

Cyber-attacks Jeopardize Companies' Pace of Innovation

All business investments require trade-offs between risk and reward. Does the interest rate on a new bond issue adequately compensate for the risk of default? Are the potential revenues from entering a new emerging market greater than the risk that the investments will be confiscated by a new regime? Does the value of oil extracted via deep-water, offshore drilling outweigh the chance of a catastrophic accident? Tough questions must be answered by weighing up the business imperatives against a calculation of the risk—and the greater the risk, the harder it is to make the case for investment.

Technology investments are no different. They, too, have always been a trade-off between risk and return. However, for enterprise technology, increased global connectivity is raising the stakes on both side of the equation. The commercial rewards from tapping into this connectivity are enormous, but the more tightly we are connected, the more vulnerabilities exist that attackers can exploit and the more damage they can do once inside. Therefore, when a manufacturer invests in a new product life-cycle management system, it is making a bet that the system will not enable the theft of valuable intellectual property. When a retailer invests in mobile commerce, it is betting that cyber-fraud won't critically damage profitability. When a bank invests in customer analytics, it is betting that the sensitive data it analyzes

2 BEYOND CYBERSECURITY

won't be stolen by cyber-criminals. The odds on all those bets appear to be shifting away from the institutions and toward cyber-attackers. They could swing decisively their way in the near future given most companies' siloed and reactive approach to cybersecurity.

Our interviews with business leaders, chief information officers (CIOs), chief technology officers (CTOs), and chief information security officers (CISOs) indicate that concerns about cyber-attacks are already affecting large institutions' interest in and ability to create value from technology investment and innovation. Potential losses, both direct and indirect, reduce the expected economic benefits of technology investments, as do the high cost and lengthy time frame required to build the defense mechanisms that can protect the organization against a growing range of attackers. In short, the models companies use to protect themselves from cyber-attack are limiting their ability to extract additional value from technology.

RISK OF CYBER-ATTACKS REDUCES THE VALUE OF TECHNOLOGY FOR BUSINESS

Concern about cyber-attacks is already having a noticeable impact on business along three dimensions: lower frontline productivity, fewer resources for information technology (IT) initiatives that create value, and—critically—the slower implementation of technological innovations.

Lower Frontline Productivity

Compared to even a few years ago, companies have many more security controls in place that limit how employees can use technology. They prevent users from installing applications on their desktops. They turn off USB ports and block access to consumer cloud services such as Dropbox. They prohibit executives from taking their laptops to certain countries or require that the laptop be reimaged on return. Layers of security controls can even make turning on a desktop or laptop a prolonged and frustrating process at some companies.

Cybersecurity teams may have good reason to implement these measures. Unknown applications can contain malware that antivirus programs can't detect. USB ports can be a source of infection, and both USB ports and consumer web services can be a mechanism for inappropriately copying sensitive data.

Employees, however, can see such measures as draconian. Worse, they can directly affect productivity and morale. The salesperson can't hand a USB stick with a video about a new product to a potential customer. The executive traveling overseas has to spend time copying her contacts onto another disposable phone before the visit and is unable to access Skype from her laptop to speak to her husband back home while away.

Security controls also limit frontline experimentation, which has been the source of so much of the value users derive from IT. In the 1980s, the first bankers who started using Lotus 1-2-3 to construct proforma models didn't have approval from corporate IT. Twenty years later, IT had no idea that small groups of executives had started using Blackberries to communicate with one another. Today, such innovations would be an explicit violation of most large companies' information security policies.

As a result of these factors, 9 out of 10 technology executives say cybersecurity controls have at least a moderate impact on end-user productivity; in the high-tech sector, 60 percent say the impact on productivity is a major pain point. A senior technology executive at a large bank said that if the CEO realized how many hours were lost as employees struggled with security controls, "he would hang us all." The CISO for a high-tech firm said he was convinced that the security controls he had to put in place contributed to talented engineers leaving the company.

Unfortunately, in many cases, restrictive security controls do not even solve the initial problem. They can lead users to circumvent corporate IT entirely, ironically increasing the risk dramatically. For example, at one securities firm, many bankers became so frustrated by long boot-up times and other controls that they stopped traveling with their IT-issued laptops. Instead, they just bought cheap laptops with no security controls and used free web-based e-mail services to communicate with each other.

Even government employees find workarounds. In a 2010 survey of U.S. federal officials, just under two thirds said security restrictions prevented them from getting information from some websites or using applications related to their jobs. The solution: using a nonagency device to access the information they need. In fact, more than half said they accessed information from home instead of from the office to get around the security controls.¹

¹ Rashid, Fahmida Y., "Cyber-security Hurts Federal Government Productivity, Survey Says," *eWeek*, September 30, 2010. www.eweek.com/c/a/Security/CyberSecurity-Cutting-Federal-Government-Productivity-Survey-744792.

4 BEYOND CYBERSECURITY

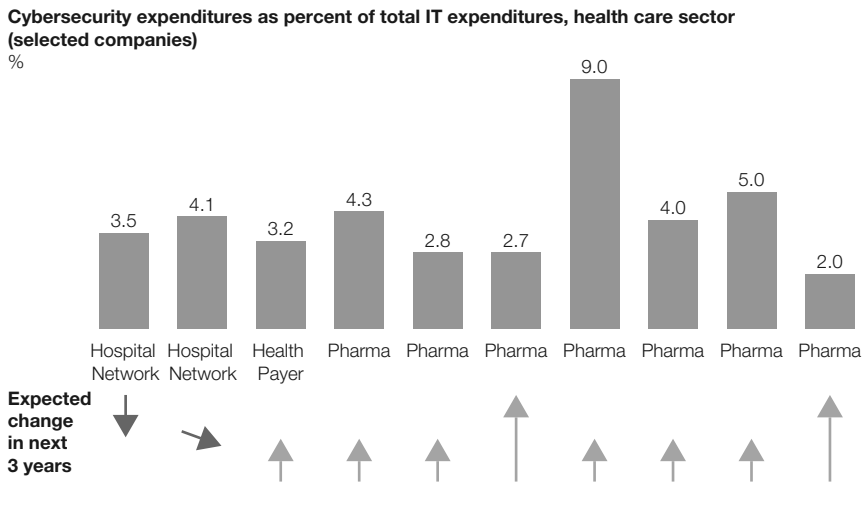
Less Money for IT Initiatives that Create Value

Direct cybersecurity expenditures are small compared to overall IT budgets and business revenues, but cybersecurity still diverts resources away from IT projects that create value because of the downstream effects it has on other IT functions such as application development and infrastructure.

It is hard to get a handle on how much companies spend protecting themselves from cyber-attacks. Some security-related functions, such as firewall management and identity and access management (I&AM), may be located in security budgets or may be found elsewhere in IT. This, as well as differences in security posture, means that there is a large range in how much companies spend on their cybersecurity function. Most commonly, cybersecurity organizations represent between 2 and 6 percent of an IT function's budget, though we know of some companies that dedicate as much as 8 or 9 percent—typically those with stringent requirements or that are in the middle of large programs to improve their security capabilities (Figure 1.1).

