INFORMATION SECURITY AND CYBER RISK MANAGEMENT

The seventh annual survey on the current state of and trends in information security and cyber risk management

EXECUTIVE SUMMARY

No company is completely safe from a catastrophic cyberattack. How concerned is your organization? What are you doing to prepare?

The seventh annual Information Security and Cyber Risk Management survey from Zurich North America and Advisen Ltd. surveyed 315 risk professionals to gain a deeper understanding of corporate attitudes and strategies around cyber risk.

This year’s survey comes on the heels of major events including the Dyn DDoS attack, WannaCry and Petya ransomware, and major data breaches that are impacting millions of consumers in the United States. These attacks, all very different in scope and effect, will each likely have lasting implications for how businesses and the insurance industry prepare for, and respond to, cyber threats in the future.

As in previous years, the 2017 study was designed to provide a benchmark for future cyber risk preparedness and response strategies. The study provides insights into the following questions:

1) Are risk professionals’ views towards business continuity risks evolving?
2) Are risk professionals remaining vigilant in their approach to data integrity risks?
3) Are boards and executive management changing their perceptions of cyber risk?
4) How are businesses implementing their cyber risk management strategies?
5) How does insurance fit in to their overall cyber risk strategies?

RISK PROFESSIONALS VIEW BUSINESS CONTINUITY RISK LESS SERIOUSLY THAN DATA INTEGRITY RISK

High-profile cyber events like those mentioned above have brought to light the potential for substantial cyber losses that go beyond data breaches. The survey revealed, however, that many risk professionals remain less concerned about these types of business continuity risks (i.e., cyber-related business interruption) than data integrity risks (i.e. data breach). This could indicate that risk professionals are either less educated about the exposures, have concluded these exposures are less significant to their business, or are confident (or overconfident) in their cybersecurity controls. Or the reason could be that risk professionals are not fully aware that the nature of cyber risk has been evolving beyond data security and toward interconnected risks including business interruption due to malware and ransomware attacks.

- Despite recent breaches and ransomware events, only 53 percent of respondents knew of changes/upgrades made following high-profile attacks in early 2017.
- When asked to rate how their company views various risks, business continuity risks are generally viewed less seriously than data integrity risks. On average, 35 percent of the respondents rated data integrity risks as “high risk” compared with 22 percent for business continuity risks.
In fact, data integrity risks account for the top four cyber exposures as rated by risk professionals. In order, those exposures are:

- Employee unintentionally infecting a company’s network with malware (rated #1 for second consecutive year);
- A cyberattack via malware;
- Reputation damage due to privacy violation/loss of customer records;
- Privacy violation/data breach of customer records;
- The highest-rated business continuity risk – the fifth highest overall – is business interruption due to a cyber disruption.

**Board members and executive management are believed to be less concerned about cyber risk than previous years**

For the first time in the seven years of this study, risk professionals believe board members and executive management view cyber risk less seriously than the prior year. This could indicate board members have become more comfortable in their understanding of cyber exposures. An increased enterprise-wide focus on cyber risk and better communication to company leadership may have eased concerns and increased confidence in cyber security controls. Or it could mean risk professionals are not up to date on the evolving nature of cyber risk and the possible magnitude of the losses.

- Sixty-two percent of the risk professionals surveyed said boards of directors view cyber risk as a significant threat to their organization. This is down from 83 percent in 2016.
- Sixty percent of the risk professionals surveyed said executive management view cyber risk as a significant threat to their organization. This is down from 85 percent in 2016.

**Businesses are taking a multifaceted approach to cyber preparation and response strategies**

When a cyber incident occurs, a coordinated and well-rehearsed response could significantly reduce the impact. Many organizations are taking a multifaceted approach to their preparation and response strategies by utilizing a combination of internal and external resources. Effective coordination among different parties can be a complicated process, but it can make all the difference when trying to keep a situation from spiraling out of control.

- Cyber risk management program assessment is the most common external pre-incident service utilized.
- Assessment of procedures for protecting sensitive data is the most common internal pre-incident resource utilized.
- Vendor risk assessment is the least frequently conducted pre-breach service by both internal and external resources.
- Cross-departmental communication is evident. Ninety-seven percent of respondents said the risk management team works with their colleagues in IT at least occasionally. Seventeen percent consider IT a member of the risk management team.
- Including security requirements in every request for proposal (RFP) and contract is the vendor management control most frequently utilized to manage supply chain risk.
- Respondents who experienced a data integrity event (i.e., data breach) most commonly utilized external resources for credit monitoring and legal services. Forensic investigation and crisis management are the internal resources most commonly utilized.
Respondents who experienced a cyber-related business continuity event (i.e., business interruption) most commonly utilized external resources for legal services. Forensic investigation and crisis management are the internal resources most commonly utilized.

