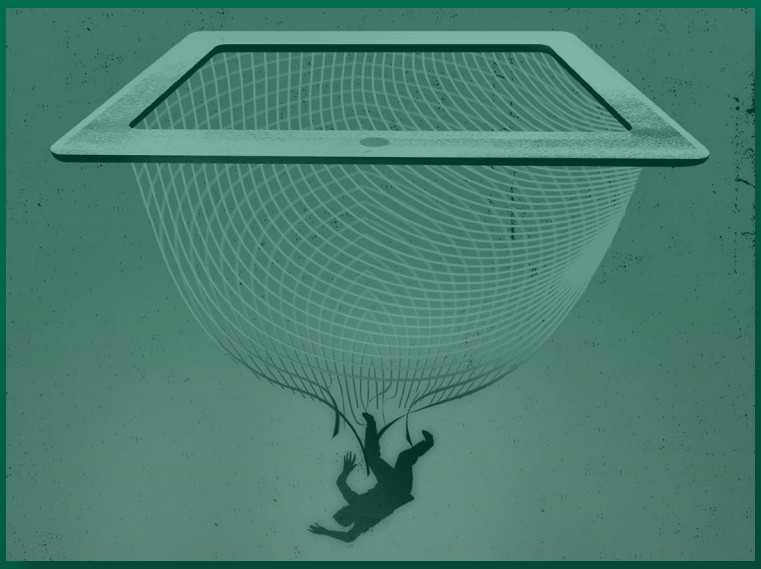
Fortifying Insurers' Defenses in an Era of Cyberrisk

BCG

The Boston Consulting Group

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 and 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 85 offices in 48 countries. For more information, please visit bcg.com.



FORTIFYING INSURERS' DEFENSES IN AN ERA OF CYBERRISK

MATTEO COPPOLA

FABRIZIO PESSINA

STEFAN DEUTSCHER

MARCO GIUNTA

ALESSIO CAVALLINI

JOHANNA WEIGAND

March 2017 | The Boston Consulting Group

CONTENTS

PREFACE

Managing cyberrisk is becoming crucial for large corporations worldwide, particularly so for those in the insurance industry. There are several reasons for this, including digitization and other business and operating model transformations, more-sophisticated hacker techniques, and the growing volume of highly confidential customer information that's available through online and offline systems. Together with the increasingly strict regulations on data privacy, these developments necessitate a rethinking of the cyberrisk management model in the insurance industry.

Big companies in virtually every industry have been investing huge amounts of money to build up their skills and increase their protection against cyberthreats. Insurance companies face the same imperative, but in many cases, they are operating with significant resource constraints. Insurers need to treat cyberrisk (which cannot be eliminated entirely) in much the same way that they treat traditional insurance risks: by defining the level of exposure they are comfortable with and prioritizing investments and projects accordingly.

This report offers an in-depth view of current market practices and emerging trends in cyberrisk management in large insurance companies. It is meant as an industry-focused follow-up to *Advancing Cyber Resilience: Principles and Tools for Boards*, a report jointly presented by The Boston Consulting Group and Hewlett Packard Enterprise at the World Economic Forum Annual Meeting 2017 in Davos. For this present report, *Fortifying Insurers' Defenses in an Era of Cyberrisk*, we interviewed chief risk officers (CROs), chief information security officers (CISOs), and other senior managers at some of the largest European and US insurance companies. In addition, we incorporated insights from discussions with a couple of Europe-based banking groups, whose challenges in the area of cybersecurity have important similarities to those of insurers.

The report describes how an internal cyberrisk management model may be designed to fit into the standard risk framework used by CROs at most insurance companies. It has four chapters:

- The first chapter focuses on governance and organization, including the roles, responsibilities, and organizational structures of the Three Lines of Defense model as it applies to cyberrisk.

- The second chapter discusses emerging best practices for developing a sound cybersecurity information strategy. Underpinning the strategy should be a specific risk appetite framework proposed by the CRO and approved by the board of directors.

- The third chapter describes how the best practices used for traditional risk processes—including risk identification, measurement, management, and reporting—can be applied to cyberrisk.

- The fourth chapter outlines the human capital and operating model considerations of setting up an effective cybersecurity system.

The audience for this study includes executive managers, CROs, and CISOs. It should also be of interest to leaders in IT, operations, and business functions who would like to better understand how their day-to-day choices affect their company's cyberattack defenses.

We hope the report's findings and recommendations can help insurers respond effectively and efficiently to the enormous challenges posed by cyberrisk in 2017 and beyond.

INTRODUCTION

Cyberrisk was barely on insurance companies' radar screens a decade ago, but it has since rocketed to a central position among operational risks. In 2016, for the second year in a row, cyberrisk was widely considered the top operational risk by financial institutions.[1]

For insurance companies in particular, this is not surprising. As insurers evolved to meet customers' emerging demands in terms of digital offers and online services, and as they modernized their operations, it was inevitable that they would expose themselves to some new areas of risk.

Here are the developments that are forcing insurers' boards of directors and top managers to pay close attention to cyberthreats:

- Insurance companies are making significant progress in the digitization of products, channels, and internal operations. Most of them now rely heavily on online networks and connectivity to operate and generate business.

- Insurers are increasingly collaborating with third parties to provide customers with the most innovative services (such as black boxes for cars). With these services, some sensitive customer data moves away from an insurer's direct control and IT infrastructure.

- New developments in software and IT, including "bring your own device" policies, have been multiplying—and scattering—the number of access points. Poor implementation has been making it easier for potential intruders to get past insurers' defenses.

- The compliance burden has been increasing, as regulators try to safeguard consumer privacy. Some of these regulations carry potentially heavy fines (most notably the upcoming General Data Protection Regulation).

