GUIDING CYBERSECURITY FROM THE BOARDROOM

ACTIONABLE ADVICE FROM PRACTITIONERS, C-SUITE EXECUTIVES, AND DIRECTORS ON CYBERSECURITY STRATEGIES FOR 2024 AND BEYOND

TAG

NEXT PEAK

GUIDING CYBERSECURITY FROM THE BOARDROOM

CONTENTS

INTRODUCTION

For most chief information security officers (CISOs), briefings to senior leadership are heavily curated experiences. It's common, for example, for such engagements to sidestep free-form discussion of cyber risks or other security-related topics. Instead, sharing with C-suite executives is carefully filtered through layers of management, including board secretaries.

This curation creates less trouble in areas such as finance, because most executives have direct personal experience in that discipline. It would be tough to find a C-suite that includes no former financial experts. Not having direct contact with practitioners is thus not much of an issue. Executives already have good instincts there.

But when it comes to cybersecurity, the reality is that the vast majority of corporate boards and C-suites will not have meaningful representation from members with experience in this area. Add to this deficiency curated interactions with CISOs and the problem is exacerbated. The result is that all too often executives are not optimally informed.

A Wall Street Journal **report** published in September seems to back this view. Its research found that only 2.3% of the directors at S&P 500 companies have cybersecurity experience. And when researchers dug deeper, they noted that cybersecurity "experience" is not necessarily the same thing as "expertise."

Our book attempts to rectify this problem. We've invited a group of industry-recognized experts in cybersecurity, along with others who have relevant experience in this field, to provide high-level advice and guidance in their respective areas of expertise. These are precisely the types of people who should be interacting openly and directly with the C-suite and the board.

We believe that the fine group we've assembled, selected based on our years of experience in the industry, rose mightily to the challenge. Their articles include useful and illuminating information on a wide range of topics, spanning geopolitics, compliance, technology, artificial intelligence, and more. These are must-read essays.

Continued

INTRODUCTION

Continued

The chapters are organized into three sections. In Part One, you'll find articles that demonstrate the range of issues we cover in the book. These include what boards need to know about the new SEC rules on cybersecurity, about handling crisis communications in a way that not only preserves a company's reputation but enhances it, and about navigating the threats and opportunities presented by new technology.

Part Two examines cybersecurity and governance by answering some of the large, looming questions in the field. What do boards need to know about cybersecurity to meet their fiduciary duties? Why is a board's partnership with management so important in strengthening a company's cybersecurity? How should companies address geo-cyber risks? And why are in-house lawyers key players in the current regulatory environment?

In Part Three, we conclude with articles on technology. But you don't have to be a CISO to understand them. They were written specifically for a general audience, even though the information and advice they contain will be of great interest to experts as well. A chapter on the quantum threat to cryptography, for example, is followed by a guide on how to approach the implications of emerging technology.

Throughout the book you'll find articles that are written from the perspective of cybersecurity practitioners. They are not repeating lessons the authors have picked up from other people's blogs or books. They draw on their own experiences, and that's what brings their chapters to life.

We think you'll find the writing here provocative, insightful—and most of all useful. We expect these pieces will be conversation-starters at your workplace.

From our combined team at Next Peak and TAG, we offer our sincere hope that this volume helps readers face the challenges ahead. In the coming years, companies will likely find that advancing threats from nation-states and criminal groups will be matched only by the unpredictable effects artificial intelligence will have on the offensive and defensive postures of our organizations. In these uncertain times, we can use all the help we can get.

David Hechler: Editor

Dr. Edward Amoroso, Founder & CEO.
President & COO: Rick Friedel
Director of Content: Lester Goodman

tag-cyber.com

CONTRIBUTORS

Dr. Edward Amoroso is the Founder and CEO of TAG. He is also a Research Professor at NYU's Tandon School of Engineering and the author of six books. Before he retired to start his own company, Amoroso was the SVP and Chief Information Security Officer for AT&T and a member of the Board of Directors for M&T Bank.

Anne Chow is Lead Director of FranklinCovey's Board of Directors, a Director of 3M, and a Senior Fellow and Adjunct Professor of Executive Education at Northwestern's Kellogg School of Management. A best-selling author, Chow is the former CEO of AT&T Business and was twice featured as one of Fortune Magazine's Most Powerful Women in Business.

Melanie Ensign is the CEO of Discernible, a cybersecurity and privacy communications advisory firm. She is Co-Chair of the Privacy Workforce Public Working Group at NIST and the former Press Department Lead for Def Con. She previously worked in communications at Facebook and Uber.

Andy Geisse is an Operating Partner at Bessemer Venture Partners. He sits on a variety of boards and plays an advisory role with a number of companies. He is the former CEO of AT&T Business Solutions, Sr. Executive VP responsible for AT&T's Wireline business, CEO of Startel Communications, CEO of VTR Cellular, CEO of CellularOne in Upstate New York, and CIO of AT&T.

Christopher Hetner is Special Advisor for Cyber Risk for the NACD, a Senior Advisor for the Chertoff Group, and Chair of Cybersecurity and Privacy for the NASDAQ Center for Board Excellence. He's also a board member of the Society of Hispanic Professional Engineers and a Research Affiliate with the MIT Sloan School of Management. He previously served as the Senior Cybersecurity Advisor to the Chair of the Securities and Exchange Commission and as Head of Cybersecurity for the SEC's Office of Compliance Inspections and Examination.

Sanjay Macwan is Chief Information Officer and Chief Information Security Officer at Vonage. He teaches Emerging Technology Ventures at the University of Pennsylvania and has 49 U.S. patents across cloud, mobility, multimedia, and information security technologies. He formerly served as SVP and Chief Technology Officer at NBCUniversal.

Continued

CONTRIBUTORS

Continued

John J. Masserini is a Senior Research Advisor at TAG. He is a 30-year security veteran and was previously the Chief Information Security Officer for Millicom (Tigo), MIAX Options, and for the Dow Jones Corporation.

Randal Milch is Co-Chair of the NYU Center for Cybersecurity, Faculty Co-Director of the NYU master's program in Cybersecurity Risk and Strategy, and a Professor of Practice at the NYU School of Law. He was formerly the General Counsel and head of public policy at Verizon. He also chaired the Verizon Executive Security Council, which oversaw information security across all Verizon entities.

David Neuman is a Senior Analyst at TAG. He's the former Chief Information Security Officer for both Rackspace and iHeart Media and is a retired Cyber Commander for the U.S. Air Force. He also teaches cyber to undergraduate and graduate students at the University of Texas at San Antonio.

Debora A. Plunkett, a cybersecurity leader and educator, is a board member of CACI International, Nationwide Insurance, Mercury Systems, and BlueVoyant. She's also a Professor of Cybersecurity at the University of Maryland. She was the Director of Information Assurance at the NSA before she retired after 31 years and was a director on the National Security Council at the White House, where she focused on cybersecurity.

Greg Rattray is a Co-Founder of Next Peak, where he is a Partner. He's also the Executive Director of the Cyber Defense Assistance Collaborative. Rattray previously served as the Global CISO and Head of Global Cyber Partnerships at JPMorgan Chase, as well as Chief Internet Security Advisor for ICANN. He retired from the U.S. Air Force as a Colonel in 2007.

Christopher R. Wilder is a Research Director and Senior Analyst at TAG, where he advises cybersecurity, climate science, and AI industry leaders. He's the former chairman and CEO of Tiga Energy Services and a former U.S. Navy intelligence expert. He's also a Forbes contributor and co-author of the book "Influencing the Influencers."

PART ONE

AN INTRODUCTION TO THE RANGE OF ISSUES

CHAPTER 1

DUOLINGO FOR MEMBERS OF THE BOARD: LEARNING TO SPEAK CYBER WITH THE SEC

CHRISTOPHER HETNER

There is a language barrier in cybersecurity that is preventing a fundamental shift in how businesses address cyber risk and improve their cyber resilience. This barrier exists because we in the cybersecurity ecosystem continue to discuss cyber risk in a language that is not familiar to business leaders, especially those who sit on their companies' boards.

The language of business is rooted in accounting, finance, and marketing. It includes terms like revenue, return on investment, margin, and capital. You can bet board directors know these terms. This language helps them understand the health of their businesses and serves as an answer key for making decisions. Words that are outside of their language may be confusing, misleading, or undecipherable.

To remove this barrier and encourage a fundamental shift in how businesses address cyber risk, their colleagues from the tech world need to speak their language. Fortunately, there are plenty of ways to do this.

MITIGATING REPUTATIONAL DAMAGE

Every business leader understands the value of a company's reputation, and the tremendous harm that can be done when it is damaged. It can happen in a flash and take years for the business to build it back—if it ever does.

A CEO can be caught engaging in misconduct. Or a new product may fail to function properly and injure customers in the process. These are the kinds of missteps that

In addition to the financials from stock exchanges that boards routinely study, they may need to learn about the data found in Security Operations Centers (SOCs).

we've read about for years. But there are new ones in the cyber world, and these are the kinds of issues that all business leaders need to understand.

When a company suffers a major data breach, board members will not be the corporation's first responders. But they must be sufficiently prepped to immediately understand the potential reputational risk. They should have roles to play in this form of crisis management, just as they would for any other kind. The company will want to measure the damage and respond to the danger in the same way they attempt to mitigate other crises.

If directors needed a sign that the world of business has recognized the need to take on the challenges posed by cybersecurity, they got it on July 26, 2023.

The technology at the center of the action is different, but the corporate governance that leads the response should be right from the business playbook. Here the board should be close to bilingual. The attack on the business may not be in their native tongue, but they know what an attack on the business means.

The bottom line is that members of the board can and must be part of their company's security defense. Cyber risk management is a team sport that requires the entirety of the enterprise to ensure business resilience. What is required is a more inclusive message and collaboration that includes all enterprise risk management leaders.

Technology changes quickly and cyber threats do, too. Static analyses of today's risks are less helpful than establishing a regular flow of information to the board that supports cybersecurity investment decisions based on business, operational, and financial considerations. With the board's eyes kept regularly on cybersecurity as an aspect of routine governance, directors will be equipped to confront the challenges ahead.

ENTER THE SECURITIES AND EXCHANGE COMMISSION

If directors needed further signs that the world of business has recognized the need to take on the challenges posed by cybersecurity, they got it on July 26, 2023. That was the day the SEC adopted its long-awaited rules on cyber risk management, strategy, governance, and incident disclosure. The rules also require companies registered with the SEC to publicly disclose how their boards of directors exercise

oversight of cybersecurity risks. So this responsibility is no longer exclusive to chief information officers and chief information security officers.

New cyber reporting will require a deeper focus on material business—and operational and financial impacts.. With cybercrime damages expected to reach $8 trillion this year, according to Cybersecurity Ventures, boards will need to better address cyber investments and the risks of business interruption, remediation costs, lost revenue, litigation, the erosion of competitiveness, and reductions in long-term shareholder value. Here are some of the specific rules companies now face (see also summary of rules changes on p.12).

Incident Reporting: Companies registered with the SEC must disclose information about a cybersecurity incident within four business days after they determine they have experienced a material cybersecurity incident. A cybersecurity incident is defined to include an unauthorized occurrence on or through a company's "information systems," including "information resources owned or used by the registrant." The primary purpose of the incident disclosure requirements is to focus on the material impacts introduced by the incident, rather than requiring details about the incident itself. The rule requires registrants to "describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations."

Third Party Incidents: This rule requires registrants to also disclose incidents occurring on third party systems. The commission emphasized that it is not "providing a safe harbor for information disclosed on third party systems." Depending on the nature of the incident, disclosures may be required by both the customer and the third party.

Previously Disclosed Incident Reporting: This rule requires businesses to provide updated disclosures relating to previously disclosed cybersecurity incidents. Examples include any material impact of the incident on the company's operations and financial condition. These requirements will place additional pressure on incident response teams to maintain a comprehensive register of risks introduced by incidents and monitor them for changes in materiality.

Reporting When a Series of Previously Undisclosed Incidents Becomes Material: This requires disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate. At that point, companies would need to disclose when the incidents were discovered, whether they are ongoing, and provide a brief description of the nature and scope of the incidents.

Policies and Procedures: Companies must disclose their policies and procedures for identifying and managing cybersecurity risks and threats, including: operational risk; intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk. Specifically, a company must disclose whether it has a cybersecurity risk assessment program and, if so, provide a description. It must also provide consistent information disclosures about its cybersecurity risk management and strategy.

Governance: This rule requires disclosure regarding board oversight of a registrant's cybersecurity risk governance and the inclusion of management's oversight of cybersecurity risks. Moreover, the rule requires a description of the implementation of related policies, procedures, and strategies that impact an investor's ability to understand how a registrant prepares for, prevents, or responds to cybersecurity incidents. It also requires disclosure of a registrant's cybersecurity governance, including the board's oversight of cybersecurity risk and a description of management's role in assessing and managing cybersecurity risks, the relevant expertise of management, and its role in implementing the registrant's cybersecurity policies, procedures, and strategies.

Management's Role: This rule requires a description of management's role in assessing and managing cybersecurity-related risks and in implementing the company's cybersecurity policies, procedures, and strategies. This description should include but not be limited to whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of these people or members.

The costs of cyber crime—including the cost for recovery and remediation—are expected to grow to $10.5 trillion per year by 2025.

TRANSPARENCY IN CYBER-RISK GOVERNANCE

So, what's different now? What should boards be focused on? Being transparent about cybersecurity isn't just a best practice, it's now a requirement for U.S. companies. The SEC's new cybersecurity rules "require publicly enlisted companies to disclose their cybersecurity governance capabilities, including the board's oversight of cyber risk, a description of management's role in assessing and managing cyber risks, the relevant expertise of such management, and management's role in implementing the company's cybersecurity policies, procedures, and strategies." This kind of disclosure allows investors to evaluate the attention executives and business leaders are paying to cyber risks.

More broadly, management needs to understand how these threats can cause material harm. Examples abound. For instance, the ransomware attack on Hanesbrands disrupted order fulfillment for three weeks, causing a $100 million loss in revenue. Another example is the IT outage caused by a cyberattack at Tenet Healthcare, which also resulted in $100 million of lost revenues. And the Kaseya VSA breach was the result of insecure operational software that ultimately led to the postponement of an initial public offering that sought to raise $875 million.

Under the new rules, companies are also required to report within four days of incidents that are deemed "material." The materiality determination is influenced by the incident's impact on the company's business, operations, and financial conditions. This mandatory incident reporting allows investors to evaluate the effectiveness of the firm's cyber risk policies and may provide lessons for future improvements in cyber risk management. And there is a

significant opportunity for improvement, since the costs of cyber crime—including the cost for recovery and remediation—are expected to grow to **$10.5 trillion per year** by 2025. That should get the board's attention.

SUMMARY OF THE SEC DISCLOSURE REQUIREMENTS

Item	Summary Description of the Disclosure Requirements
Regulation S-K Item 106(b)– *Risk management and strategy*	Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
Regulation S-K Item 106(c) – *Governance*	Registrants must: • Describe the board's oversight of risks from cybersecurity threats. • Describe management's role in assessing and managing material risks from cybersecurity threats.
Form 8-K Item 1.05 – *Material Cybersecurity Incidents*	Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its: • Nature, scope, and timing; and • Impact or reasonably likely impact. An Item 1.05 Form 8-K must be filed within four business days of determining an incident was material. A registrant may delay filing as described below, if the United States Attorney General determines immediate disclosure would pose a substantial risk to national security or public safety. Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.
Form 20-F	Foreign Private Issuers (FPIs) must: • Describe the board's oversight of risks from cybersecurity threats. • Describe management's role in assessing and managing material risks from cybersecurity threats.
Form 6-K	FPIs must furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders.

CHAPTER 2

FROM CYBER CRISIS TO SUSTAINED REPUTATION MANAGEMENT: LEADING COMMUNICATIONS FROM THE BOARDROOM

MELANIE ENSIGN

On June 5, 2013, The Guardian began publishing what turned out to be the first of many articles about the National Security Agency's (NSA) collection of domestic email and telephone metadata. At the time, I was leading cybersecurity communications for AT&T through an engagement with their PR agency of record. The revelation that AT&T had been secretly turning over customer communications to the NSA for years (even behind the back of its own security team) quickly ignited intense scrutiny from journalists, politicians, and customers from around the world. Tensions were high inside AT&T as employees grappled with new information about the company they worked for.

According to news reports, AT&T willingly gave the NSA access to billions of emails as these flowed across the company's domestic networks. The company also provided technical assistance in carrying out secret court orders to wiretap internet communications at targeted AT&T customers, including the United Nations headquarters in New York.

Now, AT&T's security and communications teams were both well-versed in managing security incidents. At the time, AT&T owned the largest global mobile network, giving us visibility into the most prolific as well as the most novel attacks

against corporate networks to date. The company was recognized as one of the foremost leaders in defending against the then-exploding threat of distributed denial of service (DDoS) attacks. Journalists sought the expertise of our security team when covering stories ranging from telecom fraud to nation-state attacks.

But the news cycle in 2013 wasn't about an unauthorized intrusion or coordinated attack. AT&T's systems remained intact and operational. Yet, the NSA revelations completely shut down the company's ability to speak publicly about any of its cybersecurity investments or services without having to address its relationship with government intelligence agencies. All executives and company spokespeople had to be prepared to field press and customer questions about the company's commitment and ability to keep personal information safe. Public skepticism lingered. Our credibility did not.

NSA/AT&T parody T-shirt

Nine months later, at the end of February 2014, things weren't any better. When members of AT&T's cybersecurity team attended a social gathering related to the annual RSA Conference in San Francisco, they were asked by a prominent cybersecurity reporter how they felt about all the parody T-shirts donned by attendees showing the NSA logo with an eagle using its talons to plug into AT&T's network. The response was chilling, and the resulting article caught the attention of company executives. It was clear there was still a lot of work to do to repair the company's cybersecurity reputation.

All of this happened without the presence of a single "hacker," software vulnerability, or compromised password.

A constant cloud of public distrust should concern every executive and board member, not only because of the immediate distraction and costly legal battles it provokes, but also because it makes your brand a toxic affiliation to all the allies you're going to need later on. You've lost reputation capital, and every sale, partnership, or endorsement just became a lot more expensive.

CYBERSECURITY IS A PERMANENT REPUTATION ISSUE: IT NEVER STOPS

Historically, executives and their boards viewed cybersecurity as a crisis communication challenge because they saw it as a one-off or infrequent occurrence. The truth is, very few have had complete visibility or knowledge of just how often incidents occur at their companies. Today, cybersecurity risk and reputation are key components of brand trust. They are significant

considerations in B2B contract negotiations and deal-making. Like it or not, they are now boardroom conversations. That's why you're reading about them here.

At the same time, organizations are facing a growing number of new requirements from global regulators focused on consumer protection, securities, and corporate governance. Customers—both business and consumer—expect cybersecurity to be an integral part of the way organizations operate and build products. So, no matter how many cybersecurity incidents an organization must publicly disclose (pro tip: disclose more than you have to), this is no longer a one-off exercise with a clear-cut beginning and end. Rather, speaking publicly about cybersecurity is either an ever-present albatross around your neck or an opportunity to proactively build trust before you need it.

Companies that earn credibilty for their security investments and capabilities receive the benefit of the doubt, even when their overall brand reputation is struggling.

As a member of the board, do you know how your company fares in terms of trust and reputation around cybersecurity and privacy? Are you encouraging proactive and transparent communications from your executive teams to establish trust in how the company treats security investigations, incident response, and customer support? It's not enough anymore to simply ask how the security team is keeping up with the growing threats. Executive teams are also responsible for communicating those efforts to business stakeholders.

Perhaps the most important role of a board member is allocating appropriate resources to cover not only the technical aspects of security, but the human-to-human aspect as well. If your security team doesn't have a dedicated security communications role, create one. Someone needs to be focused on this full-time while the CISO is focused on communicating with you.

Here's another tip worth keeping in mind. Companies that earn credibility for their security investments and capabilities receive the benefit of the doubt, even when their overall brand reputation is struggling. Here's an example. I was leading global security, privacy, and engineering communications at Uber in 2017, when I received an email on Christmas Day from a weekend editor of a popular tech publication who didn't normally cover cybersecurity topics. (I am not naming him because I have no desire to pick a fight or embarrass anyone.) He was calling to fill in the blanks on a story already in the pipeline for publication regarding claims that Uber was trying to stiff a security researcher who had submitted a vulnerability report to its bug bounty program.

This was seemingly a slam dunk, anti-Uber clickbait headline. Bug bounty programs typically pay external security researchers for finding vulnerabilities in an application or system so they can be fixed before they're exploited by an adversary. If Uber was trying to get out of paying a well-intentioned researcher for helping to secure its products, this would have been an easy story to believe and add to the company's reputation for being untrustworthy.

I instantly knew exactly which security issues the editor was calling about because I'd worked with Uber's bug bounty team on their communications with

the researcher over the past few weeks. The researcher had violated the terms of our program, provided no information to validate his claims, and attempted to bully a member of our team.

In a matter of minutes, I was able to explain the situation to the editor and refer him to several public comments made by prominent and well-respected security experts from other large tech companies as well as other security researchers who'd seen this man's allegations on social media. They not only condemned the abusive behavior demonstrated in the researcher's correspondence with our team, they acknowledged the professionalism and accuracy of our security team's response.

The article still ran (Christmas is a slow news day), but the story was very different now. The editor characterized Uber's response as detailed and professional, while the researcher's behavior was called combative and labeled harassment. I have no doubt this researcher likely has many redeeming qualities outside his engagement with our team, but he hadn't considered how his actions in this situation would help or hurt his own credibility.

For Uber, a cybersecurity story that easily could have become a PR crisis on Christmas, ended with a public gathering of unlikely, unsolicited, yet influential allies. Despite the company's perceived shortcomings overall, the security team demonstrated in that moment that Uber had redeeming qualities as well. We'd considered from the very first correspondence that our response could proactively and positively impact the way people thought about Uber.

Again, there was no breach here, and we could have adopted a reactive approach with a simple company statement defending our position. Being proactive about our security reputation led to the decision to put communication advisors alongside our bug bounty team to guide our engineers—and that gave us more control.

For board members concerned with the impact of security issues on external perception, it's a good exercise to ask how security communication plans extend beyond mandatory disclosures to build goodwill and establish allies in advance of the next security incident. Ask for communication-specific tabletop exercises and note where the business needs more reliable relationships, intel, and experience to help steer the outcome.

BUILDING TRUST WITH PROACTIVE COMMUNICATION: DEMONSTRATE HONESTY AND COMPETENCE

So much of what a CISO does is focused on communicating the impact of their team to the business. Why not turn that on its head and ask how they're educating external stakeholders like business partners, customers, and regulators about all the work they're doing to be trusted stewards of data, shareholder profits, and consumer safety?

In cybersecurity, trust is earned by consistently demonstrating two things well: honesty and competence. Poor execution is enough to invalidate good intentions. These are familiar principles for corporate communication teams, and they have even more importance for long-term credibility issues like cybersecurity that build on all previous incidents. The statement, "Security is our top priority" is rendered meaningless when accompanied by a notification that an organization's security systems failed to protect its clients and/or customers.

If security is, in fact, a top priority, why are so many organizations scared to talk about it proactively? Could it be that it hasn't truly been prioritized by the business to the extent we want people to believe? Is it not the role and duty of corporate communication professionals to advise organizations on how to close the gap between perception and reality by helping them become who they aspire to be? If security is not the top priority, don't say it is. If it should be, dust off your powers of persuasion in order to make that statement true.

One of the most common pitfalls organizations make when it comes to managing cyber incidents is to wait for an incident to occur before engaging.

During my time at Uber, giving conference talks and writing blog posts was very popular among our engineering teams. It was a critical part of the company's culture for technical teams to exchange experiences and learnings with peers in the industry. Solving shared technical challenges and adopting best practices delivered net-positive results for everyone. At the same time, I knew that if the public believed we lagged behind in basic application security practices, we'd never have the credibility we needed to be given the benefit of the doubt if a serious incident occurred. We needed to build credibility in advance.

