The Importance of Senior Executive Involvement in Breach Response

Sponsored by HP Enterprise Security Services

Independently conducted by Ponemon Institute LLC

Publication Date: October 2014

The Importance of Senior Executive Involvement in Breach Response

Ponemon Institute, October 2014

Part 1. Introduction

Ponemon Institute is pleased to present the results of *The Importance of Senior Executive Involvement in Breach Response,* sponsored by HP Enterprise Security Services. The study surveyed 495 senior executives in the United States and United Kingdom to understand their perspective about the importance of executive and board level involvement in achieving an effective and strategic incident response process.

In the past, senior executives and boards of directors may have been complacent about the risks posed by data breaches and cyber attacks. However, there is a growing concern about the potential damage to reputation, class action lawsuits and costly downtime that is motivating executives to pay greater attention to the security practices of their organizations.

Our study confirms senior executives' motivation to become involved in breach response in order to help reduce the financial impact of potential incidents and to protect their companies' reputation and brand. Seventy-nine percent of respondents say executive level involvement is necessary to achieving an effective response to data breaches. Recently Jamie Dimon, CEO of JP Morgan Chase, personally informed shareholders that by the end of 2014 the bank will invest $250 million and have a staff of 1,000 committed to IT security.[1]

Key Terms

Security event and security incident are often used interchangeably. A security event is a change in the everyday operations of a network or information technology service, indicating that a security policy may have been violated or a security safeguard may have failed.

A **security breach** is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical IT perimeter. A security breach is also known as a security violation.

A **data breach** is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank details, personal health information (PHI), Personally identifiable information (PII), trade secrets of corporations or intellectual property.

The financial consequences from a security breach can be particularly severe. In this year's annual *Cost of Cyber Crime Study*, we found that the mean annualized cost for 59 U.S. companies studied in the research is $12.7 million per year, with a range from $1.6 million to $61 million per company. The average cost for 38 UK organizations is £3.56 million per year, with a range from £544,964 to £14 million.[2]

According to the study, the primary barriers to an effective breach response are: poor communications, lack of leadership and a lack of board oversight. Communication is a particular concern among respondents. Less than half of respondents (47 percent) say they are informed about their organizations' incident response plan.

Other research has shown that IT and IT security practitioners often have a difficult time talking about security risks with senior executives, especially when it involves explaining the

[1] *New JPMorgan Chase Breach Details Emerge* by Mathew J. Schwartz, Bankinfosecurity.com, August 29, 2014

[2] *2014 Cost of Cyber Crime Study: United States & United Kingdom,* conducted by Ponemon Institute and sponsored by HP Enterprise Security, October 2014.

consequences of a data breach. In one Ponemon Institute study[3], 65 percent of IT practitioners surveyed said that when asked to provide a report on a security incident that had major consequences for the organization they would modify, filter or water-down reports about a security incident. It is highly likely, therefore, that many CEOs, boards of directors and other corporate leaders are in the dark about the state of their organizations' breach preparedness.

Following are the most salient findings from this research:

Poor communications, lack of leadership and lack of board oversight are barriers to effective incident response. Seventy percent of respondents say poor communications is a barrier and 68 percent of respondents believe organizations do not have the appropriate leadership in place to deal with data breach incidents. Consistent with other findings in this study, board oversight would improve breach response.

Senior executives believe their involvement in the incident response process is necessary. Seventy-nine percent of respondents say executive level involvement is necessary to achieving an effective incident response to a data breach and 70 percent believe board level oversight is critical. However, less than half (47 percent) are kept informed about the process and only 45 percent believe they are accountable for the incident response process. Only about half of the companies represented in this study incorporate this information in their incident response plans.

Current incident response plans are more reactive than proactive. Less than half, (44 percent of respondents) characterize their organization's incident response process as proactive and mature. An important step to making these plans more effective would be to take into account both the value and importance of data to their organization's business operations.

Executive level oversight is critical to minimizing financial loss and protecting reputation and brand. How do senior executives view their responsibility when an incident occurs? Senior executives are most concerned about the long-term effects and sustainability of the organization when sensitive and confidential information is stolen. Their focus is on minimizing financial loss and avoiding reputational damage.

Understanding the risk and approving incident response plans should be on the board of directors' agenda. Seventy-seven percent of respondents say the board should be involved in reviewing risk assessments followed by approving the incident response plan (69 percent). Receiving regulatory and compliance updates (68 percent) and approving insurance coverage (66 percent) are other areas in which the board should be engaged.

From the perspective of a senior executive, what makes a data breach significant? In the context of this research, a material breach is one that requires more resources to resolve in order to minimize financial loss and reputational damage**.** Fifty-seven percent of respondents say the lost or theft of more than 10,000 records containing confidential or sensitive information constitutes a significant data breach. In terms of cost, a data breach that averages approximately $2 million is considered significant.

Negligent and malicious insiders are considered the biggest security risks. Senior executives are more concerned about the threat within than with external risks caused by cyber criminals and hactivists. Forty-two percent of respondents say they worry most about negligent insiders followed by 25 percent who say they are concerned about malicious insiders.

[3] *Threat Intelligence & Incident Response: A Study of U.S. & EMEA Organizations*, conducted by Ponemon Institute and sponsored by Access Data, February 2014.

Incident response should focus on understanding the cause of an incident and addressing the negligent insider risk. Forensics investigations are key to responding to a breach (86 percent of respondents) followed by training and awareness of employees (81 percent)—probably because of executives concern about negligent insiders. Reporting to the CEO and board of directors is also considered important because there is recognition of their accountability when an incident occurs.

Part 2. Key Findings

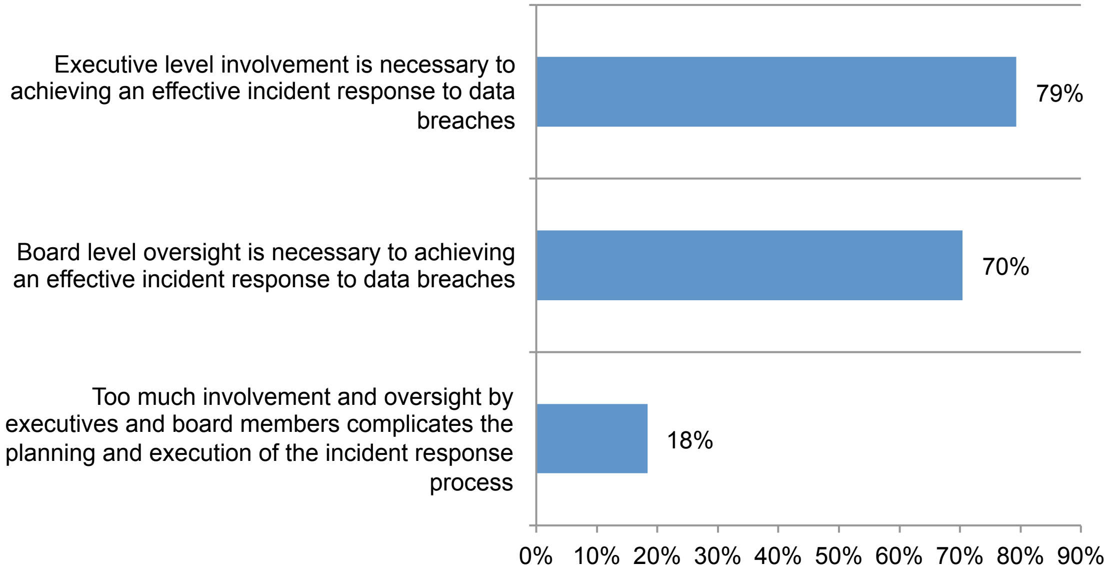
In this section, we provide an analysis of the key findings. The complete audited findings are presented in the appendix of this report. Following are the main topics of this report:

- Senior executive involvement in incident response planning
- The strategic role of senior executives in incident response
- Barriers to achieving a stronger incident response plan

Senior executive involvement in incident response planning

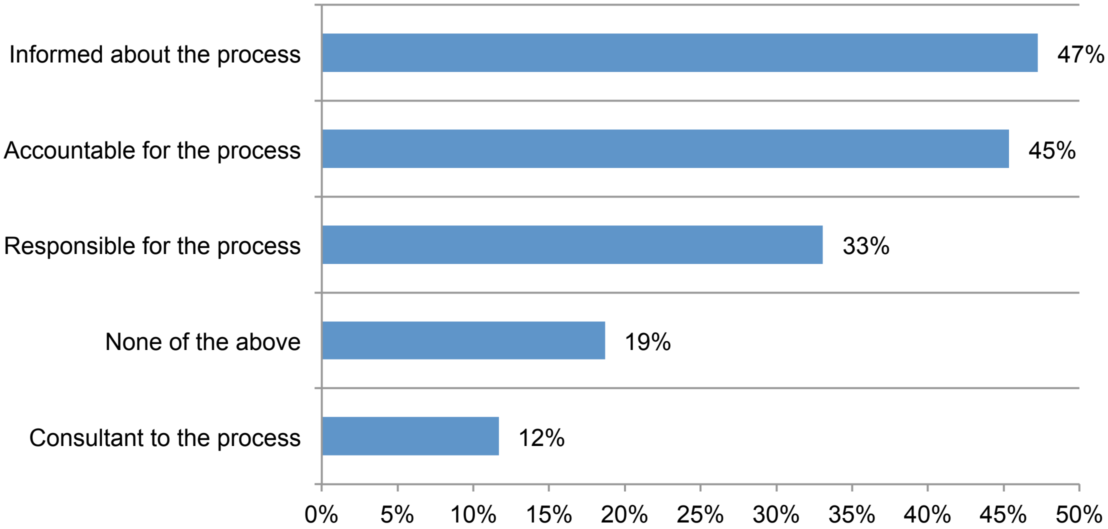
Senior executives believe their involvement in the incident response process is necessary. As shown in Figure 1, 79 percent of respondents say executive level involvement is necessary to achieving an effective incident response to a data breach and 70 percent believe board level oversight is critical. As further evidence of their intention to take a larger role in breach response, only 18 percent say too much involvement and oversight by executives and board members complicates the planning and execution of the incident response plan.