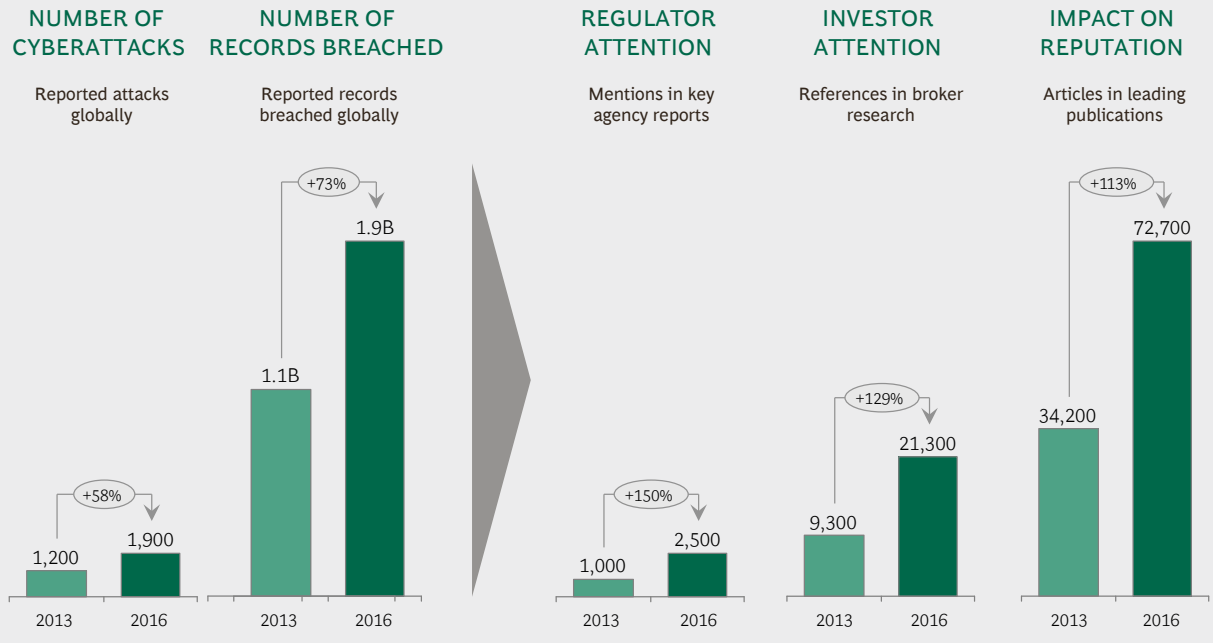
- The possibility of losing hundreds of millions of euros in operational losses, stemming from intrusions and breaches, is rapidly increasing. Although recovery costs are usually measurable, the impact on a company's reputation is much harder to assess.

These real-world developments have shown insurers that they need to invest heavily in not only technology but also end-to-end risk management techniques to adequately protect their business against cyberthreats.

Although cyberthreats and possible breaches are not entirely new to the insurance industry, there are two main differences today, compared with a few years ago. First, a breach is more likely to happen. Second, a breach is apt to get greater attention from key external stakeholders, starting with regulators and investors. (See Exhibit 1.)

The biggest problem for insurance companies, compared with other types of companies, involves the type of data they typically manage and, therefore, the type of cyberthreats they are exposed to. To be sure, many companies have reasons to be concerned about how hackers could harm their customers. Automobile manufacturers need to make sure that hackers don't get access to their control systems—especially as the era of autonomous cars approaches. Banks need to protect their customers' online banking and credit card activities. For insurance companies, however, the data itself is highly confidential. If an insurer's records slip out, employers could learn about prospective employees' chronic diseases or identity thieves could get a hold of personal information, such as social security numbers and tax account numbers. These events can create problems for policyholders

Exhibit 1 | The Increase in the Number of Cyberattacks and the Fallout That Has Resulted



Source: BCG analysis.
Note: B = billion.

that take far longer to resolve than stolen credit card information or hacked bank accounts alone.

Another problem is that insurance companies have lagged in IT infrastructure and cybersecurity investments, compared with other financial institutions. In the past, many insurers made acquisitions or merged but kept separate databases, resulting in an old and complicated network of systems. When online services were added on top of these old structures, more-vulnerable systems were created.

Insurers have also struggled to attract the technical talent needed to defend themselves from cyberattacks. Compared with banks, which have already built up capabilities and teams, insurers are light on cybersecurity talent.

Insurance executives should make their cyberrisk management model more robust along several dimensions. Doing so would allow the executives to reduce the risk of sanctions, financial losses, and harm to their company's reputation in the case of an attack. The executives could also become more adept at anticipating and limiting successful attacks and responding effectively when attacks occur, fulfilling the expectations and trust placed in them by their policyholders.

For these things to happen, the approach to cyberrisk needs to change radically. It can't be a purely technological one that is managed entirely by IT. Instead, the complexity and challenges of cyberrisk require a holistic approach and attention at the highest levels of an organization.

By increasing their understanding of cyberthreats and developing a solid cyberrisk management framework, insurance companies may also help the revenue-generating sides of their businesses. Deep knowledge of a risk area in which expertise is rare will allow insurers to strengthen their underwriting capabilities when it comes to cyberrisk. Such knowledge may also allow insurers to offer advisory services to their corporate clients in the area of cyberrisk.

Note
1. Risk.net, accessed February 10, 2017.

GOVERNANCE AND ORGANIZATION

Cyberrisk management at insurance companies has typically been driven by IT, which used an approach that was purely technological in terms of measures taken and skills applied. The chief risk officer (CRO) typically had little to no involvement and usually didn't have the appropriate resources to address cyberrisk and cybersecurity anyway.

Now, however, the approach is changing. Insurance companies are starting to manage cyberrisk through a full-fledged Three Lines of Defense model, which is what they use for mitigating traditional insurance risks. (See the sidebar "The Three Lines of Defense Model.") As part of this change, information security is becoming a C-suite responsibility, fulfilled in most organizations by a chief information security officer (CISO). The CISO's job is to provide clear guidance and priorities to the entire organization and especially to IT on implementing cybersecurity measures, given the overarching risk framework and risk appetite established by the CRO. Besides being a regulatory requirement, extending the Three Lines of Defense model to cyberrisk also happens to be a progressive way to effectively manage this risk.

European and US insurance companies are implementing the Three Lines of Defense cyberrisk model in subtly different ways. In Europe, insurance companies are typically moving to a model in which the CISO sits within the CIO or COO area as a 1.5 line of defense (1.5LoD) and the CRO (equipped with new ICT risk skills and shouldering an expanded set of responsibilities) serves as the second line of defense (2LoD). In such a model, the CISO and IT both report directly or indirectly to the CIO or COO. This has the advantage of giving the CISO more direct access to IT controls and projects. On the downside, it pits the CISO's priorities against the CIO's or COO's other priorities, both from an attention and a budget perspective.

Some US insurance companies are targeting a model in which the CISO is a proper 2LoD, in some cases within the CRO area. In such a model, the CISO represents a full-fledged 2LoD with direct access to the board of directors and, as a result, with a direct line to those who can make top-level resource decisions. This access may be part of the explanation why, for example, US banks have been able to spend much more than their European counterparts on cybersecurity projects and activities. On the other hand, in this model the CISO is functionally more distant from IT and operations, with less ready access to mitigation activities and systems that are already in place. (See Exhibit 2.)

