SPECIAL REPORT

A New Era In Information Security and Cyber Liability Risk Management

A Survey on Enterprise-wide Cyber Risk Management Practices

October 2011

Sponsored by:

ZURICH®

A New Era In Information Security and Cyber Liability Risk Management

A Survey on Enterprise-wide Cyber Risk Management Practices

EXECUTIVE SUMMARY

The vast majority of risk professionals acknowledge that information security and other cyber risks are at least a moderate threat to their organizations. Most say cyber exposures are the focus of specific risk management activities within their organizations. The level of sophistication in addressing these risks varies widely, though a growing number of organizations are adopting an enterprise-wide – or at least a multi-departmental – approach to information security and cyber risk management. However, only about one third of organizations currently purchase insurance as a part of their cyber risk management strategy.

INTRODUCTION

A growing number of organizations are now realizing that cyber security extends well beyond the IT department.

Cyber-related risks traditionally were regarded strictly as the domain of an organization's Information Technology (IT) department. Many believed that the IT department would keep the organization secure because viral infections and data breaches by hackers were issues best addressed by protections such as firewalls and antivirus software, which were IT solutions.

A growing number of organizations are now realizing that cyber security extends well beyond the IT department. A wide range of issues such as lost or stolen data, violation of privacy laws, intellectual property infringement and social media-related risks such as cyber-bullying and textual harassment constitute a much broader scope of cyber exposures. This has led many organizations to recognize that relationships among Risk Management, Information Technology, and other departments are essential in defending against cyber-related threats and implementing comprehensive protection mechanisms that minimize risks.

ABOUT THE SURVEY AND THE RESPONDENTS

Most respondents classified themselves as risk managers (58 percent), followed by risk management department professionals at 17.8 percent and enterprise risk managers at 8.7 percent.

To gain insight into the current state of enterprise-wide information security and cyber liability risk management, Zurich sponsored a survey administered by Advisen Ltd. In addition to collecting data on information security and cyber risk management, the survey was designed to help create a framework for identifying and addressing cyber risks throughout an organization. The survey was conducted for one week, beginning September 26, 2011 and ending October 3, 2011. Invitations to participate were distributed by email to 7,672 risk managers, insurance buyers and other risk professionals. The survey was completed at least in part by 503 respondents, for a response rate of 6.6 percent.

Most respondents classified themselves as risk managers (58 percent), followed by risk management department professionals at 17.8 percent and enterprise risk managers at 8.7 percent. Respondents with more than 20 years of risk management and insurance experience represent the largest group at 44.1 percent of the total, followed by 28.5 percent with between 11-20 years, 16.2 percent between 6-10 years and 11.1 percent with 5 years or less.

A broad array of industries is represented. Health Care Providers and Services account for the largest industry sector with 12.9 percent of the total respondents, followed by Government-Local at 5.9 percent, Education-Post Secondary at 4.8 percent and Finance-Banks/Commercial at 4.6 percent. Others/Not Listed comprised 7.9 percent. The survey includes businesses of all sizes but is weighted towards the larger companies with 59.7 percent of respondents having revenues greater than $1 billion.

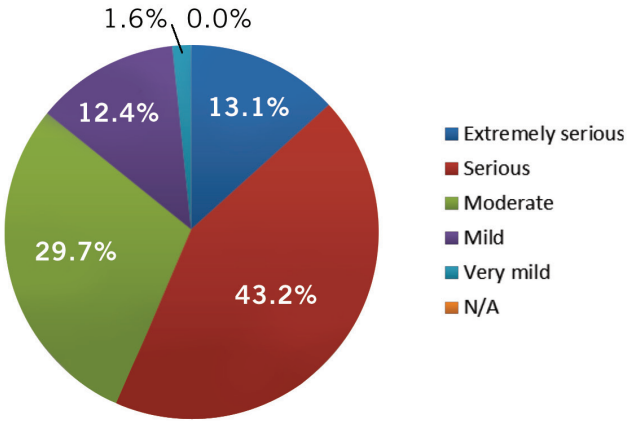
ATTITUDE TOWARDS INFORMATION SECURITY AND CYBER RISKS

The vast majority of respondents believe that information security and other cyber-related exposures pose a threat to their organizations. In response to the question "How would you rate the potential dangers posed to your organization by cyber & information security risks." 13.1 percent said extremely serious, 43.2 percent said serious, 29.7 percent said moderate, 12.4 percent said mild and 1.6 percent said very mild.

