THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

Emerging Practices in Cyber Risk Governance

THE CONFERENCE BOARD creates and disseminates knowledge about management and the marketplace to help businesses strengthen their performance and better serve society.

Working as a global, independent membership organization in the public interest, we conduct research, convene conferences, make forecasts, assess trends, publish information and analysis, and bring executives together to learn from one another.

The Conference Board is a not-for-profit organization and holds 501(c)(3) tax-exempt status in the USA.

www.conferenceboard.org

EXPLORE THE FULL PORTFOLIO

This Member Report is part of a suite of products The Conference Board is offering to help you and your organization identify and mitigate cyber risks through effective governance.

Functional Executive Reports (all 8 pages)

CEO Strategic Implications

CFO Strategic Implications

General Counsel Strategic Implications

Connect with our experts, your peers, and more thought leadership on this topic at:

www.conferenceboard.org/cyber-risk-governance

Emerging Practices in Cyber Risk Governance

KEY BUSINESS ISSUES

By Andrea Bonime-Blanc

Contents

Executive Summary

Cyber risk is not a stand-alone or isolated issue—it cuts across many other major risks that can adversely affect the strategy and business plan of an organization. No entity is completely immune from cyber risk.

Good governance on any risk issue is not only about the board, its oversight, responsibilities, duties, obligations, and possible liabilities. Cyber risk governance begins with the board, but it is only complete if it is in essence a triangular relationship that includes the CEO/C-suite, which has primary responsibility for cyber security strategy and risk management, and the top cyber security talent leading and implementing the details of the cyber risk and cyber security plan on a daily basis within an organization.

This report draws on the learning and experiences of a wide array of corporations, think tanks, associations, experts, and data from publicly available sources as well as from one-on-one interviews with representatives of some of the leading global companies today in the health care, financial, infrastructure, outsourcing, and technology fields.

Underlying this perspective is the belief that if any entity—corporate, nonprofit, public—does not have a well-formed, thought-through, and constantly tested cyber risk governance framework, the work of managing, mitigating, and countering cyber risk will be exponentially more difficult.

Cyber risk governance is all about getting the architecture of cyber risk strategy and management right for your organization. Thus "cyber risk governance" is a framework adopted within an organization to deal with the new and evolving risks relating to cyber space both within the organization and as the organization interfaces with the outside world. In this framework, the key and critical actors are the board, the C-suite or executive team, and frontline management in charge of executing cyber risk management. This cyber risk governance triangle:

- Adopts, oversees, and promotes an appropriate, concerted, and coordinated philosophy or approach to cyber risk and cyber security for the organization;
- Develops the necessary and appropriate strategy (and budget, resources, and incentives) to execute on that philosophy or approach; and
- Implements that strategy in the most nimble and effective manner possible at an operational and tactical level.

One of the most cutting-edge and revolutionary approaches to cyber risk governance that we encountered in the research for this report was the one being built at a US-based Fortune 250 global business outsourcing and computing services company. There, a completely independent "business" is being created to serve the rest of the company for all of its technology and security services, including cyber risk management. This business has its own independent financial accountability to the CEO and the board, just like any other business segment, and it is not beholden to the other business segments for its budget and resources.

By the same token, this is not a rogue corporate security function; it has clear, direct, and frequent lines of accountability and reporting to both the CEO of the overall business and the board, perhaps on an even more regular and periodic basis than the other more established businesses given the nature of the company. While this may not be a model for everyone, it is an example of the creativity and customization that leading companies are experimenting with and succeeding at in this quickly changing and cyber threat-based global economy.

Without the proper governance stance toward an issue as complicated, new, and rapidly changing as cyber risk/cyber security, no company (or other type of entity for that matter, including governmental agencies) will have a chance at dealing with this risk preventively, let alone dealing effectively with a cyber-related crisis event.

Lessons Learned: The 10 Key Takeaways of This Report

1 Develop a triangular governance approach to cyber risk management

a. **The board must take a proactive approach to cyber risk oversight** Whether the domain of one or more committees or of the entire board and/or its chairman, the board sets the tone from the top on cyber risk governance and must take the governance lead. Key elements the board should consider for cyber risk governance oversight include an update on the architecture of cyber risk management, the resources and budget allocated, and a list of company "crown jewels" from a cyber risk standpoint.

b. **The CEO and the C-suite must take charge of cyber risk strategy and management** Depending on the cyber risk readiness required at a given company, more or less direct CEO involvement on a regular and periodic basis is highly recommended. The more readiness that is needed, the more actual attention, leadership, and support will be needed from the very top of the executive food chain. Depending on the type of industry and other criteria that determine cyber risk intensity, the C-suite should consider whether to have a dedicated cyber risk/security executive at the executive table.

c. **The CEO and the board must ensure that the right frontline talent and resources are deployed** Cyber risk governance is complete when a company has the board engaged, the CEO and C-suite deployed, and the right balance of top technological and cyber expertise within its management ranks. This also entails getting the right outside experts in place for specific tasks, assessments, and reviews.

2 Understand the reputation risk consequences to strategic cyber risk management gone wrong

Cyber risk should be considered at the top of many companies' risk prioritization, whether they have suffered from a major or material cyber attack (yet) or not. When a company doesn't have the right overall cyber risk governance program in place, the potential reputation risk consequences can amplify the company's exposure to both tangible and further intangible consequences that may be difficult, costly, and lengthy to repair.

3 Know who your cyber risk actors and stakeholders are

All companies should undertake a critical exercise consisting of two activities: updating an ongoing threat matrix (as to actors and potential perpetrators) and understanding who the stakeholders are of your cyber risk exposure, what their expectations are of your company's cyber risk management, and what would happen if those expectations were not met.

4 Have a deep understanding of your organization's "crown jewels"

By knowing what cyber attackers are looking for—whether it is intellectual property, personally identifiable information, trade secrets, executive personal profiles, or financial information—the cyber risk governance triangle can exercise more effective oversight and management.

5 Engage in a relevant cyber risk public-private partnership

Corporate sector reception of the US government NIST framework has been generally positive, showing that public-private partnerships on developing the best cyber risk governance and management frameworks can be powerful. Such public-private partnerships, though voluntary, should be encouraged and become the norm. Austria, Germany, the Netherlands, Spain, and the United Kingdom have established formal public-private partnerships for cyber security, while both Japan and Malaysia have set up official partnerships.

6 Develop a cross-disciplinary approach to cyber risk management

Recognition of the complexity and novelty of cyber risk means no one expert can really "own" the issue; cyber risk morphs too quickly for silos to work. Instead, the best and brightest minds from a variety of disciplines need to be engaged. Whether one or more functions take the lead (information security, corporate security, enterprise risk management), each function should own a piece of the puzzle while working with others to understand the entire puzzle.

7 Develop a cross-segmental/divisional approach to cyber risk management

Another cutting-edge trend among companies at the high end of creating effective cyber risk governance entails deploying an integrated cross-disciplinary and cross-divisional team to keep a steady eye on cyber risk management within and across the company. In this way, each relevant function and each business segment owns one or more relevant slices of cyber risk management.

8 Make cyber risk governance an essential part of your organization's resilience approach

Those that perceive their cyber risk to be high or very high (e.g., utilities and global technology companies) can do periodic, even surprise, cyber security-related crisis management drills with executives and occasionally even board members. They should also have a well-developed emergency response and business continuity program in place.

9 **Choose one of the three effective cyber risk governance models**

- **The Vigilant Model:** Involves leadership that is engaged, knowledgeable, and vigilant on cyber risk issues, even though the entity has a relatively low to medium exposure to cyber risk given its operations, products, services, and footprint.
- **The Integrated Model:** A highly evolved form of cyber risk governance that has engaged, knowledgeable, and vigilant leadership, with effective, integrated cyber risk management and governance at a largely decentralized, medium to high exposure organization
- **The Command & Control Model:** Another form of highly evolved cyber risk governance with engaged, knowledgeable, and vigilant leadership as well as an effective form of cyber risk management and governance that is organized in a more centralized, command-and-control manner for a more centralized organization that has medium to high cyber risk exposure.

10 **Transform effective cyber risk governance into an opportunity for better business**

While not every company can transform its cyber risk into possible additional value in the form of new products and services and new revenues to the company, as some of the companies we profiled have done, every company can certainly implement business process improvements, with greater efficiency and coordination that in turn will provide cost savings in the form of fewer incidents, not losing important stakeholders (investors, customers, employees), and not paying exorbitant fines or legal and litigation costs.

Introduction and Overview

"We live in an age of digital Darwinism … Evolution doesn't wait." Though this quote from digital trend analyst Brian Solis of Altimeter Group is not directly about technology (it's about innovation),[1] it could just as easily be said about the subject of this report: cyber risk governance. It speaks to the pace, breadth, and depth of change taking place. It speaks to the era we live in of limits being pushed, molds being broken, and the unexpected shattering the expected.

Innovation and change in cyber tools, techniques, armor, and weapons is breathtaking. Because of this rapid-fire change, cyber risk governance is no longer a "nice to have" but a "must-have," regardless of the type of entity: big or small; domestic or international; for-profit, nonprofit, university, or governmental agency.

While much of the focus on cyber risk and cyber security has been on the technical perspective, this report aims to provide an overview of how companies can incorporate cyber risk into their existing enterprise risk management (ERM), executive, and board governance structures. What are the emerging models for board involvement? What is the proper delineation of responsibilities between the board and management? Where have companies chosen to house oversight for cyber risk management within their organizations?

In the wake of the well-known and massive cyber breaches in the United States (Target, Anthem, Sony, JP Morgan) and other international cases—notably, Malaysian Airlines, the Government of Singapore, European cases, and increasingly, financial and governmental targets in Latin America,[2] what do post-breach crisis management practices and disclosure to shareholders look like? And where are companies that are leaders in tackling cyber risk management and oversight taking cyber risk management and governance in the medium-term future?

In the research conducted for this report, The Conference Board approached a number of corporate executives and experts from a broad cross-section of industries and professions. While some were reluctant to draw attention to their companies given the truly disquieting nature of the subject, a good majority of those we contacted were willing to share their concerns and provide information on their current practices. The Conference Board agreed to conduct these interviews on a not-for-attribution basis, as the purpose of its research is to share emerging best cyber risk governance practices with others in an effort to inform and disseminate knowledge.

This report draws on the learning and experiences of a wide array of corporations, think tanks, associations, experts, and data from publicly available sources as well as from one-on-one interviews with representatives of some of the leading global companies today in the health care, financial, infrastructure, outsourcing, and technology fields.

The focus is on cyber risk at the top of the corporate house:

- The board of directors, which provides oversight on critical risk issues and sets appropriate performance incentives related to risk management;
- The C-suite/executive team, which executes the strategy and issues tactical guidance to the rest of the organization on critical risk matters; and
- The frontline management tackling the critical cyber risk issue itself on a daily basis.

For any entity—corporate, nonprofit, public—that does not have a well-formed, thought-through, and constantly tested cyber risk governance framework, the work of managing, mitigating, and countering cyber risk will be exponentially more difficult. Proper cyber risk governance is all about getting the architecture and substance of cyber risk management right for your organization.

Cyber Risk and Cyber Security in Context

> "Good boards…recognize the need to adapt to new circumstances—such as the increasing risks of cyber-attacks. To that end, board oversight of cyber risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cyber security issues. Given the heightened awareness of these rapidly evolving risks, directors should take seriously their obligation to make sure that companies are appropriately addressing those risks."[3]
>
> **Luis Aguilar, SEC Commissioner, June 2013**

Aguilar of the US Securities and Exchange Commission made this statement before the attacks on Target, Home Depot, JP Morgan, Sony, and the US government itself (in June 2015, the identities and personal employment details of 21 million current and former US government employees were apparently hacked or compromised; in September, it was also first revealed that the fingerprints of approximately 5 million of these US employees were acquired through these cyber attacks).[4]

Organizations need to understand and conquer their cyber risks and develop an appropriate and effective cyber risk governance framework.

Cyber Risk: From the Not So Sublime to the Not So Ridiculous

Two recent incidents illustrate just how sweeping cyber risk can be:

1. **Executives specifically targeted by state-sponsored hackers** The top global executive team of a Fortune 100 company was specifically targeted by nation-state hackers through a persistent long-term effort that eventually yielded these executives' and their families' complete personal data, including Social Security numbers, health insurance and health information, home addresses, emails, phone numbers, and anything and everything else that was kept in this company's "secure" C-suite human resources database. To this day, the company and its executives do not know what the nation-state is interested in doing with this information.
2. **35 million users of adultery website Ashley Madison "outed" by cyber hackers; CEO steps down because of related "reputation risk"** There's trouble for 35 million would-be adulterers who are members of the Ashley Madison website (motto: "Life is short. Have an affair.") as they have fallen victim to hackers who claim to have captured the personal information of all the site's users. The consequences of this revelation have been multiple so far and are likely to continue for some time as new stories are revealed of fake accounts and possible misrepresentation, leading to the recent resignation of the company's CEO and possible suicides by individuals who have been outed.[5]

What Is Cyber Risk Governance?

Governing cyber risk is "not just about addressing technology gone wild," as a cross-section of cyber risk expert executives at the front lines of managing this issue have noted.[6] Rather, cyber risk governance is a framework adopted within an organization to deal with the new and evolving risks relating to cyber space both within the organization and as the organization interfaces with the outside world. In this framework, the critical actors are the board, the C-suite or executive team, and frontline top management in charge of executing cyber risk management. This cyber risk governance triangle:

- Adopts, oversees, and promotes an appropriate, concerted, and coordinated philosophy or approach to cyber risk and cyber security for the organization;
- Develops the necessary and appropriate strategy (and budget, resources, and incentives) to execute on that philosophy or approach; and
- Implements that strategy in the most nimble and effective manner possible at an operational and tactical level.

Table 1 provides an overview of the role, duties, and responsibilities of the board with regard to cyber risk governance under current law (specifically Delaware).

Many good resources have been developed by knowledgeable technical, risk, and governance experts and and institutions over the past few years, including The Conference Board, although the literature on understanding the risk governance aspect of this issue is fairly new and still underdeveloped.[7]

Table 1

Legal duties and responsibilities summary for US-based boards: Where cyber risk fits

- Under Delaware law, there are three fiduciary duties directors owe to their corporations:
  - Duty of care
  - Duty of loyalty
  - Duty of good faith (an element of the duty of loyalty)
- There also exists the duty of oversight (another aspect of the duty of loyalty)
- Suggested ways to fulfill oversight responsibilities with respect to cyber security:
  - Understand cyber risk
  - Evaluate the organizational approach to cyber security
  - Request regular briefings on cyber risk/threats
  - Prioritize material cyber risks to protect business value
  - Request a security technology "road map" and budget estimates to implement the strategy
  - Test the company's response plan with a cyber exercise
- SEC Commissioner Luis Aguilar suggests "ensuring the adequacy of a company's cyber-security measures needs to be a part of a board of director's risk oversight responsibilities."[a]
- The commissioner also suggests using the NIST frameworks, creating separate risk committees, and delving into what roles information security should play within management[b]

a Speech by SEC Commissioner Luis Aguilar, "Cyber-Risks and the Boardroom," NYSE, June 10, 2014 (http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.U_qxa2NpfuY).

b This table is a summary of the memo written by the general counsel of a leading company, incorporated in Delaware, to the board featured in this post from The Conference Board Governance Blog describing what the general counsel believes the board's duties may be regarding cyber risk oversight quoted in: Marcel Buscescu, "Duties and Liabilities of the Board regarding Information Security," The Conference Board Governance Blog (http://tcbblogs.org/governance/2015/02/05/duties-and-liabilities-of-the-board-regarding-information-security/).

How Cyber Risk and Other Risks Intersect

Cyber risk is not a stand-alone or isolated issue. It cuts across other major risks that can adversely affect the strategy and business plan of an organization, and it is frequently related to criminal and even national security risks.

1. THIRD-PARTY AND SUPPLY CHAIN RISK

A wide array of third parties, ranging from individuals to global corporations, can have physical and/or digital access to company employees, systems, or properties, creating cyber risk.

Figure 1

Defining the components of cyber crimes and cyber espionage

According to the International Institute for Strategic Studies, a UK-based think tank considered one of the foremost authorities on global political and military conflict, cyber crime and cyber espionage can be broken down into six main categories:

1. The loss of intellectual property (IP) and business confidential information. Ironically, in an era of big data, predictive analytics, and increased data mobility and mobile access, IP that a company has yet to realize as IP may be going out the door.
2. Cyber crime, which costs the world hundreds of millions of dollars every year.
3. The loss of time-sensitive financial and business information that can be used for possible stock market manipulation.
4. Opportunity costs, including service and employment disruptions, and reduced trust for online activities.
5. The additional cost of securing networks, insurance, and recovery from cyber attacks.
6. Reputational damage to the hacked company.

Source: "Reframing the Issue: New Ways to Think about Cyber Risk and Security," The Conference Board, *Council Perspectives*, 2013.

Some of the third parties organizations should be concerned about are:

- Individual consultants or temporary workers
- Small to medium-size contractors and subcontractors who work on company premises or facilities
- Third-party vendors and suppliers to whom sensitive access may be given and who do not have sufficient internal cyber readiness of their own
- Business process outsourcing third parties who manage some of a company's "crown jewels" when it comes to cyber risk—like personal, health, or financial data
- Joint venture and other partners
- Suppliers and vendors along an organization's supply chain, which can be extensive and involve many layers of contractors, subcontractors, and sub-subcontractors, with possible access to physical or virtual assets

A weakness anywhere along this complicated chain of relationships and subrelationships can become a golden opportunity for an alert or stealthy cyber attacker.

2. EMPLOYEE OR OTHER INSIDER RISK

An organization's own employees are often the weakest link in the chain of cyber security since they possess legitimate access to physical and virtual assets, to which they can also gain illegitimate access. An *Economist* piece called "The Enemy Within" discussed how rogue or negligent employees pose a cyber security and an overall risk to an organization.[8]

Employees who are ignorant (because their company may not provide proper training) or negligent (despite their company's reasonable efforts to train) about protecting the company's assets by not following simple protocols (like using password protection for a company-issued device or not clicking on an unknown link and letting malware in) are often the way in which hackers, both pranksters and others with more broadly nefarious objectives (state-sponsored hackers, for example) get into a cyber system quietly, eventually making their way to the cyber "crown jewels."[9]

3. SOCIAL MEDIA OR OTHER TECHNOLOGY RISK

Social media risk intersects with cyber risk when employees, executives, board members, or third parties, using social media apps, download the wrong apps or allow themselves to be preyed upon by cyber attackers lurking within the specific social network. This can happen on any platform—Twitter, Instagram, LinkedIn—when individuals open their devices to possible cyber hacking, including through malware.

It can also occur when company secrets or material nonpublic information is casually revealed to the public, opening a company up to be targeted by cyber criminals or nation-state actors.

4. IP THEFT OR INDUSTRIAL ESPIONAGE RISK

Intellectual property (IP) theft and industrial espionage risk often relate to third party, supply chain, employee, or insider risk, where a weak link allows a cyber attacker seeking IP assets, commercial secrets, or trade secrets to find a way into the organization's system and finds its strategic plans, unpublished financial data, confidential projects, or blueprints.

5. PHYSICAL SECURITY AND SAFETY RISK

Physical security and safety risk can intersect with cyber risk when state-sponsored hackers penetrate organizations and target the personal data of employees, including high-level leaders, executives, and even board members. Investigators believe the hackers of the US Office of Personnel Management (see the case profiled on page 34) were state sponsored.

It is not yet clear what the intruders will do with the personal records of millions of people, but one possible avenue is to build individual dossiers on high-level executives and leaders for future extortion or other criminal or reputation-harming purposes.

6. GEOPOLITICAL RISK

Geopolitical risk intersects with cyber risk when cyber acts or crimes are or become issues of national security. This can occur in a commercial setting, such as when cyber espionage takes place within the private sector when a company like a defense contractor or a research university has sensitive government contracts that become juicy targets, especially for state-sponsored or even direct nation-state cyber espionage.

Other times, such cyber espionage activities can have geopolitical risk implications when cyber hacking takes place directly against government and military targets, whether through third parties or directly by nation-state actors. Clearly the Edward Snowden case is a leading case of an insider (in his case an approved independent contractor) having top-secret access to data and information (whether approved or attained wrongfully as an insider) at the National Security Agency, ostensibly one of the most secure governmental agencies in the world.

THE SPECIAL CASE OF REPUTATION RISK

The Reputation Risk Handbook: Surviving and Thriving in the Age of Hyper-Transparency provides the following working definition of "reputation risk":

> "Reputation risk is an amplifier risk that layers on or attaches to other risks—especially (environmental, social and governance) ESG risks—adding negative or positive implications to the materiality, duration or expansion of the other risks on the affected organization, person, product or service."[10]

The significance of reputation risk as an amplifier of another underlying risk like cyber risk cannot be overstated in this age of hypertransparency and superconnectivity, when it takes just a moment for information—whether accurate, inaccurate, or malicious—to travel to a worldwide network of willing recipients. In "The Downside: Five Cases of Cyber Risk Management Gone Wrong" (page 23), the effects of cyber risk management gone wrong on the reputations of the companies profiled will be further illustrated.