In Europe and the US, the Three Lines of Defense cyberrisk management model has specific roles with clearly segregated duties.

THE THREE LINES OF DEFENSE MODEL

Three levels of controls are used to mitigate risk at insurance organizations:

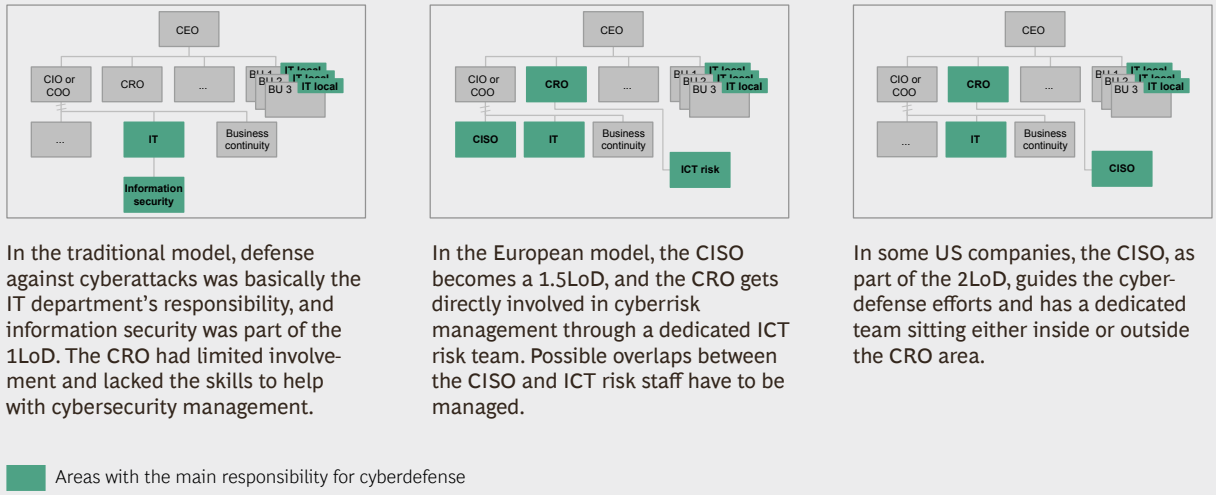
- The first line of defense (1LoD) generally sits within the business or wherever the day-to-day risk exists. The role of the 1LoD is to implement and operate controls and to respond to risk events.
- The second line of defense (2LoD) generally sits within the risk management and compliance functions. The job of the 2LoD is to define standards for controls, design them, and monitor the first line's control efforts and effectiveness.
- The third line of defense (3LoD) generally sits within internal audit. The task of the 3LoD is to review controls and ensure the efficacy of the overall risk management framework.

IT, as the first line of defense (1LoD), is responsible for implementing and executing the information security strategy. The IT staff executes all day-to-day IT controls (for example, passwords and firewalls), implements policies and guidelines, and tests for adequacy and efficiency. The staff also responds to threats and executes most of the recovery activities. Finally, IT provides the CISO and the CRO with the input they need (such as the number of attacks received) for reporting purposes.

The CISO's role is to be the expert on cyberrisk and cybersecurity. This role involves identifying the key gaps in the current architecture, setting the overall information security strategy, and defining an appropriate investment plan. The CISO drives the definition of controls, policies, and mitigation actions; ensures the adequacy and effectiveness of all solutions that have been implemented; guides IT in the definition of controls, policies, and mitigating actions; and provides input to help the CRO measure cyberrisk exposure and determine the relevance and impact of proposed investments in the cybersecurity area.

The CRO, as the 2LoD, maintains an overall view of all risks, with a day-to-day focus on

EXHIBIT 2 | Where Cyberrisk Governance Has Been and Where It's Headed



In the traditional model, defense against cyberattacks was basically the IT department's responsibility, and information security was part of the 1LoD. The CRO had limited involvement and lacked the skills to help with cybersecurity management.

In the European model, the CISO becomes a 1.5LoD, and the CRO gets directly involved in cyberrisk management through a dedicated ICT risk team. Possible overlaps between the CISO and ICT risk staff have to be managed.

In some US companies, the CISO, as part of the 2LoD, guides the cyberdefense efforts and has a dedicated team sitting either inside or outside the CRO area.

Areas with the main responsibility for cyberdefense

Source: BCG analysis.
Note: CIO = chief information officer. COO = chief operating officer. CRO = chief risk officer. CISO = chief information security officer. BU = business unit. LoD = line of defense.

identifying and measuring risk as well as ensuring that a common approach is consistently applied across all operational risks, including cyberrisk. The CRO should leverage the methodologies and measures typically used in the risk management area to support cybersecurity investment prioritization and ensure that the security strategy translates into a sustainable risk exposure for the company. (See the sidebar "CISO and CRO: Two Evolving Roles.")

Compliance is the other part of the 2LoD. The role of compliance is to assess the adequacy of internal solutions and their alignment with regulatory requirements as well as to keep all functions up to date on regulatory changes.

Internal audit is the third line of defense (3LoD) and provides an independent assessment of the adequacy of the cyberrisk management framework and whether the processes and controls are being applied effectively.

CISO AND CRO: TWO EVOLVING ROLES

As insurance companies change their approach to cybersecurity, two roles are evolving and becoming key to these organizations.

Chief Information Security Officer

The main cyberrisk management responsibilities of the CISO are the following:

- Design IT security strategy and supervise its implementation.
- Define and continually fine-tune IT security controls and testing activities.
- Ensure that the insurer's IT security systems comply with current and upcoming regulations.
- Monitor and analyze security threats, coordinate mitigation actions, and perform periodic assessments.
- Participate in risk exposure measurement exercises led by the CRO.
- Define and review policies and guidelines related to IT security and escalation procedures for the entire organization.
- Monitor the implementation of those policies and guidelines.
- Spearhead the reporting about cyberthreats to relevant business functions.
- Steer business continuity and disaster recovery programs and participate in other initiatives that affect IT security.

Chief Risk Officer

The main cyberrisk management responsibilities of the CRO are the following:

- Ensure that the IT strategy is adequate to properly address IT risk exposure.
- Measure IT risk exposure and assess the adequacy of the controls that are in place.
- Lead scenario analysis and the collection of loss data, key risk indicators, and key security indicators with the help of the CISO and IT.
- Determine the additional mitigation actions and areas of data analysis that are needed.
- Contribute to and review policies and guidelines related to IT risk.
- Lead reporting on cyberrisk exposure to the risk committee with the help of group IT security.
- Measure IT risk exposure of critical business projects (for example, business continuity) using IT inputs to ensure their adequacy.

