Ponemon INSTITUTE

Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age

Sponsored by Experian® Data Breach Resolution

Independently conducted by Ponemon Institute LLC

Publication Date: August 2013

Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age

August 2013

Part 1: Introduction

With the increasing cost and volume of data breaches, cyber security is quickly moving from being considered by business leaders as a purely technical issue to a larger business risk. This shift has spurred increased interest in cyber insurance to mitigate the cost of these issues.

Traditionally the CIO and IT department has been considered the domain for cyber security. However, more companies are looking to other corporate leaders to help manage the financial risks of a cyber attack. Risk managers often find themselves in the eye of the security storm with the greater acknowledgement that data breaches have serious financial consequences for organizations. In Ponemon Institute's *2013 Cost of Data Breach Study,* the average cost of a data breach was $188 for each lost or stolen record. In response, major corporate risk underwriters offer policies specifically devoted to helping companies manage the financial costs related to data breaches.

In the wake of a serious data breach or security exploit, companies will often increase investments in enabling technologies and training and awareness programs to prevent or reduce the severity of future incidents. In addition to these important steps, more companies are considering the purchase of cyber security insurance. These policies are designed to mitigate losses from a variety of cyber incidents, including data breaches, network damage and cyber extortion. A cyber insurance policy can be one way to protect the company against future losses.

In a new study sponsored by Experian® Data Breach Resolution, Ponemon Institute surveyed risk management professionals across multiple sectors that have considered or adopted cyber insurance. Based on responses, many understand that security is a clear and present risk. Indeed a majority of companies now rank cyber security risks as greater than natural disasters and other major business risks.

Some of the most noteworthy findings include the following:

- **Security exploits and data breaches result in multi-million dollar losses**. The findings of the research reveal that the average financial impact to companies for one or more incidents was $9.4 million. Respondents estimate that the average potential financial risk of future incidents is estimated to be $163 million. Most involved the loss of business confidential information.

- **Concerns about cyber risks are moving outside of corporate IT teams**. Protecting against the financial impact of cyber security risks rank high as or higher than other insurable risks (natural disaster, fire, etc.) Of those that have experienced a security exploit, 76 percent think they are greater to or equal to a natural disaster, business interruption, fire, etc.

- **Worries about costly future data breaches and security exploits drive interest in cyber security insurance**. Among those companies that had an incident in the past 24 months, 70 percent of respondents say the experience increased their interest in these policies.

- **Most companies either have cyber security insurance or are considering adoption.** Currently, 31 percent of companies in the study have a policy and 39 percent of respondents say their organization plans to purchase a policy.

- **Satisfaction with policies runs high.** Forty-four percent of respondents say they would be extremely likely to recommend their insurance provider to a friend or colleague. The findings also show that the longer the policy has been held, the greater the satisfaction.

- **A stronger security posture follows the purchase of cyber security insurance**. Sixty-two percent of respondents believe the insurance has made the company better prepared to deal with security threats. Fifty-five percent say it is an important part of their risk management program.

- **Some companies are still skeptical about policies.** Thirty percent of respondents note their company has no interest in purchasing a policy at this time. Key roadblocks include price and concerns about too many exclusions, restrictions and uninsurable risks that inhibit their organizations from purchasing a policy.

- **However, those with a policy believe premiums are fair**. Sixty-two percent of respondents in companies with this insurance believe the premiums are fair given the nature of the risk. Most also do not anticipate an increase.

Part 2. Key Findings

In this section we present the key findings of this research. The complete audited results are presented in the Appendix of this report.

We have organized the key findings according to the following themes:

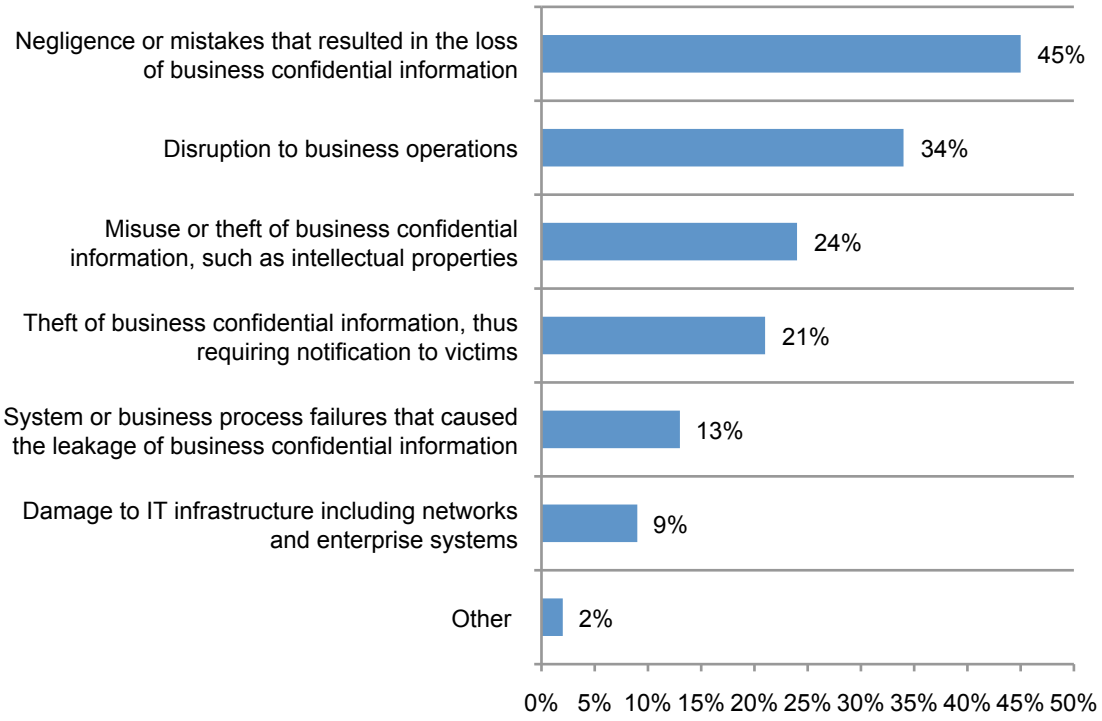
- The influence of security exploit and data breach costs on cyber insurance purchases
- The value of cyber insurance to the organization
- The purchase decision and policy coverage
- Special analysis on customer satisfaction and industry differences

The influence of security exploit and data breach costs on cyber insurance purchases

Fifty-six percent of the organizations represented in this study have had a material security exploit or data breach one or more times during the past 24 months. For purposes of this research, a material security exploit is a cyber attack that infiltrates a company's networks or enterprise systems. A material data breach is one that results in the loss or theft of 1,000 or more records.

Loss of confidential information and business disruption were the cause of most incidents. As shown in Figure 1, the most common data breaches are due to negligence or mistakes that resulted in the loss of business confidential information. Most common cyber attacks are those that caused disruption to business operations (such as denial of service attacks). Not as frequent are those cyber attacks that caused damage to their company's IT infrastructure, including networks and enterprise systems.

Figure 1. Data breaches or security exploits experienced over the past 24 months
More than one response permitted



Security exploits and data breaches result in multi-million dollar losses. The average financial impact of these security exploits and data breaches experienced by companies represented in this research is $9.4 million. In some cases, companies had multiple incidents. The costs included are those to resolve the incident such as consultant and legal fees, indirect business costs such as productivity losses, diminished revenues, legal actions, customer turnover and reputation damages.