So, I implemented a requirement for engineers to close all security tickets assigned to them before seeking approval to publish a blog post or speak publicly about their work. After all, why would we bring more public attention to products or areas of our tech stack that we knew had vulnerabilities or security weaknesses? I couldn't honestly tell anyone that security was a priority if we weren't even holding software creators accountable for their products. The end results were a shorter lifetime for vulnerabilities in our code, less time spent responding to media inquiries about bugs found by external parties, and more time for telling our security story proactively, on our terms, with the proof to back it up.

The second element of trust, competence, is where corporate communication teams often feel less comfortable. That's why support and encouragement from the board are so important. Publicly sharing details about technical cybersecurity work often requires more than surface level subject matter knowledge. You may need to convince more risk-averse colleagues, like legal or PR compatriots, to engage in proactive communications as well, and that is often out of their comfort zones. Understanding where your organization's risk tolerance intersects

with cybersecurity best practices is a helpful place to start, showing that even if your organization isn't (yet) leading the pack on cybersecurity innovation, at the very least you're aligned with industry standards.

Proving honesty and competence means avoiding hype, misrepresentations, or false statements. Many costly cybersecurity and data privacy settlements between private sector companies and the Federal Trade Commission (FTC) start with inaccurate statements on websites or marketing materials. If you can't prove it, you probably shouldn't say it at all. And if you want to say it, especially if you know it will help in the event of an actual cyber crisis, then prove it first and publish it now, so it's ready when you need it. For example, if your organization requires customers to create user accounts, confirm your organization is following best practices for multifactor authentication and make that information available on your website.

PREVENTING CYBER INCIDENTS FROM BECOMING A CRISIS: A LESSON ON INCENTIVES

One of the most common pitfalls organizations make when it comes to managing cyber incidents is to wait for an incident to occur before engaging. A traditional crisis communication approach may offer helpful principles for responding to an incident after the fact, but it lacks structure for preventing or minimizing incidents in the first place. The corporate communications function has valuable skills and organizational visibility to guide a business away from a disaster, so simply waiting for a crisis to occur is a dereliction of duty. And if they're paying attention, directors can make a difference. As a member of the board, it's important to understand that expressing your expectations for security communications goes a long way in determining which approach the communications team will take.

There are best practices for technical security teams to harden their potential attack surfaces. It's expected that an organization serious about security would consider potential risks throughout product development, employee onboarding/offboarding, and supply chain relationships in order to prevent avoidable incidents from occurring. The same should be true for corporate communications teams. We can help organizations minimize or completely avoid incidents that escalate to the point of crisis.

For example, multiple U.S. tech companies have been fined and sued for misleading users about how their contact information collected for account security would be used. Both Facebook and Twitter were issued hefty fines from regulators in recent years for using telephone numbers for targeted advertising that were provided by users specifically to enable two-factor authentication. While their PR teams insisted for years that this information was only used for security purposes, the truth is that they didn't really know. They weren't

engaged deeply enough in the day-to-day work of the business to adequately ensure the accuracy of long-held assumptions, and they weren't notified when things changed.

The most common inquiries I received from journalists during my time at Uber were about credit card fraud—consumers seeing Uber charges on their credit card that weren't showing in their trip history. The volume of media questions about this topic easily outnumbered questions about advanced cyber threats 10:1. This was an important factor for consumers in deciding whether they could trust the security of Uber's platform overall, and I wanted to provide a compelling rather than a defensive answer.

How an organization responds to an incident has a greater impact on its reputation than the incident itself.

This led me to develop a close partnership with Uber's anti-fraud and account security teams. We developed a reliable process for confirming the accuracy of every claim brought to us by the media. (More than once I had to break the news to a reporter that it was actually their own teenager who was using their account, not a hacker.) We were able to influence critical product decisions that increased consumer security and provided a compelling response for media inquiries, such as how much personal information should be visible in a rider's account. Credit card numbers were not shown in the mobile app or web account, so fraudsters couldn't steal that information by hacking into individual user accounts. That message resonated with media because it dispelled a common myth and demonstrated we'd thought proactively about consumer security.

As a result, many of these stories simply died on the cutting room floor. Few reporters at the time wanted to report a positive story about Uber, and the stories that did survive became opportunities for us to talk about our security investments and build trust in the platform. Over time we added even more anti-fraud capabilities, such as blocking credit card numbers stolen from other platforms or services from being used on Uber's platform. Every time, it was an excuse for me to engage with investigative and consumer protection reporters and give them another reason to fact-check their next "gotcha" story. Our team even became go-to experts for questions journalists had about the security of our competitors' platforms because their corporate communications teams couldn't (or wouldn't) respond with the same level of detail and concern that we did.

WHEN SH*T HITS THE FAN: PREPARING FOR THE WORST

How an organization responds to an incident has a greater impact on its reputation than the incident itself. The emotion solicited by your response will linger even after the details are forgotten. This includes the technical detection and remediation efforts as well as internal and external communications. A proactive cybersecurity communications strategy aligns with an organization's technical playbooks to consider how public perception impacts—or is impacted by—potential security threats.

For example, vulnerabilities discovered in widely used open source packages simultaneously affect thousands if not millions of organizations. If you're exposed, you're usually one among many and, so long as your technical response is sufficient, you may not experience any public attention for being vulnerable. If, on the other hand, you're the victim of a targeted attack, there are fewer relevant voices to satisfy the media's appetite. If you don't engage, the possible alternative sources will be far less informed, and thus, less accurate. They may or may not give your organization any credit at all for the efforts you made to prevent or minimize damage, or for how well you responded.

Being proactive gives your organization more options and resources for minimizing or eliminating the impact of a potential incident. I mentioned earlier how valuable it can be to have important information prepared in advance. It's impossible to include all relevant context and justifications in media statements or customer notifications. There simply isn't space. News outlets will not quote a five-paragraph essay, so if you want additional information to be considered by your most important stakeholders, you have to create a home for it and establish a norm for sharing information in this way.

Many engineering-first companies maintain network performance websites where they report updates on any service outages. This is a good model for conditioning customers and media to look for more information beyond what's in your media sound bite. These details matter because, over time, this is how you build credibility before something happens.

Keeping this information up to date is critical. As your technical systems change, so should your public content. New products and features under development should have a security story to accompany the launch, explaining how you addressed any potential security risks. Help your technical teams share their learnings with their peers, not just their cutting edge work. This is how you earn informed allies (perhaps even unexpected ones) who can speak up for you when needed.

Finally, consider how closely your response plan follows your day-to-day escalation path. A playbook that only gets used once in a while gets dusty and requires more cognitive effort to follow. Playbooks and plans that don't evolve with your organization are quickly abandoned when situations become intense. I prefer response plans that mirror daily operations as much as possible with appropriate escalation triggers based on severity and legal requirements.

If corporate communications wants to have oversight and input on what is said to various stakeholders in an incident notification (because someone will share those messages with media), then they need to be engaged in ongoing security communications with stakeholders. A breach notification shouldn't be the first introduction stakeholders have to your security team. That's how crises happen.

CHAPTER 3

WHAT I NEEDED TO KNOW ABOUT CYBERSECURITY AS A CEO AND LATER AS A BOARD MEMBER

ANDY GEISSE

As the CEO of a startup, my first experience with cybersecurity was … missing in action. There was no experience. My "IT department" consisted of a contractor who ran our server and reported to the CFO. This was in the 1990s, before the internet transformed business. We had PCs, we had systems that those PCs connected to, and we even had email! But we were not familiar with the term "cybersecurity." Most of our employees had one password they used for every system, and you'd be surprised how many desks you could walk by and see those passwords posted. Security never even occurred to us.

A couple of years later, as the CEO of two different startups in Chile, my cyber discussions with the boards, with the chief information officers (CIOs) who reported to the CFOs, and with management were remarkably similar. There were none. The same was true when I was the CEO of a cellular company in New York. We never discussed it at the CEO or board level. Our IT team was expected to take care of it and keep us safe. It went without saying.

Little did I suspect that my first real experience with cybersecurity would be in IT itself. I was asked to run the software group for a Fortune 500 company with a worldwide programming staff that supported over 4,000 applications. I quickly learned that most of the conversation in application development is around functionality for the business and how to do more with less. Security was an afterthought. Usually the security team would come in and do app reviews and point out the holes we had and where we needed to add functionality. Security was never first in the application programmers' priorities.

Things changed abruptly when we were hit with our first major worm right before the turn of the century. It brought down applications across the whole company, infecting many of our systems and servers. We spent the entire weekend, day and night, on calls trying to restore applications and eradicate the worm. We eventually figured out how the worm got in. An employee who wasn't even in IT had attached a server to our internal network and the internet without basic security.

It was an extremely painful lesson in cybersecurity. I was on the phone with the CEO and every top business executive trying to explain something they had never heard of and had no concept of. Yet it greatly impacted our customers, our business brand, and it had a major financial impact. We immediately tried to identify all "rogue" systems inside the company—a task we found to be nearly impossible (and never-ending). We then tried to apply basic security features to each system the various business units had. This was when I started thinking that cybersecurity, far from an afterthought, needed to be considered first.

When I started meeting with the board, I quickly figured out that they didn't want to know about cybersecurity. They just wanted to know that we were "safe and secure."

LEARNING TO TALK ABOUT CYBERSECURITY TO BOARDS

Obviously, a lot has changed over the years. Cybersecurity is a household name. Everyone knows about it, even people who have nothing to do with it professionally and couldn't explain it very well to their children, know enough to worry about it.

Things started changing dramatically for me when I found myself working at a global telecom company with a very experienced chief information security officer (CISO). By this time I was the CIO, and I spent quite a bit of time working with the CISO to understand how we could better fortify our systems, how we could think about security up front in our application development processes, and how we could better manage our own internal security.

That close relationship with tech extended to my next CEO role. I ran the phone company division (consumer and business telecom groups), and eventually I was CEO of the business group. In my new role cybersecurity was not only something we used internally to protect our systems and data, but something my group sold as well. We were responsible not only for our own internal behavior, but for our customers' networks. We were the cybersecurity professionals!

That was when I learned my first important lesson about cybersecurity and boards of directors. When I started meeting with the board, I quickly figured out that they didn't want to know about cybersecurity. They didn't want to talk about it, understand it, or have anything to do with it. They just wanted to know that we were "safe and secure." And they weren't alone. Even my top customers didn't really want to know a whole lot more. They kept asking me "can't you just deliver a clean pipe," meaning data with no security threats. That was impossible to do. Yet data losses, hacks, denial of service attacks, employee/contractor lapses and intrusions—all of that and more happened daily.

I learned quickly that even if the board and customers wanted to take

cybersecurity for granted, as the CEO I could not. I had to work with the CISO to develop a security framework, be able to audit against that framework, and report the results to management and the board. There was nothing worse than having to go to the board's audit committee to explain a cyber threat and intrusion. When we did, we had to have the right reports to explain what we were doing in a way a non-technical board could understand.

Later, when I was a board member, some of the reports I found useful were ones that helped me understand brand and business continuity risks. These included reports that showed us intrusions and how they were being mitigated; loses of customer and employee data and the steps we were taking for each; issues found in the cybersecurity audits and the severity and how they were being addressed. Let me add one more that is often overlooked: reports on employee and contractor cybersecurity education. As important as it is to track security issues, it's also important to track efforts to prevent security issues.

GETTING A BOARD'S ATTENTION

So how do you get their attention? How do you make the board understand that cybersecurity is too important to ignore, or treat as an afterthought? It turned out that news reports were great teaching devices. Some high-profile breaches made a real impression. The **breach at Target** in 2013 was a big one. As many as 110 million customers' data records (40 million credit and debit records and 70 million customer records) were compromised. Target's profit fell nearly 50% in the 4th quarter of 2013. The company lost customer confidence and the stock fell almost 10%. That got the board's attention! I bet it got the attention of most boards. Several leaders in Target's IT department lost their jobs over this breach. Yet it was a hack that was incredibly hard to find. It had gotten in through some contractor clicking on the wrong file. If the right employee/contractor education had been done, could it have prevented this hack?

The 2014 Sony Pictures attack was an event that got the attention of boards everywhere.

Another breach that made an indelible impression was the **Sony Pictures film studio hack** in 2014. It happened shortly before the planned release of a fictional movie about the assassination of North Korean leader Kim Jong-un. It shut down the studio, cost $35 million in investigation and mediation expenses, and erased Sony's computer infrastructure. Above all, it embarrassed Sony with leaked emails about and from executives and stars that turned the mess into a monumental public relations disaster—the kind they make movies about.

What happened to Target and Sony forced boards to sit up and pay attention. They started to realize the huge impact cybersecurity can have on business continuity, on brand reputation, on market value. And, of course, on customer confidence. This was no longer a "back room audit" issue.

One of my goals was to impress on boards that a major data loss can bring the business to its knees. And the regulatory implications have skyrocketed given the data privacy laws in Europe, California, and a growing number of states. Cybersecurity is not just "an IT issue." I often use examples I find in the press where a company's marketing or human resources department lost sensitive information. The whole company must be aware and involved.

THE CHALLENGE FOR STARTUPS

By the time 2015 rolled around, I found myself facing a new challenge. I was starting to participate on boards of startups. By this time I was an operating partner at Bessemer Venture Partners (BVP), and based on my relationships in the startup world, I began to realize that cybersecurity was not a major topic of discussion at many of those boards. The new companies were so busy building their products, selling their products, raising money—all the things that go with being a startup—that there just wasn't time. Or so they thought.

To sum it up, governance is the key. Especially for startups, because that's often the last thing on their minds.

I was on one startup board where the issue seemed to be handled by the audit committee, which looked at the issue from a risk management perspective. But this audit committee, like others I saw at startups, was filled with former CFOs, who were much more steeped in financials than tech, and really didn't understand cybersecurity or its implications. One of those startups had a major leak of customer information caused by a marketing executive extracting data and putting it on a cloud database to study the analytics. The marketing group didn't have any security at all on the data. Why would they? These were marketing executives, not IT or security folks.

Something good came out of this. The company's leaders recognized they were in over their heads. The audit committee asked me and another board member who had cybersecurity experience to get involved. What we found was typical of startups: there was no CIO, there was no CISO, everything was handled by the product folks who were technically savvy but much more focused on product features and releases. There wasn't a security framework to audit against, no reporting, no understanding of the risks to brand reputation, customer confidence, etc. What made the situation particularly fraught is that this company handled sensitive communications for companies. One major hack could have taken the company down, especially since its service was cloud-based. The whole area of cybersecurity required an entirely different way of thinking.

So what did we do? We set up a cybersecurity committee of the board. We used it to push management to appoint a CIO and a CISO who could report to us the various issues, risks, and mitigation activities. We then hired an outside

consultant who helped the new CISO get a security framework we could use to audit against. We ran a complete review of the company using that framework, and we created a list of vulnerabilities and priorities. We established reporting capabilities that would be reviewed each month, looked at actual incidents that had occurred, additional vulnerabilities, and prioritized the mitigation of all those vulnerabilities.

BESSEMER'S FIVE CYBERSECURITY LESSONS

1. Build a cybersecurity culture.

2. Invest in identity.

3. Secure your cloud and development environments.

4. Manage your data assets and environment.

5. Monitor your third-party risks.

BOILING IT DOWN

To sum it up, governance is the key. Especially for startups, because that's often the last thing on their minds. Startups are all about delivering the product or service. Often for the leaders it feels too early to worry about audit committees and risks. And the board, too, is almost always focused on business results and company strategy. The board doesn't run the company. Its job is governance. It must worry about brand reputation. It's supposed to ask questions and focus on larger issues like strategic alternatives and the company's long-term health.

But neither startups nor any other company can afford to ignore cybersecurity. The board should be asking questions about it. I have often done that myself at those meetings, asking management how they measure this area, how they report on it to the board, and who is responsible. The audit committee? A separate cybersecurity committee? A board member who has cyber experience and can do a complete review of the systems with the technical folks and then report back to management?

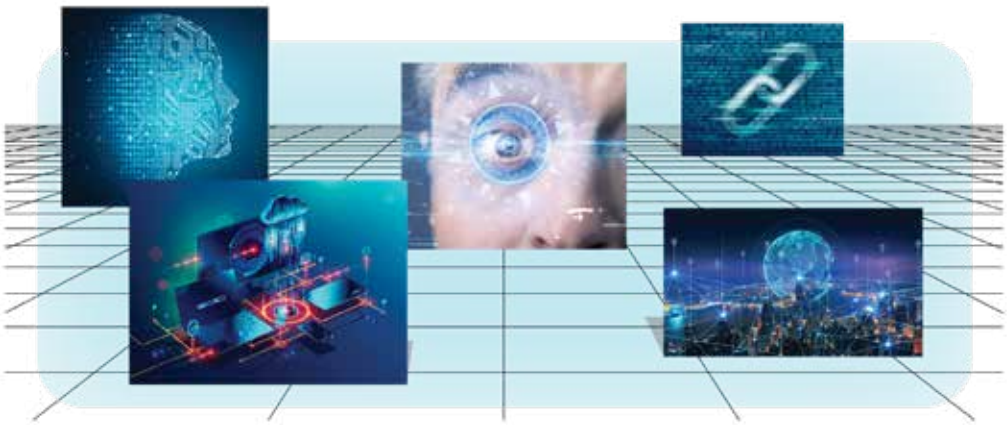
Sometimes it comes down to this: The board at a startup needs to make management understand that it cannot afford to ignore basic needs, any more than an EV car manufacturer focused on developing a perfect battery can afford to skip the steering wheel. The board needs to communicate to management that today's companies need IT departments and CISOs who can oversee cyber risks and vulnerabilities and report these up the chain. And hire outside talent, if they need to, in order to mitigate the risks. Failing to understand these principles is placing the entire enterprise at risk. And that is the absence of governance.

BUILDING CYBERSECURITY COMPETENCE ON THE BOARD

- **Recruit board members with cybersecurity expertise.**
- **Ensure management has a proactive rather than a reactive strategy.**
- **Develop cybersecurity awareness and knowledge among board members.**
- **Leverage external resources, such as cybersecurity consultants or advisers.**
- **Establish effective communication with the board on this subject.**
- **Utilize clear and concise reporting formats to convey cyber risks.**
- **Encourage proactive reporting of cyber incidents and near-misses.**
- **Conduct regular cybersecurity briefings and training sessions for the board.**
- **Align cybersecurity metrics and performance indicators with overall business objectives.**

CHAPTER 4

EMERGING TECHNOLOGY AND THREATS: THE LANDSCAPE OF OPPORTUNITY AND RISK



DAVID NEUMAN

Many years ago, I was asked to speak to a group of board members from various Fortune 50 companies at a retreat. The event was organized by a group that brought them together and created a safe space for them to discuss and learn from industry experts on various challenges they had in common. Cybersecurity was one of them, and I was their expert. I described the benefits of cloud adoption and the risks that must be understood. These were highly experienced business leaders, but their questions and discussions surprised me. Fortunately, they were comfortable asking questions that leaders should always be willing to ask. My answers were constructive but candid.

Our conversation led to a discussion that has stuck with me ever since. A board member said, "We sometimes ask, 'Are we protected from cyberattack?'" I asked her if she had received satisfactory answers. She replied with an unequivocal no. The answers were always filled with the nicknames of cyber adversaries (which she didn't recognize), technical details about attacks, and vulnerability numbers that didn't tie to business risk. Others nodded in agreement, indicating that they had had similar experiences. When I asked what usually followed, many explained that they often moved on to other issues on their packed agendas. They were frequently frustrated that they couldn't get the information they needed to perform their roles as board members.

I suggested they were asking the wrong questions. I recommended they try the following instead: Do we understand the most critical digital assets to our business

and their dependencies? Do we have the right capabilities, response plans, and experienced leaders to respond to an attack when (not if) it happens? If the answer to the first two questions was yes, how did they know? These questions help illuminate where technology has introduced business risks. They force technologists to speak in a business risk language that everyone at the company can understand, including board members and other leaders who need to make informed decisions.

Building on that conversation, my aim now is to demystify the landscape of emerging technologies and the unique set of challenges (and opportunities) they bring.

By reframing the dialogue around emerging technologies in terms of business risk, board members and business leaders can not only ask the right questions but also derive actionable insights that align with their strategic goals.

Let's start with the basics. The need for translating technical jargon into the language of business risk has never been greater. This is especially true as companies venture into adopting transformative technologies like artificial intelligence (AI), blockchain, and the internet of things (IoT). These technologies offer enormous potential benefits, but they also contain a lexicon of risks that must be clearly understood and managed. By reframing the dialogue around emerging technologies in terms of business risk, board members and business leaders can not only ask the right questions but also derive actionable insights that align with their strategic goals. With that in mind, let's explore the emerging advancements redefining the corporate landscape.

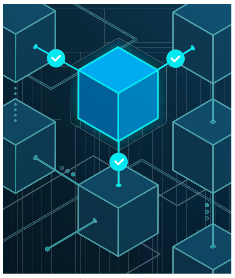
INTERNET OF THINGS

Nest smart thermostat

The actual value of IoT lies in its connectivity and data collection capacity. From smart thermostats in office buildings to advanced sensors on manufacturing floors, IoT devices gather a wealth of data that can be analyzed for actionable insights. For example, IoT can monitor manufacturing machinery in real time, allowing for predictive maintenance that saves time and money. In retail, IoT devices can track consumer behavior and inventory levels to improve customer experiences and streamline operations. In agriculture, IoT sensors can monitor soil conditions, crop health, and weather patterns, providing farmers with the insights they need to optimize yield. By facilitating more intelligent decision-making, IoT has the potential to revolutionize almost every facet of business.

As IoT ecosystems expand, they create multiple entry points that could be attacked. It's crucial to consider the potential fallout should one of these interconnected devices become compromised. Such an event could lead to data loss and operational disruptions, which could significantly impact revenue and reputation. To mitigate these risks, businesses must continually assess their IoT networks' security protocols. The risk isn't merely technical; it's operational. When thinking about IoT security, one must also think about supply chain integrity, data governance, and the financial implications of a security lapse.

Moving on to blockchain, this technology goes far beyond its most famous application: cryptocurrency. The decentralized nature of blockchain can make



transactions and data storage more transparent, secure, and democratic. This is particularly useful in sectors like supply chain management, where blockchain can provide immutable records of product movement from manufacturer to distributor to retailer. For industries like health care, blockchain can secure the integrity of medical records. In finance, blockchain can expedite transactions and reduce fraud, thereby minimizing costs and improving efficiencies. Moreover, smart contracts can automate many business processes, reducing the need for intermediaries and slashing operational costs.

It's easy to be captivated by the promise of secure, transparent transactions. However, this doesn't make the technology invincible. Smart contracts, a cornerstone of many blockchain applications, can contain exploitable vulnerabilities. If a smart contract is compromised, the integrity of the entire blockchain to which it's linked could be at risk. From a business risk perspective, this translates into contractual disputes, financial loss, and reputational damage. Therefore, businesses should conduct thorough due diligence before implementing blockchain solutions, considering legal and compliance risks alongside technical ones.

ARTIFICIAL INTELLIGENCE

The transformative power of AI comes from its ability to process enormous amounts of data at speeds no human could match, providing unprecedented insights into customer behavior, market trends, and operational efficiencies. AI's application ranges from simple tasks, like customer service chatbots, to complex processes, like predictive analytics and automation. Marketing departments can use AI to analyze consumer behavior and tailor promotions, increasing sales and customer loyalty. In health care, AI algorithms can analyze medical images and provide diagnostic suggestions, thus aiding medical professionals in making more accurate decisions faster. Additionally, AI can automate routine, time-consuming tasks, allowing human employees to focus on more complex, value-added activities.

The strength of AI—its ability to learn from data—is also its Achilles' heel. The AI algorithm could make damaging decisions when the training data is tampered with or poisoned. If an AI system that controls inventory, for example, is compromised, it could lead to stockouts, excessive inventory costs, and lost sales opportunities. The ramifications could extend beyond the immediate financial loss, including long-term customer attrition and brand devaluation. Hence, businesses adopting AI should invest in securing the data pipelines and operational processes surrounding their AI platforms.

