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

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
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

- Executive level involvement is necessary to achieving an effective incident response to data breaches: 79%
- Board level oversight is necessary to achieving an effective incident response to data breaches: 70%
- Too much involvement and oversight by executives and board members complicates the planning and execution of the incident response process: 18%
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

<table>
<thead>
<tr>
<th>Informed about the process</th>
<th>47%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable for the process</td>
<td>45%</td>
</tr>
<tr>
<td>Responsible for the process</td>
<td>33%</td>
</tr>
<tr>
<td>None of the above</td>
<td>19%</td>
</tr>
<tr>
<td>Consultant to the process</td>
<td>12%</td>
</tr>
</tbody>
</table>

**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

- Minimizing financial loss to the organization: 72%
- Protecting the organization’s reputation and brand: 66%
- Ensuring high availability of enterprise systems and networks: 60%
- Avoiding regulatory actions, fines and lawsuits: 59%
- Maintaining operational efficiencies: 52%
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

- Does not require board-level governance: 60%
- Hampers incident response execution: 56%
- Director’s lack of technical understanding: 48%
- Director’s legal liability: 19%
- Complicates incident response planning: 17%
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

- Engage experts to inform and educate the board about the issues: 67%
- Ensure reports and briefings are not overly technical: 54%
- Report only those risks and threats that would have the greatest impact on the organization: 50%
- Keep reports and briefings to the minimum: 38%
- Schedule briefings only when threats to the organization are imminent: 25%
- Nothing is being done: 17%
- Other: 3%
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

- Poor communications: 70%
- Lack of leadership: 68%
- Lack of board oversight: 58%
- Inability to measure effectiveness of response: 54%
- Organizational silos or lack of cooperation: 52%
- Decentralized governance of data protection: 45%
- Insufficient resources and technologies: 29%
- Lack of in-house expertise: 26%
- Lack of executive-level involvement: 25%
- Other: 2%
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

- Minimize data breach costs: 72%
- Time to contain the incident: 67%
- Minimize disruption to business processes: 64%
- Ensure high availability: 61%
- Ensure compliance with laws and regulations: 54%
- Minimize negative media coverage: 51%
- Time to discover the incident: 50%
- Time to notify breach victims: 41%
- Minimize impact on share value: 33%
- Minimize customer churn: 18%
- None of the above: 11%
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

<table>
<thead>
<tr>
<th>Security Risk</th>
<th>Concerns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligent insider</td>
<td>42%</td>
</tr>
<tr>
<td>Malicious insider</td>
<td>25%</td>
</tr>
<tr>
<td>Cyber syndicate</td>
<td>15%</td>
</tr>
<tr>
<td>System glitch</td>
<td>11%</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>7%</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief information officer (CIO)</td>
<td>52%</td>
</tr>
<tr>
<td>Chief operating officer (COO)</td>
<td>34%</td>
</tr>
<tr>
<td>Chief security officer (CSO)</td>
<td>30%</td>
</tr>
<tr>
<td>Chief information security officer (CISO)</td>
<td>27%</td>
</tr>
<tr>
<td>Chief financial officer (CFO)</td>
<td>23%</td>
</tr>
<tr>
<td>Chief compliance officer (CCO)</td>
<td>20%</td>
</tr>
<tr>
<td>Chief privacy officer (CPO)</td>
<td>4%</td>
</tr>
<tr>
<td>Not sure</td>
<td>8%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Information</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer or consumer information</td>
<td>5.3</td>
</tr>
<tr>
<td>Financial, business confidential information</td>
<td>4.8</td>
</tr>
<tr>
<td>Supplier or business partner</td>
<td>3.4</td>
</tr>
<tr>
<td>Employee information</td>
<td>3.2</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>2.4</td>
</tr>
<tr>
<td>Non-financial, business confidential information</td>
<td>2.1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Information</th>
<th>Difficulty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer or consumer information</td>
<td>5.5</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>4.3</td>
</tr>
<tr>
<td>Employee information</td>
<td>3.5</td>
</tr>
<tr>
<td>Supplier or business partner</td>
<td>2.8</td>
</tr>
<tr>
<td>Non-financial, business confidential information</td>
<td>2.5</td>
</tr>
<tr>
<td>Financial, business confidential information</td>
<td>1.6</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Essential and very important response combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conducting forensic investigations</td>
<td>86%</td>
</tr>
<tr>
<td>Training and awareness for employees</td>
<td>81%</td>
</tr>
<tr>
<td>Reporting to the CEO and board of directors</td>
<td>80%</td>
</tr>
<tr>
<td>Conducting fire drills and/or war games to assess readiness</td>
<td>77%</td>
</tr>
<tr>
<td>Minimizing disruption to business processes</td>
<td>69%</td>
</tr>
<tr>
<td>Notifying data breach victims</td>
<td>69%</td>
</tr>
<tr>
<td>Consulting with law enforcement</td>
<td>66%</td>
</tr>
<tr>
<td>Minimizing disruption to IT operations</td>
<td>63%</td>
</tr>
<tr>
<td>Conducting post mortem analysis of the data breach incident</td>
<td>50%</td>
</tr>
</tbody>
</table>