Although cybersecurity is growing more quickly than other areas of enterprise IT, direct cybersecurity expenditures do not appear to be that big an issue for most companies. While some of the largest banks and telecommunications firms can spend several hundred million dollars

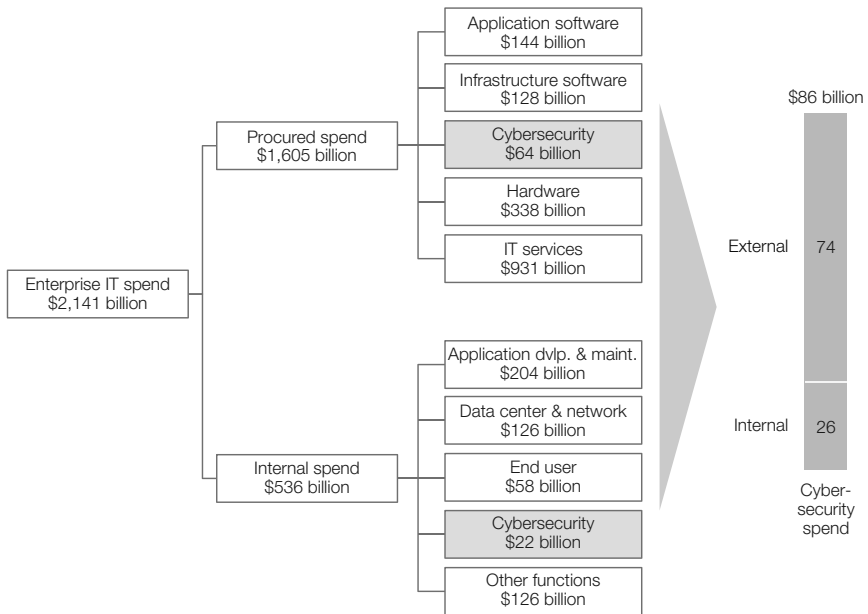
FIGURE 1.1 **Cybersecurity's Share of the Overall IT Budget Can Vary Widely—Even within One Sector**



on cybersecurity, many other large companies spend much smaller amounts. For example, a \$25 billion manufacturing company that devotes 2 percent of revenues to IT and 5 percent of that IT spend to cybersecurity would be spending just \$25 million—a financial nit. Of the \$2.1 trillion in global enterprise IT spend, only about \$90 billion falls into the cybersecurity budget, of which three quarters goes to hardware, software, and services, and the other quarter on internal labor (Figure 1.2).

Many technology executives believe that they already spend enough to protect their companies. Slightly more than half of those we interviewed said their company spent about the right amount on cybersecurity, while only about a third said that their company spent significantly too little. Some CISOs told us that they received whatever budget they asked for. For them, the constraint is the lack of available talent rather than money. Cisco estimates that the gap between security roles that need filling globally and the talent available may be as high

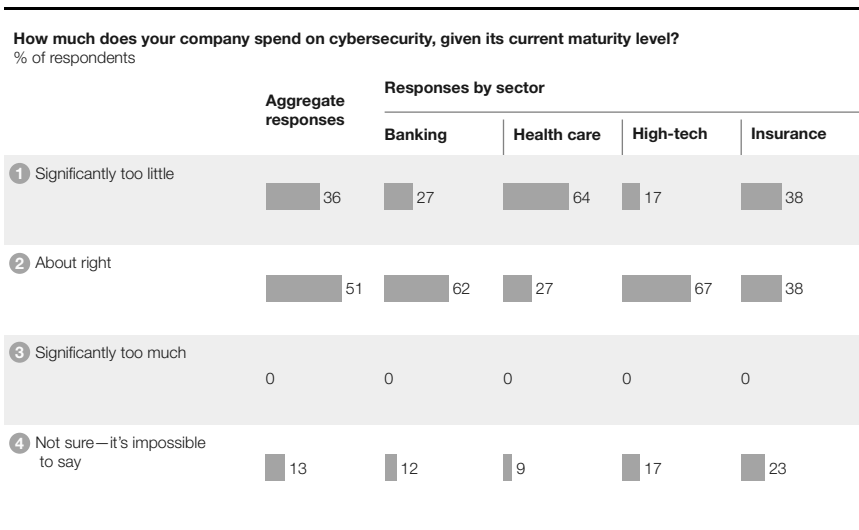
FIGURE 1.2 **Cybersecurity Spend Is Less than \$100 Billion of Total Business IT Spend of \$2 Trillion**



Note: Excludes telecommunications services.
Source: Gartner, Computer Economics, McKinsey & Company

6 BEYOND CYBERSECURITY

FIGURE 1.3 **Half of Technology Executives Believe They Spend Enough on Cybersecurity**



as 1 million professionals.² Almost all CISOs told us they could get approval for more head count but cannot hire quickly enough to fill the slots that they have.

CISOs' perceptions of their budgets did vary significantly by sector. More than 60 percent of financial services and high-tech companies said they had big enough cybersecurity budgets. But less than 40 percent of insurance companies and only about a quarter of health care companies felt the same. Nearly two thirds of health care technology executives say their company's cybersecurity budgets are significantly too small (Figure 1.3).

Cybersecurity's cost increases dramatically when it includes the indirect security activity undertaken outside the security organization itself. Not only do many organizations perform some security-related functions outside IT security, but many actions the security organization takes create unfunded mandates for application development, infrastructure, and the broader business groups. Developers spend months or years rearchitecting applications to meet security standards; network teams spend tens of millions of dollars reconfiguring networks to make them more secure; system administrators devote countless hours to applying security patches across tens of thousands

²Cisco 2014 Annual Security Report, January 2014.

of servers; and after years of infrastructure optimization, many IT departments can provision a server in hours or days, but then spend three or four weeks doing the security-related configuration, with all the cost that implies.

We asked CIOs, CTOs, and CISOs to estimate how much of the nonsecurity IT budget is actually spent on security. Quite frankly, many had no clue but were sure it was large. Many of those that offered a figure said it could be 25 to 30 percent of the budget, which would imply that the combination of direct and indirect security activity is consuming a third of IT budgets.

In a world where business aspirations for technology innovation bump up against constrained IT budgets, where business leaders complain bitterly about the cost of developing and running applications, and where there are pitched battles about which projects IT can afford to do each year, this means security requirements are diverting significant resources away from IT that creates value.

Slower Adoption of New Technologies

CIOs and CTOs have a crowded innovation agenda. Senior executives, customers, and ultimately shareholders expect them to roll out new capabilities in areas including cloud computing, big data, e-commerce, the Internet of Things, mobile commerce, and enterprise mobility.

Almost everyone told us that security is often the bottleneck in implementing new technologies. It takes real work to assess vulnerabilities in new vendor offerings and to figure out how to engineer a secure solution. For example, the security team has to assess new types of mobile devices to determine what data they store locally and how strong the authentication mechanisms are that prevent unauthorized access. It has to assess new external web-facing functionality to see whether it creates an entry point into customer-facing systems that attackers can exploit. It also has to analyze how an attacker would penetrate a new capability, identify potential vulnerabilities, and engineer controls that are acceptable in terms of cost and convenience.

All these tasks take time, especially for relatively new technologies that have not been extensively pressure tested in the real world, and can significantly delay the introduction of new capabilities. The CISO of a medical devices company explained that it took a year to work out how to integrate the network-connected devices into an operating room environment in a secure way.

8 BEYOND CYBERSECURITY

For many technologies, the lag time is relatively small—at least so far. IT executives told us that security requirements added less than three months to the implementation of big data analytics, mobile servicing, online servicing, and online payments. Many explained, though, that the business imperatives were such that there was no alternative to rolling out new technologies, even if the security issues were still unclear.

The impact of incorporating security measures is felt most keenly in cloud computing and mobile (Figure 1.4). On average, enterprise mobility capabilities were delayed by more than six months and public cloud capabilities far longer, with many companies saying they wouldn't put sensitive data in the public cloud in the foreseeable future because of security concerns.

Delays in enterprise mobility are driven largely by what many CISOs perceive as a rickety enterprise mobile security model. A financial services CISO told us, "We've started to experiment with mobile devices; however, the delay has been because of the number of potential threats they create." The CISO of a hospital network faces similar challenges. "We've got thousands of physicians who all want access," he said, "but who also want to do their own thing. We have had to make sure everything is going between them securely, so naturally a few of the systems have been delayed."

The result is that most organizations have focused on a relatively narrow set of mobile capabilities such as e-mail and calendar synchronization, that give users only a small fraction of the capabilities they would have on a laptop.


Delays in the use of the public cloud are driven by multiple factors. While some executives highlighted reasons unrelated to security (e.g., compliance considerations or "not invented here" syndrome), a few explicit security considerations came up frequently in interviews, specifically, a perceived lack of transparency into many providers' security models, a sense that multitenant public cloud architectures lack the defense in depth that a well-designed local environment provides, and uncertainty about how contract terms and conditions can be crafted to address cybersecurity concerns.

