Ponemon INSTITUTE

The Post Breach Boom

Sponsored by Solera Networks

Independently conducted by Ponemon Institute LLC

Publication Date: February 2013

The Post Breach Boom

Ponemon Institute, February 2013

Part 1. Introduction

Data breaches have become a fact of life for organizations of all sizes, in every industry and in many parts of the globe. While many organizations anticipate that at some point a non-malicious or malicious data breach[1] will occur, the focus of this study is to understand the steps organizations are taking—or not taking--to deal with the aftermath of a breach or what we call the Post Breach Boom.

Sponsored by Solera Networks, *The Post Breach Boom* study was conducted by Ponemon Institute to understand the differences between non-malicious and malicious data breaches and what lessons are to be learned from the investigation and forensic activities organizations conduct following the loss or theft of sensitive and confidential information. The majority of respondents in this study believe it is critical that a thorough post-breach analysis and forensic investigation be conducted following either a non-malicious or malicious security breach.

Understanding the differences between these two types of breaches can help organizations anticipate the financial consequences. In Ponemon Institute's most recent Cost of Data Breach study published in March 2012, the average cost of a data breach per compromised record is $194. However, if the root cause is the result of a malicious insider or attack the average per record cost climbs to $222. While breaches attributed to a negligent insider averages far less at $174 per compromised record.

In this study we surveyed 3,529 IT and IT security practitioners in the following eight countries: United States, Canada, United Kingdom, Australia, Brazil, Japan, Singapore and United Arab Emirates. Most of the respondents (54 percent) report directly to the chief information officer or head of corporate IT. Fifty percent of respondents are at the supervisor level or higher.

To ensure quality responses, all participants in this study are in organizations that had one or more data or security breaches in the past 24 months. They also have significant or at least some level of understanding about the data or security breach incidents experienced by their organizations.

Some of the most noteworthy findings based on the consolidated findings.

- Data breaches have increased in severity and frequency but many organizations do not have the tools, personnel and funding to prevent, quickly detect and contain data breaches.

- Respondents believe understanding the root causes of breaches will strengthen their organization's security posture. This information can provide insights into where their security gaps and vulnerabilities exist. However, the majority of respondents do not have the tools, personnel and funding to determine root causes of a data breach.

- Employee or contractor negligence and system error or malfunctions are the two primary types of data and security breach incidents experienced by organizations. Malicious insiders and external attacks (exfiltration) are less prevalent.

- In the aftermath of a breach, security spending increase and many make the decision to invest in forensic and investigative tools.

[1] In this study we define a non-malicious breach as a system error, employee negligence or third-party snafu and a malicious breach is defined as one involving the theft of information assets by a criminal insider or

Following are some of the most salient global findings:[2]

Security breaches have increased in severity and frequency in the past 24 months, according to the majority of respondents. However, less than half of respondents say their organizations have the tools, personnel and funding to prevent, quickly detect and contain data breaches.

Sixty-three percent of respondents say understanding the root causes of breaches has strengthened their organization's security posture but only 40 percent say they have tools, personnel and funding to determine the root causes.

Employee or contractor negligence and system error or malfunctions are the two primary types of data and security breach incidents experienced by organizations. Malicious insiders and external attacks (exfiltration) are less prevalent.

Most non-malicious data breaches occur within the business unit or in transmission or transit to a third party. Most malicious incidents take place in an off-site or remote location or the organization was unable to determine the location of the breach.

Endpoints (63 percent of respondents) followed by databases (21 percent of respondents) were most often involved in the non-malicious data breach. In the case of malicious incidents, it was applications (42 percent of respondents) followed by user accounts (36 percent).

Failure to degauss or thoroughly wipe a device containing sensitive or confidential data (44 percent of respondents) and an employee or contractor losing a device containing sensitive or confidential data (39 percent) were the primary reasons the breach occurred. SQL injections, targeted attacks and advanced malware (30 percent, 28 percent and 27 percent of respondents) caused the malicious breach.

In the non-malicious breach the discovery was accidental (34 percent) followed by a loss prevention tool such as DLP (16 percent). Malicious breaches were most often discovered through the use of forensic methods and tools (28 percent) and DLP or other loss prevention tools (19 percent).

Non-malicious breaches were discovered in an average of 49 days and for malicious breach 80 days. Resolution was also shorter on average for non-malicious breaches at 83 days and malicious breaches took an average of 123 days.

There is more confidence that organizations understand the root cause of a non-malicious than a malicious breach. In the case of non-malicious, the most common method used was existing forensics/monitoring tools (48 percent) and existing security management tools (40 percent).

Used to determine the root cause of a malicious breach were existing forensics/monitoring tools (55 percent) and existing security management tools (42 percent). Remediation following the breach was to update security policies and training for both types of breaches.

