2017 CYBER RISK PREPAREDNESS AND RESPONSE SURVEY

A Crisis in Cyber Confidence: Risk Experts Concerned Over Continued Client Complacency

Sponsored by: Experian® Data Breach Resolution
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>3</td>
</tr>
<tr>
<td>KEY FINDINGS</td>
<td>6</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>14</td>
</tr>
<tr>
<td>METHODOLOGY</td>
<td>15</td>
</tr>
<tr>
<td>APPENDIX</td>
<td>16</td>
</tr>
<tr>
<td>RISK MANAGER SURVEY RESULTS</td>
<td>17</td>
</tr>
<tr>
<td>INSURANCE BROKER SURVEY RESULTS</td>
<td>21</td>
</tr>
<tr>
<td>LEGAL EXPERT SURVEY RESULTS</td>
<td>24</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

How confident are you in your company’s or client’s ability to respond to a cyberattack? What threats are keeping you up at night, and are you prepared to handle them if they strike?

In a new survey sponsored by Experian® Data Breach Resolution, Advisen surveyed 307 risk managers, insurance brokers and legal experts to better understand what cyber threats had them most concerned. The survey took a different approach than most preparedness studies, asking respondents for their opinions on their company and clients’ ability to manage a cyber incident and what they think needs to be done to improve their overall security posture.

The study found that while external risk experts and risk managers were aligned on the risks facing companies, the third-party experts were concerned about their clients’ complacency. While many respondents noted that their company or clients had a response plan in place, this did not translate to confidence among external risk experts in their clients’ ability to effectively manage an incident.
Companies overestimate their cyber preparedness

Given the evolving security landscape, and the increasing frequency and severity of cyberattacks, a sense of unease among cyber risk experts is expected, but the gap in confidence between internal risk professionals and third-party risk experts is concerning. This indicates that companies may be overconfident in their ability to effectively manage an incident.

Eighty-six percent of risk managers reported that their company was at least somewhat prepared to respond to a breach. And, while legal experts and insurance brokers generally agreed, there appears to be a discrepancy in the perceived performance of cyber risk practices. Risk managers consistently rated their company’s performance of cyberattack prevention practices higher than the external risk experts rated their clients’ performance.

• On average risk managers rated their employee education programs as average or 3.36 (out of 5) with insurance brokers and legal experts ranking their clients as below average (2.57 and 2.91 rating, respectively). (Exhibit 1)

• While over 72 percent of risk managers rated their network protection as above average, most insurance brokers and legal experts rated their clients as average or below average (67 percent and 52 percent, respectively).

Additionally, external risk experts also lacked confidence in their clients’ ability to navigate these threats:

• Eighty percent of legal experts and 68 percent of insurance brokers were strongly or extremely concerned with a breach of personal or financial information due to phishing or social engineering, while only 61 percent of risk managers shared the same concern.

• Both legal experts and insurance brokers (54 percent and 61 percent respectively) felt that their clients did not have the knowledge required to work with vendors and the government to navigate cyber risks.

Exhibit 1: Overall, on a scale from 1 (poor) to 5 (excellent), how would you rate your (or your clients) performance on the following cyber risk practices?

<table>
<thead>
<tr>
<th>Risk Mangers</th>
<th>Average Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Mangers</td>
<td>3.36</td>
</tr>
<tr>
<td>Insurance Brokers</td>
<td>2.57</td>
</tr>
<tr>
<td>Legal Experts</td>
<td>2.91</td>
</tr>
</tbody>
</table>

Rating Average
Reputational costs worry businesses and external risk experts alike

There is a clear concern among risk experts that companies are not communicating appropriately following an incident. This goes beyond public relations to how organizations are communicating with all affected parties, particularly consumers.

- Risk managers (54 percent), insurance brokers (50 percent) and legal experts (38 percent), all identified crisis communications as a top priority to help mitigate reputational damage following a cyber incident.
- Many qualitative responses indicated that this is most likely due to the reputational risks associated with data breaches.

Cybersecurity remains a challenge for small businesses

Overwhelmingly, respondents noted that small businesses continue to struggle with managing cyber risks, this issue seems to stem from complacency and the dangerous misconception that small businesses are too small to be targeted by hackers, when in reality they are often the lowest hanging fruit.

- Most insurance brokers and legal experts (66 percent and 50 percent, respectively) reported that small businesses were generally less concerned about cyber risks than larger businesses.
- Seventy-five percent of insurance brokers and legal experts noted that their small business clients were either “not prepared at all” or “not very well prepared” to respond to a cyber incident.
- External risk experts reported that less than 25 percent of their small business clients were confident in their team’s ability to manage a cyber incident.