Figure 1. Executive or board level involvement in the incident response process
Strongly agree and agree response combined



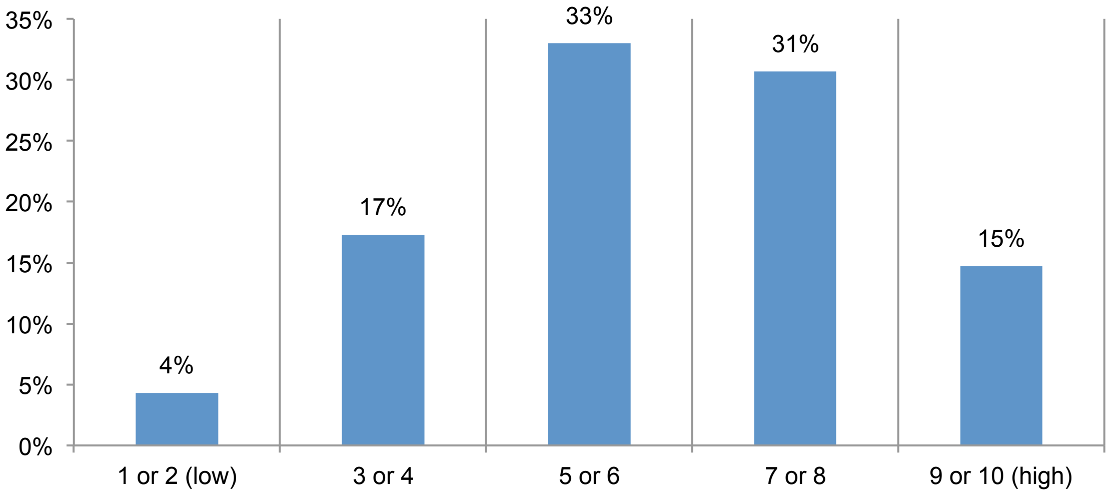
Despite the desire to be involved, less than half (47 percent of respondents) say they are informed about the process and a similar percentage (45 percent) say they are accountable, as shown in Figure 2. Only about one-third say they have responsibility for the actual response plan.

Figure 2. What best describes your involvement in the incident response process?
More than one response permitted



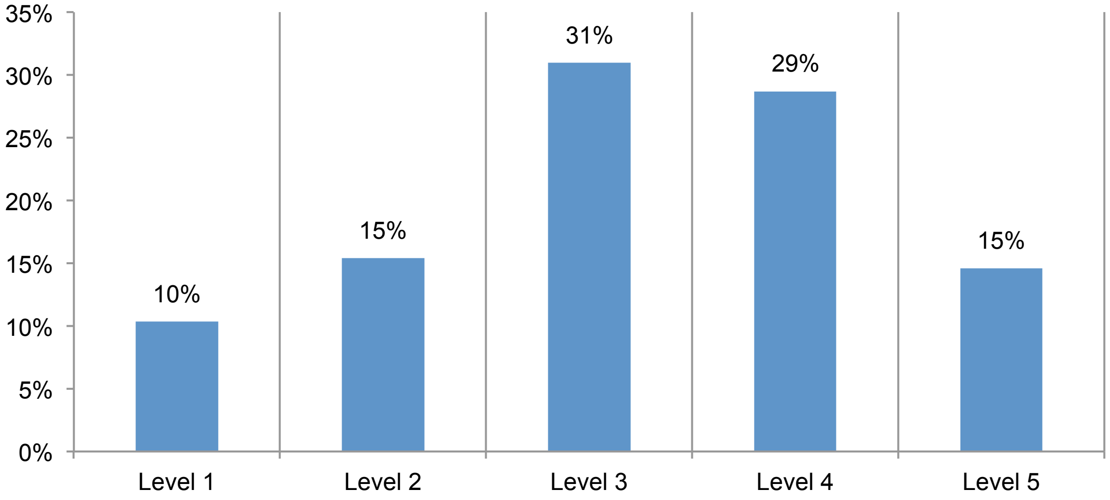
Are organizations prepared to respond to a security breach? Respondents were asked to rate on a scale of 1 to 10 how prepared their organizations are to respond to a data breach. As shown in Figure 3, 54 percent (4 percent + 17 percent + 33 percent of respondents) rate their organizations at 6 or below, indicating that their organizations are not as well prepared as they should be to respond to a breach.

Figure 3. Preparedness to deal with data breaches
Extrapolated value = 6.18



Current incident response plans are mostly reactive. The majority of respondents do not have confidence in their organization's level of breach preparedness. Respondents were asked to rank their organization's incident response capabilities from 1 = immature (completely reactive) to 5 = mature (completely proactive). Only 44 percent of respondents (29 percent + 15 percent) would characterize the breach response as mature and proactive (level 4 or 5), as shown in Figure 4.

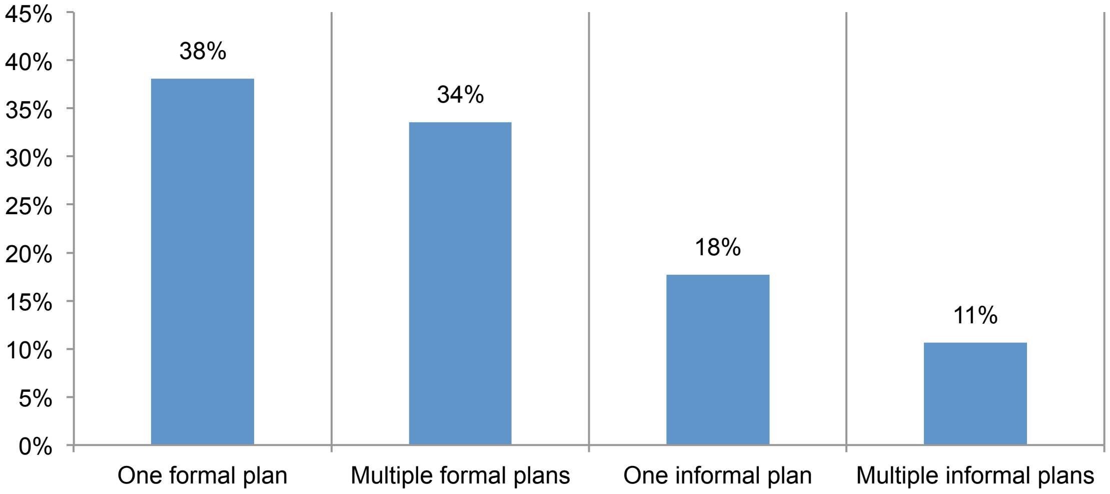
Figure 4. How mature is your organization's data breach incident response?
1 = immature to 5 = mature



As discussed above, senior executives believe the current state of breach preparedness is more reactive (immature) than proactive. This can be due to the current lack of board involvement and oversight in preparing the incident response plan and ensuring that it takes into account the value and importance of data to their organization's business operations.

Figure 5 reveals that the majority of organizations have either one formal plan (38 percent of respondents or one informal plan (18 percent of respondents). However, multiple plans may be required because of how the organization is structured. Forty-five percent of respondents say they have multiple formal plans or multiple informal plans.

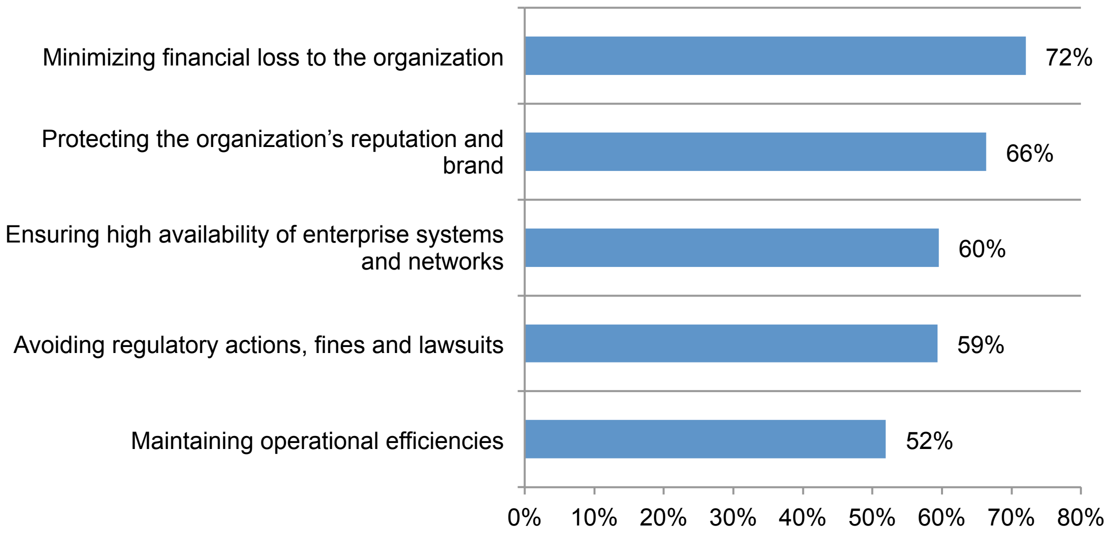
Figure 5. What best describes your response plan for data breach incidents?