In total, 86.0 percent of respondents agree that cyber and information security risks pose at least a moderate danger to their organization. (Exhibit 1)

Exhibit 1

How would you rate the potential dangers posed to your organization by cyber & information security risks?



Information security and cyber liability has become an important topic for organizations of all sizes across all industries.

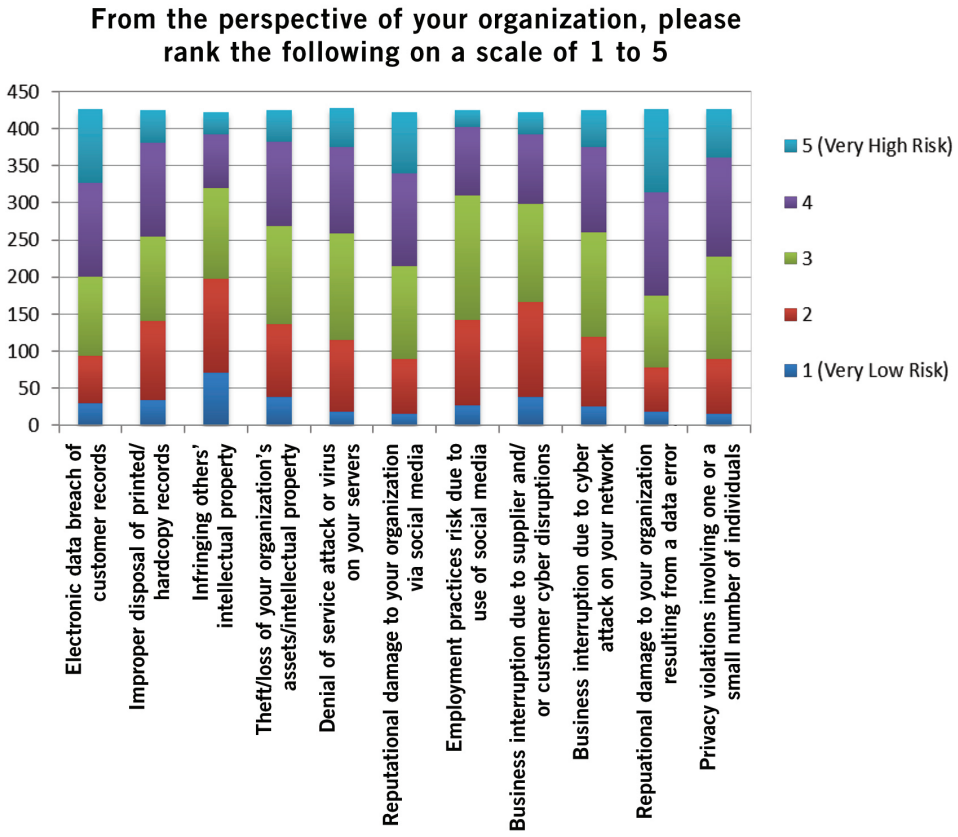
Information security and cyber liability has become an important topic for organizations of all sizes across all industries. Smaller companies (revenue less than $250 million) viewed cyber risks less seriously than the largest companies (revenue greater than $10 billion), with 79.3 percent of smaller companies saying the risks pose at least a moderate danger compared to 97.2 percent of large companies.

Of the total respondents, 71.7 percent said that information security risks are a specific risk management focus within their organization. However, in the opinion of the survey respondents, the threat is viewed less seriously by key decision-makers. In response to the question "in your experience, are cyber risks viewed as a significant threat to your organization by:" 45.3 percent said yes to board of directors and 57.9 percent said yes to C-suite executives. This suggests that more communication may be necessary with upper level management to educate them on the risks of cyber-related exposures.

On a scale of one to five, with 5 as a very high risk and 1 as a very low risk, "reputational damage to an organization as a result of a data breach" was the biggest concern of respondents, with 59.4 percent giving it rating of a 4 or 5. This was followed by "electronic data breach of customer records" with 53.7 percent and "reputational damage to the organization via social media" with 49.3 percent. In contrast, the exposures that were perceived as representing the lowest risks, and had the highest percentage of respondents providing a rating a 1 or 2, included "infringing on others' intellectual

property" with 46.7 percent, "business interruption due to supplier and/or customer cyber disruptions" with 39.3 percent and "employment practice risks due to use of social media" at 33.6 percent. (Exhibit 2)