In October 2015, Marsh released an important new survey of global corporate executives showing that the two top global risks concerning C-suites and risk executives today were cyber and reputation risk, especially the reputation risk associated with cyber breaches: "79% of respondents selected reputational damage from a sensitive data breach as the most likely and high-impact risk."[11]

Cyber Risk Actors and Stakeholders

In addition to (and because of) the age of hypertransparency and superconnectivity, we are also witnessing the rise of the age of virtual warfare, which involves all manner of actors and stakeholders. It isn't confined to national or international government actors or boundaries. It isn't just the bailiwick of governments, militaries, and their leaders. It may not involve traditional weaponry, but it involves a variety of new, outside-of-the-box tactics, strategies, and virtual weapons with potential and real impacts as devastating as those of traditional warfare—or possibly worse.

Who are the strategists, generals, admirals, captains, and soldiers of this new form of borderless asymmetrical warfare? In one corner (the commercial corner) are the board, the C-suite, and the subject matter experts from companies, NGOs, universities, agencies, towns, small businesses, and individuals, all of whom are potential actors. Many if not all are also potential stakeholders and potential victims, as we are learning with every new cyber incident that unfolds. Joining them in that corner are a host of governmental (national and international) agencies and departments that are not only assisting in some cases but also withstanding serious and continuous attack from other actors "in the other corner."[12]

In the other corner, we have a vast array of cyber actors ranging from the unhappy hacker sitting in his basement, intruding on systems and networks around the world for fun or mischief, to the highly organized and purposeful nation-state that is looking to get into another nation-state's or its leading corporations' systems and networks for hostile, espionage, or other nefarious purposes (see Figure 2 on page 14). In the middle of this range are a variety of other insiders and outsiders.

In such a chaotic and not-so-brave new world, the leaders of organizations and the governance function of every entity (whether a company, a government agency, an NGO, or a university) must act with the knowledge, preparation, oversight, deliberateness, and effectiveness of a war machine—not necessarily because they will engage in warfare but because they need to be prepared.

In fact, there is much debate right now about the legality and desirability of nongovernmental entities like banks, for example, taking it upon themselves not only to proactively defend but also to retaliate against cyber intruders. This is the new Wild West, and it will take time for this area to sort itself out from a legal standpoint. As the *Financial Times* stated in a recent series on "Cyber Insecurity": "Companies are seeking to use more aggressive tactics to neutralise hackers. But the law limits how far active defence can go."[13]

This virtual war is new and misunderstood, without clearly defined targets, "enemies," or other objective boundaries, and it is constantly metamorphosing—changing in size, nature, quality, and impact not just periodically, but daily—even hourly. Cyber insecurity occurs in a new dimension and involves a form of virtual tribalism and possible warfare without frontiers. It involves attacks, counterattacks, defense, counterdefense, and the need for unprecedented thinking in a time of asymmetric information and reality.

CYBER ACTORS

There are basically three kinds of cyber actors:

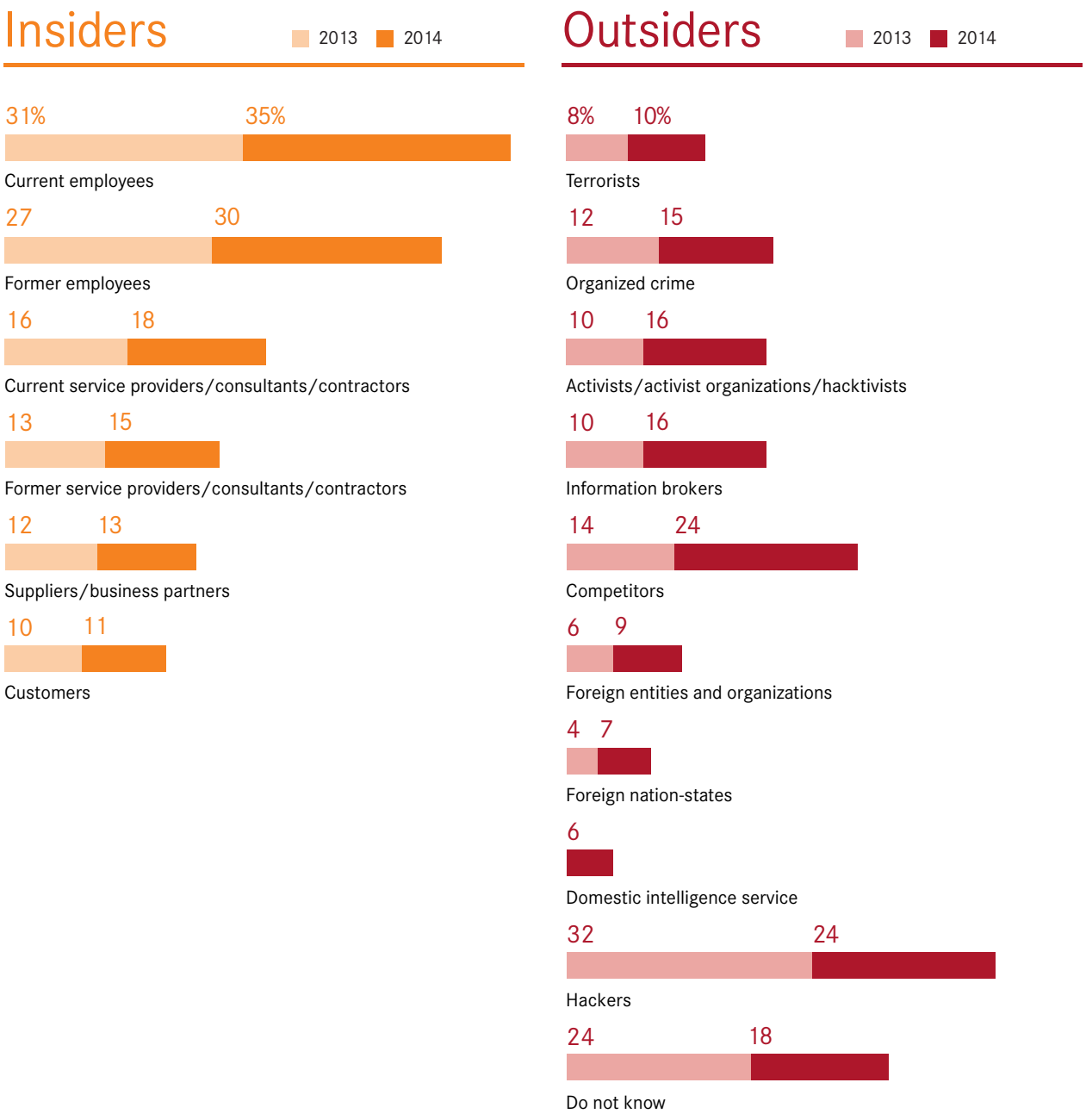
1. **Pedestrians:** those that act within cyber space in a largely lawful and unhurtful manner for either personal or professional purposes—most daily users of the internet and related technologies whether for personal or professional purposes;
2. **Attackers:** those that act in cyber space for more obscure, illegal, nefarious, criminal, or terrorist purposes; and
3. **Defenders:** those that are the cyber cops, counterterrorists, cyber militaries protecting their populations, businesses, countries, or other legitimate interests. This latter group isn't past being aggressive as well, but its principal purpose is to bring order to chaos, defend people and assets, and hunt down the "bad guys."[14]

The Intel IT Threat Agent Library's threat agent risk assessment provides an overview of the variety of possible cyber actors and the activities they are mostly likely to be engaged in.[15]

Figure 2

CYBER ACTORS: INSIDERS AND OUTSIDERS

Sources of security incidents, 2013–2014



Source: "Managing Cyber-Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015," PwC, 2015 (http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml).

CYBER STAKEHOLDERS

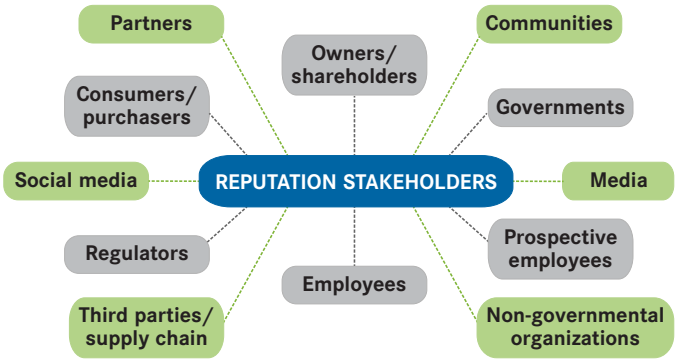
Everyone is a cyber stakeholder sooner or later—even those who do not frequent the internet or use social media. Otherwise completely disconnected people, perhaps an elderly person who doesn't know how to use a computer or an impoverished rural family without the means to own a computer, still have a stake in cyber safety because they are likely to have their personally identifiable information stored digitally at an insurance company, bank, government agency, or health care facility.

Even if we are roaming the cyber world as mere cyber pedestrians, generally minding our own business and not inflicting harm on anyone else, we have a stake in the cyber world not being dangerous to our health or well-being or that of our family, friends, and colleagues. In other words, we have an expectation that others in the cyber world—our employers, banks, and health care facilities that hold our confidential personal data, for instance—have the proper defenses and protections in place against cyber criminals, spies, bullies, and others who may seek to invade privacy, steal identities, or abscond with other valuable or sensitive information.

A given company or organization could have a variety of possible reputation stakeholders on a given issue or crisis at any given time (including a cyber security incident).

Figure 3

REPUTATION STAKEHOLDERS



Source: Andrea Bonime-Blanc, *The Reputation Risk Handbook: Surviving and Thriving in the Age of Hyper-Transparency* (Oxford: DŌ Sustainability, 2014).

The people ultimately responsible for proper oversight, strategy, and implementation of a sound cyber risk governance program are the board, the CEO and C-suite, and frontline executives in charge of cyber risk and cyber security. The effectiveness of an organization's cyber risk governance triangle is the only thing that stands between that organization managing through a cyber risk crisis relatively successfully or stumbling and falling with material financial and reputational costs. Some of the downside cases we examine later in this report speak to this issue.

Figure 4

Organizational Reputation Stakeholders

Internal	External
Owners/shareholders/investors:	Customers, purchasers, & clients
• Family	Users of products and services
• Private	Prospective owners, shareholders, investors
• Public	Partners & suppliers
• Government	Communities
• Institutional	Non-governmental organizations
• Activist hedge funds	Prospective employees
Boards of directors, trustees, or supervisors	Government agencies, regulators, enforcers:
Board committee & chairs	• Local
Council of advisors	• Provincial/state
Employees	• National
Temporary & contract workers	• International
Labor unions	• Media & social media
Workers councils	

Source: Andrea Bonime-Blanc, *The Reputation Risk Handbook: Surviving and Thriving in the Age of Hyper-Transparency* (Oxford: DŌ Sustainability, 2014).

Cyber Risk in a Technological Context

SOCIAL MEDIA

Social media is "anywhere users can communicate with each other through an application."[16] While commonly cited examples of social media include Facebook, Twitter, Instagram, and Snapchat, sites such as Match.com, Tumblr, and Shazam can also be categorized as such. While social media was once believed to be no more than a fad, this is no longer the case, as it has created significant change in how people and businesses communicate. While many people recognize positive uses of social media—one-fourth of the global population had a social media profile of some kind in 2014—many fail to consider the risks associated with these tools.[17]

Since few regulations exist regarding social media, it can be easily exploited for malicious purposes. For individuals, this can include identity theft, as hackers can extract mass quantities of personal information from social media profiles.[18] Attackers can also use these profiles to propagate "consumer scams, phishing, malware, and the sale of stolen goods."[19] For businesses, the implications extend beyond this. Even a fake social media profile created for a company executive can wreak long-lasting damage on the company's reputation. Using social media to infiltrate an organization is another possibility—over one-quarter of data breaches in 2012 used social tactics.[20]

The threats arising from social media exploitation often come from hackers trying to make money, collect data, or disparage businesses, but another cyber risk has come about from terrorist organizations. These organizations, most notably ISIS, largely use social media to communicate with their members and enlist new ones. Techniques used include hashtag hijacking—when the organization "piggybacks on trending hashtags to spread propaganda." ISIS and its supporters have also been able to hijack social media profiles of US Central Command to not only spread propaganda but to dismantle the credibility of the government institution's security measures.[21]

BIG DATA

Big data is the term used for data sets massive enough to extend beyond the capacity of what modern data processing systems can handle. Over the past few years, it has become a buzzword often associated with creating new technologies and more precise marketing mechanisms, but it also has great implications for cyber security. One clear negative impact of big data is that with more useful data sets come more hackers who want that data. However, the importance of "big data" gives rise to companies performing big data analytics. From IBM to smaller firms, many believe combining current cyber security knowledge with data analytics on a massive scale is the next step in cyber security.[22] Using big data analytics to run through vast amounts of data needed for use cases and software testing, cyber security technology can grow faster than ever.[23]

INTERNET OF THINGS (IOT)

The IoT is the network of objects electronically connected in some capacity to either other objects or to manufacturers/operators. The ultimate goal of the IoT is to push society forward through automation and "smart" products, ultimately creating much more convenience in everyday life. However, having such an interconnected network leads to the risk of both more frequent and more harmful cyber attacks.

The IoT increases the threat of a cyber security attack for all firms. According to a study on the IoT by HP, 70 percent of the most frequently used IoT devices contain vulnerabilities and thus create risk for the network at large. Cyber criminals, as a result, are quickly seeking out ways to exploit this system for their personal gain. The IoT creates more points of access for hackers as it opens operating technology systems that have traditionally been closed.[24]

Only recently, several incidents have been reported in the media of remote access and control by hackers of computerized car systems, for example. One such event took place in July 2015: "In the first action of its kind for the auto industry, Fiat Chrysler last week announced the recall of 1.4 million US vehicles to install software to prevent hackers from gaining remote control of the engine, steering, and other systems."[25]

Risk for cyber attacks is further increased through the IoT's need for cloud computing. Cloud computing, essentially storing and processing data on the internet rather than locally, has its benefits, but like the IoT itself, it comes with many risk challenges that have yet to be adequately addressed.[26]

ARTIFICIAL INTELLIGENCE

> "The development of full artificial intelligence could spell the end of the human race."[27]
>
> Stephen Hawking

Artificial intelligence (AI) is an area of computer science that has the goal of developing computer systems that can function and solve problems like humans.[28] Modern computer systems have the capacity to perform simple tasks with remarkable efficiency. AI is not designed with these problems in mind. Rather, AI is being designed to reason as humans do and to adapt to situations so that computers can tackle more complex issues, perhaps with some human involvement, but eventually autonomously.[29]

The idea of AI elicits mixed reactions from both the typical person and the world's greatest minds. Bill Gates, Stephen Hawking, and Elon Musk have all expressed concerns that AI will one day pose a serious threat to humans, to the extent that it may one day lead to our extinction.[30] This idea, however, is only a long-term concern. For now, AI has been used successfully for military and retail purposes (drones), among others. Looking to the near future, experts believe it will create remarkable change in myriad industries, including in cyber security.[31]

However, the applications of AI to some other technologies currently under development—for example, machines that could be equipped with AI and deployed for warfare (so-called killer robots, which military in various parts of the world are interested in or already developing) could spell serious if not truly deadly consequences to mankind.

AI has already played a role in cyber attacks. At the start of the Arab Spring in 2011, the hacker group Anonymous used AI to clog the networks of the Tunisian government, ultimately bringing down the websites of the president, prime minister, and the Tunisian stock exchange. For the most part, however, AI is believed to be beneficial for cyber security. Once developed enough, AI will have the capacity to "implement algorithms designed to identify cyber threats in real time and provide an instantaneous response."[32] Because humans often identify cyber threats too late, evolving computer systems are believed to be a beacon of hope in preventing cyber attacks by hackers.

THE CLOUD

The cloud is a network of servers, each with a different function. One function can be to run applications, as is the case with the Adobe Creative Cloud. Another more commonly spoken of use of the cloud is data storage, such as through Dropbox, Google Drive, Microsoft Azure, and iCloud. Cloud computing, "the process of sharing resources to optimize performance," is adopted by businesses for its efficiency, scalability, and reduced cost when compared to hardware.[33]

While the benefits of cloud computing are many, so are the risks. The amount of information stored in "cloud applications has significantly increased the threat surface for cyber attacks." The risk increases further because 1 in 4 employees violates "corporate data security policy in public cloud applications, opening organizations to risk of data breach and compliance concerns." In the event of a cyber attack on a cloud application, not only can hundreds of thousands of files be exposed and stolen ("the average organization has 100,000 files that contain sensitive information stored within public cloud applications"), but the attacker can also use administrator privileges to change user passwords and delete accounts.[34]

The Cyber Legal Framework in the United States, European Union, China, and Latin America

UNITED STATES

REGULATION & LEGISLATION

Considering cyber security regulation, the consensus among lawyers and industry leaders is that there is a growing distance between cyber threat development and the law. There is some legislation regarding cyber security, but for the most part, only tangentially. As of now, there is no comprehensive federal legislative framework for cyber security. Revisions to the existing laws have been considered, but there has not been any major cyber security legislation since 2002 (though there have been major attempts).[35]

While the United States has had a federal privacy law in place since 1974 (the 1974 Privacy Act), it has always had a different take from other countries on how to protect such data, creating a post-breach reporting obligation rather than requiring too many pre-breach precautionary measures. Since the dawn of the age of the internet, California has led the way in terms of digital data breach reporting requirements, adopting the first comprehensive state law of this kind in 2003. Most of these laws focus on aspects of cyber risk having to do with the reporting of the breach, loss, or theft of protected data to appropriate government authorities. As summarized by a leading publication on this topic, since 2003:

> Approximately 47 states, the District of Columbia and other US jurisdictions, and the federal banking, health care, and communications agencies have also required companies to provide mandatory data breach notification to affected individuals, and imposed affirmative administrative, technical, and physical safeguards to protect the security of sensitive personal information. Dozens of other medical and financial privacy laws also exist in various states. There is, however, no single omnibus federal privacy law in the US. Moreover, there is no designated central data protection authority in the US, though the Federal Trade Commission (FTC) has essentially assumed that role for consumer privacy.[36]

Despite legislation around cyber security being somewhat decentralized, there are some provisions worth noting. Among them is the Homeland Security Act of 2002 (HSA), which gave the Department of Homeland Security some cyber security responsibilities beyond those assumed by its general responsibilities. The E-Government Act of 2002 is one of the more significant federal efforts. This law guides federal IT management and initiatives to make information and services accessible online and has various cyber security requirements.[37]

While federal legislation is lacking, regulatory bodies have introduced industry-specific legislation. Section 5 of the Federal Trade Commission Act is one example of this. It states that the FTC has the capacity to investigate "unfair or deceptive acts or practices in or affecting commerce." The wording of this section has afforded the FTC the right to look into "unfair and deceptive" privacy and data security practices. In many ways, the FTC has become, almost by default, the federal agency most involved in the oversight of federal cyber security regulations and issues.[38]

Another example of regulatory efforts is the Securities and Exchange Commission's Division of Corporate Finance Disclosure Guidance. Released in 2011, the guidance requires disclosure, as with any other potentially material issue, of a cyber risk incident, development, or threat that may be material to the investor.[39] Government agencies also have responsibilities regarding cyber security in specific sectors. For the Department of Transportation, this is of course the transportation sector. The National Security Agency is in charge of all cyber security efforts in national security; and military cyber space operations are handled by the Department of Defense's US Cyber Command.[40]

EXECUTIVE BRANCH INITIATIVES AND GUIDELINES: NIST

The National Institute of Standards and Technology (NIST) was established in 1901 to better the nation's measurement infrastructure. While NIST now does some of the same work, it has since expanded into a number of fields, including information technology (IT).[41] Within the IT space, NIST's mission involves "accelerat[ing] the development and deployment of systems that are reliable, usable, interoperable, and secure."[42] To continue on this mission, and in response to President Obama's Executive Order 13636, NIST worked on creating a framework "for reducing cyber risks to critical infrastructure."[43]

Issued in February 2013, Executive Order 13636, Improving Critical Infrastructure Cybersecurity, is meant to help establish a more innovative and efficient cyber environment while also promoting security and civil liberties. The Executive Order directed NIST to create what is now known as the Cybersecurity Framework ("Framework") first delivered approximately one year later. While the Framework is meant to allow critical infrastructure organizations to better manage and limit cyber security risk, the Executive Order (and NIST) did not make it mandatory; rather, it is a voluntary guidance formed by a collaborative effort between NIST and thousands of industry leaders.[44] Ultimately, the main purpose of this Executive Order has been to facilitate the flow of information and collaboration between the US government and the critical infrastructure companies.

NIST defines critical infrastructure as:

> Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cyber security, national economic security, national public health or safety, or any combination of those matters.[45]

The Framework is composed of the Framework Core, Implementation Tiers, and Profiles. The Core, "a set of cyber security activities, desired outcome, and applicable references that are common across critical infrastructures," is made up of five Functions: Identify, Protect, Detect, Respond, and Recover.[46] These Functions make up a loose view of the cyber security risk management life cycle of a company. Within each Function, there are actions to be taken.

For the **Identify Function**, one action is to conduct a NIST Cyber Framework Readiness Assessment. This is meant to compare and contrast a critical infrastructure's current information security program attributes with those of the five Functions. Simultaneously, the infrastructure using the Framework must develop a cyber security or information governance charter to help coordinate activities between departments. Updating the security and data protection policy suite to incorporate NIST vocabulary and structure, thus allowing ease of communication with internal and external parties, should also be considered.

The **Protect Function** consists of three actions: the critical infrastructure must receive anticipatory alerts to potential threats, participate in cyber information sharing, and build safeguards. These are both vendor assessment processes and enhanced contractual safeguards.

