Harvard Business Review

A REPORT BY HARVARD BUSINESS REVIEW ANALYTIC SERVICES

Meeting the Cyber Risk Challenge

Sponsored by

ZURICH

FERMA
Federation of European Risk Management Associations

ABOUT ZURICH INSURANCE GROUP

Zurich Insurance Group (Zurich) is a leading multi-line insurance provider with a global network of subsidiaries and offices in Europe, North America, Latin America, Asia-Pacific, the Middle East, and other markets. It offers a wide range of general insurance and life insurance products and services for individuals, small businesses, mid-sized and large companies, and multinational corporations. Zurich employs about 60,000 people serving customers in more than 170 countries. Founded in 1872, the group is headquartered in Zurich, Switzerland.

LEARN MORE: www.zurichcorporateforum.com

ABOUT FERMA

The Federation of European Risk Management Associations (FERMA) brings together 22 national risk management associations in 20 European countries. FERMA has 4,500 individual members representing a wide range of business sectors from major industrial and commercial companies to financial institutions and local government bodies. These members play a crucial role for their organisations with respect to the management and treatment of complex risks and insurance issues.

Meeting the Cyber Risk Challenge

Executive Summary

THE ENORMOUS EXPANSION in the availability of information presents opportunities and challenges for business and government. Keeping their own data secure is a major task for organizations that face threats from competitors and others who may find their proprietary information too tempting not to try to steal. At the same time, tightening laws and regulations and the demands of customers, citizens, suppliers, their own employees, and others with whom they interact make it imperative that they carefully control access to data about those outside parties. Accordingly, more than three out of four respondents to a recent Harvard Business Review Analytic Services survey sponsored by Zurich said information security and privacy have become more significant areas of concern in the past three years.

- Cyber risk comes in a bewildering variety of forms. More than one in four survey respondents mentioned each of the following as being among the most serious information security concerns for their organizations: malware and other viruses, administrative errors, incidents caused by data providers, malicious employee activity, attacks on Web applications, theft or loss of mobile devices, and internal hackers.
- Concerns about regulation and compliance appear to be driving much of organizations' planning around cyber risk. While survey respondents most frequently placed business income loss and the cost to restore crucial proprietary electronic information among their top five concerns, the next three were all related to legal liability: legal defense and settlement costs from third-party claims, costs to comply with regulatory settlements, and costs to defend against regulatory investigations.
- Top executives often tend to regard themselves as doing a great job controlling cyber risk. But too often, responsibility remains concentrated with the chief information officer (CIO) or head of technology. Only 16.3 percent of companies have designated a chief information security officer to oversee cyber risk and privacy, according to the survey.
- In fact, bringing together all of the organization's stakeholders in cyber security is key to designing an effective process for forestalling cyber risk and responding when an event occurs. During a November 2012 *Harvard Business Review* webinar, Julia Graham, FERMA board member and chief risk officer (CRO) of DLA Piper, noted that aside from the CIO or the IT department, cyber security is also the business of the human resources manager, for example, in managing confidentiality agreements in people's contacts.
- Organizations' success at creating organization-wide plans to address cyber risk is mixed, however. Almost two-thirds of survey respondents said their organization has formally assigned roles and responsibilities to key individuals as part of an incident response plan. But less than half said they have a strategy for communication to the general public in case of a cyber risk incident.
- Three out of four organizations, however, have introduced new IT infrastructure, and more than two of three now regularly update their antivirus software, while a similar proportion have introduced secure configurations for network devices such as firewalls, routers, and switches. But a sizable minority—more than 20 percent—say their company's budget for activities to maintain information security and privacy is inadequate, while nearly 10 percent said they don't know whether it is or not.

SURVEY HIGHLIGHTS

16.3%
of companies have a chief information security officer

20%
of companies say they have an inadequate security budget

60%
of companies have no plans to purchase privacy and security insurance

- The solutions need not be highly complex. Much can be accomplished simply by regularly training and educating employees and taking commonsense measures such as not letting sensitive information be copied onto unencrypted memory sticks. This is especially the case in an age when much work is done on mobile devices and by employees working offsite.
- Communication, then, is key. Avoid technospeak, and bring in highly credible outside experts to deliver the message to the board.
- Traditional insurance policies, like commercial general liability insurance, do not cover cyber crime and security and information risks. Yet few organizations—less than 20 percent, according to survey respondents—have purchased security and privacy insurance specifically designed to cover exposures associated with information security and privacy-related issues. More than 60 percent said their company has no plans at all to purchase coverage.

