BCG

THE BOSTON CONSULTING GROUP

Cybersecurity Meets IT Risk Management

A Corporate Immune and Defense System

The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries. For more information, please visit bcg.com.

BCG

THE BOSTON CONSULTING GROUP

Cybersecurity Meets IT Risk Management

A Corporate Immune and Defense System

Stefan A. Deutscher, Walter Bohmayr, William Yin, and Massimo Russo

AT A GLANCE

As digitization's role in companies' operations continues to grow, vulnerability to data theft, leakage of intellectual property, denial-of-service attacks, and the like is growing apace. Many companies are significantly underprepared.

Companies at Greatest Risk

Businesses most at risk of an attack and its consequences are those in which information drives a large portion of value generation and the information passes through many interconnected systems. Companies with complex application and system landscapes are also at high risk, as are those that rely on complex or meshed networks or whose business is driven heavily by mobile transactions.

Optimized IT and Information Security

Effective security for a company's information and the technology used to store and process it will address a number of critical elements, including confidentiality, integrity, availability, accountability, and the provenance of the information.

IT Security as a Component of Overall Risk Management

IT security should be viewed as a necessary cost of doing business and as a component of the company's overall IT risk-management program.

For most forms of life, the threat of attack—from a predator, changing environmental conditions, lower forms of life (such as bacteria and viruses), or some other force—is ever present. Indeed, for many of the natural world's inhabitants, the question is not *if* but rather *when* they will be subject to some form of attack—and how (or whether) they will respond and emerge from the experience.

Businesses, of course, face an analogous situation and must contend with their own potential threats. Most companies therefore make risk identification, assessment, and mitigation a high priority. Yet there is a specific type of threat today for which many companies, in our view, are significantly underprepared: the risk associated with IT and information management. As digitization's role in companies' operations continues to grow—according to Ben Hammersley, contributing editor at *Wired UK* magazine, "Cyberspace is becoming the dominant platform for life in the 21st century"—companies' vulnerability to data theft, leakage of intellectual property, corporate sabotage, denial-of-service attacks, and the like is growing apace. The damage such events can pose to a company's profits, reputation, brand, competitive position, and even viability is potentially vast. One technology company, for example, sustained material damage to its business as a result of extensive hacking of its systems. Another suffered considerable harm to its reputation after a breach compromised the security of its customers' personal data.

Many companies are significantly underprepared for the risk associated with IT and information management.

In the natural world, a strong immune and defense capability is essential for survival (much as in human society, vaccines and health care systems are critical to protecting life). For today's companies, the ability to safeguard IT systems and information may be equally vital. To properly arm themselves, companies must understand the IT and information-related risks they face and construct sufficiently robust protection systems—and they must do so with an eye toward controlling costs and minimizing any negative impact on the business. Of course, perfect security is beyond any company's reach. The trick is to determine and provide the right *amount* of defense, at a reasonable cost, and to do so without significantly compromising the organization's business practices or culture. Moreover, the company must strike this balance while understanding and managing the risks associated with security-related compromises. In our experience, few companies have so far managed to achieve this.

Who Is at Risk?

As a rule, the companies that are most at risk of an attack and its consequences are those in which information drives a large portion of value generation and passes

through many interconnected systems. Industries with complex application and system landscapes are also at high risk, as are those that rely on complex or meshed networks. Companies in these categories include banks, automotive suppliers, and energy companies (which face a range of vulnerabilities along their entire value chain, including generation, distribution, and infrastructure).

Companies whose business is driven to a large degree by mobile transactions are also at particular risk. (In many Asian markets, for instance, mobile online transactions now exceed the number of transactions conducted through the traditional desktop platform.) For such companies, rapidly growing mobile transactions can translate into swelling revenues—as well as greater likelihood of a breach and data theft. It can also make them increasingly attractive targets for hackers and the like as these companies accumulate larger and more varied types of customer data.

Businesses that process large amounts of customer and financial information face an elevated risk.

In general, businesses that process large amounts of customer and financial information (credit card details, for example) likewise face an elevated risk, with small and medium-size firms especially vulnerable. Many of these smaller businesses lack the budget and skills necessary to properly safeguard their online or point-of-sales environments, for instance, making them popular targets.