To successfully cascade the Three Lines of Defense model into an approach that limits an insurer's cyberrisk exposure, four overarching principles should be followed:

- **Clear Segregation of Duties.** This should be done within the 1.5LoD and 2LoD and specifically between the CISO and CRO.
- **Consistent Control Framework and Methodology.** These should be adopted across the 3LoD.
- **Clear Accountability Between the Group and Local Entities.** This is possible when two things happen. First, everyone at the group and local levels understands how information security responsibilities cascade through the company. Second, the roles within the business units and any shared-services companies are made clear.
- **Rapid Adoption of New Competencies and Skills.** This should be done to enable the CRO and CISO to handle their expanded duties. On the CRO side, this means adding functional ICT risk skills to the CRO's traditional risk management competencies. On the CISO side, it means adding specialist and technical cybersecurity skills.

The application of these principles will help move traditional governance structures toward more advanced and mature models. Regardless of the exact setup of the Three Lines of Defense model, it is very important for top management, risk committees, and boards of directors to be involved in cyberrisk management. They need to drive the cyberrisk strategy at least as aggressively as they are moving to mitigate other operational risks.

INFORMATION SECURITY AND RISK STRATEGIES

The special characteristics of cyberrisk, compared with those of other operational risks, create the need for additional investments and management attention. Those characteristics include the following:

- **Tail Risk with Huge Effects on Strategy and Reputation.** Up to 50% of losses from cyberattacks are from aftershocks that hinder a company's strategy and harm its reputation, according to a 2016 benchmarking study by Ponemon Institute. This suggests there could be a loss of business volume and overall company value in a short amount of time.

- **Highly Fragmented Sources of Risk, both Technically and Geographically.** The fact that attackers can use any Internet-connected device, for instance, makes full prevention of successful cyberattacks almost impossible.

- **Emerging and Fast-Evolving Challenges That Require Technical Capabilities.** Insurance companies traditionally haven't had IT staff with the appropriate skills. They will face challenges in filling the gap, as threats are quickly changing and solutions are a moving target.

Historically, IT security strategies haven't gotten much attention from top management or boards of directors. The lack of attention was an outgrowth of the traditional governance model described earlier, as cybersecurity was managed directly by IT with a purely technical approach and little to no board involvement. On top of this, investments related to IT security were generally a hard sell. This is still true today. They involve long-term programs that are capital intensive and deeply technical, such as the review of the overall infrastructure system or the deployment of an internal security operation center. Many of the projects are focused on preventing extreme (and also relatively unlikely) events; none of them make a positive near-term contribution to the P&L. As a result, these investments usually become a matter for the COO, competing against his or her other budget priorities.

The net result of cyberrisk being treated as an IT responsibility and cyberattacks becoming pervasive is that most companies today have significantly underinvested in this area. They generally don't have a holistic approach to cybersecurity and haven't made information security investments that would adequately protect them.

So how can this be fixed? The reshaped governance models are good starting points, with more-informed CROs, who are supported by CISOs, advocating to the board for an increased level of cybersecurity funding.

Additionally, to further facilitate the investment discussions around cybersecurity, insurance companies should move away from a traditional return on investment (ROI) assessment of security investment in favor of a return on security investment (ROSI) evaluation. ROSI is defined as the decrease in risk exposure with respect to investments made; it allows for better assessing the effectiveness of investments to reduce risk and for determining the tradeoffs that must be made to accomplish it, beyond a mere near-term contribution to the P&L.

Finally, companies should create a dedicated cyberrisk strategy that is put in place by the CRO and that feeds into the larger information security strategy. The CRO's cyberrisk strategy should be like other risk strategies in that it should consist of a risk appetite framework that the board approves and monitors on an ongoing basis. It should have three main elements:

- **A Qualitative and Quantitative Synthetic Measure of Cyberrisk Tolerance.** Such a measure could be, for example, risk capital. It should be defined by the board and later used by the board to illuminate the company's cybersecurity performance.
- **A Set of Operational Key Security Indicators and Key Risk Indicators.** KSIs and KRIs should grow out of the cyberrisk tolerance level defined by the board. These indicators reflect specific technology and cyberthreats and become limits that IT can track and all operating functions can use in their day-to-day monitoring. The limits could involve the percentage of successful attacks leading to data breaches. (See Exhibit 3.)
- **A Sound Escalation Process.** This process is important in case either the risk tolerance defined by the board via the synthetic measure or the operational limits on KSIs and KRIs are exceeded.

Allowing the board and top management to focus on a relatively small number of qualitative and quantitative indicators makes it easier to define a security strategy through a risk-based approach.

With the priorities clearly identified, the investments can be concentrated where the risk is greatest, ensuring a transparent and optimal use of the insurer's resources.

EXHIBIT 3 | New CRO Responsibility Includes the Creation of Metrics for Cyberrisk

ILLUSTRATIVE RISK MEASURES AND CISO-REPORTED METRICS

KEY RISK AND SECURITY INDICATORS	LIMITS SET BY BOARD[1]		REPORTED PERFORMANCE			
	Soft	Hard	Q1	Q2	Q3	Q4
Number of attacks leading to compromised data	1 in 100	2 in 100	1 in 1,000	2 in 1,000	1.2 in 100	3 in 1,000
Number of clients affected by fraud attempts	5	10	11	2	7	4
Number of ransomware attacks	2	4	3	0	1	3
Number of critical application or infrastructure service interruptions	3	5	6	4	2	2

Acceptable performance | At or above soft limit | At or above hard limit

Source: BCG analysis.
Note: CRO = chief risk officer. CISO = chief information security officer.
[1]If limits are exceeded, mitigation actions are triggered; more severe actions are taken when a hard limit is exceeded than when a soft limit is exceeded.

RISK PROCESSES

As is done for all other types of insurance risk, day-to-day cyberrisk should be managed through four processes, with the CISO and CRO both involved to varying degrees:

- **Risk identification** is the early identification of new and evolving cybersecurity threats, classifying them by standard risk event types.
- **Risk measurement** is the quantification of actual and forward-looking cyberrisk exposure for each of the risk events identified.
- **Risk management** is the active management of controls to detect, protect against, respond to, and recover from cyberattacks.
- **Risk monitoring and reporting** is the ensuring of full awareness of cyberrisk exposure at top management and board levels and the existence of escalation procedures in case of major events.