The **Detect Function** is fairly simple in that the sole action is to continuously scan for threats and malware. Updating the **Respond Function** to meet guidelines entails developing plans for any sort of cyber security breach; these plans can and should be tested with simulations. The action suggested for the **Recover Function** is to classify all assets with regard to criticality and sensitivity so as to help companies focus their efforts accordingly.

After considering these functions, an organization can identify its Categories and Subcategories for each Function. The Framework's Implementation Tiers are designed to describe the degree to which and organization's cyber security risk management practices exhibit the characteristics defined in the Framework. The tiers, from 1 to 4, display how reactive an organization is to how risk informed it is. Lastly, the Framework's Profile explores the outcomes that derive from a business' choice of Framework Categories and Subcategories. [47]

As it stands, the industry is receiving the NIST Framework well. An Intel use case indicates approval of the Framework and a desire to continue using it to further improve the company's risk management systems. As the Framework is constantly being updated, Intel does suggest the Framework include the cyber threat intelligence life cycle.[48] While Intel views the Framework in a positive light, opinion is split among industry experts; the consensus, however, is that its mere existence is a success.[49]

EUROPEAN UNION

> "The [EU cyber security] strategy highlights our concrete actions to drastically reduce cybercrime. Many EU countries are lacking the necessary tools to track down and fight online organized crime. All Member States should set up effective national cybercrime units that can benefit from the expertise and the support of the European Cybercrime Centre EC3."[50]
>
> **Cecilia Malmström, EU Commissioner for Home Affairs.**

This statement from an EU leader shows the importance that the European Union is placing on cyber security while working on a long-term plan that will include consideration of an EU-wide cyber security directive similar to the long-established and well-regarded EU Data Protection Directive.

EU measures that have been put into place on cyber security are not yet as well developed as those relating to the European Union's data privacy regulations embodied in the Data Protection Directive, which provides detailed rules on data protection that all member states must comply with. These rules include those of lawful processing, of security of processing, on transparency of processing, and on promoting compliance.[51] Though not specifically created for cyber security purposes, the Data Protection Directive is an example of a supranational regime that is among the most developed in the world certainly when it comes to data privacy protection as an important subset to cyber risk issues.

Data protection laws exist not only through the European Union's member states' laws but also in the Council of Europe's (CoE) data protection laws. The CoE specifies that security measures should be taken to protect against accidental and unauthorized destruction or loss of data.

Beyond data protection, per se, the European Union also has strict laws on cyber crime (not only on data but also on computer systems in general). These laws, decided upon at the Budapest Convention, forbid the following:

- Illegal access—obtaining access to a computer system without right, not necessarily with the intent of accessing data
- Illegal interception—intercepting the transmission of nonpublic data
- Data interference—damaging, deleting, altering, or suppressing data without right
- System interference—hindering the functioning of a computer system without right
- Misuse of devices—producing, selling, importing, or distributing a device or computer program that is to be used in committing the above offenses

The Budapest Convention also outlines laws on computer-related forgery, fraud, child pornography, and copyright infringement, among others.[52]

However, the European Union has a major cyber security strategy initiative under way, including passing a cyber security directive that is expected to be adopted shortly.[53]

CHINA

China has some of the most stringent cyber security measures of any nation or region, including the European Union. These regulations may seem unreasonable from a Western perspective as they can severely limit market access opportunities for international information and communication technology (ICT) firms and may create significant risks for related intellectual property. One industry perspective is that these stricter regulations, which came into place earlier this year and are often strategically vague, have been disingenuously placed under the rubric of national security (due to the Edward Snowden situation) but are actually thinly veiled protectionist measures designed to promote local businesses.[54]

A number of the new cyber security regulations apply mostly to the banking industry. Imposed by the China Banking Regulatory Commission (CBRC), these regulations require banks to strengthen their cyber security infrastructure. Specifically, by 2019, 75 percent of IT needs to be "secure and controllable," as defined by the CBRC. From 2015 to 2019, banks need to increase the use of "secure and controllable IT" by 15 percent annually, and they can allocate no less than 5 percent of their annual IT budgets to research and development of "secure and controllable IT."[55]

The purposefully vague phrase "secure and controllable"—which featured heavily in the July 1, 2015, promulgation of China's new National Security Law—is the focus of concern for many multinational corporations. The Chinese leadership has not clarified what makes information technology "secure and controllable," but in early drafts of the as-yet-unfinished Counter-terrorism Law (which will eventually buttress the National Security Law), legislators included the requirement that foreign ICT firms hand over source code, encryption keys, and other vital intellectual property, or that they install "back doors" specifically for Chinese authorities. If these regulations eventually emerge as such, they will effectively block many foreign ICT firms from participation in much of the Chinese market, given that many MNCs would not capitulate to those requirements.

The National Security Law also assigns regulators wide-ranging powers to "establish national security review and supervision institutions and mechanisms, and conduct national security reviews of key technologies and information technological products and services that influence or are likely to influence national security."[56]

And cyber security initiatives have not been limited solely to finance—they have now become a focal point in China's government. Political leadership has made the State Council Information Office the head of China's cyber security initiatives. Ultimately, the government's policies read as a combination of promoting local business and protecting genuine national security interests. Because foreign software potentially threatens national security, domestic businesses, state-owned enterprises, and government ministries are encouraged—and increasingly required—to use domestic software, even if it is lower quality.[57] Technocratic pushback on the quality issue from local managers concerned about their ability to function with substandard ICT infrastructure seems to have been mostly suppressed by the national security establishment.

Most of China's cyber crime laws are present in articles 285, 286, and 287 of the Chinese Penal Code. Article 285 states that it is illegal to intrude "into computer systems with information concerning state affairs, construction of defense facilities, and sophisticated science and technology." Article 286 is broader and states "whoever violates state regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences" will be imprisoned. It continues in saying the interference of data transmission and the creation and distribution of computer viruses is illegal. Article 287 focuses on using computers for financial crimes.[58] There are some other laws, but the five main cyber crimes are: illegal accessing, illegal data retrieval, illegal controlling of computer systems, providing tools for illegal accessing or controlling, and sabotaging computer systems.[59]

LATIN AMERICA

Latin American nations, especially those at the forefront of economic growth and financial services within the hemisphere (Colombia, Brazil, Mexico), have recently developed much greater cyber security awareness and, in some cases (e.g., Colombia), laws or public national policies that specifically address cyber security issues in highly targeted industries such as the banking sector and the government and critical infrastructure sectors.

An extensive report made in June 2014 by the Organization of American States (OAS) and Symantec, together with several leading companies and other regional organizations, provides an overview of the state of cyber security legislation in 30 of the 32 countries that constitute Latin America and the Caribbean.[60] The most comprehensive overview so far of this topic in this region, the 2014 OAS/Symantec report shows that only a few countries even have a law or national public policy on cyber security, although all of them seem to have in greater or lesser measure federal or national agencies dedicated or at least mobilized to understand and crisis manage cyber security events affecting the nation or major parts of the nation such as the financial sector, for example.

The OAS/Symantec report also distinguishes several clear trends in Latin America with respect to cyber security:[61]

- **Manufacturing is the most targeted industry.** Of the top 10 industries targeted in 2013, manufacturing, construction, and professional services topped the list by far.
- **Data breaches are on the rise.** Dubbed "The Year of the Mega Breach," 2013 saw over 552 million identities exposed by data breaches. At risk were the typical types of private data contained in credit cards, financial, medical, and other forms of personal information.
- **Targeted attacks continue to grow.** The report states that "Attacks against specific individuals or organizations are evolving, with cybercriminals adapting spear-phishing campaigns to be stealthier and adding watering-hole attacks to their toolkits."
- **Social media scams are on the rise.** In 2013, cyber criminals continued to mine social media as a rich source of data.
- **Banking Trojans and heists increase.** The report states that "across Latin America and the Caribbean, the number of incidents involving banking Trojans has increased significantly. Initially discovered in Mexico, malware targeting ATMs has spread to other countries through-out the Americas."
- **Major events provide rich targets.** The World Cup in Brazil became a major target for cyber criminals who have engaged in "countless malware operations, phishing schemes, and email scams related to the tournament." The fact that Brazil will be hosting the 2016 Olympics will certainly not lower the allure of the region to cyber criminals.

The Downside: Five Cases of Cyber Risk Management Gone Wrong

Target

In December 2013, Target disclosed that it had been the victim of one of the largest security breaches to date, affecting over 100 million people. Some of these individuals had their credit card information stolen, some had their personal information stolen, and approximately 12 million people had both stolen.[62] The breach was of such magnitude that it created a 46 percent drop in profits for that quarter compared to the year prior, and it ended with the resignation of CEO and Chairman Gregg Steinhafel approximately six months later.[63]

Russian hackers were said to be behind this breach.[64] They worked their way into Target's corporate network by compromising a third-party vendor. Through this vendor, the hackers were eventually able to gain control of Target's servers and point-of-sale systems, from which they were able to grab all the credit card information easily.[65]

By February 2014, the costs associated with the breach had risen above $200 million. The company laid off about 500 employees and left another 700 positions unfilled. Employee morale was also at an all-time low, and Target had to devise new ways to improve it, including allowing employees to wear jeans and polos to get them motivated again.[66]

In an effort to prevent a similar breach from happening again, Target has spent approximately $100 million in upgrading its payment system to support chip-and-PIN enabled cards. Had this been enabled prior to the breach, no customer card information could have been stolen. From the card information stolen, the hackers were able to make about $54 million.[67]

With a breach of this magnitude, there are several cyber security lessons to be learned. For any company, network segmentation—the breaking up of a network into many separate parts—is a must. Had Target's networks been segmented, the hackers could not have gotten such easy access to the company's POS systems by going through a third-party vendor. And Target already knew that it had cyber weaknesses; in fact, its own cyber detection tool had discovered these concerns, but they were not properly reported and elevated.[68]

Many banks lost money in the canceling and reissuing of cards after the breach, and part of their mandate has to be ensuring that their third-party vendors are using secure systems.[69] Since this incident, the credit card industry seems to have learned some important lessons and introduced new cyber defensive measures, most recently in the form of chip technology embedded in newly issued cards.[70]

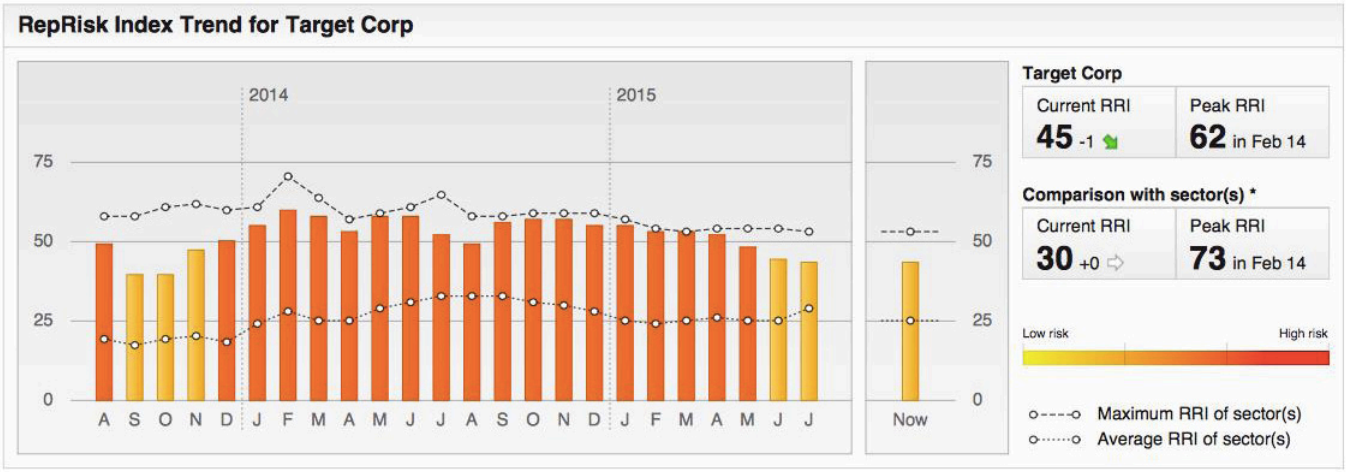
Target's board throughout this process went through a learning curve that has prompted other boards and the governance industry as a whole to wake up and maybe even overdo it a little on learning about and preparing for a potential cyber crisis. Important governance takeaways from this case are that boards and company management need to be vigilant in advance, pay attention to their IT and audit departments, and adapt their approach to cyber risk to their industry and potential exposure. At Target, the board took steps to minimize the likelihood of further breaches, including replacing its CEO and hiring new top talent to manage cyber security.[71]

REPUTATION RISK ASSOCIATED WITH CYBER RISK

From the database of RepRisk ESG Business Intelligence, the RepRisk Index (RRI) of Target shows a "Peak RRI" of 62 in February 2014 (which, out of a possible maximum score of 100, is considered to be a "high risk" exposure). The company's RRI, notably, continued to be high for the rest of the year into the first half of 2015.

Figure 5

Reputation risk analysis for Target, 2014-2015



Note: RepRisk monitors environmental, social, and governance (ESG) issues in relation to various entities, updated daily by highly trained analysts, and conducts searches for negative stakeholder sentiment in 15 languages across thousands of sources. The RepRisk Index (RRI) is RepRisk's proprietary algorithm that dynamically quantifies reputational risk exposure related to ESG issues. The RRI does not measure a company's overall reputation, but rather is an indicator of the company's reputational risk. The RRI ranges from 0 to 100, with 0 to 25 indicating low risk exposure, 25 to 50 indicating medium risk exposure, 50 to 75 indicating high risk exposure, and 75 to 100 indicating very high risk exposure. The "Peak RRI" signifies the highest level of criticism in the last two years. For more on RepRisk's methodology, please visit: http://www.reprisk.com/methodology/.

Source: RepRisk AG

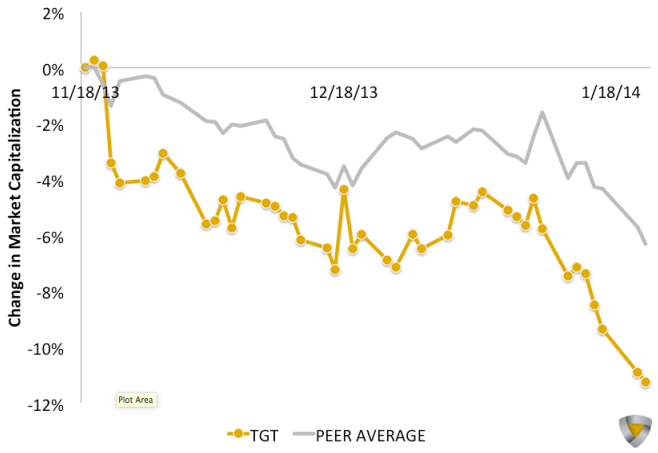
FINANCIAL PERFORMANCE RISK ASSOCIATED WITH CYBER RISK

Figure 6 shows the change in market capitalization of Target, starting one month before the cyber event was disclosed and ending one month afterward, relative to a group of peer companies listed in Table 2. Based on market data analyzed by Steel City Re following standard reputation risk analysis methods, there is an immediate impact of the cyber incident publicly disclosed on December 18, 2013, with a period of underperformance of around 5 percent relative to the average of the peer companies (Table 3, page 33).

Notwithstanding the cyber incident—or other reasons in conjunction with or separate from it—it appears that strong reputation value built into Target over a period of years provided it with some resilience. The Target stock outperformed its peers by 10 percent over the next year through January 2015, for a net gain of 3.64 percent (Table 3, page 33) or around $1.45 billion (Table 4, page 33).

Figure 6

Market capitalization analysis for Target



Note: Steel City Re is a provider of quantitative solutions for corporate reputation value. For Target, 5 peer companies were identified from compilations generated by Google Finance and Factset. For determining the short-term enterprise effect, stock price returns were measured over a window beginning 4 weeks before the public announcement of the cyber event and continuing 4 weeks beyond the announcement.

Source: Steel City Re

Table 2

Dates and peer groups used for market capitalization data

	Public notice of event	4 weeks prior	14-month window	Peers
Target	12/18/13	11/18/13	01/18/15	Costco, Walmart, Dollar General, Dollar Tree, Family Dollar Stores
JP Morgan	10/02/14	09/02/14	11/02/15	Wells Fargo, Citigroup, Goldman Sachs, PNC Financial Services, American Express
Sony	11/24/14	10/24/14	12/24/15	Canon, Panasonic, Toshiba, Harman International Industries, Whirlpool
Anthem	02/24/15	01/24/15	03/24/16	UnitedHealth Group, Cigna, Aetna, Humana, Health Net, Molina Healthcare

Source: Steel City Re

JP Morgan Chase

In October 2014, JP Morgan Chase announced that Russian hackers had successfully breached its systems and retrieved information on 76 million households and 7 million small businesses. The attack was first identified in July, but only publicly announced months later.[72] Slightly fewer than a dozen other financial institutions were also targeted, though almost all these attacks failed.[73] Though JP Morgan Chase has not disclosed the cost the breach represented for the company, its security budget increased thereafter by $250 million annually.[74] In August 2015, CEO and Chairman of the Board Jamie Dimon announced that the bank's cyber security budget would double over the next couple of years to $500 million a year.[75]

The hackers perused JP Morgan's computer system for several weeks undetected and successfully obtained identification information on the customers, but they failed in getting more sensitive financial information. The cyber attackers may have been acting as part of a complicated international effort by five individuals who may or may not be connected to any governments.[76] It is not clear whether the purpose of the attack was purely financial, political, or both. It may have been an effort to signal to the United States that Russia can penetrate the systems of even the largest and most secure financial institutions.

Others think these actions may have been in retaliation for the sanctions placed on Russia due to the Ukraine conflict, although the latest information also raises the possibility of purely financial motivation.

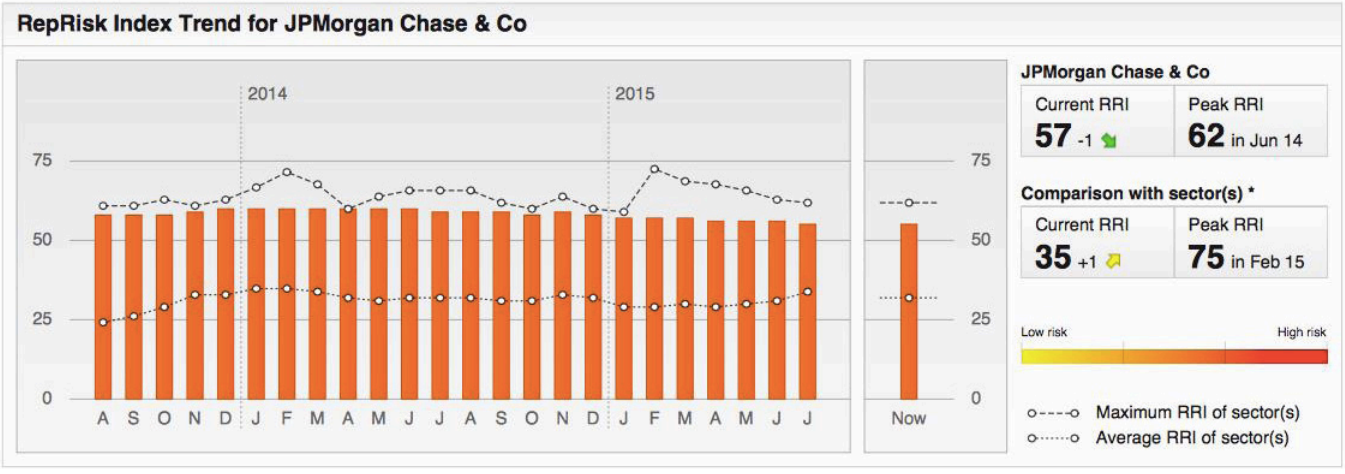
A key lesson in this case is that even well-prepared companies are susceptible to security breaches, and they must always be vigilant. In this case, the hackers were able to stay in JP Morgan's system entirely under the radar. Another lesson is that security software cannot be limited to defenses against commonplace attacks. The hackers were successful in this instance because they deeply analyzed JP Morgan's system and created malware specifically to get through the company's security. More specialized security mechanisms are needed to provide a strong defense against serious attackers.[77]

REPUTATION RISK ASSOCIATED WITH CYBER RISK

The RepRisk Index for JP Morgan shows a "Peak RRI" of 62 in June 2014 (before the cyber incident was publicly disclosed in October 2014). The numerous other legal, litigation, and government settlement issues that JP Morgan was dealing with at the time would explain this peak before the cyber incident was publicly disclosed. The bank's current RRI is 57, a relatively high score that has nevertheless remained steady for the past year.

Figure 7

Reputation risk analysis of JP Morgan, 2014-2015



Note: The RRI ranges from 0 to 100, with 0 to 25 indicating low risk exposure, 25 to 50 indicating medium risk exposure, 50 to 75 indicating high risk exposure, and 75 to 100 indicating very high risk exposure. The "Peak RRI" signifies the highest level of criticism in the last two years. For more on RepRisk's methodology, please visit: http://www.reprisk.com/methodology/.

Source: RepRisk AG

FINANCIAL PERFORMANCE RISK ASSOCIATED WITH CYBER RISK

As a powerful chairman of the board and CEO of JP Morgan, Dimon appeared to have control over the public relations on this matter which, as tracked in reputation risk and financial impact terms, did not seem to negatively affect either the financial or reputational profile of JP Morgan materially or significantly.

This may be partly explained because of the banking sector's already relatively low reputation with stakeholders as a consequence of many years of bad news, litigation, and fines. Thus, the additional impact of the cyber incident was not significant.

