Information Security & Cyber Liability Risk Management

The Second Annual Survey of Enterprise-wide Cyber Risk Management Practices in Europe

February 2013
Executive Summary

It seems hardly a day passes without another high profile data breach being reported. Increasingly, these breaches are sophisticated and highly targeted attacks, and no company can consider itself immune. While at one time hackers were often no more than bored teenagers out to cause a bit of mischief, many of today’s sophisticated attacks are executed with clear malicious intentions, usually financially or politically motivated, by organized crime rings, hacktivist alliances or state-sponsored industrial espionage teams. As a result, information security and other cyber risks increasingly are viewed as a significant threat by the European risk management community, and are becoming a specific risk management focus for more organizations.

About the Survey Respondents

For the second consecutive year Advisen Ltd administered a survey sponsored by Zurich to gain insight into the current state of and trends in information security and cyber risk management in Europe. The survey was conducted for 10 days beginning on Monday, 11 February, 2013, and ending on Wednesday, 20 February, 2013. The survey was completed at least in part by 41 risk managers, insurance buyers and other risk professionals.

The largest percentage of respondents (59.0 percent) classified themselves as Members of Risk Management Departments (not Head), followed by Chief Risk Manager/Head of Risk Management Department at (37.0 percent) and Other Executive Management (5.0 percent). Respondents with more than 20 years of risk management experience represented the largest group at 56.1 percent of the total, followed by 22.0 percent with between 11-20 years, 19.5 percent with 6-10 years and 2.4 percent with 5 years or less.

The distribution of survey respondents based on the location of their head office is 36.6 percent in the UK, 34.2 percent other EU country, 12.2 percent Europe other than EU, 4.9 percent North America, 7.3 percent Asia, 2.4 percent Africa and 2.4 percent Australia/New Zealand. The survey includes businesses of all sizes but is weighted towards larger organizations, with more than two thirds of respondents having annual turnover of greater than €1 billion.
Perception of Cyber Risks

The vast majority of respondents (85.7 percent) believe that cyber risks pose at least a moderate threat to their organizations. This is slightly lower than the 90.0 percent reported in 2012. However, the threat level has elevated for more respondents, with 25.7 percent believing cyber risks pose an extremely serious threat to their organization, a 15.7 point increase over 2012.

While cyber risk is viewed as a more serious threat by some in the risk management community, the perception is basically unchanged for Board Members and Senior Executives. In response to the question “In your experience, are cyber risks viewed as a significant threat to your organization by:” 52.9 percent said “yes” for Board of Directors (53.8 percent in 2012) and 71.4 percent said “yes” for Senior Executives (69.2 percent in 2012). Fewer said “yes” this year for Suppliers/Customers: 23.5 percent compared to 31.6 percent a year ago.

In response to the same question, for larger organizations (those greater than £1billion annual turnover), information security and cyber liability is viewed as a slightly greater threat by Board Members at 56.5 percent and by Senior Executives at 73.9 percent.
Respondents were asked to rank enumerated risks on a scale of 1 to 5, with 5 as very high risk and 1 as very low risk. Based on the weighted average of responses, the biggest concern of this year’s respondents is a denial of service attack or virus on their server (weighted average of 3.55), followed by reputational damage to their organization due to a data breach (3.44). In contrast, the exposures perceived as representing the lowest risks are infringing others’ intellectual property (2.71), preceded by employment related risk due to social media (2.76).

In 2012, the biggest concern was reputational damage via social media (3.58) and the exposure with the lowest perceived risk was also infringing on others’ intellectual property (2.81).
Research has shown that organizations that have implemented a comprehensive disaster response plan prior to a breach fare much better after a breach occurs than those that have not. According to the results of this survey, it appears that this message is indeed gaining traction with many organizations. When asked “Does your organization have a disaster response plan in place in the event of a data breach incident?” 58.8 percent said “yes.” This represents nearly a 9 point increase from 2012. However, this percentage is still significantly lower than their North American counterparts who were asked the same question in a similar survey in 2012. Of the total respondents to that survey, 80.4 percent said that they have a disaster response plan in place – a 21.6 point difference.