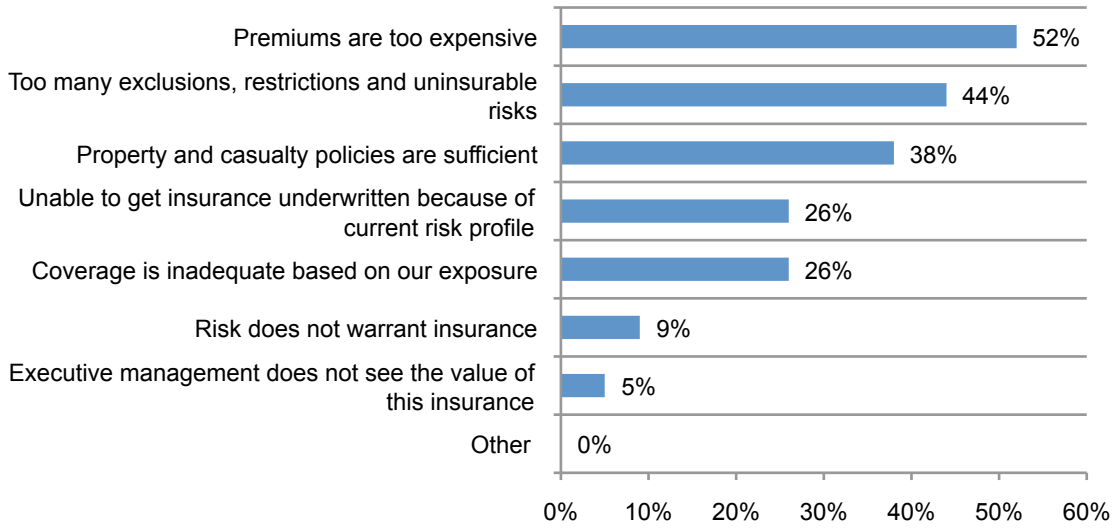
Respondents are not optimistic that the financial impact will decline and this might be influencing the increased interest in cyber security insurance. When asked to predict their company's maximum financial exposure of security exploits and data breaches for the next 24 months, the average estimate is approximately $163 million.

Majority of companies plan to purchase cyber security policies. The financial impact of a security exploit or data breach influences the purchase of a cyber insurance policy. Seventy percent of respondents say their companies became much more interested in these policies after an incident.

Desire to purchase policies is also due to the perception by most respondents that their companies' financial exposure due to security exploits and data breaches will either stay the same or actually increase.

Currently, less than one-third of respondents (31 percent) in this study say their organization has a cyber security insurance policy. However, among those companies that do not have a policy 57 percent of respondents say they plan to purchase one in the future. If they don't have plans to purchase (43 percent of respondents), it is because of the cost and too many exclusions, restrictions and uninsurable risks, as shown in Figure 2.

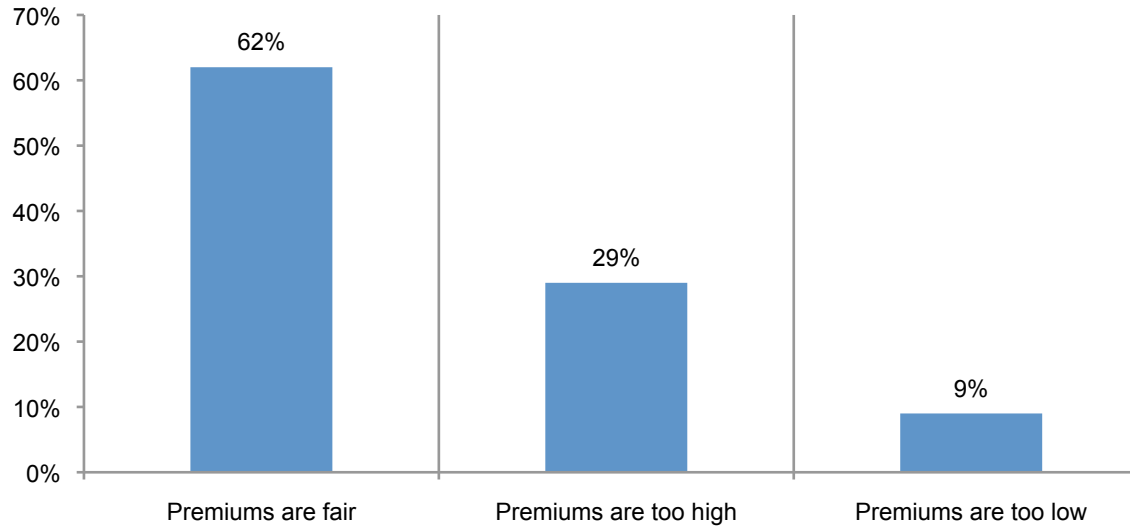
Figure 2. Main reasons for not purchasing cyber security insurance
Two choices permitted



Premiums are considered fair. According to Figure 3, 62 percent of those who did purchase a policy believe the premiums are fair given the nature of the risk. Only 29 percent believe the premium is too high.

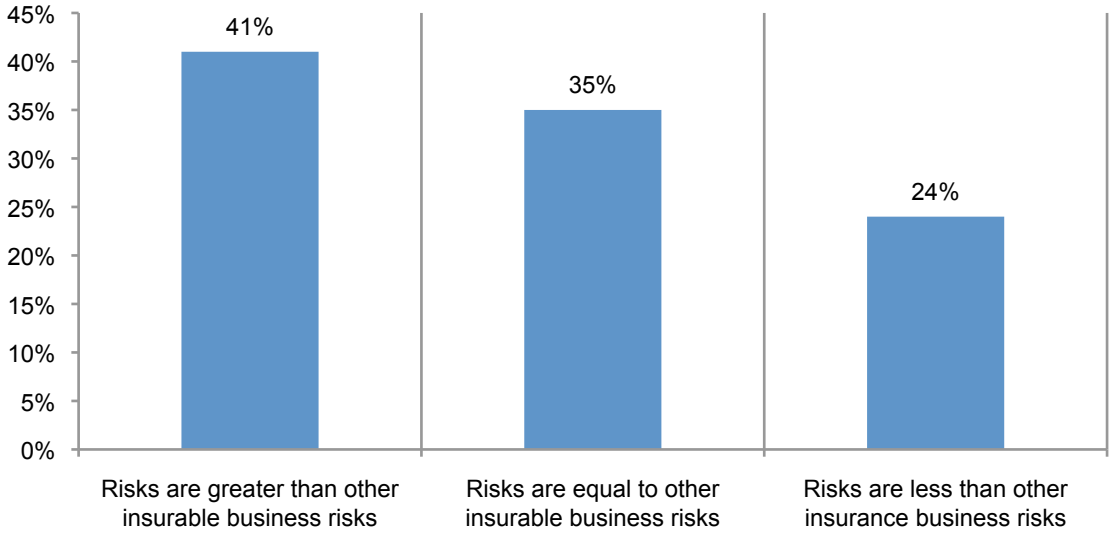
When asked to predict what premiums will be in the near future, 33 percent do believe that the annual premiums will increase. However, a much higher percentage of respondents (61 percent) believe premiums will stay the same.