Figure 8 shows only a minor immediate impact of the cyber incident publicly disclosed on October 2, 2014. At less than 1 percent, it is not significant and didn't deviate substantially at that time from the peer financial companies (Table 3, page 33).

What this seems to indicate is that the cyber event, while mildly impactful, did not have a material or lasting effect on the financial condition or performance of JP Morgan's stock relative to its peers used in this case. Again, because the bank had established a reputation for cyber security that was evidenced by substantial investments in security (it described itself as a technology company that accepted deposits) and it handled the cyber crisis relatively well, it is possible to suggest that the cyber incident itself did not have a major impact on either the financial viability or reputation risk profile of JP Morgan. Subsequent to disclosure of the breach, JP Morgan outperformed its peers by about 9.5 percent (Table 3, page 33), adding an excess of $15 billion to its market capitalization (Table 4, page 33).

Figure 8

Market capitalization analysis for JP Morgan

Note: For JP Morgan, 5 peer companies were identified from compilations generated by Google Finance and Factset. For determining the short-term enterprise effect, stock price returns were measured over a window beginning 4 weeks before the public announcement of the cyber event and continuing 4 weeks beyond the announcement.

Source: Steel City Re

Anthem

On February 24, 2015, Anthem Inc. announced a data breach involving data on 80 million former and current customers and employees. In the breach, no medical information was compromised, though the hackers obtained personal identification information, from Social Security numbers and birth dates to contact information and employment data.[78]

The breach is expected to cost Anthem well over $100 million, which is how much it has in cyber insurance coverage. This cost covers informing its consumers and providing complimentary credit monitoring and identity-theft services; further unforeseen costs will ramp up the total bill even higher.[79]

The breach is believed to have happened anywhere from one to eight months prior to Anthem's announcement. While no perpetrator has been confirmed, industry analysts speculate that it may be the Chinese cyber espionage group Deep Panda, which may or may not be affiliated with the Chinese government. This hypothesis rests on how the breach was conducted—what is known as an Adobe Flash zero-day exploit. While personal identification information is typically stolen for use in financial fraud or identity theft, Deep Panda is not associated with such acts, so the theory is that the data were stolen either to be sold or to be used by the Chinese government.[80]

Among the takeaways from this breach is that companies, be they in the health care industry or another industry, should encrypt personal data to limit the damage of an attack and thus limit damages faced in court, even if, like Anthem, they are not legally obliged to do so.[81]

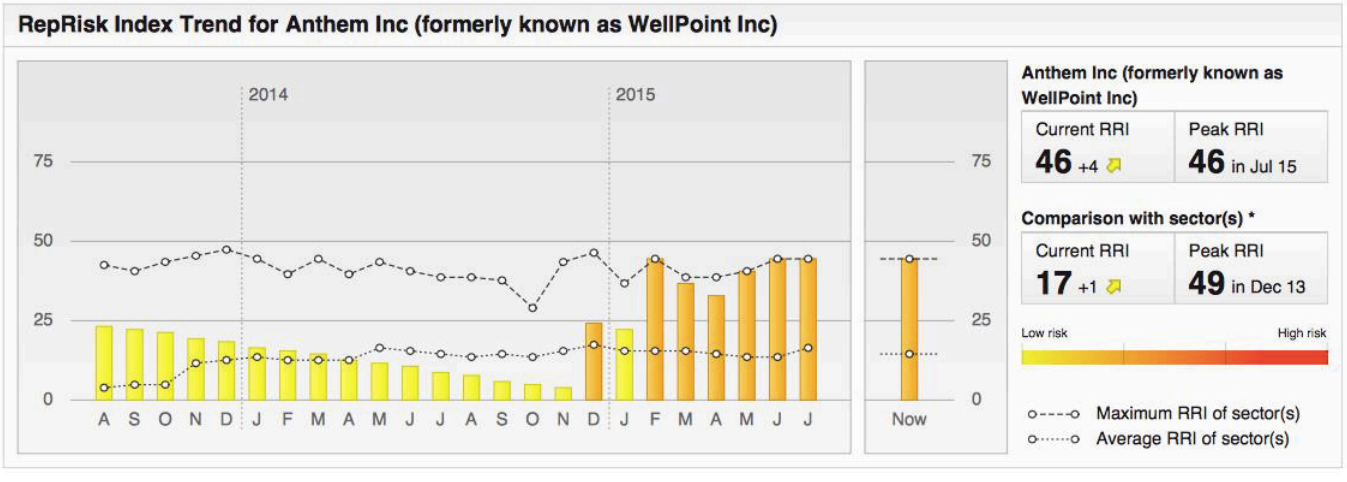
Companies also need to closely monitor anomalies in their systems, as this can be immensely helpful in preventing attacks. In health care specifically, companies should ensure their security measures are more stringent than merely adequate, as the information used in health care is of great use to identity thieves, so the industry faces more threats than some others.[82] Boards of health care organizations and others, like banks, that have vast troves of personal data must be proactive in ensuring that management has the right governance, tools, and people in place to protect such assets.

REPUTATION RISK ASSOCIATED WITH CYBER RISK

The RRI for Anthem shows a "Peak RRI" of 46 (out of 100, considered a "medium risk" exposure) in February 2015, right after the incident was publicly disclosed and lasting at least through September 2015. Though not considered a high risk exposure within the RRI, Anthem's risk exposure prior to the incident was consistently low (at under 25). Even more telling, as compared to its peer group at an RRI of 17 (low risk exposure), its current (and peak) RRI of 46 is relatively high.

Figure 9

Reputation risk analysis of Anthem, 2014-2015



Note: The RRI ranges from 0 to 100, with 0 to 25 indicating low risk exposure, 25 to 50 indicating medium risk exposure, 50 to 75 indicating high risk exposure, and 75 to 100 indicating very high risk exposure. The "Peak RRI" signifies the highest level of criticism in the last two years. For more on RepRisk's methodology, please visit: http://www.reprisk.com/methodology/.

Source: RepRisk AG

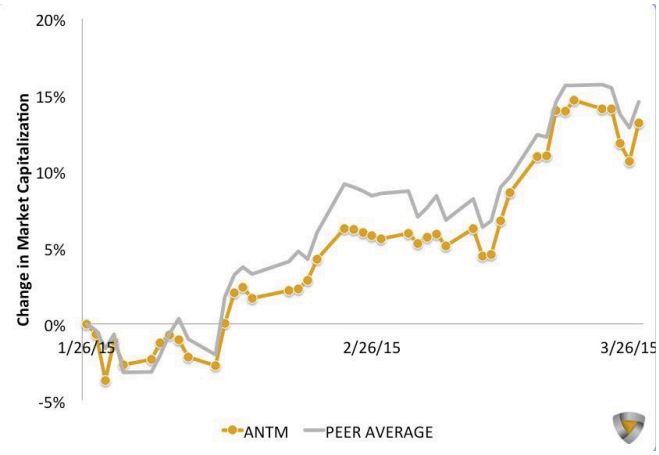
FINANCIAL PERFORMANCE RISK ASSOCIATED WITH CYBER RISK

The qualitative and quantitative consequences of this event to the financial and reputational well-being of the company—and its stakeholders—are several and continue to unfold given that this case is relatively recent.

Figure 10 shows a low immediate impact of the cyber incident publicly disclosed in February 2015 as compared to the overall trend line of peer companies. The period of underperformance was only around 1.4 percent. However, Anthem management had been forewarned of its cyber exposures, and Anthem's electronic health records are governed by protection requirements under the Health Insurance Portability and Accountability Act of 1996. Expectations among health care insurance stakeholders are higher, or put a little differently, because of the highly regulated nature of the health care insurance industry and the increasing number of incidents, stakeholders have higher expectations than ever. In the months subsequent to the breach, Anthem's equity value continued to underperform relative to peers, ultimately underperforming by 11.5 percent, depriving shareholders of an estimated $4 billion (Table 4, page 33).

Figure 10

Market capitalization analysis for Anthem



Note: For Anthem, 6 peer companies were identified from compilations generated by Google Finance and Factset. For determining the short-term enterprise effect, stock price returns were measured over a window beginning 4 weeks before the public announcement of the cyber event and continuing 4 weeks beyond the announcement.

Source: Steel City Re

Sony

On November 24, 2014, hackers released a massive amount of Sony Pictures Entertainment's (SPE) confidential data as the result of a major malware attack that likely started a year before. Among the data was the personal identification information of past and present employees. This included employees' names, addresses, government identification (passport, license, Social Security, etc.) information, bank account and credit card information, usernames, passwords, compensation, and other employment information.[83] Beyond this, private emails and electronic files owned by SPE were also released. Though this attack was against a multinational company, the US government also became visibly involved in this case partly due to purported national security reasons.[84]

The perpetrators of the hack were a group called Guardians of Peace (GOP). GOP members first stated that they conducted the breach because of the imminent release of SPE's film, "The Interview." The motive later seemed to include monetary compensation.[85] It is not clear who is behind GOP. Because "The Interview" concerns the death of North Korean leader Kim Jong-un, many, including the US government, claimed the hack was the work of North Korea. Other theories include a frustrated former or current employee, hacking groups such as Anonymous (which often conducts such breaches for pure enjoyment), or other cyber criminals.[86]

Many lessons can be learned from this attack. SPE officials had previously made clear that they opted not to invest heavily in cyber security, as they believed the cost was not worth the "minuscule" risk of a breach. In fact, with an information security team of only 11 people at the time of the hack, Sony barely invested in cyber security at all. However, some assess the current cost estimate to Sony for this incident in the $100 million range. As such, one major lesson is that cyber security is worth the investment, even if chances of an attack seem minute.[87] It also bears mentioning that while this case became notorious, SPE is only a small part of a much larger publically traded corporation, Sony, and as such would not necessarily or easily have a material effect on its parent.

Other lessons are not related directly to cyber security but rather the implications of an attack. The senior executives and board of Sony became visibly involved in the drama surrounding this case as it became fodder for the media and social media given the somewhat gossipy and salacious nature of the high-level executive emails that were revealed, leading up to the resignation of SPE Co-chair Amy Pascal, who was the author of many of these emails, including some considered to be racially insensitive or racist regarding President Obama.[88] Since this episode, Sony has disclosed greater investments in cyber security.

REPUTATION RISK ASSOCIATED WITH CYBER RISK

The RRI for each of Sony and SPE shows a "Peak RRI" of 63 and 71, respectively (out of 100, considered a "high-risk" exposure) in January 2015, soon after the initial cyber incident was disclosed in November 2014. Both RRIs have decreased substantially since then to stabilize in the range of the company's peers in the high 20s and low 30s.

Figure 11

Reputation risk analysis of Sony Corp, 2014-2015

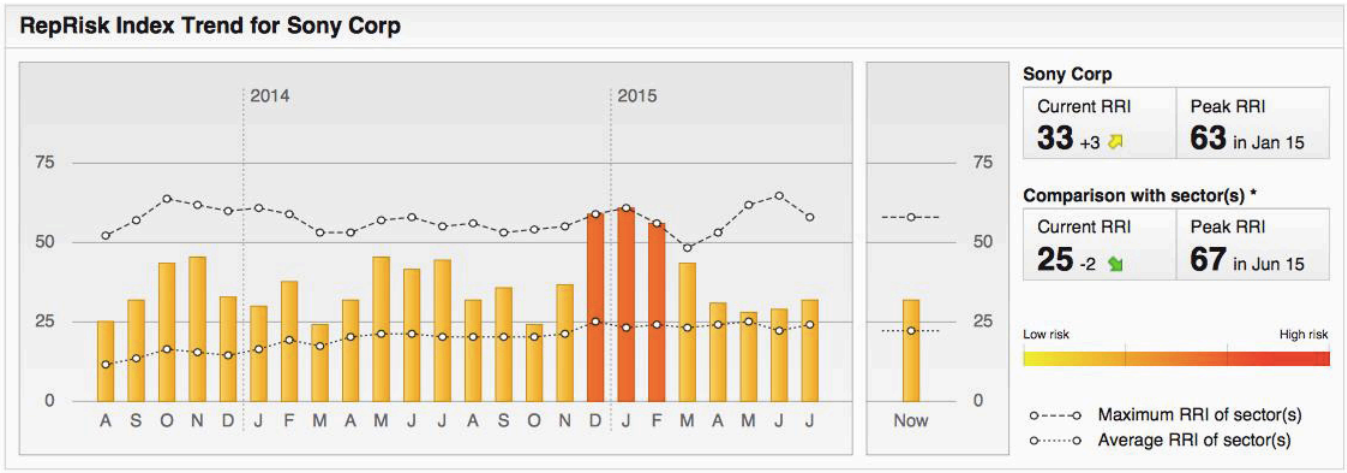
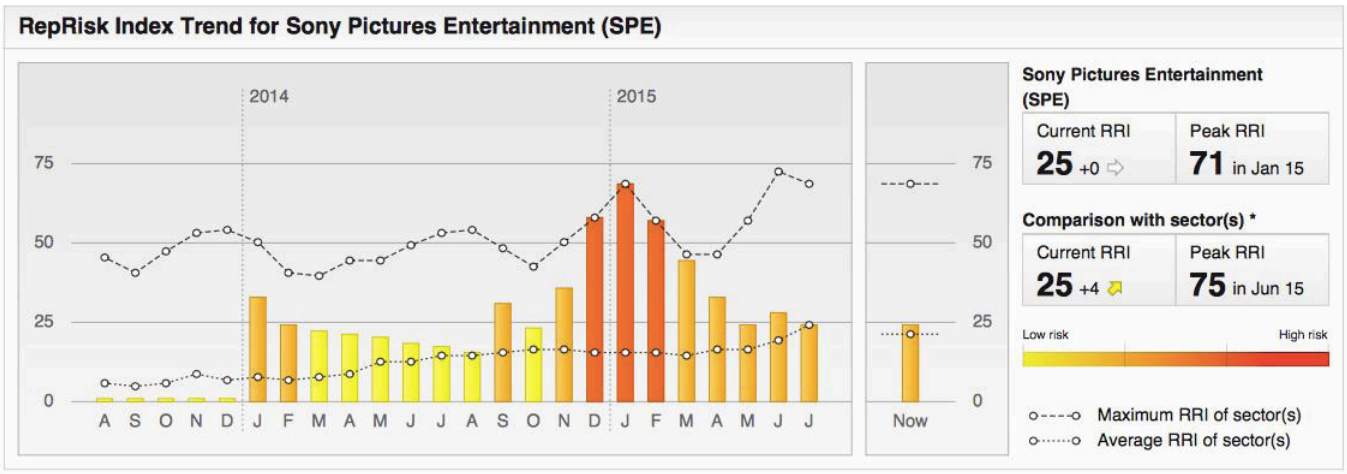


Figure 12

Reputation risk analysis of Sony Pictures Entertainment, 2014-2015



Note: The RRI ranges from 0 to 100, with 0 to 25 indicating low risk exposure, 25 to 50 indicating medium risk exposure, 50 to 75 indicating high risk exposure, and 75 to 100 indicating very high risk exposure. The "Peak RRI" signifies the highest level of criticism in the last two years. For more on RepRisk's methodology, please visit: http://www.reprisk.com/methodology/.

Source: RepRisk AG

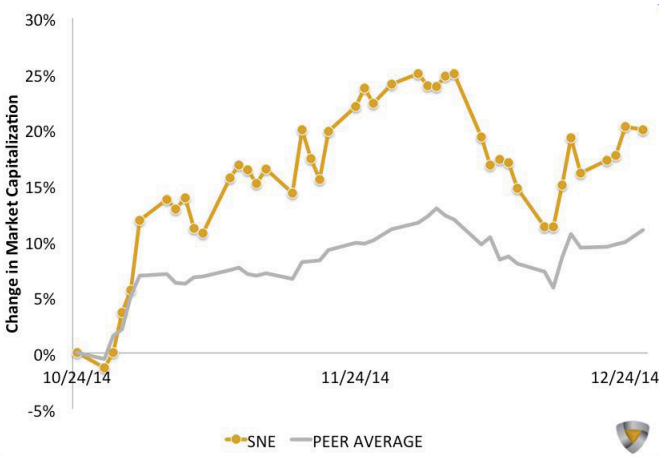
FINANCIAL PERFORMANCE RISK ASSOCIATED WITH CYBER RISK

The market capitalization chart (Figure 13) for Sony Corp, the parent company where the financial impact of reputation risk is likely to concentrate (as SPE is not a publicly traded entity), the immediate impact of the cyber incident publicly disclosed in November 2014 does not seem to be significant, certainly in comparison to its peer group of companies. SPE is only a small portion of a much larger diversified global company, and thus the financial implications of the cyber event at one unit would not necessarily have a major impact on the financial performance of the larger entity.

Whereas stakeholders likely held Anthem's management culpable, they likely excused Sony's management due to the extenuating circumstances: that a nation-state actor was the alleged perpetrator of the crime and that SPE is not a health care insurance company with heightened legal data privacy obligations. Indeed, compared to its peers, Sony appears to have a better-than-average performance in the marketplace, outperforming its peers by 62 percent and adding an excess of $12 billion to the company's market capitalization (see Tables 3 and 4 on page 33).

Figure 13

Market capitalization analysis for Sony Corp



Note: For Sony, 5 peer companies were identified from compilations generated by Google Finance and Factset. For determining the short-term enterprise effect, stock price returns were measured over a window beginning 4 weeks before the public announcement of the cyber event and continuing 4 weeks beyond the announcement.

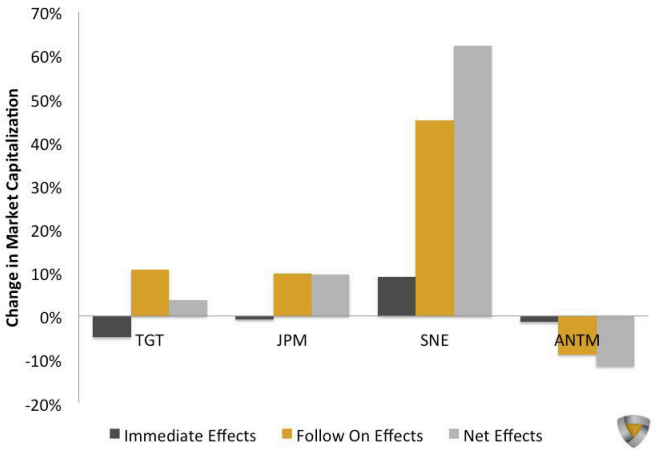
Source: Steel City Re

Summary of Financial Implications

Tables 3 and 4 and Figure 14 provide a summary overview of financial data regarding the four publicly traded companies examined that have suffered cyber attacks in the past two years. Building reputation resilience over the years yields material dividends, as evidenced by Target's and JP Morgan's relative recoveries and net gains relative to peers, notwithstanding the attacks. Failing to do so or inviting allegations of culpability by not addressing risk, as evidenced by Anthem's relative underperformance, appears to destroy value. Major media events, even when they involve major media companies, are not necessarily adverse reputation events, as evidenced by Sony's equity performance relative to its peers.

Figure 14

Change in market capitalization for four publicly traded companies: immediate, follow on, and net effects



Note: For determining the follow on enterprise effects, stock price returns were measured from 4 weeks beyond the announcement to the sooner of the present or to 12 months beyond. For determining net effects, stock price returns were measured beginning 4 weeks before the announcement to the present or 14 months from the start if possible. The gain or loss for the index company was determined relative to the average performance of the peer group over the comparable period.

Source: Steel City Re

Table 3

Equity performance (in percentage) **of four publicly traded companies with cyber security events**

Equity performance effect relative to peers (%)

	Immediate effects	Follow on effects	Net effects
Target	-4.92%	10.67%	3.64%
JP Morgan	-0.80	9.80	9.50
Sony	8.98	45.07	62.19
Anthem	-1.39	-8.84	-11.52

Table 4

Equity performance (in dollars) **of four publicly traded companies with cyber security events**

Equity performance effect relative to peers ($MM)

	Immediate effects	Follow on effects	Net effects
Target	($1,829)	$4,848	$1,450
JP Morgan	(1,920)	17,165	14,945
Sony	1,900	8,906	12,030
Anthem	(715)	(3,160)	(3,947)

Note: For determining the follow on enterprise effects, stock price returns were measured from 4 weeks beyond the announcement to the sooner of the present or to 12 months beyond. For determining net effects, stock price returns were measured beginning 4 weeks before the announcement to the present or 14 months from the start if possible. The gain or loss for the index company was determined relative to the average performance of the peer group over the comparable period.

Source: Steel City Re

US Office of Personnel Management

In early June 2015, the US Office of Personnel Management (OPM) announced that a cyber attack had occurred in which the personal data of millions of federal employees had been hacked. The government's latest reports on this incident state that not only were the records of 21.5 million current and former employees acquired by hackers, but so were the fingerprint records of 5.6 million of these individuals.[89]

The data breach apparently began in March 2014. In July, Katherine Archuleta, then the director of OPM, acknowledged that there had been an attempted breach; however, she denied that any personal identification information had been compromised. At that point, the attempted breach was thought to have been done by Chinese hackers, though this had not been confirmed.[90]

Among the data obtained in the breach are government employees' Social Security numbers, military records and veterans' status information, addresses, birth dates, job and pay history, health insurance, life insurance, and pension information, age, gender, race, and union status, as well as information on spouses and friends. Also obtained were the results of background checks for employees seeking security clearances. These results include more detailed personal information, including names of the applicants' friends, and make this breach not only a gross oversight and error but also an issue of national security.[91]

While many still insist that Chinese hackers, possibly government employees, conducted the hack, most US government officials have so far been hesitant to make any absolute claims. The Chinese have stated that they are not responsible, and even if they were, that the United States has been responsible for most cyber attacks on Chinese government websites.[92]

Though the US government deals with attempted hacks on a daily basis, this event is particularly notable because it succeeded on such a large scale.[93] According to audits of the OPM, it had significant security deficiencies since at least 2013 that made this breach significantly easier.[94]

An important lesson from this case for cyber risk governance is that while the intrusion was first detected because of computer upgrade work OPM was beginning to make and involved intrusion through another department (the US Department of the Interior's personnel department as a back door into OPM itself), it also involved compromised credentials of a third-party contractor. There did not appear to be a concerted approach to cyber risk management that included, specifically, acknowledging and acting upon issues identified in audits, rather than knowing issues existed and opting not to fix them. Of course, some of the issues endemic to the operations of the federal government may have also played a role in the low cyber risk defense capability of this department having to do with lack of appropriations.[95] What this shows, once again, is that the weakest link in the chain will open the door to a cyber savvy intruder with much greater ambitions.