Effectively implementing risk processes requires a sound interaction between the CISO and CRO on the basis of common language and methodologies. Specifically, it's critical to define and operationalize, across all functions, a standard control framework and control system to be used consistently across all risk processes by CRO and CISO areas.

Risk Identification

With cyberthreats evolving regularly, and new, cheap hacker technologies becoming available on a daily basis, an insurer needs to develop cyberrisk intelligence capabilities. The objective is to monitor the threat environment and identify the latest methodologies and techniques (in areas such as malware and ransomware) that could hamper the effectiveness of the controls already in place. An insurer also needs to identify the new targets and objectives of hackers (since attackers' priorities change over time) and ensure the resilience of the existing IT systems.

To further increase the effectiveness of cyberthreat intelligence capabilities, an insurer should partner with external counterparties, such as banks and other insurers. Such partnerships allow the parties to securely exchange information and build up mutual competencies.

Armed with all this intelligence about cyberattacks, the CRO can create a structured internal taxonomy of risk that can be used consistently across the organization. There are three broad types of risk events into which cyberthreats usually fit:

- **Breach of Data Confidentiality.** This is the violation and publication of customer or other internally sensitive information (such as employee e-mails and internal presentations).

- **Breach of Data Integrity.** This is the manipulation of customer or other internal data (such as the premium for a life insurance policy or the account number for reimbursements).

- **Business Service Unavailability.** This is when an attack interferes with the functioning of an internal or customer-facing IT system (such as a website for direct policy distribution) or when an attacker encrypts internal data. In both cases, attackers can demand ransom to stop the attack or to decrypt the data.

Different companies have different levels of vulnerability to these risk events based on the underlying characteristics of their business and operating models. Among other things, the degree of business innovation (the number of digital products and services), the makeup of the IT landscape (such as whether it includes data encryption), the sophistication of the IT architecture (such as an advanced data network design), and the geographical footprint (some countries are traditionally more exposed than others) heavily and differently change the underlying risk exposure of each company.

It is up to the CRO, with the support of the CISO, to identify and highlight those drivers of risk and to influence the evolution of business and operating models, with the goal of containing the company's cyberrisk exposure.

Risk Measurement

Two main mechanisms should be used to measure cyberrisk exposure. The first is internal loss data collection, which is aimed at identifying recurring internal losses caused by relatively common but usually minor cyberrisk events, such as a website outage lasting several hours. The second mechanism is scenario analysis, which is aimed at assessing potential losses stemming from major and rare events and estimating the probability of occurrence.

Internal loss data collection is the simpler of the two. It requires the systematic identification of internal cyberrisk events, the quantification of the losses caused by each specific event, and their reconciliation with P&L figures. This is something that insurers do for all operational risk events, so the idea isn't new. The results of internal loss data collection should be compared and benchmarked in terms of frequency and size against external loss data. This can be done with the help of information from consortiums such as the Operational Riskdata eXchange Association (ORX) and ORIC International, both of which share sanitized loss data among participating companies.

Scenario analysis offers a more insightful and actionable measure of cyberrisk. Traditionally used for capital calculation models and Own Risk and Solvency Assessment purposes, insurers should take advantage of this methodology to identify and prioritize interventions and investments.

An appropriate scenario analysis consists of two components. The first is qualitative: understanding the key sources of risk for a company. The second is quantitative: estimating how often the threats may materialize and the worst damage they could do.

On the qualitative side, a risk register can be used. This is a bottom-up methodology that analyzes each ICT asset in use at a company (hardware, applications, and networks) along two dimensions: the asset's vulnerability to cyberrisk and its relevance to the company business.

Assessing the vulnerability to cyberrisk by ICT asset takes into account multiple factors, such as the effective implementation of standard controls aimed at mitigating cyberthreats (as defined by international guidelines and standards, including those from the National Institute of Standards and Technology [NIST], the International Organization for Standardization [ISO], and Control Objectives for Information and Related Technology [COBIT] from ISACA[1]), any available results of penetration tests, and other readily available qualitative and quantitative information.

The assessment of an asset's relevance to the company business is often derived from the company's internal business continuity and disaster recovery plans. However, a deeper assessment can be made by using other sources

as well. Taking this extra analytic step provides additional data that in turn can be used to update the business continuity and recovery plans. Confidentiality of the data stored in or processed with the ICT assets should also be a factor in this evaluation. Insurers can do this by classifying data on the basis of the level of confidentiality needed, from the most sensitive (such as client health data, board presentations, and documents) to the least sensitive.

These two dimensions have to be assessed for each ICT asset and then used to create a vulnerability-relevance matrix to identify the most relevant scenarios to test and to determine the right mitigating actions and investments. (See Exhibit 4.)

On the quantitative side, realistic scenarios should be designed jointly among the 1LoD, 1.5 LoD, and 2LoD to assess the impact of a cyberrisk event, as defined in the risk identification process, on those ICT assets classified as highly vulnerable and highly relevant.

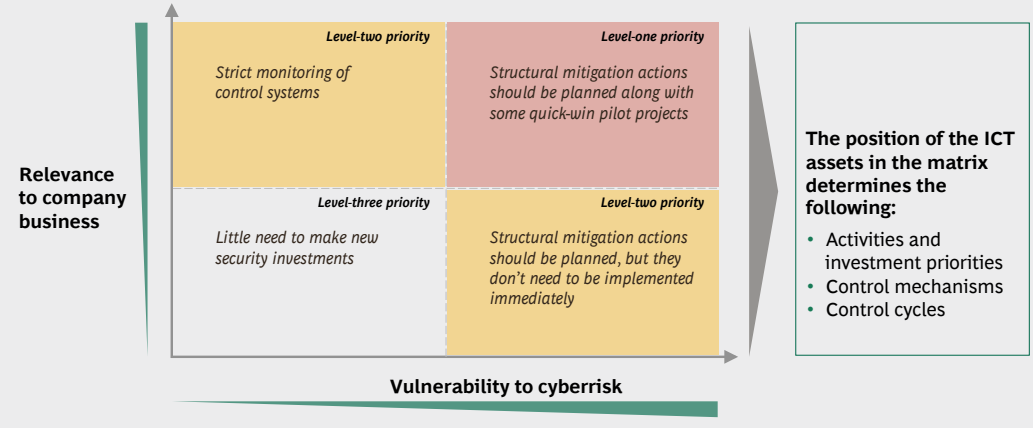
The expected frequency and financial impact of these scenarios should be estimated for a standard case as well as for a worst case. The financial impact reflects the need to compensate customers, cover professional and consulting fees, and pay penalties resulting from sanctions, among other things. (See Exhibit 5.) An analysis should also be done to properly assess, at least on a qualitative basis, any impact on strategy and reputation, both of which are inherently harder to quantify.