Figure 3. Are premiums properly priced?



Cyber security risks are significant. From a business perspective, 41 percent of respondents believe cyber security risks are greater than other insurable business risks such as natural disasters, business interruption and fires, as shown in Figure 4. Thirty-five percent say they are equal to other insurable business risks.

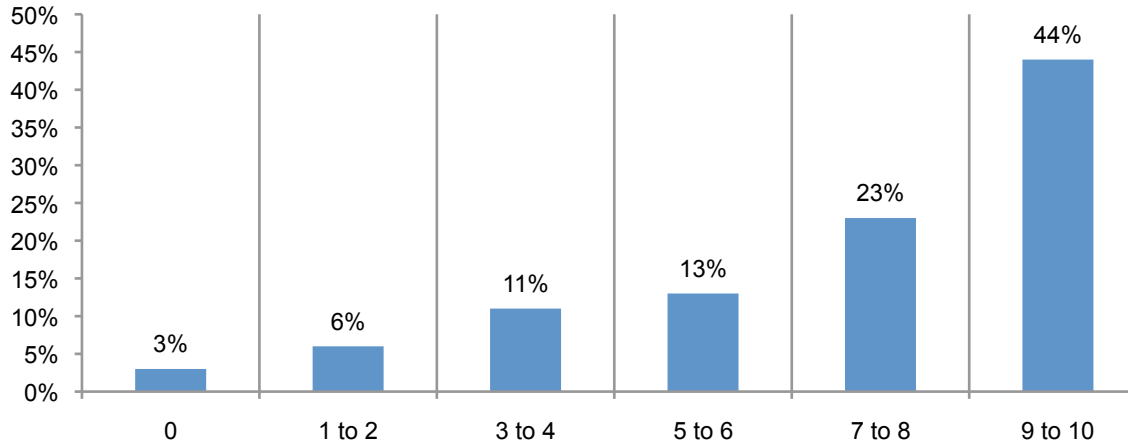
Figure 4. How cyber security risks compare to other insurable risks



The value of cyber security insurance to the organization

Organizations find value in cyber insurance. Most companies with cyber security insurance have had their policies between one and four years. As shown in Figure 5, customer satisfaction runs high with 44 percent of respondents extremely likely to recommend their insurance provider to a friend or colleague.

Figure 5. Would you recommend cyber insurance to your friends or colleagues?
Product recommendations are measured using a 11-point rating from 0 (low) to 10 (high)



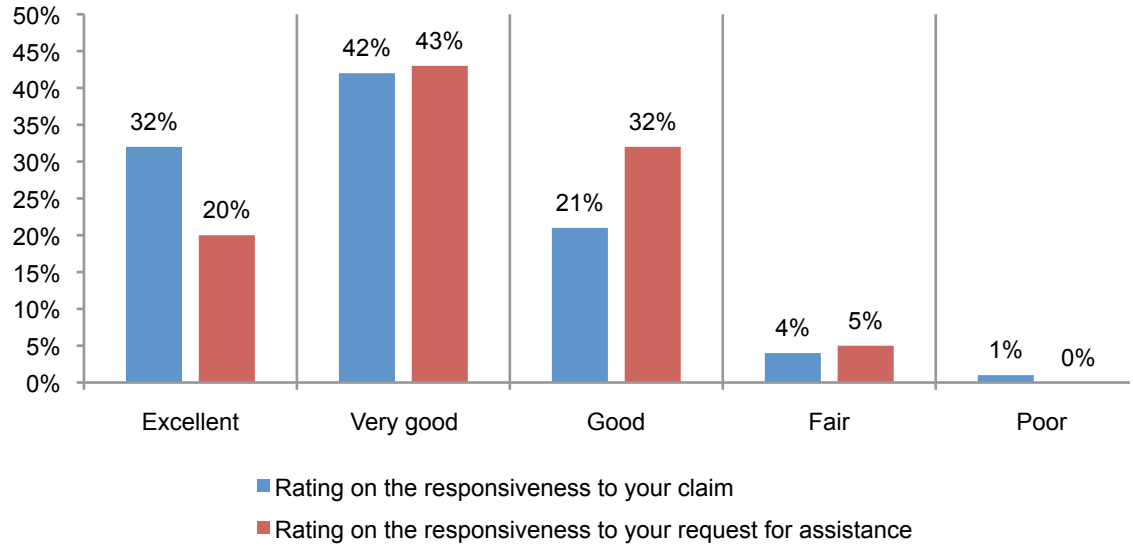
Security posture improves. In addition to reducing the potential financial liability of a breach or security exploit, companies' security posture becomes stronger with the purchase of cyber security insurance. According to 62 percent of respondents, their companies' ability to deal with security threats improved following the purchase of the policy. Assessments and other steps required to complete the purchase of the policy could have an impact on these improvements.

Insurers prove to be responsive to companies' needs. Since purchasing the cyber security policy, 30 percent of respondents say their company experienced a security exploit or data breach and submitted a claim for losses.

Figure 6 shows satisfaction with responsiveness to the claim submission and request for assistance. Most rated the responsiveness of the insurer to their claim as excellent (32 percent) or very good (42 percent).

Fewer organizations (29 percent of respondents) asked their insurer to assist in responding to a security exploit or data breach incident. However, those respondents that asked for assistance rated the responsiveness of the insurer as excellent (20 percent) and very good (43 percent). It is interesting that more respondents rate responsiveness to claims as excellent than requests for assistance.

Figure 6. How responsive was the insurer to claims and requests for assistance?



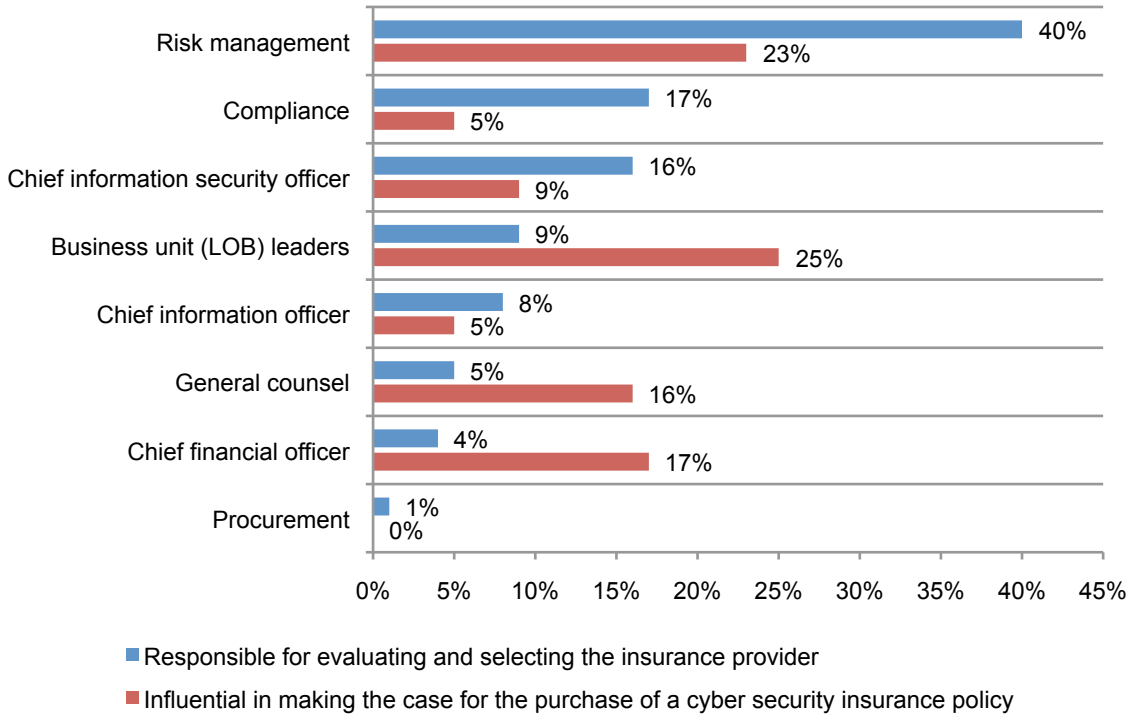
The purchase decision and policy coverage

Risk managers are most often responsible for the decision-making process. Figure 7 reveals the functions most influential in the purchasing decision and evaluating and selecting the insurance provider.