AUGMENTED AND VIRTUAL REALITY

The realm of immersive technologies, like augmented reality (AR) and virtual reality (VR), presents a rich tapestry of opportunities for businesses looking to transform user experiences. Initially confined to gaming and entertainment, these technologies are now making significant inroads into the corporate sector,

Apple's Vision Pro

fundamentally changing how businesses interact with customers, train employees, and design products. Consider the retail industry, which has been especially receptive to AR's possibilities. Imagine a consumer standing in a brick-and-mortar store, smartphone in hand, using an app to overlay digital information onto physical products. The app could provide immediate access to customer reviews, alternative color options, or even allow the user to visualize how a piece of furniture would fit into their living room. Such enhancements engage the customer and can substantially impact purchasing decisions, adding a new dimension to the in-store experience.

VR, on the other hand, offers potential benefits for sectors that rely heavily on training and simulation. For example, the health care industry has been experimenting with VR to create virtual operating rooms where surgeons can practice complex procedures in a risk-free environment. Similarly, companies in sectors like manufacturing or energy can use VR simulations to train employees on handling hazardous materials or emergencies without the associated real-world risks. The immersive nature of AR and VR doesn't just create a wow factor, it offers real, measurable value. Businesses are seeing increased engagement rates, better training outcomes, and even boosted sales figures when implementing these technologies strategically.

Businesses using AR and VR for customer engagment, training, or data visualization must be mindful of how data is stored, encrypted, and used, lest they find themselves in a privacy scandal.

As always, however, these innovations come with a downside. The transformative potential of AR and VR is accompanied by new risks that could affect businesses at multiple levels. As with other emerging technologies, the magic of AR and VR lies in their ability to offer enriched experiences, yet this magic comes with unique vulnerabilities.

These applications often require access to cameras, microphones, and location services. This raises the risk of unauthorized data access and breaches, not to mention the potential to misuse sensitive information. Businesses using AR and VR for customer engagement, training, or data visualization must be mindful of how data is stored, encrypted, and used, lest they find themselves in a privacy scandal. This risk extends beyond data to include potential issues of user surveillance, which would severely erode trust and could have legal repercussions.

Next, there's the threat of content manipulation. Because AR overlays digital information in the real world and VR creates entirely artificial environments, there's potential for what's known as "deepfake" technology to generate highly convincing but completely fabricated scenarios. In a business context, this could mean manipulated virtual meetings, falsified recordings, or deceptive training scenarios. The implications range from reputational damage to severe legal and financial consequences, depending on the scale and intent.

User health and safety also present a concern. Extended use of these technologies can cause physical and psychological damage, including motion sickness, eye strain, and more severe conditions. Businesses utilizing the apps

for employee training or customer services must recognize these health risks to mitigate potential liability and ensure users' well-being.

QUANTUM COMPUTING

Lastly, quantum computing is expected to be one of the most transformative technological frontiers for business in the coming years. Unlike classical computing, which uses bits to represent a zero or a one, quantum computing employs quantum bits or qubits. These qubits can exist in multiple states at once due to quantum phenomena like superposition and entanglement. The result will be an exponential increase in computational power, offering the ability to solve problems and perform calculations at previously inconceivable speeds.

This could change industries that are particularly reliant on heavy computational tasks. Take cryptography, the practice of secure communication, as an example. Quantum computing provides pathways to entirely new forms of secure communication through quantum cryptography, which could offer unprecedented security. In the realm of material science, the possibilities are equally groundbreaking. Material scientists often need to simulate molecular structures and reactions, requiring enormous computational resources. Quantum computing could accomplish these simulations with a level of detail and speed currently out of reach, potentially accelerating the discovery of new materials with customized properties. Imagine lightweight yet solid materials for construction or highly efficient, environmentally friendly energy sources.

Similarly, the drug discovery process could be dramatically accelerated, transforming pharmaceutical research. At present, simulating the interactions between various proteins and compounds is a grueling process, sometimes taking years. A quantum computer could simulate these interactions at much higher speeds, potentially reducing the time it takes to discover new drugs from years to months or weeks. This capability would be a boon for the rapid development of treatments for emerging health crises.

Again, there's a downside. While the technology stands to revolutionize various sectors, it poses significant challenges to existing systems and protocols, particularly cybersecurity. One of the most talked-about threats associated with quantum computing is its potential to break current cryptographic systems. Many modern security protocols rely on the computational difficulty of factoring large composite numbers into their prime components, which could be done exponentially faster with a quantum computer. This means that secure data transmission, digital signatures, and online banking systems could all be rendered vulnerable. The business risk here is not just data loss or theft; there's also the potential for massive financial fraud and a consequent erosion of customer trust, which could devastate any business.

Additionally, there's the threat of "quantum sabotage." As quantum computing would enable incredibly complex simulations and problem-solving, it could also

be used to model and potentially exploit weaknesses in various systems, from financial markets to energy grids. An attacker with access to quantum computing capabilities could uncover vulnerabilities not readily apparent through classical computing methods, posing new threats that are not yet fully understood.

FINAL THOUGHTS

Emerging technologies are not just disrupting the way business is done; they are redefining it. Each offers unique advantages that can lead to increased operational efficiency, reduced costs, and enhanced customer experiences. The interconnected nature of these technologies means that their combined impact is greater than the sum of their parts. Businesses strategically adopting and integrating these technologies stand to gain a significant competitive advantage in an increasingly digital world.

It's essential not to compartmentalize cybersecurity as a mere technical issue but to view it as an integral part of overall business strategy, affecting everyting from operational continuity to brand reputation.

While they offer groundbreaking opportunities for business transformation, they also represent new forms of risk that must be carefully managed. As companies forge ahead in this digital age, those investing in understanding and mitigating cybersecurity risks will be best positioned for long-term success. For business leaders and board members, the task isn't just to adopt new technologies and thoroughly understand their associated vulnerabilities. The future may be fraught with challenges, but a proactive approach to understanding the opportunities and threats of emerging technologies will prepare businesses to face them effectively. To navigate this complex landscape successfully, board members and business leaders must understand these threats and contextualize them within the broader framework of business risks.

One vital approach is ensuring that cybersecurity strategies align with broader business objectives. It's essential not to compartmentalize cybersecurity as a mere technical issue but to view it as an integral part of overall business strategy, affecting everything from operational continuity to brand reputation. That's what makes proactive due diligence so important. A passive, reactive approach to cybersecurity is inadequate in today's complex digital environment. Regular audits of your organization's cyber ecosystem can provide valuable insights, and staying updated on the latest advancements in cybersecurity can equip you with the tools to protect your business more effectively.

Finally, effective communication is critical to bridging the often-significant gap between technical teams and business leaders. Encouraging discussions that translate technical vulnerabilities into terms of business risk ensures that decisions are made in a language that everyone, from board members to technical staff, can understand. This shared understanding enables a more robust and unified approach to managing the complexities introduced by emerging technologies.

CHAPTER 5

WHAT SHOULD A BOARD UNDERSTAND ABOUT AI?

DR. EDWARD AMOROSO

The governing role of the board member is generally well-defined, but often misinterpreted by observers. So let me start with a reminder of what corporate board members are expected to do. First, they must participate in reviewing and overseeing management. This requires the skill to know when and where to chime in, and this is easier said than done.

Second, they must participate in corporate strategy to help drive the company to an optimal decision when something truly consequential is being considered. Major mergers and acquisitions, for example, generally demand the attention of the board, but minor, day-to-day management decisions do not. Again, the principle sounds easy but sticking to it in practice is not..

Finally, corporate board members are expected to review and ensure the accuracy of important financial statements and other key data reported by the company. This does not imply using a fine-toothed comb to review every ledger item, but it does require active enough participation to ensure that public reporting is correct.

In addition to these responsibilities, board members frequently find themselves wading into new areas of concern that their companies confront. Cybersecurity is one such area that has spurred considerable debate about whether directors should play a significant role in making decisions, and if so, how involved they should be. Certainly, they are not expected to be security experts, but general agreement exists that broad awareness is now necessary.

A comparable issue involves artificial intelligence (AI). In recent months the public dialogue has been intense (to say the least). You can be sure there have

Business leaders will obtain guidance on future trends in the same way a radiologist can work with AI to view data and create accurate interpretations.

been innumerable private conversations behind closed doors. What are AI's implications for the business? And by the way, how will it affect security? Just as corporate directors are not expected to be experts in that field, they are not expected to be experts in AI. But a consensus is emerging that it is a key aspect of a board's responsibilities.

That said, what are the key considerations for board members on this subject? What should they know about the business implications and security implications? How much do they need to understand about this important technology?

BUSINESS IMPLICATIONS

The effects of AI on business will differ from one industrial sector to another, but some general statements can be made. Hopefully, these broad characteristics in the context of modern business will start the intellectual process for board members to begin integrating AI-related impacts to their governing responsibilities.

Below I've listed issues with an emphasis on how they relate to boards. I've skipped over those that might have a substantial impact on business but not on board responsibilities. Please keep this in mind. My guidance here is for boards, not day-to-day executives and practitioners.

Business Writing Will Become Software-Defined

Board members should recognize that for many years the quality of normal business writing has varied considerably. I'm talking about the memorandums, policy statements, agendas, meeting minutes, and other narratives that have been used in business for decades.

The problem is that so much of this writing has been just terrible, often including nonsensical reports, lengthy papers, and unclear narratives. Board members are certainly familiar, for example, with the large volume of often unintelligible materials presented in advance of meetings. This is common across all aspects of modern business.

AI will have a direct influence on the quality of these written artifacts because automation is so well-suited to this task. Auto-generated notes after online meetings are already common, and this will extend to a fully software-defined approach to business writing that will have considerable consequence on all forms of business communications. And it should represent a tremendous improvement.

AI Will Drive Business Macro Trend Analysis

Board members and corporate executives have depended for many years on the predictions and observations of trends in the marketplace. These often come from industry analysts who opine based on their admittedly limited view of the many factors that influence any type of prediction.

While there will always be interesting personalities who can provide incisive and even humorous observations on macro trends, the use of AI to analyze market trends will be a more common occurrence. The advantage AI has is that it can include virtually every factor for which some evidence is available to drive the optimal prediction.

Board members should expect to see a symbiotic relationship between human and automated market trend analysis. Business leaders will obtain guidance on future trends in the same way a radiologist can work with AI to view data and create accurate interpretations.

Customers Will Learn to Accept AI for Certain Applications
The ongoing debate with respect to the suitability and acceptability of using AI for certain applications will gradually wane in favor of societal acceptance of the technology. This happens for every new technological advance, including early industrial advances as well as the advent of computing.

The implications for board members is that aggressive adoption of AI, where appropriate, is the best course of action, and hesitation related to concerns about societal qualms is not recommended. Certainly, regulation and some degree of control will be required, but I advise businesses to be aggressive.

SECURITY IMPLICATIONS

The security implications for any type of business will involve offensive considerations ("Can we be hacked by an adversary using AI?") as well as defensive considerations ("Can we use AI to protect ourselves from an adversary?"). As one would expect, use of AI for both is an obvious corollary.

Below I lay out key security-related issues that emerge for board consideration. These should be addressed and coordinated across the entire management chain, and that should include the chief information security officer (CISO).

Major Adversaries Will Use AI to Attack
An important recognition that every business must understand is that their country of origin will certainly be targeted by nation-state adversaries using AI-based offensive measures. Organizations located in the United States, for example, should expect that countries such as China and Russia will most likely develop and use these methods.

The implication from a corporate perspective is that the front line for cyber threats is not the military or even the government, but rather is the distributed collection of data from business, enterprise, industrial groups, families, individuals, and other non-government targets. This is where an adversary nation will target with cyber threats.

Countries Will Need AI to Protect Infrastructure
Special consideration is obviously needed in protecting critical infrastructure, if only because the consequences of an attack can be so much more severe

than attacks to other sectors. For board members with responsibility to manage critical and essential services, the need to maintain secure defenses against AI-based smart attacks will be paramount.

An implication of the existence of AI-based offensive cyber methods is that organizations will need AI-based defensive measures to put a reasonable protection in place. It should be obvious that if an automated attack is being levied, then the defender will not be able to stop such an attack merely by using manual, procedural methods.

Board members should be cognizant of major investments in AI-based security infrastructure, not to review or approve the specifics of the technology or vendors selected, but rather to ensure that a strategic plan is in place to maintain the ability to stop these new forms of attack with a solid AI-based protection scheme.

The first obligation that every board member should recognize—and this point should be patently obvious—is that a basic working knowledge and baseline understanding of AI is a requirement for modern board members.

Social Engineering Will Benefit from AI

One attack that all board members will be familiar with involves the use of social engineering tactics to trick an individual into sharing sensitive information or to perform inappropriate tasks such as transferring money from one account to another (e.g., through fake text or email to a finance officer).

The foundational basis for social engineering involves skill to take advantage of the trust of a targeted person, and this requires having information about that target. Since AI is so good at collecting and analyzing information to establish context, it should be expected that social engineering, including phishing, will become more difficult to stop.

As with nation-state attacks, social engineering attacks will also demand a strategic plan to ensure proper protection. Boards should monitor their companies' defensive programs and should request to see evidence that these are working. Past methods, such as phish testing, will be useful components but will not be sufficient as the basis for such protection plans.

BOARD OBLIGATIONS

The first obligation that every board member should recognize—and this point should be patently obvious—is that a basic working knowledge and baseline understanding of AI is a requirement for modern board members. I wrote this article with this initial goal in mind.

In addition, however, there are emerging tasks that should become part of the day-to-day board ecosystem. While these tasks will evolve over time, let me point out a few below that I expect to see become important in the coming years. Local business conditions should certainly be used to tailor these general points.

Mergers and Acquisitions Must Include AI as a Factor

If the organization regularly performs mergers and acquisitions (M&A), then it must become a standard component of the evaluation rubric that potential AI

disruption be considered. The last thing any organization needs is to make a major investment in a company that will soon be disrupted or even replaced by AI.

The M&A team should be directed by senior leadership, with governance from the board, to ensure that this factor is thoroughly considered, especially for mergers that are sizable with consequence to the firm. Without such careful scrutiny, the possibility of a poorly conceived merger or acquisition seems possible—and potentially disastrous.

Human Decision-Making Will Not Be Replaced by AI
A commonly stated point in the popular media, and one that might have some influence on board member thinking, is the claim that AI will replace human decision-making. This may be true in certain situations where data is perused and processed in a structured manner. Radiologists, for example, might replace certain of their data tasks with AI.

The suggestion, however, that this will occur in the context of board strategy, corporate governance, and organization oversight is not reasonable. Good board governance will make use of technologies such as AI to ensure optimal context for discussion and debate, but robots are not likely to gain a seat at the board any time soon.

Cost Reductions Can be Considerable Using AI
One advantage that AI does bring to most business contexts is the ability to reduce cost. Customer care, help desk support, and other tasks that involve procedural steps will be good targets for such reduction. And boards would be wise to establish oversight where such cases are being considered.

The goal, obviously, should be to balance the needs of the firm for cost optimization with the needs of customers, who will demand high quality interactions, and also the needs of employees to feel safe that their career paths will be preserved—or at least guided toward areas that will complement the use of advanced technologies such as AI.

ACTION PLAN

The best course of action for corporate boards and individual board members may have already begun with perusal of this article. Education will be a key differentiator between boards, and any governance team that takes the time to learn the implications of AI will have a clear advantage.

My advice for an action plan is to over-index on education and training. The steps implied by the comments above should be included in local planning, but each organization is different. In the coming years, board members will have to earn their paychecks by developing effective plans for governance and oversight in this new technological era.

PART TWO

CYBERSECURITY AND GOVERNANCE

CHAPTER 6

IN A LANDSCAPE CRAWLING WITH REGULATION, LAWYERS CAN MITIGATE CYBER RISK

RANDAL MILCH

In the last five years, cybersecurity has become the focus of an unrelenting increase in regulatory scrutiny. The theory seems to be that increased regulation will produce better security. One way of looking at this is that companies are at last being held "accountable" for their profit-driven neglect of cybersecurity. Others see newly empowered state and federal regulators roaming the cyber battlefield to finish off the wounded, creating an atmosphere of punishment and distrust antithetical to fostering safety.

Although I favor the second view, increasing cyber regulation isn't going away. So the question is: How should companies respond? I say, call in the lawyers.

Increased regulation has changed the nature of cyber risk. In addition to the business risk associated with data loss or business interruption, companies now face significant compliance and governance risks arising from their cybersecurity efforts. From a risk mitigation perspective, these risks can be a net positive for companies with meaningful in-house counsel offices. As a former large company general counsel, I know that in-house lawyers can leverage compliance and governance obligations to help companies meet regulatory mandates. And, if the regulatory theory proves out, meeting those mandates should lead to better security.

I admit from the outset that there are limitations to my approach. First, there is a scope problem. The corporate legal department cannot be a critical part of better cybersecurity where there is no corporate legal department, which is the

case in much of corporate America. Although each of the hundreds of thousands of entities doing business in the United States faces potentially existential cyber risk, only a minority employ lawyers. We are expensive, and it is an entirely rational business decision to allocate scarce resources to product development, sales, or marketing instead. For many entities facing increasing cyber regulation—smaller public companies, private companies of all stripes, nonprofits—legal help comes from the outside, and then only when a problem comes up.

Second, there is a performance problem. At one extreme, compliance and governance can devolve into long to-do lists, and a drive to do no more than check those boxes. At the other extreme, compliance and governance can smother the flexibility and risk-taking that is critical to business success. Compliance and governance are not ends in themselves; the trick is using them to achieve laudable ends (like better cybersecurity).

The SEC is a primary regulator of the financial industry. For all other public companies, its cyber governance regulation is done in the name of public company disclosure.

Even with these limitations, there is a positive way of looking at increased regulation. What follows are my suggestions on how corporate boards and senior managers can use regulation and compliance as positive forces in the security wars. Companies can and should turn their lawyers into a critical cybersecurity asset in these complicated times.

Before I get going, I need to give you the stuff in fine print. In keeping with the scope limitation just noted, these suggestions are aimed at a public company that's not in the securities business, that's incorporated in Delaware, and that has a wide shareholder base . I focus on a public company because it is subject to the **disclosure regime** crafted by the Securities and Exchange Commission (SEC), but not one in the securities business to avoid an additional layer of prescriptive SEC cyber regulation. I choose a company with a wide shareholder base to avoid the fiduciary complexities associated with one or two founder shareholders who, through **dual class stock structures**, effectively control the board of a "public" company. And the company is incorporated in Delaware because **The First State's** well-developed corporate law has an outsize influence on issues of corporate governance and directors' fiduciary duties.

CYBERSECURITY AND CORPORATE GOVERNANCE

Cybersecurity has a widely held **definition**: protecting the confidentiality, integrity, and availability of data and networks. But what is corporate governance?

To answer that, we need to back up. The starting point is discerning who governs a company. The modern corporation is built on a foundational deal between a company's board of directors and its shareholders: In exchange for limited liability, shareholders cede the running of the company to the individuals they elect as members of the board. If the company faces ruinous liability and goes bankrupt, corporate creditors cannot go after the shareholders for unpaid bills. Shareholders can lose no more than their shares. This liability shield means, however, that shareholders cannot direct the business. The board does this in their stead.

Shareholders do retain a few levers of control. They have the opportunity each year to vote (or abstain from voting) for board-nominated directors and can approve or disapprove a small handful of other items—such as the company's independent auditor and senior executive compensation—proposed by the board. The vote tallies are almost always lopsidedly in favor of the board's recommendations. In return for being placed in charge, the directors owe fiduciary duties to the company and the shareholders, and the latter can sue the directors if they believe the directors have failed in those duties.

Corporate governance, then, is essentially everything the board does to run the company for the shareholders. The lion's share of the board's time is spent in four governance areas: working with management to formulate the **company's strategic goals;** setting the company's **risk appetite and tolerance** in achieving those goals; overseeing management's execution toward them; and allocating resources to achieve these endeavors.

Governance doesn't happen in a regulatory vacuum. For all public companies, the SEC has a lot to say on how boards go about governing, and over the last five years the commission has increasingly turned its regulatory attention toward cybersecurity. For most public companies, however, SEC cyber regulation is done in a round-about fashion. The SEC is a primary regulator of the **finance industry** and mandates affirmative, prescriptive cyber obligations for that part of the economy. But for all other public companies—where the SEC has no substantive regulatory muscle—its cyber governance regulation is done in the name of public company disclosure.

The New York Stock Exchange circa 1934

Let's take a minute to review how we got here. In the heady first years of the New Deal, Congress passed the **Securities Act of 1933,** governing the sale by companies of their stock to the public, and the **Securities Exchange Act** of 1934, creating the SEC and governing the markets on which those shares were traded. Disclosure by the issuing company of information material to an investment decision is the **bedrock investor protection** provided by both acts. As any public company general counsel knows, these disclosure requirements can be quite complex, and working out what to say and when to say it can be hotly debated topics within the C-Suite and, at times, with the board. But the disclosure rules effects go deeper. The SEC insists that disclosures be accurate when made and—as facts may change—over time. In order to ensure this accuracy, the SEC expects public companies to create internal reporting policies and procedures to keep relevant information flowing to the top of the house.

I'll return to policies and procedures in a bit, but a few words on the disclosures themselves and the somewhat bizarre nature of the "accuracy" that so concerns the SEC. As with so many aspects of cybersecurity, there is a strong degree of regulatory theatre here. Take as an example Verizon's cyber security disclosures, in particular the "Risk Factors" set out in its Annual Reports on SEC **Form 10-K,** with which for a few years I had some experience as Verizon's general counsel.

Cybersecurity first appears as a risk factor in Verizon's 2008 10-K, where a short, older warning about the potential effects of "natural or man-made disasters" was amended to a slightly longer disclosure noting: "Natural disasters, terrorist acts, acts of war, cyber attacks or other breaches of network or information technology security may cause equipment failures or disrupt our operations." The same disclosure is made in the next year's filing, and then is slightly enlarged in the 2010 10-K with the additional warning that "a failure to protect the privacy of customer and employee confidential data against breaches of network or IT security could result in damage to our reputation."

In 2018, the SEC reminded public companies that they were obliged to disclose the board's role in risk oversight, including material cybersecurity risks.

These basic risk disclosures evolved even before the SEC had issued any guidance to public companies on what to tell investors about cybersecurity risks. That changed in late 2011, when the SEC's first Cyber Guidance was published. It was a concise reminder to public companies that a "cyber incident" could be material to a reasonable investor's investment decision because victims of cyberattacks could also suffer significant financial, operational, and reputational harms. The SEC suggested that "appropriate disclosures may include:

- Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage."

The effect on public company disclosure was immediate. The description of the cybersecurity risks Verizon faced doubled in size in its next Annual Report filed in early 2012. Read it for yourself, but I doubt reasonable investors had a better handle on the risks Verizon faced in 2012 than they did in 2011, even after twice as many words.

Company disclosures were responding not to risks but to regulatory diktat. Consider this: A strong argument can be made that cyber risks have multiplied considerably since 2012, yet changes to Verizon's cyber disclosures through 2022 have—with one exception—only been incremental. The increments included moving "natural disasters" to its own risk factor (filed in 2013); mentioning that Verizon was at risk from attacks on its "service providers"; and that attacks could come from "any geography," including within or at the behest of nations where "law enforcement measures" are "unavailable or ineffective" (filed in 2015). The

important exception, first found in the **2013 filing** and repeated every year since, advised investors that while Verizon had not, to date, "been subject to cyber attacks or other cyber incidents which, individually or in the aggregate, have been material to our operations or financial condition, the preventive actions we take to reduce the risk of cyber incidents and protect our information technology and networks may be insufficient to repel a major cyber attack in the future."

While the actual disclosure has changed only a little in the last decade, I would bet that behind the scenes a significant amount of internal process change has occurred at Verizon (I have no inside knowledge, as I left the company in 2015). That's because the SEC has doubled down on insisting that cybersecurity-related information flow to the top of the house, and to the board of directors, putting greater pressure on the policies and procedures necessary to make that happen.

The SEC issued new and longer **cyber guidance** in 2018. The SEC focused in part on reminding companies that they must develop and maintain "robust disclosure controls and procedures" to "ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications." The "adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact" must be certified quarterly by the company's CEO and CFO as part of obligations imposed by the post-Enron **Sarbanes-Oxley** law.