0% 10% 20% 30% 40% 50% 60% 70% 80% 90%
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>
<thead>
<tr>
<th>Table 1. Sample response</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling frame</td>
<td>9880</td>
<td>5754</td>
<td>15634</td>
</tr>
<tr>
<td>Total returns</td>
<td>368</td>
<td>211</td>
<td>579</td>
</tr>
<tr>
<td>Rejected or screened</td>
<td>46</td>
<td>38</td>
<td>84</td>
</tr>
<tr>
<td>surveys</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final sample</td>
<td>322</td>
<td>173</td>
<td>495</td>
</tr>
<tr>
<td>Response rate</td>
<td>3.3%</td>
<td>3.0%</td>
<td>3.2%</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Sample response</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling frame</td>
<td>9880</td>
<td>5754</td>
<td>15634</td>
</tr>
<tr>
<td>Total returns</td>
<td>368</td>
<td>211</td>
<td>579</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>46</td>
<td>38</td>
<td>84</td>
</tr>
<tr>
<td>Final sample</td>
<td>322</td>
<td>173</td>
<td>495</td>
</tr>
<tr>
<td>Response rate</td>
<td>3.3%</td>
<td>3.0%</td>
<td>3.2%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q1. What best describes your organization’s response plan for data breach incidents? Please select only one response.</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>One formal plan</td>
<td>36%</td>
<td>42%</td>
<td>38%</td>
</tr>
<tr>
<td>Multiple formal plans</td>
<td>36%</td>
<td>29%</td>
<td>34%</td>
</tr>
<tr>
<td>One informal plan</td>
<td>17%</td>
<td>19%</td>
<td>18%</td>
</tr>
<tr>
<td>Multiple informal plans</td>
<td>11%</td>
<td>10%</td>
<td>11%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>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).</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>10%</td>
<td>11%</td>
<td>10%</td>
</tr>
<tr>
<td>Level 2</td>
<td>14%</td>
<td>18%</td>
<td>15%</td>
</tr>
<tr>
<td>Level 3</td>
<td>32%</td>
<td>29%</td>
<td>31%</td>
</tr>
<tr>
<td>Level 4</td>
<td>28%</td>
<td>30%</td>
<td>29%</td>
</tr>
<tr>
<td>Level 5</td>
<td>16%</td>
<td>12%</td>
<td>15%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Cost Range</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than $250,000</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>$250,100 to $500,000</td>
<td>15%</td>
<td>16%</td>
<td>15%</td>
</tr>
<tr>
<td>$500,100 to $1,000,000</td>
<td>43%</td>
<td>49%</td>
<td>45%</td>
</tr>
<tr>
<td>$1,000,100 to $5,000,000</td>
<td>29%</td>
<td>23%</td>
<td>27%</td>
</tr>
<tr>
<td>$5,000,100 to $10,000,000</td>
<td>8%</td>
<td>7%</td>
<td>8%</td>
</tr>
<tr>
<td>More than $10,000,000</td>
<td>3%</td>
<td>3%</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Extrapulated value</td>
<td>2,212,750</td>
<td>2,006,500</td>
<td>2,140,667</td>
</tr>
</tbody>
</table>

Q5. What type of security risk does your organization worry about most? Please select only one choice.