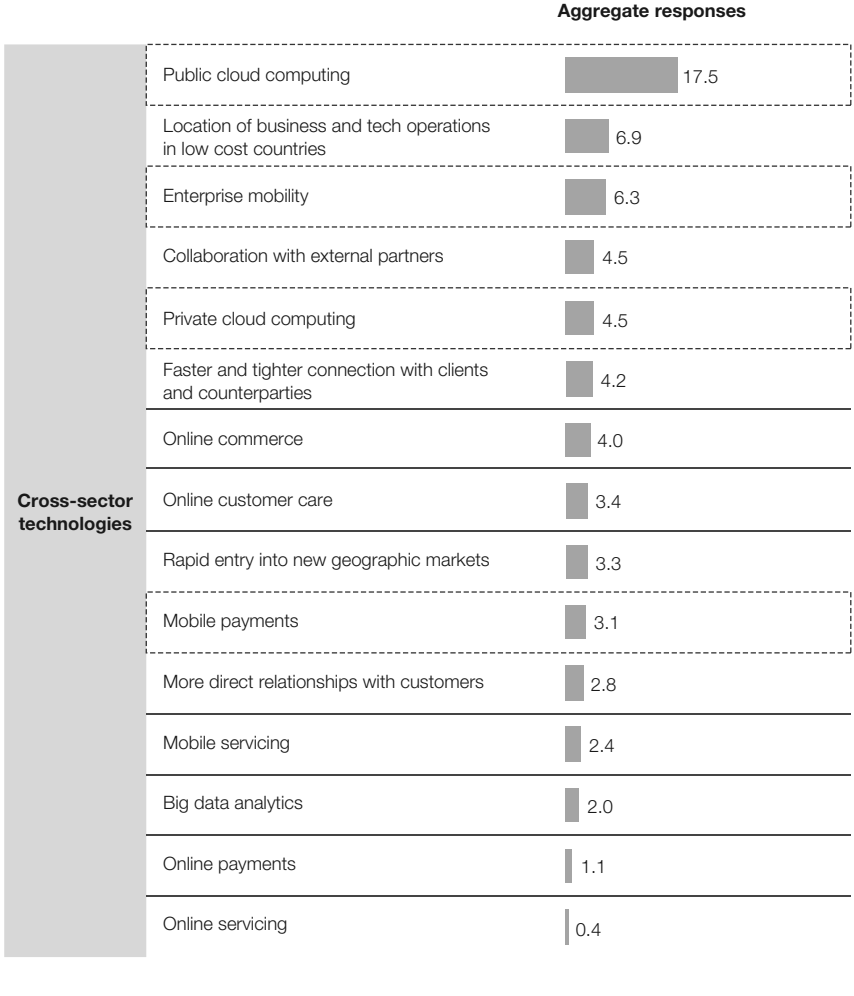
As a result, 60 percent of executives surveyed said that security concerns were delaying their institution's use of cloud environments by a year or more. As we'll see in the next chapter, such delays, when spread across the global economy, could have major economic implications.

FIGURE 1.4 **Companies Are Most Concerned about Security Implications of Mobile and Cloud Computing**

How many months delay do you think that concern over cyber-attacks will create for the following innovations for your institution? (participants were asked to select at least three innovations)

Delay in months

 Most frequently mentioned technologies



Many CIOs also worry that concerns about cyber-attacks could slow down adoption of the “Internet of Things”—the connection of devices from refrigerators and thermostats to automobiles and heavy machinery to the Internet. It’s easy to understand the trepidation in

connecting cars to the Internet if attackers could exploit those connections to wreak havoc or even just monitor movement. Cybersecurity researchers in Israel have already proven they can take over a car remotely.³

Regulatory scrutiny can add further delay to the rollout of technology innovations. One bank underwent 98 regulatory audits in 2013. When a company has to explain how a new technology can be secured to dozens of different regulators, each with a different agenda and questions, the pace of innovation can slow dramatically.

THE RISKS ARE HIGH FOR EVERYONE, EVERYWHERE

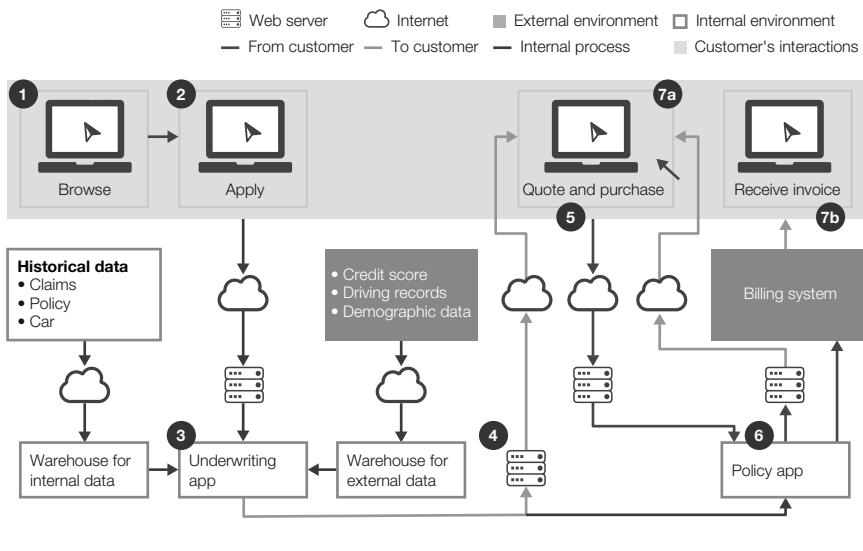
Digitization may be a buzzword in technology circles, but it also represents a real and important dynamic: the pervasive migration of economic value online. Institutions are automating business processes, establishing networked connections with customers and suppliers, and manipulating valuable intellectual property in digital formats. Already today, manufacturers can bid on online platforms for basic materials in fully automated real-time enterprise-scale online auctions. Hospitals increasingly store patients' medical records online so that they can be shared easily, ensuring better collaboration, more comprehensive storage of results, and even enabling remote treatments. Much securities trading never touches a human hand; it is driven entirely by algorithms and happens in milliseconds (or even microseconds in some cases).

Take an example as prosaic as car insurance; every step in the process has become dependent on technology, and often on networks talking to each other (Figure 1.5).

- The customer browses the web for different providers, reading reviews and ratings left by other customers. She may also go to a third-party aggregator site to get the best deal.
- To get a quote, she fills in some basic information online, which carriers can match against a variety of public and proprietary databases to gauge the risk (e.g., public crime statistics for the postcode, and the insurer's own database on the reliability of a particular model of car).

³Bigelow, Pete, "Israeli Cyber-security Researchers Remotely Hack a Car," *autoblog*, November 8, 2014. www.autoblog.com/2014/11/08/car-remotely-hacked-israel-cyber-security.

FIGURE 1.5 **External Connectivity Is Integral to Most Businesses—Auto Insurance Example**



- Next, she fills out a full application—again all done online via secure e-mail and, for the most sophisticated, using a digital signature—and pays via a secure website. The policy and all the details are e-mailed to her.
- When she has to make a claim after a minor accident, the insurer may already be fully aware of what's happened thanks to the car's telematics that are constantly reporting back information to the manufacturer and that are then passed on to the insurer. The company may even have already automatically alerted its preferred body shop to book the car in for repairs.

The value yielded for both insurer and customer is immense, in the form of cost reductions, new customer offerings, more intimate customer relationships, and better customer service. What's true for car insurance is true for almost every industry imaginable.

Companies Must Contend with a Wide Range of Risks and Threats

As digitization continues to increase, companies face a broad range of business risks associated with cyber-attacks.