Lest the buck stop with the most senior management, the SEC pointedly reminded public companies that their obligation to "disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure" includes board oversight of material cybersecurity risks. Thus, the **notable increase in 2019** of disclosures that board audit committees were overseeing cyber risk:

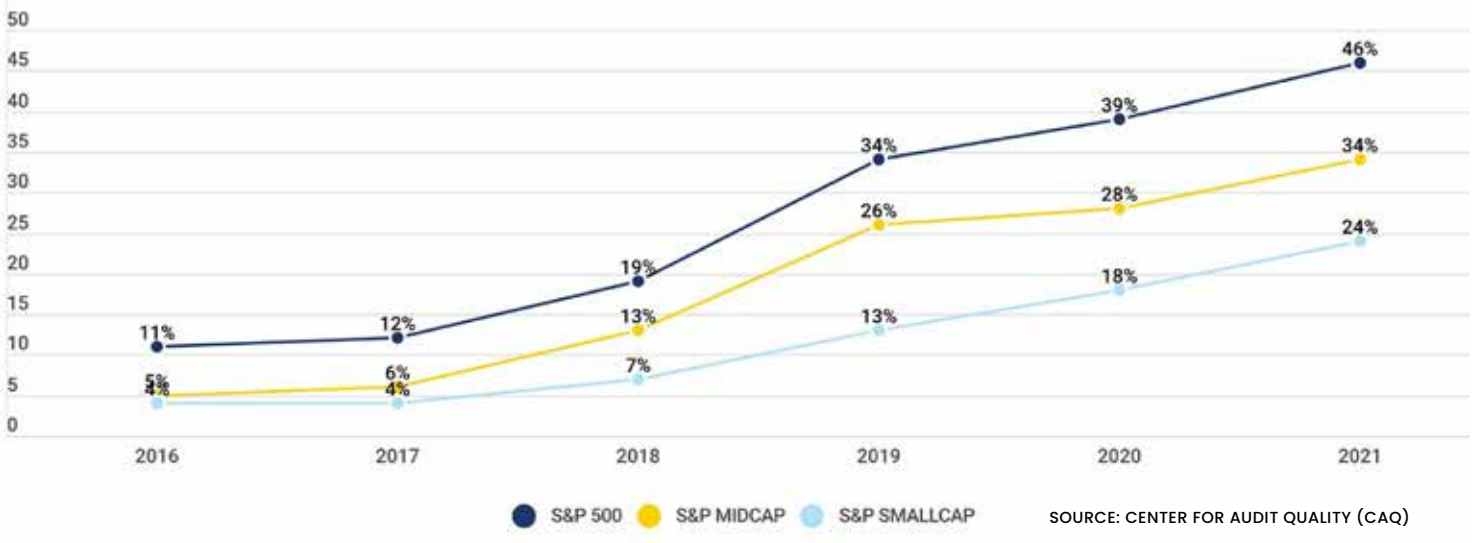


Figure 1: Is the Audit Committee Responsible for Cybersecurity Risk Oversight? (% Disclosed)

In July 2023, the SEC pushed further on disclosure of how the corporation deals with cyber risk and the board's obligation to oversee cybersecurity. For management, it required more detailed annual report disclosure on what it now calls corporate "processes" for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand. The commission decided not to ask for disclosure of "procedures" or "policies" for fear that those terms were too formal. The annual report must disclose whether these processes are part of the company's overall risk management program, whether the company uses third parties to assist, and whether the processes encompass cyber threats arising from third party service providers. In addition, the annual report must disclose which management positions are responsible for the assessment of cyber risk and the relevant expertise of these managers, how they are informed about cyber risk, and whether they report such information to the board.

As the cybersecurity landscape becomes littered with additional laws and regulations, cyber business risk is being transformed into cyber compliance risk.

The SEC also required more information about the board's oversight of these processes. Annual reports must now "describe the board's oversight of risks from cybersecurity threats," "identify [if applicable] any board committee or subcommittee responsible" for oversight, and "describe the processes by which the board or such committee is informed about such risks."

Many of the SEC's new requirements are phrased conditionally: Processes "if any" must be described and the responsible board cyber oversight committee must be named "if applicable." Don't be fooled. The new requirements will in fact drive public companies to first review their current approach to cyber risk and then to create the various positions and "processes" consistent with the SEC's demands, if they don't already exist. This review and modification will also extend to the public company board under the new SEC rules.

Although I've given what must seem to be a terrible amount of detail on the SEC's current rules, I assure you that this is only a thumbnail sketch. The corporate legal department will be integral in forging a workable accommodation between the SECs requirements and how senior management and the board wish to allocate their time dealing with this one issue. Time and resources are limited, and cyber is not the only material risk a company faces. It may be less of a business threat than a change in interest rates, or geopolitics, or some new substantive regulation of the company's core business. One silver lining: As I am about to explain, the disclosure framework required by the SEC fits nicely with the way courts see directors' fiduciary duties of oversight. At least there are two birds to be killed here, and boards of directors should aim for both.

CYBERSECURITY AND THE BOARD'S FIDUCIARY DUTIES

Experienced directors know that they have two fundamental fiduciary duties to the corporation and its shareholders: the duty of care and the duty of loyalty. Because our target company, like over half of all public companies, was formed

in Delaware, we turn to Delaware law to figure out what these duties entail. Corporate governance guru Peter Atkins **wrote** that the duty of care requires "informed, deliberative decision-making based on all material information reasonably available." He added that the duty of loyalty requires directors to act, or refrain from acting, "on a disinterested and independent basis, in good faith, with an honest belief that the action is in the best interests of the company and its stockholders."

What about the board's obligation to oversee company risks like cybersecurity? Where does the "duty of oversight" fit? While it might be logical to assume that the duty of care—to act in an informed way—subsumes the board's duty to oversee risk, another aspect of Delaware corporate law drives a different result. Because Delaware corporations can, and frequently do, provide in their charters that directors have no liability for failing to meet their obligation of care (so-called exculpation provisions), the Delaware courts have determined that the duty of oversight sits instead within the directors' general duty of loyalty. The opposite conclusion—that oversight is part of the duty of care—could relieve the directors from any responsibility to ensure that the corporation is acting within the bounds of the law—a result that was unpalatable to the Delaware courts.

But placing oversight duties within the duty of loyalty has significant ramifications for determining what directors need to do meet their obligations. Delaware courts are at pains to preserve a sphere for the duty of care exculpation provisions. These allow directors to be negligent, and even grossly negligent, and still meet their fiduciary duty. As a result, violating the duty of loyalty requires directors to do more than be negligent or even grossly negligent: They need to fail to act in good faith. To paraphrase a Delaware judge, the question is not whether the board failed to prevent an attack through deficient oversight; rather the question is whether the board "undertook its monitoring duties *. . . in bad faith.*" Even in instances where a company's cybersecurity efforts themselves have been seen as atrocious—from the repeated **Wyndham** breaches in the last decade, to the **SolarWinds** supply chain breach in 2020—the relevant directors nevertheless have been found by courts to have met their fiduciary duties.

The board, via management, needs to take two steps to deal with cyber risk. These will sound familiar, given the SEC rules. First, it must ensure the corporation sets up a system of information reporting and controls regarding cybersecurity. Second, once established, the board must monitor that system. If the directors

attempt these tasks in good faith, they are meeting their fiduciary obligations. The new SEC cybersecurity disclosure rules dovetail nicely with the directors' duties. Public companies must disclose the "processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats" as well as how the "board is informed" of cyber risks and how the board oversees these risks.

Regulation of cybersecurity has brought more risk. Companies that employ in-house lawyers to meet their regulatory, compliance, and governance obligations will find that these new risks play into their lawyers' strengths.

Setting up an appropriate set of reporting processes is important for an additional reason—one that extends beyond public companies subject to the SEC disclosure rules. As the cybersecurity landscape becomes littered with additional laws and regulations imposing substantive security obligations, cyber *business* risk is being transformed into cyber *compliance* risk. This is a big change. Compliance issues arise whenever a corporation might operate in a fashion that subjects it to criminal or civil liability at the hands of the government. Corporate compliance programs were originally set up to take advantage of the federal criminal sentencing guidelines, which offered the prospect of leniency if the defendant corporation had a program in place to prevent noncompliance with the law through the creation, implementation, and monitoring of appropriate policies and procedures. Although a comprehensive compliance program will require resources that extend beyond the processes necessary to meet the SEC's cybersecurity disclosure rules, there will be a significant overlap between the two efforts.

HOW IN-HOUSE LAWYERS CAN MAKE A DIFFERENCE

The confluence of the SEC heightened disclosure rules, the growing "complianceification" of cybersecurity, and the Delaware fiduciary standards for oversight make a persuasive argument for company boards to get a better handle on their firm's cyber risk while ensuring the company makes appropriate disclosures and complies with any substantive cyber requirements it might face. For boards of companies that lack in-house counsel, this might be a good reason to consider investing in a legal department. There is a boatload of information and third-party assistance available to help a company set up an appropriate internal cyber reporting and monitoring system, both steady state and in dealing with a cyber incident of some kind. But having a full-time employee who knows the business and its personalities can be crucial to effectively navigating the legal requirements.

In-house counsel can be of critical importance in setting up these processes in at least three ways. First, there is the matter of senior-level organization. The SEC's requirement that public companies disclose "which management positions are responsible for the assessment of cyber risk and the relevant expertise of these managers" will further drive the hiring of chief information

security officers. But to whom should the CISO should report? One can find proponents for having the CISO report to nearly every traditional member of the C-suite, from the CEO on down. Putting aside for a moment the reality that the personality of C-suite members has a lot to do with organizational decisions, I believe that the CISO should report to the Chief Legal Officer (CLO). This is for two reasons.

First, the other popular choices have significant downsides. It is a bad idea to have the CISO report to the CEO. While the professional CISO associations and those whose livings depend on the status and compensation of CISOs think this makes sense, there are reasons it does not. The CEO ought to be supervising senior executives making strategic decisions for the company, and much of the **CISO's role is tactical**. In addition, if a horrible cyber incident occurs, it may make sense to signal a rededication to cyber risk management by naming the CISO a direct CEO report. This move is foreclosed if the CISO reports there to begin with. The other popular choice—the CIO—has a certain logic ("it's all computers, no?"), but will likely induce conflict. The CIO's job is to ensure that the company has cost-efficient systems enabling all business processes while the CISO will be charged with prioritizing security over efficiency. A CISO cannot be boxed in by her boss because security makes the CIO's metrics look bad. A CISO needs support outside the CIO's organization to push through necessary security controls.

Second, there are unique upsides to placing the CISO with the CLO. The CLO can provide the CISO a high level of access and support. There are only three senior officers who commonly attend every meeting of the board and the audit committee: the CEO, the CFO, and the CLO. Familiarity with board members performing initial oversight of cybersecurity is a leg up for the CISO. Working for the CLO also provides the company a more seamless route to asserting attorney-client and attorney work product privileges to post-incident information gathering.

Closely related to these senior level organizational advantages are the day-to-day cybersecurity benefits that the legal team can and should be providing. As a substantive security matter, members of the legal team, dispersed as they are to assist non-lawyer colleagues across the business, can be exceptionally useful in urging that consideration be given to avoiding the accumulation of data, in reminding development teams that products and services be structured with an eye toward security, and in serving as listening posts for workers concerned that these sorts of efforts are not happening. In my experience, many employees regard the lawyer they work with day to day as a trusted and discreet colleague with good access to senior management. Having the CISO within the same reporting chain will signal that employees can and should take cyber compliance concerns to "their lawyer."

The third benefit the legal department can bring runs to the board itself. In the event of a breach, the prepared CLO will not have to waste time thinking about which outside firms to call. The law firm that will assist in the post-breach investigation and the firm or firms that will defend the company in follow-on regulatory investigations and class actions will all be on speed-dial. But I strongly suggest that the one dispute these firms should not take on is the claim by shareholders that the cyber incident was the result of the directors' and officers' breach of their fiduciary duties.

Such claims are brought by a shareholder derivative action, where the plaintiffs seek to have the company hold its directors and officers liable for their injuries (the post-breach decline in the stock price) due to an alleged failure to oversee cyber risk. These cases are extremely difficult for shareholders to win, particularly if there is a record of reasonable attempts to keep tabs on cybersecurity. But they are time consuming and distracting for those running the firm, who are publicly alleged to be failed fiduciaries. One key to winning is the investigation that a good law firm does to document oversight steps taken by the various fiduciaries. This investigation allows the independent members of the board the leeway to reject the shareholder's demands in a way that is nearly always upheld by the courts.

It is crucial that the investigation be seen as independent. That independence can be impugned if the investigating firm receives such a large amount of the company's legal work that it would be against its interests to find that the directors and officers had breached their duties. The shareholder derivative suit that followed the Wyndham breaches was marked by allegations that a prestigious national firm was conflicted by its simultaneous representation of Wyndham in the breach-related FTC investigation and in the shareholder derivative action. The court eventually dismissed these concerns, but a needless diversion would have been avoided if the general counsel had kept a good governance firm on reserve for just such an occasion.

THE BOTTOM LINE

For me, it boils down to this. Increasing regulation of cybersecurity has brought more risk to companies across the economy. Companies that employ in-house lawyers to meet their regulatory, compliance, and governance obligations will find that these new risks play into their lawyers' strengths. If properly arrayed against the growing challenges, companies will find that their lawyers can make unique and important contributions to the enterprise's cybersecurity.

CHAPTER 7

WHAT BOARDS NEED TO KNOW ABOUT CYBERSECURITY TO MEET THEIR FIDUCIARY DUTIES

DEBORA A. PLUNKETT

The fall of 2013 was ripe with almost daily reports of malicious attacks against a myriad of companies, touching businesses across many industries and sectors. These attacks, largely of the distributed denial of service (DDoS) variety, not only interrupted business operations but began to instill insecurities in those who worked at these businesses. It appeared to be the start of a rash of incidents that impacted the banking and retail industries as well as government organizations.

As the deputy director of information assurance for the National Security Agency, my job was to develop and deliver security solutions to protect national security systems, largely defined as classified data and networks as well as any that might be used for certain military operations. While focused on this mission, the Information Assurance Directorate (IAD) had long been sought after to provide advice on security topics, and we held robust, productive, and mostly non-public relationships with a number of entities in the security and technology arenas as well as pure play businesses across a myriad of industries. IAD had the largest and, according to many, the most concentrated number of experts in security, from engineers, programmers, and cryptanalysts to those with deep experience in the practical and implementable applications of security measures. IAD's engagements ran the gamut, from sharing in our mutual understanding of current or impending

security challenges to partnerships that resulted in the development of security solutions to meet the challenges.

It was in this context that I was first exposed to corporate boards. During this time of significant cyber activity, it was not unusual for a company to contact senior NSA leadership to ask for help in understanding a particular threat. To the extent time and authorities permitted, we would provide our best judgement to help the board members understand cybersecurity at a basic level, understand how a particular event may be impacting their companies, and to help them navigate mitigation options.

WHAT ARE A BOARD'S DUTIES?

Board members do not need to be deeply technical. But they do need to have lived experiences that help them understand cyber well enough to ask the right questions.

What was clear then is even clearer now. Corporate boards not only have fiduciary responsibilities to shareholders, but also a responsibility to be knowledgeable about key topics that could impact share performance. To meet these obligations, boards must be sufficiently informed, be provided with the right environment to ask, and get answers to, their questions. and be able to seek the advice of expert counsel when needed. The board environment must be conducive to learning and encourage dialog if board members are going to be best positioned to respond effectively in the event of a cyberattack.

In these early engagements with boards on cyber incidents, there were a few prevailing themes. The first issue, of course, was: "What happened and why did it happen?" Knowing what happened was achievable, but knowing why was, and still is, a difficult climb. Stepping through the basics of cybersecurity, including threats, vulnerabilities, risks, and mitigations, was often sufficient preparation to begin the more complex discussions around motivations, threat actors, and impacts to the company.

Board members were eager to learn, but they were also frustrated with some of the technical complexities to which they had already been exposed. I realized that they needed clear explanations of cyber complexities in order to understand what could, and could not, be confirmed. It was during these sessions that I began to develop a personal passion for board service. I saw the need for having someone on a board who had a measure of depth in cybersecurity topics. That person, in my view, did not need to be deeply technical (I certainly was not), but did need to have lived experiences that positioned them to understand cybersecurity well enough to know the right questions to ask.

THE CYBERSECURITY CURRICULUM

What do boards need to know about cybersecurity to satisfy their fiduciary responsibilities? First, they need to understand what is at risk for their company in the event of a cyber incident. While this might seem to be a no-brainer, surprisingly it is not a topic they regularly consider. What are the company's

crown jewels? Which threats to specific networks and/or data would have the gravest impact on the ability of the company to operate successfully? Areas that should be considered crucial to board knowledge and understanding include the following:

- **Insider Company Data:** Information regarding company strategies, competitors, financial plans, and schedules could impact a company's ability to remain competitive and deliver shareholder value.
- **Personally Identifiable Information:** Unauthorized access to PII held by the company could put others (e.g., customers or clients) at risk. This would include customer data that could be used for identity, for example a name, social security number, etc.
- **Intellectual Property:** Any cyber event that exposes IP could impact an entity's ability to continue to exist competitively, particularly if the IP is key to the company's business. Copyrighted and patented materials should be included in this list.
- **Competitive Data:** This includes contract bidding criteria, selection data, financial and legal data, and personnel files. Access to any of these could significantly impact a company's ability to perform, endanger its standing among peers, and affect its ability to hire and retain employees.
- **Reputation:** Threats to a company can upset and create uncertainty for shareholders, employees, and customers/clients. Their unease could translate into decisions to withdraw support (sell equity or switch to a competitor for products, services, employment, etc.). Reputational risk is not only very real, it's a compelling reason to act decisively and transparently in order to minimize impacts to trust.
- **Risk:** An understanding of the company's risk appetite is important to inform decisions that might need to be made in the event of a cyber event. Since managing risk is a prime responsibility of boards, including cyber risk in the topics they discuss is crucial to ensure the board is fully informed about the company's risk posture.
- **Education:** Can be achieved through periodic training sessions conducted either by inhouse or outside experts. Having an outside expert occasionally present to the board has the added benefit of giving them other perspectives and experiences.

The training should consist of the basics of cybersecurity (definitions and examples of threats, risks, and vulnerabilities and the relationships between them; explanation of mitigations versus responding after an attack has occurred; key legal, legislative, and regulatory rulings that apply to the company/business; and a history on any significant prior cyber events, particularly if they impacted the company). There are a multitude of opportunities for boards to be exposed to these basics, from books to online training opportunities for formal training provided by various credentialed

organizations. What is important is that there is a clear, stated expectation that every board member will receive this basic exposure, and that periodic updates will be provided.

Next, a board needs to understand how the company protects networks and data. This includes the challenges it faces, the costs it incurs, and the areas that are not sufficiently funded. The information should be presented to the board on a regular (at least semi-annual) basis and should include a discussion about current threats—to the company, to others in the same business sector, to the broader business world. The board should know what the cybersecurity budget is and should be satisfied it is sufficient given the company's overall investment in technology and the risks inherent in the company's business. Evidence of a strong focus on cybersecurity includes:

A company's incident response plan should specify criteria for board notification and any decisions that are their responsibility.

- **Clear lines of authority for making decisions regarding technology and cybersecurity.** The company should have decision documents and processes that are documented and exercised regularly so that they are well-practiced in advance of an actual cyber event.
- **Sufficient budget to address current and emerging threats.** There are various metrics to determine what should be spent on cybersecurity. General industry standards suggest that 15% of the technology budget should be focused on security. This number should be modified based on several factors, including the size of the company and maturity of the business.
- **A knowledgeable, accountable, and proactive chief information security officer (CISO).** The CISO should meet with the board regularly and be viewed as the company expert on all things cybersecurity. This person should have demonstrated success in the field, an appropriate academic background, and should communicate regularly with CISO networks. This last point is especially important because CISOs often share threat information that later impacts their companies, providing an opportunity to prepare in advance of a cyber event. The CISO should be the point person for cybersecurity compliance issues, risk assessments, risk management, control decisions, service provider arrangements, penetration (and other) testing, security breaches or violations, management's responses, and recommended changes to the company's security programs.
- **A strong and sufficiently resourced IT/security team.** While having a strong CISO is important, equally important is having a strong team supporting the CISO. This team should have clearly defined roles and responsibilities. It should be the company's focal point for implementing security measures and responding to incidents.
- **A business continuity plan.** The board should receive regular (at least biannual) updates on data recovery, reconstitution, and storage plans. The ability to continue operations despite an attack can instill confidence in both customers/clients and employees.

- **A relationship with an expert cybersecurity firm that could be invoked as needed to assist with assessment, mitigation, and recovery.** Such expertise can assist with internal assessments, reconstitution, and any redundancy requirements.
- **An established personnel cybersecurity training and awareness plan.** This plan should not only include exercises on common exploits (e.g., phishing), but also inform personnel about new and emerging threats and their potential impacts on the company. It is well established that having such a plan and diligently exercising it creates a more aware workforce that is less likely to fall prey to an attacker's exploits.

THE BOARD'S ROLE IN INCIDENT RESPONSE

Given the current environment, a cyber event is likely to impact a company. Boards should be prepared for this by having a working knowledge of the company's plans should there be a cyberattack. One such plan is the incident response plan, which is a detailed document that defines how a company considers threats and how it will respond should there be an attack. This plan should not only define how the company will respond to an event, but also identify key individuals and their responsibilities, external resources available that the company could leverage, and should outline key aspects of a response to an incident. Having a company incident response plan is essential, and the board should be informed of the plan, ideally participating in periodic tabletop exercises that give the board an opportunity to see how the company intends to respond and to understand its own role.

An incident response plan should include guidance on how the company will respond, decision criteria for key operational continuity, recovery from an incident, communications, and engagement. This plan should specify the criteria for board notification, and any decisions that are their responsibility. Having this documentation ensures that the directors can fulfill their fiduciary duties, specifically the duty of care, in identifying how the company will operate if under attack, and what might constitute a decision to degrade or cease operations that could impact shareholder value. Making this decision is an important one and must be made with a fully informed view of impacts, outcomes, and long-term recovery needs. Recovery should be addressed from both from a technological as well as an operational perspective.

Knowing when to inform the board, how often to keep them informed, and when there is a decision that requires board approval is critical. Quite often, early in the life of an event, the information available is not verified. While this might cause management to delay notifying the board, management should

consider at least informing the board of the fact of a validated event as early as possible. As cyber events progress and discovery results in learning about impacts not previously known or understood, it is best to have a board that is informed early and often so that they can be fully prepared to support management and fulfill their fiduciary responsibilities.

In the event of an incident, communications with the board regarding not only the incident, but any engagement with external legal or regulatory entities should be initiated and documented. Currently, all 50 states have data breach notification laws. Additionally, in July 2023 the SEC adopted rules governing incident disclosure requirements for public companies. Boards should be informed when an incident reaches the threshold that requires legal or regulatory notifications. This is important because, should there be any adverse responses to an incident, investigation could include interviews with board members. Keeping the board informed in a timely manner positions the directors to respond appropriately and exercise their fiduciary responsibilities of care and loyalty to the company and its stockholders.

THE BOTTOM LINE

There are other issues boards should consider as they focus on fiduciary responsibilities specific to cybersecurity. Should there be a board member designated as the "cyber expert"? Given the risks potentially impacted by a cyber event, should the CISO have a direct relationship with the board? Should the board be an approval authority for the company's security plan?

Once you start asking these kinds of questions, they keep flowing. And they suggest to me, at least, that boards have often been overlooked as players in this area. Should the board receive a periodic written report from the CISO regarding the state of security in the company? Do the company's insurance policies (property, casualty) cover business interruption losses caused by a network that is shut down due to a cyber event? Is the board's directors and officers (D&O) insurance sufficient? What are the terms and conditions for these policies? How should the board be involved in decisions regarding these policies? These are among the questions boards should be asking as they prepare to fulfill their fiduciary obligations.