Introduction

Information—even the most private, it sometimes appears—is more available today than ever, thanks to digitization, the Internet, and social media. This presents a double-edged challenge for business and government. The demands of competition require them to take extra pains to keep their own data secure from competitors and cybercriminals. But laws and regulations give them an extra incentive—the possibility that they could be fined or even sued by a customer, client, employee, or supplier if the organization fails to keep their data secure as well.

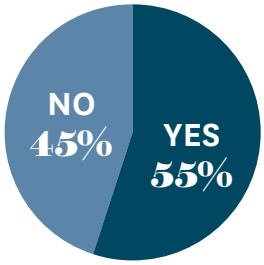
Julia Graham, FERMA board member and CRO at the global law firm DLA Piper, defined cyber security as "the organization's ability to secure its people, information, systems, and reputation in cyberspace." Being in business today means not only selling goods and services, but being a steward of a mass of "personally identifiable information and how that is stored and collected and used."

That understanding is catching on at global companies. More than three out of four respondents to a recent Zurich-sponsored survey by Harvard Business Review Analytic Services said that information security and privacy have become more significant areas of concern in the past three years, about the same proportion who said the commitment of key individuals in their organization was high, moderate, or increasing. And 55.1 percent said their board now receives regular updates on key issues relating to information security and privacy management. figure 1

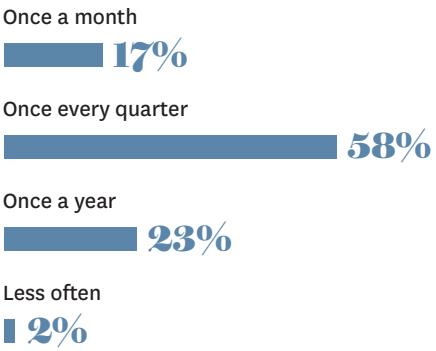
Figure 1

Board Updates on Information Security

DOES YOUR BOARD RECEIVE REGULAR UPDATES ON THE KEY ISSUES CONCERNING INFORMATION SECURITY AND PRIVACY RISK MANAGEMENT?



HOW FREQUENTLY IS THE BOARD UPDATED?



More than three out of four survey respondents said information security and privacy are more significant concerns than they were three years ago.

One major reason for the new attention from top executives: liability. This was underscored in 2011 when some 77 million Sony PlayStation accounts around the world were hacked. The stolen information included usernames, passwords, and possibly credit card information. The incident prompted government investigations in more than a dozen countries and class action lawsuits in the US.

Today, Andrew Horrocks, a partner at the international commercial law firm Clyde & Co, said there is a "significant risk of third party claims" for data breaches, especially in North America and potentially in Europe and the UK as well. But beyond the threat from individuals harmed, regulation concerning management of personal data is becoming more demanding and the fines and penalties more stringent. "The cost of failure to deal with cyber risk and failure to comply with [regulations] is great," said Horrocks. "It's not just costly in terms of cost and damage to the company and the brand, but that these penalties are quite large."

Areas of Concern

Companies can capture value through cyber security as well, noted Mark Fishleigh, a director with BAE Systems Detica, an international information intelligence firm. "Sometimes you can identify opportunities through this process," he said. "We are increasingly finding that companies that work in sectors where they're handling confidential information belonging to other people, and are able to demonstrate really strong security posture around that information, are more attractive and potentially able to win more business."