Besides the quantification of risk exposure that it provides, the results of the scenario analysis also enable insights on technological issues and the adequacy of controls, both of which could influence management actions. Scenario analysis is also a useful business and management tool in three respects:

- It underscores the potential consequences of a large-scale attack.
- It creates awareness of and consensus on the need for additional mitigation actions.
- It provides practical input for the ROSI evaluation, helping make the benefit-to-cost calculation of cybersecurity investments clearer.

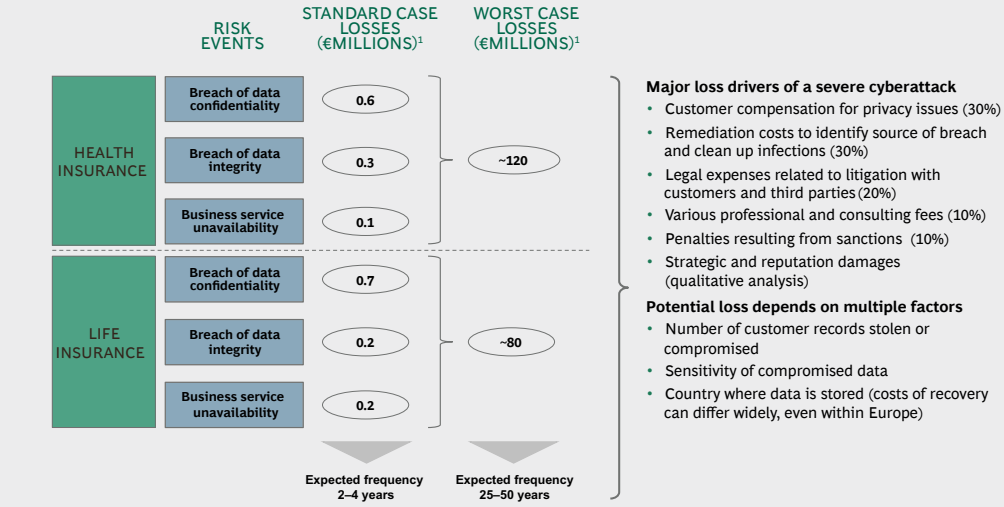
On top of the above, the scenario analysis approach can be leveraged in two ways internally. First, it can be used by the underwriting department to appropriately identify and price cyberrisk coverage for other corporations. Second, a sound internal scenario analysis outcome can help insurance companies figure out which type of insurance and how much they themselves should buy to cover cyberrisks that, however unlikely, could be devastating if they materialize.

Exhibit 4 | The Approach to ICT Assets Will Differ on the Basis of Vulnerability and Relevance



Source: BCG analysis.

EXHIBIT 5 | Measuring Risk Exposure Through Scenario Analysis



Source: BCG analysis.
[1]Numbers are illustrative.

Risk Management

Cyberrisk management has two main objectives, which are both best achieved using strong systems of control. The first goal is to protect against and detect internal and external cyberattacks. The second objective is to respond to and recover from cyberattacks, usually using an incident management framework.

The first step in protecting against and detecting internal and external cyberattacks is the implementation of control systems in these most important areas of security enhancement (a complete list can be found in the international standards and guidelines issued by NIST, ISO, and COBIT):

- **ID and access management**, preventing internal threats by ensuring that only the right individuals access the right resources at the right times and for the right reasons; among the tools that can help with this are role-based access control and user entitlement reviews.

- **Cyberdefense**, preventing breaches from external attacks (through data encryption, firewalls, network protection, and other things).

- **Policies and practices**, formalizing and enforcing practices and processes that prevent breaches and minimize their impact; such practices and processes include information security governance frameworks, information security procedures, secure internal software development, and third-party security.

- **Physical security**, defining the actions to take (in areas such as facility management, perimeter security, and internal security) to keep a breach in physical security from becoming a cybersecurity issue.

The complexity and the cost of these controls vary significantly. A simple control might involve placing a security guard at the entrance of a data center. A more sophisticated control could involve implementing complex software for intrusion detection.

Indeed, one of the challenges of protection and detection is finding the right balance among cost, investment, and risk reduction. Insurers can do this with the help of ROSI and the risk register, which categorizes ICT assets by their vulnerability to cyberattacks and their relevance to the business. Without such prioritization, there is a chance of implementing an overly complicated and costly set of controls that exceeds an insurer's needs.

The second step in protecting against and detecting cyberthreats is the use of mitigating actions should the standard controls prove in-

adequate. These mitigating actions could include the hiring of new staff or the development of additional controls, both of which would make the organization more resilient. (See "Building a Cyberresilient Organization," BCG article, January 2017.) They could also include the purchase of cyberrisk insurance policies as a way for insurers to protect themselves against losses.

Response and recovery should be managed using an incident management framework, which classifies attacks by cyberattack severity levels and lays out the appropriate response (escalation, communication, and technological processes). As with other types of risk management in insurance, it is imperative that the response be strong enough to contain the damages.

To this end, cyberattacks should be comprehensively classified by the severity of the damages. The severity can be defined as the exceeding of given lower and upper limits of, for example, the number of affected data records or the number of affected users. The three cyberattack severity levels follow:

- **Business as usual**, when no limits are reached, the cyberattack is manageable within the IT function.
- **Medium alarm**, when only lower limits are exceeded and only a certain number of lower limits are affected, the cyberattack requires several functions to work together.
- **High alarm**, when upper limits are exceeded or a certain number of lower limits are exceeded, the cyberattack requires a dedicated response team to guide and coordinate all relevant functions.

Escalation is a key response mechanism within the incident management framework. It's vital that the escalation criteria relate to cyberrisk and that there is a mechanism for alerting not only internal departments but also external authorities if an attack is serious enough to warrant it.

The framework should also include a communication strategy that assures stakeholders of the company's ability to address the attack; provides transparent, complete, and consistent information on what's happening; and takes into account customer retention and includes a plan for safeguarding the company's reputation.

Furthermore, it is vital that communication strategies are in place to inform affected customers and the media to prevent misinformation and limit damages. Partners, such as reinsurers, and relevant distribution channels, such as brokers or banks, have to be informed and supported in their communication.

Sound reaction plans need to be developed and practiced regularly with all affected functions. These plans should include several scenarios from the scenario analysis and different degrees of severity to make sure everyone is prepared and knows what to do in the event of a major breach. The results and lessons from these practices should then be implemented in insurers' operations.