CHAPTER 8

NAVIGATING THE NEXUS: HOW COMPANIES CAN ADDRESS GROWING GEO-CYBER RISK

GREG RATTRAY

When Russia invaded Ukraine on February 24, 2022, most national security and cybersecurity watchers expected to see the Kremlin direct large-scale cyberattacks at Ukrainian networks and critical infrastructure. Early indications included disruption of Ukraine government entities and wiper attacks on **satellite** and communications infrastructure. Global security and intelligence agencies issued multiple warnings of potential impacts from coordinated attacks as part of the ongoing offensive. Private sector companies increased coordinated tracking of cyber threats and defensive assistance trends to deal with denial of service, wiper malware, and disinformation campaigns. For cyber defenders, of particular concern were attacks aimed at Ukraine's critical infrastructure, given previous assaults on its electric grid as well as supply chain attacks with high potential for widespread international spillover, like the devastating **NotPetya** onslaught in 2017. The U.S. government warned America's private sector about the potential for Russian cyberattacks in retaliation for support of Ukraine, calling for a "**Shields Up**" set of cyber defensive measures.

In the first 18 months after the invasion, we saw Russian state-sponsored and affiliated threat groups continue their cyberattacks, including cyberespionage, DDoS, and the launch of new malware variants. So far, however, we have not seen evidence of large-scale strikes like NotPetya, the **Microsoft Exchange** breaches, or the **SolarWinds** intrusions. Instead, we have seen high **coordination** between Russian kinetic strikes, cyberattacks, and influence operations on Ukraine and in Eastern Europe.

While the face of Russia's offensive actions has looked different from what was expected, the invasion marked the latest crisis catapulting geopolitically driven cyber risk, or "geo-cyber risk," to public consciousness. Worries about cyberattacks as an essential element of potential conflicts in geopolitical hotspots, such as Taiwan, have grown dramatically. In an era where major power conflicts are resurfacing, often waged in the digital realm, the concept of geopolitics driving cyber risk has taken center stage and companies must have the foresight to be ready.

The acceleration of digital transformation has created growing cybersecurity risks across all industries. Attacks from nation-states or their proxies can cripple a company's operations, steal its intellectual property, and undermine its competitive advantage. Management and boards of directors need to ask themselves tough questions about digital strategies and attendant digital risks. Together, boards and management must look at how rapid geopolitical changes can cause cyber risks and potentially undermine digital business strategies. They need to have honest conversations about future scenarios that could threaten their company's future. Mitigating geo-cyber risk starts when company leaders are thinking forward and acting now. Reducing risks requires strategic, enterprise-wide foresight and investment.

Geo-cyber risk, as a concept, links cybersecurity to political risk influenced by geographical factors and international relations.

GEO-CYBER RISK

Politics and wars motivating efforts to disrupt communications are not a new phenomenon. Ever since governments, enterprises, and their agents have moved into the digital realm, geo-cyber risk has existed in the nexus of international relations, geopolitics, and technology. The English cut submarine telegraph cables in the North Sea early in World War I as part of efforts to isolate Germany. The advent of the internet and the information revolution have made cyberspace the new theater of operations, where nation-states engage in activities ranging from intelligence gathering and economic espionage to cyberattacks and information warfare.

Geo-cyber risk, as a concept, links cybersecurity to political risk influenced by geographical factors and international relations. In the last 20 years, though awareness of cybersecurity risk has grown, we have experienced a relative lull in great power conflict following the end of the Cold War. But now we are witnessing a shift in the international order, characterized by the rise of increasingly assertive nation-states operating across the globe. Cyber and digital operations are how corporations and governments work these days, and they have become a major part of geopolitical competition.

I began to see this myself in 2007, when I was serving as commander of the U.S. Air Force Information Warfare Center Operations Group. Even then we

General Keith Alexander

were seeing repeated cyber intrusions into defense industry networks and assets by sophisticated threat groups. We needed to make private sector operators aware of the dangers in order to strengthen mitigation. I coined the term "advanced persistent threat" (APT) out of necessity—to facilitate open discussion of foreign state espionage with civilian counterparts in the defense industry. It was General Keith Alexander, former director of the National Security Agency and the first commander of the Defense Department's Cyber Command, who in 2012 **described** the U.S. loss of industrial information and intellectual property through cyber espionage as the "greatest transfer of wealth in history."

The term APT has been adopted by the cybersecurity industry to describe a pattern of sophisticated computer network attacks, often by states or state-sponsored actors, aimed at governments, companies, and individuals. The origin demonstrates the nexus of geo-cyber risk. Our defense secrets, commercial intellectual property, and national competitiveness are digitally dependent. We have sought to characterize, capture, and communicate this risk for more than fifteen years.

Over that time, political, economic, social, and technological factors have driven conditions that have broadened geo-cyber risk across industries. Nevertheless, this risk has remained largely overlooked in the corporate landscape. The primary challenge is that geo-cyber risk is characterized by high-impact, low-probability events that are challenging to quantify, predict, and model. However, as great power conflict and strategic competition reemerge and a number of geopolitical crises loom, geo-cyber risk is now a fundamental concern that C-suites and corporate boards must address as a part of enterprise risk management.

STRATEGIC FORECASTING—LONG-TERM GEO-CYBER RISK MITIGATION

A major challenge for companies in managing geo-cyber risk is the combination of long- and short-term factors exacerbated by a web of dependencies with cascading effects. Management of organizations must address tactical and immediate problems and tend to have limited engagement in long-term planning. Or they conduct long-term planning around simple extrapolation of current trends. This approach leaves them unprepared for rapidly shifting digital and geopolitical developments.

In order to effectively manage geo-cyber risk, leaders need to shift their organizational mindsets out of a reactive mode and into analytically driven long-term strategic thinking. Efforts that increase this capability will require engagement of multidisciplinary people, teams, and processes. In my experience, one of the most effective frameworks for strategic planning and forecasting was developed by Peter Schwartz, first at Royal Dutch Shell in the 1980s and later codified in his book "The Art of the Long View." At Shell, Schwartz's planning team revolutionized what it means to incorporate scenario forecasting into corporate strategy and decision-making at the boardroom level. Through this approach, Royal Dutch Shell was able to prepare for the fall of the Soviet Union and Middle East-led OPEC's ascent well before any of the company's competitors thought these were even plausible.

Strategic foresight is not prediction. It is the process of constructing future possibilities as an investigative tool for us to make better decisions today.

Fast forward to 2020, when I led an initiative by the **New York Cyber Task Force** to leverage scenario-based forecasting to investigate steps the United States' public and private sectors can take to strengthen national cyber response readiness against national security challenges in cyberspace. We investigated key cyber risk drivers across geopolitical, economic, social, and technological advances in order to develop four severe, yet plausible, scenarios. By looking ahead to 2025, we sought to shift from yesterday's issues to longer-term cyber readiness, and to identify gaps that would require resources and investment to prepare for the future.

Based on our analysis, the task force developed concrete recommendations for public and private entities based on projected risk impacts. The same approaches can be applied to geo-cyber risk management to help companies identify complex risk scenarios that are crucial in understanding the scale and scope of possible problems and opportunities.

RISK DRIVER IDENTIFICATION AND MAPPING

Strategic foresight is not prediction. It is the process of constructing future possibilities as an investigative tool for us to make better decisions today. Driver identification is a key phase in developing strategic intelligence to inform planning and investment. It involves the identification, investigation, and prioritization of key drivers of risk and opportunity. One useful tool to advance the process is called the **PESTLE analysis** (the acronym stands for political, economic, social, technological, legal, and environmental factors). The table below shows examples of cyber risk drivers that a PESTLE analysis might turn up.

P	**Political**	Factors related to a government's international & domestic policy and actions.	• Great power competition & changing balance of power • Lack of consensus on cyber norms • Rise of transnational cybercrime • Growing digital divide between nations
E	**Economic**	Factors related to the economy, including economic growth, inflation, interest & unemployment rates.	• Decline of globalization • Increasing economic protectionism & digital/technological decoupling • Trade wars between global powers affecting supply chains
S	**Social**	Factors relating to culture, education, demographics & society.	• Increasing digitalization of society • Political polarization combined with widespread use of social media • Rise of disinformation • Decline of trust in public institutions • Cybersecurity workforce talent shortage

T	**Technological**	Factors relating to technological developments & advancements.	• Advancements / increasing use of:
			  • Artificial intelligence & machine learning
			  • Internet of Things, embedded devices & edge computing
			  • 5G, Cloud
			• Digital transformation broadening cyberattack surface
			• Proliferation of offensive cyber tools
			• Overconfidence in attribution methods resulting in errors
			• Quantum computing

L	**Legal**	Factors impacting current & future legal regulatory requirements.	• Increasing cybersecurity & data protection regulations • New legislation on cyber incident reporting requirements
E	**Environmental**	Factors that influence or are impacted by the surrounding environment	• COVID-19 pandemic & move to remote work • Increasingly connected devices controlling environmentally sensitive productions

SOURCE: NEXT PEAK

Figure 1. Example PESTLE analysis for cyber risk drivers

The factors above are not exhaustive. Relevant drivers will be heavily dependent on a given company's business, industry, size, geographic distribution, and operating model. Companies will need to triage and prioritize drivers to use as building blocks for scenario planning and strategic foresight.

TRIAGING DRIVERS AND DEFINING FORESIGHT HORIZONS

Not all drivers apply equally to each organization. Synthesizing and prioritizing drivers is a core part of strategic foresight and planning. Triage, or assigning degrees of urgency for specific drivers, must be undertaken. Otherwise, organizations will rapidly become overwhelmed by the breadth of possible crises that may occur. An organization can begin assessing and prioritizing drivers by specifying the unique risks facing the organization's industry; identifying the geographic distribution of its business; listing current and planned infrastructure; and addressing its strategic dependencies.

One way to group key drivers is to break them down into a combination of trends, external forces, and discontinuities in order to conceptualize the time dimension of future developments.

- **Trends** are patterns of change with recognizable developmental paths rooted in historical path-dependency. Individual trends can combine to create megatrends—long-term social, economic, political, environmental, or technological changes that affect perception and culture on both societal and individual levels.
- **External forces** are drivers that shape the structure, behavior, and development relating to a particular group, market, or strategy. External forces could be new legislation or regulations altering how a particular technology is used.
- **Discontinuities** are changes in trends that alter the trajectory of their path and cause social, economic, political, or environmental change rapidly and unexpectedly. These are culminations, breaks, or decisive turning points that cause accelerations, slowdowns, or cessations of the known path of development. Major discontinuities can have the effect of altering megatrends. A good example is the global COVID-19 pandemic, which changed the nature of work and societal interaction in just a few months.

Companies can analyze and categorize drivers to triage and prioritize scenario planning and strategic foresight. In the visualization below, the drivers identified through PESTLE analysis in the previous table could be analyzed, categorized according to horizon length, and then represented in a risk radar. Visualizations such as this one can be useful in illustrating risks' relative severity (color or size of blob) and time horizon in order to focus scenario building and strategic foresight analysis. Of course, the severity and impact of identified risk drivers will change depending on an organization's industry, geographic distribution of operations, and strategic dependencies.

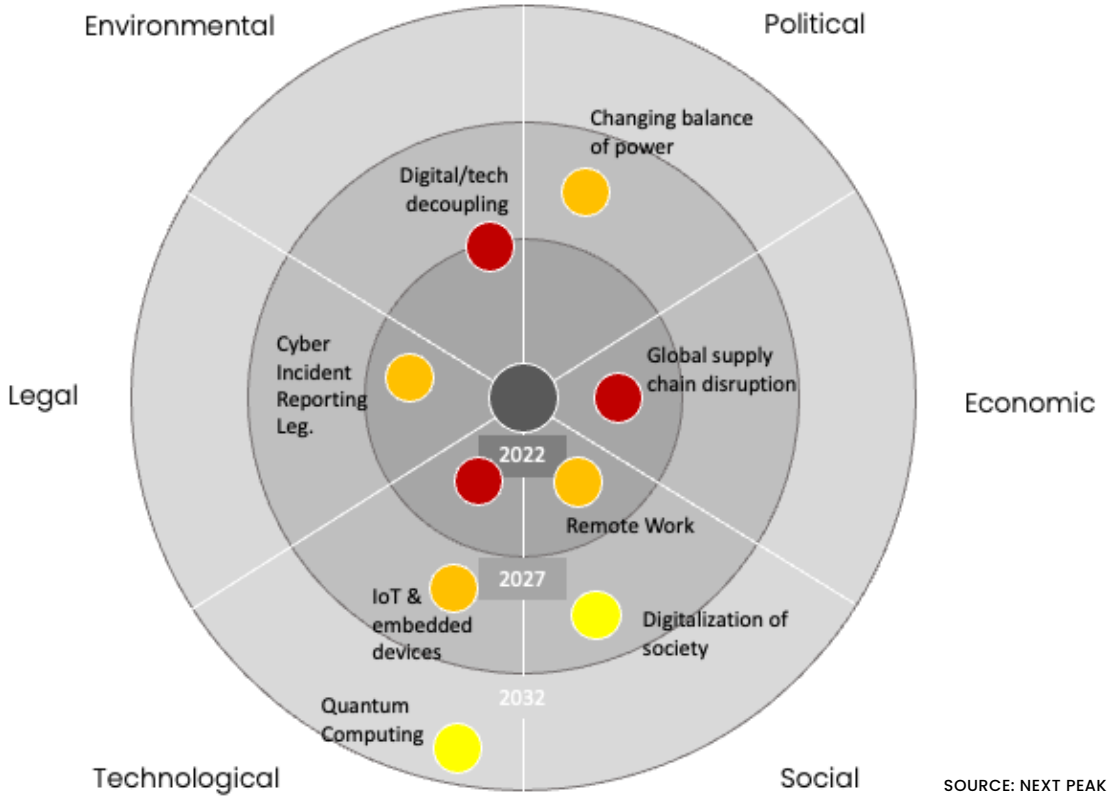


Figure 2. Example Driver Mapping by Horizon Length and Severity

COMBINING DRIVERS TO ANALYZE CHALLENGING SCENARIOS

Once primary risk drivers for analysis have been identified and the foresight horizon has been set, strategic planning teams can get to work projecting potential futures, imagining "wicked problems" or "toxic brews"—i.e., combinations of drivers that could catalyze into a much more challenging situation. Another way to think about future challenges would be the possible advent of multiple crises, often driven or exacerbated by geopolitical events—like the security, energy, and food crises all precipitated by Russian aggression in Ukraine in 2022. Such events that occur in a compact period of time are increasingly referred to as **polycrises**. Involving board members and senior management in discussions about risk drivers and how they might come together—and then in developing scenarios worthy of the time and effort for a company to analyze and plan for—will make these scenarios better and help drive future-focused action by the company.

In an effort to improve the utility of scenarios, the New York Cyber Task Force (which I mentioned earlier) used the ones we had developed as starting points. We then conducted workshops in which task force members worked through the scenarios

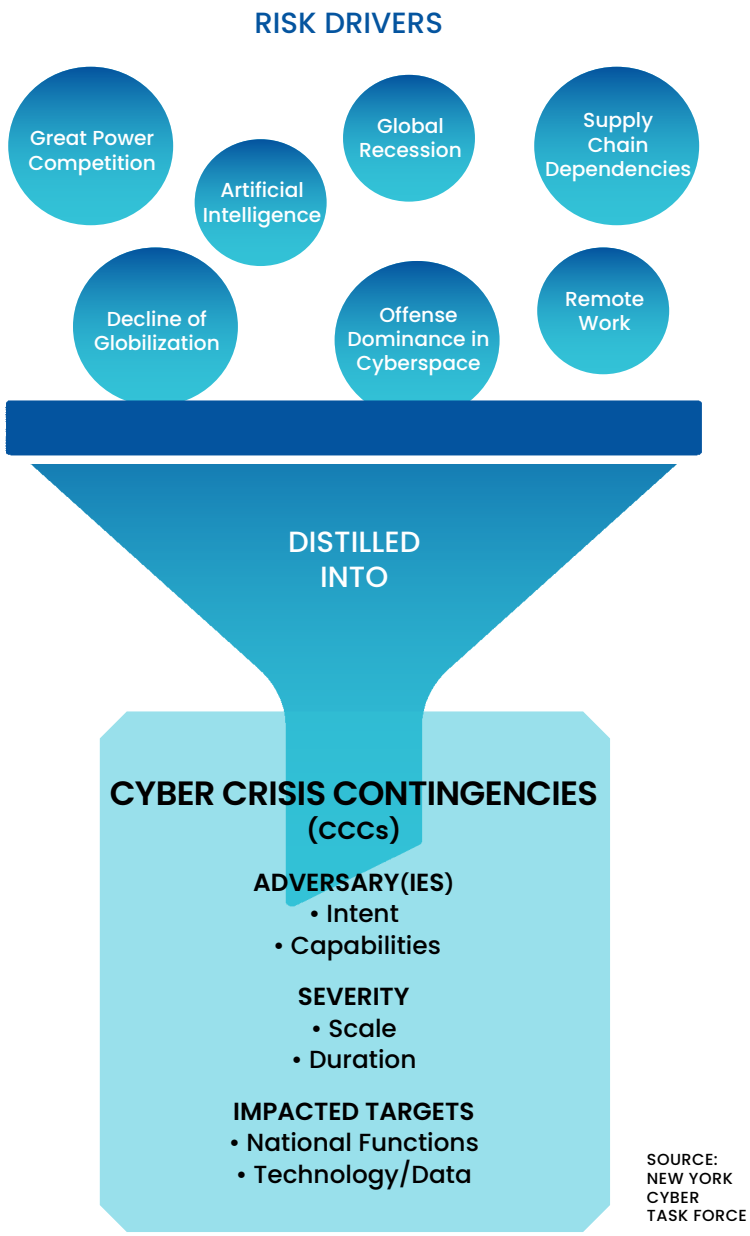


Figure 3. Identifying Cyber Crisis Contingencies

to identify collaboration activities that would be required, challenges to conducting these activities, and recommendations for overcoming those challenges. Each workshop had two phases. The first placed participants in the year 2025, during the crisis posed by a given scenario, and it focused on identifying likely gaps in our operational collaboration capabilities. The second phase brought participants back to the present to determine the short-term organizational and legislative actions necessary to enhance operational readiness. From the scenarios, we identified national cyber crisis contingencies that formed the basis for our final recommendations on how to start preparing for future crises today.

Implementing strategic foresight methodologies as part of risk analysis can help companies identify root issues in order to imagine what processes and capabilities will be needed to counter future risk. While strategic forecasting can take many different approaches, I think that the risk driver and scenario planning approach pioneered by Schwartz enables a creative and constructive process to discuss what we really think the future holds—and what we can do about it. Strategic forecasting must be an iterative process involving stakeholders across enterprise functions and lines of business coming together to discuss and challenge assumptions about the future. At a minimum, Information Security, Risk, Technology, Strategy, Business, and External Communications teams should be closely integrated.

The recent COVID pandemic, the rising number and severity of climate events, and the Russian aggression against Ukraine all demonstrate how quickly major shifts can impact a company's operating environment.

HIGH RISK ENVIRONMENT IDENTIFICATION AND HORIZON SCANNING

Long-term strategic forecasting requires a strong enterprise-wide approach, which may require significant resource allocation and investment. Though that may seem daunting, there are actions that company executives and boards can begin to implement immediately to understand their company's geo-cyber risk exposure.

Geo-Cyber Risk Index

As the cyber defense community began to understand the risks posed by aggressive nation-state behavior in cyberspace, I began trying to come up with a way to measure geo-cyber risk that would help companies understand their exposure across global operations. I found that existing tools and approaches failed to capture the complexity of the relationship between cyber and risks to digital operations posed by operating in various locations. I wanted to be able to explain what types of cyber risks were more or less present based on a company's digital and physical presence in different places and how governments and other factors there behaved. I wanted to know which places constituted high risk environments. I worked closely with the Eurasia Group in 2013 to develop the framework for what has ultimately evolved to become Next Peak's Geo-Cyber Risk Index. This provides a multi-dimensional view of risk across 40 countries (covering over 88% of global GDP).

When I worked at JP Morgan Chase (2014-2019), I applied a similar approach to strategic decision-making around the bank's operational initiatives. At the time, the bank was looking to expand its Asia operations, including required increases in staffing, data flows, and network capabilities. Based on an analysis of comparative risks of different locations and the bank's strategic ambitions, we built a framework to enable expansion of operations with policies, procedures, and controls to counter potential risks.

Companies need to understand how their global presence impacts their digital risk, and take steps to reduce those risks. The Geo-Cyber Risk Index measures over 80 variables across five cyber risk categories: states, foreign states,

cybercrimes, hacktivists, and network infrastructures. It enables companies to identify high risk cyber environments based on institutional profile, industry, and global footprint. Identified high risk environments can be analyzed to assess global risk exposure and to evaluate whether existing controls are sufficient to protect critical assets. Integrating geo-cyber risk analysis into risk management and mitigation strategies can be a highly impactful way to limit digital risk.

Horizon Scanning

While horizon scanning can take many forms, efforts should be driven by a strategic objective to investigate evidence about trends to analyze whether organizations are adequately prepared for potential opportunities and threats. Enterprise teams looking to implement horizon scanning must work with risk teams and lines of business to define data collection requirements, applicable methodologies, and analytical frameworks to assess data and drive insights.

Over the last decade, I have had the opportunity to work closely with Japanese government entities, including the Japanese External Trade Organization, to develop requirements and deliver horizon scanning reports as part of how they understand the growing risks. This, in turn, has helped them move toward a future-looking approach. I would argue that Japan's growing understanding of its own geo-cyber risk has allowed the country to take a more proactive stance on the nation's cybersecurity investments, as evidenced by its recent National Security Strategy released in December 2022.

FINAL THOUGHTS

Companies find themselves navigating increasingly rough geopolitical waters. Risks to digital strategies and assets are increasingly prominent. Boards must engage closely with management teams to understand how geolocation impacts geopolitical risks, how geopolitics may motivate cyberattacks, and how these factors may impact their companies. The recent COVID pandemic, the rising number and severity of climate events, and the Russian aggression against Ukraine all demonstrate how quickly major shifts can impact a company's operating environment. Anticipating cyber risks and having the foresight to understand how to respond can strengthen a company's resilience and illuminate better ways to navigate the digital environment's ever-growing churn.

CHAPTER 9

A STRONG MANAGEMENT-BOARD PARTNERSHIP IS CRITICAL FOR A COMPANY'S CYBERSECURITY

ANNE CHOW

Over the years I've worked with an array of business leaders in the context of their strategy, digital transformation, customer and employee experiences, and use of technology. In all cases, one of the greatest challenges they've faced is the complex, ever-changing, unpredictable nature of the environment. No doubt this is due to imperatives such as the need to dynamically access global talent pools, broaden partner ecosystems, and diversify supply chains while harnessing powerful emerging technologies and new innovations. The continued expansion of the digital landscape around the world, increasing the depth and breadth of the "connectedness" and "intelligence" of organizations will, by definition, result in greater exposure to vulnerabilities, risks, and threats.

Cybersecurity is relevant to all of this, for every business. "Cyber everywhere" is a reality, going far beyond the walls of an organization. It's now relevant to a company's entire infrastructure and ecosystem, touching their plants, mobile and remote workers, connected devices (which propagate vast amounts of sensitive data), as well as home and company networks. It's estimated that by the year 2025, damages from cybercrimes will hit $10.5 trillion annually.

A CEO, no matter how competent and tech-savvy, can't counter these challenges alone. Not even with an excellent management team. It takes an all-company effort. This obviously includes the chief information security officer (CISO) and the IT department, but it doesn't end there. It's important that the

board of directors is engaged and involved, and works in cooperation with executives. If one component of a company simply defers to another to create and implement the cybersecurity strategy, the engine is not firing on all cylinders. "Cyber everywhere" requires an all-hands defense—and offense.

I've learned a lot about this over the years from experiences as a senior executive and as a board member. I started from a pretty good perch. As a second-generation telecom professional (also known as a "Bell Labs baby"), it seems I was destined for leadership roles that placed me at the intersection of technology and people. When I entered the industry in 1990, with degrees in electrical engineering and business, I was a fledging network engineer. My earliest notions of cybersecurity at that time were about computer viruses and bad people trying to hack into private, often mission-critical, systems. From my early vantage point, protecting the network—that of my customers and company—was paramount.

While at face value cybersecurity may appear to be a technology issue, it is not. It is, and forever must be, a priority business issue for all boards and senior management teams.