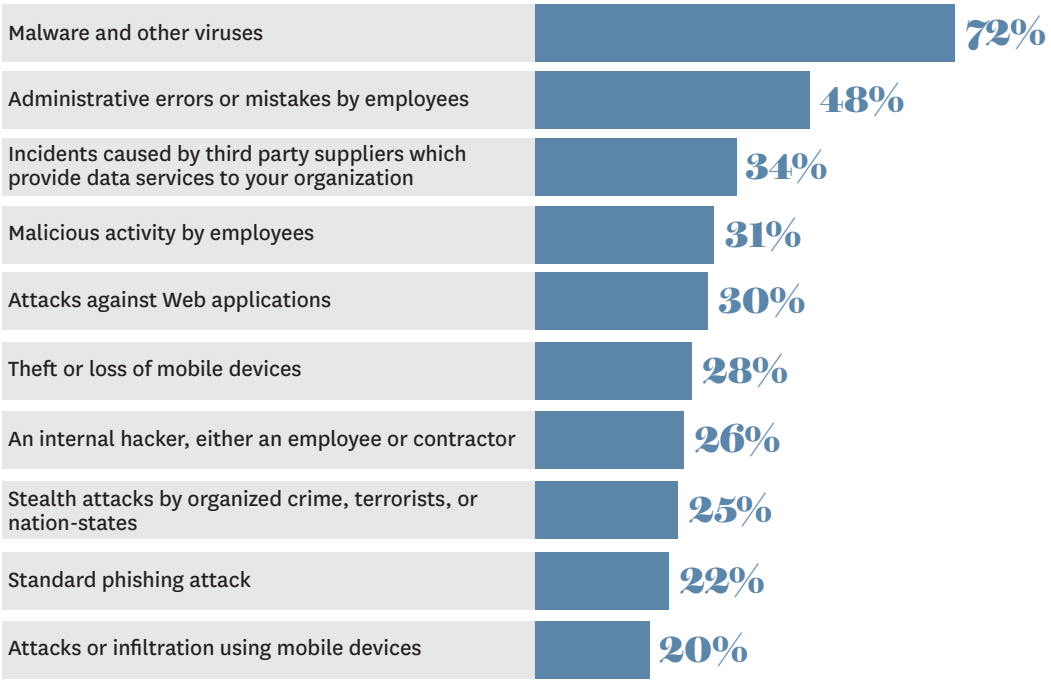
There appears to be a disconnect, however, between organizations' confidence in their efforts to instill a cyber risk culture and its actual implementation. "Chief executives all seem to think they're doing a great job, and maybe it's because they're talking about it and their budgets indicate it," said Graham. "But what I've seen is it's still often the domain of the CIO or head of technology." Only 16.3 percent of companies have designated a chief information security officer to oversee cyber risk and privacy, according to the survey.

Awareness and attention to cyber risk may not be penetrating fast enough to all levels of the organization to keep the risk of such events under control. Only 36.3 percent of survey respondents said their organization conducts information security and risk training at the enterprise level for all employees, and less than half said it occurs either annually or biannually. The lag was even more pronounced in the public sector, where only 9 percent of respondents said their organization was providing training at the enterprise level and only one in three were doing so annually or biannually.

Figure 2

Top 10 Info Security and Privacy Threats

QUESTION: WHICH INFORMATION SECURITY AND PRIVACY THREATS ARE OF MOST CONCERN TO YOUR ORGANIZATION? PLEASE SELECT UP TO 5 OF THE HIGHEST CONCERNS.



The sheer number of ways in which data can be lost, stolen, or misappropriated illustrates the prevalence of the threat. More than one in four survey respondents mentioned each of the following as being among the most serious information security concerns for their organizations: malware and other viruses (72.4 percent), administrative errors (48 percent), incidents caused by data providers (34.2 percent), malicious employee activity (30.9 percent), attacks on Web applications (30.3 percent), theft or loss of mobile devices (28.3 percent), and internal hackers (25.7 percent). figure 2

Data risks create fundamental threats to how organizations conduct business and manage their supplier, customer, and other relationships. More than 62 percent listed wrongful disclosure of customer information as a top-five concern, while 55.9 percent cited network events that result in loss or corruption of key systems or software and 53.9 percent cited data breaches resulting in loss or theft of confidential proprietary information, including customer lists.