Concluding Observations about the Downside Cases

These five downside cases provide a sample of what can happen under a variety of circumstances for different industries, sectors, and situations, from a diversity of perpetrators and attackers, for a host of different reasons. These cases illustrate what happens when:

- You are somewhat prepared and the consequences are not that dire (JP Morgan)
- Cyber risk is considered a low probability in your industry and you get a major cyber hit (Sony)
- Your third parties' access to company assets isn't protected properly, devastating your defenses (Target)
- You have Insufficient funds and your antiquated systems have not been upgraded in a long time, leading to the broadest breach ever of employee records including highly sensitive records (OPM)
- Intruders are interested in exposing salacious details about the internal workings of your company and publish damaging emails (Sony)
- You are in a very high-risk, regulated industry and don't take your sector's exposure seriously enough (Anthem)
- You had earlier knowledge of the issue but did not heed alarm bells (Target, Anthem, Sony, OPM)
- Attacks on your organization come from another or multiple other countries, to this day unclear whether for national security, criminal, or other reasons (Sony, JP Morgan, Anthem)

These are all cases that can provide valuable lessons to the critical role that proper cyber risk governance must play in any kind of entity, including the board, the CEO and C-suite, and the top functional leaders heading up cyber security and risk management. Indeed, a June 2015 Ponemon Institute survey of about 250 US board members indicates the serious impact that the cases examined here, among others, have had on boards of directors (and therefore, we can assume, the other two elements of the cyber risk governance triangle).

Table 5

The impact of known cyber breaches on board of directors' awareness

Significant and moderate responses combined

89%	Target data breach
72	Recent case involving Chinese spys operating within Pittsburgh area companies
68	JP Morgan Chase cyber attack
62	Insider threats and recent cases involving malicious employees
62	Home Depot data breach
40	Sony PlayStation data breach
36	Chatter about cyber terrorist attacks against critical infrastructure
32	TJX data breach
17	Veterans Administration data breach
11	Successful hack of the Healthcare.gov website

n=245

Source: "Defining the Gap: The Cybersecurity Governance Study," Ponemon Institute, June 2015 (http://www.fidelissecurity.com/bridgingthegap/Board_of_Directors_Cybersecurity_Governance.pdf).

Table 6

Reputation risk effects at the four companies examined

TARGET

Peak RRI Occurred at height of bad publicity and consequences of cyber breach becoming fully known.

Current RRI Has recovered over time slowly but still relatively high for its peer group of companies suggesting a longer-term reputational taint from this affair.

JP MORGAN CHASE

Peak RRI Occurred a couple of months prior to cyber breach being made public and potentially reflecting other bad publicity regarding multiple fines and litigation JP Morgan was dealing with at the time.

Current RRI Not much lower and still relatively high compared to peer companies, reflecting the fact that from a reputation risk standpoint JP Morgan continues to be very much in the crosshairs of regulators and the media.

SONY

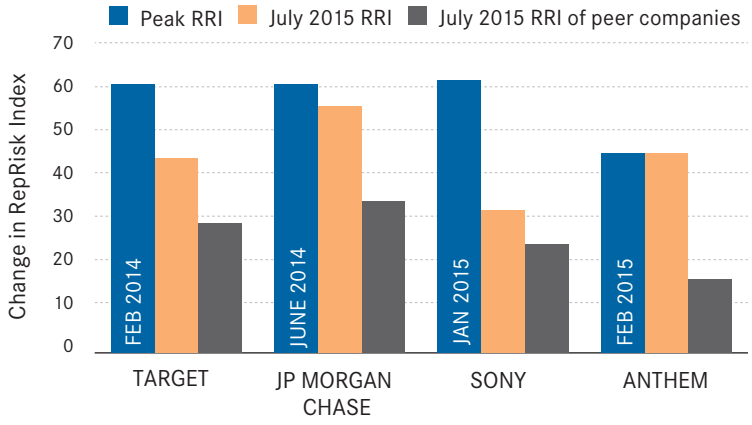
Peak RRI Occurred as the fuller implications of the Sony Pictures Entertainment cyber hack became known, including major salacious inside Hollywood details revealed by hacked emails.

Current RRI Has dropped to within the range of peer companies, reflecting the fact that the cyber hack did not have long-term negative reputation risk consequences on the company.

ANTHEM

Peak RRI Occurred immediately upon revelation of the cyber hack and has continued to this day.

Current RRI Continues through mid-2015, showing an ongoing high reputation risk impact and pressure on Anthem, with a very high RRI relative to its peer companies.



Note: The RepRisk Index (RRI) captures criticism and quantifies a company's or projects' exposure to controversial environmental, social, and governance issues. It does not measure overall reputation but rather is an indicator of reputational risk. The range is from 0 to 100, with 0 to 25 indicating low risk exposure, 25 to 50 indicating medium risk exposure, 50 to 75 indicating high risk exposure, and 75 to 100 indicating very high risk exposure. The "Peak RRI" signifies the highest level of criticism in the last two years. For more on this methodology, see: http://www.reprisk.com/methodology/.

Sources: RepRisk AG and The Conference Board

Reputation risk—a strategic risk just like cyber risk can often be—can only aggravate and amplify the financial and other risks unleashed by a major cyber incident. And boards are finally putting the two together and consider them the top two global risks today.[96]

These events are feeding into a much greater awareness overall, but specifically and finally in the boardroom and executive suite, with greater pressure on proper resources and budgets being allocated to a risk that is going nowhere but up in likelihood and impact. A 2014 Gartner summary of worldwide security spending from 2012 projected to 2016 demonstrates the increased pressure on budgets by industry sector, showing a change of $60 billion in 2012 to a projected $83.2 billion in 2016.[97]

The Upside: Five Companies Taking a Proactive Approach to Cyber Risk Governance

This section drills down into the heart of what five leading global companies in different sectors are doing today to meet, mitigate, and perhaps even get ahead of the constantly encroaching, mutating, and diversifying cyber risk threat.

Because of the nature of the threat—imminent, changeable, potentially devastating—we are not disclosing the identities of the companies profiled in this report. Like their peers, they are under siege from a host of cyber attackers. Their willingness to share the basics of how they are managing and developing their cyber risk governance is a tribute to the fact that many companies, for-profit and nonprofit organizations, and government agencies are engaging in unprecedented cooperation, sharing, and development of tools, techniques, and best practices to meet and defeat cyber risk.

The companies profiled range from a purely domestic, highly regulated, leading electric power utility to a global technology company with a presence in 100-plus countries. From sectors in which data privacy is king (health care and business process outsourcing (BPO)) to sectors where physical security is paramount (protection of the electric grid), these five companies provide a strong cross-section of leading and even best practices in cyber risk governance in the corporate world today.

This report's review of the cyber risk governance framework of each of these five leading companies zeroes in on the following questions:

- When and why did cyber risk governance begin at the company?
- Who owns cyber risk management?
- What is the role of the CEO and C-suite?
- What is the role of the board in cyber risk oversight today?
- What are important current and future cyber risk governance practices and opportunities?

Table 7

Summary overview of five companies' cyber risk governance frameworks

Company profiled	Industry	Key challenges	Keys to success	Future trend/opportunity
US-based Fortune 50 global technology company	Technology (software & hardware)	• The cloud • Protecting customers • Protecting executives • Staying ahead	• Hybrid centralized/ distributed approach • Conquering cloud security	• Integrated cross-disciplinary nimble teams • Evolving cloud security strategies and business opportunities
US-based Fortune 250 electric power utility	Utility	• Critical infrastructure protection • Big data usage of private data	• Constant crisis drills • Partnership with government agencies • Industry information sharing • Cross-functional team approach • Proactive interested experienced board	• Rolling and constant crisis management and readiness exercises • Public private partnership (information and actual crisis management)
European-based global Fortune 50 insurance company	Insurance/ financial	• Data privacy • Heavy & multiple regulatory regimes • Selling solutions requires internal perfection • Prime target financial crimes • Dual board structure might hamper oversight	• Finding solutions through own experience developing own cyber-readiness program	• Financial companies that provide cyber risk insurance need to find solutions for themselves to be credible in an increasingly competitive but confusing cyber risk insurance marketplace
US-based Fortune 50 global health care company	Health care	• Data privacy • Multiple regulatory regimes • Prime target identity crimes • Heavy acquisition spree and investment in high-risk environments (China)	• Developing integrated due diligence platform for aggressive acquisition strategy to include cyber risk review • Creating global platform for cyber risk readiness	• Combining and deploying NIST and ISO 27001 platforms to manage cyber risk • Moving information security into an integrated global security function & platform
US-based Fortune 250 global business outsourcing and computing services company	BPO & computing services	• Data privacy • Heavy & multiple regulatory regimes • Selling solutions requires internal perfection	• High data driven environment has forced first mover advantage in finding useful solutions	• Independent global security platform unbeholden to other businesses' P&L

Source: The Conference Board

US-Based Fortune 50 Global Technology Company

WHEN AND WHY CYBER RISK GOVERNANCE BEGAN AT THE COMPANY

The company began to formalize its enterprise risk management (ERM) program in 2005 and then created a cyber risk governance program in 2009. It is in an industry—global software and hardware—that is at the center of cyber issues, including cyber security considerations that occur daily around the world. This is a company that was sensitive to cyber issues even before we began to learn of the large-scale cyber attacks of 2011 and beyond.

When it formally adopted cyber risk governance in 2009, the company had a decentralized global business and functional structure, with a cyber risk governance program at global headquarters and a distributed or decentralized cyber risk governance program organized at each of its five fairly autonomous divisions. This structure, according to the executive interviewed for this case, represented a "loose coalition of the willing" where the divisions could but were not obligated to participate in the centralized program.

Partly reflecting an overall corporate restructuring and partly reflecting the recognized need for a more centralized—maybe even command-and-control—approach to cyber risk governance, the company restructured its cyber risk governance in 2014 to become a centralized program, driven from global headquarters.

Among the key drivers for this centralization were:

- An increasingly hostile cyber environment
- The increasing frequency and sophistication of cyber attacks
- The concerted movement to a cloud-based operating model and the fact that the cloud poses a new series of cyber risk threats and cyber security challenges
- A couple of specific incidents that exposed the potential for (or actual) vulnerabilities under the decentralized model
- The fact that cyber attacks are not just coming from individuals and criminal rings but from nation-states looking for more than financial proceeds of a crime, targeting executives and other high-profile individuals for potentially more nefarious reasons (blackmail, extortion, etc.)

WHO OWNS CYBER RISK MANAGEMENT

The company has created a truly cross-disciplinary approach to cyber risk management. The chief information security officer (CISO), the chief information officer (CIO), the head of cloud engineering, the head of ERM, and the head of internal audit all own a part of cyber risk management. A security function—including the information and the physical and executive protection unit of the company—also owns pieces of cyber risk management, including these priorities:

- Security of online services and the protection of customer data
- Ensuring device integrity
- Safeguarding the supply chain
- Security and protection of intellectual property

The company's fraud detection unit also has a role in cyber risk management, as does the data center operations team, through its monitoring and testing activities, which include penetration testing and threat vector analysis.

THE ROLE OF THE CEO AND C-SUITE

In 2014 and 2015, four critical developments took place at the executive level:

- **Monthly CEO risk reviews** This has created a real change of the tone at the top on risk issues, including opening previously closed doors
- **Senior leadership team (CEO direct report) acceptance of cyber security-related risk** Via appropriate escalation process, final acceptance of cyber security risk is now at the highest level of the company
- **Risk assessment quality improvements** To capture the highest priority risks across the company, whether divisional or enterprise wide
- **Funding** Ensuring that proper funding is never an obstacle to proper risk management of the highest priority risks

The CISO, CIO, EVP of cloud engineering, divisional security VPs, and the head of risk & audit provide the CEO with a monthly security review that includes a detailed review of the progress in mitigating the highest priority cyber security risks. For the past five years or so, the CISO had owned the discussion of these topics with the board, but now that the divisional and corporate security operations have merged into one global virtual team, the CIO, CISO, and EVP of cloud engineering are the trio that takes the lead in providing the CEO with these monthly briefings. Board discussions are led by the CISO, the CIO, and the head of risk & audit, with rotating security executives depending upon the topic.

Informally, the entire C-suite also becomes involved in hearing about and seeing the monthly CEO briefings. The role of IT, risk, and audit executives is to ensure that the cyber security issues map well to the cyber defense initiatives. The coordination of attendance at all the relevant preparatory meetings is critical to ensure this is happening.

Cyber risk is managed at the executive team level through the top 20 or so executives having full knowledge of and regular briefings on cyber risk issues, with the principal goal that the executive team is on the same page about the risk priorities that need to be mitigated.

THE ROLE OF THE BOARD IN CYBER RISK OVERSIGHT

In the new centralized model, the board plays a critical and proactive role in cyber risk governance and oversight. What began as an audit committee function has now morphed into two board committees (which sometimes meet jointly)—the audit committee and the regulatory and public policy committee—that proactively exercise joint oversight.

Additionally, the full board has adopted greater oversight responsibility than ever before, receiving until recently a biannual state of information security update, which is now morphing into a quarterly rhythm, complemented with bringing in the external perspective at formal board sessions as well as breakout sessions in the annual board retreat.

Moreover, the executives in charge of cyber risk management have taken the full board through an extensive cyber security review. Because of board turnover, this exercise has become even more important to keep all board members fully informed.

Board members recognize that there is an expanded personal liability dimension to this issue, which partly explains why cyber risk and security have now become the domain of the full board.

IMPORTANT CURRENT AND FUTURE CYBER RISK GOVERNANCE PRACTICES AND OPPORTUNITIES

Because of the nature of its business, the company sees a large opportunity for creating a cyber security competitive advantage in its products and services. This has served as an additional driver of board and executive attention, especially with cloud-based services, including cyber security solutions and services and products that are now generally being delivered through the internet as opposed to shrink-wrapped boxed products. Through robust risk management practices and predictable and repeatable operational security hygiene programs, the company feels it can meet the objectives set forth in its core security priorities.

US-Based Fortune 250 Electric Power Utility

WHEN AND WHY CYBER RISK GOVERNANCE BEGAN AT THE COMPANY

This company has had a formal cyber risk governance program in place for the past two to three years. The program was formalized once its executives and leadership realized that cyber risk was only becoming more severe given its critical physical infrastructure, which is susceptible to a cyber attack with potentially devastating consequences.

Additionally, federal, state, and local governments have become much more interested in and collaborative with companies like utilities that have critical infrastructure; a number of important public-private initiatives are under way, including utility and federal government working groups on cyber risk and security issues (see discussion of NIST framework, pages 18-19).

Not only are a utility's physical facilities susceptible to cyber attack, but it also holds and uses a broad swath of its customers' personal data. And, in this age of big data analytics, additional serious privacy concerns go beyond the traditional ones of holding personally identifiable information like addresses, phone numbers, and email addresses to being able to track, slice, and dice information on customer behaviors. This is especially so with the dawn of IoT, which increasingly allows those holding data retrieved from multiple IoT devices to perform a variety and breadth of previously unheard-of behavioral analyses.

WHO OWNS CYBER RISK MANAGEMENT

The company's cyber risk management was originally led by what it calls its "information resources" team, which most companies refer to as information security.

As the program became more formal in the past two to three years, a larger cross-functional senior steering committee was formed to include operations executives, customer relations executives, service executives, and legal and corporate security, which includes two separate but coordinated groups—one that handles physical security and the other that handles cyber security.

The ERM function also plays a role in managing this risk as part of the ongoing ERM program run by the chief risk officer (CRO), who reports to the chief financial officer (CFO).

The cyber risk team engages in regular crisis management planning to include a variety of possible scenarios. Crisis management includes a cyber risk plan—dealing with this risk as with any other emergency response plan—that the board is regularly briefed on.

THE ROLE OF THE CEO AND C-SUITE

The CEO is also chairman of the board, thus providing, at least theoretically, a very close and direct line from the C-suite to the board on all things cyber risk.

The executive team has its own cyber security steering committee that meets regularly and includes the senior vice president (SVP) of shared services, to whom the VP of information resources reports. Within the executive team, the SVP for shared services is the lead executive on cyber issues.

The remainder of the executive team includes the business heads for each division of the utility, who are present and engaged in all presentations and updates made by the SVP shared services on cyber issues and developments.

THE ROLE OF THE BOARD IN CYBER RISK OVERSIGHT

The board is highly engaged and informed on this issue on a regular basis. A number of board members have actual operational utility experience, so they are very familiar with the details of running a utility and therefore with the growing concern about and need to oversee cyber risk and cyber security within the utility space.

This highly engaged board wants to know about any significant event, not just a cyber one. Because the CEO is also the chairman of the board, connecting back to the board on any risk is direct and immediate. The CEO and chairman makes the determination on whether the full board has a need to know.

Cyber risk is considered one of the most significant enterprise risks; thus, unless there is an intervening serious event, every two to three quarterly board meetings, there is a full review of cyber and physical security issues.

IMPORTANT CURRENT AND FUTURE CYBER RISK GOVERNANCE PRACTICES AND OPPORTUNITIES

The company has a living, breathing crisis response plan in place that is adaptable to changing circumstances, is reviewed regularly, and provides for periodic drills as well as:

- Drills for all kinds of risks
- Keeping in touch with a variety of public and private entities that can provide information at a time of crisis
- Interfacing with the government

This utility is also looking at personally identifiable information housed in the company databases—from medical and Social Security numbers to driver's license information (from 10,000-plus employees) and asking important questions like:

- Where is the information being collected from?
- Do we need to collect this information?
- If we don't need the information, why not stop collecting it?

Specifically, the team consists of people from information resources, legal, and customer operations, all of whom are presently looking at this area of private data collection and proactively trying to understand the parameters and uses. The company knows a lot about its customers' use of power, but what parameters need to be placed around using big data about customers—what privacy issues, societal-good issues, or other issues exist? For example, collecting gross customer electric use information may be very helpful to managing climate change issues and improving the green performance of buildings or communities.

Europe-Based Global Fortune 50 Insurance and Financial Company

WHEN AND WHY CYBER RISK GOVERNANCE BEGAN AT THE COMPANY

At this company, the first formal cyber risk/cyber security program was put in place in 2003 as the result of a merger with a banking institution that already had stricter cyber security measures in place. Another reason for the formalization of the program was triggered by the contemporaneous results of an audit.

WHO OWNS CYBER RISK MANAGEMENT

The chief operating officer (COO) owns cyber risk and cyber security. Lead executives with direct daily responsibility for cyber risk and security are the CIO, who reports to the COO, and the information technology security officer (ITSO), who reports to the CIO and is the sole owner of information security globally.

Though there is no cross-functional team dedicated to cyber risk management, members of senior management from operations, information technology, risk management, or human resources become involved with specific cyber issues as warranted. More specifically, there is a close and continuous collaboration between the offices of the CIO and ITSO, on the one hand, and the ERM function, on the other hand, supported by structured processes such as top risk assessment and operational risk assessment programs.

THE ROLE OF THE CEO AND C-SUITE

The CIO and ITSO issue a quarterly information security report, which is discussed with the COO and includes current challenges, mitigation measures, and funding status and requirements.

Because it is based in Europe, the company is structured to include an executive board made up of sitting management and a supervisory board made up entirely of outside directors. Thus, information security risks are also presented to the executive board-level risk committee as part of the quarterly risk report. There is no dedicated information security committee to exercise oversight. The ITSO brings ad hoc matters to the COO via the CIO.

Information security is not only related to IT but to business information more broadly. Awareness campaigns are conducted across functions involving all employees. Awareness and processes play an important part of the information security efforts (i.e., they are not purely focused on technical solutions).

Among some of the reasons for heightened awareness of cyber risk within the company are the fact that digitalization (e.g., bring your own device, the cloud, etc.) attacks are getting more complex and the company's realization that it needs to be ahead of or at least up to date with what the hacker community is developing.

Formal plans are in place for business continuity management and disaster recovery, including the possibility of an information security-driven crisis scenario-planning exercise. However, there are no dedicated information security crisis plans in place as of now. One of this company's business lines is to provide client companies with cyber risk insurance coverage.

THE ROLE OF THE BOARD IN CYBER RISK OVERSIGHT

Because this is a Europe-based company with a dual board reporting line, dual reports go to the executive board and supervisory board on a regular basis.

Executive Board The CIO and ITSO have quarterly meetings and information sessions with the risk committee of the executive board of the company. In the event of a cyber crisis, an impromptu discussion is scheduled as well.