Then, seemingly overnight, the world became connected with explosive internet-catalyzed innovation. The accompanying solutions and growth transformed the experiences of consumers, communities, businesses, governments, and society as a whole. In the three plus decades that ensued, I held numerous leadership roles with increasing responsibilities in telecom and technology that focused on the business marketplace across many areas, including product management and development, marketing, strategy, customer service, operations, and sales. In 2019 I became CEO of AT&T Business, a global $35 billion operating unit with 35,000 employees serving business customers with a full realm of technology solutions. Cybersecurity was mainstream and relevant to all facets of an organization by then—no matter the industry. AT&T had its own portfolio of services and partnerships that helped customers safeguard their network security. In fact, one of my mantras for my team, when it came to our customer relationships and services, was: *Connect … Protect … and Respect.*

In addition to my operating executive roles, in 2016 I had an opportunity to join my first public company board. To this day, I still serve on this small cap board, now as the lead independent director of FranklinCovey, a leadership, development, and training company. Later I also joined the board of the well-known global conglomerate 3M. With my additional perspectives as a director, I've grown particularly passionate about the relationship between executives and their boards, viewing it as vital to an organization's success, no matter the company's size or sector. And a lot of that is due to the impact of cybersecurity.

It's a domain that is perpetually evolving. Perhaps that's why clarity on the board's role in partnership with senior management is elusive and often fluid.

Several years ago, at a board director summit whose participants hailed from different industries across the private and public sectors, I heard a common sentiment from fellow board members: "Cyber risk is well managed by the IT team." Even if the statement is true, it leaves me unsettled, given my knowledge of and experience with the threats, risks, and vulnerabilities that businesses face—whether they are aware of them or not.

The roles of a board are not limited to strategic planning, leadership governance, and oversight of CEO evaluation, succession planning, and executive compensation. They foundationally include the fiduciary responsibility to protect and grow shareholder value responsibly. While at face value cybersecurity may appear to be a technology issue, it is not. It is, and forever must be, a priority business issue for all boards and senior management teams.

Cybersecurity and geopolitics have become inextricably linked. As boards work to navigate geopolitical risk, cyber must be part of their scope. Unfortunately, the world of technology has in and of itself become political, which further exposes global businesses, especially across interconnected supply chains, to escalating levels of threats.

No doubt each of us has been subject to phishing attacks, and businesses are constantly being bombarded with various social engineering tactics by bad actors seeking to gain access to sensitive information. Ransomware attacks are on the rise, with extortion techniques evolving in sophistication and impact. And the unprecedented, exponential advancement of generative AI serves as an accelerant to the flames of cyber risk on an ever-growing attack surface. Let us also acknowledge that AI will fuel innovations from both the "good guys" and "bad guys," compelling us to always be wary about what's happening around us.

Management's efforts to mitigate strategic risks is a key area of collaboration between executives and boards. In the case of cybersecurity, this must be handled with both proactive and reactive plans. Meaning, management must ensure that their boards understand:

- What the company is doing to identify risks based on their view of the greatest vulnerabilities, and what is being done to protect the environment, including both physical and digital assets. Of particular interest are what controls and protocols are in place from a human perspective, as in this mobile, hyper-connected world, people (whether employees, suppliers, partners, or otherwise) are often the weakest link. This includes identity management, verification, and authentication of not only people, but also processes, system handshakes, and more.
- What the company is ready to do if an incident occurs—how they will detect it, respond, and ultimately recover. This includes not only recovering from the

incident itself, but remedies developed from root cause analyses to prevent future exposure. It is vital for the board and management team to be on the same page of the incident response playbook. This playbook must be comprehensive enough to cover the roles of all key players. It must also recognize that the operational teams involved in the incident management cannot be expected to simultaneously manage stakeholder communications. A systematic approach to customer communication must also be a critical element of the plan.

THE ROLE OF THE BOARD

Boards must understand what their role is—in times of crisis as well as in a steady state. Oversight, governance, and risk management require a focus on several key areas to enable shared accountability for cybersecurity with executives. When I work with senior leaders, including those who serve on boards, a common concern I hear is, "I'm not that technically fluent and don't fully understand cyber." One does not have to be a technologist to learn about the cyber world, and more importantly, what the implications are to the business an individual is responsible for. As with any area of concern—geopolitical, regulatory, environmental, social, legal—the board's role is to strategically connect the dots, working hand in hand with management.

Traditionally, boards have viewed cybersecurity as the responsibility of the audit committee. But the understanding and insight required often exceed the expertise found on most of them.

Here are some of the questions board members and senior management need to consider:

Context and Critical Resources: What is the strategic context and framework for how the business views cybersecurity? What explicit and implicit linkages exist between the company's overall infrastructure, cyber ecosystem (hardware, software, network, people, data), and critical business success factors? How are data, data protection, and cyber integral parts of the organization's business strategy, value proposition, and competitive differentiation? What is the holistic enterprise level view of cyber? Do we have sufficient cyber talent on hand? Do we have a cyber-clear culture where our team members understand what's required of them to do their jobs in a secure way? Do our people know what exposures to be aware of? And do we "test" the cyber rigor of our processes and resilience of our culture?

Metrics and Measurements: What are the right metrics for the board to understand? What operational data are provided to the board (which could include efficiency, effectiveness, regulatory, and compliance-oriented metrics)? What does the data mean? Beyond traditional red-yellow-green scorecards that indicate degrees of risk, what do trend results tell us? Do we know where we have the greatest exposure—strategically, operationally, and technically? And are we sufficiently investing in resources, technology, and partnerships to mitigate and manage the concerns? Do we understand what our most valuable assets are, and do our measures and methods help us protect and secure them? Do the answers to these questions create the need for a small set of enterprise-wide board level metrics which supplement the operational ones?

Education and Expertise: What base knowledge should the board understand? Not necessarily deeply technical, but information that links the technical to business implications? What cyber fundamentals feel vital to use, such as the NIST cyber framework, and how do we ground ourselves in where we are rather than where we should be? Is this an area of strength or weakness for us? Do we have a cyber-oriented culture not only in the company and across the management team, but also at the board level? How do we sustain it?

Communications and Governance: How frequently should we be communicating with the board on our progress? How do we utilize board meetings and committee meetings in these updates? Do we have a robust crisis management process and incident playbook, tested periodically with tabletop exercises? These exercises must include post-breach protocols; use of outside counsel and forensic consultants, as appropriate; communications with key external stakeholders, such as the FBI; and potentially, board involvement. Are we bringing in outside and industry experts on a regular basis to ensure that we have the most current thinking on threats and opportunities going forward?

Speaking of governance, I've also heard the following from board members (from both publicly traded and privately held companies): "There are board members who have cyber experience, and I'm counting on them to represent me." Unlike when you're in an operating role and have clear domain and/or functional responsibility, as a board member your responsibilities span the enterprise. High-performing boards collaborate actively across all strategic priorities, which helps to elevate perspectives and enhance collective decision-making.

Yet, traditionally there has been a belief on boards that "cybersecurity is the responsibility of the Audit Committee." Review and management of the topic has been done in the context of enterprise risk management. However, the understanding of cyber risks and the strategic insight needed to manage them go far beyond the typical financial breadth and depth of expertise found on most of these committees. Alternatively, some companies have moved to establish separate cybersecurity committees and/or IT/Technology committees where cyber is in scope. Leading the way are financial services and health care corporations. Some organizations have even begun treating cybersecurity committees the way they do Internal Audit, giving the CISO/CSO/CIO not only direct access to the board and committee chairs but even direct reports to the board via the appropriate independent director committee chair and a tight partnership with the general counsel (given the expanding legal liability).

More and more companies are placing CISOs or executives who have direct operational and technical experience in the cybersecurity arena on their boards to ensure a diverse range and depth of expertise. As a Nominating and Governance Committee chair myself, I can vouch for the power of such diversity when it comes to effective board succession, development, and planning.

WORKING IN PARTNERSHIP WITH MANAGEMENT

On July 26, 2023, the SEC adopted new rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by public companies. Foreign private issuers are also required to make comparable disclosures. The basis for these new rules is the commission's observation that cybersecurity threats and incidents are a growing concern to public companies, investors, and the market. This is a regulatory affirmation of the risks that have increased given global digital transformation. While disclosing a material cyber incident is not a new requirement, what's new about this latest rule-making is the specificity of what, how, and when. This places an even greater emphasis on a common understanding and definition of what is material prior to any actual incidents occurring, understanding that the expectation is that materiality is based on whether the issue is important to investors today and/or potentially in the future.

From a management standpoint, it is vital not to use a technology-first or technology-only approach when working with the board on cyber.

While the dialogue about these new rules is active and ongoing, there is no question that the roles of the CISO, CIO, and CTO, in partnership with their general counsel and chief financial officer, have become even more critical, given this development. The SEC rules underscore requirements for reporting on management's role in handling these cyber risks, and the board's role in oversight in the face of a growing threat landscape. Timeliness and agility become even more critical. Orchestrated communications led by management across key stakeholder groups must ensure board awareness and alignment.

The board's strategic scope includes the full span of business, technology, regulatory, and market realities. It must be equipped to understand the strategic threats and vulnerabilities to the business that could negatively impact the company's value, both in the short and long term. Its focus is oversight, however, and it must not overstep into the operational realm of decision-making. Management must own all operational responsibilities,

working to establish the measures and metrics along with the necessary assessments and audits required to mitigate and manage these risks.

As part of this responsibility, management and board must work together to ensure that the board is devoting sufficient time to the company's technology strategy, operations, and investments. Capital allocation, including optimizing ROI, in the context of strategic imperatives, which improve the customer and/or employee experience, are vital to the competitive differentiation of the company's products and services. Understanding the role of cyber is key to ensure that the appropriate investments are made, including resources dedicated.

From a management standpoint, it is vital not to use a technology-first or technology-only approach when working with the board on cyber. There should always be a business and strategy lens placed on the discussion, including financial dependencies and stakeholder concerns as applicable. When reviewing risk, the conversation should focus on business outcomes and impacts, including contingency plans. In today's digital world, a base level of technical fluency should be expected from the board and senior management team, and the importance and relevance of data must be part of their shared base level understanding—whether it be customer, employee, operational, financial, or other data. An explicit understanding of the greatest vulnerabilities and risks, including potential financial impacts, is required of both board and management teams. And in the inevitable need for prioritization of investments, tradeoffs must be clearly understood.

The downside is significant if cyber is not embraced in this partnership. Not only are there the costs of cyber breaches, which can be monumental, there is also the potential for litigation and reputational losses. At the core is the operational functioning of the organization, which, if disrupted, especially for a significant amount of time, can have severe economic, community, and stakeholder impacts. Whether the breach occurs in a government organization responsible for commerce, a banking institution that plays a key role in global financial markets, a city's transportation infrastructure, or a group responsible for a major energy grid across a large metroplex, the impact of a cyber incident can range from negligible to minimal to moderate to severe to devastating.

THE BOTTOM LINE

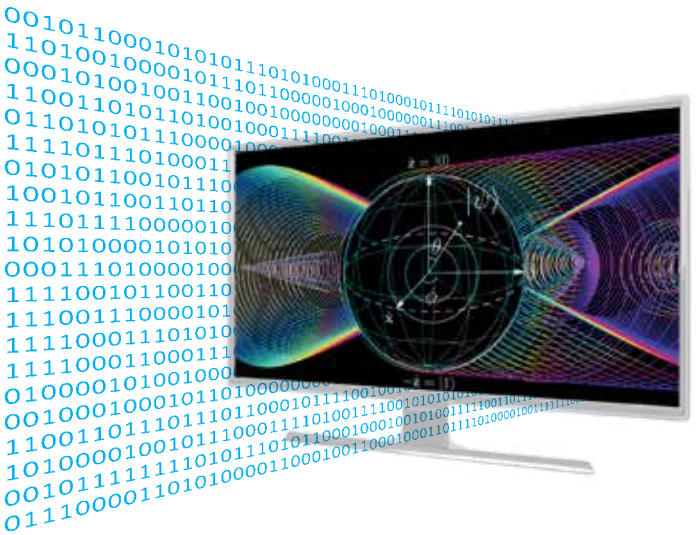
In a data-first world, cybersecurity vigilance is a must. This steadfast attention, including controls and compliance, must be owned as a joint responsibility between the senior management team and the board—each with clear roles and a clear understanding of the issues. Systemic, periodic, and ad hoc communications are all critical to the success of the enterprise. There are no guarantees in the world of cyber, but strong alignment and commitment coupled with a collaborative team approach are the best equation for a company to prevail.

PART THREE

CYBERSECURITY AND TECHNOLOGY

CHAPTER 10

EXECUTIVE OVERVIEW OF THE QUANTUM THREAT TO CRYPTOGRAPHY

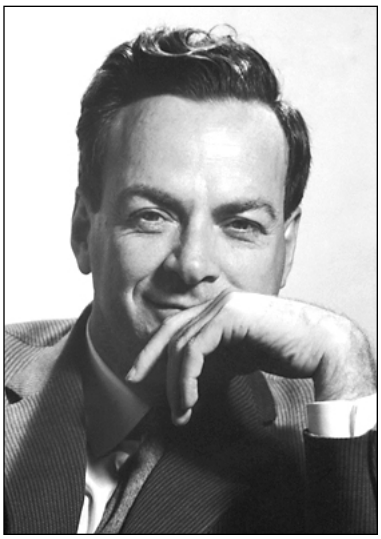


DR. EDWARD AMOROSO

One of the greatest scientific minds, perhaps of all time, was the wonderful Professor **Richard Feynman**. His contributions to physics, his various writings, and even the archived video series of his lectures are pure treasures for anyone who delights in physics. Feynman is relevant here because he may have been the first person ever, back in the 1980's, to have surmised that a so-called *quantum computer* might be useful to explore the mysteries of quantum physics, to which he had been a major contributor for years.

Since then, researchers have in fact made considerable progress in this area— sufficiently so that business leaders are advised to take notice of their work. The specific aspect of quantum computing that should be understood is the risk that such futuristic machines bring to the use of modern cryptography. In particular, quantum computers may one day be well-positioned to break the public key cryptography that powers the internet, and specifically eCommerce.

In this brief article, without getting too deep into the weeds of the physics, I will explore what business executives and practitioners should understand about the pending threat that quantum computing presents to the internet. And I will include a five-step action guide explaining how businesses can begin addressing the challenge, along with a suggested timeline.



Physicist Richard Feynman

Without jumping too quickly to the answer, I can add that the solution appears to be more about execution than about the need for additional invention. You will see that there seem to be good solutions, but they will require work.

HOW DOES CRYPTOGRAPHY SECURE DATA?

The use of cryptography to secure data is well-established in modern business. It should come as no surprise that to secure their data, businesses rely on algorithms and protocols using methods related to symmetry single key cryptography. In addition, they must use asymmetric public and private key-based cryptography and the associated infrastructure (often known as public key infrastructure or PKI) to manage security and establish compliance.

That said, several of the methods in use today, especially the ones related to public and private key usage, rely on the mathematic property that identifying the factors of any large number that is the product of two prime numbers is incredibly difficult. It is so difficult, in fact, that for a sufficiently large product of two big primes, it could take more time that exists in the remainder of the universe to find the answer.

What this implies is that businesses rely on the limited power of computers, including ones working together in massive, distributed, cooperative arrays. These ensure that when you negotiate a key using a protocol such as the **Diffie-Hellman key exchange** (used when your browser visits an https website), your data will be secure. This assumption works, so long as giant leaps in processing power do not ensue, and this is where quantum computing introduces new risk.

WHAT ARE QUANTUM COMPUTERS?

Conventional computers use tiny logic gates that can be in an "on" or "off" state, thus corresponding to a 1 or a 0. Binary arithmetic can be constructed by arranging so-called bits in linear arrays called registers, from which logical operations can be performed. By constructing successively more abstract means for directing these operations, called programming, we've been able to create networks of powerful applications and systems.

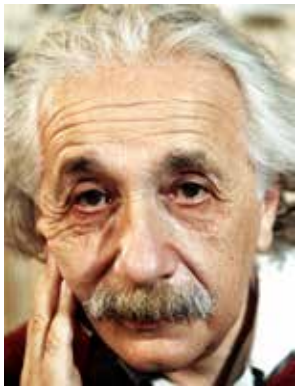
And yet, the model is severely limited. Despite the growth and magnitude of global network communications, the scale of on-demand cloud computing, and the huge computational support for applications such as artificial intelligence, the only problems a conventional computer can solve are ones

that can be analyzed using a total of two binary digits. That's all existing computers can do: represent bits as zeros or ones.

Quantum computers can't copy information without destroying the original information. That's why they will never replace the computers we all use today.

A quantum computer uses an entirely different processing model, and I will do my best to explain it in terms that a business person with no background in physics might understand. If you are not in the mood to pore through descriptions of the inner-workings of these unique new machines, then feel free to just skip down to the next section on quantum threats. You'll have no problem picking up the thread from that point.

For those brave souls who choose to dive into the quantum, here is a brief summary: First, recognize that when electrons associated with materials such as phosphorus are subjected to a magnetic field, they can spin in either an up or down orientation. On first glance, this would seem to mimic a conventional computer with two electrons representing up or down. But the wonders of quantum physics introduce two new pieces of information to this state.



Albert Einstien

It turns out that electrons subjected to a magnetic field can spin up, spin down, or spin both up and down at the same time—a property known as *superposition*. Furthermore, when two electrons are subjected to a property known as *entanglement*, they can have a remote effect on each other in a manner still hard to grasp by some physicists. Einstein died still grappling with how two electrons can entangle in what he called a "spooky manner."

Nevertheless, we know that it works, and scientists have now been able to create quantum computers that can perform calculations by reading information—called coefficients—about the up spin, down spin, superposition, and entanglement of each pair of electrons. This implies that whereas a conventional pair of bits is described by two numbers, a quantum pair of so-called qubits is described by four numbers—hence, it's remarkable power to compute.

To actually collect the information from the electrons is tougher than one would expect, because of a property discovered by Werner Heisenberg called "uncertainty," which means that *reading* the quantum state can *impact* the quantum state. For this reason, quantum computers (get this) cannot copy information from one series of qubits to another without destroying the original information. This is why quantum computers will never be for general purpose tasks.

Werner Heisenberg

In a quantum computer, a clever arrangement of really, really tiny transistors, whose dimensions are a thousandth the width of a piece of paper, are placed next to the electrons and used to collect residual energy from the quantum states. This is how the quantum computer collects data and reads information from a series of qubits. It is also how algorithms would be implemented and run on a quantum computer.

WHAT IS THE QUANTUM THREAT TO CRYPTOGRAPHY?

A Bell Labs scientist named Peter Shor developed an interesting algorithm for solving the prime factoring problem of cryptography using successively better guesses of candidate prime factors. The algorithm uses an obscure number theorem that for any two primes x and y, if you multiply x by itself enough times, it will eventually reach a number that is one greater than a direct multiple of y. (You can try it yourself for some smaller primes. It works.)

When Shor's algorithm is combined with the power of a quantum computer, it turns out that computer scientists have been able to demonstrate that large factoring can be performed an order of magnitude more quickly than in a conventional computer. This will demand that some advances continue to be made in the practical development and use of quantum machines. IBM has developed a quantum computer with 433 qubits, and advances continue.

The U.S. National Institute of Standards and Technology (NIST) has estimated that within the next seven to 10 years, the field of quantum computing will have advanced to the point where modern PKI-based protocols and algorithms can be cracked. You might think that this leaves a sufficient amount of time to relax and wait, but there is a problem.

Security experts refer to this problem as the store-now-decrypt-later threat. A well-funded adversary, probably a nation-state, could collect encrypted information from its enemy now and tuck it away in long-term cold storage. Once quantum computers are available, the adversary would then cryptanalyze the information, thus unleashing whatever threats correspond to the collected data. You can sit and think about how this could, for example, be an issue for intelligence agencies.

WHAT IS POST-QUANTUM CRYPTOGRAPHY?

The good news is that cryptographers, being the clever bunch of mathematicians that they are, have developed a series of new cryptographic protocols and algorithms that can serve to replace the vulnerable approaches in place today. NIST has even sponsored a long series of reviews and tests and has approved a collection of algorithms from various sources, including startups, that will be resistant to quantum threats.

The problem, as one might expect, is not that any so-called post-quantum cryptography (PQC) is available, but rather that the complex sprawl of existing cryptography makes it incredibly difficult to locate the algorithms and protocols that demand replacement. This might seem silly, given the existence of advanced IT systems management (ITSM) and software inventory tools, but cryptographic routines have found their way into all sorts of places.

According to NIST, we have between four to seven years until the arrival of Q2K—the emerging quantum threat.

Consider, for example, that your web development team might be managing, hosting, and operating an infrastructure for your customers that could include public-facing websites, private account access to applications, and massive back-end systems to do processing or analysis. This complex tangle of software likely includes a great number of commercial tools, platforms, and software, as well as a wide assortment of free and open source utilities. This is typical.

Now, if you ask your development team which aspects of their infrastructure have embedded cryptography, in most cases they can offer a reasonable estimate, perhaps even a guess, but for proprietary software or certain open source software, they may not know. So, the challenge here is to develop an understanding of the inventory and posture of vulnerable PKI-based technologies in use across the enterprise in advance of the emerging quantum threat—a date known as Q2K.

WHAT BUSINESS ACTIONS ARE RECOMMENDED REGARDING QUANTUM THREATS?

Business executives are thus encouraged to put into place a simple action plan today that can begin to address this approaching threat. I listed the steps in such a plan below, recognizing fully that a spy agency will have significantly greater need to act than, say, a small retail company. But I believe the action plan applies nicely to both edge cases, and by tailoring the threat model to the local conditions, I think the following steps apply generally.

Step 1: Initiate a cryptographic inventory. This is sensible practice for any organization, and it should be viewed as an ongoing effort. Your IT, security, and infrastructure teams will know how to do this. They won't necessarily like the tedious investigatory work, but automated tools are available to assist. You should fund procurement of such tools to help this work scale across your infrastructure.

Step 2: Perform a cyber risk assessment. This is also sensible and is how spy agencies and retail companies will come to very different conclusions about the store-now-decrypt-later threat. Both are vulnerable, but the consequences are quite different. Your security team, perhaps in conjunction with the finance or risk teams, would be good choices to lead this effort. Platforms exist that can help, but this can also be done manually using simple common sense.

Step 3: Prioritize your inventory. This is basically combining your inventory with the cyber risk assessment. It will help to identify obvious places where perhaps you have really sensitive information being encrypted versus places where there is little or no risk. This is an essential aspect of the action plan because it will dictate exactly where you will eventually start the replacement process.

Step 4: Contact your third parties. Yes, this is necessary, especially if you outsource key elements of your IT, security, or other business program to suppliers, partners, or other external businesses. You should expect blank stares when you ask about their cryptographic posture against quantum threats. You may want to forward them a copy of this article to help them get started.

Step 5: Begin the stepwise upgrade to PQC. This is the first step in replacing PKI systems with PQC systems. You will likely have to do this in conjunction with a vendor, and I suspect that for many teams, the initial process will not work. It may seem like a straightforward IT task to replace one cryptosystem with another, but it's very complicated. Expect to learn as you move along through your replacement list.

Timing: My advice is that for most companies, Steps 1 and 2 can and should be done in 2024. Steps 3 and 4 can and should be done in 2025, and Step 5 should start in 2026. If we believe NIST, then this leaves roughly four to seven years until Q2K, which in my view seems like a reasonable cushion. Obviously, if you are an intelligence agency, then you are probably not relying on my article for guidance and you are doing the work right now. At least I hope you are.

CHAPTER 11

EXECUTIVE GUIDE ON HOW TO APPROACH THE CYBERSECURITY IMPLICATIONS OF EMERGING TECHNOLOGIES

SANJAY MACWAN

There are three things certain in life: taxes, mortality, and emerging technologies. There will always be emerging technologies around us. Executives and board members alike need to stay in tune with them to understand and manage the impact on their businesses, including cybersecurity implications.

Of course, technology comes in many forms, from physical and electromechanical, to biological and chemical breakthroughs, to those related to software and computing. Many of the recent technological advances—including our understanding and uses of natural sciences—are underpinned by computing and software. That's why this discussion will focus on these technologies.