The survey noted numerous differences between the public and private sectors in regard to cyber risk, and this was one: respondents from governmental organizations expressed greater concern about data breaches affecting employee information (nearly half, compared with just over one-third of private-company respondents), while the private side was twice as concerned about customer data breaches—over 60 percent saying so, compared with just over 30 percent on the government side.

But organizations are nearly as concerned about the legal and regulatory threats that can result from breaches. While respondents most frequently placed business income loss (39.5 percent) and the cost to restore crucial proprietary electronic information (35.5 percent) among their top five concerns, the next

A sizable minority—more than 20 percent—say their company's budget for activities to maintain information security and privacy is inadequate.

three were legal defense and settlement costs from third party claims (34.9 percent), costs to comply with regulatory settlements (30.9 percent), and costs to defend against regulatory investigations (30.3 percent).

"Regulation and compliance are absolutely the key drivers of what most organizations are attempting to do in the way of cyber risk," said Graham. And while more than two out of three survey respondents felt government and business need to do more to collaborate on programs to increase information security and privacy risk management, they also expressed concern about legislative and regulatory overreach in this area, with more than half citing restrictive new data protection rules now under consideration by the EU and almost half citing a proposed breach notification requirement—changes that would, of course, apply to all 27 EU member states.

"European-wide potential sanction [for data breach] would be up to €1 million for individuals and no less than 2 percent of annual worldwide turnover for companies," noted Graham. Yet only 39 percent of survey respondents said their organization is in compliance with baseline standards set by law on information security and privacy—although here, the public sector appears to be doing better, with almost three-quarters of respondents saying their organization is in compliance. But only 22.4 percent of all respondents said their organization is in compliance with baseline standards set by standards-setting bodies.

Managing Cyber Risk

Cyber risk is not something that organizations can suppress or reduce to insignificance, however. "All companies now rely on IT and technologies such as computing [and] mobile devices, and allow employees to work on their own devices," pointed out Jérôme Gossé, financial lines underwriter at Zurich Global Corporate. So incidents will happen, and preparations for incident response are vital.

The news, in this respect, is mixed. Almost two-thirds of survey respondents say their organization has formally assigned roles and responsibilities to key individuals as part of an incident response plan. But few have made contingency plans with preferred vendors. And less than half said they have a strategy for communication to the general public in case of a cyber risk incident, although the public sector is doing better in this respect, with more than 60 percent of respondents saying they have done so.

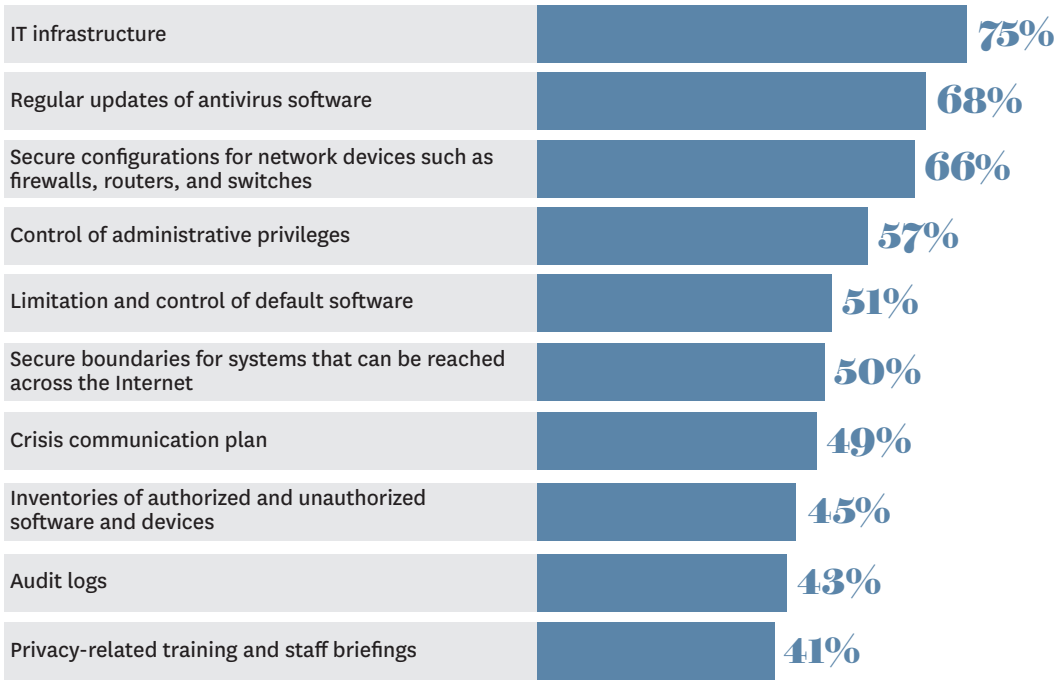
Organizations surveyed are introducing new systems and standard practices to mitigate information security and privacy risk. Three out of four respondents said their organization has introduced new IT infrastructure and more than two out of three now regularly update their antivirus software, while a similar proportion have introduced secure configurations for network devices such as firewalls, routers, and switches. figure 3