As value creation becomes increasingly digitized across the corporate landscape, however, virtually all companies are becoming more vulnerable—and concerns are rising. (See Exhibit 1.) Health care companies, telecommunications businesses, media companies, public-service organizations, and industrial and consumer goods businesses rich in intellectual property are all increasingly likely targets that have much to lose if their IT systems and information are not sufficiently secure. (See *The Trust Advantage: How to Win with Big Data,* BCG Focus, November 2013.)

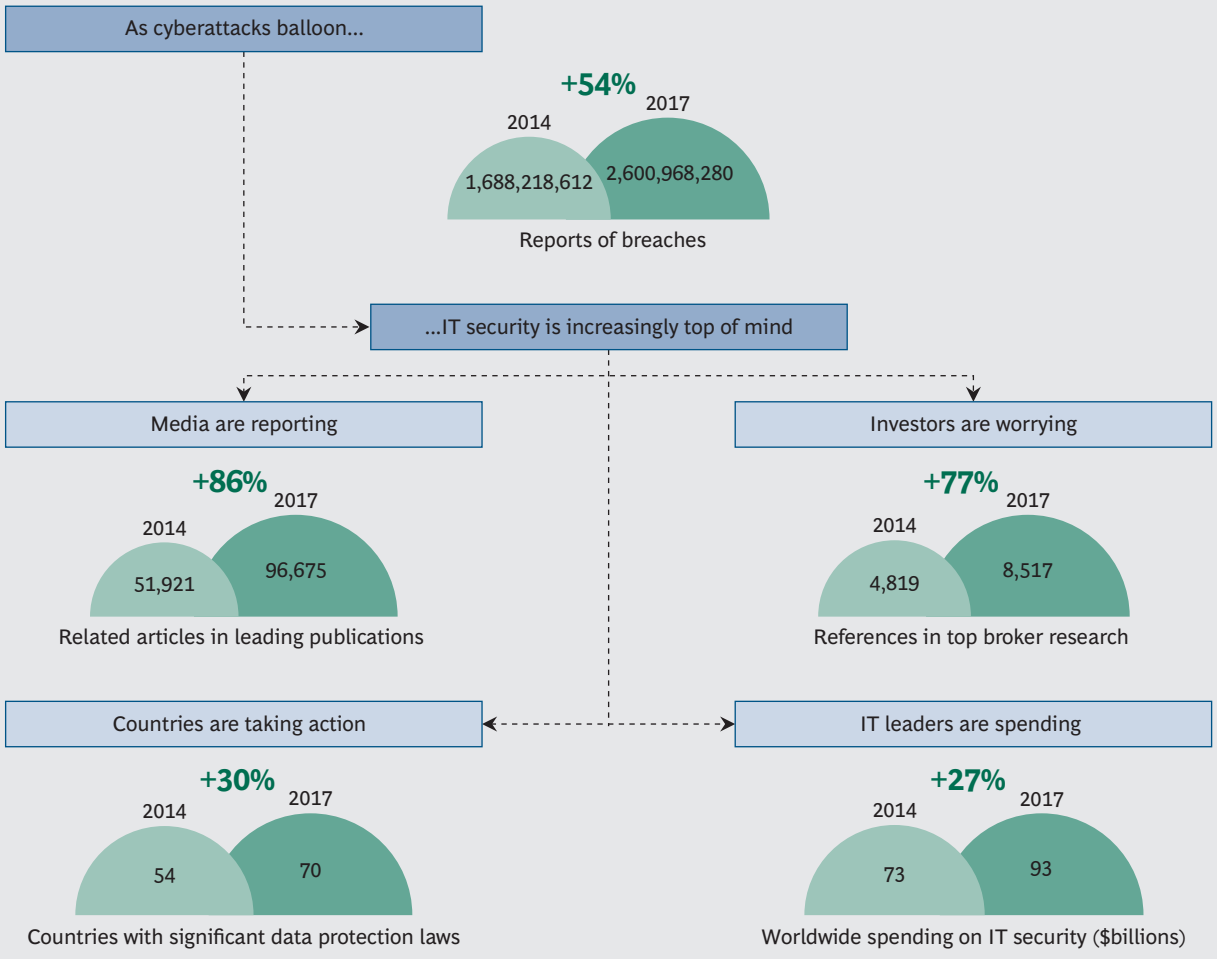
After all, the targets of hackers and data thieves are often not the systems themselves but rather the information that they store and process. And the value of that information often lies in the eyes of the (illegitimate) beholder. Strategic plans and information related to a company's market, production, and pricing strategies are obviously high-value assets that must be carefully protected. But other information, which the company might deem far less critical, could well be of utmost interest to competitors, criminals, nation-backed third parties, or the public. (A food services company, for example, might consider its customer orders to be of relatively little value to third parties and might not go to great lengths to protect that information; but if, say, one of the company's customers happens to be a law enforcement agency, an atypically large order on a given day could signal to an interested outsider that the agency is planning a major operation.)

