be effective. The underlying reasons for this course of action directly relate to incentives and accountability or, more precisely, the lack of it. The platitude "it's a people problem" only serves to mask the issue.

Protect the Crown Jewels

Perhaps the most common type of reported cyber breach is loss of personal information, including financial data, medical information, credit card details, national identity numbers, and passwords, because of attacks on corporate and government computer systems. Close behind are losses of trade secrets, intellectual property, strategic plans, and internal financials. Given that not all digitized assets are of equal worth, it makes sense to prioritize the protection of the most valuable. The problem with the platitude "protect the crown jewels" is that it often promotes activities that are neither appropriate nor effective in reducing a company's most significant cyber risks.

The directive to protect the crown jewels implicitly places the greatest priority on the confidentiality of information. The thinking goes that it's better to delay the speed or convenience of sending or sharing information in order to make sure it doesn't fall into the wrong hands.

However, depending on your specific business or needs, data confidentiality may not be your number-one priority.

For example, if your company operates a multiplayer online game, the necessary computing power and network bandwidth are of utmost priority since you want your games to be available to your hundreds of thousands of gamers whenever they want to play. If they can't play, you'll quickly go out of business.

If your company uses industrial control systems that drive, for example, oil refining, chemical manufacturing, or electric power generation, then speed of communications is critical. These systems comprise many individual computers, often quite old, that are quite sensitive to delays in network communications. If one machine doesn't get a message from another machine when expected, it can malfunction, causing a cascading effect throughout other components of the industrial control system that could result in disruption to or the complete halt of operations.

Speed can also be critical in medical settings. Although cybersecurity priorities in health care tend to center on confidentiality, cybersecurity priorities are flipped upside down in emergency situations. When a patient is in the emergency room or on the operating table, doctors want to get as much patient medical history information available, as quickly as possible. Lives depend on it. During the fog of surgery, if someone gets access to information they shouldn't have, that can be investigated and resolved when the patient is recovering.

These examples show, however, that companies face many other cyber risks unrelated to confidentiality. A focus on protecting crown jewels will not help you in identifying and mitigating these risks. Nor will this approach necessarily provide the comprehensive protection your confidential information needs. This is because many attempts at protecting crown jewels focus on protecting information where it is stored. Hence, the common post-breach question, Was the data

encrypted? This question usually refers to the primary database where the information is stored. However, in order for information to provide value, it has to be taken out of the database, shared, and used. The risk exposure is much greater during these activities than when the information is resting in a database. To address the goals of prioritizing cybersecurity attention and providing complete protection, your company should focus on protecting its most important business activities, and you'll get the protection of sensitive information as part of the process.

Take, for example, customer service for accounts and billing. This business activity requires access to sensitive personal information, such as addresses and ID numbers, and sensitive financial information, such as credit card and bank account numbers. By tracing the process of creating a new customer account to customer service interactions while the account is active, to the closing of the account, your company will know all the computers where this information is stored, all the computer networks the information traverses, and all the individuals and organizations who have access. Your company needs to protect not only sensitive customer information but, more broadly, your customers' trust.

An additional benefit of focusing on critical business activities is that you may identify types of information you previously didn't realize were so critical. The relatively low-tech business of growing and selling almonds, walnuts, and pistachios in California's Central Valley provides a case in point. Nuts are an attractive target for thieves. One truckload of nuts can be worth up to US$500,000 and, unlike electronic equipment, the nuts have no serial numbers. Once eaten, the evidence is gone. Innovative thieves have moved beyond hijacking trucks on lonely stretches of road in favor of cyber-based attacks. They start by hacking into nut growers' and processors' computers to steal information about planned shipments. This allows them to generate legitimate-looking paperwork for already scheduled shipments and then send their own

trucks before the real drivers arrive. In some cases, the thieves hire drivers who are unaware that they are participating in a robbery.[10]

A characteristic that "protect the crown jewels" shares with other cybersecurity platitudes is that it makes it easy for people to think that they already understand a problem and know how to solve it. This discourages them from examining cybersecurity problems more thoroughly and therefore finding better and more effective solutions.

Cyber Threats Are New and Constantly Changing

Because companies are overwhelmed by the seemingly ever-increasing number of new cyber threats, they make two common mistakes. They think that investment in protection should be proportionate to the size of the threat. If the threat is increasing dramatically, so should the investment. In a similar vein, they think they need to make more investment to combat a threat never seen before. Given that these perceptions of urgency influence cybersecurity investment decisions, it's useful to explore them more thoroughly.

How Fast the World Turns Depends on Where You Stand

The rapid changes in the cyber threat landscape are an oft-quoted reason for boards of directors' more frequent briefings on cybersecurity. While we fully agree that cybersecurity warrants more time on your agenda, it is because of the breadth and importance of the topic, not its pace of change.