According to 40 percent of respondents, risk management is most responsible for evaluating and selecting the insurance provider followed by compliance (17 percent of respondents) and the chief information security officer (16 percent of respondents). However, the most influential in making the case for the purchase are business unit leaders followed by risk managers.

The chief information officer and chief information security officer seem to have very little influence. As discussed later, IT security also has very little involvement in determining the adequacy of coverage

Figure 7. Most responsible for cyber security insurance decisions



.

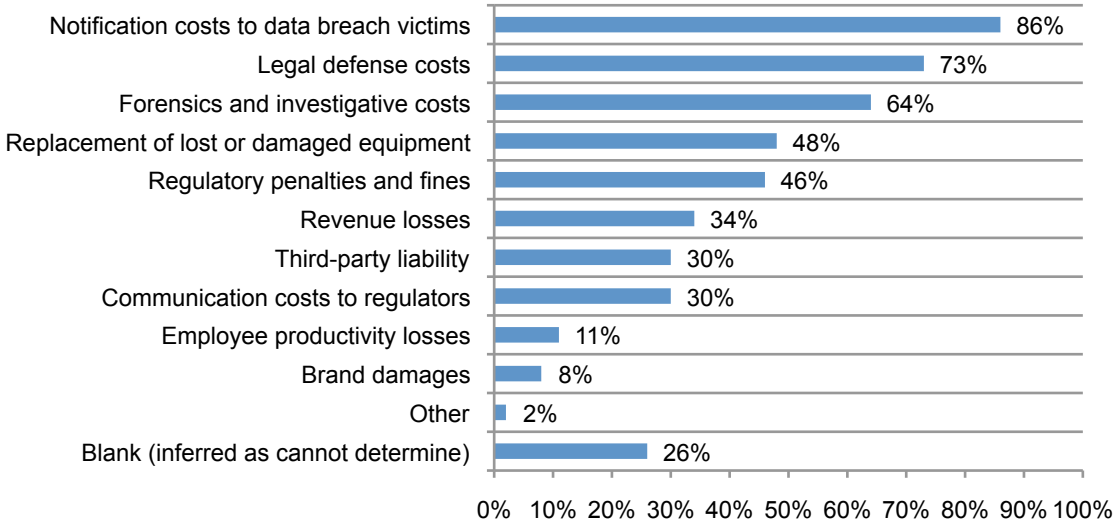
Policies typically cover the most common and costly incidents. The primary types of incidents covered include human error, mistakes and negligence followed by external attacks by cyber criminals, system or business process failures and malicious or criminal insiders, as shown in Figure 8. Only 11 percent of respondents say their policies cover attacks against business partners, vendors or other third parties that have access to their company's information assets.

According to the *2013 Cost of Data Breach Study: United States*, malicious or criminal attacks result in the highest per capita data breach cost. Consistent with prior reports, data loss or exfiltration resulting from a malicious or criminal attack yielded the highest cost at $277 per compromised record, on average. In contrast, both system glitches and employee mistakes resulted in a much lower per capita cost at $177 and $159, respectively

Figure 8. Incidents covered by the cyber security insurance policy
More than one response permitted

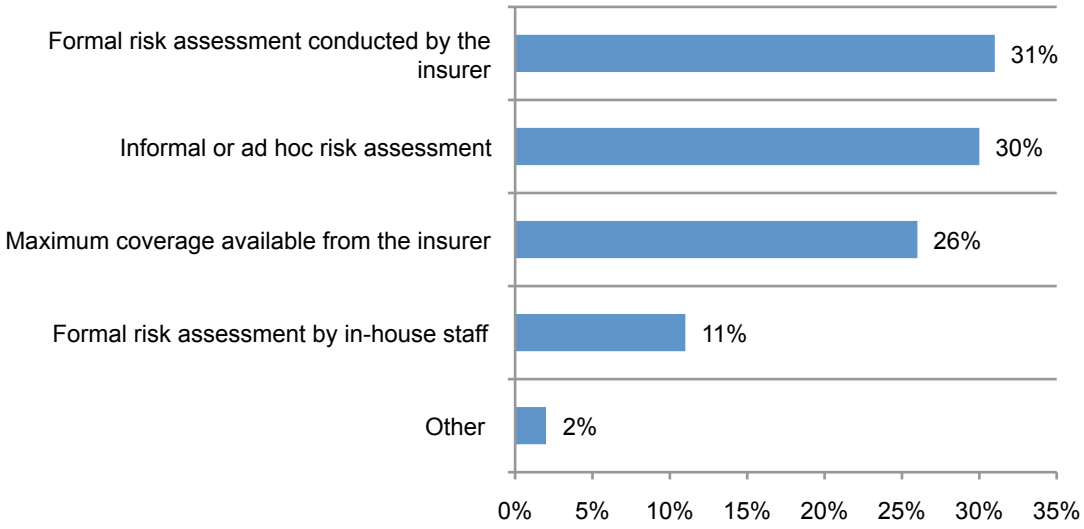
According to Figure 9, the notification costs to data breach victims, legal costs and forensics and investigative costs are mostly covered. Costs related to employee productivity and brand damage are rarely covered perhaps due to the difficulty in quantifying the costs.

Figure 9. Protections or benefits covered by the policy
More than one response permitted