Employee negligence is a concern across the board

Creating a culture of security was a theme that emerged among the qualitative and quantitative responses from risk managers, legal experts and insurance brokers, with all three groups noting the importance of employee education. Considering that breaches of personal or financial information due to phishing or social engineering were a top concern for all three, this is not surprising given that these breaches are due to employee negligence.

- On average, all three groups rated their client/company’s employee education as “about average.”
- But, all three groups recognized the need to continue to educate employees, rating it as the top area of cyber incident prevention that should be prioritized (broker – 36 percent; legal – 42 percent; risk manager – 32 percent).

Overall, the results indicate that companies are not only not prepared to respond to a breach, they are not doing all they can to prevent them in the first place. To move beyond this and build confidence in their capabilities, companies need to spend more time educating employees on the cyber risks and practice responding to a wide variety of incidents. They should also regularly involve their third-party risk experts in these exercises.
KEY FINDINGS

Companies overestimate their cyber preparedness

The likelihood a company will be impacted by a cyber incident grows daily. Businesses and their trusted advisors are rightfully worried about a wide array of risks. Respondents were asked to rate on a scale from 1 (no concern) to 5 (extreme concern) how they or their clients feel about a variety of cyber risks. All agreed that the potential breach of personal or financial information due to phishing or social engineering is of greatest concern. (Exhibit 2)

While it is impossible to obtain 100 percent security, the implementation of sound cyber risk practices significantly reduces the odds of becoming a victim, as well as reduces the severity of a loss should a breach occur. Therefore comprehensive and regularly tested cyber incident response plans are important. They can significantly improve a company’s performance following a cyber incident and reduce the impact.

“I think that the lack of preparedness will create as many problems as the incident itself,” a broker explained. “For those clients who rely on public trust, I think that the lack of preparedness will erode that trust and place the company more at risk.”

With this in mind, the survey respondents were asked how well-prepared they, or their clients, are to respond to a cyber incident.

Exhibit 2: Please rate the level of concern you (or your clients) have, in general, for the following cyber risks.

<table>
<thead>
<tr>
<th>Cyber Risk Description</th>
<th>Score by Respondents</th>
<th>Score by Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware (Holding your network hostage for extortion)</td>
<td>3.48</td>
<td>3.84</td>
</tr>
<tr>
<td>Transfer of funds to unauthorized recipient due to spear phishing or social engineering</td>
<td>3.62</td>
<td>3.84</td>
</tr>
<tr>
<td>Breach of personal or financial information due to phishing or social engineering</td>
<td>3.81</td>
<td>4.08</td>
</tr>
<tr>
<td>Vulnerability of cloud data storage</td>
<td>3.22</td>
<td>3.28</td>
</tr>
<tr>
<td>Targeting of Intellectual Property (IP) and financial data during M&amp;As</td>
<td>2.93</td>
<td>3.23</td>
</tr>
<tr>
<td>Nation state cyber attacks</td>
<td>2.81</td>
<td>2.88</td>
</tr>
<tr>
<td>Internet of Things (IoT) Vulnerability</td>
<td>2.67</td>
<td>3.23</td>
</tr>
<tr>
<td>Vulnerability of cloud data storage</td>
<td>3.33</td>
<td>3.28</td>
</tr>
<tr>
<td>Breach of personal or financial information due to phishing or social engineering</td>
<td>3.52</td>
<td>4.08</td>
</tr>
<tr>
<td>Transfer of funds to unauthorized recipient due to spear phishing or social engineering</td>
<td>2.93</td>
<td>3.84</td>
</tr>
<tr>
<td>Ransomware (Holding your network hostage for extortion)</td>
<td>3.34</td>
<td>3.84</td>
</tr>
</tbody>
</table>

Exhibit 2: Please rate the level of concern you (or your clients) have, in general, for the following cyber risks.
The majority of risk managers surveyed (86 percent) believe they are at least somewhat prepared to respond to a cyber incident. (Exhibit 3) Even the smallest companies surveyed (revenue less than $25M) believe they are at least somewhat prepared.

“The company is confident that it is well protected against cyber incidents but needs to develop a response plan,” one risk manager explained.

“We conduct annual cyber security table tops and work closely with our insurance provider to engage in these exercises,” said a risk manager. “We have an incident response team established with specific responsibilities assigned in case of such an event.”