Executive level involvement is critical to minimizing financial loss and protecting reputation and brand. How do senior executives view their responsibility when an incident occurs? Senior executives are most concerned about the long-term effects and sustainability of the organization when sensitive and confidential information is stolen.

According to Figure 6, 72 percent of respondents say it is their responsibility to reduce the financial impact of the incident and 66 percent say it is to protect the reputation and brand. To a lesser extent—but still important--they are concerned about avoiding regulatory actions, fines and lawsuits (59 percent) and maintaining operational efficiencies, such as avoiding downtime.

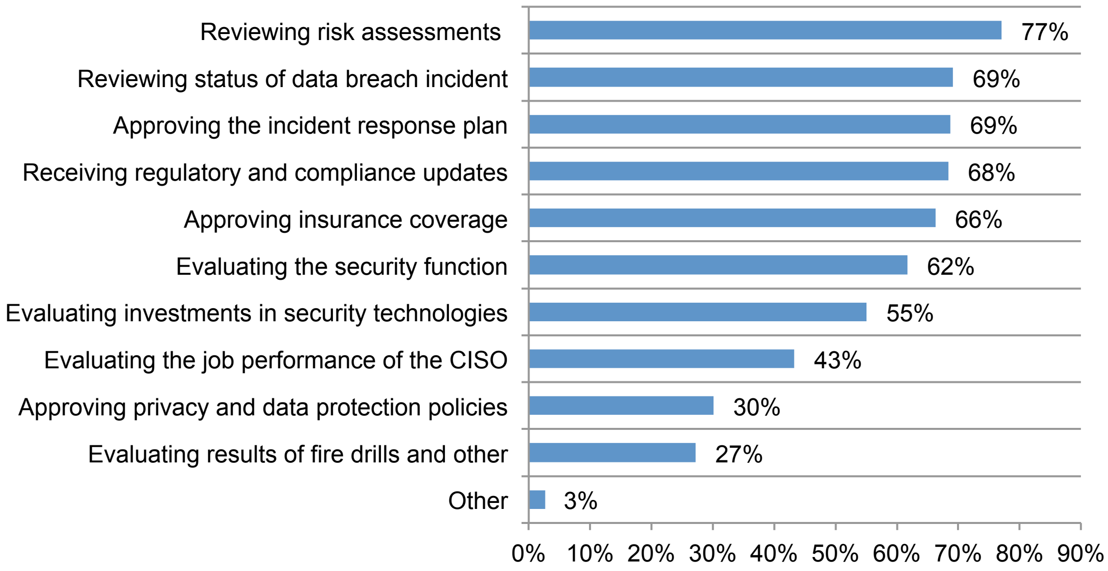
Figure 6. How important is executive-level involvement in the incident response process?
Essential and very important response combined



The strategic role of senior executives in incident response

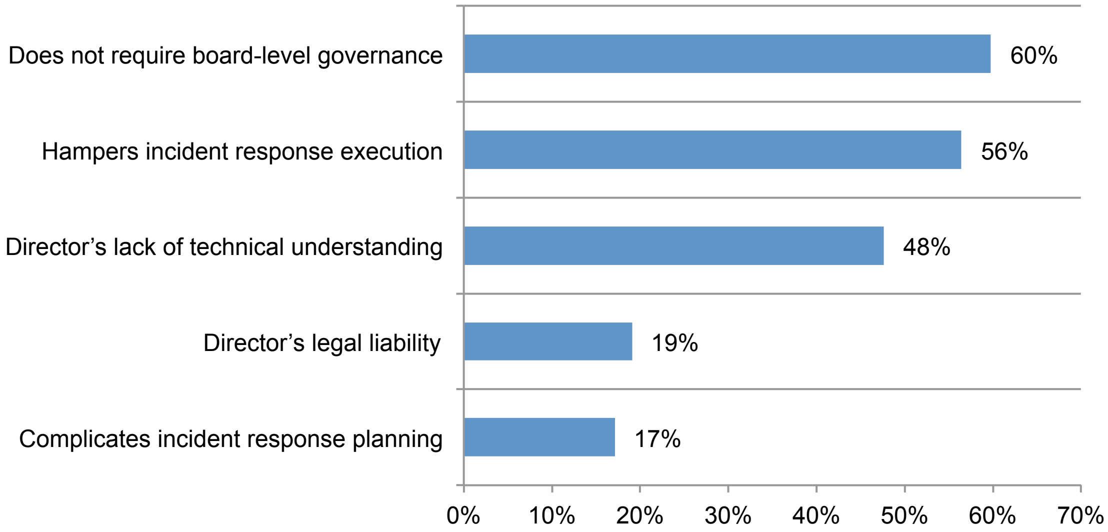
Understanding the risk and approving incident response plans should be on the board of directors' agenda. Figure 7 reveals that 77 percent of respondents say the board should be involved in reviewing risk assessments or briefings followed by approving the incident response plan (69 percent). Receiving regulatory and compliance updates (68 percent) and approving insurance coverage (66 percent) are other areas in which the board should be engaged. Not as important are evaluating the CISO's job performance and results of fire drills and other similar activities.

Figure 7. What should be on the board of directors' agenda?
More than one response permitted



While senior executives want to be involved and informed about the incident response plan, they do not want to be active in helping resolve the actual incident. According to Figure 8, 60 percent of respondents do not believe responding to actual data breach incidents should be on the board's agenda because it does not require board-level governance. Another 56 percent say it would actually hamper the execution of the response plan and 48 percent say the lack of technical understanding might not make their involvement productive.

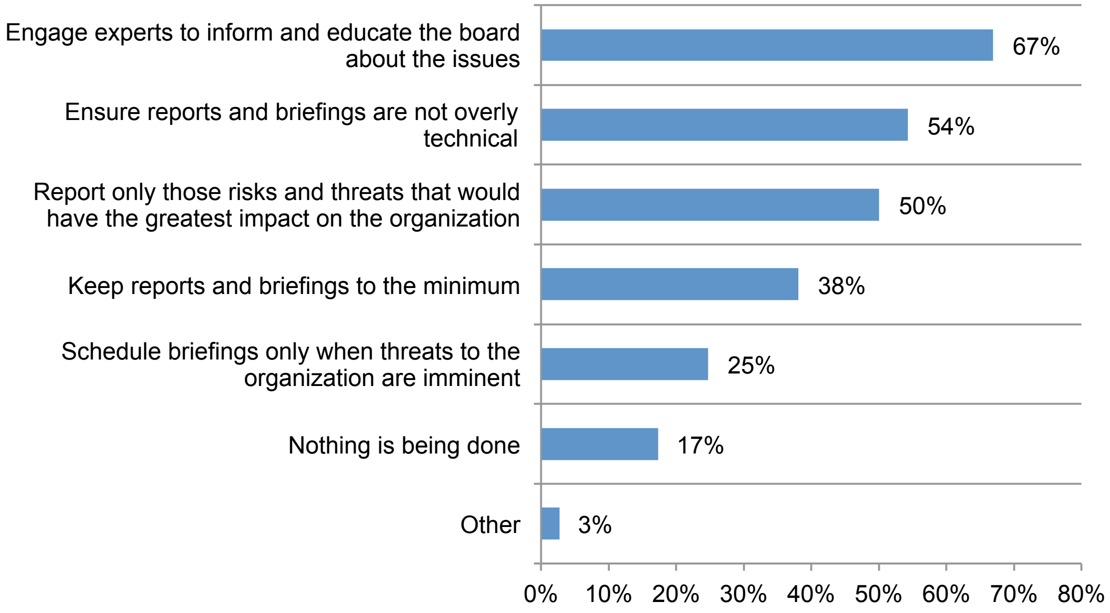
Figure 8. Why are data breach incidents not on the board's agenda?
Two responses permitted



Boards of directors do understand what they are told about data breach response. Sixty-one percent of respondents say their organizations' board of directors comprehends briefings and reports about data breach response.

Of the 27 percent of respondents who say their boards have difficulty in comprehending briefings about data breach response, 67 percent say they are engaging experts to inform and educate the board about issues or ensuring reports and briefings are not overly technical (54 percent), as shown in Figure 9.

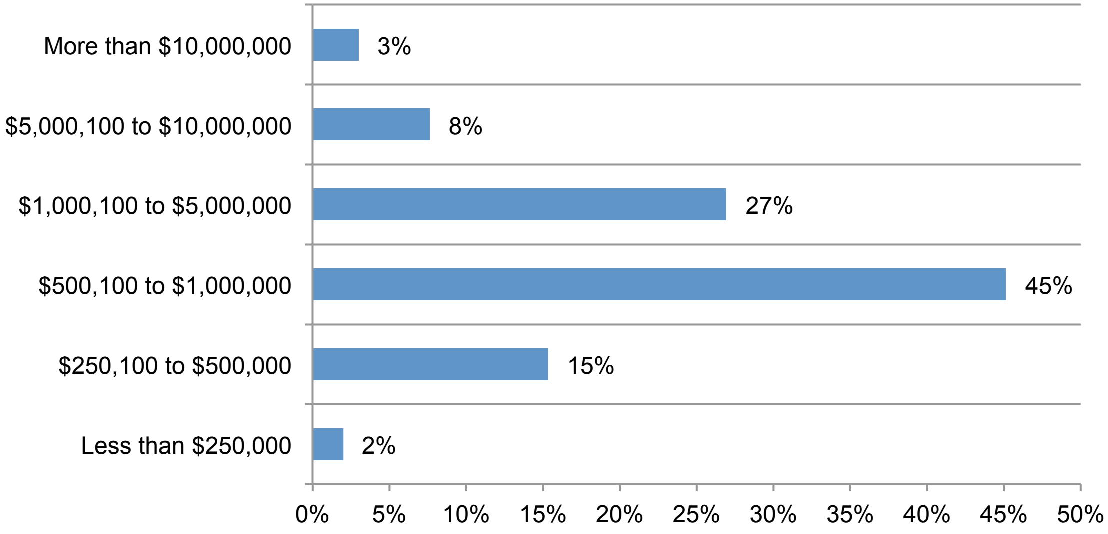
Figure 9. How to better articulate the state of data breach planning response
More than one response permitted



From the perspective of a senior executive, what makes a data breach significant? In the context of this research, a material breach is one that requires the allocation of more resources to resolve in order to minimize financial loss and reputational damage**.**

Fifty-seven percent of respondents say the lost or theft of more than 10,000 records containing confidential or sensitive information constitutes a significant data breach. Figure 10 shows in terms of what an incident could cost, a data breach that is approximately $2 million is material to the organization's operations. As noted previously, the average cost to resolve the consequences of a cyber attack in the U.S. is $12.7 million.