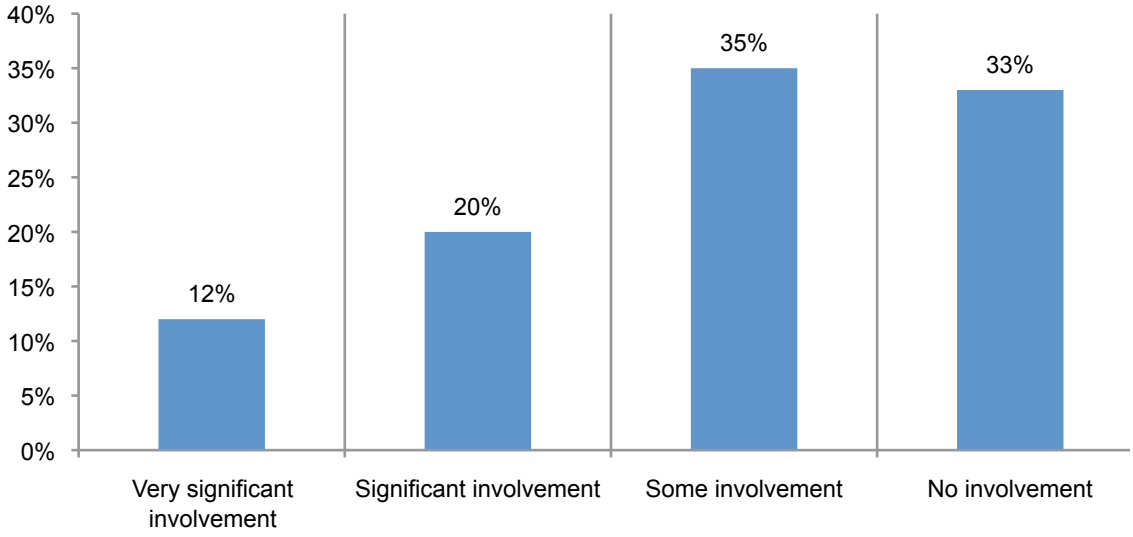
How the amount of coverage is decided. Companies rarely use formal risk assessments by in-house staff to determine how much coverage should be purchased. Instead they rely upon the insurer to do a formal risk assessment or they conduct their own informal ad-hoc assessment, as shown in Figure 10.

Figure 10. Steps taken to determine the amount of coverage



As shown in Figure 11, only 32 percent of respondents say the IT security function has a very significant level of involvement (12 percent) or significant involvement (20 percent). One-third of respondents say there is no involvement from IT security.

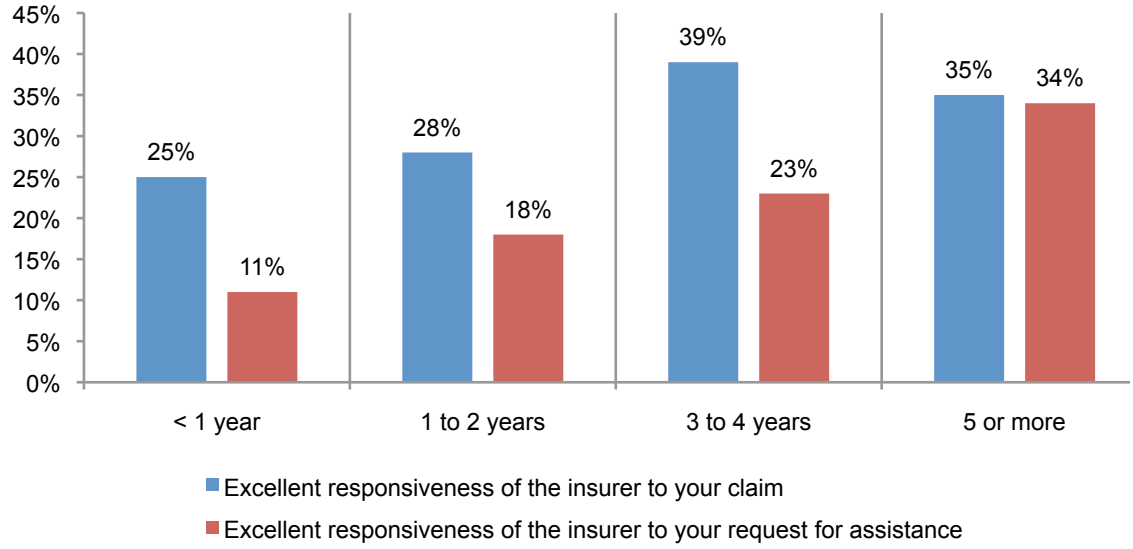
Figure 11. IT security's level of involvement in determining the adequacy of coverage



Special analysis on customer satisfaction and industry differences

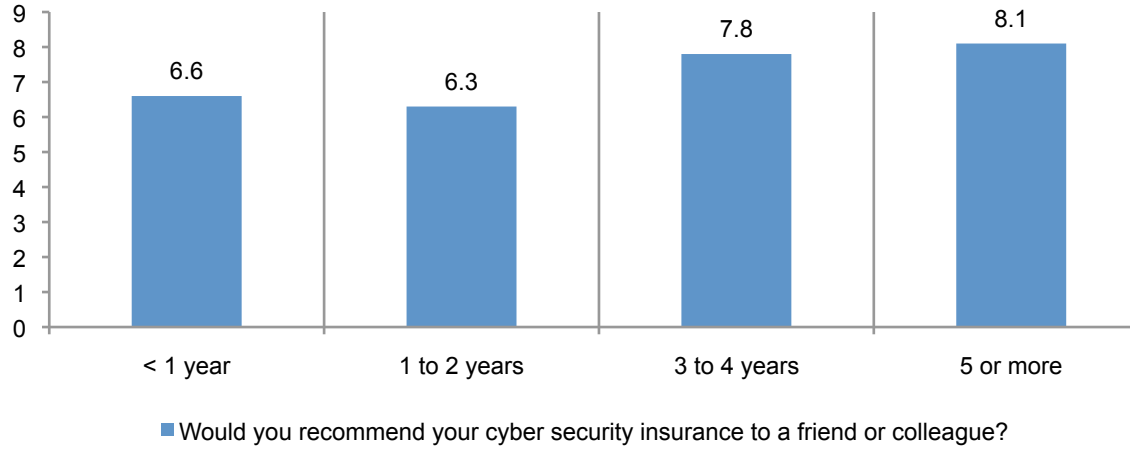
The following two cross-tabulations analyze the length of time a cyber insurance policy is held (a.k.a. policy age) and the perceptions about their insurer's responsiveness to claims and other requests for help by the insured. Figure 12 provides a clear indication about the insurer's responsiveness to claims and related assistance or services. That is, the longer the policy is held, the more favorable the respondents' ratings.

Figure 12. Relationship between policy age and perceived responsiveness of the insurer to claims and other requests for assistance
Percentage of respondents who rated the insurer as excellent



Consistent with the above finding, Figure 13 shows that respondents are more likely to endorse or promote the cyber insurance product the longer it is held.

Figure 13. Relationship between policy age and product recommendation ratings
Product recommendations are measured using a 11-point rating from 0 (low) to 10 (high)



The next two cross-tabulations show the influence of industry on insurance adoption or "take up" rates and consumer satisfaction.[1] Figure 14 shows marked differences in adoption by industry. At 41 percent, companies in the technology and software industry have the highest take up rate. In contrast, public sector organizations have the lowest rate of adoption at 19 percent.