<table>
<thead>
<tr>
<th>Risk Type</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious insider</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>System glitch</td>
<td>12%</td>
<td>8%</td>
<td>11%</td>
</tr>
<tr>
<td>Negligent insider</td>
<td>43%</td>
<td>40%</td>
<td>42%</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>6%</td>
<td>9%</td>
<td>7%</td>
</tr>
<tr>
<td>Cyber syndicate</td>
<td>14%</td>
<td>18%</td>
<td>15%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q6. Who is most responsible for coordinating the incident response process within your organization? Please select no more than two choices.

<table>
<thead>
<tr>
<th>Responsible</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief information officer (CIO)</td>
<td>49%</td>
<td>58%</td>
<td>52%</td>
</tr>
<tr>
<td>Chief security officer (CSO)</td>
<td>33%</td>
<td>24%</td>
<td>30%</td>
</tr>
<tr>
<td>Chief information security officer (CISO)</td>
<td>28%</td>
<td>26%</td>
<td>27%</td>
</tr>
<tr>
<td>Chief privacy officer (CPO)</td>
<td>5%</td>
<td>2%</td>
<td>4%</td>
</tr>
<tr>
<td>Chief operating officer (COO)</td>
<td>32%</td>
<td>39%</td>
<td>34%</td>
</tr>
<tr>
<td>Chief financial officer (CFO)</td>
<td>25%</td>
<td>20%</td>
<td>23%</td>
</tr>
<tr>
<td>Chief executive officer (CEO)</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Chief compliance officer (CCO)</td>
<td>18%</td>
<td>23%</td>
<td>20%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
<td>2%</td>
<td>1%</td>
</tr>
<tr>
<td>Not sure</td>
<td>9%</td>
<td>6%</td>
<td>8%</td>
</tr>
<tr>
<td>Total</td>
<td>200%</td>
<td>200%</td>
<td>200%</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Role</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Financial Officer</td>
<td>57%</td>
<td>52%</td>
<td>55%</td>
</tr>
<tr>
<td>General Counsel</td>
<td>89%</td>
<td>82%</td>
<td>87%</td>
</tr>
<tr>
<td>Chief Information Officer</td>
<td>90%</td>
<td>83%</td>
<td>88%</td>
</tr>
<tr>
<td>Chief Information Security Officer</td>
<td>43%</td>
<td>34%</td>
<td>40%</td>
</tr>
<tr>
<td>Compliance Leader or Officer</td>
<td>45%</td>
<td>49%</td>
<td>46%</td>
</tr>
<tr>
<td>Chief Marketing Officer</td>
<td>33%</td>
<td>37%</td>
<td>34%</td>
</tr>
<tr>
<td>Human Resources VP</td>
<td>26%</td>
<td>29%</td>
<td>27%</td>
</tr>
<tr>
<td>Chief Security Officer</td>
<td>40%</td>
<td>37%</td>
<td>39%</td>
</tr>
<tr>
<td>Chief Risk Officer</td>
<td>56%</td>
<td>48%</td>
<td>53%</td>
</tr>
<tr>
<td>Cross-functional committee</td>
<td>78%</td>
<td>63%</td>
<td>73%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>559%</td>
<td>517%</td>
<td>544%</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Information Type</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer or consumer information</td>
<td>1.2</td>
<td>2.6</td>
<td>1.7</td>
</tr>
<tr>
<td>Supplier or business partner</td>
<td>3.3</td>
<td>4.1</td>
<td>3.6</td>
</tr>
<tr>
<td>Employee information</td>
<td>4.0</td>
<td>3.4</td>
<td>3.8</td>
</tr>
<tr>
<td>Financial, business confidential information</td>
<td>2.5</td>
<td>1.7</td>
<td>2.2</td>
</tr>
<tr>
<td>Non-financial, business confidential information</td>
<td>5.1</td>
<td>4.6</td>
<td>4.9</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>5.2</td>
<td>3.5</td>
<td>4.6</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Information Type</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer or consumer information</td>
<td>1.4</td>
<td>1.7</td>
<td>1.5</td>
</tr>
<tr>
<td>Supplier or business partner</td>
<td>4.2</td>
<td>4.2</td>
<td>4.2</td>
</tr>
<tr>
<td>Employee information</td>
<td>3.5</td>
<td>3.4</td>
<td>3.5</td>
</tr>
<tr>
<td>Financial, business confidential information</td>
<td>5.3</td>
<td>5.6</td>
<td>5.4</td>
</tr>
<tr>
<td>Non-financial, business confidential information</td>
<td>4.4</td>
<td>4.7</td>
<td>4.5</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>2.6</td>
<td>2.7</td>
<td>2.7</td>
</tr>
</tbody>
</table>