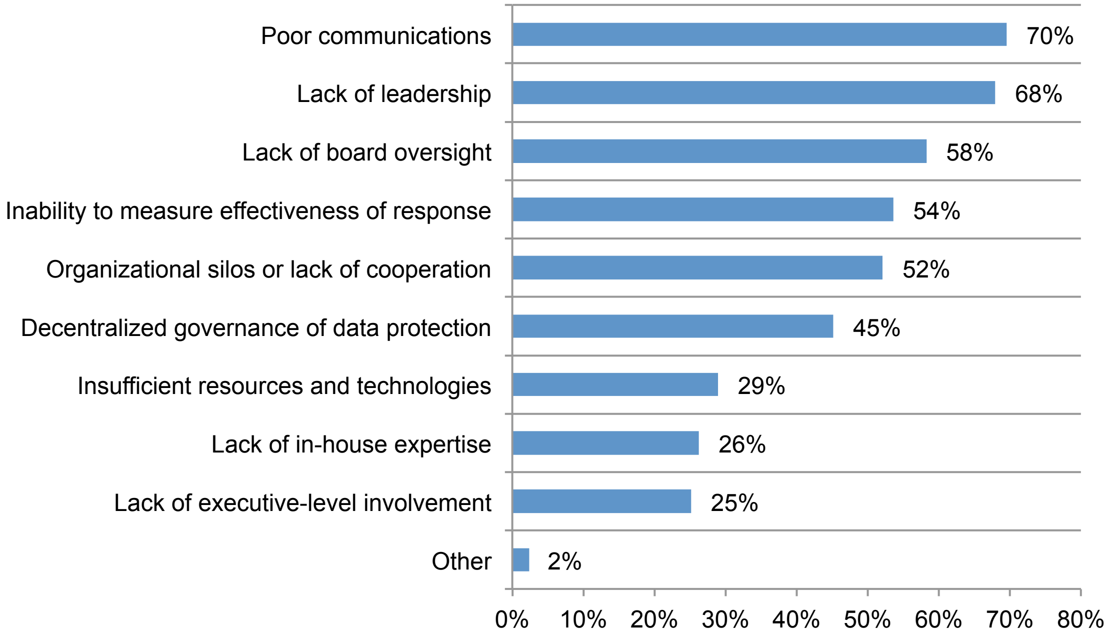
Figure 10. What constitutes a significant data breach?
Extrapolated value = $2,140,666.67



Barriers to achieving a stronger incident response plan

Poor communications, lack of leadership and lack of board oversight are barriers to effective incident response. Seventy percent of respondents say poor communications is a barrier and 68 percent of respondents believe organizations do not have the appropriate leadership in place to deal with data breach incidents. Consistent with other findings in this study, 58 percent of respondents say increased board oversight would improve breach response.

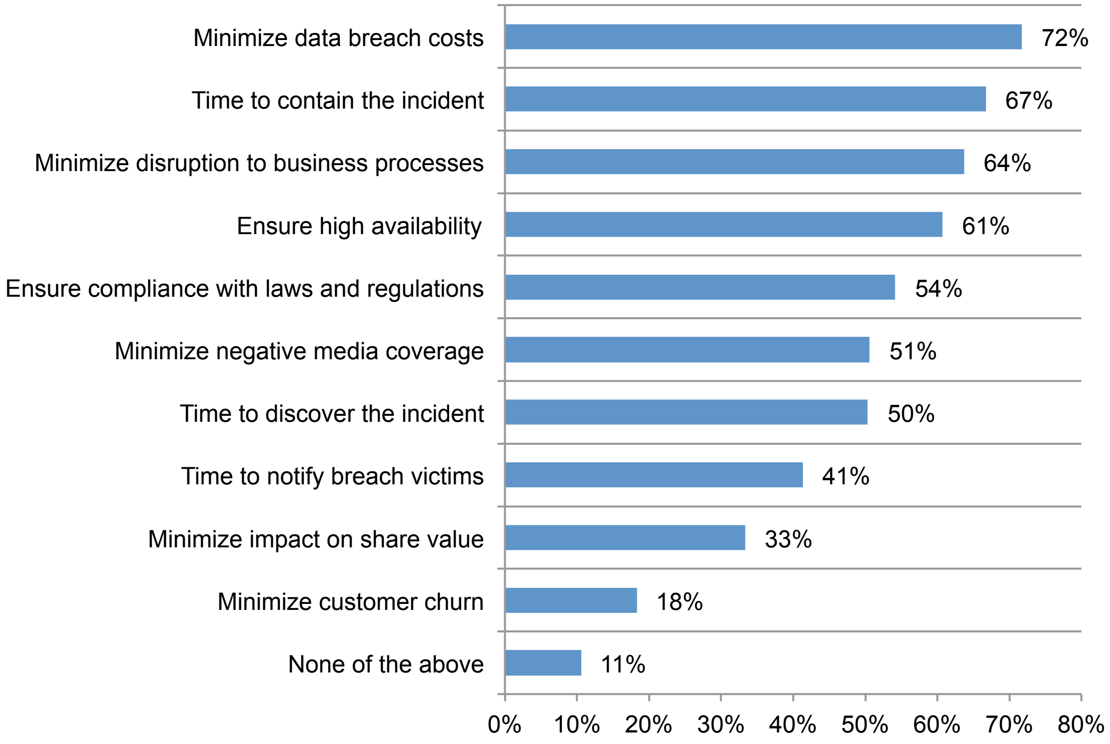
Figure 11. Main barriers to responding effectively to data breaches
More than one response permitted



Measures that track how well an organization responds to a breach can improve its ability to minimize the consequences of a future security incident. As shown above, 54 percent of respondents say not being able to measure how well the organization responds to a breach prevents them from having a more proactive and mature incident response process.

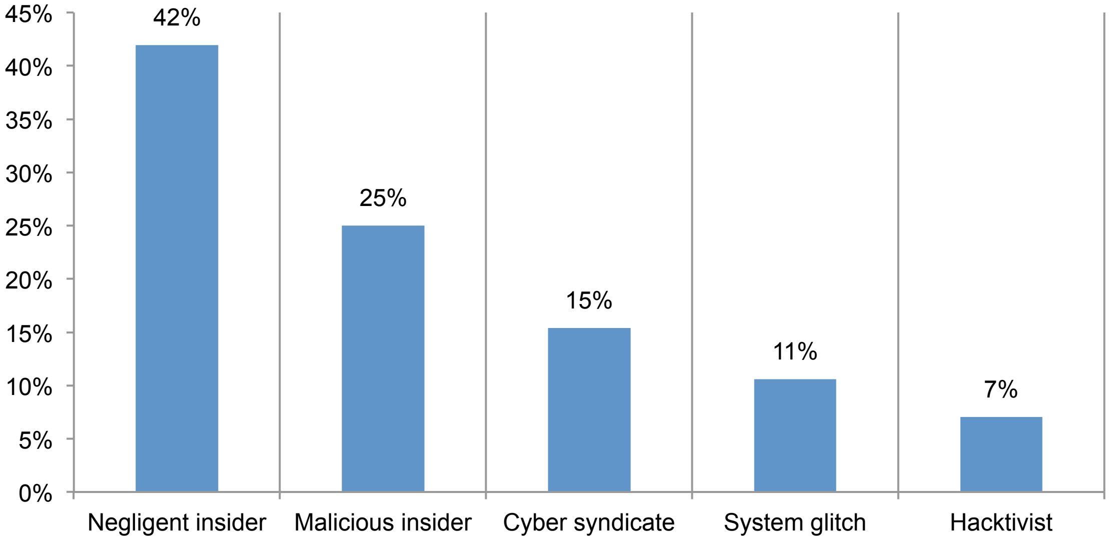
According to Figure 12, to determine the effectiveness of their organizations' response, 72 percent say they measure the ability to minimize costs and contain the incident (67 percent). Also important measures are minimizing disruption to business processes and ensuring minimal downtime in the aftermath of an incident. Because of the financial consequences of customer churn more measures should be used to determine the effectiveness of retaining the loyalty of customers.