News of an important development in technology often fills business leaders with anxiety. Their reaction is almost always based on fear, and there are three common forms:

1) Fear of missing out (often referred to as FOMO): When leaders become aware of the buzz surrounding a hot new technology tool, they may be caught flatfooted. All they may know is that everyone seems to be talking about it, including their competitors, and they fear that they will be left behind while other companies use it to accelerate their growth to a new level.

2) **Fear of the unknown.** New technology doesn't arrive with a user's manual designed specifically for your company. It may not be clear how a company should use it, what standards apply, and what governance practices are implicated. It takes time for industry best practices to emerge. In the meantime, you may have to create your own.

3) **Fear of how it may be used.** If FOMO is all about how competitors may take advantage of the technology, there is also fear of how adversaries may use it to harm your company. How might threat actors use it? Or nation-states? Or competitors (domestic or international) looking to create an advantage—whether it's legal or not?

Given the complex and amorphous nature of emerging technologies, it is helpful to have a framework through which we can evaluate and address them.

CREATING PLANS TO GUIDE YOUR COMPANY

It is incumbent on business leaders, including the board, to provide appropriate guidance and oversight on how best to address these anxieties. FOMO can be traced all the way back to the dawn of time. Many millennia ago, when a primitive homo sapien returned to the communal cave holding aloft a better club, he was probably greeted with general panic and fear. This seems to be an inherent trait in the human species. Businesses are not immune. The fear of missing out is as real for executives as it is for individuals. And this fear pushes them to take an aggressive approach to jumping in. History is crowded with leaders and companies chasing the next emerging technology with blind faith—only to experience setbacks when it doesn't prove out for businesses that aggressively invest in it.

Conversely, there are companies—albeit fewer—that take a wait-and-see approach. This "second mover" or even third mover approach is all about examining the technology's inflection points more deeply, learning from the early mistakes or setbacks suffered by the competition, and trying not to repeat them.

Equally important is to allow time for standards and best practices to take shape. Even better is to help shape the standards and best practices yourself. This requires a strategic and comprehensive approach in directly engaging with industry standards organizations as well as legislative and regulatory groups. Furthermore, in today's highly interconnected and data-driven ecosystem, security and privacy implications are absolutely critical for executives and boards to pay attention to. And they should do so in the earliest possible phase of any emerging technology investments.

Thus, executives and board members alike need to focus on developing plans around key guiding principles for their organizations. These should help counter any ad-hoc approaches primarily driven by fear, while also providing steady and strategic guidance in dealing with emerging technologies.

Robert Morris and his floppy disk containing the source code for the Morris Worm (at the Computer History Museum)

HOW CYBERSECURITY FIGURES IN

In 1988, the internet was the emerging technology—or collection of technologies—of the time. On November 2 of that year, **Robert Morris**, a graduate student at Cornell University, released the now infamous worm of the internet at 8:30 pm. It quickly crippled that world. It's important to keep this in mind because the incident remains a powerful example of the need to examine the cybersecurity implications of any emerging technology very carefully to be able to avoid or minimize adverse security and privacy implications.

Forty-five years later, the technology that raises concern has changed, but we're still dealing with the same issues. Today, virtual reality (VR) has driven leaders across multiple industries to make early bets—in several waves—only to see the expected widespread adoption fail to materialize. The FOMO factor has been quite prominent.

While this technology is extraordinarily promising, it has lacked certain inflection points to propel it into the mainstream. At the same time, it is another great example of the need to take a holistic approach in examining the totality of information: security, privacy, trust, and compliance.

The technology holds tremendous promise across education, health care, entertainment, and industrial applications, yet a number of researchers have also shown that a person's hands and eye movements can be used as reliably as fingerprints to identify the user behind the VR set. This underscores the security and privacy challenges. Furthermore, there is broad concern that the technology could leave impressionable youth feeling isolated, damaging their mental health. Together these issues have undermined trust in the technology.

DEVELOPING A FRAMEWORK TO EVALUATE NEW TECHNOLOGY

Given the complex and amorphous nature of emerging technologies, it is helpful to have a framework through which we can evaluate and address them. Also, it is important to look at cybersecurity and related issues holistically when doing so. This approach can not only help solve a business need, it may even help create entirely new capabilities for a business.

Our first principle, then, has to be to take a holistic approach to cybersecurity through interconnected aspects of a) information security, b) privacy, c) trust, and d) compliance.

As you can imagine, every emerging technology has dual information security implications. We can see this in Edward Amoroso's writing on quantum computing. On one hand, quantum computing makes cryptography even stronger than the current prevailing standard, but at the same time it can be used to break current cryptography, putting information security at risk for a wide array of information we rely on.

We can further illustrate the duality of these implications by examining the recent (and exciting) advances in artificial intelligence. AI can help find anomalous patterns in massive amounts of network data, or identify anomalous application behavior through its machine learning algorithms. This can be used to efficiently identify and tackle a cybersecurity threat. But in the hands of threat actors, the technology can be used to maliciously conduct a highly sophisticated and hard-to-detect phishing campaign. It can be used to steal credentials or create highly accurate voice impersonations that can bypass voice-based biometric authentications. We can identify similar dualities of cybersecurity implications in many emerging technologies.

Just as with human relationships, where trust is gained slowly and steadily but lost quickly with one major misstep, it is also true for organizations and leaders.

Privacy of data is another key tenet, and it should be anchored on sound information security implementations along with transparent policies. Emerging technologies often challenge or disrupt established privacy expectations and practices. Staying with AI as an example, we can already see that it opens up new and previously unexplored privacy concerns. Take, for example, AI-enabled facial recognition software, which is now broadly used in public as well as private enterprise settings. Efficacy and accuracy of this technology is useful, but it stretches privacy boundaries and opens up new questions about surveillance without proper, or any, consent.

This leads to our second principle: Carefully examine the dual cybersecurity and privacy implications of any emerging technology under business consideration.

Trust as a core value is paramount for society as whole, but also for enterprises. Trust in emerging technologies is hard to come by early on. History is replete with initial trust deficits in technological advances. For example, early steam engines were hugely mistrusted. Earlier we discussed mistrust in VR technology. We can also see how AI algorithms and recommendation engines for content have spawned mistrust on many social network platforms.

Generative AI is another example. Its transformative impact is real, but it will have to overcome significant trust issues. Various generative AI models have been famously known to "hallucinate"—in essence, produce false output.

Just as with human relationships, where trust is gained slowly and steadily but lost quickly with one major misstep, it is also true for organizations and leaders. Therefore, the board and executive leaders need to take the time to understand what trust issues might surface from a new technology, and plan deliberate steps to address them.

First and foremost, it is important to acknowledge if there is a trust deficit in a given technology. Second, identify the most objective ways to address those deficits. For example, for generative AI it is prudent to acknowledge the hallucination problem and use erroneous outcomes to retrain the models. Companies should also explain to the stakeholders—consumers, business partners, industry groups, and regulators—what progress has been made, and do so in a timely and transparent fashion.

Finally, our third and final principle: Get ahead of regulations by engaging in developing standards, best practices, and guardrails for emerging technologies.

Inevitably, technological advances attract regulatory interest—especially due to security, privacy, and trust, as we discussed earlier. This leads to regulations and compliance regimes, which are often combinations of industry standards and government rules. These developments invariably lag behind emerging technologies. Organizations that want to stay ahead of the regulatory and compliance curve should engage early on in helping to shape appropriate industry best practices, and should even develop self-imposed guardrails until clearer policies and practices emerge. It can be worth investing as much in this effort as in the technology itself. It can go a long way to establish real trust.

THE BOTTOM LINE

The board and executives are understandably intensely focused on the core business and near to midterm business priorities. But new technologies will always come around, and therefore it is critical that the board and executives adopt a consistent approach in guiding their teams when they do. Emerging technology as a theme has to have a seat at the table among all other priorities. This approach must not be driven by fear of missing out or fear of the unknown. It must be grounded in dispassionate analysis and a clear understanding of the promises as well as the challenges that must be overcome.

A company's approach should also pay close attention to the potential misuse of the technology in the hands of unscrupulous adversaries—whether cyber criminals, unethical competitors, or nation-state threat actors. This is best done through a holistic focus on cybersecurity and its related components: security, privacy, trust, and compliance. This approach has the best chance of serving companies well in methodically exploiting emerging technologies to deliver innovation and sustained business success.

CHAPTER 12

THE IMPERATIVE FOR CORPORATE BOARDS TO PRIORITIZE IDENTITY MANAGEMENT

JOHN J. MASSERINI

In an increasingly interconnected and digital world, the importance of identity management cannot be overstated. As businesses increasingly adopt distributed cloud environments, head down the path to zero trust architectures, and rely more and more on third parties for critical information processing, the need for adequate access control to protect sensitive information is of the utmost importance.

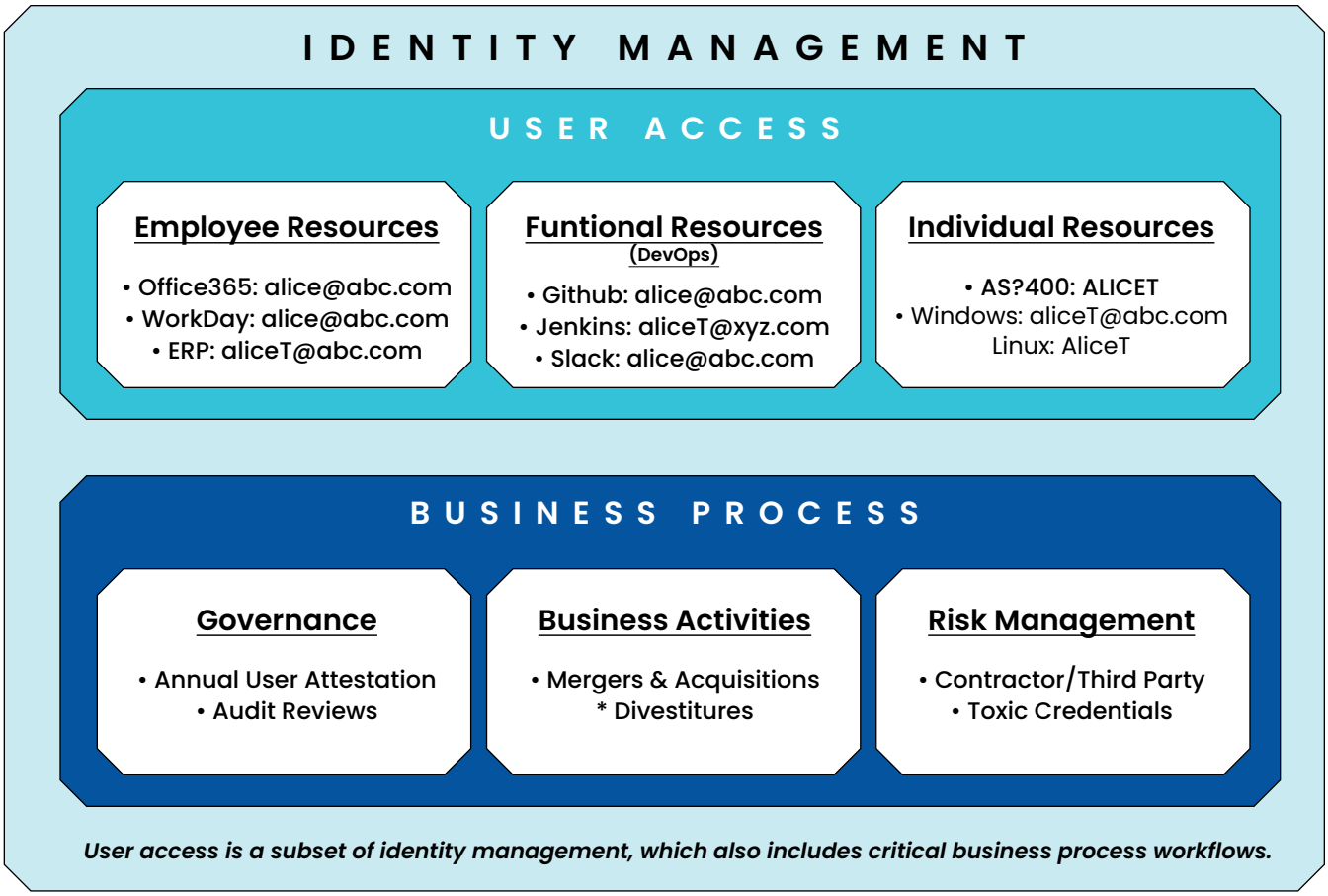
Corporate boards should be deeply concerned about their organizations' identity management programs, and with good reason. They would do well to study the potential risks and benefits associated with this critical aspect of modern business operations.

IDENTITY'S EVOLVING LANDSCAPE

Conceptually, identity management includes a broad range of business practices and solutions focused on ensuring individuals have appropriate access to resources within an organization's technical infrastructure. A mature identity management program not only includes the company's employees, but also business partners, customers, and third-party suppliers who may interact with a company's applications and network resources. With the seemingly endless adoption of cloud computing, mobile devices, and work-from-home initiatives, traditional perimeter-based security models have given way to a more dynamic and varied threat vector.

Unfortunately, most people equate identity management with user access. While similar, it's critical not to confuse the two. Identity management should be considered the overarching umbrella for all user access types, business processes, and maintenance activities that occur in the user ecosystem. User access typically pertains to a specific application or system, whereas identity management is the holistic overview of all user access across the entire infrastructure.

In a mature identity management program, risks can be determined based on user actions and their inherent risk to other systems and environments to which they have access. This holistic view of managing identities by applying risk metrics to user access and activities is what separates companies with well-understood risk exposure from those likely to be the next headline (and not in a good way).



SOURCE: JOHN J. MASSERINI

In reviewing the chart above, multiple components make up an Identity Management Program versus day-to-day user access management procedures. As pictured under User Access, there are three main pillars of functionality:

- **Employee Resources:** These are normal corporate services that every employee needs regardless of job function—the HR platform for benefits (WorkDay), the mail and communications platform (Office365), and the ERP platform for travel and expense (ERP).

- **Functional Resources:** This is an example of a specific team (DevOps) or a functional group's needs within an organization. The DevOps teams need access to their code repositories, ticket and release tools, and communication channels. One could easily replace DevOps with Finance, HR, or Legal, and the appropriate access for those specific teams would follow.
- **Individual Resources:** The access requirements under this pillar are around the specific needs users have in order to perform their job functions. In this case, Alice is a systems administrator, so she has specific "admin" level credentials for some systems. This can also be exemplified, for example, by the differences in access between an accounts receivable clerk and an accounts payable clerk, or a payroll administrator versus a benefits administrator.

When we evaluate the Business Process section of Identity Management, it has little to do with user access but is more focused on governance, business processes, and risk. These verticals break down in the following manner:

- **Governance:** The ability of an organization to prove they are compliant with industry or government regulations is a critical aspect of a mature identity management program. All of the leading regulations require companies to have a solid understanding and control of how users access systems and manage the assigned permissions. This is primarily achieved by consistently running User Attestations, which ensure user access reviews are performed in line with expectations. Similarly, Internal Audit will be spot-checking the attestation process to ensure it aligns with the corporate policies and standards.
- **Business Activities:** Reorganizations, mergers, acquisitions, and divestitures all wreak havoc on technology organizations that are trying to provide a standard level of service to their user population. A well-conceived identity platform allows for easier integrations of new users en masse as well as the selection and movement of departing users. Also, not only does a mature identity platform make IT's job easier, it also provides detailed accountability and auditability—again, supporting those regulatory and audit requirements surrounding the business activity.
- **Risk Management:** While operational efficiency is a key element of a strong identity management program, ultimately it's about mitigating risk throughout the enterprise. Most of today's identity platforms leverage machine learning to identify toxic combinations of credentials that could allow a disgruntled employee or an external attacker access to applications and data they should not have. Additionally, having a centralized location for all third parties and contractors goes a long way in mitigating often overlooked risks in your supply chain.

Ultimately, it's critical to understand that identity management is much broader and much more risk-focused than legacy user access.

RISKS OF INADEQUATE IDENTITY MANAGEMENT

When we evaluate the risk exposure of an inadequate identity management program, it falls into three major categories: data breaches, regulatory compliance, and insider threats. Let's look at each.

Data Breaches: Without robust identity management, companies are vulnerable to data breaches and cyberattacks that can result in significant financial losses, damage to reputation, and legal liabilities. As is often the case, employees tend to use the same credentials across multiple systems throughout the corporate environment. In fact, this is one of the main contributing factors to the substantial uptick in ransomware over the last several years. Unauthorized access to sensitive data can lead to the exposure of proprietary information, trade secrets, and customer data, eroding trust and credibility. This becomes significantly more of a threat as companies move headlong into zero trust architectures which are absolutely dependent on a solid identity management program to be successful.

There have been countless examples of insiders disclosing sensitive data—either intentionally or accidentally—and causing a significant impact on a company's reputation and/or market valuation.

Regulatory Compliance: Over the past several years, there has been a substantial increase by regulators on how organizations are managing their identities and user access. Sarbanes-Oxley (SOX) audits have become increasingly focused on not just user access, but how identities are managed throughout the legacy infrastructure and within the expansive use of cloud services. With heightened data protection regulations such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), poor identity management can lead to non-compliance and substantial fines. Additionally, the Payment Card Industry Data Security Standard (PCI DSS) requires businesses that process credit card payments to implement certain security controls, including strong identity management controls. Boards must be aware that inadequate identity management practices could result in severe legal and financial consequences such as fines, sanctions, and long-term regulatory oversight.

Insider Threats: Identity mismanagement is also a key enabler of insider threats, where employees or authorized users exploit their access privileges for malicious purposes. There have been countless examples of insiders disclosing sensitive data—either intentionally or accidentally—and causing a significant impact on a company's reputation and/or market valuation. Whether it's a negligent employee accidentally disclosing information, an employee departing the company and taking sensitive information, or theft of proprietary information, these often-overlooked threats can disrupt company operations, compromise sensitive data, and cause reputational harm.

BENEFITS OF EFFECTIVE IDENTITY MANAGEMENT

An effective identity management system ensures that only authorized individuals can access company resources, reducing the risk of unauthorized access and data breaches. This is especially true in today's modern enterprise, where zero trust, DevOps, and cloud infrastructures are moving critical services outside of the legacy firewalls. Multifactor authentication, real-time, risk-based access controls, and regular identity audits and attestations contribute to a strong security foundation.

By prioritizing identity management initiatives, boards can mitigate numerous technology-centric risks by addressing underlying issues that span the enterprise. A well-implemented identity program enables the identification of potential risks and facilitates proactive measures to address them, reducing the likelihood of security incidents. Additionally, by leveraging modern identity platforms, organizations can leverage AI and machine learning to uncover user-access-related risks that would otherwise be impossible to find.

If your organization's revenue stream includes selling services to other companies, being able to demonstrate a robust identity management program instills confidence and trust with your potential clients.

Proper identity management streamlines access provisioning and de-provisioning, ensuring that employees have the right level of access throughout their tenure. New employees are onboarded substantially quicker than with legacy approaches, which reduces administrative overhead, saves time, and enhances overall operational efficiency. At the same time, modern identity management platforms provide for employee self-service and requested access when needed with supporting workflows to ensure all necessary approvals are in place. Finally, the de-provisioning process is all-encompassing, disabling access across all platforms and applications with the click of a button. Long gone are the days of abused credentials of employees who left weeks, months, or years ago.

In an era in which trust is a precious commodity, robust identity management can bolster a company's reputation. Customers, partners, and stakeholders are more likely to engage with a business that demonstrates a commitment to safeguarding sensitive information. If your organization's revenue stream includes selling services to other companies, being able to demonstrate a robust identity management program instills confidence and trust with your potential clients. It also goes a long way toward providing SSAE-18 SOC 2 compliance.

By ensuring compliance with data protection regulations such as GDPR, CCPA, PCI, and NIST, boards can avoid potential legal entanglements and financial penalties from both federal regulators and industry associations. A robust identity management program demonstrates a strong belief in corporate accountability and responsibility, helping to build a positive relationship with regulators and auditors.

THE BOTTOM LINE

Supporting and empowering your organization's identity management initiatives achieve not only the mitigation of cyber risk, they also enhance operational efficiency while minimizing the potential for regulatory actions. Corporate boards must recognize that the complexities of modern business demand a strategic and holistic approach to identity management. The risks of inadequate protection are considerable, including financial losses, regulatory fines, and reputational damage. Conversely, a well-implemented identity management framework can deliver enhanced security, operational efficiency, and stakeholder trust.

Here are some parting recommendations for corporate boards:

- Review your organization's identity management policies and procedures on a regular basis to ensure that they are up to date and effective.
- Invest in identity management technology that can help automate access provisioning and de-provisioning, and provide real-time visibility into user activity.
- Recognize that strong identity management should make employees' jobs easier, not more difficult. Haphazard applications of strong passwords and multifactor solutions will only encourage staff to find ways around the controls.
- Integrate identity management into the development/DevOps pipeline to ensure that initiatives such as zero trust and cloud deployments are addressed.
- Automate annual identity attestations, ensuring that responsible managers can easily identify risky access credentials that could potentially cause harm.

Unlike other cyber risk initiatives, identity management crosses the boundaries of the security, technology, legal, and compliance groups. The board must collaborate with the leaders of all of these areas to ensure adequate attention is being placed on identity-related initiatives. Corporate boards should educate and train themselves on not just the impact of identity management on their organizations, but general cybersecurity topics as well. Government organizations such as NIST, NICCS, and NCSC offer board training presentations, and independent organizations such as the National Association of Corporate Directors (NACD) and the Corporate Governance Institute offer formal cybersecurity training aimed at corporate directors. By prioritizing identity management and allocating appropriate resources, boards can demonstrate their commitment to protecting the interests of the company, its stakeholders, and its customers. At a time when data is the lifeblood of the enterprise, and breaches can have profound and far-reaching consequences, the impetus for corporate boards to concern themselves with identity management has never been more important.

CHAPTER 13

BOARDROOM BLUEPRINT: HARNESSING THREAT INTELLIGENCE TO SECURE OT AND IoT ASSETS

CHRISTOPHER R. WILDER

In today's distributed world, we increasingly must navigate the dynamic realms of operational technology (OT) and the internet of things (IoT). These domains are transformative, influencing our operations, from streamlining processes to enabling better customer engagement and improved operations. Even with the benefits come novel challenges, especially in defending them from attack.

Enter threat intelligence (TI)—an essential component of enterprise cybersecurity programs that offers an in-depth view of cyber threats. TI is not merely about identifying risks but providing actionable insights to prevent, respond to, and mitigate potential breaches. But be forewarned. Tools companies can use to defend themselves can also be used against them. For example, in 2017 the Ukrainian power grid was targeted by a cyberattack that created widespread blackouts. Ironically, the attackers used off-the-shelf TI solutions to identify vulnerabilities in the grid's OT systems and exploit them to cause outages. In 2018, Atlanta faced a debilitating ransomware attack that locked their computer systems, with bad actors demanding a staggering $51 million ransom.

The lesson: Defenders need to be proactive. These attacks might have been forestalled or mitigated if effective TI solutions and practices had been implemented in Ukraine and Atlanta. In Ukraine, TI could have proactively identified vulnerabilities in the grid's OT and/or **SCADA** systems, equipping operators with the information needed to fortify those areas before they could be exploited. Additionally, real-

In 2018, Atlanta was hit with a ransmware attack that affected numerous government services.

time alerts based on indicators of compromise (IOC) could have swiftly flagged suspicious or unauthorized activities. As for Atlanta, a sophisticated TI framework could have spotlighted emerging ransomware threats, giving the city the critical intel to allocate cybersecurity resources wisely and bolster its defenses. Also, enhanced email filtering capabilities should have been activated to intercept and quarantine phishing emails (the most common attack vector for ransomware). We at TAG estimate that nearly 90% of all ransomware attacks are exploited by email. Having a strong TI strategy combined with preventative measures would have reduced the odds of a successful attack, reputational harm, and unnecessary costs.