Q9. Does your response to incidents take into account both the value and importance of data to your organization’s business operations?

<table>
<thead>
<tr>
<th>Response</th>
<th>US (%)</th>
<th>UK (%)</th>
<th>Combined (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>51</td>
<td>55</td>
<td>52</td>
</tr>
<tr>
<td>No</td>
<td>30</td>
<td>23</td>
<td>28</td>
</tr>
<tr>
<td>Unsure</td>
<td>19</td>
<td>22</td>
<td>20</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

Q10. How has the frequency of data breach incidents changed in the last 12 months?

<table>
<thead>
<tr>
<th>Change</th>
<th>US (%)</th>
<th>UK (%)</th>
<th>Combined (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant increase</td>
<td>12</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>Increase</td>
<td>35</td>
<td>33</td>
<td>34</td>
</tr>
<tr>
<td>No change</td>
<td>36</td>
<td>38</td>
<td>37</td>
</tr>
<tr>
<td>Decrease</td>
<td>8</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>Significant decrease</td>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Cannot determine</td>
<td>6</td>
<td>10</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Readiness Level</th>
<th>US (%)</th>
<th>UK (%)</th>
<th>Combined (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2 (low)</td>
<td>5</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>3 or 4</td>
<td>18</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>5 or 6</td>
<td>33</td>
<td>33</td>
<td>33</td>
</tr>
<tr>
<td>7 or 8</td>
<td>30</td>
<td>32</td>
<td>31</td>
</tr>
<tr>
<td>9 or 10 (high)</td>
<td>14</td>
<td>16</td>
<td>15</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Q12a. Protecting the organization’s reputation and brand</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>65%</td>
<td>69%</td>
<td>66%</td>
<td></td>
</tr>
<tr>
<td>Q12b. Minimizing financial loss to the organization</td>
<td>71%</td>
<td>74%</td>
<td>72%</td>
</tr>
<tr>
<td>Q12c. Avoiding regulatory actions, fines and lawsuits</td>
<td>59%</td>
<td>60%</td>
<td>59%</td>
</tr>
<tr>
<td>Q12d. Maintaining operational efficiencies</td>
<td>53%</td>
<td>50%</td>
<td>52%</td>
</tr>
<tr>
<td>Q12e. Ensuring high availability of enterprise systems and networks</td>
<td>62%</td>
<td>55%</td>
<td>60%</td>
</tr>
</tbody>
</table>

Q13. Please select the functional areas that participate in your organization’s incident response planning process? Please select all that apply.