Fraud As ever more financial transactions occur online, the opportunity for cyber-fraud is exploding. Cyber-criminals can open up dummy credit accounts to purchase goods and services fraudulently. Or they can take control of legitimate accounts in order to empty them of funds. Any assessment of cyber-crime's impact is necessarily imprecise, but to take one estimate, McAfee's recent report with the Center for Strategic and International Studies calculated cyber-crime to be worth 0.8 percent of world gross domestic product (GDP).⁴

Loss of Customer Information Customer data such as social security numbers, financial records, and medical records can be used by hackers to commit cyber-fraud or sold on the black market to others with the same aim. The information contained in electronic health records, for example, can be used to bill insurance carriers for care that was never provided. Prescription data can be used to fulfill prescriptions from multiple pharmacies so that the surplus medicines can be resold. In fact, health records often contain enough information to open a new credit card or other financial accounts, leading to more direct theft. Criminals can also sell celebrities' medication information to unscrupulous media outlets or, potentially, use embarrassing medical information to blackmail patients. As a result, the street cost for a stolen medical record can be as high as \$500, compared to around \$25 for a stolen U.S. identity consisting of a social security number and date of birth, or just a dollar or two for a "stale" credit card number, that is, one that may be out of date.⁵

A large breach of customer data represents customer inconvenience, loss of customer trust, and significant remediation costs. In May 2014, eBay revealed that attackers compromised the user names, passwords, phone numbers, and physical addresses of 233 million accounts, forcing the company to request that all users change their passwords.⁶ Since then, polling in the United Kingdom has indicated that nearly half of customers there would be less likely to use eBay in

⁴ Center for Strategic and International Studies & McAfee, *Net Losses: Estimating the Global Cost of Cybercrime*, June 2014. www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

⁵ RSA, "Cybercrime and the Healthcare Industry." White paper, September 16, 2013. www.emc.com/auth/collateral/white-papers/h12105-cybercrime-healthcare-industry-rsa-wp.pdf.

⁶ McGregor, Jay, "The Top 5 Most Brutal Cyber Attacks of 2014 So Far," *Forbes*, July 28, 2014. www.forbes.com/sites/jaymcgregor/2014/07/28/the-top-5-most-brutal-cyber-attacks-of-2014-so-far.

the future as a result of the attack.⁷ In an earnings call later in 2014, eBay CEO John Donahoe said that because the attack had affected commerce volumes, the company had lowered 2014 sales targets by \$200 million.⁸ In addition to the impact on customers, remediating a breach can be expensive. The Ponemon Institute estimated that the average breach costs \$3.5 million,⁹ but bills for the largest can easily run into hundreds of millions of dollars. U.S. retailer Target told investors that the costs relating to its 2013 breach of 70 million customer records could include reimbursing fraud, card reissuance, civil litigation, governmental investigation, legal fees, and investigative fees, in addition to the incremental operating and capital expenditures required for remediation.¹⁰

Loss of Intellectual Property Much of the value of modern corporations rests in intellectual property (IP) rather than in tangible assets such as machines or buildings. Product designs, manufacturing processes, marketing plans, even film scripts—IP is a tempting target, and with so much of it now kept in digital formats, it is ripe for cyber-attack. The Report of the Commission on the Theft of American Intellectual Property estimates that cyber-enabled IP theft costs the U.S. economy \$300 billion annually.¹¹

Disadvantaged Negotiation Executives typically communicate online via e-mail or instant message, even when discussing sensitive negotiations. This might be about a possible merger or joint venture, a new sourcing deal, extraction rights—almost nothing is deemed out of

⁷ Clearswift, “eBay Cyber Attack Fallout—Consumer Response: Half of UK Adults Have Lost Trust in eBay since Cyber Attack.” Press release, May 23, 2014. www.clearswift.com/about-us/pr/press-releases/ebay-cyber-attack-fallout-consumer-response.

⁸ Mac, Ryan, “eBay CEO: Sales, Earnings Affected by Cyberattack Body Blow in Challenging Second Quarter,” *Forbes*, July 16, 2014. www.forbes.com/sites/ryanmac/2014/07/16/ebay-ceo-sales-earnings-affected-by-cyberattack-body-blow-in-challenging-second-quarter.

⁹ Ponemon, “Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis.” Press release, May 5, 2014. www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis.

¹⁰ Target, “Target Provides Update on Data Breach and Financial Performance.” Press release, January 10, 2014. <http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance>.

¹¹ National Bureau of Asian Research, “The IP Commission Report,” Report of the Commission on the Theft of American Intellectual Property, May 2013. www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

scope for e-mail. Yet information about how a company is approaching a deal, for example, the maximum amount it is willing to pay, can be damaging in the wrong hands. A petroleum exploration company calculated that the impact of losing the data on what it was willing to pay a particular government for extraction rights could run into billions of dollars and was therefore one of its most important enterprise risks. Senior managers talked in the boardroom of the “billion-dollar e-mail” with no sense of hyperbole.

Disclosure of Sensitive Management Discussions Every management team has to have confidential discussions. Naturally, information about how management thinks about future product plans could be extremely harmful if accessed by the wrong competitor. In addition, in the process of formulating and executing strategy, managers often share frank opinions about their customers, their own products, their regulators, and their employees that could harm any number of relationships if they were publicly disclosed. As an example, the U.S. State Department believes that unvarnished opinions about foreign leaders included in the documents Bradley (now Chelsea) Manning downloaded to a USB drive and released via WikiLeaks have jeopardized ties to allies.¹²

Business Disruption In late 2012 and early 2013, the al-Qassam Cyber Fighters launched a series of distributed denial of service (DDoS) attacks designed to overwhelm U.S. banks’ Internet banking presences, rendering them unavailable to customers. In the end, even though disruption was relatively limited, the attacks succeeded in doubling downtime for online banking applications in early 2013.¹³

DDoS attacks are annoying and inconvenient but CISOs tend to worry more about the sort of destructive attacks that go beyond delays and outages and that compromise financial transactions, interfere with electronic medical devices or shut down manufacturing operations. An attack on Saudi Aramco that deleted data from many hard drives significantly hurt business operations for more than two

¹²Serrano, Richard S., “Manning’s Leaks Jeopardized U.S. Ties to Allies, Diplomat Testifies,” *Los Angeles Times*, August 1, 2013. <http://articles.latimes.com/2013/aug/01/nation/la-na-manning-trial-20130802>.

¹³Schwartz, Mathew J., “Banks Hit Downtime Milestone in DDoS Attacks,” *Information Week*, Dark Reading, April 4, 2013. www.darkreading.com/attacks-and-breaches/banks-hit-downtime-milestone-in-ddos-attacks/d/d-id/1109390.

weeks.¹⁴ Aramco said that “the main target in this attack was to stop the flow of oil and gas to local and international markets.”¹⁵

Legal and Regulatory Exposure In many sectors, losing sensitive customer data has serious legal implications. In health care in the United States, for example, the Health Insurance Portability and Accountability Act (HIPAA) mandates fines of \$100 to \$50,000 per record up to a total of \$1.5 million for a single event. Class action lawsuits have the potential to be even more damaging. The California Attorney General’s office has valued lost medical data at \$2,000 per record. Sutter Health, a not-for-profit northern California health system with revenues of \$10 billion, had one desktop computer stolen via the nontechnical method of throwing a rock through a window. The company had begun rolling out an encryption program but had yet to get to desktop devices. Clinical data for almost 1 million patients and basic data for more than 3 million patients was compromised. The ensuing lawsuit ran to \$4.25 billion. Thankfully for Sutter, the case was eventually dismissed three years later because the plaintiffs couldn’t demonstrate that criminals had been able to make use of the data, but the suit still consumed management attention for all that time.¹⁶

These risks stem from a set of attackers whose capabilities have improved dramatically over the past several years.

- Organized crime groups have sought to make a business from cyber-attacks, not only conducting online fraud, but also stealing customers’ personal information, which they can integrate into their own data warehouses and use for identity theft.
- There has been much debate and discussion about cyber-warfare, but state-sponsored actors have focused overwhelmingly on espionage either to inform national strategy or to obtain valuable IP that can be passed on to favored domestic companies.
- Hacktivists such as Anonymous and Lulzsec seek to disrupt and embarrass government agencies and companies whose policies and practices they oppose.