The survey also indicates progress in monitoring and evaluating cyber security systems and practices. More than half of respondents said their company evaluates its information security and privacy systems and practices regularly—although the public sector lags here, with only a little less than a third of respondents agreeing—while nearly one in three of all respondents do so occasionally. More than 80 percent

Figure 3

Top 10 Areas Where Company Has Introduced New Information Security Standards

QUESTION: IN WHICH OF THE FOLLOWING AREAS HAS YOUR COMPANY INTRODUCED NEW SYSTEMS AND STANDARDS OF PRACTICES TO MITIGATE INFORMATION SECURITY AND PRIVACY RISK?



said they evaluate or reassess systems and practices either annually or continually. These activities are performed in-house at more than 80 percent of companies, rather than by external contractors.

Communication about cyber risk issues is better as well, said Graham: "Knowledge of breaches has improved. Two years ago, when I looked at this subject, people didn't tell each other about what was going wrong."

But a sizable minority—more than 20 percent—say their company's budget for activities to maintain information security and privacy is inadequate, while nearly 10 percent said they don't know whether it is or not. And despite the dominant opinion that information security and privacy matters have become more important over the past three years, less than half said their company's budget for these matters has increased.

Building Awareness

The substantial progress that has been made at many companies suggests that a fairly distinct picture is emerging of what constitute best practices in cyber risk management.

Fishleigh divides the task of cyber security maintenance into four buckets:

- Understanding the specific risk that you face as an organization, as opposed to generalized cyber risk, and deciding how you are going to deal with it;
- Protecting the critical information assets you hold as a business;

- Monitoring your IT estate to spot things that get past your protections; and
- Having a tried and tested capability to contain, recover, and learn from incidents, which can happen even in the most secure environments.

To make all of these segments work requires "bringing all the stakeholders together," said Fishleigh, which, Graham added, "is everybody."

Aside from the CIO or the IT department, she noted, "cyber security is very much the domain of the human resources manager, managing confidentiality agreements in people's contracts, for example. It's the domain of your marketing or development department, who often own the development and use of your social media policy. Therefore this is a classic enterprise risk. You need your whole business or organization to consider this risk from their point of view."

The solutions need not be highly complex. The focus, Graham said, "should be on managing these issues, whether that's through education or training. It doesn't have to be through spending a lot of money to put up fantastic firewalls around your systems. Some of the most simple measures of prevention can be the most effective."

For example, Graham said, "Manage your documentation correctly. Don't let that become another risk by removing documents that are properly stored electronically and putting them on unencrypted memory sticks—because you can kill one risk and then watch it become a problem somewhere else."

Getting the message across about such concerns requires good communication, said Graham: "Especially with people who work at home or are mobile, getting education and awareness right puts you 80 percent of the way there. But use language that people understand. Don't use technospeak, or people's eyes will glaze over."

That includes, especially, the board. A valuable resource, Graham suggested, is any one of the government or independent initiatives on electronic security, such as the UK's Centre for Protection of National Infrastructure or the Information Security Forum. "Get some of their people in front of your board" to discuss their findings and the need to raise awareness, she says, "so that they are getting it from a third party that has credibility internally and externally."

Building Processes

A company's security from cyber risk depends greatly on the information it collects and how it analyzes that information, however.