<table>
<thead>
<tr>
<th></th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO &amp; board of directors</td>
<td>44%</td>
<td>52%</td>
<td>47%</td>
</tr>
<tr>
<td>Compliance</td>
<td>73%</td>
<td>65%</td>
<td>70%</td>
</tr>
<tr>
<td>Finance &amp; accounting</td>
<td>50%</td>
<td>61%</td>
<td>54%</td>
</tr>
<tr>
<td>Government or public affairs</td>
<td>46%</td>
<td>35%</td>
<td>42%</td>
</tr>
<tr>
<td>Human resources</td>
<td>57%</td>
<td>52%</td>
<td>55%</td>
</tr>
<tr>
<td>Information security</td>
<td>55%</td>
<td>56%</td>
<td>55%</td>
</tr>
<tr>
<td>Information technology</td>
<td>69%</td>
<td>72%</td>
<td>70%</td>
</tr>
<tr>
<td>Internal audit</td>
<td>39%</td>
<td>43%</td>
<td>40%</td>
</tr>
<tr>
<td>Legal</td>
<td>86%</td>
<td>82%</td>
<td>85%</td>
</tr>
<tr>
<td>Logistics</td>
<td>21%</td>
<td>25%</td>
<td>22%</td>
</tr>
<tr>
<td>Marketing &amp; communications</td>
<td>24%</td>
<td>19%</td>
<td>22%</td>
</tr>
<tr>
<td>Privacy office</td>
<td>28%</td>
<td>19%</td>
<td>25%</td>
</tr>
<tr>
<td>Procurement</td>
<td>32%</td>
<td>25%</td>
<td>30%</td>
</tr>
<tr>
<td>Public relations</td>
<td>58%</td>
<td>45%</td>
<td>53%</td>
</tr>
<tr>
<td>Records management</td>
<td>16%</td>
<td>17%</td>
<td>16%</td>
</tr>
<tr>
<td>Risk management</td>
<td>23%</td>
<td>25%</td>
<td>24%</td>
</tr>
<tr>
<td>Sales</td>
<td>8%</td>
<td>11%</td>
<td>9%</td>
</tr>
<tr>
<td>Security</td>
<td>24%</td>
<td>26%</td>
<td>25%</td>
</tr>
<tr>
<td>Total</td>
<td>753%</td>
<td>730%</td>
<td>745%</td>
</tr>
</tbody>
</table>

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.

| Q14a. Training and awareness for employees | US  | UK  | Combined |
| 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.

<table>
<thead>
<tr>
<th>Statement</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q15a. Executive level involvement is necessary to achieving an effective incident response to data breaches</td>
<td>80%</td>
<td>78%</td>
<td>79%</td>
</tr>
<tr>
<td>Q15b. Board level oversight is necessary to achieving an effective incident response to data breaches</td>
<td>69%</td>
<td>73%</td>
<td>70%</td>
</tr>
<tr>
<td>Q15c. Too much involvement and oversight by executives and board members complicates the planning and execution of the incident response process</td>
<td>18%</td>
<td>19%</td>
<td>18%</td>
</tr>
</tbody>
</table>

Q16. What measures does your organization use to determine the effectiveness of the incident response process? Please select all that apply.

<table>
<thead>
<tr>
<th>Measure</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to discover the incident</td>
<td>50%</td>
<td>51%</td>
<td>50%</td>
</tr>
<tr>
<td>Time to contain the incident</td>
<td>66%</td>
<td>68%</td>
<td>67%</td>
</tr>
<tr>
<td>Minimize data breach costs</td>
<td>71%</td>
<td>73%</td>
<td>72%</td>
</tr>
<tr>
<td>Minimize impact on share value</td>
<td>34%</td>
<td>32%</td>
<td>33%</td>
</tr>
<tr>
<td>Time to notify breach victims</td>
<td>42%</td>
<td>40%</td>
<td>41%</td>
</tr>
<tr>
<td>Minimize customer churn</td>
<td>18%</td>
<td>19%</td>
<td>18%</td>
</tr>
<tr>
<td>Ensure compliance with laws and regulations</td>
<td>58%</td>
<td>47%</td>
<td>54%</td>
</tr>
<tr>
<td>Minimize negative media coverage</td>
<td>52%</td>
<td>48%</td>
<td>51%</td>
</tr>
<tr>
<td>Minimize disruption to business processes</td>
<td>63%</td>
<td>65%</td>
<td>64%</td>
</tr>
<tr>
<td>Ensure high availability (minimal downtime)</td>
<td>60%</td>
<td>62%</td>
<td>61%</td>
</tr>
<tr>
<td>None of the above</td>
<td>12%</td>
<td>8%</td>
<td>11%</td>
</tr>
<tr>
<td>Total</td>
<td>526%</td>
<td>513%</td>
<td>521%</td>
</tr>
</tbody>
</table>

Q17. Using the following 10-point scale, please rate your organization’s ability to mitigate or curtail the negative impact of data breach incidents.