¹⁴ Bronk, Christopher, and Eneken Tikk-Ringas, “The Cyber Attack on Saudi Aramco,” *Survival: Global Politics and Strategy*, 55(2), April–May 2013, pp. 81–96.

¹⁵ “Aramco Says Cyberattack Was Aimed at Production,” *New York Times*, December 9, 2012. www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html.

¹⁶ Kolbasuk McGee, Marianne, “Sutter Health Breach Suit Dismissed,” *Data Breach Today*, July 22, 2014. www.databreachtoday.com/sutter-health-breach-suit-dismissed-a-7095.

In addition, insiders are an increasingly important threat. Technology executives emphasized that the easiest way to get access to sensitive data is to badge into the building in the morning and log in to secure systems using valid credentials. Employees or contractors can be motivated by simple greed or by resentment at having been passed over for a promotion. They may be compromised by an outsider—one criminal organization used threats against a developer's family to coerce him into inserting code that authorized illicit payments into an application. Employees may also convince themselves that they are not even committing a crime, for example, when they download customer lists before leaving to work for a competitor. Perhaps most importantly, employees and contractors have context—they know where to find the most sensitive information and often will have the business insight required to use it effectively.

The Risks Are Strategic

Faced with so many potentially damaging outcomes, technology executives across sectors and regions are highly concerned about the risk of cyber-attacks. Roughly two thirds described it as a significant issue that could have major strategic implications over the next few years. Typically, they explained their perspective in terms of the risks laid out earlier: lost intellectual property, lost customer data, or disruptions to business operations. A relatively small percentage, about 10 percent, described the risk of cyber-attack as existential and believed it could “turn out their lights sometime in the next five years.”


Turning out the lights would mean either a devastatingly destructive attack or, more likely, an irreparable breakdown of customer trust. The CISO for one social media company said, “If we lose customer trust, then the product itself goes away.” The CISO for a large financial institution said that he was worried about attacks that would compromise transaction data so comprehensively that it would be impossible to unwind.

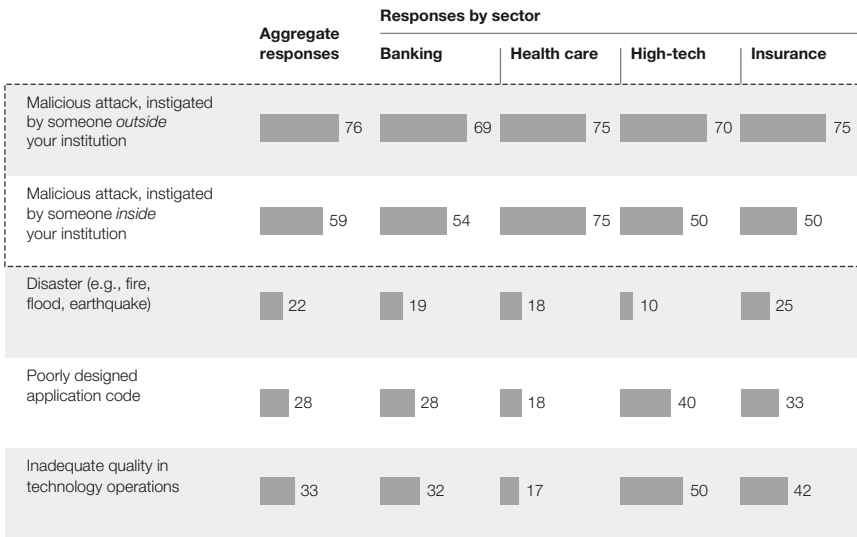
About a quarter of the people we interviewed believed cyber-attacks are a normal risk of doing business. These executives placed cyber-attacks in the context of other risks facing their institutions, such as liquidity crises for banks or physical disasters for manufacturing companies.

Interestingly, not one person we interviewed agreed with the statement, “The risks of cyber-attacks are overblown. Our institution

FIGURE 1.6 **Cyber-attacks Pose a Greater Risk than Other Technology Risks**

What type of technology risks are most likely to have a strategic and negative impact on your business?
 % of respondents who rated response in their top two concerns

 Most frequently cited risk



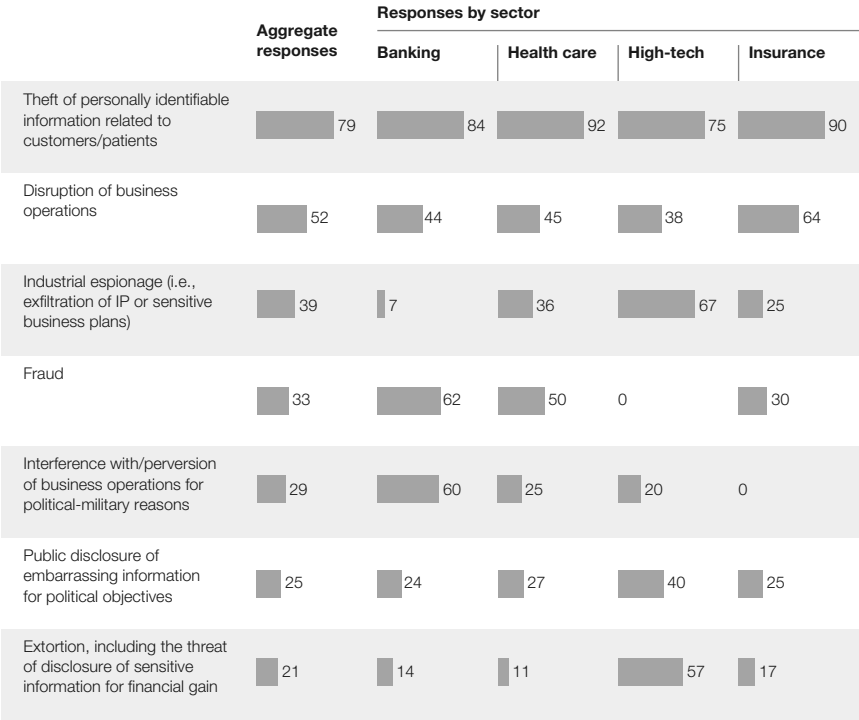
has the issue well in hand.” In fact, cyber-attacks were a much greater concern than other types of technology risk. Nearly three quarters of respondents said that external cyber-attacks were one of their top two technology risks. Nearly 60 percent said the same about insider threats. Other technology risks were rated in the top two less than a third of the time. These included disaster, poorly designed application code (which cost Knight Capital \$440 million¹⁷), and inadequate quality in technology operations such as mistakes in server configuration that crash important applications (Figure 1.6).

Although the level of concern varied barely at all across sectors, the types of risks each sector worries about are quite different (Figure 1.7). Broadly speaking, services companies prioritize theft of customer data and interference with business operations, while product companies prioritize industrial espionage. For example, barely any financial institutions cited industrial espionage as a prime concern. Investment

¹⁷ Popper, Nathaniel, “Knight Capital Says Trading Glitch Cost It \$440 Million,” *New York Times*, August 2, 2012. <http://dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million>.

FIGURE 1.7 **All Companies Are Worried about Customer Data Theft, but Their Next Priority Varies by Sector**

Which business impact from malicious cyber-attacks are you most concerned about?
 % who rated response as 1st or 2nd biggest concern



banking CISOs told us that although IP was incredibly important to their business, its structure and format limited the impact of any given breach: trading algorithms were immensely valuable, but the IP was distributed across many algorithms on many product desks (e.g., currencies, interest rate swaps) so the loss of any one algorithm would have only so much financial impact. In addition, many of the algorithms changed rapidly, so any IP stolen would have far less value in just a matter of months. Some retail banking CISOs placed an even lower value on their company’s IP; one said, “Checking products aren’t all that different from each other and don’t change that quickly.”