Figure 14. Relationship between cyber insurance adoption and major industry segments
Percentage of respondents who said their organizations procured a cyber insurance policy

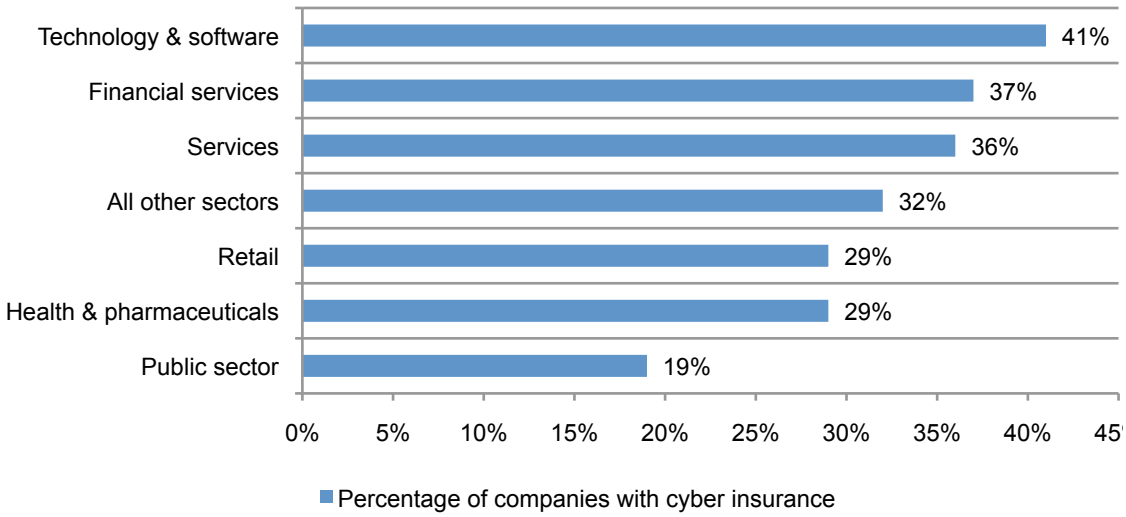
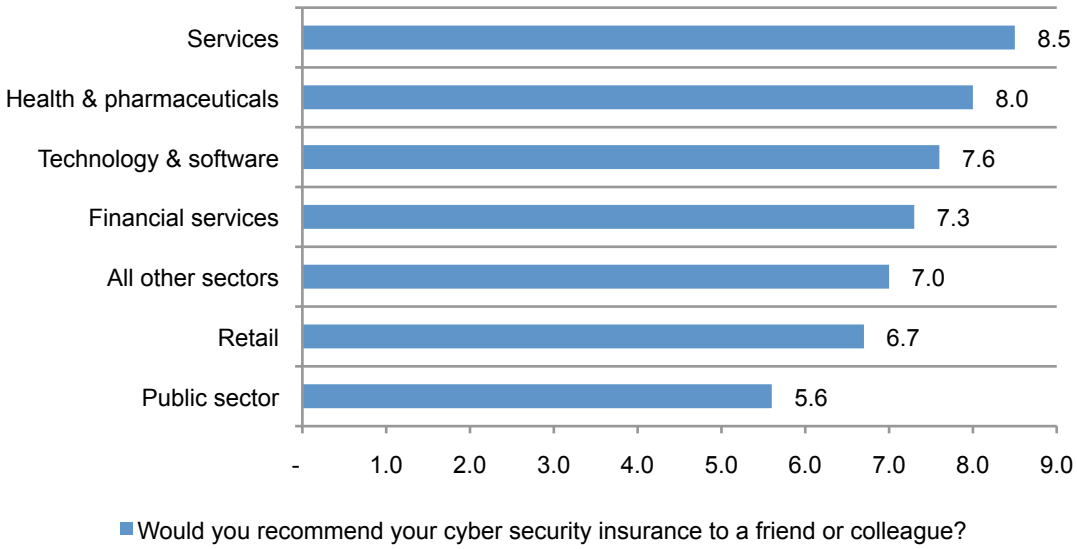


Figure 15 shows differences in respondents' willingness to endorse cyber insurance and industry. As can be seen, companies in the services industry have the highest average endorsement rate (at 8.5). In contrast, public sector organizations have the lowest endorsement rate (at 5.6).

Figure 15. Relationship between policy age and product recommendation ratings
Product recommendations are measured using a 11-point rating from 0 (low) to 10 (high)



[1]Certain industry sectors were not analyzed because of insufficient sample size. Only those sectors with more than 40 observations are shown separately. Responses below 40 are consolidated within the "all other sectors" category.

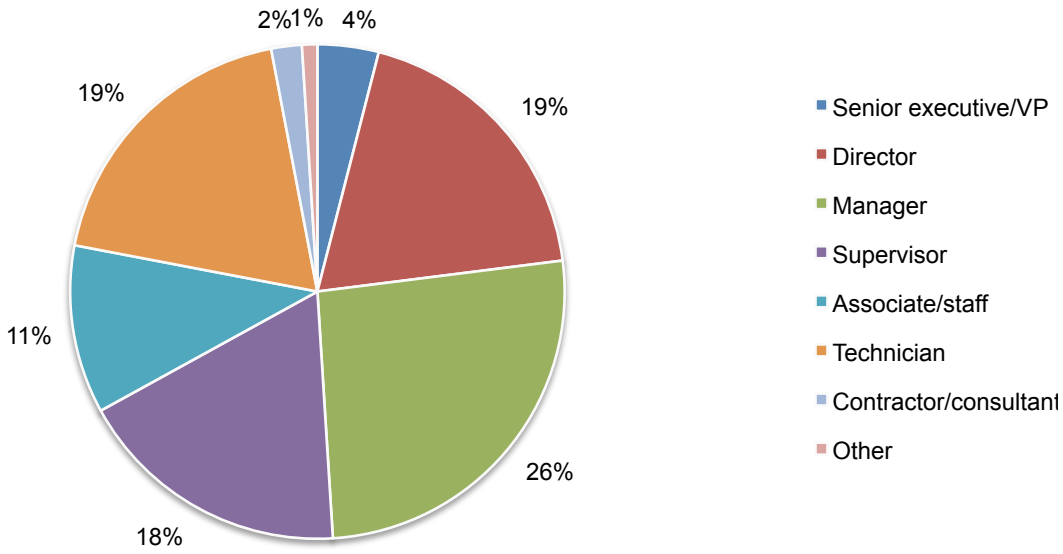
Part 3. Methods

A random sampling frame of 18,829 experienced individuals involved in their companies' cyber security risk mitigation and risk management activities in various-sized organizations in the United States were selected as participants to this survey. As shown in Table 1, 957 respondents completed the survey. Screening and reliability checks removed 319 surveys. The final sample was 638 surveys (or a 3.4 percent response rate).

Table 1. Sample response	Freq	Pct%
Sampling frame	18,829	100.0%
Total returns	957	5.1%
Rejected and screened surveys	319	1.7%
Final sample	638	3.4%

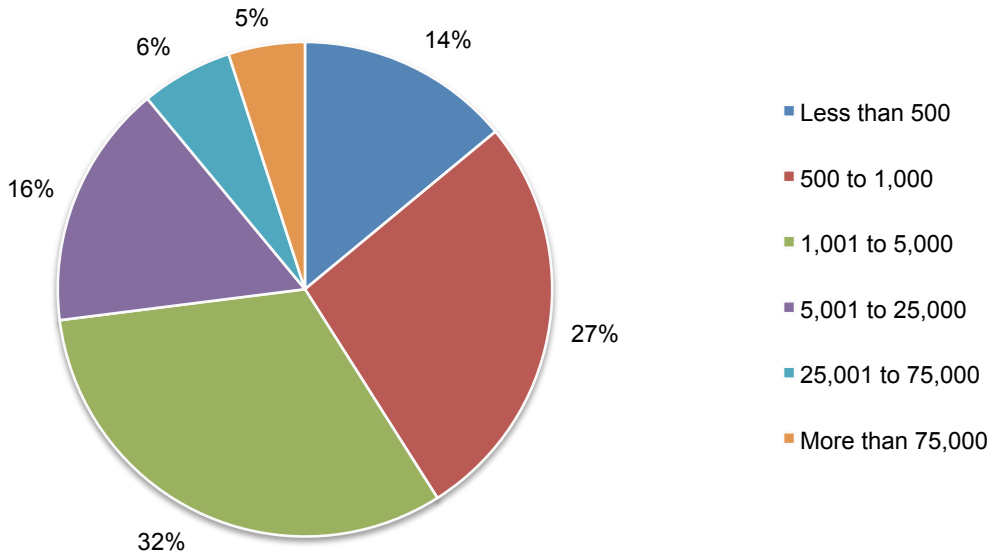
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 67 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