In response to the question “In the event of a data breach, which department in your organization is most responsible for assuring compliance with applicable privacy laws?” the most common response was Information Technology (IT) at 34.4 percent, followed by General Counsel at 31.3 percent and Regulatory/Compliance at 12.5 percent. When asked, “In your opinion is your organization prepared to respond to the data security and privacy laws of all countries in which you do business?” 42.4 percent responded “yes,” while 27.3 percent responded “no.”
In response to the question, “Are information security risks a specific risk management focus within your organization?” 75.8 percent responded “yes,” 15.2 percent responded “no” and 9.1 percent did not know.

Exactly half of the respondents claim to take a multi-departmental approach to their information security risk management efforts, with the highest percentage (48 percent) saying it is the responsibility of the Information Technology department to spearhead the initiative. Consistent with the 2012 survey, the departments most likely to be represented on this team or committee include Information Technology (100 percent), Risk Management/Insurance (76.9 percent) and General Counsel’s Office (53.8 percent).
Social media continues to be recognised as an exposure that requires risk management attention with more than half (56.3 percent) of the total respondents claiming that their organization has a written social media policy.

**Mobile Devices and Cloud Computing**

Included in this year’s survey were questions on two of the biggest information security and cyber liability topics of 2012, mobile devices and cloud computing. Respondents were asked “Does your organization have a mobile device security policy?” to which 68.8 percent responded “yes,” 21.9 percent “no” and 9.4 percent did not know.

Businesses also are increasingly allowing their employees to use their personal mobile device for business purposes. These devices are now capable of accessing proprietary company information and creating a significantly more difficult exposure to control. When asked “Does your organization have a bring-your-own-device (BYOD) policy?” 40.6 percent said “yes,” 43.8 percent said “no” and 15.6 percent did not know. Larger companies (€1 billion and above annual turnover) are more likely to have a BYOD policy with 45.45 percent responding “yes” compared to 37.5 percent of companies with annual turnover’s less than €1 billion.
Cloud computing is becoming a popular alternative for businesses seeking cost effectiveness and increased storage capacity. However, the idea of warehousing proprietary business information on third-party servers has led many to question how secure this alternative really is. In response to the question “Does your organization use cloud computing services?” 56.3 percent said “yes,” 28.1 percent said “no” and 15.6 percent did not know. Smaller organizations (less than €1 billion annual turnover) were more likely to use cloud computing services with 87.5 percent responding “yes” compared to half of larger organizations.

Respondents were also asked “is cloud computing a component of your data security risk management process?” to which 44.1 percent said “yes” and 23.5 percent said “no.”

The Role of Insurance in Information Security and Cyber Risk Management

Although information security and cyber risks are widely acknowledged as at least a moderate threat to most organizations, cyber liability insurance is still purchased by only a small percentage of respondents. This percentage, however, is trending upward. Survey participants were asked “Does your organization buy cyber liability insurance?” to which 11.8 percent said “yes” as compared to 7.9 percent in 2012. The percentage of European organizations purchasing cyber liability insurance is significantly less than their North American counterparts, where 43.9 percent of respondents said “yes” to the same question.

Conclusions

Data security and other cyber exposures are recognised as a significant threat by most risk managers, senior executive and board members of European organizations. These organizations are taking steps to manage the threats, but strategies and tactics vary widely. Experts stress that data security is a problem that requires an enterprise-wide solution, and half of respondents now have a multi-departmental approach to managing the risk. However, nearly half of respondents said that it is the IT Department’s responsibility to lead the data security initiatives in their organizations, a practice that experts say may lead to over-reliance on software solutions.

Many organizations recognise that their risk profiles are changing, and more than two-thirds now have mobile device policies. However, less than half confirmed that their organizations have policies concerning employees using their own devices for company business. Less than half of organizations incorporate cloud computing within their data security risk management process. Despite the fact that data security is perceived as a serious threat, very few organizations buy cyber insurance products. Organizations are clearly making progress in addressing data security issues and other cyber exposures, but they risk not acting quickly enough to counter a rapidly evolving threat landscape.