Instead, banks worry about fraud and any breaches that might compromise either corporate or consumer customer data—they considered

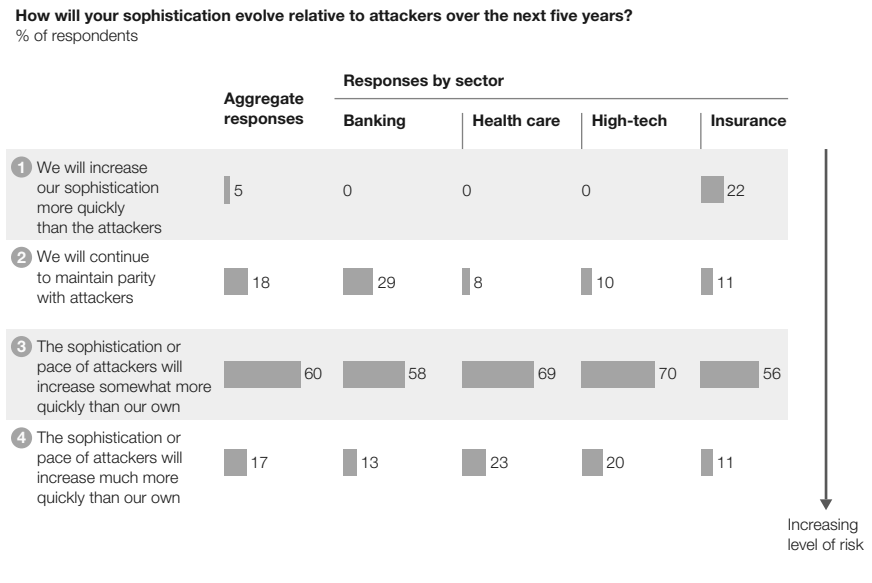
this to be a core part of their institutions' value proposition. Many also expressed a high degree of concern about politically motivated attacks on the integrity of financial transactions.

High-tech companies, by contrast, are sharply focused on IP loss, especially process-related IP. Detailed insights into a product become widely available the moment it hits the market and competitors apply tear-down techniques to it, but the detailed manufacturing specifications (e.g., what temperature to bake a component at) can stay secret for years.

DEFENDERS ARE FALLING BEHIND ATTACKERS

Technology executives believe almost universally that it is the attackers, irrespective of type, who will not only maintain their lead over the institutions they target but actually increase that lead over the next few years (Figure 1.8). More than three quarters said that the sophistication or pace of attacks would grow faster than their own defensive capabilities, and nearly a fifth believe that the attackers' advantage would increase significantly faster. The stark consensus: the defenders believe they are losing ground.

FIGURE 1.8 Executives Believe Attackers Will Increase Their Lead



Insurers were the most confident in their own ability. Slightly more than a fifth of insurance interviewees believed that they would advance more quickly than attackers (although that is, of course, still a minority), while nobody at all outside of insurance had this view about his or her company. This may be partly because cybersecurity is still relatively nascent in insurance—when you're far behind, those first few steps can feel like significant progress.

Interviewees had a range of explanations for their concerns about falling behind attackers.

Technology Changes Favor Attackers

Almost everyone accessing corporate systems used to do so from a desktop computer owned by the corporation and physically located within a company office. Information security professionals focused on defending the perimeter and keeping attackers off the corporate network. Today's world is very different. There are endless ways into networks, vastly expanding each institution's exposure. Customers can access sophisticated applications via the Internet; business partners can connect directly to the corporate network, which enables tighter collaboration but adds to the external interfaces; and users expect to access everything no matter where in the world they happen to be. The idea of an invulnerable "perimeter" is as old-fashioned as a moat. Companies are also littered with older IT systems that may rely on outdated and vulnerable technology and that are retired very slowly. Attackers therefore have a growing array of opportunities to exploit.

Attacker's Jurisdictional Advantage

In the physical world, if a criminal keeps committing crimes, the odds are that he will eventually get caught. All it takes is one slip-up, one caper that puts him in the wrong place at the wrong time. For a cyber-criminal operating from a country not focused on prosecuting cyber-crimes, the story is very different. Rather than increasing his risk, each incremental attack sharpens his capabilities and makes him smarter about the company he's attacking. "The attacker has to be right only once to do a lot of damage but can get away with being wrong time after time," said a CISO. "We have to be right every single time."

The Resources Available to State-Sponsored Attackers

Several CISOs told us that although they have a fighting chance in defending themselves against criminals and hacktivists, they cannot compete with the resources that a nation-state can bring to bear in cyber-espionage. Not only are some states technologically advanced, but they can also afford to devote dozens or even hundreds of people to probing just one company's technology environment for vulnerabilities.

State-Level Capabilities Being More Widely Disseminated

Sophisticated attack strategies developed by states don't necessarily stay exclusively in their hands. Cyber-warfare unit leaders may pass on attack strategies to groups they believe might be politically useful. More junior members meanwhile may seek to augment their salaries by freelancing the skills they've developed. Kristin Lord of the Center for a New American Security said, "We've already seen indications of states using criminal groups as proxies for attacks. We also know that countries like North Korea are aggressively trying to develop their cyber capabilities. The open black market, which already exists in the criminal world, is therefore a big concern. It provides a place for states and criminals to find each other."¹⁸

The Global Market for Cyber-attacks

Just as the Internet has created a global market for collectable trinkets, it has also begun to excel at connecting buyers and sellers of the tools required to launch sophisticated cyber-attacks—not just the states and criminals Kristin Lord referred to, but a range of players. The Rand Institute reported that researchers who discovered a new "zero-day" vulnerability in a popular piece of software¹⁹ could earn, in some cases, millions of dollars by selling this knowledge to cyber-criminals.²⁰

¹⁸ Walsh, Eddie, "The Cyber Proliferation Threat," *The Diplomat*, October 6, 2011. <http://thediplomat.com/2011/10/the-cyber-proliferation-threat>.

¹⁹ A zero-day exploit describes a previously unknown vulnerability that an adversary has discovered for which there is no current threat signature, patch, or countermeasure. All organizations are vulnerable to these. Once an attacker's use of a zero-day exploit is discovered, it can take weeks or months for a software patch to be developed and deployed to close the vulnerability.

²⁰ Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," Rand Corporation, 2014.

Institutions Lack the Insights to Make Intelligent Cybersecurity Decisions

Risk management is at the core of cybersecurity. CISOs seek to put in place a set of controls (e.g., encryption, authentication) that deliver the greatest reduction in the likelihood or impact of important risks (e.g., loss of IP, theft of customer data) at the lowest cost and with the least business disruption. Unfortunately, the overwhelming majority of large institutions simply don't have the required risk management capabilities to make intelligent decisions about cybersecurity investments and policies. They don't understand the assets they need to protect, the attackers they face, the full set of defense mechanisms they could implement, or the implications of each of these mechanisms. As a result, they see too little reduction in risk, coming at too high a cost in terms of both business impact and expenditure.