Figure 12. Measures to determine effectiveness
More than one response permitted



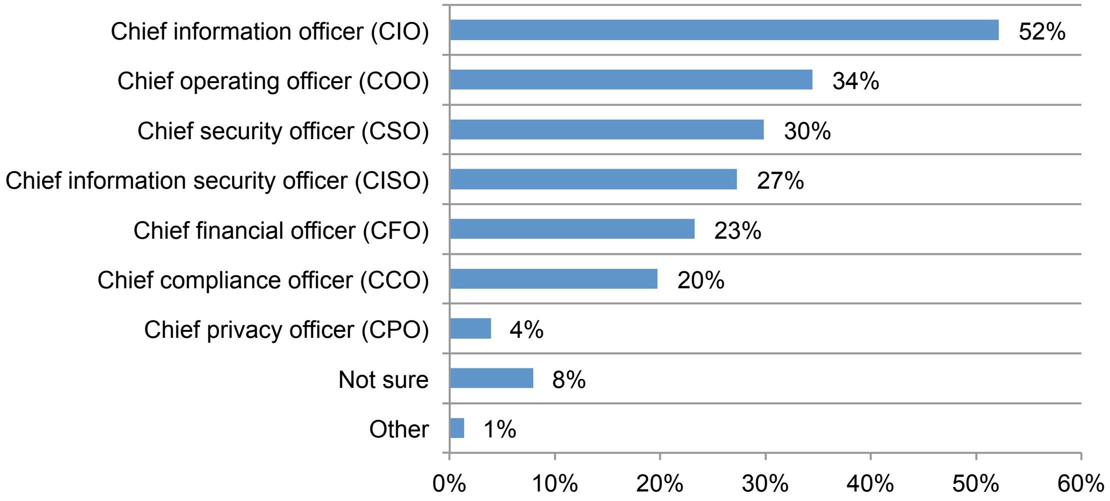
Negligent and malicious insiders are considered the biggest security risks. Incident response plans need to recognize the insider risk. Senior executives are more concerned about the threat within than with external risks caused by cyber criminals and hactivists. As shown in Figure 13, 42 percent of respondents say they worry most about negligent insiders followed by 25 percent who say they are concerned about malicious insiders.

Figure 13. Security risks that are of greatest concern



Responsibility for incident response is dispersed throughout the organization. Respondents believe a lack of leadership is a barrier to a well-executed incident response process. One possible reason is that accountability and responsibility is often spread among various functions. As revealed in Figure 14, 52 percent of respondents say the chief information officer (CIO) is most responsible for coordinating the incident response process. It is surprising that the chief information security officer, who has more security expertise, is rarely responsible for incident response.

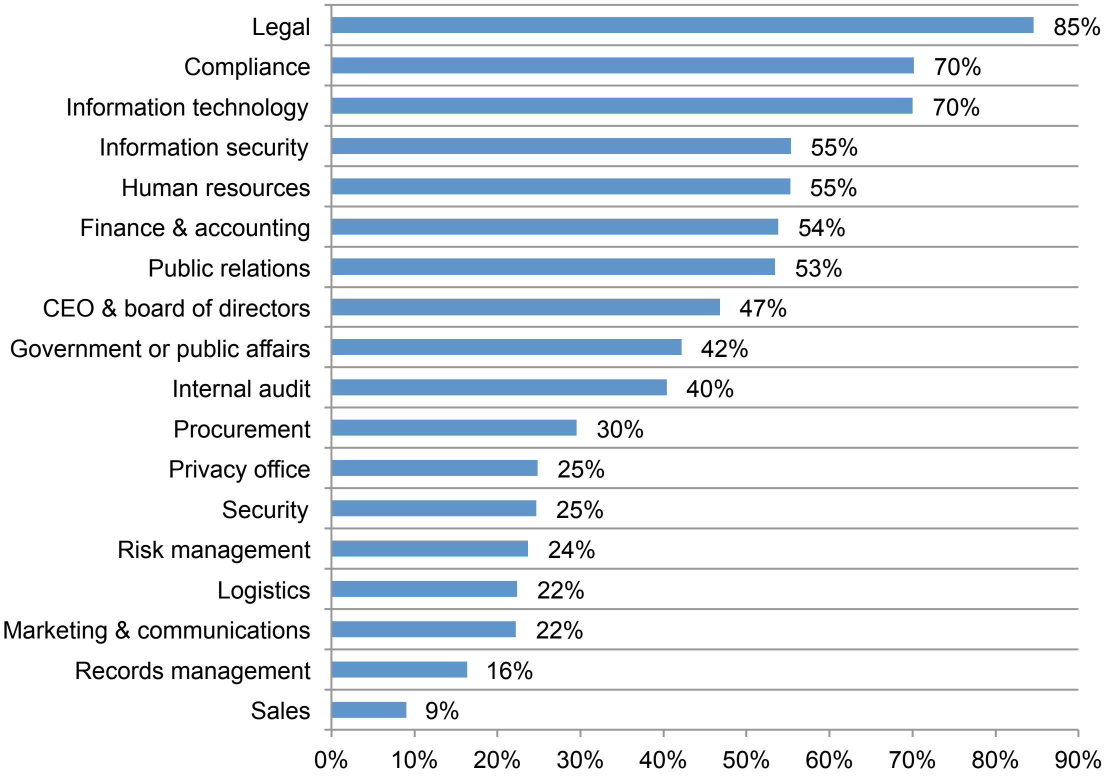
Figure 14. Who is most responsible for coordinating the incident response process?
Two responses permitted



Most often the legal department is involved in incident response planning. Eighty-five percent of respondents say their organizations' involve the legal function in the planning process, according to Figure 15. Compliance officers and CIOs follow.

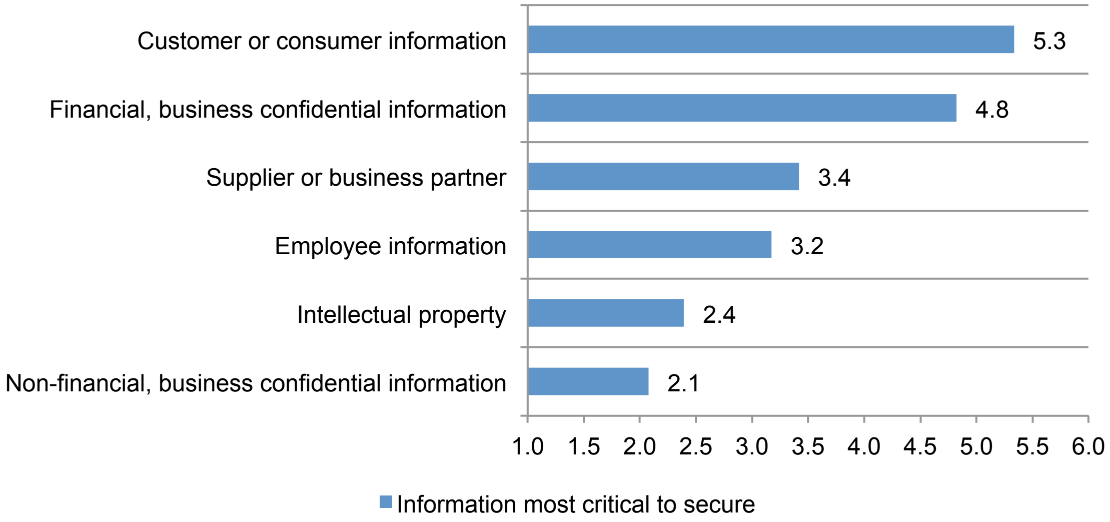
Other functions most often involved in planning are IT security, human resources, finance and accounting and public relations. It is surprising to note that risk management and the privacy office are not selected by many respondents to be part of the planning process.

Figure 15. Functional areas that participate in the incident response planning process
More than one response permitted



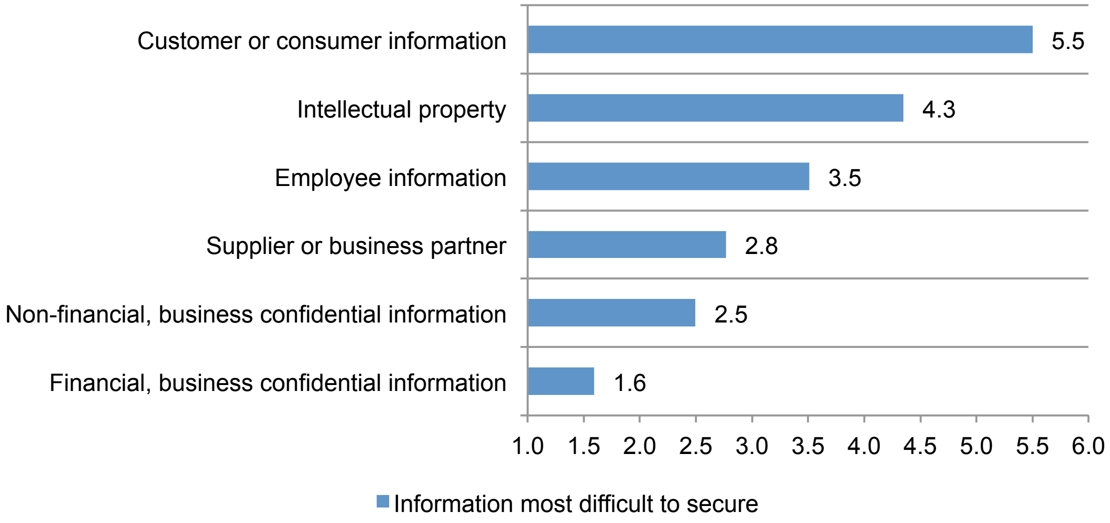
Customer or consumer information is most at risk and most critical to secure. Understanding the value and importance of an organization's information assets should be an important part of incident response preparedness. As shown in Figure 16, respondents understand the importance of safeguarding customer or consumer information and confidential business information.