Exhibit 3 (Risk Manager): How well prepared do you feel your company is to respond to a cyber incident?
Insurance brokers and legal experts are generally in agreement with risk managers when it comes to the ability of large businesses (revenue greater than $1B) to respond, but they do not have nearly the same level of confidence in small and midsize businesses. (Exhibit 4)

When looking more specifically at individual corporate cyber risk practices, however, there appears to be less confidence in businesses’ ability to respond, particularly by legal experts and insurance brokers.

When asked to rate their (or their clients) performance on specific cyber risk practices, in every instance the weighted average of risk manager response was higher than those of their trusted advisors. (Exhibit 5)
The lack of confidence by many of the insurance brokers and legal experts (61 percent and 54 percent respectively) is further confirmed by their opinion that their clients do not have the knowledge required to work with vendors and the government to navigate cyber risks.

“Most of my clients do not purchase a cyber insurance policy and I believe they would panic and make a rash decision before thinking to contact me," said one broker.

“I am concerned many clients will attempt to handle the incident themselves prior to notifying me or their carrier,” another broker explained.

**Reputational costs are a major concern**

Time and again companies are seen mishandling their response to high-profile cyber incidents resulting in customer churn and a diminished ability to meet anticipated revenues. The financial harm from a damaged reputation and loss of consumer confidence has the potential to exceed other cyber-related first- or third-party financial losses.

How a company communicates both publicly and with affected parties can significantly reduce the reputational impact of a cyber incident. Some tips include being honest and to the point, showing remorse, clearly explaining how the incident will affect those impacted, advising those impacted on how best to protect themselves, and communicating to customers their importance to the business.

“My clients and I are most concerned with public response/communication,” said a broker responding to the survey. “Most businesses can sustain the financial damage associated with network repair, credit monitoring, etc., because they purchase insurance to cover these types of costs. The costs and effects of customers’ reactions to a cyber incident are harder to quantify and much costlier to repair.”

According to the study, this potential for substantial, and even catastrophic, loss is not overlooked by risk managers and their trusted advisors. All three groups identified “crisis communications” as a priority when it comes to cyber incident response. (Exhibit 6)

“First and foremost, my clients and I are most concerned about timely effective communication to all parties affected by the cyber incident,” a broker explained.

“Reputational risk, particularly in the healthcare and technology environments is a top concern because increased levels of competition allow customers to move business with ease,” said another broker.

**Exhibit 6: In general, if you had to choose one area you, or your client, should prioritize more when it comes to cyber incident response what would it be?**

<table>
<thead>
<tr>
<th>Service Area</th>
<th>Risk Managers</th>
<th>Broker</th>
<th>Legal Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Center Operations</td>
<td>4.3%</td>
<td>2.1%</td>
<td>1.6%</td>
</tr>
<tr>
<td>Legal Services</td>
<td>11.1%</td>
<td>4.6%</td>
<td>1.6%</td>
</tr>
<tr>
<td>Credit Monitoring</td>
<td>11.1%</td>
<td>2.1%</td>
<td>1.6%</td>
</tr>
<tr>
<td>Forensic Investigation</td>
<td>25.6%</td>
<td>32.0%</td>
<td>33.3%</td>
</tr>
<tr>
<td>Crisis Communication</td>
<td>53.9%</td>
<td>50.0%</td>
<td>37.5%</td>
</tr>
</tbody>
</table>

0% 10% 20% 30% 40% 50% 60%
Cybersecurity remains a challenge for small businesses

The study revealed that cybersecurity is especially challenging for businesses with less than $15 million in annual revenue. Small businesses continue to lag behind large and midsize companies in their ability to prevent and respond to a cyber incident. Respondents to the survey believe this is in large part due to a lack of risk awareness and, in some cases, conscious decisions to simply ignore the risks.

Overwhelmingly, insurance brokers and legal experts reported small businesses were less prepared to respond to a cyber incident than midsize and large companies. Seventy-five percent of insurance brokers and legal experts said small business clients were either “not prepared at all” or “not very well prepared” to respond to a cyber incident. (Exhibit 7)

“Much of the feedback we receive from small businesses regarding cyber issues are they still don’t see it as a threat. The ‘can’t happen here’ mentality is still prevalent,” said a broker.

“Many smaller accounts do not seem to be worried about cyber risk at all,” another broker explained.

The notion that these risks are exclusive to big business is not only naïve but also dangerous as they have the potential to turn a thriving business into one that is struggling for survival.

“Based on my experience, the midsize businesses have a better understanding and are more concerned about the risks they have than small businesses,” a broker explained. “Small businesses tend to think they won’t be targeted. It all comes down to a lack of consistent education on the exposures and claims outside of what makes the news.”