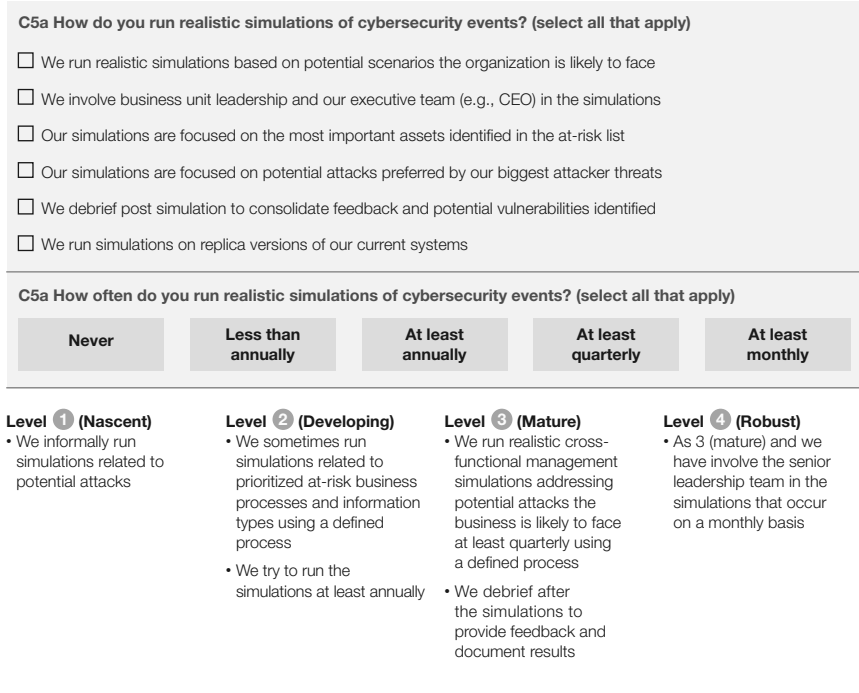
To get a better understanding of where organizations stand in their cybersecurity capabilities, we asked more than 60 Global 500 institutions to complete our Cyber-Risk Maturity Survey (CRMS). The survey measures an organization's risk management practices across eight domains—specifically, how well it understands:

- Its attackers.
- The assets it needs to protect.
- The vulnerabilities in its environment.
- Its residual risk and risk appetite.
- The range of potential controls it could put in place.
- How effective it is in assessing the cost and impact of controls it might put in place.
- How thoroughly it can implement the decisions it makes.
- The quality of cybersecurity governance and organization.

The CRMS was developed together with CISOs from leading institutions and minimizes subjectivity. Rather than asking companies to rate themselves on how well they fare in a particular area or measuring specific technologies, architectures, or controls, it asks instead whether and how frequently the company performs 28 specific activities and then grades it on a numerical scale to allow for comparisons (Figure 1.9).

FIGURE 1.9 **Cyber Risk Maturity Survey: Fact-Based Questions Lead to Maturity Rating**

Example: Practice C5: Identify vulnerabilities from simulations



There are four levels of cyber-risk management maturity:

1. *Nascent*. These are the companies that are doing their best but lack any rigid protocols or centralized security systems in place beyond the bare minimum. They have no defined single point of accountability or a clearly defined escalation path to top management.
2. *Developing*. Companies have a qualitative framework for evaluating and mitigating cyber-risks. The governance model is consistent across the company, with a single point of accountability in each business unit and a defined reporting line to top management.
3. *Mature*. There's a quantitative approach for evaluating and a qualitative approach for mitigating cyber-risks. The cybersecurity

governance model is well defined, with a single point of accountability within a business unit that owns the risks and decision making.

4. *Robust*. A robust quantitative approach for evaluating and mitigating cyber-risks is in place, and clearly identified individuals are accountable for the cybersecurity of each asset.

Companies Have a Long Way to Go to Reach Maturity The survey results were sobering. More than 9 out of 10 organizations have only nascent or developing maturity, and not one could be described as robust overall (Figure 1.10).

Only one respondent was mature or better in every practice area, and more than two thirds were only “nascent” or “developing” in at least half the areas. Looking at the scores in aggregate, only one area—knowing your systems and people—had an aggregate score of more than 3, indicating it was “robust” in more than half of the companies. Most practices were toward the low end of “developing,” with practices around knowing your vulnerabilities being particularly weak (Figure 1.11).

FIGURE 1.10 **Cybersecurity Risk Management Maturity Is Low**

Distribution of overall maturity scores
 % of participating organizations

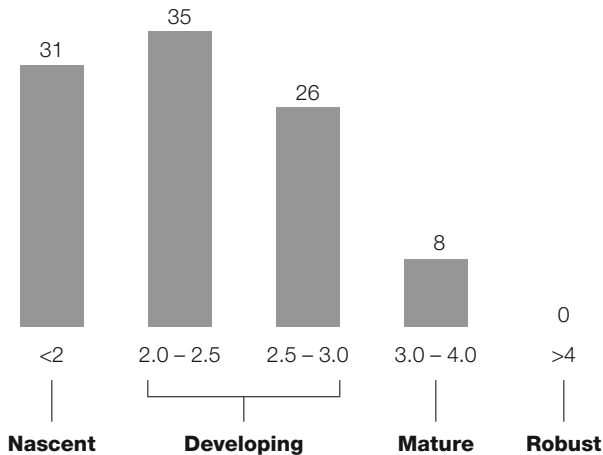
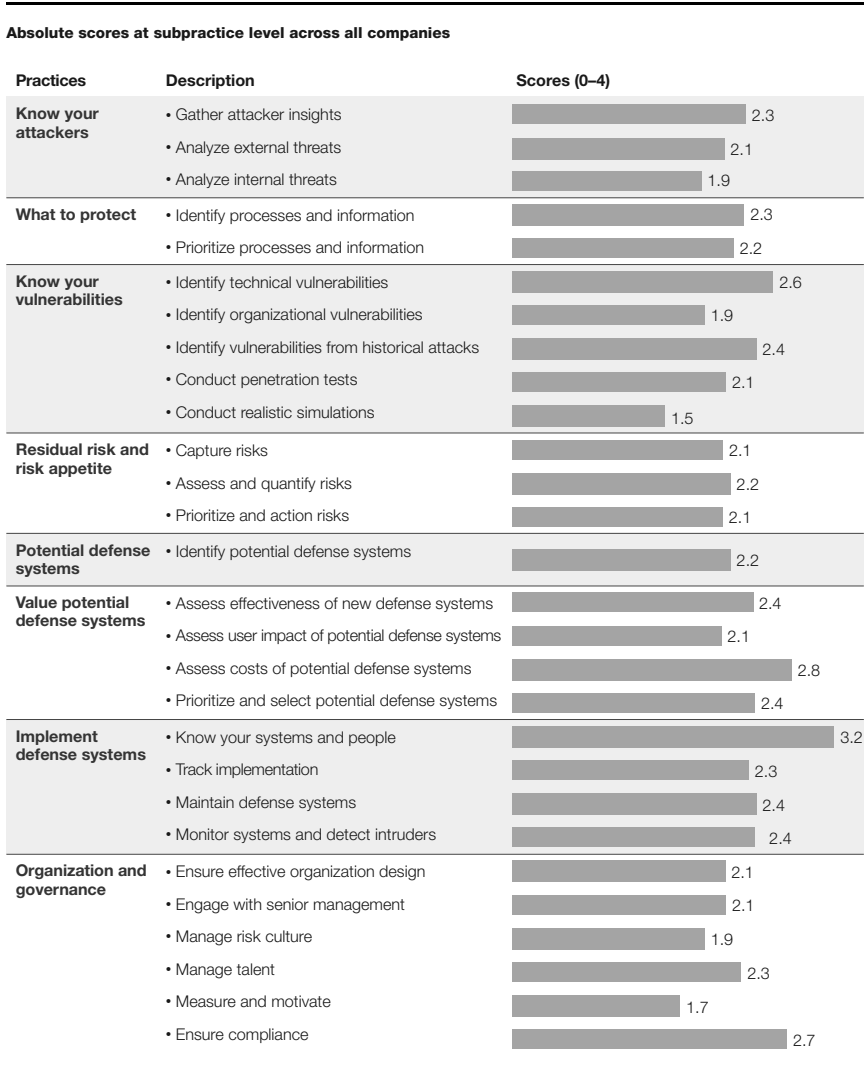


FIGURE 1.11 **Only One Practice Rates as “Mature” on Average across All Companies**



What does this relatively low maturity mean in practice?

- Only one institution in six gives the CISO the authority to stop IT projects that explicitly violate cybersecurity policies or to conduct cybersecurity simulations more than once a year.

- Only one in five ensures that the board has reviewed and approved the cybersecurity strategy in detail or includes the cybersecurity organization's impact on broader IT costs in annual performance evaluations.
- One in three enables the CISO to meet with the CEO on a regular basis, and one in three provides the board with a list of the most important information assets to protect.
- Only about half of institutions even define minimum standards for data protection for sensitive information or update intelligence about attackers more than once a year.