Insurance continues to play an important role

The cyber risk landscape is fluid and cyber insurance products continue to evolve in response to that landscape. As a result, the cyber insurance take-up rate has increased substantially since 2011, the first year of this study, although there are signs the market may be maturing.

- Over the last seven years, the proportion of companies buying cyber insurance has increased from 35 percent in 2011 to 65 percent in 2017.
- Growth in the purchase of cyber insurance appears to be slowing, however.
- Expenses/fines related to breach of customer/personal information is the primary driver for purchasing a cyber insurance policy.
- Conversely, just 10 percent of respondents identified business interruption as the primary reason for purchasing the cover.

Overall, the results indicate that businesses may not be keeping up with cyber-related risks or the steps needed to protect themselves against cyber-related attacks. And the evolving threat landscape, which increasingly exposes organizations to business continuity-related losses, has yet to reach the same level of alarm among the risk management community as the more traditional data integrity risks. Since business continuity events are growing in both frequency and severity, the insurance industry should further educate their clients on these exposures, provide access to pre- and post-incident resources, and offer products that meet the needs of their insureds.

KEY FINDINGS

Although the term has been around for quite some time, 2017 is the year ransomware became recognized vernacular for most of the general public. This is thanks to a number of high-profile events including the Petya and WannaCry attacks. Ransomware and other non-privacy related cyberattacks have proven equally destructive in terms of their impact, including slowing and in some cases totally shutting down business operations. For example, a multinational courier delivery service recently attributed a $300 million loss to the Petya ransomware attack that impacted the company’s operations across Europe in July.

With this in mind, respondents were asked if their organizations have made changes to cyber security controls as a result of these kinds of high-profile cyber events. Only 53 percent of respondents knew of changes/upgrades made following high profile attacks in early 2017.

“We have mandatory information security awareness and privacy training programs for our staff and all new hires to take (and pass)” explained one respondent. “In addition to the on line security training, our approach is to make security awareness training a part of the associate’s day-to-day life by displaying banner messages posted on the intranet home page, email communications, and lobby monitor displays.”

Another respondent said, “(We) revised all contracts to require third-party property managers on residential (properties) to have a cyber naming firm. (We are) in the process of bringing on board an IT Director and team versus third-party consultants.”
“We have implemented increased behavior-based threat detection and regular communications to the company explaining email phishing and social engineering plots,” noted another respondent.

Has your organization made changes to its cybersecurity controls as a result of recent high-profile cyber events such as the Dyn DDoS attack, WannaCry ransomware, and Petya ransomware?

Respondents were also asked to rate the two separate sets of exposures – data integrity risks and business continuity risks – on a three-point scale ranging from low risk to high risk. Overall, risk professionals remain more concerned about data integrity risks. On average, 35 percent of the respondents rated data integrity risks as “high risk” compared with 22 percent for business continuity risks. The below charts show the ratings broken out by risk.

From the perspective of your organization, please rate each of these data integrity risks from 1 (low risk) to 3 (high risk)

From the perspective of your organization, please rate each of these business continuity risks from 1 (low risk) to 3 (high risk)
A company’s industry has an influence on this perspective, however. Taking out respondents from industries that store large amounts of personal data such as communications, healthcare, finance, insurance, banking, retail and services, the average data integrity high risk rating dropped from 35 percent to 29 percent.

**Board members and executive management views on cyber risk**

In response to the question, “In your experience, are cyber risks viewed as a significant threat to the organization by….?” 62 percent of respondents answered “board of directors,” which was down substantially from 83 percent giving that response in 2016. Sixty percent said “C-suite executives,” which was also down substantially from 85 percent in 2016.

Not surprisingly, risk managers and IT personnel rated the highest at 86 percent and 93 percent respectively, while suppliers and customers rated the lowest at 17 percent and 26 percent respectively.
Survey results showing that fewer executives are worried about cyber, despite the growing risk. This could be an indication that some leaders may be not aware of the magnitude of impact that business interruption losses are beginning to have on businesses.