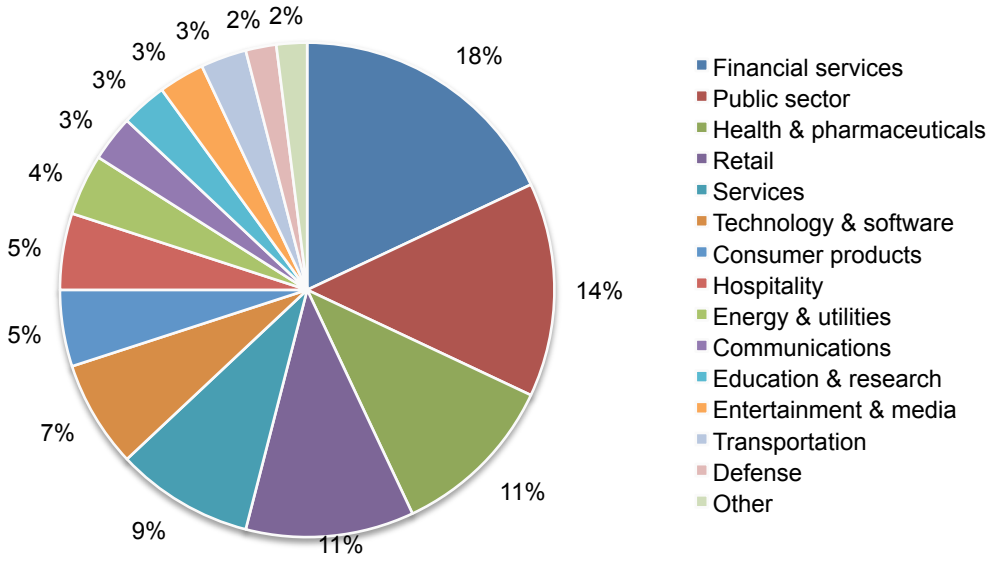
As shown in pie chart 2, 59 percent of respondents are from organizations with a global headcount of 1,000 or more employees.

Pie chart 2. Worldwide headcount of the organization



Pie Chart 3 reports the industry segments of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by public sector (14 percent) and health and pharmaceuticals and retail, both at 11 percent.

Pie Chart 2. Industry distribution of respondents' organizations



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are involved in their companies' cyber security risk mitigation and risk management activities. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in June 2013.

Sample response	Freq	Pct%
Sampling frame	18,829	100.0%
Total returns	957	5.1%
Rejected and screened surveys	319	1.7%
Final sample	638	3.4%

Part 1. Screening questions	
S1. How familiar are you with cyber security insurance products and what they offer companies?	Pct%
Very familiar	31%
Familiar	45%
Somewhat familiar	24%
Not familiar (stop)	0%
Total	100%

S2. Are you involved in your company's cyber security risk mitigation activities?	Pct%
Significant involvement	41%
Some involvement	59%
No involvement (stop)	0%
Total	100%

S3. Are you involved in your company's enterprise risk management activities?	Pct%
Significant involvement	33%
Some involvement	67%
No involvement (stop)	0%
Total	100%

Part 2. General survey questions	
Q1a. Has your company experienced a material security exploit or data breach one or more times over the past 24 months? A material security exploit is a cyber attack that infiltrates your company's networks or enterprise systems. A material data breach is one that results in the loss or theft of 1,000 or more records.	Pct%
Yes	56%
No [skip to Q2]	36%
Unsure [skip to Q2]	8%
Total	100%

Q1b. If yes, what best describes the data breaches or security exploits experienced by your company over the past 24 months? Please select all that apply.	Pct%
Cyber attack that caused disruption to business operations (such as denial of service attacks)	34%
Cyber attack that resulted in the theft of business confidential information, thus requiring notification to victims	21%
Cyber attack that caused damage to your company's IT infrastructure including networks and enterprise systems	9%
Cyber attack that resulted in the misuse or theft of business confidential information, such as intellectual properties	24%
Negligence or mistakes that resulted in the loss of business confidential information	45%
System or business process failures that caused the leakage of business confidential information	13%
Other (please specify)	2%
Total	148%

Q1c. If yes, what was the **total financial impact** of security exploits and data breaches experienced by your company over the past 24 months. Please include all costs including out-of-pocket expenditures such as consultant and legal fees, indirect business costs such as productivity losses, diminished revenues, legal actions, customer turnover and reputation damages.	Pct%
Zero	0%
Less than $10,000	1%
$10,001 to $100,000	2%
$100,001 to $250,000	4%
$250,001 to $500,000	9%
$500,001 to $1,000,000	8%
$1,000,001 to $5,000,000	19%
$5,000,001 to $10,000,000	24%
$10,000,001 to $25.000,000	17%
$25,000,001 to $50,000,000	4%
$50,00,001 to $100,000,000	2%
More than $100,000,000	0%
Cannot determine	10%
Total	100%

Q1d. If yes, did the above security exploit or data breach experience increase your company's interest in purchasing cyber insurance?	Pct%
Yes	70%
No	24%
Unsure	6%
Total	100%

Q2. [everyone answers this] Please predict your company's **maximum financial exposure** of security exploits and data breaches for the next 24 months. Please include all potential out-of-pocket expenditures such as consultant and legal fees, indirect business costs such as productivity losses, diminished revenues, legal actions, customer turnover and reputation damages.	Pct%
Less than $1,000,000	2%
$1,000,001 to $5,000,000	6%
$5,000,001 to $10,000,000	7%
$10,000,001 to $25.000,000	7%
$25,000,001 to $50,000,000	11%
$50,00,001 to $100,000,000	17%
$100,000,001 to $250,000,000	18%
$250,000,001 to $500,000,000	14%
More than $500,000,000	8%
Cannot determine	10%
Total	100%

Q3. What is the likelihood that your company will experience the maximum financial exposure due security exploits and/or data breaches over the next 24 months?	Pct%
Zero	0%
< 5%	29%
5 to 10%	36%
11 to 15%	23%
16 to 20%	10%
21 to 30%	2%
31 to 40%	0%
41 to 50%	0%
50%+	0%
Total	100%

Q4. Do you believe your company's exposure due to security exploits and data breaches will increase, decrease or stay the same over the next 24 months?	Pct%
Increase	37%
Decrease	15%
Stay the same	48%
Total	100%

Q5. From a business risk perspective, how does cyber security risks compare to other insurable risks such as natural disasters, business interruption, fires and so forth. Please select one best choice.	Pct%
Cyber security risks are equal to other insurable business risks	35%
Cyber security risks are greater than other insurable business risks	41%
Cyber security risks are less than other insurance business risks	24%
Total	100%