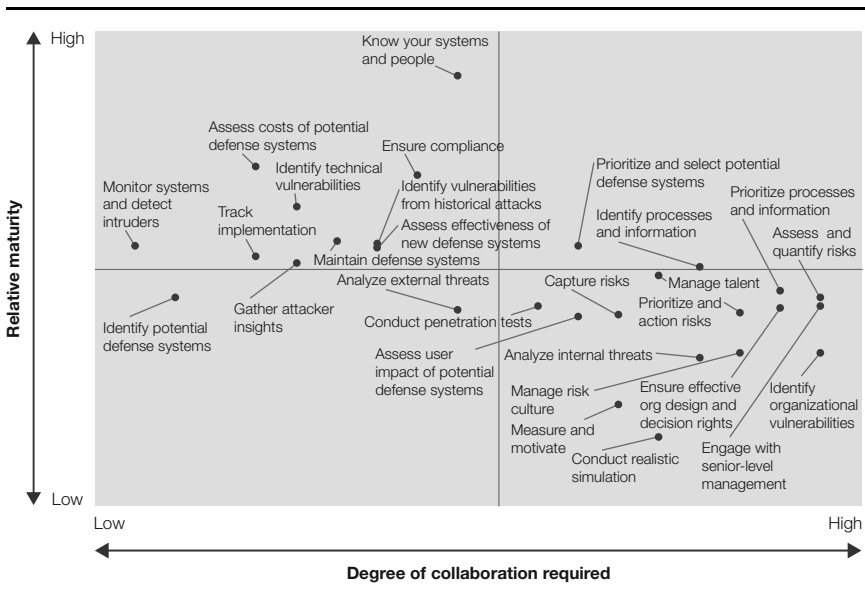
Maturity is weakest where specific practices reach beyond the immediate realm of cybersecurity. Areas that are directly under a CISO's control are more advanced, but as soon as the CISO needs to reach out—even to other people in the broader IT group, let alone the business units themselves—there is a drop-off in maturity level. For example, some of the most advanced areas are the understanding of technological vulnerabilities and assessing the costs of defense systems. For these, the CISO does not need significant cooperation from the rest of the enterprise. By contrast, understanding assets requires significant engagement from business-line executives, and maturity for this practice was much lower (Figure 1.12).

Sector, Size, and Spend Make No Difference to Cyber-risk Management Maturity

Banks scored better than other CRMS participants, but only slightly, and the differences within each sector were far greater than those between sectors. Banks were relatively strong in understanding their attackers (given their investments in intelligence capabilities in that sector), understanding their vulnerabilities, and in governance. By contrast, they were little better than average in understanding potential defense systems and their impact. Insurers were relatively weak across the board, and especially so in understanding the assets they need to protect and the vulnerabilities in their existing environment. However, the more mature insurance companies far outperformed the weaker banks.

Nor were large companies necessarily more mature than smaller ones; in fact, some companies with less than \$10 billion in revenues achieved some of the highest maturity ratings. This could be because transparency and coordination are easier to achieve in smaller, simpler organizations.

FIGURE 1.12 **Higher Maturity in Practices that Require Less Collaboration beyond Cybersecurity**

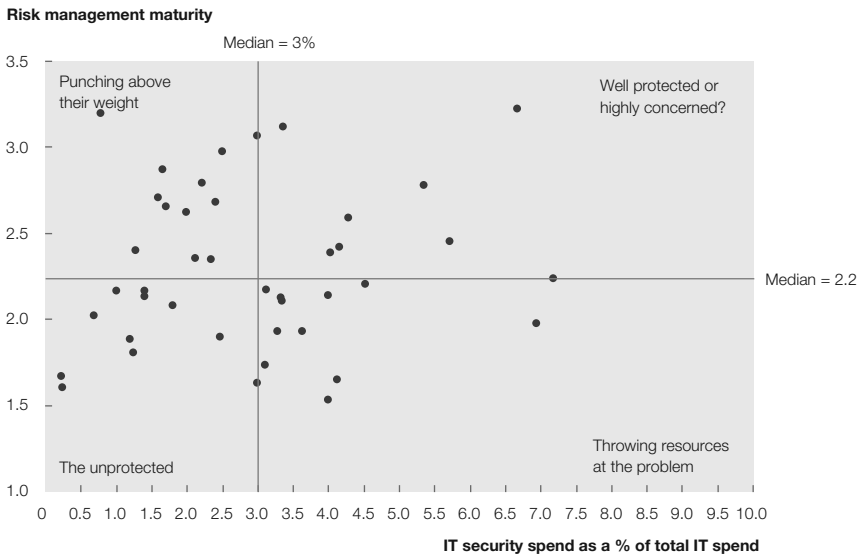


Perhaps most surprisingly, more cybersecurity spending does not lead to greater cyber-risk management maturity. Cybersecurity spend as a percentage of overall IT expenditures is an imperfect metric, but it does give some sense of the resources committed to cybersecurity in relation to the scale of what needs protecting. Plotting a company’s risk management maturity against security spend as a percentage of overall IT spend yielded results all over the map, with companies in each of the four quadrants (Figure 1.13).

The unprotected have the lowest level of capability. They have small security teams, invest relatively little in cybersecurity technology, and lack the insights to target their limited expenditures wisely. Senior managers at one financial institution believed that they would not be targeted because they did not operate in the United States. This resulted in a history of underinvestment and an exclusive focus on a very narrow and incomplete set of potential risks.

Institutions *punching above their weight* spend relatively little but are able to get more from their investments than their peers, usually because they have developed a clear idea of what assets are most worth protecting, and therefore are efficient in how they use their

FIGURE 1.13 Spending Big Doesn't Lead to Risk Management Maturity



limited budget. At one pharmaceutical company, tight budgetary constraints driven by a weakening product pipeline and concern about IP theft forced IT to develop a set of mechanisms to understand risks and focus investments on protecting the company's most important assets.

Highly concerned institutions typically have relatively high levels of both risk management maturity and spend. One sophisticated manufacturing company decided it had no choice but to devote significant resources to cybersecurity and to make smart decisions given the sophistication of its attackers and the expectations of its military and intelligence customers. It put tremendous focus on this issue, starting with very senior executives, and invested the time and effort to develop strong capabilities in understanding its attackers, assessing its own vulnerabilities, and putting in processes to select the highest-impact defense mechanisms. A corporate culture that tended to support and carry out policies once they had been set proved to be invaluable in achieving this.

Finally, there are companies *throwing resources at the problem*. They tend to have large cybersecurity teams who have implemented, or at least purchased, many of the most cutting-edge technologies. However, for all the spending, it's not clear that they are protecting the

right things or protecting them in the right way. Some institutions that have great reputations for their technical sophistication in cybersecurity fall into this last bucket. For example, one bank prioritized cybersecurity funding but failed to get the central security team, business unit leaders, and business unit IT to interact effectively. As a result, despite its sizeable budget, the central security team had limited insight into what information assets to prioritize for protection or where the vulnerabilities lay in each of the business units' sprawling application portfolios. The inevitable outcome was a damaging breach despite the heavy investment.

• • •

Institutions face a daunting cybersecurity challenge. Pervasive digitization creates tremendous value but also makes them more reliant on technology, increases the stakes in the event of a breach, and enables capable and determined attackers. Institutions thus face a damaging and expensive array of risks from cyber-attacks, ranging from loss of customer data to disruption of business operations to fraud. Attackers meanwhile can improve the pace and sophistication of their attacks much more quickly than institutions can improve their defenses.

Large institutions are further hampered because they lack the facts and processes to make intelligent decisions about cybersecurity investments and policies, meaning they don't get the maximum protection at the lowest cost and with the least business disruption.

As a result, cybersecurity, as it is practiced today, is hurting large institutions' ability to derive value from technological innovation and investment. In the course of protecting them from real and important threats, organizations' cybersecurity controls are reducing end-user productivity, diverting scarce resources from IT that creates value, and slowing the introduction of important technology capabilities.