Figure 16. What information is most critical to secure?
6 = most critical to 1 = least critical



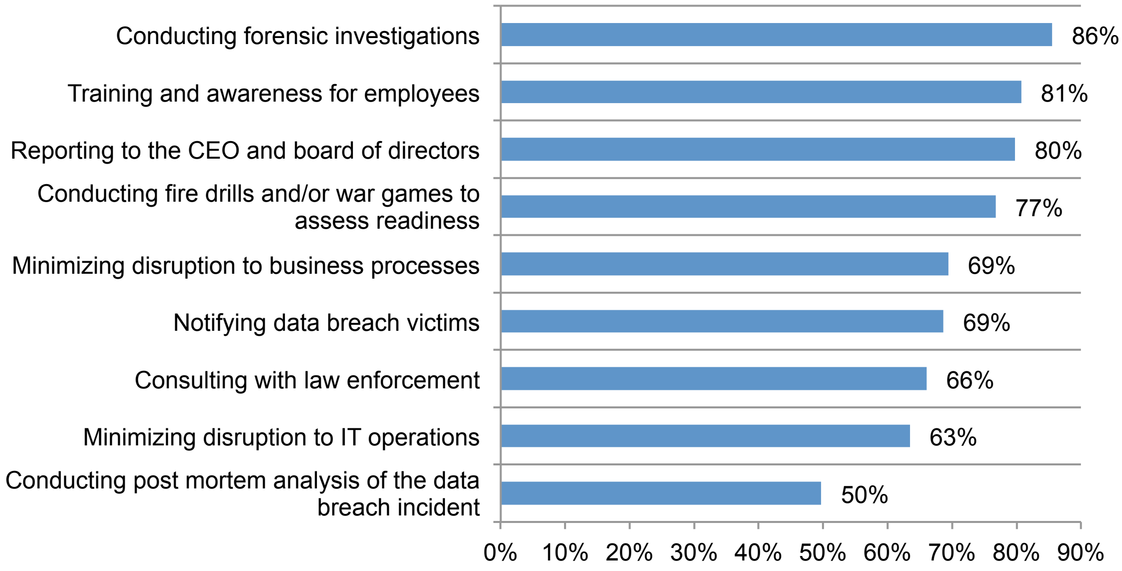
Not only is customer information critical, respondents believe that it is the most difficult to secure. While not as critical to secure, intellectual property is considered difficult to secure.

Figure 17. What information is most difficult to secure?
6 = most critical to 1 = least critical



Incident response should focus on understanding the cause, addressing the negligent insider risk and communicating with the CEO and board. Forensics investigations are key to responding to a breach (86 percent of respondents) followed by training and awareness of employees (81 percent)—probably because of executives concern about negligent insiders, as shown in Figure 18. This finding also reveals the importance of communication. Eighty percent of respondents say reporting to the CEO and board of directors is critical.

Figure 18. Importance of activities critical to incident planning and execution
Essential and very important response combined



Part 3. Conclusion: Implications & recommendations

Senior executives want greater involvement and oversight of the breach response process. Their view is the current response process is mostly reactive and not as mature and established as it should be. The existence of incident response plans that do not take into consideration the value and importance of data to the organization's business operations make communication and leadership difficult to achieve. Following are steps senior executives should take to improve breach response:

- Become proactive in understanding the security risks of the organization. Identify the valuable and sensitive information that could be targeted and have a strategy for its protection.

- Ensure security measures are put in place to address cyber attacks and data breaches. Have an independent third party provide recommendations on the adequacy of security practices and procedures.

- Schedule regular meetings (not ad hoc) with the CEO and board of directors to keep them informed about the threats to the organization and the ability of the organization to mitigate the risk of a security incident.

- Require frequent fire drills and/or war games to assess readiness. Forensics technologies and expertise should be part of the incident response plan to be able to determine the root cause of the breach as quickly as possible.

- Address the insider threat with training and awareness programs. Require audits to ensure training is ongoing and reducing employee mistakes and negligence in the handling of sensitive and valuable information. Training should especially focus on customer or consumer data because it is particularly vulnerable and difficult to secure. To reduce the malicious insider threat, review access governance practices and proof of enforcement of policies.

- Centralize leadership of the response process. The *Cost of Cyber Crime Study* provides evidence of the benefits of appointing a high-level security leader supported by certified and expert staff to be accountable and responsible for incident response. In the event of a security incident, these governance practices were shown to reduce the cost to respond to the incident by an average of $2.3 million and $2.2 million, respectively.

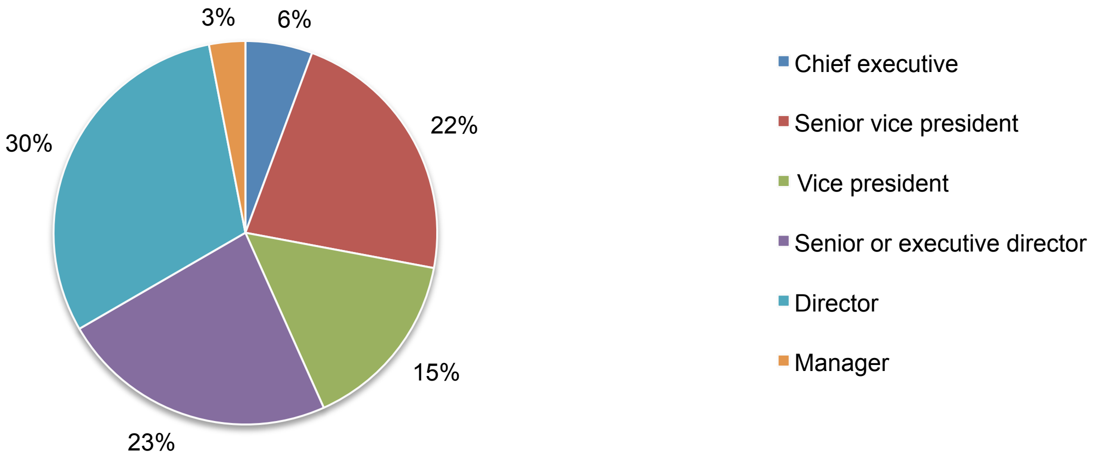
Part 4. Methods

A sampling frame composed of 15,634 senior executives located within the United States and United Kingdom was selected for participation in this survey. As shown in the following table, 579 respondents completed the survey. Screening removed 84 surveys. The final sample was 495 surveys (or a 3.2 percent response rate).

Table 1. Sample response	US	UK	Combined
Sampling frame	9880	5754	15634
Total returns	368	211	579
Rejected or screened surveys	46	38	84
Final sample	322	173	495
Response rate	3.3%	3.0%	3.2%

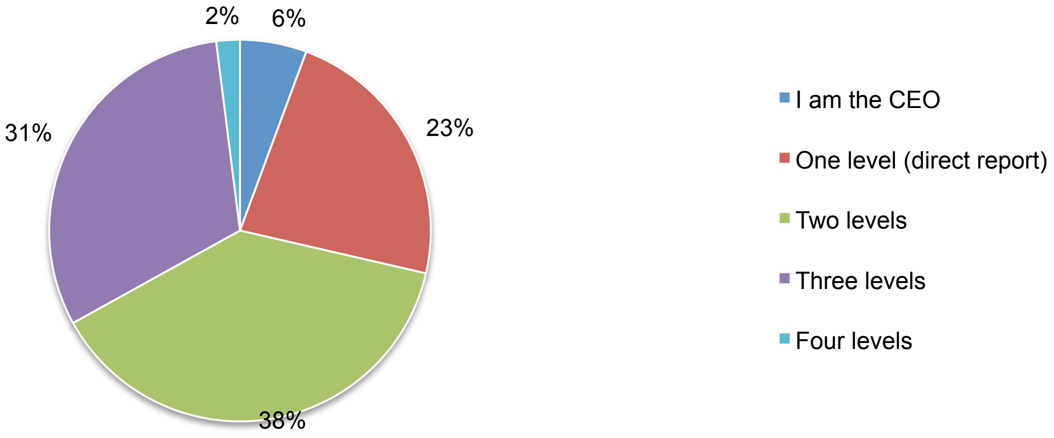
Pie Chart 1 reports the organizational level for survey participants. By design, 67 percent of respondents are at or above the senior or executive director level.

Pie Chart 1. Organizational level for current position



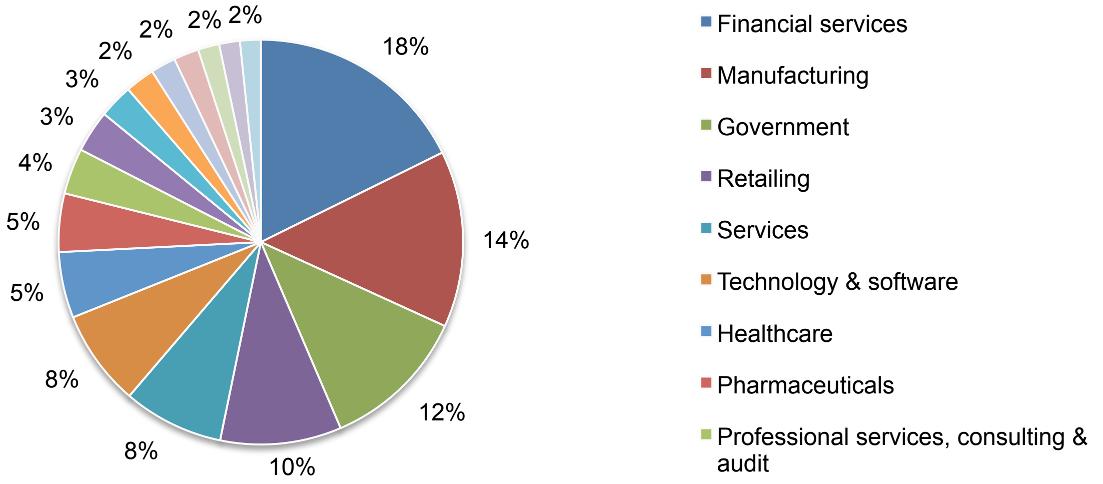
Pie Chart 2 reveals that 6 percent of respondents indicated they are the CEO, 23 percent responded they directly report to the CEO. Thirty-eight percent of respondents indicated two reporting levels to the CEO.