It’s also possible that better communication with leadership could be part of the reason. Leadership may believe cyber-related threats are less significant due to better understanding of organizational exposures and therefore be more comfortable with the risk. Thirty-one percent of risk professionals said there have been changes in the way cyber-related exposures and events are reported back to company leadership in just the past year.

“A brand new cyber security organization was developed, from one individual to eight resources. Cyber security is a board-level topic at every meeting,” said one respondent.

“The events are logged and presented to the Executive Management. Further, the logs/reports are shared with our external auditors for verification during our formal audit process,” another respondent explained.

“Incidents are reported to an Information Security team who informs the President and Board of Trustees,” answered another risk professional.

In the past year have there been any changes in the way cyber-related exposures and events are reported back to company leadership?

- Yes
- No
- Don’t know

Companies engaged in multifaceted approach to risk management by using a combo of internal and external resources

The process of implementing a comprehensive cyber risk management program can be complicated. It requires significant time, resources, and focus from a variety of people and departments across the organization.

When an incident occurs, a number of items must happen quickly and in coordinated fashion or it can rapidly become a crisis that spirals out of control. Well-prepared companies often take an enterprise approach to cyber risk management and frequently utilize a combination of internal and external resources.

With this in mind, respondents were asked what kind of pre-incident services they utilize and how they are provided. For the second consecutive year, assessing procedures for protecting sensitive data is the service most commonly provided by internal resources; and a cyber risk management program assessment is the service most commonly provided externally, including by insurance industry carriers and brokers.
What kind of pre-incident services does your company use and who provides these services?

*Respondents selected all that apply

- Not utilizing/conducting
- Provided internally (IT, Legal, HR, Comms)
- Provided externally (IT, Cyber security Firms, Legal, PR, Consultants)
- Provided by insurance broker or carrier

<table>
<thead>
<tr>
<th>Service</th>
<th>Not Utilizing</th>
<th>Provided Internally</th>
<th>Provided Externally</th>
<th>Provided by Insurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess your procedures for protecting sensitive data</td>
<td>3%</td>
<td>23%</td>
<td>41%</td>
<td>3%</td>
</tr>
<tr>
<td>Assessment of your data breach response plan and related capabilities</td>
<td>6%</td>
<td>15%</td>
<td>38%</td>
<td>6%</td>
</tr>
<tr>
<td>Evaluate your company’s ability to detect and respond to indicators of data compromise</td>
<td>4%</td>
<td>44%</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>Annually assess your exposure to cyber risk based on the current threat environment</td>
<td>6%</td>
<td>42%</td>
<td>6%</td>
<td>6%</td>
</tr>
<tr>
<td>Assessment of your cyber risk management program</td>
<td>3%</td>
<td>48%</td>
<td>3%</td>
<td>3%</td>
</tr>
<tr>
<td>Real-time updates on cyber threats specific to your company and industry</td>
<td>9%</td>
<td>12%</td>
<td>41%</td>
<td>9%</td>
</tr>
<tr>
<td>Cyber workshops and training for employees</td>
<td>8%</td>
<td>15%</td>
<td>30%</td>
<td>8%</td>
</tr>
<tr>
<td>Executive education on cyber risk</td>
<td>15%</td>
<td>11%</td>
<td>18%</td>
<td>15%</td>
</tr>
</tbody>
</table>

Developing a robust response capability well in advance of an incident can decrease pressure on the business, can lower costs, and help reduce errors. A high level of expertise is required to properly implement a pre-incident cyber strategy.

The study revealed that many businesses continue to manage pre-incident planning, such as executive cyber risk education and assessing procedures for protecting sensitive data, from inside the company.

Resource utilization for post-incident services can vary from internal or external only, to a combination of the two. Respondents who had experienced a cyber incident that did not result in a business interruption event (e.g., a data breach), but resulted in economic loss, were asked what services they engaged to respond to the incident. While many used a combination of both, external resources were most commonly utilized for credit monitoring and legal services while internal resources were most commonly utilized for forensic investigation and crisis management.

Organizations are more likely to engage external services for post-cyber response than pre-incident planning.
A company’s cyber security effectiveness is only as strong as its weakest link. In many instances, this can be the company’s own employees.

“We have implemented cyber training to employees and customers to increase awareness of email spam,” a respondent explained.