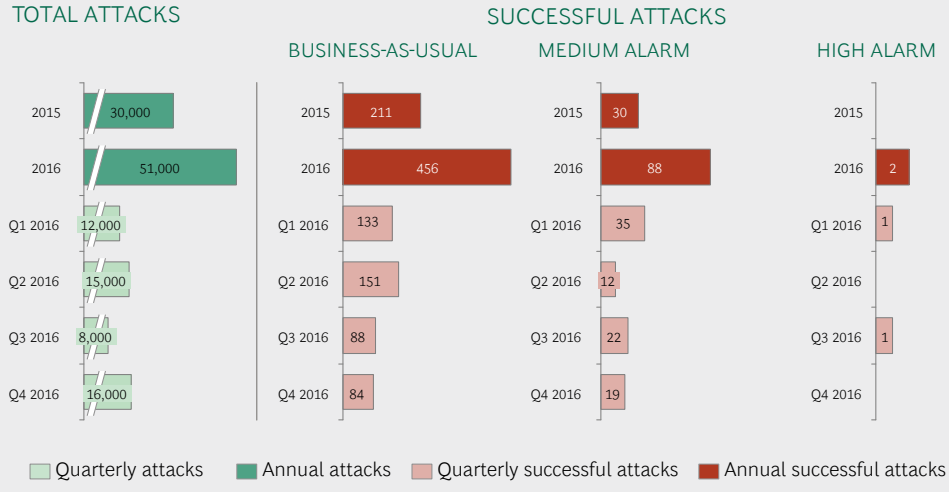
It is crucial to implement attack-specific features in the existing IT infrastructure to enable an effective and quick decision-making process. In most cases, cyberattacks are focused on not only accessing confidential data but also disrupting the services offered to the public through, for example, distributed denial of service (DDoS) and defacement. Therefore, the standard ICT recovery plans, such as business continuity and disaster recovery, in and of themselves are usually not sufficient. One need only consider how quickly cyberattacks develop—with data sometimes replicating in near real time and corruption of the primary sites generating immediate corruption of secondary sites—to grasp the inadequacy of standard ICT recovery plans.

Insurers should focus on creating cyberattack recovery plans that take into account the particular characteristics of this risk. Such plans include network resilience to ensure the availability of services in case of a DDoS attack and an improved approach to understanding the level of data corruption and of restoring the data to its original state.

A good approach and strong capabilities in the area of cyberrisk management can also be a business lever for insurance companies. Many policyholders who buy cyberrisk pro-

Exhibit 6 | Reports Keep the Board of Directors Informed

ILLUSTRATION OF DATA THAT SHOWS THREAT LEVELS OVER VARIOUS TIME PERIODS



Source: BCG analysis.
Note: Total attacks includes successful and unsuccessful attacks. A successful attack is one that breaches a company's security systems or blocks services.

tection may benefit from advisory support for day-to-day risk management, which can potentially also reduce the number and size of claims for the insurance company.

Risk Monitoring and Reporting

Risk monitoring and reporting relies on several key aspects, the first being a tree of indicators that are consistent with the risk appetite defined at the board level. At the top of the tree are high-level indicators for the board and top management. These high-level indicators are then cascaded down into operational KSIs and KRIs for day-to-day management, as mentioned earlier in the chapter on information security and risk strategies. These indicators need to be reported regularly and monitored across all lines of defense up to the board level.

Mitigation actions taken to protect against and detect cyberthreats, described in the previous section, also need to be monitored closely. There should always be a clear view of the progression and effectiveness of these mitigation actions.

Then risk monitoring and reporting requires escalation processes linked to the performance of the risk appetite indicators and to the severity of events happening in the organization. A "business as usual" event needs different escalation processes than a full-blown "general alarm."

One important piece of intelligence involves data on attacks at all security levels. (See Exhibit 6). There are several reasons for the board to get reports like this. First, such reports allow the board to see the overall number of attacks on the company, instead of only being informed when there is a medium or high alarm. Second, the board can set limits on the number of successful attacks leading to a general alarm or potential alert, which can help with investment decisions and in evaluating the effectiveness of controls. The reports could be qualitative as well as quantitative, with documents that explain new cybersecurity threats; status reports about the company's cybersecurity initiatives; information graphics that show how the company's risk exposure has evolved; and, of course, the KSIs and KRIs reflecting the company's risk appetite.

Note
1. NIST provides a taxonomy of cybersecurity controls at different levels of detail and a methodology to assess and manage those controls. NIST develops these guidelines for federal agencies in the US, but the industry widely uses them as best practices. ISO and COBIT are international standards.

SKILLS AND PEOPLE

All of these organizational and process changes will require new skills and additional people. There is considerable variability, from a human capital perspective, in insurers' readiness to safeguard themselves against cyberattacks. All lines of defense need to evolve in terms of skills and personnel. Even the insurers that are the furthest along in setting up their cyberrisk defenses are likely still to have some big skill and staffing gaps in certain departments.

The CRO team will typically have a need for enhanced ICT skills. The new ICT staff doesn't necessarily have to be experts in cyberrisk. But the staff needs to have a deep and broad knowledge of ICT risks so that the CRO team can liaise with the company's most sophisticated cyberrisk experts and fully understand (and if necessary, challenge) what those experts are working on. In this way, the CRO team can ensure that the company's risk exposure relating to cyberattacks is at a level that is sustainable for the company.

The CISO team will need the biggest staffing changes. This office will become, in effect, the locus of the insurer's technological response to cyberattacks, with personnel acting as an elite cyberrisk response team. The people who are needed won't be available through the usual recruitment channels. And insurers are starting to realize this. Some are looking to recruit professionals from intelligence agencies' or police forces' cybersecurity teams. Others are looking to hire so-called ethical hackers or white hats—people with the ability to find vulnerabilities in corporations' cyberrisk defenses. Because of their unique talents, such people are in high demand these days and can command high salaries.

HR functions will have their hands full trying to recruit these resources. The CISO needs to be tested for real-world experience in the areas of information security controls, audit and compliance, strategic program development, finance, and people management. The nonmanagement hires in the department need to have deep technical expertise in areas including viruses, computer worms, malware, network scanning techniques, system hacking, access control, ubiquitous computing, and cloud security. There are several certifications available that can guide HR departments in their search for adequate candidates.

Organizations with fewer than 3,000 users typically don't have dedicated security resources, relying instead on their IT departments to provide protection. At companies with 3,000 users or more, a common ratio of security professionals to staff is one professional for every 2,000 users supported. However, the ratio can vary on the basis of the sophistication of the cybersecurity program and the extent to which external providers are used.