Pie Chart 2. Reporting layers or levels between the data protection leader and the CEO



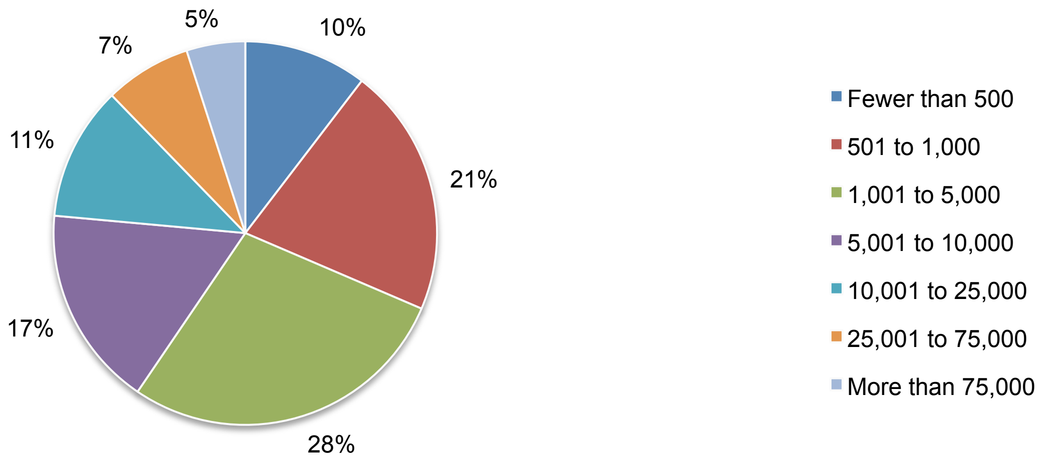
Pie Chart 3 reports the industry focus of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by manufacturing (14 percent) and government (12 percent).

Pie Chart 3. Industry distribution of respondents' organizations



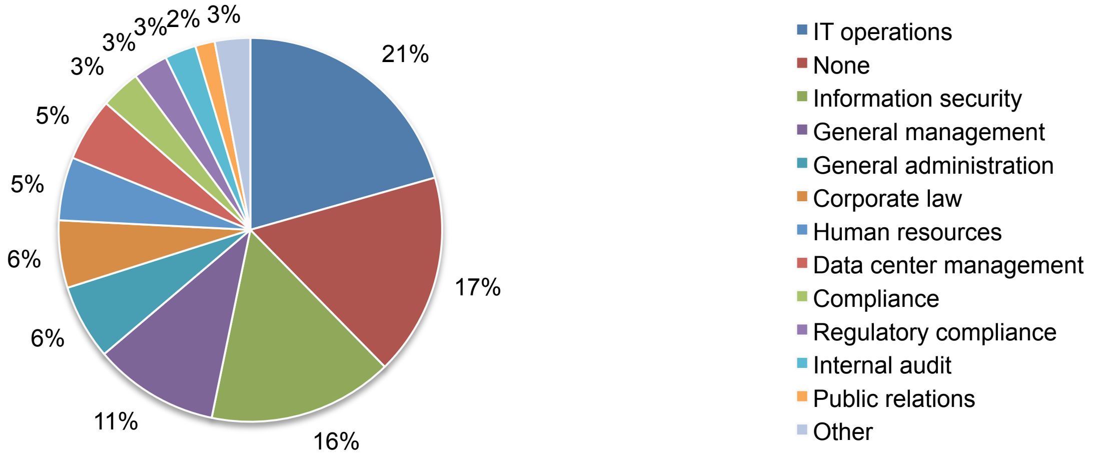
According to Pie Chart 4, more than half of the respondents (68 percent) are from organizations with a global headcount of over 1,000 employees.

Pie Chart 4. Global headcount



As shown in Pie Chart 5, 21 percent of respondents also perform job functions within IT operations, 17 percent responded they do not perform any additional job functions and 16 percent indicated they have job functions in information security.

Pie Chart 5. Other job functions performed in the organization



Part 5. Caveats

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 executives in various organizations in the United States and United Kingdom. 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 specified time period.

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 accurate responses.

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 July 2014.

Sample response	US	UK	Combined
Sampling frame	9880	5754	15634
Total returns	368	211	579
Rejected or screened surveys	46	38	84
Final sample	322	173	495
Response rate	3.3%	3.0%	3.2%

Q1. What best describes your organization's response plan for data breach incidents? Please select only one response.	US	UK	Combined
One formal plan	36%	42%	38%
Multiple formal plans	36%	29%	34%
One informal plan	17%	19%	18%
Multiple informal plans	11%	10%	11%
Total	100%	100%	100%

Q2. Please rate the maturity of your organization's data breach incident response using the 5-point scale from 1 = immature (completely reactive) to 5 = mature (completely proactive).	US	UK	Combined
Level 1	10%	11%	10%
Level 2	14%	18%	15%
Level 3	32%	29%	31%
Level 4	28%	30%	29%
Level 5	16%	12%	15%
Total	100%	100%	100%

Q3. What best describes your involvement in your organization's incident response process?	US	UK	Combined
Responsible for the process	32%	35%	33%
Accountable for the process	45%	46%	45%
Consultant to the process	11%	13%	12%
Informed about the process	49%	44%	47%
None of the above	18%	20%	19%
Total	155%	158%	156%

Q4a. In terms of lost or stolen records containing confidential or sensitive information, what constitutes a **material** data breach for your organization?	US	UK	Combined
Fewer than 10	2%	3%	2%
11 to 100	11%	9%	10%
101 to 1,000	15%	13%	14%
1,001 to 10,000	16%	15%	16%
10,001 to 100,000	31%	32%	31%
More than 100,000	25%	28%	26%
Total	100%	100%	100%
Extrapolated value	45,519	49,302	46,841

Q4b. In terms of the cost of a data breach involving confidential or sensitive information, including high value intellectual property, what constitutes a **material** data breach for your organization?	US	UK	Combined
Less than $250,000	2%	2%	2%
$250,100 to $500,000	15%	16%	15%
$500,100 to $1,000,000	43%	49%	45%
$1,000,100 to $5,000,000	29%	23%	27%
$5,000,100 to $10,000,000	8%	7%	8%
More than $10,000,000	3%	3%	3%
Total	100%	100%	100%
Extrapolated value	2,212,750	2,006,500	2,140,667

Q5. What type of security risk does your organization worry about most? Please select only one choice.	US	UK	Combined
Malicious insider	25%	25%	25%
System glitch	12%	8%	11%
Negligent insider	43%	40%	42%
Hacktivist	6%	9%	7%
Cyber syndicate	14%	18%	15%
Total	100%	100%	100%

Q6. Who is most responsible for coordinating the incident response process within your organization? Please select no more than two choices.	US	UK	Combined
Chief information officer (CIO)	49%	58%	52%
Chief security officer (CSO)	33%	24%	30%
Chief information security officer (CISO)	28%	26%	27%
Chief privacy officer (CPO)	5%	2%	4%
Chief operating officer (COO)	32%	39%	34%
Chief financial officer (CFO)	25%	20%	23%
Chief executive officer (CEO)	0%	0%	0%
Chief compliance officer (CCO)	18%	23%	20%
Other	1%	2%	1%
Not sure	9%	6%	8%
Total	200%	200%	200%

Q7. Who else in your organization's senior leadership team may be involved in coordinating the data breach incident response process? Please check all that apply.	US	UK	Combined
Chief Financial Officer	57%	52%	55%
General Counsel	89%	82%	87%
Chief Information Officer	90%	83%	88%
Chief Information Security Officer	43%	34%	40%
Compliance Leader or Officer	45%	49%	46%
Chief Marketing Officer	33%	37%	34%
Human Resources VP	26%	29%	27%
Chief Security Officer	40%	37%	39%
Chief Risk Officer	56%	48%	53%
Cross-functional committee	78%	63%	73%
Other	2%	3%	2%
Total	559%	517%	544%

Q8a. What types of information do you believe are **most critical** for your organization to secure? Please rank the following list from 1 = most critical to 6 = least critical.	US	UK	Combined
Customer or consumer information	1.2	2.6	1.7
Supplier or business partner	3.3	4.1	3.6
Employee information	4.0	3.4	3.8
Financial, business confidential information	2.5	1.7	2.2
Non-financial, business confidential information	5.1	4.6	4.9
intellectual property	5.2	3.5	4.6

Q8b. What types of information do you believe are **most difficult** for your organization to secure? Please rank the following list from 1 = most difficult to 6 = least difficult.	US	UK	Combined
Customer or consumer information	1.4	1.7	1.5
Supplier or business partner	4.2	4.2	4.2
Employee information	3.5	3.4	3.5
Financial, business confidential information	5.3	5.6	5.4
Non-financial, business confidential information	4.4	4.7	4.5
intellectual property	2.6	2.7	2.7

Q9. Does your response to incidents take into account both the value and importance of data to your organization’s business operations?	US	UK	Combined
Yes	51%	55%	52%
No	30%	23%	28%
Unsure	19%	22%	20%
Total	100%	100%	100%

Q10. How has the frequency of data breach incidents changed in the last 12 months?	US	UK	Combined
Significant increase	12%	10%	11%
Increase	35%	33%	34%
No change	36%	38%	37%
Decrease	8%	7%	8%
Significant decrease	3%	2%	3%
Cannot determine	6%	10%	7%
Total	100%	100%	100%

Q11. How prepared is your organization to deal with data breaches? Please rate your organization’s level of readiness using the 10-point readiness scale provided below.	US	UK	Combined
1 or 2 (low)	5%	3%	4%
3 or 4	18%	16%	17%
5 or 6	33%	33%	33%
7 or 8	30%	32%	31%
9 or 10 (high)	14%	16%	15%
Total	100%	100%	100%
Extrapolated value	6.10	6.34	6.18