Exhibit 2



DISASTER RESPONSE

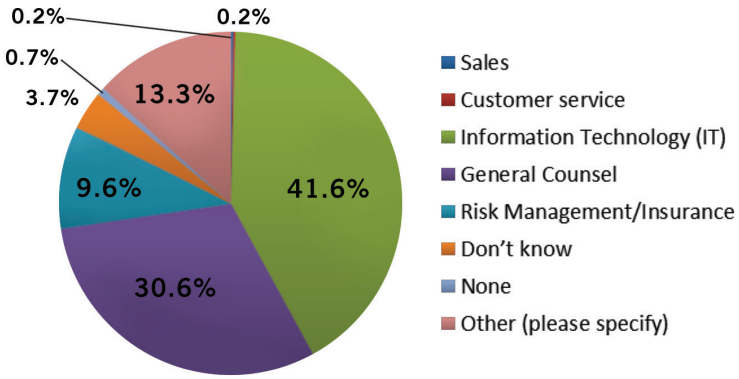
Research has shown that organizations with a comprehensive disaster response plan in place before a breach occurs fare much better after a major breach than those that do not. Of total respondents, 68.8 percent said that they have a disaster response plan in place, only 16.5 percent said that they do not and 14.7 percent did not know. The larger companies (revenue greater than $1 billion) represent a bigger portion of the total with 79 percent having a disaster response plan compared to only 55 percent of the companies with revenue under $1 billion.

In response to "In the event of a data breach, which department in your organization is PRIMARILY responsible for assuring compliance with all applicable federal, state, or local privacy laws including state breach notification laws?" the largest percentage of

respondents answered Information Technology at 41.6 percent of the total and General Counsel at 30.6 percent. (Exhibit 3) The bigger the company however, the more they rely on their General Counsel (36 percent as opposed to 26 percent IT for companies with revenue greater than $5 billion). In contrast, of the companies with annual revenues under $5 billion, 40 percent relied on IT compared to only 23 percent General Counsel.

Exhibit 3

In the event of a data breach, which department in your organization is PRIMARILY responsible for assuring compliance with all applicable federal, state, or local privacy laws including state breach notification laws?



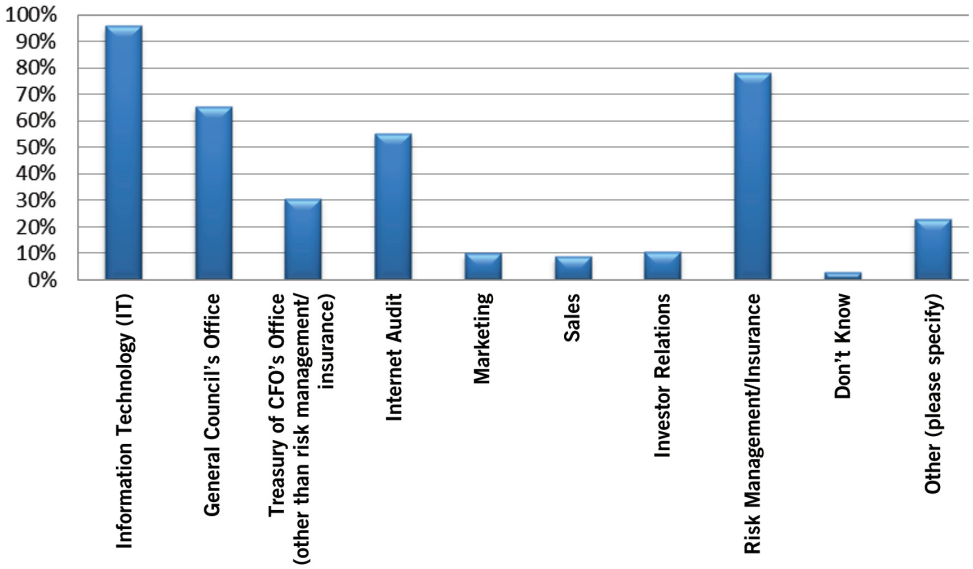
INFORMATION SECURITY AND CYBER RISK MANAGEMENT FOCUS

The majority of survey respondents recognized that it is the responsibility of the entire organization to mitigate risks. When asked "Does your organization have a multi-departmental information security risk management team or committee?" 57.2 percent of those who responded said yes and 34 percent said no. The departments or functions that are most likely to have representation in the information security risk management team are IT with 95.9 percent, Risk Management/Insurance 78.1 percent, General Counsel 65.7 percent, Internal Audit 55 percent, Treasury or CFO 30.2

percent, Other 23.1 percent, Investor Relations 10.7 percent, Marketing 10.1 percent, Sales 8.9 percent and 3 percent did not know. (Exhibit 4)

Exhibit 4

Which departments are represented on your cyber risk management team?