<table>
<thead>
<tr>
<th>Scale</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2 (low)</td>
<td>6%</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>21%</td>
<td>19%</td>
<td>20%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>33%</td>
<td>38%</td>
<td>35%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>28%</td>
<td>29%</td>
<td>28%</td>
</tr>
<tr>
<td>9 or 10 (high)</td>
<td>12%</td>
<td>10%</td>
<td>11%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Extrapolated value</td>
<td>5.88</td>
<td>5.94</td>
<td>5.90</td>
</tr>
</tbody>
</table>

Q18. What are the main barriers to responding effectively to data breaches? Please select all that apply.

<table>
<thead>
<tr>
<th>Barrier</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient resources and technologies</td>
<td>30%</td>
<td>27%</td>
<td>29%</td>
</tr>
<tr>
<td>Lack of in-house expertise</td>
<td>28%</td>
<td>23%</td>
<td>26%</td>
</tr>
<tr>
<td>Lack of executive-level involvement</td>
<td>29%</td>
<td>18%</td>
<td>25%</td>
</tr>
<tr>
<td>Lack of board oversight</td>
<td>60%</td>
<td>55%</td>
<td>58%</td>
</tr>
<tr>
<td>Lack of leadership</td>
<td>69%</td>
<td>66%</td>
<td>68%</td>
</tr>
<tr>
<td>Poor communications</td>
<td>72%</td>
<td>65%</td>
<td>70%</td>
</tr>
<tr>
<td>Inability to measure effectiveness of response</td>
<td>55%</td>
<td>51%</td>
<td>54%</td>
</tr>
<tr>
<td>Decentralized governance of data protection</td>
<td>49%</td>
<td>38%</td>
<td>45%</td>
</tr>
<tr>
<td>Organizational silos or lack of cooperation</td>
<td>50%</td>
<td>56%</td>
<td>52%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>444%</td>
<td>402%</td>
<td>429%</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th></th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluating the security function</td>
<td>61%</td>
<td>63%</td>
<td>62%</td>
</tr>
<tr>
<td>Evaluating the job performance of the CISO</td>
<td>44%</td>
<td>42%</td>
<td>43%</td>
</tr>
<tr>
<td>Evaluating investments in security technologies</td>
<td>54%</td>
<td>57%</td>
<td>55%</td>
</tr>
<tr>
<td>Approving the incident response plan</td>
<td>68%</td>
<td>70%</td>
<td>69%</td>
</tr>
<tr>
<td>Reviewing risk assessments</td>
<td>76%</td>
<td>79%</td>
<td>77%</td>
</tr>
<tr>
<td>Reviewing status of data breach incident investigations</td>
<td>73%</td>
<td>62%</td>
<td>69%</td>
</tr>
<tr>
<td>Approving privacy and data protection policies</td>
<td>28%</td>
<td>34%</td>
<td>30%</td>
</tr>
<tr>
<td>Evaluating results of fire drills and other readiness tests</td>
<td>23%</td>
<td>35%</td>
<td>27%</td>
</tr>
<tr>
<td>Receiving regulatory and compliance updates</td>
<td>68%</td>
<td>69%</td>
<td>68%</td>
</tr>
<tr>
<td>Approving insurance coverage</td>
<td>68%</td>
<td>63%</td>
<td>66%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
<td>2%</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>566%</td>
<td>576%</td>
<td>569%</td>
</tr>
</tbody>
</table>

Q20. In your opinion, why are data breach incidents not on the board’s agenda? Please select the top two reasons.