How important is executive-level involvement in your organization's incident response process? Essential and Very Important combined response	US	UK	Combined
Q12a. Protecting the organization's reputation and brand	65%	69%	66%
Q12b. Minimizing financial loss to the organization	71%	74%	72%
Q12c. Avoiding regulatory actions, fines and lawsuits	59%	60%	59%
Q12d. Maintaining operational efficiencies	53%	50%	52%
Q12e. Ensuring high availability of enterprise systems and networks	62%	55%	60%

Q13. Please select the functional areas that participate in your organization's incident response planning process? Please select all that apply.	US	UK	Combined
CEO & board of directors	44%	52%	47%
Compliance	73%	65%	70%
Finance & accounting	50%	61%	54%
Government or public affairs	46%	35%	42%
Human resources	57%	52%	55%
Information security	55%	56%	55%
Information technology	69%	72%	70%
Internal audit	39%	43%	40%
Legal	86%	82%	85%
Logistics	21%	25%	22%
Marketing & communications	24%	19%	22%
Privacy office	28%	19%	25%
Procurement	32%	25%	30%
Public relations	58%	45%	53%
Records management	16%	17%	16%
Risk management	23%	25%	24%
Sales	8%	11%	9%
Security	24%	26%	25%
Total	753%	730%	745%

Following are typical data breach incident response activities. Please rate the importance of each activity based on its criticality to the planning and execution of the response process. Essential and Very Important combined response.	US	UK	Combined
Q14a. Training and awareness for employees	80%	82%	81%
Q14b. Conducting forensic investigations	89%	79%	86%
Q14c. Consulting with law enforcement	65%	68%	66%
Q14d. Reporting to regulators	38%	33%	36%
Q14e. Notifying data breach victims	69%	68%	69%
Q14f. Responding to data breach victims' concerns (as one example, redress mechanism)	44%	40%	43%
Q14g. Determining the economic impact of the incident	37%	32%	35%
Q14h. Minimizing disruption to IT operations	68%	55%	63%
Q14i. Minimizing disruption to business processes	68%	72%	69%
Q14j. Communicating with external parties (such as media or advocates)	41%	44%	42%
Q14k. Reporting to the CEO and board of directors	78%	83%	80%
Q14l. Conducting fire drills and/or war games to assess readiness	75%	80%	77%
Q14m. Conducting post mortem analysis of the data breach incident	49%	51%	50%

The following statements pertain to executive or board level involvement in the incident response process. Please rate each statement using the scale provided below the item. Strongly Agree and Agree response combined.	US	UK	Combined
Q15a. Executive level involvement is necessary to achieving an effective incident response to data breaches	80%	78%	79%
Q15b. Board level oversight is necessary to achieving an effective incident response to data breaches	69%	73%	70%
Q15c. Too much involvement and oversight by executives and board members complicates the planning and execution of the incident response process	18%	19%	18%

Q16. What measures does your organization use to determine the effectiveness of the incident response process? Please select all that apply.	US	UK	Combined
Time to discover the incident	50%	51%	50%
Time to contain the incident	66%	68%	67%
Minimize data breach costs	71%	73%	72%
Minimize impact on share value	34%	32%	33%
Time to notify breach victims	42%	40%	41%
Minimize customer churn	18%	19%	18%
Ensure compliance with laws and regulations	58%	47%	54%
Minimize negative media coverage	52%	48%	51%
Minimize disruption to business processes	63%	65%	64%
Ensure high availability (minimal downtime)	60%	62%	61%
None of the above	12%	8%	11%
Total	526%	513%	521%

Q17. Using the following 10-point scale, please rate your organization’s ability to mitigate or curtail the negative impact of data breach incidents.	US	UK	Combined
1 or 2 (low)	6%	4%	5%
3 or 4	21%	19%	20%
5 or 6	33%	38%	35%
7 or 8	28%	29%	28%
9 or 10 (high)	12%	10%	11%
Total	100%	100%	100%
Extrapolated value	5.88	5.94	5.90

Q18. What are the main barriers to responding effectively to data breaches? Please select all that apply.	US	UK	Combined
Insufficient resources and technologies	30%	27%	29%
Lack of in-house expertise	28%	23%	26%
Lack of executive-level involvement	29%	18%	25%
Lack of board oversight	60%	55%	58%
Lack of leadership	69%	66%	68%
Poor communications	72%	65%	70%
Inability to measure effectiveness of response	55%	51%	54%
Decentralized governance of data protection	49%	38%	45%
Organizational silos or lack of cooperation	50%	56%	52%
Other	2%	3%	2%
Total	444%	402%	429%

Q19. What should be on the agenda of your organization's board of directors with respect to incident response planning and governance? Please select all that apply.	US	UK	Combined
Evaluating the security function	61%	63%	62%
Evaluating the job performance of the CISO	44%	42%	43%
Evaluating investments in security technologies	54%	57%	55%
Approving the incident response plan	68%	70%	69%
Reviewing risk assessments	76%	79%	77%
Reviewing status of data breach incident investigations	73%	62%	69%
Approving privacy and data protection policies	28%	34%	30%
Evaluating results of fire drills and other readiness tests	23%	35%	27%
Receiving regulatory and compliance updates	68%	69%	68%
Approving insurance coverage	68%	63%	66%
Other	3%	2%	3%
Total	566%	576%	569%

Q20. In your opinion, why are data breach incidents not on the board's agenda? Please select the top two reasons.	US	UK	Combined
Director's legal liability	24%	10%	19%
Director's lack of technical understanding	49%	45%	48%
Complicates incident response planning	14%	23%	17%
Hampers incident response execution	55%	59%	56%
Does not require board-level governance	58%	63%	60%
Other	0%	0%	0%
Total	200%	200%	200%

Q21a. Has your organization's board of directors complained about the difficulty in understanding briefings and reports about data breach response?	US	UK	Combined
Yes	28%	25%	27%
No	60%	62%	61%
Unsure	12%	13%	12%
Total	100%	100%	100%

Q21b. If yes, what are you doing to better articulate the state of data breach planning response in your organization? Please select all that apply.	US	UK	Combined
Ensure reports and briefings are not overly technical	56%	51%	54%
Engage experts to inform and educate the board about the issues	69%	63%	67%
Keep reports and briefings to the minimum	37%	40%	38%
Report only those risks and threats that would have the greatest impact on the organization	49%	52%	50%
Schedule briefings only when threats to the organization are imminent	24%	26%	25%
Nothing is being done	18%	16%	17%
Other	2%	4%	3%
Total	255%	252%	254%

Your position and other organizational characteristics

D1. What organizational level best describes your current position?	US	UK	Combined
Chief executive	6%	5%	6%
Senior vice president	23%	21%	22%
Vice president	15%	16%	15%
Senior or executive director	23%	24%	23%
Director	31%	29%	30%
Manager	2%	5%	3%
Other	0%	0%	0%
Total	100%	100%	100%

D2. In your organization, how many reporting layers or levels are there between the data protection leader and the CEO (or highest ranking executive)?	US	UK	Combined
I am the CEO	6%	5%	6%
One level (direct report)	24%	21%	23%
Two levels	38%	39%	38%
Three levels	30%	33%	31%
Four levels	2%	2%	2%
Five or more levels	0%	0%	0%
Total	100%	100%	100%

D3. Please select the range that best describes the global headcount (size) of your organization	US	UK	Combined
Fewer than 500	9%	13%	10%
501 to 1,000	20%	23%	21%
1,001 to 5,000	27%	30%	28%
5,001 to 10,000	18%	15%	17%
10,001 to 25,000	12%	10%	11%
25,001 to 75,000	8%	6%	7%
More than 75,000	6%	3%	5%
Total	100%	100%	100%

D4. What other job functions do you perform in your organization? Please check all that apply:	US	UK	Combined
Compliance	3%	4%	3%
Corporate law	5%	7%	6%
Corporate marketing and CRM	2%	0%	1%
Consulting	0%	0%	0%
General administration	6%	7%	6%
General management	12%	8%	11%
Governmental relations	1%	0%	1%
Human resources	5%	6%	5%
Information security	16%	15%	16%
IT operations	20%	22%	21%
Internal audit	3%	2%	3%
Physical security	0%	0%	0%
Public relations	2%	1%	2%
Research	0%	0%	0%
Regulatory compliance	4%	1%	3%
Records management	0%	0%	0%
Software development	1%	0%	1%
Data center management	5%	6%	5%
None	15%	21%	17%
Total	100%	100%	100%

D5. What is the industry or business group that best defines your organization? If your organization contains multiple industry sectors or sub-checks, please check all that apply (or write-in the space for other).	US	UK	Combined
Consumer products	1%	3%	2%
Education	2%	1%	2%
Energy	3%	4%	3%
Financial services	18%	17%	18%
Government	11%	13%	12%
Healthcare	7%	2%	5%
Hospitality & leisure	2%	2%	2%
Internet services	2%	1%	2%
Pharmaceuticals	5%	4%	5%
Professional services, consulting & audit	4%	3%	4%
Professional services, legal	2%	4%	3%
Manufacturing	13%	16%	14%
Retailing	10%	9%	10%
Services	8%	8%	8%
Telecom, cable & wireless	2%	3%	2%
Technology & software	8%	7%	8%
Transportation	2%	2%	2%
Other	0%	1%	0%
Total	100%	100%	100%

D6. Is your company publicly traded?	US	UK	Combined
Yes	44%	41%	43%
No	56%	59%	57%
Total	100%	100%	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.