And the circle of organizations at risk continues to widen. IT security is quickly becoming a critical concern for companies that use computers not just to crunch numbers but to monitor, move, and control critical equipment, machines, and production lines. For such companies, compromised IT security of their cyberphysical systems can have severe operational and health, safety, and environmental implica-

tions. A slightly maladjusted welding robot, for example, could do considerable damage to a car's stability—and its manufacturer's reputation. The Stuxnet computer virus is another, still top-of-mind example of the potential risk at hand. So it is no surprise that such companies are focusing more and more on industrial IT security.

In short, the problem now spans businesses of all types. But it does not stop there. Governments are clearly vulnerable to IT and information security risk, and increasing numbers are taking defensive actions. The UK's Centre for the Protection of National Infrastructure, the U.S. National Cybersecurity and Communications Integration Center, the Australian Signals Directorate, and Germany's National Cyber Response Centre and National Cyber Security Council are entities that have been created specifically to focus on the problem.

Exhibit 1 | Companies Are Increasingly Concerned About the Security of Their Digital Assets



Sources: Breach Level Index; Factiva; DLA Piper; Thomson One; Gartner; BCG analysis.

Optimizing IT and Information Security

A program intended to provide effective security for a company's information and the technology used to store and process it must address a number of critical elements, including the following:

- *Confidentiality:* the information is accessible only to those who have either a right or a need to view it.
- *Integrity:* the information is accurate, valid, and reliable.
- *Availability:* information, resources, and services are available when needed.
- *Accountability:* each (trans)action can be attributed to an accountable individual.
- *Provenance:* the origin and history of each piece of information (or each data item) are known and well defined.

Such a program must also provide clarity and reasonable assurance regarding the reliability of controls and the validity of the assumptions underpinning the effort. The priority associated with each of these elements will vary depending on the type of company and industry.

Given that a totally secure environment is impossible to create, a company must determine the base level of security it needs.

To ensure that their security campaign is sufficiently robust, companies must view the effort through a number of lenses. Three of the most important are technology, cost, and the potential negative impact of risk and the measures taken to mitigate it.[1] Getting the technology right entails, as a first step, understanding and quantifying the value of the risks that the company is trying to mitigate. Then the company should identify the technologies that are available for dealing with the risks of greatest concern: the mix of firewalls, intrusion detection and prevention systems, and data leakage protection that will be most effective. The company must also work to understand the use of these technologies in light of industry and national regulations—in some countries, for example, using technology to automatically identify and delete spam may violate constitutionally protected communications.

Cost is obviously another key consideration. Given that a totally secure environment is impossible to create, a company must determine the base level of security it needs—in other words, what is the maximum risk (reputational, operational, or financial, including the cost of remediation) that the company is willing to live with—and then gauge the marginal value of any additional security to be gained through further spending. The company can then decide what level of spending is optimal given its business strategy, tolerance for brand and operational risk, and other considerations. While this sounds like a reasonably straightforward assessment, it is not an easy one, and we find that most companies labor with it.