“Awareness of risk seems to correlate with size of organization, type of service (for example, retail is generally aware due to PCI-DSS and history of compromises), maturity of organization, and type of industry,” a lawyer explained. “For small businesses, cybersecurity lags behind other priorities that demand their limited resources. Making the process of mitigating risk as simple and affordable as possible for this large segment is extremely important.”

Exhibit 7: How well prepared do you feel your client’s are to respond to a cyber incident?
Interestingly, disconnect exists between risk professionals of small businesses and their trusted advisors regarding cyber incident response capabilities. In fact, none of the risk managers from the smallest companies surveyed feel they are “not at all prepared” to respond to a cyber incident. A reason for this may be a heightened awareness of the risks and consequences by external risk experts based on their experiences working with many clients. (Exhibit 8)

The insurance brokers and legal experts results consistently support the view that small businesses are lacking in the ability to respond to a cyber incident.

For example, the majority of insurance brokers and legal experts (81 percent and 61 percent respectively) reported less than 25 percent of their small business clients have in place formal cyber incident response plans. Similarly, the majority reported that less than 25 percent of their small business clients have cyber incident response teams in place (brokers 81 percent; legal experts 70 percent).

Most also said less than 25 percent of their small business clients were confident in their team’s ability to manage a cyber incident (brokers 88 percent; legal experts 42 percent).

And perhaps not surprising, most insurance brokers and legal experts (75 percent and 67 percent respectively) reported less than 25 percent of their small business clients have pre-selected third-party vendors. (Exhibit 9)
Taken as a whole, this presents a challenge to the third-party partners of small businesses.

“Small businesses are not convinced they could be targets and they do not want to add a new insurance cost. I feel this is very dangerous for the agent due to E&O exposures if we do not offer coverage or if we do and they do not buy it,” a broker explained.

Employee negligence is a leading concern

As previously noted, breaches of personal or financial information due to phishing or social engineering is a top concern of all three groups. This heightened concern reinforces the importance of employee education. All three groups rated employee education as an area of cyber incident prevention that needs to be prioritized. (Exhibit 10)

A plausible reason employee education is so highly prioritized is that exploiting a person is often easier and more effective than exploiting a vulnerability within a network or web application. Many organizations, even those that spend hundreds of millions of dollars on highly sophisticated cybersecurity technology, are vulnerable to crimes of deception.

While employee education certainly reduces the risk, all it takes is one mistake by an unsuspecting employee.

“The human element remains the weakest link, no matter how much training is provided there will be times when people are too busy or not paying attention and will fall victim to a phishing scheme,” said a risk manager.

Exhibit 10: If you had to choose one area your company (or your client’s company) should prioritize more when it comes to cyber incident prevention what would it be?

<table>
<thead>
<tr>
<th>Area</th>
<th>Risk Manager</th>
<th>Broker</th>
<th>Legal Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Education</td>
<td>32%</td>
<td>36%</td>
<td>42%</td>
</tr>
<tr>
<td>Vendor Management</td>
<td>5%</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>Exposure Identification (e.g. IP, Customer Data, Financial Data)</td>
<td>11%</td>
<td>6%</td>
<td>9%</td>
</tr>
<tr>
<td>Network Protection (e.g. Encryption, Firewalls, Network Segmentation)</td>
<td>6%</td>
<td>6%</td>
<td>9%</td>
</tr>
<tr>
<td>Network Monitoring</td>
<td>1%</td>
<td>4%</td>
<td>1%</td>
</tr>
<tr>
<td>Response Preparedness</td>
<td>14%</td>
<td>11%</td>
<td>9%</td>
</tr>
<tr>
<td>Vulnerability Identification</td>
<td>8%</td>
<td>8%</td>
<td>7%</td>
</tr>
<tr>
<td>Disclosure Obligations</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Cyber Insurance Purchasing</td>
<td>0%</td>
<td>4%</td>
<td>11%</td>
</tr>
<tr>
<td>Staffing of Cybersecurity Talent</td>
<td>7%</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
<td>2%</td>
<td>0%</td>
</tr>
</tbody>
</table>
The silver lining

After highlighting layers of cyber risk concerns, the study also revealed areas of hope.

An aspect of effective risk mitigation is the ability to identify the risks. This is an area where the study found consensus: all three groups were in agreement on the risks that would impact them the most in the coming year. (Exhibit 11)

Lastly, and perhaps most importantly, cyber risk also is no longer viewed as just an information technology (IT) issue, but rather an issue that receives cross-departmental attention in most organizations.