<table>
<thead>
<tr>
<th></th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Director’s legal liability</td>
<td>24%</td>
<td>10%</td>
<td>19%</td>
</tr>
<tr>
<td>Director’s lack of technical understa</td>
<td>49%</td>
<td>45%</td>
<td>48%</td>
</tr>
<tr>
<td>Complicates incident response planning</td>
<td>14%</td>
<td>23%</td>
<td>17%</td>
</tr>
<tr>
<td>Hampers incident response execution</td>
<td>55%</td>
<td>59%</td>
<td>56%</td>
</tr>
<tr>
<td>Does not require board-level governance</td>
<td>58%</td>
<td>63%</td>
<td>60%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>200%</td>
<td>200%</td>
<td>200%</td>
</tr>
</tbody>
</table>

Q21a. Has your organization’s board of directors complained about the difficulty in understanding briefings and reports about data breach response?

<table>
<thead>
<tr>
<th></th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>28%</td>
<td>25%</td>
<td>27%</td>
</tr>
<tr>
<td>No</td>
<td>60%</td>
<td>62%</td>
<td>61%</td>
</tr>
<tr>
<td>Unsure</td>
<td>12%</td>
<td>13%</td>
<td>12%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th></th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure reports and briefings are not overly technical</td>
<td>56%</td>
<td>51%</td>
<td>54%</td>
</tr>
<tr>
<td>Engage experts to inform and educate the board about the issues</td>
<td>69%</td>
<td>63%</td>
<td>67%</td>
</tr>
<tr>
<td>Keep reports and briefings to the minimum</td>
<td>37%</td>
<td>40%</td>
<td>38%</td>
</tr>
<tr>
<td>Report only those risks and threats that would have the greatest impact on the organization</td>
<td>49%</td>
<td>52%</td>
<td>50%</td>
</tr>
<tr>
<td>Schedule briefings only when threats to the organization are imminent</td>
<td>24%</td>
<td>26%</td>
<td>25%</td>
</tr>
<tr>
<td>Nothing is being done</td>
<td>18%</td>
<td>16%</td>
<td>17%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
<td>4%</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>255%</td>
<td>252%</td>
<td>254%</td>
</tr>
</tbody>
</table>
### Your position and other organizational characteristics

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

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

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

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

<table>
<thead>
<tr>
<th>Industry or Business Group</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer products</td>
<td>1%</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Education</td>
<td>2%</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>Energy</td>
<td>3%</td>
<td>4%</td>
<td>3%</td>
</tr>
<tr>
<td>Financial services</td>
<td>18%</td>
<td>17%</td>
<td>18%</td>
</tr>
<tr>
<td>Government</td>
<td>11%</td>
<td>13%</td>
<td>12%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>7%</td>
<td>2%</td>
<td>5%</td>
</tr>
<tr>
<td>Hospitality &amp; leisure</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>Internet services</td>
<td>2%</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>Pharmaceuticals</td>
<td>5%</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>Professional services, consulting &amp; audit</td>
<td>4%</td>
<td>3%</td>
<td>4%</td>
</tr>
<tr>
<td>Professional services, legal</td>
<td>2%</td>
<td>4%</td>
<td>3%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>13%</td>
<td>16%</td>
<td>14%</td>
</tr>
<tr>
<td>Retailing</td>
<td>10%</td>
<td>9%</td>
<td>10%</td>
</tr>
<tr>
<td>Services</td>
<td>8%</td>
<td>8%</td>
<td>8%</td>
</tr>
<tr>
<td>Telecom, cable &amp; wireless</td>
<td>2%</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Technology &amp; software</td>
<td>8%</td>
<td>7%</td>
<td>8%</td>
</tr>
<tr>
<td>Transportation</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

## D6. Is your company publicly traded?

<table>
<thead>
<tr>
<th>Publicly Traded</th>
<th>US</th>
<th>UK</th>
<th>Combined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>44%</td>
<td>41%</td>
<td>43%</td>
</tr>
<tr>
<td>No</td>
<td>56%</td>
<td>59%</td>
<td>57%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

---

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.