Finally, it is essential to take into account the potential negative impact on the business—including its culture, flexibility, ability to innovate, and speed of innovation—of both unmanaged risk and any risk-mitigation measures that are put in

place. As with cost, this is ultimately a question of balance, and companies will have to identify their particular sweet spot. We have seen a number of companies struggle with this, including several resource and engineering companies that operate internationally. One of them, in an effort to minimize the risk of data theft and espionage, does not allow its employees to bring their laptop computers and mobile devices to countries it deems high risk. The logistical challenges that this policy can pose to employees are considerable. What, for example, should an employee do when his or her itinerary for a regional, multicountry business trip calls for a visit to a high-risk country at the midpoint? Leave all this equipment home, at the expense of efficiency throughout the trip? Or follow the somewhat questionable advice of the IT department and take *two* laptops on the trip but leave the one containing sensitive information at the hotel in the high-risk location?

Similarly, a large technology company takes a very rigorous approach to elevating its IT and information security. It does not allow its employees to store company data anywhere except on company-issued computers, and it does not enable wireless local-access networks within its offices. Further, the company does not allow visitors from satellite offices to bring their company-issued notebook computers into office headquarters—instead, visitors are given "empty" computers upon arrival. For employees, this makes the execution of standard work tasks, such as accessing presentations and answering e-mails, very challenging. Returning to the metaphor of the human immune system, this is the equivalent of an allergic or even an autoimmune reaction, in which the system attacks perfectly harmless external or internal elements, compromising the body's overall ability to function properly.

Protection against leakage of intellectual property is a particular and rapidly growing concern for many companies.

Protection against leakage of intellectual property is a particular and rapidly growing concern for many companies and can force many difficult decisions. Should a company worried about leakage through employees' outbound e-mails, for example, block all such transmissions or remove all attachments? Doing so would solve the immediate problem but could introduce new ones—for example, the risk of losing business when a contract is stripped from an e-mail and never reaches its intended recipient. This approach can also reduce efficiency and potentially spur employees to find alternative means of communication that the company *cannot* monitor. (Indeed, we have seen employees of larger companies resorting to external "freemail" accounts to get their work done after trying, unsuccessfully, to change company e-mail policies that they considered impractical.) Taking the opposite approach of allowing (but monitoring) all outbound communications also has trade-offs: the company's open culture is maintained but the potential for leakage grows, necessitating investment in monitoring technology, a fast detect-and-response capability, and related staff.

These examples illustrate the types of decisions that companies will increasingly have to make. They also hint at the many complexities companies will face as they attempt to ensure security across their ecosystems—that is, the universe of organizations that they deal with in the course of operations. Note, too, that the trade-offs involved in these decisions are likely to be very different for business IT (where confidentiality is often paramount) and industrial IT (where availability is often the top priority).

Companies should aim, of course, to "do no harm" in their efforts to balance the efficacy of security measures against established norms. In cases where security measures do impinge on corporate culture and established ways of operating, companies should ensure that the necessary changes are actively managed.

Treating IT Security as a Component of Overall Risk Management

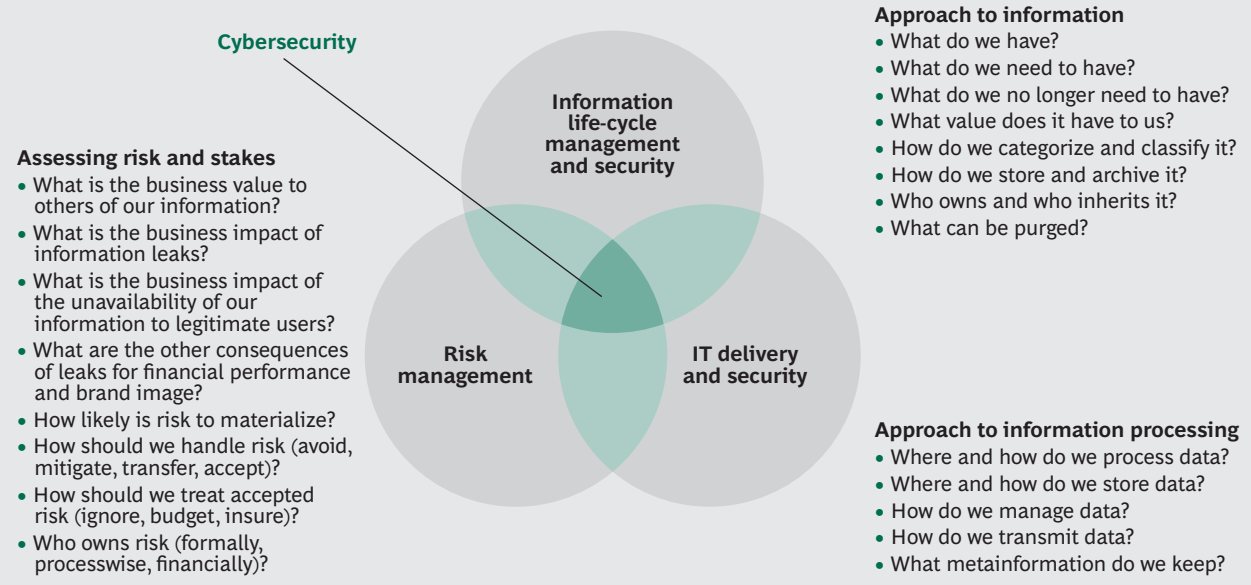
There is no ex-ante, readily calculable return on investment for IT security—like homeowner's insurance or a car with extra air bags, it is money spent today to mitigate the risk and potential cost and impact of events that may never materialize. Hence, IT security should be viewed as a necessary cost of doing business. It should also be viewed as a component of the company's overall IT risk-management program, which, in turn, should be considered an integral part of overall corporate risk management. (See Exhibit 2.) Often, however, we find that companies do neither.