Seventy-seven percent of risk managers felt their senior managements’ cyber risk concerns closely aligned with the corporate risk management and IT departments’ concerns. Likewise, 77 percent of insurance brokers and 84 percent of legal experts reported that their clients’ senior management was aligned with them on cyber incident response.

Exhibit 11: Which cyber risk do you think will impact you (or your clients) the most in the coming year?

<table>
<thead>
<tr>
<th>Cyber Risk</th>
<th>Legal Vendor</th>
<th>Broker</th>
<th>Risk Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware (holding your network hostage for extortion)</td>
<td>14%</td>
<td>12%</td>
<td>26%</td>
</tr>
<tr>
<td>Transfer of funds to unauthorized recipient due to phishing or social engineering</td>
<td>6%</td>
<td>12%</td>
<td>22%</td>
</tr>
<tr>
<td>Breach of personal or financial information due to phishing or social engineering</td>
<td>4%</td>
<td>4%</td>
<td>32%</td>
</tr>
<tr>
<td>Vulnerability of cloud data storage</td>
<td>6%</td>
<td>3%</td>
<td>39%</td>
</tr>
<tr>
<td>Targeting of intellectual property (IP) and financial data during M&amp;As</td>
<td>2%</td>
<td>4%</td>
<td>3%</td>
</tr>
<tr>
<td>Nation State cyber attack</td>
<td>2%</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>Internet of Things (IoT) vulnerability</td>
<td>6%</td>
<td>4%</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
<td>8%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Other
SUMMARY

The challenges of cyber risk preparedness and response can lead to a crisis in confidence in an organization since the cyber risk landscape is constantly changing, making it difficult to stay abreast of the latest threats. Being prepared and properly training employees and associated response teams, however, is essential to effectively managing a cyber incident. Unprepared companies risk potentially catastrophic outcomes.

The Experian/Advisen survey of risk managers and their trusted advisors revealed areas of strength, but also numerous areas where work is required. Smaller companies, in particular, appear to not fully understand their exposure to potentially crippling cyber risks, and are less diligent in their defenses and response preparations. The fact that there tends to be alignment throughout organizations on cyber risk priorities is a good sign, and suggests that further progress on security and preparedness issues is nearly certain.
METHODOLOGY

The survey was conducted for three weeks in March and April 2017. Invitations to participate were distributed by email to cyber insurance professionals (risk managers and insurance brokers) as well as a sample of the top legal professionals in the niche market of cybersecurity and privacy protection counseling. It was completed at least in part by 143 risk managers, 139 insurance brokers, and 25 legal experts for a total of 307 responses.
RISK MANAGER SURVEY

Figure 1
Which of the following best describes your role within your organization?
- 46% Chief Risk Manager / Head of Risk Management Department
- 9% Member of Risk Management Department (not head)
- 6% Other Executive (CIO, CEO, CFO, etc.)
- 4% Chief Information Security Officer / Chief Privacy Officer
- 3% Chief Risk Officer
- 3% Other
- 1% Not sure

Figure 2
Pick the choice that best describes your firm’s industry.
- 21% Finance, Banking, and Insurance
- 16% Technology
- 16% Healthcare
- 12% Healthcare
- 12% Real Estate
- 12% Construction
- 7% Energy and Mining
- 6% Services
- 6% Transportation
- 5% Retail Trade
- 5% Automotive
- 5% Wholesale Trade
- 5% Agriculture
- 4% Other
- 4% Not sure

Figure 3
What is your company’s annual sales revenue or budget (nonprofit or government entities)?
- 24% Less than $25M
- 20% $25M to $100M
- 13% $100M to $250M
- 12% $250M to $500M
- 9% $500M to $1B
- 7% $1B to $5B
- 7% $5B to $10B
- 8% More than $10B

Figure 4
Please rate the level of concern your company has for the following cyber risks.

Figure 5
Overall, what is senior management’s level of concern regarding cyber risks?
- 45% No concern
- 32% Mild concern
- 17% Moderate concern
- 6% Strong concern
- 1% Extreme concern

Figure 6
Do you feel senior management’s concerns closely align with the corporate risk management’s and/or IT department’s concerns?
- 15% Yes
- 7% No
- 78% Don’t know
Figure 7

What is your level of confidence that the federal government will set forth policies to address cyber risks?

- No confidence: 3%
- Mild confidence: 26%
- Moderate confidence: 31%
- Strong confidence: 40%
- Extreme confidence: 0%

Figure 8

Which cyber risk do you think will impact your company the most in the coming year?