If those events suggest that the danger is past, a similar ransomware attack plagued the JBS meatpacking company in 2021, halting the company's North American and Australian operations. The attackers demanded a ransom payment of $11 million. JBS paid the ransom, but the attack still caused significant disruption to the company's operations. The following year, the Colonial Pipeline was the victim of a ransomware attack that shut down the pipeline for several days. The attack caused widespread fuel shortages in the southeastern United States. The company paid a ransom of $4 million to the attackers to restore operations. Also in 2022, a group of hackers known as Lapsus$ targeted several major companies, including NVIDIA, Samsung, and Okta. The hackers were able to steal sensitive data, including source code and customer information. These are the tangible effects of companies' failure to prepare. Each company took over 120 days to recover from the attacks, but that was the least of it. Their brands and reputations " suffered long-lasting and immeasurable damage from being in the "blast radius."

The JBS meatpacking company was hit with a ransomware attack in 2021.

For boards, understanding TI is pivotal. While OT and IoT bring technical complexities, the strategic implications of these technologies are of utmost importance to governance and decision-making across the entire security organization. Without adequate protection, organizations are vulnerable. TI provides an avenue to assess and act upon strategic risks, ensuring that the enterprise remains resilient and forward-looking. Like an

early warning system for bad actors.

WHAT IS THREAT INTELLIGENCE AND WHY IS IT IMPORTANT?

At its core, TI refers to organized, analyzed, and refined information about potential or current attacks on a system. Over the years, TI has evolved from basic threat data feeds into a sophisticated discipline that identifies risks and contextualizes and prioritizes them based on relevance to an organization's specific environment. This evolution has been driven by the increasingly complex nature of cyber threats and organizations' growing digital footprints.

In today's digital era, where cyber threats are numerous and highly sophisticated, TI stands as the first line of defense. More importantly, it can level the playing field against adversaries that use TI to identify vulnerabilities and attack methods used by other bad actors. It equips organizations with proactive insights, ensuring they're not just responding to threats but anticipating them. By understanding adversaries' tactics, techniques, and procedures (TTPs), organizations can tailor their defense mechanisms more effectively, reducing the risk and impact of potential breaches.

In addition to understanding and mitigating risks, boards must promote a culture of cybersecurity within the organization.

TI goes beyond merely recognizing external threats. It's about discerning their significance, grasping their potential ramifications, and making well-informed decisions to maintain the organization's digital integrity.

BEYOND IT AND OT ENVIRONMENTS

It's important to understand what TI is and what it's not. At a foundational level, TI transcends basic threat data. It collates, analyzes, and interprets information from multiple intelligence sources concerning potential cyberattacks, offering a dynamic, constantly evolving picture of the threat landscape. With AI and data management solutions, it has the capacity to consider historical patterns and forecast future vulnerabilities.

When operational disruption leads to significant financial and reputational damages, TI is one of the key guardians of an organization's operating assets. It aids in identifying vulnerabilities, devising response strategies, and fortifying the castle's garrison. A proactive approach ensures that risks are identified and dealt with in a manner that safeguards critical business operations.

Beyond the broader organizational framework, TI is invaluable in enhancing executive protection, providing a sort of "Digital Overwatch." Understanding potential threats becomes pivotal in an age where cyber threats can be personalized and targeted. TI aids in identifying potential risks to the executives, their families, or colleagues, and helps ensure that personal and professional data remain safeguarded. Furthermore, by incorporating TI boards can mitigate their exposure, and improve the odds that strategic decisions are informed, relevant,

The Colonial Pipeline

and resilient against the backdrop of the cyber threat landscape.

For security organizations, TI is a powerful tool to help guide strategic decision-making. By understanding the nuances of the threat landscape and forecasting potential vulnerabilities, organizations can provide boards with actionable insights. Such insights inform immediate security postures and influence long-term strategic planning, resource allocation, and risk management. By aligning TI with board-level objectives, security organizations can also provide cyber risk management that is not an isolated endeavor but is intrinsically linked with broader organizational goals.

In summary, the value of threat intelligence isn't restricted to enhancing cybersecurity protocols. Its implications are far-reaching, influencing executive protection, board-level decision-making, and safeguarding the overall resilience of the organization in an interconnected world.

BOARD-LEVEL ENGAGEMENT IN CYBERSECURITY

Cybersecurity has become a central business imperative in recent years, with tangible impacts on reputation, stock prices, and operational continuity. Consequently, board members are delving into this area as a cornerstone of strategic decision-making. A critical function the board can perform is championing a comprehensive risk management approach that recognizes the entire spectrum of cybersecurity threats looming over the organization, including supply chain disruptions caused by data breaches suffered by third-party vendors. While neither the board nor the security team can prevent all such attacks, they are responsible for guaranteeing that the organization has robust security measures in place to counter them.

In addition to understanding and mitigating risks, boards must promote a culture of cybersecurity within the organization. This includes educating employees about cybersecurity threats and best practices and creating a process for reporting and investigating cybersecurity events.

Several high-profile examples demonstrate that board involvement in cybersecurity decisions may prove pivotal in navigating and mitigating cyber threats. In 2020, for instance, when SolarWinds was the victim of a significant cyberattack, its board of directors quickly intervened and disclosed the situation. They didn't just acknowledge the breach; they actively sought external expertise for a thorough investigation and transparently liaised with stakeholders, speeding the brand's recovery.

Target's experience in 2013 serves as another example. After the company endured a massive data breach (through an HVAC system on a store) that left if with compromised customer data, the board embraced an active role. Board members spearheaded an exhaustive investigation, revamped cybersecurity protocols, onboarded a new chief information security officer (CISO), invested in cutting-edge security tools, and championed a reinforced security awareness drive for employees.

Their proactive stance fortified Target against subsequent threats.

These instances underscore the indispensable role of board-level commitment. By grasping the gravity of risks, cultivating a cybersecurity-centric organizational ethos, and judiciously allocating resources to security endeavors, board members can safeguard their organizations from the ever-evolving cyber menace.

Here are some additional real-world use cases for board-level engagement in this area:

- **Supply chain risk management:** Boards can work with their organizations' supply chain partners to identify and mitigate cybersecurity risks. For example, they can require partners to have certain security certifications or to implement specific security controls.
- **Third-party risk management:** Boards can review the security of their organizations' third-party vendors and service providers. They can also require them to undergo security assessments.
- **Compliance:** Boards can ensure that their organizations comply with relevant cybersecurity regulations. They can also work with their organizations to develop and implement a cybersecurity compliance program.
- **M&A:** Boards can conduct cybersecurity due diligence on potential merger and acquisition targets. This due diligence should assess the target's risks and controls.

By engaging in these activities, boards can help to protect their organizations from cyberattacks and mitigate the risks of a cybersecurity incident. TI helps organizations safeguard their critical infrastructure outside the enterprise. That's particularly important because the technological landscape has evolved. And with it, so has the risk landscape.

THE ESCALATING CYBERSECURITY CONCERNS IN OT AND IOT

OT and IoT are pillars of today's business framework, bolstering operations and crafting new avenues for growth. Yet, their widespread adoption reveals vulnerabilities. Tightly intertwined with primary business functions, they pose alluring opportunities for cyber adversaries. An IoT or OT system breach can reverberate throughout the organization, jeopardizing operations. Consider recent episodes:

- **February 2023:** A cyber infiltration at a Florida water treatment facility led to the dispersal of untreated water, made possible by the exploited internet-connected treatment system.
- **March 2023:** A factory in Germany was attacked, culminating in a destructive fire. The assailants manipulated a connected temperature sensor, which subsequently ignited the blaze.

The Oldsmar, Florida, water treatment facility

- **April 2023:** China's transport network faced substantial disruptions attributed to a cyberattack on an interconnected train signaling apparatus.

These instances reveal the mounting cyber threats plaguing OT and IoT domains, underscoring the urgency for fortified defenses.

TI is the "tip of the spear" for the OT and IoT realms. It acts as a watcher over the evolving and everchanging threat matrix. Its strong detection of technology-specific vulnerabilities and prescriptive countermeasures combined with analyst tradecraft fortify these systems. The unique and varied nature of threats trained on OT and IoT mandates a custom-tailored defense strategy, which is precisely where TI's expertise becomes indispensable.

Boards should begin with an educational foundation. The core message is cybersecurity is everyone's responsibility. This should be a focus throughout the enterprise, and one that starts from the top.

With TI, organizations can:

- Pinpoint and mend weaknesses in the armor of OT and IoT devices.
- Introduce security measures tailored for them.
- Educate the workforce to recognize and escalate anomalies.
- Blueprint responsive protocols to address breaches in these technologies.

TI serves as a multi-faceted tool in securing an organization's OT/IoT environments. These actions, from identifying weaknesses to closing the skills gap, form a cohesive strategy designed to fortify the organization. It is crucial to remember, however, that the importance of device security is not limited to specialized networks. It permeates every level of a business, from core data centers to manufacturing systems—even reaching the personal devices of high-level executives.

DEALING WITH THE AFTERMATH OF COMPLACENCY

But what happens when companies are ill-prepared and the defense fails? What are the aftereffects of a data breach? Often enterprises experience a drop in morale. They may lose the trust of customers. They may need to launch a crisis management campaign to lessen the damage to the company's brand.

Apathy or ill-informed choices exact a heavy toll. Beyond immediate disruptions, infringements within OT and IoT can bleed finances, tarnish reputations, and invite legal entanglements. Moreover, given our intertwined business networks, the fallout from a breach can trigger a domino effect, denting stakeholder confidence and market standings.

Take the Florida incident, where the unchecked spillage could have spurred health crises and ecological mishaps. Or the German factory episode, where the fire could have destroyed the entire establishment, wreaking financial havoc.

As the landscapes of OT and IoT continue to evolve, so do the associated threats. Leveraging the insights from threat intelligence, board members must lead with foresight, helping their organizations remain robust and poised for the challenges ahead.

INTEGRATING TI INTO BOARD-LEVEL DECISIONS

Embracing new technologies such as AI and blockchain has brought myriad new cyber vulnerabilities. The complexity of these threats is continually growing, and threat actors are adopting new vectors and techniques at an unparalleled pace. On average, over 25,000 new vulnerabilities are found every year, and the number is growing at a 13% rate year-over-year.

For board members, whose expertise typically centers around business strategy and finance, TI can feel foreign and challenging to navigate. Traditional boardroom discussions are often grounded in tangible metrics such as revenues and market share. In contrast, TI presents qualitative and quantitative data that may include technical terminology and nuanced details.

In today's distributed world, where cyber threats are increasingly complex and pervasive, boards cannot afford to overlook the strategic importance of threat intelligence.

While board members are adept at managing traditional business risks, cybersecurity threats are more nebulous. They may bring financial losses and long-term damage to reputation, trust, and brand value. Navigating security risks requires more than traditional business experience and tradecraft. For board members, it means expanding their perspectives and approaches. It requires integrating a holistic approach that considers both internal and external threats and incorporates them into decision-making processes.

Integrating TI into board-level decisions involves more than understanding the risks and understanding current threats. It requires a proactive approach to forecasting future vulnerabilities, assessing organizational readiness, aligning cybersecurity strategies with broader business objectives, and ensuring that security measures don't hinder innovation.

The challenge of assimilating TI at the board level is multifaceted and demands a shift from conventional risk management thinking. Board members must grasp the dynamic nature of cyber threats and recognize how TI can be leveraged to protect assets and add value to the organization.

SO, WHAT CAN BOARDS DO?

For boards to be successful, they must take a multidimensional approach. By embracing solutions that are rooted in education, robust frameworks, internal and external expertise, collaboration, and integration into governance structures, board members can make informed decisions that position their organizations to be at the forefront of cybersecurity defenses. In addition to my list of suggestions above, here's a roadmap for boards to consider when working with their companies to improve their security posture.

- **Foster a Cyber Culture of Contextual Threat Education:** Boards should begin with an educational foundation. The core message is cybersecurity is everyone's responsibility. This should be a focus throughout the enterprise, and one that starts from the top. Board leadership must drive this culture and lead by example by

attending seminars, workshops, and even regular briefings about the latest cyber threats and how TI can elevate their understanding, leaving them better equipped to integrate these insights into strategic decisions.

- **Implement a Cyber Risk Framework:** A robust framework not only structures the organization's approach to cyber risks but also highlights the role of TI in preempting, detecting, and responding to these risks. Most companies adhere to the NIST Cybersecurity Framework (CSF), ISO/IEC 27001/2 for global organizations, SOC2 for security compliance, HIPPA for health care, and NERC CIP for electric utilities.
- **Utilize Third-Party Experts and Services:** In areas where in-house expertise may fall short, third-party cybersecurity consultants can offer specialized insights and recommendations, ensuring that board-level decisions are informed by the latest industry best practices.
- **Encourage Cross-Functional Collaboration**: It's essential to break silos. Encouraging departments like IT, Operations, Business Strategy, and DevOps to collaborate promotes a holistic approach to cybersecurity, where TI informs every facet of business operations.
- **Introduce Threat Intelligence into GRC (Governance, Risk Management, and Compliance):** Embedding TI into the organization's GRC processes ensures that governance structures and compliance protocols are always informed by the most recent threat data, positioning the enterprise to better anticipate and mitigate cyber risks.

The complexity of today's cybersecurity landscape requires board members to be more proactive than ever. By understanding the challenges and adopting tailored approaches, boards can help their organizations remain resilient and ahead of the curve in an increasingly volatile cyber environment.

THE BOTTOM LINE

In today's distributed world, where cyber threats are increasingly complex and pervasive, boards cannot afford to overlook the strategic importance of threat intelligence. Effective tools go beyond mere risk mitigation; they equip organizations with the foresight to understand evolving cyber threats and fortify OT and IoT assets. A robust threat intelligence strategy enhances situational awareness and helps prioritize cybersecurity investments, thereby offering a more proactive defense against cyberattacks that could result in significant financial and reputational damage. For boards, the adoption of a threat intelligence strategy isn't merely a technical consideration—it's a fiduciary duty to protect shareholders, secure customer data, and safeguard the long-term health of the business.

CHAPTER 14

MODERN CYBERSECURITY: HARNESSING THE POWER OF CLOUD AND SAAS

DAVID NEUMAN

Businesses continually search for scalable, efficient, and cost-effective solutions to support their operations. Public cloud and software as a service (SaaS) technologies offer unparalleled value propositions to meet these needs. By transitioning to these services, companies can reduce upfront capital expenses, as there's no need to purchase and maintain costly in-house servers and software. They provide the flexibility to scale resources up or down in response to demand, allowing businesses to be agile and responsive to market changes. They also offer robust disaster recovery and business continuity features, often with a global network of redundant servers to ensure uptime and data integrity. In short, they drive operational efficiencies and empower companies to innovate and grow in a secure digital ecosystem.

However, they also come with both technical and business risks. Business leaders, including board members, need to understand how to think about these—and how to identify risks introduced by cyber threats within cloud-based platforms. They also need to know how to collaborate effectively with their colleagues, including those on the tech side, to help guide their companies around the dangers.

IT STARTS WITH STRATEGY GOVERNANCE

Adoption of cloud and on-demand software comes with a double-edge sword. It is designed for rapid adoption and scalability. In most cases, this is as easy as a credit card and a laptop. Before the advent of cloud and SaaS, technology platform implementations could take weeks or months, depending

on the product being designed and implemented. Now, with a few clicks, basic infrastructure and services can be quickly activated. With the appropriate planning, design, and maintenance, these implementations will likely deliver the necessary resilience and security to protect business interests for years. But they're not like a self-driving car. They don't operate independently.

Who is responsible for driving a company's cybersecurity strategy? The board of directors is responsible for protecting shareholders' and investors' interests, establishing management policies, overseeing the corporation's (or organization's) governance, and making critical business decisions. Does this include adopting technology to bolster cybersecurity? Board members are not the technology experts, but they can certainly help establish governance on the strategy.

Board members are not the technology experts, but they can certainly help establish governance on the strategy.

For example, when incorporating cybersecurity into the governance strategy for public cloud and SaaS applications, with the understanding that cyber threats are a priority risk, the approach requires a heightened focus on security practices, compliance, and incident response. And it's going to require a team to make it happen.

These could be the group's marching orders: Start by setting clear strategic objectives that align technology adoption with business outcomes. Beyond the standard objectives, prioritize cybersecurity goals such as achieving specific security certifications and reducing incident response times. Then outline responsibilities for team members.

Among them will be the board of directors, of course, but it doesn't stop there. IT leadership, cloud providers, SaaS vendors, and various cybersecurity teams will be involved. Assign specific roles for monitoring, responding, and reporting cyber incidents. Use a cloud governance framework with a strong emphasis on security, such as the Cloud Security Alliance's guidelines or NIST's Cloud Computing Security Reference Architecture. Ensure all cloud and SaaS solutions comply with the organization's cybersecurity policies. When considering managing cybersecurity risks, focus on ones like data breaches, ransomware attacks, insider threats, and supply chain vulnerabilities. Prioritize risks related to cloud and SaaS. Create clear cybersecurity policies specifically for them. Board members may also consider creating subcommittees that focus specifically on cybersecurity strategy.

UNDERSTANDING THE TECHNOLOGY

At a high level, public cloud services operate on a multi-tenant architecture where third-party service providers offer the infrastructure, storage, and networking capabilities to the general public over the internet. These services often rely on virtualization to pool together physical resources and deliver them to users as virtual resources. There are various service models in the public cloud, including infrastructure as a service (IaaS), platform as a service (PaaS), and SaaS. Each provides different levels of control, flexibility, and management according to business needs.

SaaS applications are a subset of cloud computing, where software applications are hosted remotely on cloud servers. Unlike traditional software that requires installation on individual machines, SaaS applications can be accessed directly through a web browser. This means that all data and settings are stored in the cloud, allowing for real-time collaboration and data syncing across multiple devices and locations. These applications often use a multi-tenant model, where multiple customers share a common infrastructure and code base but have their own separate data and configurations. SaaS providers handle maintenance, compliance, and security, which are encapsulated into a subscription-based pricing model. This offers businesses the advantage of always using the latest software versions without needing manual upgrades, allowing quick deployment and scalability.

Organizations can leverage cloud and SaaS-based platforms hosted in remote data centers rather than investing in and maintaining physical servers and software applications on-premises. These services provide on-demand access to a wide range of scalable resources—from computing power and storage to specialized software applications—all via the internet. Managed by third-party vendors, these platforms handle routine maintenance, updates, and security measures, freeing up businesses to focus on core objectives. The cloud-based model offers unparalleled flexibility, cost-efficiency, and accessibility, making it vital to modern business strategy.

The board's role is not to manage security capabilities protecting these services directly, but to ensure they are aligned with the organization's broader goals and risk tolerance. The specifics may be complex, but the principles are clear: Robust cyber protection is about more than technology; it's about an integrated approach that encompasses strategy, processes, technology, governance, and culture. Understanding and embracing this complexity is crucial in an era in which cyber threats are not just a risk to be managed but a fundamental challenge to be overcome. In this intricate dance between innovation and protection, the board's role is to lead with vision, vigilance, and unwavering commitment to organizational integrity.

WHEN THE CYBER INCIDENT HAPPENS

I once worked with a client who had a digital near-death experience. Sensitive data and their proprietary applications were hosted in a large public cloud. A known weakness within rules used to provide access to data was accidentally exposed externally by an engineer who should never have had permission to do so. The weakness was exploited by a swarm of bots designed to find and exploit it without direct human interaction. An expensive and disruptive incident response ensued to contain the exploit, assess the damage, and recover from the incident. The client was lucky. There was no data exposure or material

damage to the organization. That outcome resulted from preparedness, leadership during the response, and a bit of luck. Then the questions started. Isn't the cloud supposed to be more secure? Why weren't there better controls? Should we change or move away from the public cloud? And my personal favorite: Who was responsible?

You can compare the use of service infrastructure and subscription software to driving an automobile on a long trip. If you are planning a journey that takes you over rough terrain and you drive a vehicle that is not equipped with four-wheel drive, the appropriate tires, suspension, and, most importantly, an experienced driver, your trip will be short-lived. Suppose you acquire the best vehicle for this trip but don't plan your route or have an experienced driver. You will likely have a successful start, but you will take on serious risks due to a lack of planning and preparation.

In the intricate dance of modern enterprise, the rhythm of digital evolution beats persistently, challenging board members with an ever-changing landscape. It's vital to remember that the board's role isn't to grapple with every technological detail, but to shape and guide the overarching strategy.

The same will be true if you adopt these technologies. There will be incidents—period. Full transparency is necessary to learn and improve. In the aftermath of a cyber incident, there is always a mixture of concern, urgency, and the need for clarity. A cyber incident, irrespective of its size or direct implications, is a testament to the vulnerabilities within an organization's digital walls. For a board of directors, a comprehensive debrief isn't just desirable—it's imperative.

Picture this: You're a board member when news of a cyber incident involving your cloud or SaaS technology trickles in. Understanding the breach's intricacies is crucial. The board gathers, awaiting a debrief. The CEO and the chief information security officer (CISO) step forward to unravel the events. The presentation begins with an overview of the incident. The type of breach, the moment it was detected, and the initial reactions set the scene. The board leans in, absorbing the gravity as the scope of the incident unfolds. You learn of several affected systems, potential clients at risk, and external parties entangled in this digital web. But here's the key question. How did the organization respond? The immediate actions taken to contain and combat the cyber onslaught are outlined, painting a picture of agility and resilience. At the same time, the intricate technical findings are deciphered, presenting a tale of exploited vulnerabilities or malicious tools that found their way in.

The narrative inevitably shifts to the financial aftermath. The tangible costs, looming legal implications, and silent yet profound reputational costs are laid bare. The board is then guided through the maze of regulatory and legal implications, shedding light on potential infringements of regulations, the legal landscape, and the punitive shadows that might be cast. In the age of information, the communication and public relations plans adopted become a pivotal chapter in this tale.

As the dust settles, reflections begin. The board is walked through the lessons learned—those stark revelations about gaps in the digital armor or perhaps oversights that, in hindsight, appear glaring. But with lessons come the promise of change. The future mitigation strategies, a blueprint of resolutions and

reinforcements, offer determination to learn from the incident and improve against future threats.

The narrative winds down with insights into the employee and insider impacts, a testament to the human element within this digital saga. It's complemented by stakeholder feedback that encapsulates the broader ecosystem's reactions, concerns, and sentiments. As the debrief concludes, a timeline is presented, a chronological tapestry detailing the incident's ebb and flow. The board is also apprised of any external support sought—a reflection of collaborations forged in the crucible of a crisis. Armed with knowledge, understanding, and a roadmap, the board is poised to guide the organization into a future defined by resilience, learning, and an unwavering commitment to cybersecurity.

FINAL THOUGHTS

In the intricate dance of modern enterprise, the rhythm of digital evolution beats persistently, challenging board members with an ever-changing landscape. Amid their vast responsibilities, the cybersecurity domain, especially regarding public cloud and SaaS applications, emerges as a nuanced segment demanding attention and foresight. The breadth and depth of this domain can indeed feel overwhelming. Still, it's vital to remember that the board's role isn't to grapple with every technological detail, but to shape and guide the overarching strategy.

Frequent dialogues with technology leaders or external cybersecurity experts with business acumen can offer invaluable insights. These regular briefings ensure that the board remains abreast of the latest threats and technological shifts without being submerged in operational intricacies. Beneath this high-level awareness and empowering ethos lay a sturdy foundation. By investing in and supporting cybersecurity teams through finances and continued professional development opportunities, boards ensure the organization's frontlines are manned by the best and brightest.

Risk assessment provides a structured lens to view potential weak points, particularly weaknesses associated with public cloud and SaaS platforms. When incorporated into the broader risk management framework, these assessments offer a more straightforward path forward, delineated by priority and impact. And yet, while the internal mechanisms of an organization are crucial, there's immeasurable value in extending the gaze outward. By collaborating and exchanging insights with industry peers, boards can tap into a wellspring of collective experience and wisdom, magnifying their understanding and enhancing strategic decision-making.

A cornerstone that can't be emphasized enough is embedding cybersecurity within the very fabric of organizational culture. When every company tier, from entry-level personnel to the executive suite, respects and values the importance of digital safety, the collective strength against potential threats multiplies.

ABOUT TAG

TAG is a trusted, next-generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, advisory support, and personalized content—all from a practitioner's perspective.

Photographs on pages 74, 75 : Getty Images

Publisher. TAG Cyber, a division of TAG Infosphere, Inc., 45 Broadway, Suite 1250, New York, NY 10006.

GUIDING CYBERSECURITY FROM THE BOARDROOM

TAG

NEXT PEAK