One metric commonly used to indicate the rapid growth of cyber threats is the volume of new malware. Numbers for 2017 range from

15,107,232 to 128,160,000, and that only accounts for the malicious software that anti-malware vendors were able to detect.[11] While these numbers are large, they are also largely meaningless. There is no real difference between how a company protects itself from a million types of malware versus 10 million or 100 million. The real issue is how to neutralize any malware.

If You Don't Know It, It's New to You

The relative recentness of broad cybersecurity awareness contributes to the perception that the cyber threats we are facing are new. Yet the cybersecurity field can trace its roots back more than five decades to the 1960s when the US Air Force was concerned about something that now fills headlines as a new threat: nation-state attacks on critical infrastructure. The nation-state in question was the Soviet Union, and the critical infrastructure was the US nuclear arsenal. The specific risk—use of malware to compromise computer systems—seems strangely contemporary as well. A preeminent concern at that time, according to (Ret.) Air Force Colonel Roger Schell, who was intimately involved in these matters, was that malware in the computers controlling the navigation of land-based nuclear missiles could redirect these missiles to attack US cities.[12]

Given that internet connectivity in the 1960s was nothing like what we have today, the primary methods for infecting computers with malware were software developers and the tools to turn the programs they wrote into instructions that machines could understand. To address these risks, developers underwent background investigations, and all their tools were developed in-house. While the economics of software development have changed over the years, a risk cybersecurity experts understood in the 1960s reappeared in 2015.

Apple provides a tool named Xcode for programmers who are developing applications for iOS devices, such as iPhones and iPads. While Apple provides this tool for free, it can also be downloaded from websites catering to software developers. One of these sites, Baidu Yunpan, contained a malware version of Xcode, called XcodeGhost, that added extra instructions into programs without the knowledge of the software developer.[13] These instructions, when incorporated into popular applications downloaded tens of millions of times, could steal personal information from the users of the applications and send it to an unknown server.

Beyond the insight that the US Air Force recognized this type of cyberattack fifty years earlier, the broader lesson for companies is the importance of understanding just what and whom they are depending on for protection against cyber threats. Companies do not ask this question nearly enough, and you are ideally positioned to correct this situation.

In the winter of 1970, the US Defense Science Board Task Force on Computer Security published a report entitled "Security Controls for Computer Systems."[14] Commonly referred to as the Ware Report after its primary author Willis Ware, it identified a majority of cyber vulnerabilities and risks that we still face today, a sample of which we summarize in table 1-1.

TABLE 1-1

Sample of ongoing cyber vulnerabilities

Topic area	Specific concern	Relevance today
Files	Theft, copying, and unauthorized access to sensitive information	This is still one of the most significant cyber risks organizations face.
Software	Failure of protection features, including control over what information people can access	In most cases of insider theft of company information, a failure of access controls facilitated the theft.

(*Continued*)

TABLE 1-1

Sample of ongoing cyber vulnerabilities (*Continued*)

Topic area	Specific concern	Relevance today
Users	Weak authentication of computer users	Criminals impersonating users, often through the use of stolen passwords, continue to haunt both companies and individuals.
Network communications	Ability to tap and intercept network traffic	The risk still exists, but fortunately encryption solutions are widely deployed.
System administration	Administration mistakes resulting in compromise	One of the major risks of the internet of things and the expanding adoption of technologies outside IT department control is that the users of these devices do not know how to manage them securely. In addition, many of the breaches of corporate information stored in the cloud are due to configuration mistakes.
Programmers	Programmers modifying their software to disable security features introduce back doors and otherwise subvert security	All these concerns currently exist.

The fundamental cyber vulnerabilities computers face are neither growing nor new. The innovative ways in which we are using and combining digital technologies introduce new challenges, but these are all variations on existing themes.

Further, although computers now come in a variety of packages ranging from mainframes and laptops to watches and refrigerators, and require new approaches for protection, the cybersecurity issues are fundamentally the same. In a similar vein, so are the attacks. Certain particulars of an attack may be different, but the attack is not fundamentally different. Think, for example, of emails containing links that, when clicked, result in the download of malicious software onto your laptop. Now think of an SMS that, when clicked, results in the download of malicious software onto your phone. The delivery mechanisms are different, email versus SMS, and the malicious software

will be different to accommodate running on a laptop versus a phone, but they are the same cyberattack. This situation is analogous to a store that claims to have forty different shirts, but in reality, it is selling one shirt in four sizes and ten colors.

In this chapter, we showed how common cybersecurity platitudes draw our attention from what really is important to what only seems to be. In the next chapter, we show how dynamics that are just out of sight expose commonly accepted truths about cyber defenses.