- Ransomware (holding your network hostage for extortion): 14%
- Transfer of funds to unauthorized recipient due to phishing or social engineering: 12%
- Breach of personal or financial information due to phishing or social engineering: 3%
- Vulnerability of cloud data storage: 11%
- Targeting of intellectual property (IP) and financial data during M&As: 39%
- Nation State cyber attack: 2%
- Internet of Things (IoT) vulnerability: 13%
- Other: 6%

Figure 9

How well prepared do you feel your company is to respond to a cyber incident?

- Extremely well prepared: 2%
- Very well prepared: 10%
- Somewhat well prepared: 32%
- Not very well prepared: 14%
- Not at all well prepared: 2%
- Don’t know / Not sure: 4%

Figure 10

How will your company’s cyber protections (including insurance) spending in 2017 compare with 2016? In 2017, do you think your company will spend...

- Much more: 41%
- Somewhat more: 46%
- About the same: 0%
- Somewhat less: 4%
- Much less: 10%
- Don’t know / Not sure: 0%

Figure 11

On a scale from 1 to 5, how do you think your company’s cyber security practices compare to similar organizations?

- Staffing of cybersecurity talent: 3.86
- Cyber insurance purchasing: 3.61
- Disclosure obligations: 3.44
- Vulnerability identification: 3.44
- Response preparedness: 3.36
- Network monitoring: 3.36
- Network protection (e.g. encryption, firewalls, network segmentation): 3.04
- Exposure identification (e.g. exposure data, customer data, financial data): 3.04
- Vendor management: 2.99
- Employee education: 2.99

Figure 12

If you had to choose one area your company should prioritize more when it comes to cyber incident prevention, what would it be?

- Employee education: 32%
- Response preparedness: 14%
- Exposure identification (e.g. IP, customer data, financial data): 14%
- Network protection (e.g. encryption, firewalls, network segmentation): 11%
- Vulnerability identification: 10%
- Staffing of cybersecurity talent: 9%
- Cyber insurance purchasing: 7%
- Network monitoring: 5%
- Disclosure obligations: 5%
- Other (please specify): 4%
If you had to choose one area your company should prioritize more when it comes to cyber incident response what would it be?

- Crisis communication: 54%
- Forensic investigation: 11%
- Legal services: 26%
- Call center operations: 11%
- Other: 4%
- Credit monitoring: 3%

Does your company have a formal cyber incident response plan?

- Yes: 24%
- No: 58%
- Don't know / Not sure: 18%

How frequently is your cyber incident response plan tested?

- Never: 43%
- Monthly: 9%
- Quarterly: 9%
- Twice a year: 10%
- Annually: 22%
- Once every two years: 4%
- Less often than every two years: 1%
- Don't know / Not sure: 2%

How frequently does the risk management department collaborate with the IT department on cybersecurity risk management in your organization?

- Never: 38%
- Rarely: 19%
- Sometimes: 32%
- Often: 9%
- Don't know: 3%

Do you use inside counsel for cyber events or do you seek outside legal advice?

- Inside: 70%
- Outside: 23%
- A combination of both: 7%

Does your company have an internal cyber incident response team in place?

- Yes: 19%
- No: 60%
- Don't know / Not sure: 21%
Figure 19

What departments are represented on your cyber incident response team or committee?

Figure 20

Has your company pre-selected third-party vendors to assist with breach preparation and response?

Figure 21

What kind of third-party vendors have you pre-selected?

Figure 22

How did your company select your cyber-incident preparation and response vendors?

Figure 23

How concerned are you about the following when it comes to vendor selection?
Please share any additional thoughts

NATION STATE CYBER ATTACKS

Breach of personal or financial information due to phishing or spear

Figure 1

Do these concerns vary based on size of business?

Figure 2

In general, how closely aligned are your clients’ senior management and risk management teams with regard to cyber incident response?

Figure 3

In general, do your clients have the knowledge required to work with vendors and the government to help navigate cyber risks?

Figure 4

What is your level of confidence the federal government will set forth policies to address cyber risks faced by your clients, both current and emerging?

Figure 5

Which cyber risk do you think will impact your clients the most in the coming year?

Figure 6
Figure 7

In general, how well prepared do you feel your clients are to respond to a cyber incident?

- LARGE BUSINESSES (GREATER THAN $1B IN REVENUE): 3.21
- MIDSIZE BUSINESSES BETWEEN $1M AND $1B IN REVENUE: 2.78
- SMALL BUSINESSES (LESS THAN $1M IN REVENUE): 1.82

Rating Avg (1 = not at all prepared, 5 = extremely prepared)

Figure 8

In general, do your clients plan to spend more on cyber protections (including insurance) in 2017 compared with 2016?