To put things in context, there are six broad categories of IT risk:

- *The Risk Related to IT Security in the Narrowest Sense.* For example, what are the risks of an inappropriate or poorly enforced password policy or out-of-date software and firmware patches?

- *The Risk Related to IT Operations and Business Continuity.* What are the risks to a bank, for example, if its core banking and payment systems do not perform as expected, become unavailable, or simply break down and remain unreliable for days or even weeks?

EXHIBIT 2 | Cybersecurity Should Be Viewed as a Component of Overall IT Risk Management



Source: BCG analysis.

- *The Risk Related to IT Projects and Investments.* What risks does a company face if an IT project undertaken to meet a regulatory deadline is not delivered on time or if a project designed to seize a new market stalls for a year because the underlying IT systems do not perform as required?

- *The Risk Related to Outsourced IT Activities.* What are the risks to a company if a vendor's data center is flooded or if the owner of the source code for one of its key applications goes out of business? What are the risks if some of the company's hardware or software is compromised—or if one of a vendor's employees accidentally (or deliberately) publishes the company's customer records on the Internet? Service-level contracts cannot mitigate such risks.

- *The Risk to a Company's Reputation.* What is the risk to the reputation of a bank or telecommunications company from a major, IT-driven gaffe in customers' billing statements or from repeated website crashes?

- *The Risk to Data Protection and Privacy.*[2] What risks does a health care company face if hackers make its customers' records public? What is the risk if human resources data stored in the cloud ends up in a remote geographic location?

Organizations should strive to develop a unified, cohesive plan for addressing these risks. The first step is to identify the specific risks that the company faces in each of the six categories. The second step is to determine which of the four strategies for dealing with risk—avoidance, transfer, mitigation, or absorption—to apply to each specific risk and risk category and how best to handle any remaining risks (for example, by buying insurance against the financial impact of a given primary or residual risk). Then the company must decide how best to incorporate those strategies into its way of working.

Tipping the Scales in Your Favor

In our work on IT and information security with companies in a wide range of industries, including banking, insurance, defense, aerospace, industrial goods, energy, raw materials, telecommunications, and logistics, we have identified a number of other actions that executives can take to improve their companies' chances of success. They include the following:

- Take a systemic and holistic, rather than a component-based, view of your IT systems and information and the related risks. If your company is a bank, for example, instead of focusing on database, network, or interactive voice response (IVR) uptime, look at the end-to-end availability of your client-facing online banking service (and consider fixing an IVR outage by routing calls to your call center).

- Push to ensure that IT security and risk management processes and principles are incorporated into the company's corporate processes by design rather than as an afterthought or bolt-on. Make sure, for example, that IT security becomes an integral part of your enterprise-architecture, coding, testing, and contracting practices, and that compliance with the company's IT-security policies is part

of the project (and the budget approval or budget release) process from the start.