Supervisory Board There is no risk committee at the supervisory board level of the company. However, risk management topics—namely, the top risks within the ERM process that make it to red or amber significance (the highest) are presented regularly to the supervisory board; from time to time, these include cyber risks.

IMPORTANT CURRENT AND FUTURE CYBER RISK GOVERNANCE PRACTICES AND OPPORTUNITIES

Plans are currently in place to increase cyber risk and security monitoring, detection, and mitigation within the company through advanced malware detection and the creation of a Security Operations Center.

Knowing that this is a risk that will continue to grow exponentially, and as an insurer with a cyber crime insurance product, the company recognizes the need to understand this risk in real time and to have a well-informed view of what works internally within a company to combat cyber risk and maintain healthy cyber security. This extends to an understanding of what a systemic threat is, not only to a company but also to an entire sector or industry and to business generally.

US-Based Fortune 50 Global Health Care Company

WHEN AND WHY CYBER RISK GOVERNANCE BEGAN AT THE COMPANY

This company decided to upgrade its approach to cyber risk and security management approximately two to three years ago. At the time, a company-wide governance and risk committee had begun to form around the top risks (including cyber risks) facing the company. There were no major issues driving this change; it was more of a proactive and preventive stance fueled by the realization of changes and heightened cyber risks in the marketplace.

The key cyber risk challenges to this company emanate from the fact that it holds a lot of private data of its customers, on the one hand, and that it is active in M&A on a global scale, on the other hand. It is cognizant of and proactive about the cyber risk embedded in acquiring and integrating new companies and assets.

Another key challenge for the company is that it entered the Chinese market a few years ago and has heightened concerns regarding cyber issues there, not only for such issues within China but with such issues coming back to its North American headquarters and assets. However, China is such a big and lucrative market that it does not make sense to avoid it, so the company has established certain parameters around the types of business it will pursue in China—only business that does not involve deeply sensitive private data that the company would otherwise deal with in other countries where data protection and other legal protections are more robust and predictable.

Among the serious challenges the Chinese market presents is that nothing is "private"; there are different views on data generally, and dealing with state ownership of many of the means of production, companies, and suppliers creates other serious challenges.

WHO OWNS CYBER RISK MANAGEMENT

The company has two major divisions. Cyber risk is managed both enterprise-wide and at the two business divisions.

Since it began its cyber risk governance program, the company has developed a multitiered cyber risk governance approach at the operational (including information technology operators working on technology risk issues including cyber on the front lines), advisory, and executive levels.

The person with direct overall ownership and responsibility for cyber risk is the CISO, who dually reports to the company's CIO and the chief compliance officer, both of whom, in turn, are direct reports of the CEO.

Bimonthly, there is a management-level cyber risk committee meeting. Additionally, there are three different cross-functional risk committees—one for the overall enterprise and one each for the two business segments that sit above the cyber risk committee. This committee was created specifically for the multifaceted risks that cyber presents to the company; it is one of a few separate committees created around a specific risk. By way of illustration, another such stand-alone issue is that of data privacy, a major challenge facing this company globally.

The cyber risk committee is chaired by the CISO and includes the person who chairs the data privacy committee; several people who sit on both committees (data privacy and cyber risk) are from complementary fields like IT, legal, compliance, and physical security. In this company, there isn't a chief risk officer but a chief compliance officer who wears many hats.

THE ROLE OF THE CEO AND C-SUITE

At the highest levels of the organization, there is an executive committee made up of key executives who have a role in aspects of cyber risk management, the heads of information security, legal, operations, and enterprise risk management among them. Several of these individuals also report to the chief compliance officer, who has ultimate responsibility for legal and regulatory compliance, quality, import/export, and environment, health, and safety.

THE ROLE OF THE BOARD IN CYBER RISK OVERSIGHT

The board of directors committee most responsible for cyber risk oversight is the audit committee. A formal cyber risk presentation is made to this audit committee twice a year or every other quarter. The full board receives a cyber risk and security update at least once a year. The board is much more proactive about this issue today than it was even a year ago. In recent board self-evaluations, cyber risk has emerged as one of the key issues the board is focused on and wants the company to focus on.

From an oversight standpoint, the board is most concerned about making sure that:

- There is the right tone at the top on cyber issues
- Management allocates the right resources, talent, and expertise to deal with these issues
- Management hears and acts upon the results of impartial assessments

IMPORTANT CURRENT AND FUTURE CYBER RISK GOVERNANCE PRACTICES AND OPPORTUNITIES

The company is focusing in on using both the NIST and ISO 27000 frameworks from an operational and governance standpoint as they are very relatable to the C-suite and board, and both map and tie together very closely.

This health care company is on a global acquisition path; as such, cyber risk management is at the forefront of its strategy and business plan. It is building cyber due diligence into its acquisition approach, seeking to be fully cognizant of the risks and profile of the companies it contemplates integrating into its fold.

The company is looking to expand its program from separate "process, people and technology" platforms to tying all together to deliver a complete platform for the cyber market today—rationalizing across the platform. It also commissions a periodic assessment of its physical and IT security by outside independent advisors.

New kinds of attacks on or from new kinds of technology will require a nimble and immediate response to eradicate the threat. Understanding that it is critically important to determine what is normal and what is abnormal, this company also pays deep attention to the changing cyber marketplace; its experts are constantly expanding on their current knowledge. It is also developing a variety of table-top cyber-attack simulation exercises, which will be rolled out to its C-suite in short order.

As the top executive interviewed for this case at the company stated, "Integrating cyber with overall risk is the way to go."

US-Based Fortune 250 Global Business Process Outsourcing and Computing Services Company

WHEN AND WHY CYBER RISK GOVERNANCE BEGAN AT THE COMPANY

This company, a global leader in business process outsourcing and computing services, has had a cyber risk governance framework in place since 2011. The instigation for creating the framework was the company's need to implement a next-generation security operational risk and privacy program. The effort was consolidated over a two-year period in which the security organization was elevated to the executive level at the company, with a new and completely independent organization, new and independent resources, new operational transparency, and direct access to the C-suite and the board.

This global cyber risk governance program is innovative in that it is the equivalent of a stand-alone business within the company, catering to the various other segments of the company, devoid of dependencies and politics. The head of global security, a converged multidiscipline internal security provider, acts at the general manager of this business segment, with all the attendant aspects of a business: operations and program management, technology research and development, and chief technology officer-like as well as other functions (marketing, communications, engagement, clients).

Why is this possible? In great part because of the nature of the business, which requires a keen sense of cyber defenses and protection of deep and broad data coming from all over the world. But this is also possible because of the clearly visionary and committed nature of senior management, evident through the CEO's participation in the Executive Security Oversight Committee, and the board's determination to make cyber risk governance best in class, recognizing that it is necessary not only for maintaining its already strong reputation but for enhancing it even further.

WHO OWNS CYBER RISK MANAGEMENT

The global chief security officer (GCSO) is a vice president at the corporate level who reports to the CFO and the Executive Security Council, comprised of six of the 12 executive committee members. The GCSO was hired mainly for preventive purposes, though there had been a couple of near misses by the time he was hired in 2011. The company then proceeded to remove the independent security programs that existed at the business segment levels and create one unified, global, and transparent security operations platform including physical and cyber security, information security, threat management, criminal and civil investigations, financial crimes and fraud prevention teams, client security, program security, and cyber architecture—all under one global security umbrella.

There is also a vice president of ERM who reports to internal audit and whose focus is a total analysis of all risk, including financial, tax, and legal. However, operational risk ownership stays with the GCSO, who owns security, IT, and business process risk and reports these risks to the ERM system, which has a process to determine priorities, GRC process, tracking, and monitoring.

THE ROLE OF THE CEO AND C-SUITE

There is an overall company executive committee, which includes the CEO, business division heads, and functional executives.

The GCSO is chairman of the Executive Security Committee, which is made up of corporate executives like the general counsel, head of human resources, presidents of the business segments, head of BPO, CFO, and technology, and products head. They meet monthly to set policy, review strategy and mission, and exercise risk oversight. The CEO will from time to time attend these meetings as well.

On a quarterly basis, the GCSO briefs the executive committee on issues such as cyber defense measures and the ongoing list of cyber-related risks and shows up-to-date scorecards on the effectiveness of the company's defenses. These scorecards are also shared with the board.

THE ROLE OF THE BOARD IN CYBER RISK OVERSIGHT

The board hears about cyber risk on a quarterly basis and will also hear from the GCSO two to three times a year on special topics like business resilience, including what is referred to within the company as the "three-legged stool": business continuity, crisis management, and disaster recovery. The company has a highly developed and integrated system for these three parts of the three-legged resilience stool and conducts regular and surprise crisis exercises involving top executives and management.

Among the key agenda items that will be presented at board and executive committee meetings are: the previous month/quarter issues, new cyber issues, new incidents, major programs being tracked around identity, policy needs, the top 20 risks of the business, new business risks, and risk exceptions.

IMPORTANT CURRENT AND FUTURE CYBER RISK GOVERNANCE PRACTICES AND OPPORTUNITIES

Not a lot of companies have an Executive Security Committee, which includes six members from the C-suite who report to the CEO and participate in monthly meetings. This structure allows for a top-down and a bottom-up holistic view of cyber risk and related issues. Because it is centralized and independent, this approach to global cyber security management allows the entire organization's profile to be reviewed at the CEO and board levels. Having an independent organization that sits outside of information technology and the businesses allows it to be nimble, fast, transparent, and unencumbered by political intrigue and business expediency.

This unique model from a convergence standpoint works well as all relevant parties are housed within the organization—there is no need to "argue" with security as the team is within the group. This increases leverage and allows the company to combat risks and threats from a single operational command and control function. Thus, politics has been removed from the equation while oversight has been dramatically increased—from both the executive team and the board. It would be near impossible for someone in this organization to go rogue given this degree of oversight.

An area the company is investing heavily in—from both a resource and a monetary standpoint—is building a world-class operational privacy program. Privacy operational experts are being deployed globally as well as embedded in engineering, and new job families and job codes are being created such as "privacy expert in technology."

The executive interviewed stated: "The bad guys have a lot of money and resources. While you can get mad at a lot of companies and government, these companies had good security, perfect no, but good cyber defensive postures, yet they still got taken for a ride…I'm struggling with not getting hit the same way as Target got hit. How do you defend against a constantly changing attack? The speed at which cyber threats are changing daily and weekly is unprecedented: How fast can I get polymorphic defenses into place to move where they need to move?"

Cyber Risk Governance: Emerging (Best) Practices

Lessons Learned: The 10 Key Takeaways of This Report

In the process of building cyber resilience, the five profiled companies that are proactively building a cyber risk governance strategy have done one thing consistently: they have created a triangular framework to address their cyber risk profile that involves their highest governance body (board or supervisory board), their highest executive group (CEO and C-suite), and their top cyber risk managers and owners (from CISOs to Security to ERM). They have discovered that cyber resilience begins with effective cyber risk governance.

What follows are some of the good and best practices gleaned from the 10 cases we examined in this report, which should help other organizations to develop their own customized approach to either improving or building their cyber risk governance from scratch.

No entity is completely immune from cyber risk. Effective cyber risk governance entails a robust and synchronized triangular relationship between the board, the executive team, and the top expert managers who implement cyber risk strategy. Let's looks now at what that means in some detail:

1 **Develop a triangular governance approach to cyber risk management**

The board must take a proactive approach to cyber risk oversight Good governance is not strictly the domain of the board. It entails an effective triangular relationship between the board, the top leadership (CEO and C-suite), and top management talent within the organization all working in synchrony on strategy and risk, among other key organizational themes.

Table 8
What's on your board's cyber risk governance dashboard?

Architecture of cyber risk governance	Threat matrix — substantive cyber risk issues	Technology & liability defenses in place	Incident reporting	Cyber attack crown jewels
How is the company positioned, organized and deployed for cyber risk management? Is this the optimal approach?	Top issues Industry trends and benchmarking Technology trends and benchmarking Global heat map	Status report on what cyber defenses are in place: techno-logical, assessments, audits, monitoring, testing, insurance	Statistical overview of all incidents at company Specific mention of serious to material incidents	Know exactly what your company's crown jewels are – what are the perpetrators and potential perpetrators after?
Budget & resources	**Toolkit & proactive measures**	**Internal technology talent & skills assessment**	**External experts used/needed**	**Cyber actors & stakeholders matrix**
What is being spent? What is needed for proper cyber risk management?	Status report on the main policies and programs in place and what is needed	Review top expert executives Review C-suite and CEO performance on cyber risk management	Are the right experts in place? Including for periodic board report	Who are the potential perpetrators? Who are the company stakeholders and potential victims?

Source: GEC Risk Advisory LLC

And it shouldn't just be the domain of the audit committee. Consider what other committees might have joint jurisdiction or perhaps even priority jurisdiction. If a company has a risk, public affairs, or compliance committee, perhaps one of these committees should take the lead. If a company is at high risk for cyber attack, perhaps it should even consider a technology and cyber committee. Boards of companies at medium to high risk for cyber attack should also consider whether to have a board member with experience in technology and/or cyber security.

Depending again on the cyber risk profile of the company, the full board should have visibility into cyber risk management as well, if not quarterly, certainly biannually or at the very least annually. In this era of serious strategic risks like cyber risk and reputation risk, boards are increasingly entertaining the idea of adding board members with deep and broad risk expertise, including in some cases, cyber risk expertise specifically.

The CEO and the C-suite must take charge of cyber risk strategy and management Depending on the cyber risk readiness required at a given company, more or less direct CEO involvement on a regular and periodic basis is highly recommended. The more readiness is needed, the more actual attention, leadership, and support will be needed from the very top of the executive food chain.

This may also entail having someone within the executive team or even C-suite who has deep expertise on cyber matters or who has visibility into, and can discuss in informed detail, the cyber risk profile of the company.

The CEO and the board must ensure that the right frontline talent and resources are deployed A company will require greater or lesser technological and cyber expertise depending on how complex and global it is and what its services and products are. The right kind of technology and information leader—whether a CIO, a CISO, or a CSO—will have to be in place to take leadership or ownership of cyber risk issues. This also entails getting the right outside experts in place for specific tasks, building the right cyber defenses, investigating intrusions and attacks, and otherwise providing industry and marketplace benchmarking and intelligence.

2 Understand the reputation risk consequences to strategic cyber risk management gone wrong

Depending on the cyber risk exposure of a particular business, cyber risk can often become a material risk with potential additional and amplifying reputation risk consequences. Cyber risk is related to and potentially cuts across many other types of risks. For this reason, it should be considered at the top of many companies' risk prioritization, whether they have suffered from a major or material cyber attack (yet) or not.

Cyber risk and reputation risk are two strategic risks that are intimately intertwined. When a company is not prepared for its cyber risks, meaning that it doesn't have the right overall cyber risk governance program in place, the potential reputation risk consequences in today's social media world can amplify the company's exposure to both tangible and further intangible consequences that may be difficult, costly, and lengthy to repair.

3 Know who your cyber risk actors and stakeholders are

Critical to the success of a cyber risk governance framework is having a clear sense and inventory of who the key cyber risk actors are and who those with a principal stake or interest in proper cyber risk governance might be. A critical exercise all companies should undertake should consist of two activities: the updating of an ongoing threat matrix (as to actors and potential perpetrators) and the understanding of who the stakeholders are of your cyber risk exposure, what their expectations are of your company's cyber risk management, and what would happen if those expectations were not met.

This allows an entity to gauge the downside risk of not meeting stakeholders' expectations, which is a clear indicator of increasing potential reputational damage or downside.

4 Have a deep understanding of the organization's "crown jewels"

A successful triangular cyber risk governance framework necessitates a clear, in-depth understanding of the cyber risk crown jewels residing within the organization—whether they are intellectual property, personally identifiable information, trade secrets, executive personal profiles, or financial information. By knowing what cyber attackers are looking for, the cyber risk governance triangle can exercise more effective oversight and management.

5 Engage in a relevant cyber risk public-private partnership

Corporate sector reception of the US government's NIST framework has been generally positive, showing that public-private partnerships on developing the best cyber risk governance and management frameworks can be powerful. Although we haven't yet witnessed a major national cyber incident (that has made it to the public domain so far), especially regarding critical infrastructure, it would only make sense that such public-private partnerships, though voluntary, be encouraged and become the norm. Austria, Germany, the Netherlands, Spain, and the United Kingdom have established formal public-private partnerships for cyber security, while both Japan and Malaysia have set up official partnerships.[98]

6 Develop a cross-disciplinary approach to cyber risk management

One of the important lessons we have learned from both the cyber hit cases we have reviewed and from what the five companies building cyber resilience are doing is that there is a strong trend toward cross-disciplinary or cross-functional collaboration. This is partly in recognition of the complexity and novelty of cyber risk, where no one expert can really "own" the issue. It is partly in recognition of the quickly morphing aspect of cyber risk, requiring the best and brightest minds from a variety of disciplines. And it is partly a recognition that silos don't work in today's superconnected, fast-moving era of megarisk.

Thus, whether one or more functions take the lead—information security, corporate security, enterprise risk management, others—each of these and other functions should own a piece of the puzzle but always work together to understand the entire puzzle.

7 Develop a cross-segmental/divisional approach to cyber risk management

Another useful and cutting-edge trend among companies at the high end of creating effective cyber risk governance entails not only deploying an integrated cross-disciplinary and cross-divisional team to keep a steady eye on cyber risk management within and across the company. In this way, each relevant function and each business segment owns one or more relevant slices of cyber risk management.

Whether this means that overall cyber risk management is done in a single global command-and-control structure or a more distributed model, where each segment or division has a segmental or divisional version of the global cyber risk structure, is up to the company. Both models can work well so long as they are suited to the culture and structure of a particular organization.

8 Make cyber risk governance an essential part of your organization's resilience approach

A practice at leading companies is to have cyber risk fully embedded in and part of what some call the resilience triangle: crisis management, business continuity, and disaster recovery planning. For those that perceived their cyber risk as high to very high (e.g., utilities and global technology companies), that means doing cyber security-related crisis management drills on a periodic and even surprise basis, with executives mainly but sometimes even including board members. It also means having a well-developed emergency response and business continuity program in place, ready at all times for the cyber event that might occur.

9 Choose one of the three effective cyber risk governance models

If we examine the possible types of cyber risk governance along a continuum of least to most evolved models depending on two key criteria: leadership engagement and awareness, on the one hand, and relative cyber exposure (low to high), on the other hand, we come up with five types. Based on these criteria and what the cases examined in this report have shown, these cyber governance types include (from least to most evolved):

The Irresponsible or Nonexistent Cyber Risk Governance Model This is the least evolved or nonexistent form of cyber risk governance. There is little to no leadership awareness, engagement, or knowledge of cyber issues (or willingness to learn) and simultaneously a medium to high exposure to cyber risk given what the entity does, where it operates, etc.

The Complacent Cyber Risk Governance Model This is the next step in evolution of cyber risk governance but is not much better than the first type. There is little leadership awareness, engagement, or knowledge of cyber issues (or willingness to learn), and thus a general sense of complacency, within an entity with relatively low to medium exposure to cyber risk given what the entity does, where it operates, etc.

The Vigilant Cyber Risk Governance Model This form of cyber risk governance is more evolved as it involves leadership that is more engaged, knowledgeable, and vigilant on cyber risk issues even though the entity has a relatively low to medium exposure to cyber risk given its operations, products, services, footprint, etc.

The Integrated Cyber Risk Governance Model This is a highly evolved form of cyber risk governance that has engaged, knowledgeable, and vigilant leadership, with an effective, integrated cyber risk management and governance at a largely decentralized, medium to high exposure organization.

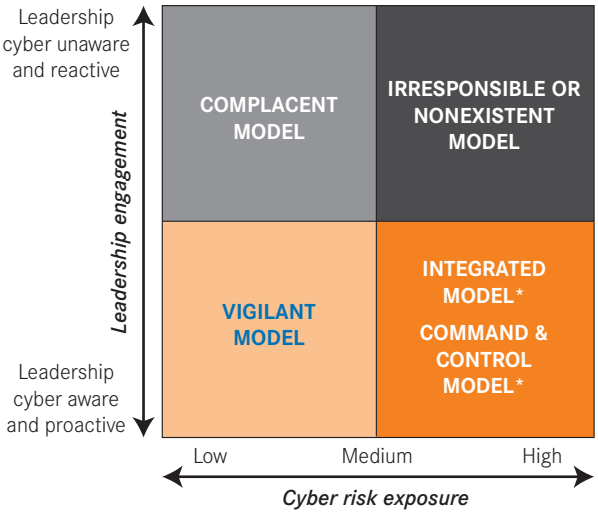
The Command & Control Cyber Risk Governance Model This is another form of highly evolved cyber risk governance, with engaged, knowledgeable, and vigilant leadership and an effective form of cyber risk management and governance that is organized in a more centralized, command-and-control manner for a more centralized organization that has medium to high cyber risk exposure.

One of the more cutting-edge approaches to cyber risk governance that we encountered in the research for this report was the one being built at the US-based Fortune 250 global business outsourcing & computing services company. There, a completely independent "business" is being built to serve the rest of the company on all of its technology and security services, including cyber risk management. This business has its own independent financial accountability to the CEO and board, just like any other business segment, and is not beholden to the other businesses segments for its budget and resources. By the same token, this is not a rogue corporate security function; it has clear, direct, and frequent lines of accountability and reporting to both the CEO of the overall business and the board, perhaps on an even more regular basis than the other more established businesses, given the nature of its mission.