There are two typical sourcing approaches for cybersecurity and risk management. Some organizations work toward a full in-house model, with as many cyberdefense activities performed internally as possible. This is most common among large organizations that want to control the entire process. Other organizations prefer to outsource a portion of the defense effort to third parties. This is a good option for smaller insurers and may be a good way of managing some of the more technical aspects of cyberrisk. (See "Building a Cyberresilient Organization," BCG article, January 2017.)

CONCLUSION

Increasing digitization in all areas, collaboration, the use of third parties, and new software and IT solutions such as cloud computing—all of these are making cyberrisk management a priority for insurance company boards of directors and executives. Awareness and discussion of cyberrisk have risen dramatically in the insurance industry, with the number of attacks rising and large losses becoming more common. As our study shows, many players have already started the journey toward structured and risk-based cyberrisk management practices that are analogous to those the companies already follow for more traditional insurance risks.

Nonetheless, there is still significant work to be done. In this report, we have outlined four dimensions that insurers should strengthen:

- **Governance and Organization.** This entails a number of things, including a full-fledged Three Lines of Defense model with a dedicated CISO as a 1.5LoD or 2LoD and a clear segregation of responsibilities and duties between the CISO and the CRO. It also entails a consistent framework and methodology across all lines of defense; clear accountability between group and local entities; and a CRO and a CISO aided by a new set of ICT risk, specialist, and technical cybersecurity skills. Lastly, it entails the involvement of a board that is informed about cyberrisk and committed to combatting it.

- **Information Security and Risk Strategies.** Insurers need a risk appetite framework defined at the board level. This framework is an essential part of setting a risk strategy and helping prioritize investments in the information security domain. ROSI logic can help assess which investments will do the most to reduce cyberrisk exposure.

- **Risk Processes.** There are four parts to this. First, the insurer must develop cyberrisk intelligence capabilities to identify risks and classify attacks into standard risk events. Second, it must systematically quantify that risk through loss data collection and scenario analyses focused on the underlying ICT assets and the exposure those assets have to cyberattacks. Third, it must implement controls to limit and detect successful cyberattacks and develop an incident management framework and response capabilities to respond to and recover from attacks when they occur. And fourth, it needs clear reporting and escalation procedures up to the board level.

- **Skills and People.** The CRO and CISO need to develop skills and hire people with new kinds of talent. Some of this

may involve new recruiting methods and some of it may be more easily accomplished by outsourcing certain cyber-risk-related tasks.

The value at stake is already huge and is going to become even bigger, as new and upcoming regulations create urgency for insurance companies to quickly develop and strengthen their cybersecurity models. Moving from a pure IT compliance approach to a real risk-based approach is essential. The goal is not for insurers to be able to fully prevent all incidents—that isn't possible. The goal is to limit widespread losses and damages in the event that a cyberattack occurs. Sooner or later, it will.

NOTE TO THE READER

About the Authors

Matteo Coppola is a partner and managing director in the Milan office of The Boston Consulting Group and the global topic leader of the Risk and Regulation taskforce of the Insurance practice. **Fabrizio Pessina** is a partner and managing director in the firm's Milan office and a leader of the Technology Advantage practice for projects in insurance, banking, and energy. **Stefan Deutscher** is an associate director in BCG's Berlin office and global topic leader for cybersecurity and IT risk management as well as for IT infrastructure and data center operations. **Marco Giunta** is a principal in the firm's Milan office and leads risk and regulation projects in the Insurance practice. **Alessio Cavallini** is a consultant in BCG's Milan office and actively involved in risk and technology projects in the Insurance and Financial Institutions practices. **Johanna Weigand** is a consultant in the firm's Munich office and actively involved in projects in the Insurance and Financial Institutions practices.

Acknowledgments

The authors would like to thank the external stakeholders that generously supported the development of the study, providing insights and bringing visibility. The authors are particularly grateful to the insurers and banks that made their CRO, CISO, and other senior executives available to discuss current industry trends and best practices for managing cyberrisks.

For Further Contact

For further information about this report, please contact one of our experts.

Walter Bohmayr
Senior Partner and Managing Director
BCG Vienna
+43 1 537 56 80
bohmayr.walter@bcg.com

Matteo Coppola
Partner and Managing Director
BCG Milan
+39 02 65 59 91
coppola.matteo@bcg.com

Fabrizio Pessina
Partner and Managing Director
BCG Milan
+39 02 65 59 91
pessina.fabrizio@bcg.com

Stefan Deutscher
Associate Director
BCG Berlin
+49 30 28 87 10
deutscher.stefan@bcg.com

Marco Giunta
Principal
BCG Milan
+39 02 65 59 91
giunta.marco@bcg.com

Alessio Cavallini
Consultant
BCG Milan
+39 02 65 59 91
cavallini.alessio@bcg.com

Johanna Weigand
Consultant
BCG Munich
+49 89 231 740
weigand.johanna@bcg.com

For information or permission to reprint, please contact BCG at:
E-mail: bcg-info@bcg.com
Phone: +39 02 65 59 91
Mail: The Boston Consulting Group, Inc.
Via Ugo Foscolo 1
Milan 20121
Italy

To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcgperspectives.com.

Follow bcg.perspectives on Facebook and Twitter.

3/17

BCG

THE BOSTON CONSULTING GROUP

Abu Dhabi
Amsterdam
Athens
Atlanta
Auckland
Bangkok
Barcelona
Beijing
Berlin
Bogotá
Boston
Brussels
Budapest
Buenos Aires
Calgary
Canberra
Casablanca
Chennai
Chicago
Cologne
Copenhagen
Dallas
Denver
Detroit
Dubai
Düsseldorf
Frankfurt
Geneva
Hamburg
Helsinki
Ho Chi Minh City
Hong Kong
Houston
Istanbul
Jakarta
Johannesburg
Kiev
Kuala Lumpur
Lagos
Lima
Lisbon
London
Los Angeles
Luanda
Madrid
Melbourne
Mexico City
Miami
Milan
Minneapolis
Monterrey
Montréal
Moscow
Mumbai
Munich
Nagoya
New Delhi
New Jersey
New York
Oslo
Paris
Perth
Philadelphia
Prague
Rio de Janeiro
Riyadh
Rome
San Francisco
Santiago
São Paulo
Seattle
Seoul
Shanghai
Singapore
Stockholm
Stuttgart
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Vienna
Warsaw
Washington
Zurich