- Again, ask yourself how much risk your business can afford rather than how much security can be gained for a given budget. Attempt to quantify the financial impact of different types of risk and classes of incident, including costs related to business downtime; recovery and remediation efforts; potential damage to customers, staff, and the company's reputation; and mitigation efforts. Think about which risks might be worth absorbing rather than mitigating.

- Make sure that IT personnel focused on IT and information security do not act as naysayers. Rather, they should strive to be viewed as advisors to the business who—in the long run—by ensuring that projects meet all security requirements, help the company protect critical information and systems in an economically sensible way and, in the short run, help projects go through without any cost to innovation speed.

- Acknowledge the fact that, despite your best efforts, 100 percent security is not possible and a security breach of some type is likely inevitable. Then, prepare accordingly. Test systems, and their ability to recover, regularly; identify vulnerabilities; design emergency operating procedures and response plans and test them. Ask yourself some tough questions, such as: Can we take the company offline in a controlled manner if necessary? Are we really offline when we take, say, Europe offline, or is there some back channel to our Asia operations (for example, a disaster-recovery failover network link) that no one has thought about in this context? Are our communications and PR departments prepared to manage the necessary internal and external communication efforts in the event of a breach?

- Use scenario planning and war-gaming to help identify security threats and process gaps and to design appropriate responses. (See "Rethinking Scenarios: What a Difference a Day Makes," BCG Perspectives, October 2010.) Tabletop security-incident-management exercises are a good way to get started; advanced companies don't stop there, however, but rather test in vivo. Some Internet giants, for example, have departments tasked with bringing down their service in order to trigger a continually updated immune response, and many of our clients commission "ethical hacking" (also known as penetration testing) exercises, much as car manufacturers crash test their vehicles.

- Consider having your company's IT risk-management capability assessed using a pragmatic, outcome-focused framework, such as the Innovation Value Institute's IT Capability Maturity Framework. (See "Managing IT for Business Value: The New Gold Standard," BCG article, September 2010.)

IMMUNE SYSTEMS HAVE evolved over millions of years and offer insights into what an effective corporate cybersecurity program should look like. For example, they identify what is "self" and what is not, recognizing an intruder, determining how to disable it, and continuing to learn as the intruder evolves. They bring the right re-

sources (for example, an army of T cells) to the battle. Undoubtedly, there is much more to learn from these systems—and, given the increasing risk that companies face, an ever-greater urgency to do so.

No immune system (or cybersecurity effort) is 100 percent effective, however. While there are ways to tip the odds in your favor, most of us will come down with a sore throat eventually, no matter how cautious we are. Whether this causes only minor discomfort or has more severe consequences depends on whether you caught a cold or a full-blown flu—as well as on environmental conditions that you can influence, your degree of preparedness, the speed of your reaction, and the depth of your defenses. To understand where you stand, ask your physician for a health check. And consider having your company's IT security checked at the same time.

This report was originally published in October 2014. The data in Exhibit 1 and the About the Authors section were updated in October 2018.

NOTES

1. This is often the order in which IT departments address the challenge, even though the more prudent approach is generally to focus first on risk itself.
2. Strictly speaking, this is part of the risk related to IT security, but it has received so much attention lately that it is worth a separate mention.

About the Authors

Stefan A. Deutscher is an associate director in the Berlin office of The Boston Consulting Group. You may contact him by e-mail at deutscher.stefan@bcg.com.

Walter Bohmayr is a senior partner and managing director in the firm's Vienna office. You may contact him by e-mail at bohmayr.walter@bcg.com.

William Yin is a senior partner and managing director in BCG's Hong Kong office. You may contact him by e-mail at yin.william@bcg.com.

Massimo Russo is a senior partner and managing director in the firm's Boston office. You may contact him by e-mail at russo.massimo@bcg.com.

Acknowledgments

The authors would like to thank their colleagues at The Boston Consulting Group who contributed to this report, especially Alex Asen, Astrid Blumstengel, Richard Helm, Stefan Mohr, Stuart Scantlebury, and BCG's Technology Advantage knowledge team.

For Further Contact

If you would like to discuss this report, please contact one of the authors.

BCG

THE BOSTON CONSULTING GROUP

bcg.com