“We have increased behavior-based threat detection and regular communications to the company explaining email phishing and social engineering plots,” said another respondent.

Another vulnerability often overlooked is the cyber security controls of vendors and other business partners within a supply chain. Many companies with robust cyber security controls have found themselves compromised by cybercriminals entering through the back door – a company in the supply chain that has access to their systems.

With this in mind, respondents were asked which vendor management controls they have implemented to manage cyber supply chain risks. The most common control is including security requirements in every RFP and contract, followed by requiring compliance with critical standards and regulations, and including cyber insurance requirements in appropriate RFPs and contracts.

Which vendor management controls have you implemented to manage cyber supply chain risks?
Cyber insurance purchasing trends

Cyber insurance continues to play a significant role in corporate cyber risk management programs. Participants were asked if their company purchased a cyber insurance policy. Sixty-five percent said “yes,” 27 percent “no,” and eight percent did not know.

Overall, the percentage of respondents who purchase cyber insurance has increased by 30 percentage points since 2011.

Seven-year cyber insurance purchasing trend

<table>
<thead>
<tr>
<th>Year</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>35%</td>
<td>60%</td>
</tr>
<tr>
<td>2012</td>
<td>44%</td>
<td>50%</td>
</tr>
<tr>
<td>2013</td>
<td>52%</td>
<td>38%</td>
</tr>
<tr>
<td>2014</td>
<td>52%</td>
<td>35%</td>
</tr>
<tr>
<td>2015</td>
<td>61%</td>
<td>26%</td>
</tr>
<tr>
<td>2016</td>
<td>65%</td>
<td>23%</td>
</tr>
<tr>
<td>2017</td>
<td>65%</td>
<td>27%</td>
</tr>
</tbody>
</table>

Of the respondents who purchase cyber insurance, the primary driver (37 percent) behind the purchasing decision is expenses/fines related to a breach of customer/personal information. This was followed by liability costs at 25 percent. Interestingly, only 10 percent of respondents said business interruption was a primary driver for purchasing the cover. This could be an indication that risk professionals are less knowledgeable about business continuity risks than data integrity risks, or that the insurance industry needs to do a better job of product education.

What was the primary reason for purchasing cyber insurance?

Expenses/fines related to breach of customer/personal information
Liability costs
Company reputation (legal costs, public relations costs)
Business interruption
Theft/loss of intellectual property/proprietary processes
Although the rapid growth in the cyber insurance market appears to have plateaued, there remains substantial opportunity to write new business. Of the respondents who have not yet purchased a cyber insurance policy, 86 percent said it is something that they have considered. For many of these companies, price is the obstacle that must be overcome.

**SUMMARY**

Taken as a whole, the insurance industry remains a significant player in combating cyber security challenges. According to the survey, high-profile business interruption attacks — and the evolution of cyber risks beyond data breaches — have not yet translated into concern or action from risk managers.

There remains a great need for guidance in developing cyber risk management programs and improving cyber resiliency. For the cyber insurance market to continue to grow, the industry must seize the opportunity to bring value by helping develop strategic cyber prevention and response initiatives, and demonstrating the benefits of cyber insurance policies.

**METHODOLOGY**

For a seventh consecutive year, Advisen and Zurich North America collaborated on a survey designed to gain insight into the current state and ongoing trends in cyber risk management. Invitations to participate were distributed by email to risk managers, insurance buyers and other risk professionals.

The survey was completed at least in part by 315 respondents. The majority classified themselves as either Chief Risk Manager/Head of Risk Management Department (45 percent) or Member of Risk Management Department (31 percent).

Many industries are represented. Finance, Banking and Insurance has the highest representation at 19 percent of the total. Other highly represented industries include services (hospitality, legal, educational, social etc.) at 17 percent; and manufacturing and healthcare, both at 11 percent.

The survey is represented by business of all sizes. Overall, it is slightly weighted towards smaller companies with 56 percent of respondent companies having revenues (or budgets for nonprofit or government entities) of $1B or less. In terms of employee count, 17 percent have fewer than 250, 7 percent have 250 to 500, 12 percent have 500 to 1,000, 24 percent have 1,000 to 5,000, 17 percent have 5,000 to 15,000, and 24 percent have more than 15,000 employees.

**Disclaimer:** The information in this publication was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute legal advice and accordingly, you should consult with your own attorneys when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.

©2017 Zurich American Insurance Company – All Rights Reserved