While this may not be a model for every organization, it is an example of the creativity and customization that leading companies are experimenting with and succeeding at in this quickly changing and cyber threat-based global economy. Figure 15 may provide readers with a bird's eye view of where their entity might fall and where it perhaps should be if it's not in the right place at this time.

Figure 15

A typology of cyber risk governance readiness and resilience



* In this category the integrated model would be more likely for decentralized companies and the command and control model for more centralized companies.

Source: GEC Risk Advisory LLC

10 **Transform effective cyber risk governance into an opportunity for better business**

Some of the leading companies we researched have also cracked another welcome code: finding ways to improve their cyber risk governance is leading them to find new business opportunities and potentially greater value. In essence, they are transforming their cyber risk into possible additional value in the form of new products and services and new revenues to the company.

While not every company can do this, every company can certainly find better ways to do things that provide opportunities for business process improvements, efficiency, and coordination that in turn will provide cost savings in the form of fewer incidents, not losing important stakeholders (investors, customers, employees), and not paying exorbitant fines or legal and litigation costs.

Creating the Right Cyber Risk Governance Approach for Your Company: A Questionnaire

When it comes to cyber risk preparedness, each organization needs to assess its own risk profile and governance needs. However, there is one point in today's age of hypertransparency, superconnectivity, and megarisk on which no one should compromise: all entities—even the smallest mom-and-pop businesses—require some form of cyber risk governance. Every entity—whether for profit, nonprofit, university, government, even religious—has a cyber risk profile and therefore can make use of the findings in this report.

That said, it is critical that the right balance be achieved, and for that purpose, the questionnaire in Table 9 (pages 54–55) should help any organization determine the extent, cost, and resources it needs to achieve the right balance of cyber risk governance.

Table 9

Cyber risk governance questionnaire for executives and boards

1	What type of industry is the company in? Is it an industry that has low, medium, or high exposure to cyber risk?	Nontechnological services Media[a]	Manufacturing Automotive Management Consulting	Financial Insurance Retail Health care Chemicals BPO	Technology Defense Utility Infrastructure Transportation
2	What are the company's "crown jewels" that cyber attackers may be interested in capturing?	There are few or none[b]	Some: Employee private data Company IP	Employee & customer private data Valuable company IP	Government contracts State secrets Valuable IP
3	What is the company's global footprint?	Low	Medium	High	Intense
4	What is the company's R&D and/or M&A appetite?	Low	Medium	High	Intense
5	Has/should the company have an outside cyber risk assessment made?	No	Under consideration	Yes, once	Yes, periodically
6	What is the company's overall approach to management and enterprise structure?	Decentralized		Coordinated/distributed	Centralized
7	Has the company done a cyber risk stakeholder review and impact assessment?	No		Informally	Yes
8	Does/should the company get involved in a public/private partnership on cyber security matters?	No, not a critical infrastructure company (CIC))		Maybe, though not a CIC	Yes, a CIC
9	Does/should the company have an enterprise risk management program?	No	Yes, informal	Formal (under development or early stages)	Formal, sophisticated

(continued on next page)

Note: This table depicts on a spectrum from left to right (with greater intensity as you move right) some of the key criteria companies should consider when designing their cyber risk governance framework. Thus, depending on its cyber risk exposure, industry, global footprint, and other strategic and tactical considerations, a company (and its executives and board) must decide how intense/proactive its cyber risk governance framework should be.

a, b Executives and board directors should be cautious in answering this question as every company or business has some data–whether personally identifiable information, health care information of employees including executives and even board members, or other organization's valuable data–that may be a target. Law firms, in one clear and daunting example of this, have been notoriously lax about compliance and cyber defenses, yet they hold some of their client's most valuable secrets.

Table 9

Cyber risk governance questionnaire for executives and boards (continued)

10	Should the company's ERM or Risk Management Program include cyber risk in its highest priorities?	No	Somewhat	Yes	A top-five priority
11	Who has direct management ownership for cyber risk?	IT/CIO or Security	IT/CIO + others separately	IT/CIO + Others Jointly	Cross-Disciplinary Cross-Divisions Fully integrated Cross-Disciplinary & Divisional
12	Should corporate security play a role in cyber risk management?	Separate	Coordinated Loose	Coordinated Integrated	Command & Control HQ
13	Should there be a cyber risk presence at the C-suite/executive team level?	No	Concerns raised through another	Concerns part of another executive's portfolio (e.g., CAO or COO)	CIO, CSO or equivalent is an Executive Team member
14	What committee at the board level hears/should hear about cyber risk?	Audit	Audit + another committee (Compliance, Risk, Public Affairs)	Joint committee meetings	Full board
15	How often should cyber risk experts (internal or external) report to the C-suite / executive team?	Annually	Biannually	Quarterly	Monthly Periodically + whenever necessary
16	How often should cyber risk experts (internal or external) report to the board/ board committee?	Annually	Biannually	Quarterly	Monthly Periodically + whenever necessary
17	Should cyber risk be specifically recognized as part of the company's crisis management team and plan?	No	Under consideration	There are executive team drills	There are executive team & board committee drills Cyber specific Full board
18	Should cyber risk fully integrated into the company's resilience plan (crisis management, business continuity, disaster recovery)?	No	Maybe	Partially	Fully

Source: GEC Risk Advisory LLC

Preparing for an Uncertain Cyber Future

Effective cyber risk governance requires a strong triangular internal relationship between the board of directors, the executive management or C-suite, and the heads of the pertinent internal functions dealing with cyber risk daily. This triangular relationship must be synchronized, integrated, seamless, focused, and informed. Without this framework and without these attributes, entities run the risk of opening themselves up to weak links, attacks, subversion, and conquest (at least temporarily and with serious financial, reputational, and other consequences).

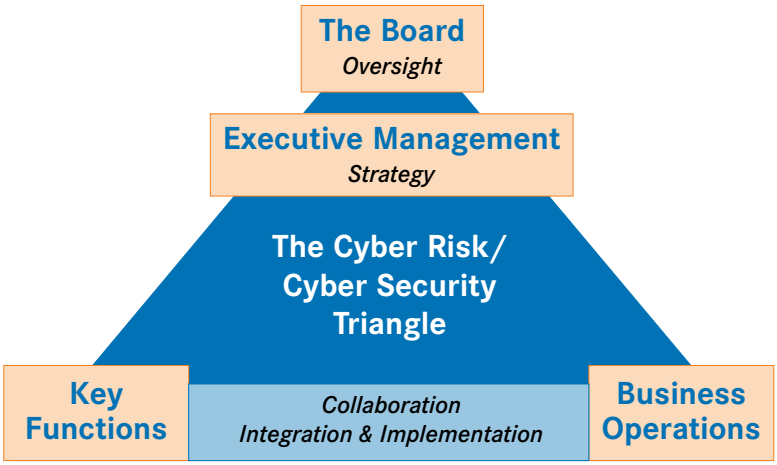
Without a deliberate cyber risk governance approach, no entity will be able to meet, let alone withstand, the onslaught of cyber risk. Cyber risk is not a passing fad like Y2K (for those who can remember that far back).

Cyber risk is a constant, and a constantly morphing, reality that will be with us for the foreseeable future. Without the highest levels of leadership of an entity paying deliberate and close attention, and devoting the right mix of resources and incentives, businesses and other entities are bound to be embarrassed, hurt, financially and reputationally hit, or worse.

Good cyber risk governance, at the end of the day, is about strong leadership, a coherent culture, and a creative, expert team all working well together not only to defeat a difficult, amorphous, and constantly changing enemy but also to conquer the problem and maybe even extract some real value through increased efficiency and new products and services.

Figure 16

The governance, risk, and reputation triangle as applied to cyber risk



Source: Andrea Bonime-Blanc, "Implementing a Holistic Governance, Risk and Reputation Strategy for Multinationals: Guidelines for Boards," *Ethical Boardroom*, September 1, 2014 (http://ethicalboardroom.com/risk/implementing-holistic-governance-risk-reputation-strategy-multinationals-guidelines-boards/).

APPENDIX A

Cyber Risk Glossary

Back door: An undocumented method of entering a system that avoids typical entry mechanisms

Biometrics: An access mechanism that involves physical characteristics of the user

Botnet: a group of compromised computers used to harm other networks or computers

Bots: An automated process which interacts with other network services

Code injection: An attack used to steal information or take control of web servers

Day zero: The day when a new vulnerability is made known

Denial of service: Delaying of system operations and functions or the prevention of authorized access to a system

Dictionary attack: An attack that attempts using all dictionary phrases and words to break a password or key

Drive-by exploits: Attacks that target Internet-related software and infects them automatically

Encryption: Transforming data into a form that hides the data's original meaning

Event: A system or network occurrence that can be observed

Exploit: A piece of software, a command, or methodology that attacks a particular security vulnerability

Firewall: A discontinuity in a network intended to protect against unauthorized access to data or resources

Gateway: A point of entry between two networks

Hybrid attack: An attack incorporating the elements of a dictionary attack, but with the addition of numerals and symbols to the words used

Incident: The threat or execution of an adverse network event in an information system or network

Logic bombs: Programs or pieces of code that execute when a predefined event or set of circumstances occurs

Malware: Software designed to damage, disrupt, or otherwise have a negative effect on data, hosts, or networks

Passive attack: An attack by a legitimate attacker that attempts to use a system's information without negatively altering the system

Patch: An update by a software manufacturer to fix the software's existing bugs

Phishing: A type of scam using emails disguised as trustworthy to fool a target into inputting personal information at a fake website. See *Spear phishing* below.

Search engine poisoning: Leaving "bait" for searches that redirects users to malicious content

Spam: Flooding a target with emails

Spear phishing: Essentially the same as phishing, but the scam email is personalized. Spear phishers capitalize on their ability to track the online presence of their potential victims.

Targeted attacks: Long-term attacks either to obtain data or increase control of the target system

Trojans: Inconspicuous software that steals target information through back door methods

Virus: A type of malware that replicates itself and becomes part of another program

Worms: A type of malware that uses vulnerabilities of their target to replicate and redistribute themselves

Zombies: One of typically many compromised computers in a botnet that is connected to the Internet and is used to perform malicious tasks

Sources: "What Is the Difference: Viruses, Worms, Trojans, and Bots?" Cisco; "Glossary of Security Terms," SANS, 2015; Aisha Gani et al.,"Guide to Cyber Security Threats," *Financial Times*, June 5, 2013; "Explore Terms: A Glossary of Common Cybersecurity Terminology," National Initiative for Cybersecurity Careers and Studies, Department of Homeland Security; "Spear Phishing: Scam, Not Sport," Norton, Symantec Corporation.

APPENDIX B

Cyber Risk Fast Facts

Cyber Risk Numbers

The table on page 59 lays out some important cyber risk trends and developments in quantitative terms. Among some of the most interesting are:

- 205 is the median number of days an attacker is left undetected in a system after data has been compromised[99]
- 3 percent of all global organizations lost over $1 million each due to cybercrime in 2013[100]
- 77 percent of these survey respondents detected a security event in the past year[101]
- US$375 billion to $575 billion is the estimated annual cost to the global economy from cybercrime[102]
- 85 percent of firms with fewer than 1,000 employees reported their systems had been hacked
- 62 percent of security professionals say insider threat rates have risen in the last 12 months[103]

A COMPENDIUM OF CYBER RISK TRENDS, FACTS, AND NUMBERS

DESCRIPTION	DATA
Number of organizations from business, financial, educational, government, and healthcare sectors that publicly disclosed data breaches in 2013	614
Number of records exposed from publicly disclosed data breaches in 2013	92 million
Percentage of publicly disclosed data breaches in 2013 in healthcare	43.8%
Percentage of publicly disclosed data breaches in 2013 in business	34.4%
Percentage of total records exposed (in publicly disclosed data breaches in 2013) attributable to business	84%
Percentage of US organizations that lost over $1 million due to cybercrime in 2013	7%
Percentage of US organizations that lost $50 thousand to $1 million due to cyber crime in 2013	19%
Percentage of global organizations that lost over $1 million due to cybercrime in 2013	3%
Percentage of global organizations that lost $50 thousand to $1 million due to cybercrime in 2013	8%
Percentage of survey respondents who detected a security event in the past year	77%
Percentage of survey respondents who reported an increase in security events detected in the past year	34%
Percentage of survey respondents who reported being more worried about security threats this year than in the past	59%
Percentage of US survey respondents worried about the impact of cyber threats to their growth prospects	69%
Number of security incidents detected per organization in 2013	135
Estimated annual cost to the global economy from cybercrime	$375-575 billion
Percentage of Internet value extracted by cybercrime	15-20%
Annual cost of online fraud to Mexican banks	$93 million
Annual cost of online fraud to Japanese banks	$110 million
Percentage of profits lost by Indian companies due to cybercrime	5%
Typical stock price decline after a significant hack	1-5%
Cyber crime as a percentage of US GDP	0.64%
Median number of days an attacker is left undetected in a system after data has been compromised	205
Percent of attack victims that had to be notified by an external entity about a breach	69%
Percentage of security professionals who say insider threat rates have risen in the last 12 months	62%
Percentage of firms with fewer than 1,000 employees who reported their systems had been hacked	85%
Percentage of firms with more than 1,000 employees who reported their systems had been hacked	15%
Percentage of board members across industries that believe they have a "high level" of understanding about cyber security risk	11%

Sources: Robert Hartwig and Claire Wilkinson, "Cyber Risks: The Growing Threat," Insurance Information Institute, June 2014 (http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf); David Burg et al., "US Cybercrime: Rising Risks, Reducing Readiness," PwC, 2014 (http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf); "Net Losses: Estimating the Global Cost of Cybercrime," Center for Strategic and International Studies, June 2014 (http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf); Teren Bryson, "Big Security Breaches and How Big Data Can Prevent Them," Enterprise Networking Planet, June 25, 2015 (http://www.enterprisenetworkingplanet.com/netsecur/big-security-breaches-and-how-big-data-can-prevent-them.html); Nathan Eddy, "Insider Attacks Rise, Though Some Businesses Unaware of Risks," eWeek, June 29, 2015 (http://www.eweek.com/small-business/insider-attacks-rise-though-some-businesses-unaware-of-risk.html).

APPENDIX C

Cyber Risk Insurance

Cyber Insurance–The Jury Is Still Out

The National Association of Insurance Commissioners provides the following overview of cyber risks:[104]

> As data breaches occur more frequently, there are additional pressures for business to step up efforts to protect the personal information in their possession. Cyber attacks may come from nation states, terrorists, criminals, activists, external opportunists and company insiders (both intentional and unintentional). Cyber criminals attack to gain some type of political, military, or economic advantage. They usually steal money or information that can eventually be monetized, such as credit card numbers, health records, personal identification information, and tax returns.

Additionally, NAIC provides the following assessment of cyber risk insurance policies:

> **Cyber Liability Policies**
>
> Most businesses are familiar with their commercial insurance policies providing general liability coverage to protect the business from injury or property damage. However, most standard commercial lines policies do not cover many of the cyber risks mentioned above.

NAIC'S LIST OF POSSIBLE TYPES OF CYBER RISK COVERAGE

- Liability for security or privacy breaches. This would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.
- The costs associated with restoring, updating or replacing business assets stored electronically.
- Business interruption and extra expense related to a security or privacy breach.
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media.
- Expenses related to cyber extortion or cyber terrorism.
- Coverage for expenses related to regulatory compliance for billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings.

NAIC'S LISTING OF CYBER RISKS

- **Identity theft** as a result of security breaches where sensitive information is stolen by a hacker or inadvertently disclosed, including such data elements as Social Security numbers, credit card numbers, employee identification numbers, drivers' license numbers, birth dates and PIN numbers.
- **Business interruption** from a hacker shutting down a network.
- Damage to the firm's **reputation**.
- Costs associated with damage to **data records** caused by a hacker.
- Theft of valuable **digital assets**, including customer lists, business trade secrets and other similar electronic business assets.
- **Introduction of malware**, worms and other malicious computer code.
- **Human error** leading to inadvertent disclosure of sensitive information, such as an email from an employee to unintended recipients containing sensitive business information or personal identifying information.
- **The cost of credit monitoring services** for people impacted by a security breach.
- Lawsuits alleging **trademark** or **copyright infringement**.

Source: National Association of Insurance Commissioners

To cover these unique cyber risks through insurance requires the purchase of a special cyber liability policy. However, cyber risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. Insurers compensate by relying on qualitative assessments of an applicant's risk management procedures and risk culture. As a result, policies for cyber risk are more customized than other risk insurers taken on, and, therefore, more costly. The type of business operation will dictate the type and cost of cyber liability coverage. The size and scope of the business will play a role in coverage needs and pricing, as will the number of customers, the presence on the Web, the type of data collected and stored, and other factors.

Where the cyber insurance policy rubber meets the cyber road is in the following:

Securing a cyber liability policy will not be a simple task. Insurers writing this coverage will be interested in the risk-management techniques applied by the business to protect its network and its assets.

The insurer will probably want to see the business' disaster response plan and evaluate it with respect to the business' risk management of its networks, its website, its physical assets, and its intellectual property. The insurer will be keenly interested in how employees and others are able to access data systems. At a minimum, the insurer will want to know about antivirus and anti-malware software, the frequency of updates and the performance of firewalls.

The debate will continue to rage in the marketplace about the viability, usability, benefits, and detriments of cyber risk insurance. As one piece puts it: "Unlike other types of insurance, there is no standard form on which the insurance industry as a whole underwrites cyber coverage."[105]

One thing is clear, however—as with all other types of insurance coverage, especially new ones that are time untested and still evolving, this kind of insurance coverage will only be available to those companies that show a keen interest in, and implementation of, an appropriate cyber risk management program including, most importantly, an effective cyber risk governance program.

Endnotes

1 Jeff Elder, "Hacking HQ: New Study Looks at Non-Tech 'Innovation Centers'," *Wall Street Journal*, July 22, 2015 (http://blogs.wsj.com/digits/2015/07/22/hacking-hq-new-study-looks-at-non-tech-innovation-centers/tab/print/).

2 Eduard Kovacs, "Cybercriminals Exploiting Malaysian Airlines Flight MH17 Tragedy," *SecurityWeek*, July 28, 2014 (http://www.securityweek.com/cybercriminals-exploiting-malaysia-airlines-flight-mh17-tragedy); AFP, "Singapore Boosts Cybersecurity after Hacking Incidents," *SecurityWeek,* August 26, 2014 (http://www.securityweek.com/singapore-boosts-cybersecurity-after-hacking-incidents). For more information on the European cases, see: "International Case Report on Cyber Security Incidents: Reflections on Three Cyber Incidents in the Netherlands, Germany and Sweden," November 2014 (https://www.gccs2015.com/sites/default/files/documents/ICR_CYBERCECURITYINCIDENTS_LR.PDF). For an extensive review of the state of cyber security in Latin America, see: OAS & Symantec, "Latin American and Caribbean Cybersecurity Trends," June 2014 (http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf).

3 "Boards of Directors, Corporate Governance and Cyber Risks: Sharpening the Focus," speech by SEC Commissioner Luis Aguilar, June 10, 2013 (http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VPxpsEJtIRF).

4 David E. Sanger, "Hackers Took Fingerprints of 5.6 million US workers, Government Says," *New York Times*, September 23, 2015; Julie Hirschfeld Davis, "Hacking of Government Computers Exposed 21.5 million People," *New York Times*, July 9, 2015.

5 Geoffrey Smith, "Hackers Have Got All of Online Adultery Site Ashley Madison's Data," *Fortune*, July 22, 2015 (http://fortune.com/2015/07/20/ashley-madison-hack-leak-adultery-online-impact-team/); "Ashley Madison Chief Steps Down after Data Breach," *New York Times*, August 28, 2015.

6 "Reframing the Issue: New Ways to Think about Cyber Risk and Security," The Conference Board, *Council Perspectives*, 2013 (https://www.conference-board.org/topics/publicationdetail.cfm?publicationid=2666).

7 The Conference Board has a wide array of cyber risk and security resources and publications available (https://www.conference-board.org/governance/index.cfm?id=23202). Additionally, one of the pioneers in discussing risk and risk governance is the DC-based nonprofit Internet Security Alliance (ISA), which published the then-innovative "Internet Security Social Contract" in 2008 with policy recommendations that the Obama administration adopted years later in its Executive Order on Cyber Security in 2013 (https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636). Additional ISA resources can be found here: (http://www.isalliance.org/isa-publications/). Finally, the National Association of Corporate Directors (NACD) with the assistance of ISA executive director Larry Clinton, published one of the first governance guides on cyber security oversight, "The Cyber Risk Oversight Handbook," in June 2014 (https://www.nacdonline.org/cyber).

8 "The Enemy Within: Rogue Employees Can Wreak More Damage on a Company Than Competitors," *The Economist*, July 25, 2015 (http://www.economist.com/news/business/21659776-rogue-employees-can-wreak-more-damage-company-competitors-enemy-within).

9 In this PwC Survey, employees were identified as the primary and growing threat to cyber security within organizations: "Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security® Survey 2015," PwC, September 30, 2014 (http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml).

10 Andrea Bonime-Blanc, *The Reputation Risk Handbook: Surviving and Thriving in the Age of Hyper-Transparency* (Oxford: DŌ Sustainability, 2014), p. 45.

11 "The International Business Resilience Survey 2015," Marsh, October 2015 (http://uk.marsh.com/Portals/18/Documents/International%20Business%20Resilience%20Survey%202015-10-2015.pdf).

12 The National Security Agency has created a map of purported Chinese attacks on US business over the past five years; "Exclusive: Secret NSA Map Shows China Cyber Attacks on US Targets," NBC News, July 30, 2015.