- LARGE BUSINESSES (GREATER THAN $1B IN REVENUE): 3.32
- MIDSIZE BUSINESSES BETWEEN $1M AND $1B IN REVENUE: 3.35
- SMALL BUSINESSES (LESS THAN $1M IN REVENUE): 3.22

Rating Avg (1 = much less, 5 = much more)

Figure 9

Overall, how would you rate your clients' performance on the following cyber risk practices?

- Employee education: 4.22
- Network protection (e.g., encryption, firewalls, network segmentation): 3.91
- Network monitoring: 3.42
- Vulnerability identification: 3.20
- Risk assessment: 2.99
- Vendor management: 2.64
- Employee education: 2.37

Rating Avg (1 = poor, 5 = Excellent)

Figure 10

In general, if you had to choose one area your clients should prioritize more when it comes to cyber incident prevention what would it be?

- Employee education: 35%
- Network protection: 12%
- Cyber insurance purchasing: 10%
- Supplier management: 10%
- Cyber security awareness training: 7%
- Other: 5%
- Vulnerability identification: 3%
- Response preparedness: 3%
- Encryption of data: 2%
- Encryption of data: 2%
- Encryption of data: 1%

Figure 11

Understanding that each situation is unique, how would you rate your clients’ ability to respond to a cyber incident?

- Excellent: 44%
- Above average: 10%
- Average: 10%
- Below average: 9%
- Poor: 4%

Figure 12

In your opinion, which industries are most at risk for a cyber incident?

- Health and Human Services: 27%
- Finance: 24%
- Retail Trade: 24%
- Technology: 15%
- Manufacturing: 15%
- Education: 12%
- Healthcare: 12%
- Real Estate: 6%
- Construction: 3%
- Transportation: 3%
- Other: 3%
- Wholesale Trade: 2%
- Agriculture: 1%
Figure 13

What percentage of your clients have formal cyber incident response plans?

<table>
<thead>
<tr>
<th>Revenue Range</th>
<th>Small Businesses (less than $15M in revenue)</th>
<th>Midsize Businesses (between $15M and $1B in revenue)</th>
<th>Large Businesses (greater than $1B in revenue)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 25%</td>
<td>23%</td>
<td>33%</td>
<td>31%</td>
</tr>
<tr>
<td>26 - 50%</td>
<td>21%</td>
<td>38%</td>
<td>35%</td>
</tr>
<tr>
<td>51 - 75%</td>
<td>21%</td>
<td>42%</td>
<td>38%</td>
</tr>
<tr>
<td>76 - 100%</td>
<td>19%</td>
<td>30%</td>
<td>25%</td>
</tr>
<tr>
<td>N/A</td>
<td>2%</td>
<td>8%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Figure 14

What percentage of your clients have internal cyber incident response teams in place?

<table>
<thead>
<tr>
<th>Revenue Range</th>
<th>Small Businesses (less than $15M in revenue)</th>
<th>Midsize Businesses (between $15M and $1B in revenue)</th>
<th>Large Businesses (greater than $1B in revenue)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 25%</td>
<td>26%</td>
<td>36%</td>
<td>33%</td>
</tr>
<tr>
<td>26 - 50%</td>
<td>24%</td>
<td>32%</td>
<td>29%</td>
</tr>
<tr>
<td>51 - 75%</td>
<td>20%</td>
<td>21%</td>
<td>17%</td>
</tr>
<tr>
<td>76 - 100%</td>
<td>13%</td>
<td>13%</td>
<td>15%</td>
</tr>
<tr>
<td>N/A</td>
<td>7%</td>
<td>4%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Figure 15

What percentage of your clients are confident in their team’s ability to manage a cyber incident?

<table>
<thead>
<tr>
<th>Revenue Range</th>
<th>Small Businesses (less than $15M in revenue)</th>
<th>Midsize Businesses (between $15M and $1B in revenue)</th>
<th>Large Businesses (greater than $1B in revenue)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 25%</td>
<td>33%</td>
<td>31%</td>
<td>31%</td>
</tr>
<tr>
<td>26 - 50%</td>
<td>29%</td>
<td>30%</td>
<td>28%</td>
</tr>
<tr>
<td>51 - 75%</td>
<td>26%</td>
<td>27%</td>
<td>28%</td>
</tr>
<tr>
<td>76 - 100%</td>
<td>22%</td>
<td>24%</td>
<td>24%</td>
</tr>
<tr>
<td>N/A</td>
<td>2%</td>
<td>8%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Figure 16

What percentage of your clients have pre-selected third-party vendors to assist with cyber incident preparation and response?