Q6a. Does your company have a cyber security insurance policy (or set of policies)?	Pct%
Yes	31%
No	69%
Total	100%

Q6b. If no, does your company plan to purchase a cyber security insurance policy?	Pct%
Yes, in the next 12 months	18%
Yes, in the next 24 months	23%
Yes, more than 24 months	16%
No	43%
Total	100%

Q6c. If no, what are the two main reasons why your company is not planning to purchase cyber security insurance?	Pct%
Premiums are too expensive	52%
Coverage is inadequate based on our exposure	26%
Too many exclusions, restrictions and uninsurable risks	44%
Risk does not warrant insurance	9%
Property and casualty policies are sufficient	38%
Executive management does not see the value of this insurance	5%
Unable to get insurance underwritten because of current risk profile	26%
Other (please specify)	0%
Total	200%

NO responders go to Part 3

Q7. Who in your company is (or was) **most responsible** for evaluating and selecting the insurance provider (A.K.A. insurer)?	Pct%
CEO/executive committee	0%
Chief financial officer	4%
Business unit (LOB) leaders	9%
Chief information officer	8%
Chief information security officer	16%
Risk management	40%
Procurement	1%
General counsel	5%
Compliance	17%
Other (please select)	0%
Total	100%

Q8. Who in your company is (or was) **most influential** in making the case for the purchase of a cyber security insurance policy?	Pct%
CEO/executive committee	0%
Chief financial officer	17%
Business unit (LOB) leaders	25%
Chief information officer	5%
Chief information security officer	9%
Risk management	23%
Procurement	0%
General counsel	16%
Compliance	5%
Other (please select)	0%
Total	100%

Q9. How long has your company been insured under this cyber security policy?	Pct%
< 1 year	16%
1 to 2 years	39%
3 to 4 years	33%
5 to 6 years	8%
7 to 8 years	3%
9 to 10 years	1%
10 years +	0%
Total	100%

Q10a. Since purchasing the policy, did your company experience a security exploit and/or data breach and submit a claim for any losses?	Pct%
Yes	30%
No	70%
Total	100%

Q10b. If yes, how would you rate the responsiveness of the insurer to your claim?	Pct%
Excellent	32%
Very good	42%
Good	21%
Fair	4%
Poor	1%
Total	100%

Q11a. Did your company ever ask the insurer/agent for assistance in responding to a security exploit or data breach incident.	Pct%
Yes	29%
No	71%
Total	100%

Q11b. If yes, how would you rate the responsiveness of the insurer to your request for assistance.	Pct%
Excellent	20%
Very good	43%
Good	32%
Fair	5%
Poor	0%
Total	100%

Q12. How would you describe the premiums paid to the insurer/agent	Pct%
Premiums are fair given the nature of the risk	62%
Premiums are too high given the nature of the risk	29%
Premiums are too low given the nature of the risk	9%
Total	100%

Q13. Do you believe the annual premiums will increase, decrease or stay the same over the next 24 months?	Pct%
Increase	33%
Decrease	6%
Stay the same	61%
Total	100%

Q14. What types of incidents does the cyber security insurance policy cover? Please select all that apply.	Pct%
External attacks by cyber criminals	72%
Malicious or criminal insiders	54%
System or business process failures	61%
Human error, mistakes and negligence	76%
Attacks against business partners, vendors or other third parties that have access to your company's information assets	11%
Other (please specify)	3%
Blank (inferred as cannot determine)	24%
Total	301%

Q15. What protections or benefits does this policy offer your company? Please select all that apply	Pct%
Forensics and investigative costs	64%
Notification costs to data breach victims	86%
Communication costs to regulators	30%
Employee productivity losses	11%
Replacement of lost or damaged equipment	48%
Revenue losses	34%
Legal defense costs	73%
Regulatory penalties and fines	46%
Third-party liability	30%
Brand damages	8%
Other (please specify)	2%
Blank (inferred as cannot determine)	26%
Total	458%

Q16. What percentage of losses do you believe the cyber security insurance policy would cover?	Pct%
Less than 10%	5%
10 to 25%	13%
26 to 50%	27%
51 to 75%	30%
76 to 99%	13%
Everything (100%)	12%
Total	100%

Q17. How does your company determine the level of coverage it deems adequate?	Pct%
Formal risk assessment by in-house staff	11%
Formal risk assessment conducted by the insurer	31%
Informal or ad hoc risk assessment	30%
Maximum coverage available from the insurer	26%
Other (please specify)	2%
Total	100%

Q18. Please rate the level of involvement of the IT security function in determining the adequacy of coverage?	Pct%
Very significant involvement	12%
Significant involvement	20%
Some involvement	35%
No involvement	33%
Total	100%

Q19. In addition to cost coverage, what other services does the cyber security insurer provide your company in the event of a security exploit or data breach? Please check all that apply.	Pct%
Access to cyber security forensic experts	54%
Access to legal and regulatory experts	82%
Access to specialized technologies and tools	32%
Advanced warnings about ongoing threats and vulnerabilities	75%
Assistance in the remediation of the incident	65%
Assistance in the notification of breach victims	63%
Identity protection services for breach victims	25%
Credit monitoring services for breach victims	18%
Assistance in reputation management activities	26%
Other (please specify)	3%
Blank (inferred as cannot determine)	16%
Total	443%

Q20. Does your insurer specify and/or restrict the choice of vendors you can engage to help remediate the incident? Vendors include forensic experts, law firms, identity protection service providers and others.	Pct%
Yes	62%
No	30%
Unsure	8%
Total	100%

Q21. In your opinion, how does cyber insurance affect the cyber security posture and readiness of your company?	Pct%
Improves our company's cyber security posture and readiness	62%
Diminishes our company's cyber security posture and readiness	5%
No impact on our company's cyber security posture and readiness	33%
Total	100%

Q22. If you had the opportunity, how likely would you be to recommend your company's cyber security insurance provider to a friend or colleague?	Pct%
0 (not at all likely)	3%
1 to 2	6%
3 to 4	11%
5 to 6	13%
7 to 8	23%
9 to 10 (Extremely likely)	44%
Total	100%

Please rate each one of the following statements using the five-point scale provided below the item.	Strongly agree	Agree
Q23a. Cyber security insurance is an essential part of our company's risk management program.	23%	32%
Q23b. Cyber security insurance lessens the urgency to having strong IT security safeguards in place.	11%	14%
Q23c. The benefits of cyber security insurance does not offset its cost.	16%	12%

Part 4. Organizational characteristics

D1. What organizational level best describes your current position?	Pct%
Senior executive/VP	4%
Director	19%
Manager	26%
Supervisor	18%
Associate/staff	11%
Technician	19%
Contractor/consultant	2%
Other	1%
Total	100%

D2. What is the worldwide employee headcount of your organization?	Pct%
Less than 500	14%
500 to 1,000	27%
1,001 to 5,000	32%
5,001 to 25,000	16%
25,001 to 75,000	6%
More than 75,000	5%
Total	100%

D3. What best describes your organization's industry focus?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer products	5%
Defense	2%
Education & research	3%
Energy & utilities	4%
Entertainment & media	3%
Financial services	18%
Health & pharmaceuticals	11%
Hospitality	5%
Public sector	14%
Retail	11%
Services	9%
Technology & software	7%
Transportation	3%
Other	1%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.