13 Hannah Kuchler, "Cyber Insecurity: Hacking Back," *Financial Times*, July 27, 2015 (http://www.ft.com/intl/cms/s/2/c75a0196-2ed6-11e5-8873-775ba7c2ea3d.html#axzz3hnKwzt4i); Sam Jones et al., "Cyber Insecurity: West Eyes Dr. Strangelove Tactics in Cyber Wars," *Financial Times*, July 29, 2015 (http://www.ft.com/intl/cms/s/0/2d23d4c8-35d2-11e5-b05b-b01debd57852.html#axzz3hnKwzt4i).

14 This is a somewhat oversimplified categorization of cyber actors. The very same folks who are "defenders" (e.g., a government agency trying to assist and protect the financial sector) may also position themselves as "attackers" when they take on the mission of proactive cyber hacking and cyber warfare against nation-state or state-sponsored cyber "enemies."

15 McAfee, Critical Infrastructure Readiness Report (http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf).

16 "The Intersection of Social Media & Cyber Security," ZeroFOX, 2014.

17 "The Intersection of Social Media & Cyber Security," ZeroFOX, 2014.

18 "Cyber Security Risks of Using Social Media–Guidance for the Government of Canada," Communications Security Establishment, Government of Canada, September 2013 (https://www.cse-cst.gc.ca/en/node/233/html/9869).

19 Dr. Kenneth Geers and Spencer Wolfe, "The Social Takeover: A Close Look at Threats Old & New on Social Media," ZeroFOX, 2015.

20 Geers and Wolfe, "The Social Takeover," p. 1.

21 Geers and Wolfe, "The Social Takeover," p. 4.

22 Jenny Mangelsdorf, "Using Big Data to Defend against Cyber Security Threats," Computer Sciences Corp (http://www.csc.com/cybersecurity/publications/93325/104033-using_big_data_to_defend_against_cyber_security_threats); Alastair Stevenson, "Big Data Analytics Are the Future of Cyber Security," V3.co.uk, May 5, 2015 (http://www.v3.co.uk/v3-uk/news/2406862/big-data-analytics-are-the-future-of-cybersecurity).

23 "IBM Security Intelligence with Big Data," IBM (http://www-03.ibm.com/security/solution/intelligence-big-data/).

24 "Internet of Things Research Study," HP, 2014 (http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en).

25 David Morgan, "Car Hacking Risk May Be Broader Than Fiat Chrysler: U.S. Regulator," Reuters, July 31, 2015 (http://www.reuters.com/article/2015/07/31/us-fiat-chrysler-hacking-regulator-idUSKCN0Q525U20150731).

26 "Cybersecurity and the Internet of Things: Insights on Governance, Risk and Compliance," EY, March 2015 (http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf).

27 Quoted in Gary Marcus, "Artificial Intelligence Isn't a Threat—Yet," *Wall Street Journal*, December 11, 2014 (http://www.wsj.com/articles/artificial-intelligence-isnt-a-threatyet-1418328453).

28 Kris Hammond, "What Is Artificial Intelligence?" *Computerworld*, April 10, 2015 (http://www.computerworld.com/article/2906336/emerging-technology/what-is-artificial-intelligence.html).

29 Alex J. Champandard, "Artificial Intelligence," AI Depot, 2002 (http://ai-depot.com/Intro.html); "Cybersecurity and Artificial Intelligence: A Dangerous Mix," InfoSec Institute, February 24, 2015 (http://resources.infosecinstitute.com/cybersecurity-artificial-intelligence-dangerous-mix/).

30 "Cybersecurity and Artificial Intelligence," InfoSec Institute; Nayef Al-Rodhan, "The Security Implications and Existential Crossroads of Artificial Intelligence," Georgetown Journal of International Affairs, April 2, 2015 (http://journal.georgetown.edu/the-security-implications-and-existential-crossroads-of-artificial-intelligence/); "The Dawn of Artificial Intelligence," *The Economist*, May 9, 2015 (http://www.economist.com/news/leaders/21650543-powerful-computers-will-reshape-humanitys-future-how-ensure-promise-outweighs).

31 "The Dawn of Artificial Intelligence," *The Economist*, 2015.

32 Mark Odell, "Tech Leaders Warn of Killer Robot Arms Race," *Financial Times*, July 27, 2015 (http://www.ft.com/intl/cms/s/2/50f209f4-3494-11e5-b05b-b01debd57852.html#axzz3kVfn89mr).

33 Jess Fee, "The Beginner's Guide to the Cloud," *Mashable*, August 26, 2013 (http://mashable.com/2013/08/26/what-is-the-cloud/); Adam Clark Estes, "What Is "the Cloud"—and Where Is It?" *Gizmodo*, January 29, 2015 (http://gizmodo.com/what-is-the-cloud-and-where-is-it-1682276210).

34 "Cloud Cybersecurity Report: The Extended Perimeter," CloudLock, 2015. (http://www.cloudlock.com/wp-content/uploads/2015/04/Cloud-Cybersecurity-Report-The-Extended-Perimeter-CloudLock.pdf).

35 Eric A. Fischer, "Federal Laws relating to Cybersecurity: Overview and Discussion of Proposed Revisions," Congressional Research Service, June 20, 2013 (http://fpc.state.gov/documents/organization/211410.pdf).

36 Alan Charles Raul, ed., "The Privacy, Data & Cybersecurity Law Review," Law Business Research, November 2014 (http://www.sidley.com/~/media/files/publications/2014/11/the%20privacy%20data%20protection%20and%20cybersecurity%20la__/files/united%20states/fileattachment/united%20states.pdf).

37 Fischer, "Federal Laws relating to Cybersecurity."

38 Raul, "The Privacy, Data & Cybersecurity Law Review."

39 US Securities and Exchange Commission, "CF Disclosure Guidance Topic N. 2 –Cybersecurity," October 13, 2011 (https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm); Hanover Research, "The Emergence of Cybersecurity Law," Indiana University Maurer School of Law, February 2015 (http://info.law.indiana.edu/faculty-publications/The-Emergence-of-Cybersecurity-Law.pdf).

40 Hanover Research, "The Emergence of Cybersecurity Law," 2015.

41 "About NIST," National Institute of Standards and Technology, February 25, 2015 (http://www.nist.gov/public_affairs/nandyou.cfm).

42 "Information Technology Portal—Overview," NIST, July 2, 2015 (http://www.nist.gov/information-technology-portal.cfm).

43 "Cybersecurity Framework," NIST, July 8, 2015 (http://www.nist.gov/cyberframework/index.cfm).

44 "Cybersecurity Framework Frequently Asked Questions," NIST, February 12, 2015 (http://www.nist.gov/cyberframework/cybersecurity-framework-faqs.cfm).

45 "Framework for Improving Critical Infrastructure Cybersecurity," NIST, February 12, 2014 (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf).

46 "Framework for Improving Critical Infrastructure Cybersecurity," NIST, 2014.

47 "Overview of NIST Cybersecurity Framework," Booz Allen Hamilton, March 2014.

48 Tim Casey et al. "An Intel Use Case for the Cybersecurity Framework in Action," Intel, 2015 (http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html).

49 Taylor Armerding, "NIST's Finalized Cybersecurity Framework Receives Mixed Reviews," *CSO*, January 31, 2014 (http://www.csoonline.com/article/2134338/security-leadership/nist-s-finalized-cybersecurity-framework-receives-mixed-reviews.html).

50 EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity, European Commission press release, February 7, 2013 (http://europa.eu/rapid/press-release_IP-13-94_en.htm).

51 Philippe Boillat and Morten Kjaerum, *Handbook of European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2014) (http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf#2013.9195_EN.indd%3A.143272%3A8126).

52 "Convention on Cybercrime," Council of Europe, November 23, 2001 (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

53 "EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity—Cyber Security Strategy and Proposal for a Directive"(http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cybersecurity); Alexander DeGaye and Michael Brown, "Progress Update on the EU Cybersecurity Directive," February 27, 2015 (http://privacylawblog.fieldfisher.com/2015/progress-update-on-the-draft-eu-cybersecurity-directive).

54 Christian Oliver and Tom Mitchell, "EU and US Groups Sound Alarm on China Cyber Security Rules," *Financial Times*, February 26, 2015 (http://www.ft.com/intl/cms/s/0/12a7a126-bd67-11e4-9902-00144feab7de.html#axzz3fNOorxoZ).

55 "Cyber Security and the Impact on Banks in China," KPMG, March 2015 (https://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/cybersecurity-and-the-Impact-on-Banks-in-China-201503.pdf).

56 Jun He Bulletin, "National Security Law," July 17, 2015 (http://www.junhe.com/images/ourpublications/Bulletin/Bulletin_EN/20150717_01.pdf).

57 China Monitor, "Cyber Security in China: New Political Leadership Focuses on Boosting National Security," Mercator Institute for China Studies, December 9, 2014 (http://www.merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf).

58 "People's Republic of China," CyberCrime Law (http://www.cybercrimelaw.net/China.html).

59 PI Yong, "New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime," Council of Europe, December 2011 (http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/Cyber_cp_china_Pi_Yong_Dec11.pdf).

60 Organization of American States and Symantec, "Latin American and Caribbean Cybersecurity Trends. June 2014," (http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf).

61 OAS & Symantec, "Latin American and Caribbean Cybersecurity Trends," 2014.

62 Rachel Abrams, "Target Puts Data Breach Costs at $148 Million and Forecasts Profit Drop," *New York Times*, August 5, 2014 (http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html).

63 Meagan Clark, "Time of Target's Data Breach and Aftermath: How Cybertheft Snowballed for the Giant Retailer," *International Business Times*, May 5, 2014 (http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056); Brian Krebs, "The Target Breach, By the Numbers," Krebs on Security, May 6, 2014 (http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/).

64 Marie-Louise Gumuchian and David Goldman, "Security Firm Traces Target Malware to Russia," *CNN*, January 21, 2014 (http://www.cnn.com/2014/01/20/us/money-target-breach/).

65 Michael Kassner, "Anatomy of the Target Breach: Missed Opportunities and Lessons Learned," *ZDNet*, February 2, 2015 (http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/).

66 Kassner, "Anatomy of the Target Breach," p. 2.

67 Kassner, "Anatomy of the Target Breach," p. 3.

68 "Target CEO Ouster Shows New Board Focus on Cyber Attacks," *Bloomberg*, May 6, 2014 (http://www.bloomberg.com/news/articles/2014-05-05/target-ceo-ouster-shows-new-board-focus-on-cyber attacks).

69 Tracy Kitten, "7 Lessons from Target's Breach," Bank Info Security, December 10, 2014 (http://www.bankinfosecurity.com/7-lessons-from-targets-breach-a-7658/op-1).

70 "October 2015: The End of the Swipe and sign Credit Card," *Wall Street Journal*, February 6, 2014 (http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/).

71 "Target Appoints New Chief Information Officer, Outlines Updates on Security Enhancements," Target press release, April 29, 2014 (http://pressroom.target.com/news/target-appoints-new-chief-information-officer-outlines-updates-on-security-enhancements).

72 Dominic Rushe, "JP Morgan Chase Reveals Massive Data Breach Affecting 76m Households," *The Guardian*, October 3, 2014. (http://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach).

73 Matthew Goldstein et al., "Hackers' Attack Cracked 10 Financial Firms in Major Assault," *New York Times*, October 3, 2014. (http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1&#).

74 Michael Hatamoto, "Lessons Learned from JPMorgan Chase Data Breach, as Attacks Increase," TweakTown, November 4, 2014. (http://www.tweaktown.com/blogs/Michael_Hatamoto/113/lessons-learned-from-jpmorgan-chase-data-breach-as-attacks-increase/index.html).

75 "JP Morgan to Accelerate Timeline for Cybersecurity Spending Boost," *Wall Street Journal*, August 3, 2015 (http://www.wsj.com/articles/j-p-morgan-to-accelerate-timeline-for-cybersecurity-spending-boost-1438641746).

76 Michael Riley and Jordan Robertson, "US Racing to Show Links to Elusive Hackers in JP Morgan Attack," *Bloomberg Business*, July 23, 2015 (http://www.bloomberg.com/news/articles/2015-07-23/u-s-racing-to-show-links-to-elusive-hackers-in-jpmorgan-attack).

77 "Lessons Learned from JPMorgan Chase Breach," PYMNTS.com, September 3, 2014 (http://www.pymnts.com/news/2014/lessons-learned-from-jpmorgan-chase-breach/#.VZ5e4EaDSRF); Michael Riley and Jordan Robertson, "Digital Misfits Link JP Morgan Hack to Pump and Dump Fraud," *Bloomberg Business*, July 21, 2015 (http://www.bloomberg.com/news/articles/2015-07-21/fbi-israel-make-securities-fraud-arrests-tied-to-jpmorgan-hack).

78 John Zorabedian, "What Healthcare Orgs Should Know about the Anthem Breach and HIPAA Compliance," SOPHOS Blog, February 26, 2015 (https://blogs.sophos.com/2015/02/26/what-healthcare-orgs-should-know-about-the-anthem-breach-and-hipaa-compliance/).

79 Charlie Osborne, "Anthem Data Breach Cost Likely to Smash $100 Million Barrier," *ZDNet*, February 12, 2015 (http://www.zdnet.com/article/anthem-data-breach-cost-likely-to-smash-100-million-barrier/); Charlie Osborne, "Health Insurer Anthem Hit by Hackers, up to 80 Million Records Exposed," *ZDNet*, February 5, 2015 (http://www.zdnet.com/article/health-insurer-anthem-hit-by-hackers-up-to-80-million-records-exposed/).

80 Brian Krebs, "China to Blame in Anthem Hack?" *Krebs on Security*, February 6, 2015 (http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/).

81 Lance Whitney, "Anthem's Stolen Customer Data not Encrypted," *CNET*, February 6, 2015 (http://www.cnet.com/news/anthems-hacked-customer-data-was-not-encrypted/).

82 Phil Britt, "5 Lessons Learned from Anthem Data Breach," eSecurity Planet, February 12, 2015 (http://www.esecurityplanet.com/network-security/5-lessons-learned-from-anthem-data-breach.html).

83 Sony Pictures Entertainment employee memo, December 8, 2014. (http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf).

84 Jeffrey Roman, "Sony's Breach Notification: The Details," Bank Info Security, December 16, 2014 (http://www.bankinfosecurity.com/sony-pictures-a-7682/op-1).

85 "A Breakdown and Analysis of the December, 2014 Sony Hack," Risk Based Security, December 5, 2014 (https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/).

86 David E. Sanger, Michael S. Schmidt, and Nicole Perlroth, "Obama Vows A Response to Cyber-Attack on SONY," *New York Times,* December 19, 2014.

87 "A Breakdown and Analysis of the December, 2014 Sony Hack," Risk Based Security.

88 Alexia Tsotsis, "Employee Data Breach The Worst Part Of Sony Hack," *TechCrunch*, December 16, 2014 (http://techcrunch.com/2014/12/16/hack-sony-twice-shame-on-sony/); Lisa Richwine, "Cyber Attack Could Cost Sony Studio as much as $100 Million," *Reuters,* December 9, 2014 (http://www.reuters.com/article/2014/12/09/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209); Ryan Gajewsk, "Lisa Kudrow on Sony Emails: Execs Need "Boundaries and Accountability," *The Hollywood Reporter*, December 13, 2014 (http://www.hollywoodreporter.com/news/lisa-kudrow-sony-emails-execs-757499).

89 Sanger, "Hackers Took Fingerprints of 5.6 Million Workers, Government Says"; David Auerbach, "The OPM Breach Is a Catastrophe," *Slate*, June 16, 2015 (http://www.slate.com/articles/technology/future_tense/2015/06/opm_hack_it_s_a_catastrophe_here_s_how_the_government_can_stop_the_next.html).

90 George Jackson, "Archuleta on Attempted Breach and USIS," *ABC 7*, July 21, 2014 (http://www.wjla.com/articles/2014/07/archuleta-on-attempted-breach-and-usis-105274.html).

91 Davis, "Hacking of Government Computers Exposed 21.5 Million People."

92 David Welna, "In Data Breach, Reluctance to Point the Finger at China," Northwest Public Radio, July 2, 2015 (http://nwpr.org/post/data-breach-reluctance-point-finger-china).

93 Michael Schmidt et al., "Chinese Hackers Pursue Key Data on US Workers," *New York Times*, July 9, 2014 (http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?hp&action=click&pgtype=Homepage&version=HpSum&module=first-column-region&region=top-news&WT.nav=top-news&_r=3).

94 US Office of Personnel Management, Office of the Inspector General, and Office of Audits, "Final Audit Report," Office of the Inspector General, November 12, 2014 (https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf).

95 Davis, "Hacking of Government Computers Exposed 21.5 Million People."

96 "The International Business Resilience Survey 2015," Marsh, October 2015 (http://uk.marsh.com/Portals/18/Documents/International%20Business%20Resilience%20Survey%202015-10-2015.pdf).

97 "Financial Firms Bolster Cyber Security Budgets," *Wall Street Journal,* November 14, 2014 (http://www.wsj.com/articles/financial-firms-bolster-cybersecurity-budgets-1416182536).

98 EU Cybersecurity Dashboard, A Path to a Secure European Cyberspace and Asia-Pacific Cybersecurity Dashboard, A Path to a Secure Global Cyberspace, published by the BSA | The Software Alliance (www.bsa.org).

99 Teren Bryson, "Big Security Breaches and How Big Data Can Prevent Them," Enterprise Networking Planet, June 25, 2015 (http://www.enterprisenetworkingplanet.com/netsecur/big-security-breaches-and-how-big-data-can-prevent-them.html).

100 Bryson, "Big Security Breaches and How Big Data Can Prevent Them," 2015.

101 David Burg et al., "US Cybercrime: Rising Risks, Reducing Readiness," PwC, 2014 (http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf).

102 "Net Losses: Estimating the Global Cost of Cybercrime," Center for Strategic and International Studies, June 2014 (http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf).

103 Nathan Eddy, "Insider Attacks Rise, Though Some Businesses Unaware of Risks," eWeek, June 29, 2015 (http://www.eweek.com/small-business/insider-attacks-rise-though-some-businesses-unaware-of-risk.html).

104 "NAIC Topics: CyberRisk," National Association of Insurance Commissioners (http://www.naic.org/cipr_topics/topic_cyber_risk.htm).

105 Steve Raptis, "Analyzing Cyber Risk Coverage," *Risk & Insurance*, March 13, 2015 (http://www.riskandinsurance.com/analyzing-cyber risk-coverage/).

READER SURVEY Please take a few moments to answer two questions Click here

CONNECT with our experts, your peers, and more thought leadership on this topic:
www.conferenceboard.org/cyber-risk-governance

Follow/join the conversation on Twitter #tcbCyber

OUR EXPERT

Andrea Bonime-Blanc is the CEO and founder of GEC Risk Advisory LLC, the global governance, risk, integrity, reputation, and crisis advisory firm serving executives, boards, investors, and advisors in diverse sectors worldwide.

Bonime-Blanc spent two decades as a senior executive in companies ranging from start-ups to Fortune 250, leading governance, legal, ethics, compliance, risk, crisis management, internal audit, information security, external affairs, and corporate responsibility functions, including at Bertelsmann, the global media company; Verint Systems, a "big data" technology company; and PSEG Global, a division of PSEG, the leading US energy and utility company. She began her career as an international project finance lawyer at Cleary Gottlieb Steen & Hamilton and has served as chair, audit committee chair, and a member of several boards for the past 25 years.

Bonime-Blanc is the author of *The Reputation Risk Handbook: Surviving and Thriving in the Age of Hyper-Transparency*, which the Wall Street Journal calls "The book on reputation risk." She writes The GlobalEthicist for *Ethical Corporation Magazine*. Recognized as an Ethisphere 2014 100 Most Influential People in Business Ethics and a 2014 Top 100 Thought Leader in Trustworthy Business, she recently also joined the Advisory Board of Spain's leading think tank, Corporate Excellence: Centre for Reputation Leadership and is a life member of the Council on Foreign Relations.

Bonime-Blanc was born and raised in Europe and holds a joint JD in law and PhD in political science from Columbia University. She is an adjunct professor at New York University and a frequent international keynote speaker.

Email: abonimeblanc@gecrisk.com
Twitter: @GlobalEthicist

LEARN MORE

RELATED RESOURCES FROM THE CONFERENCE BOARD

CEO and Executive Compensation Practices: 2015 Edition
August 2015

The Next Frontier for Boards: Oversight of Risk Culture
Director Notes, June 2015

Big Data Doesn't Mean 'Big Brother' (Implications for Legal and Risk Officers)
May 2015

The Board's Role in Cybersecurity
Director Notes, March 2014

WEBCASTS

Governance Watch, hosted in collaboration with Cleary Gottlieb Steen & Hamilton
December 17, 2015

Cyber Risk Communications (on-demand webcast)
April 23, 2015

THE CONFERENCE BOARD, INC. | www.conferenceboard.org
AMERICAS | +1 212 759 0900 | customer.service@conferenceboard.org
ASIA | +65 6325 3121 | service.ap@conferenceboard.org
EUROPE, MIDDLE EAST, AFRICA | +32 2 675 54 05 | brussels@conferenceboard.org
THE CONFERENCE BOARD OF CANADA | +1 613 526 3280 | www.conferenceboard.ca

PUBLISHING TEAM
Sara Churchville, Peter Drubin, Kathleen Mercandetti, Marta Rodin

R-1592-15-RR

ISBN: 978-0-8237-1196-3