"Get the group of stakeholders together who own the information assets," said Fishleigh. "That group needs to work with the risk and security specialists to assess the specific threats the organization is likely to be facing. Then you layer over them your company's particular controls—not just technical but also governance processes, organization, and human factors—to develop a view of the net information security risk exposure of the organization. At the detailed level, you end up with a matrix that plots all those risks against the likelihood of them occurring and the impact should they occur."

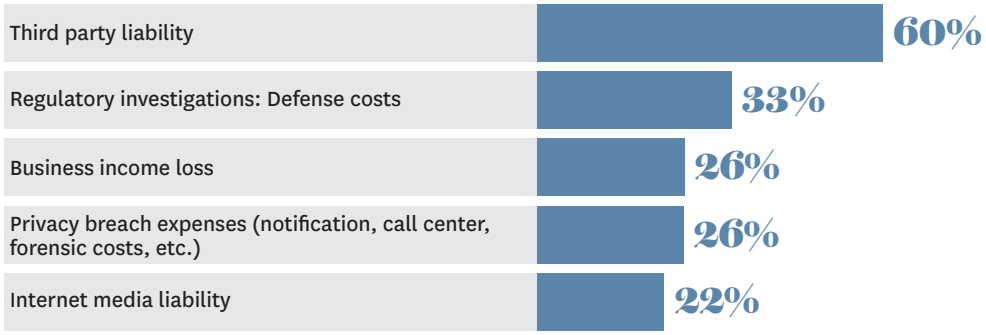
Humanizing it also helps, Fishleigh added. When presenting the findings to the board or other stakeholders, "consider using a few scenarios that show how this could happen, bringing to life both the event and the impact," he suggested. "Once you have that matrix, you can then work out which risks are above the risk tolerance that your organization is prepared to live with."

While many companies report success at maintaining internal cyber security, their links with other organizations—particularly suppliers, as supply chains grow longer and more complex—are less easy to manage. "Monitoring must be multilayered" to detect, prevent, and respond to threats that could be impinging on the organization from these directions, said Fishleigh, "and that could evade your first line of defense."

Figure 4

Top Five Types of Insurance Coverage

QUESTION: WHAT TYPES OF COVERAGE(S) DID YOU PURCHASE?



Once the risks that exceed the risk tolerance level have been identified, the organization must decide how to address these. Ideally this should be through a pragmatically sized program that employs a combination of people, process, and technology measures to address the highest risks first. "Not all the information an organization holds is equally confidential," Fishleigh argued. "It may be worth building walls around the more sensitive information, but if you do this you should also understand where you're going to put gates in the walls and how you're going to set up the rules that allow information to pass through those gates."

Technologies are now becoming more available, he noted, that allow information to be exchanged between networks of greater or less security while maintaining overall segregation between them.

Insuring Against Cyber Risk

"Insurance is the last step in the process of addressing cyber risks," said Gossé—the last line of defense after organizational and technological processes and tools are in place. But given the frequency of incidents in sensitive industries such as finance, retail, and manufacturing as well as government, "there's wide interest in cyber insurance." The problem, Gossé noted, is that traditional policies, like commercial general liability insurance, do not cover these risks and generally cannot be extended to do so.

Cyber insurance policies are now available to fill the gap. But few organizations—less than 20 percent, according to survey respondents—have purchased security and privacy insurance specifically designed to cover exposures associated with information security and privacy-related issues. Of these, the type of coverage most frequently cited—by a little more than 10 percent of respondents—is third-party liability insurance, which can cover costs related to a claim resulting from a security breach, a data breach, or violation of a privacy regulation. Regulatory and litigation concerns were the most cited reasons for doing so. But more than 60 percent of respondents said their company has no plans at all to purchase coverage. The results were largely similar in both the public and private sectors. figure 4

This analysis reflects the results of a Harvard Business Review Analytic Services Web-based survey conducted with 152 respondents involved in risk management for their organization. Virtually all respondents were based in Europe. Data was collected July-September 2012.

FOR MORE INFORMATION ON
HARVARD BUSINESS REVIEW ANALYTIC SERVICES:

hbr.org/hbr-analytic-services

Harvard
Business
Review