<table>
<thead>
<tr>
<th>Revenue Range</th>
<th>Small Businesses (less than $15M in revenue)</th>
<th>Midsize Businesses (between $15M and $1B in revenue)</th>
<th>Large Businesses (greater than $1B in revenue)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 25%</td>
<td>41%</td>
<td>41%</td>
<td>41%</td>
</tr>
<tr>
<td>26 - 50%</td>
<td>30%</td>
<td>30%</td>
<td>30%</td>
</tr>
<tr>
<td>51 - 75%</td>
<td>28%</td>
<td>27%</td>
<td>27%</td>
</tr>
<tr>
<td>76 - 100%</td>
<td>23%</td>
<td>23%</td>
<td>23%</td>
</tr>
<tr>
<td>N/A</td>
<td>6%</td>
<td>8%</td>
<td>8%</td>
</tr>
</tbody>
</table>

In general, if you had to choose one area your clients should prioritize more when it comes to cyber incident response what would it be?

- Crisis communication
- Forensic investigation
- Legal services
- Other
- Credit monitoring
- Call center operations

32%
Please share any additional thoughts.

Targeting of Intellectual Property (IP) and financial data

Vulnerability of cloud data storage

Breach of personal or financial information due to phishing or social engineering

LEGAL EXPERTS SURVEY

Figure 1

Do these concerns vary based on size of business?

Figure 2

Figure 3

In general, how closely aligned are your clients’ senior management and risk management teams with regard to cyber incident response?

Figure 4

In general, do your clients have the knowledge required to work with vendors and the government to help navigate cyber risks?

Figure 5

What is your level of confidence the federal government will set forth policies to address cyber risks faced by your clients, both current and emerging?

Figure 6

Which cyber risk do you think will impact your clients the most in the coming year?
**LEGAL EXPERTS SURVEY**

**Figure 7**

In general, how well prepared do you feel your clients are to respond to a cyber incident?

![Graph showing preparedness levels by business size.]

**Figure 8**

In general, do your clients plan to spend more on cyber protections (including insurance) in 2017 compared with 2016?

![Graph showing planned spending increase by business size.]

**Figure 9**

Overall, how would you rate your clients' performance on the following cyber risk practices?

![Graph showing performance ratings by risk practice.]

**Figure 10**

In general, if you had to choose one area your clients should prioritize more when it comes to cyber incident prevention, what would it be?

![Pie chart showing prioritization of risk practices.]

**Figure 11**

Understanding that each situation is unique, how would you rate your clients' ability to respond to a cyber incident?

![Graph showing response ability ratings.]

**Figure 12**

In your opinion, which industries are most at risk for a cyber incident?

![Bar chart showing industry risk levels.]

---

In general, if you had to choose one area your clients should prioritize more when it comes to cyber incident prevention, what would it be?

- Employee education
- Response preparedness
- Vulnerability identification
- Exposure identification (e.g., IP, customer data, financial data)
- Network protection (e.g., encryption, firewalls, network segmentation)
- Network monitoring
- Staffing of cybersecurity talent
- Vendor management
- Disclosure identification
- Cyber insurance purchasing
- Other
Figure 13

What percentage of your clients have formal cyber incident response plan

- Small business (less than $15M in revenue)
- Midsize business (between $15M and $1B in revenue)
- Large business (greater than $1B in revenue)

Figure 14

What percentage of your clients have internal cyber incident response teams in place?

- Small businesses (less than $15M in revenue)
- Midsize businesses (between $15M and $1B in revenue)
- Large businesses (greater than $1B in revenue)

Figure 15

What percentage of your clients are confident in their team’s ability to manage a cyber incident?

- Small businesses (less than $15M in revenue)
- Midsize businesses (between $15M and $1B in revenue)
- Large business (greater than $1B in revenue)

Figure 16

What percentage of your clients have pre-selected third-party vendors to assist with cyber incident preparation and response?

- Small businesses (less than $15M in revenue)
- Midsize businesses (between $15M and $1B in revenue)
- Large businesses (greater than $1B in revenue)

Figure 17

In general, if you had to choose one area your clients should prioritize more when it comes to cyber incident response, what would it be?

- Crisis communication
- Forensic investigation
- Legal services
- Credit monitoring
- Call center operations
- Other

38%
33%
17%
13%
4%
4%