The fact that nearly half of respondents that do not currently buy insurance but are considering buying coverage or are not sure is a strong indication that this coverage represents a growth opportunity for brokers and insurers.

Although information security and cyber risk management was recognized as an enterprise-wide responsibility by many respondents, the IT department still is acknowledge as the front line defense against information losses and other cyber liability risks. Of those who answered the question "Which department is PRIMARILY responsible for spearheading the information security risk management effort?" 73.2 percent said it was the responsibility of the IT department, followed by 13.2 percent who said it was the Risk Management/Insurance department's responsibility.

As noted above, nearly half of organizations consider reputational damage via social media a significant threat to their organizations. Of the companies surveyed, 63.6 percent have social media policies in place, 26.7 percent do not and 9.7 percent do not know. The larger companies represent a bigger portion of the companies who have social media policies in place with 71 percent compared to 54 percent of the smaller companies.

THE ROLE OF INSURANCE IN INFORMATION SECURITY AND CYBER RISK MANAGEMENT

Although information security and cyber risks were widely acknowledged as serious concerns, cyber liability insurance is not purchased by a majority of organizations. Survey participants were asked "Does your company buy cyber liability insurance?" Of those answering the question, 35.1 percent said yes while 60.1 percent said no. The larger organizations ($1 billion in revenue and above) represent only a slightly higher percentage of the total yes responses at 36 percent compared to 34 percent of the smaller organizations.

More than two-thirds of respondents claimed that information security risks are a specific risk management focus within their organizations.

According to the participant's comments, some explanations for why companies do not purchase cyber liability insurance include:

- investment in prevention rather than insurance,
- limited markets,
- broker disconnects,
- lack of coverage clarity,
- lack of information to make informed decisions,
- too expensive,
- application process is difficult,
- deductibles are too high,
- difficult to quantify, and
- policy coverage is too limited.

Of those who purchase coverage, 37.9 percent said that they have purchased coverage for less than two years, 37.1 percent said between three and five years and 25 percent said over five years. This suggests that the number of organizations that recognize the role that insurance can play as part of an information security and cyber risk management program is increasing.

Companies that currently do not purchase cyber liability insurance were asked "Are you considering buying this coverage in the next year?" 24.3 percent said yes, 52 percent said no and 23.6 percent said that they do not know. The fact that nearly half of respondents that do not currently buy insurance but are considering buying coverage or are not sure is a strong indication that this coverage represents a growth opportunity for brokers and insurers.

ANALYSIS AND CONCLUSIONS

The IT department often is ill-equipped to interpret the notification requirements of dozens of states and to marshal the resources necessary

The vast majority of organizations view information security and other cyber risks as at least a moderate threat. Larger organizations view the risk as only slightly more important than their smaller counterparts, but as a whole they tend to be more involved in enterprise-wide risk management.

More than two-thirds of respondents claimed that information security risks are a specific risk management focus within their organizations. Organizations increasingly have implemented, or are in the process of implementing, an organization-wide information security approach. Most organizations have some form of multi-departmental information security and cyber risk team or committee. For most, the IT department plays a leadership role in the information security and cyber risk management process, but the Risk Management department, the General Counsel's office and Internal Audit play significant roles in a majority of the companies having multi-departmental teams or committees.

More than two thirds of respondents said their organizations have a disaster response plan in place in the event of a major breach. For 41 percent of respondents, the role of the IT department includes fulfilling state data breach notification laws following a breach. This may represent a significant deficiency in emergency response planning. The IT department often is ill-equipped to interpret the notification requirements of dozens of states and to marshal the resources necessary to fulfill the requirements of each state following a major breach.

While most companies have implemented information security and cyber risk management programs, for the majority of these organizations, cyber insurance is not incorporated as part of the overall strategy for many. The growing interest in the coverage, however, is apparent with the increased number of companies that have purchased protection in recent years, or are planning on buying coverage in the near future. ■

This Special Report was written by Josh Bradford, Associate Editor, Advisen Ltd.

ABOUT ZURICH

Zurich Financial Services 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, Middle East as well as other markets. Zurich offers a wide range of general insurance and life insurance products and services for individuals, small businesses, mid-sized and large companies as well as multinational corporations. Zurich employs about 60,000 people serving customers in more than 180 countries. Founded in 1872, the Group is headquartered in Zurich, Switzerland.