Respondents cite lack of in-house expertise (50 percent) and inadequate security processes (37 percent) as reasons for not preventing the non-malicious breach. This is similar for malicious breaches. Sixty-four percent of respondents blame a lack of expertise followed by inadequate forensic capabilities (47 percent).

In the case of the non-malicious breach, lost reputation, brand value and market place image was the most serious consequence followed by no impact. With the malicious breach, organizations

[2] Please note that these summarized findings pertain to the consolidated sample, which combines the eight country samples on a weighted average basis.

suffered lost time and productivity followed by loss of reputation. Non-malicious data breaches on average were less costly $500,000 vs. $840,000.

Following a malicious breach, organizations more often invested in enabling security technologies (65 percent vs. 42 percent of respondents). More often they also made changes to its operations and compliance processes to better prevent and detect future breaches (63 percent vs. 54 percent).

Endpoint security and encryption tools were the most popular following a non-malicious breach and SIEM and encryption tools were most frequently purchased following a malicious breach.

Breaches drive increased spending on data security, according to 61 percent of respondents. The average increase is 20 percent.

A smaller percentage (52 percent) of respondents say the breach resulted in an increase in spending on forensic capabilities. However, among those organizations that spent more the increase was an average of 33 percent. This represents 13 percent more than the increase in data security funding.

Beyond the consolidated results summarized above, our study also found substantial differences across country samples. These differences mainly focused on the organization's breach experience and approaches to breach containment.

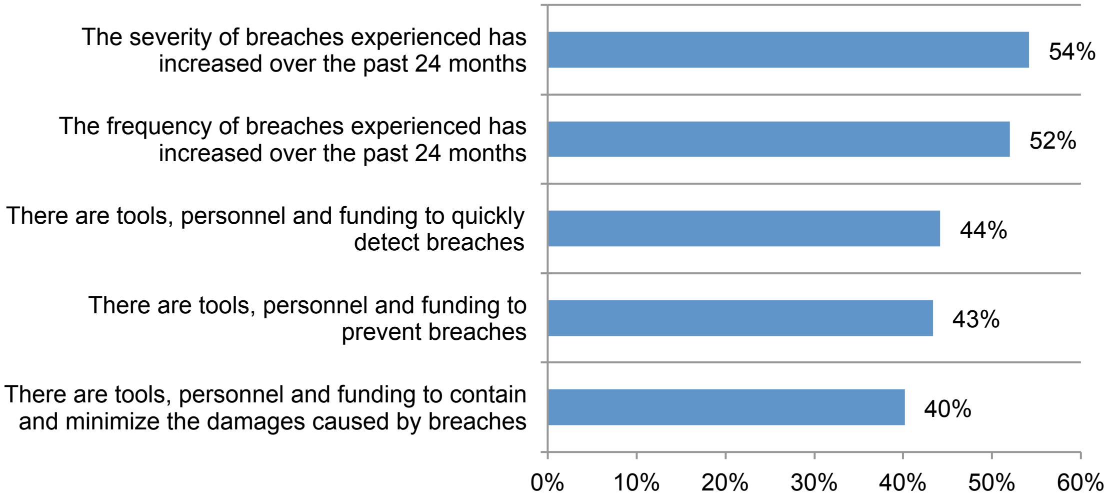
Part 2. Overall Findings

In this section, we present an analysis of the consolidated key findings from the eight countries represented in this study. We will provide country sample differences in Part 3. The complete audited findings for the consolidated sample are presented in the appendix of this report.

Breach experience of participating companies.

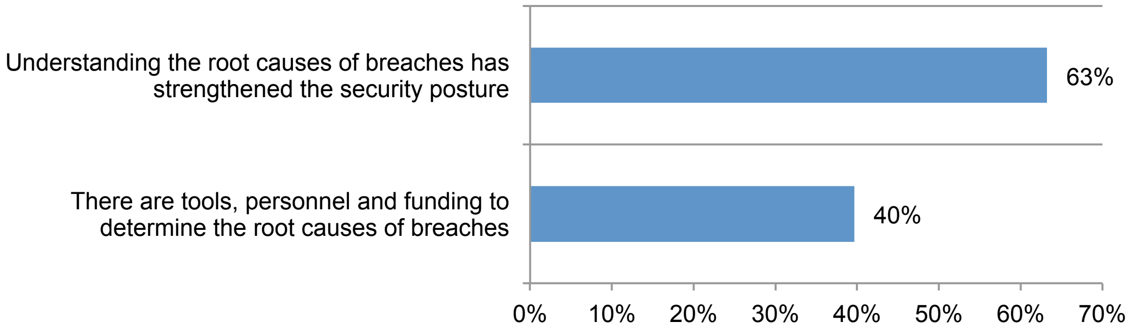
Data breaches are on the rise and more lethal. Figure 1 shows that breaches have increased in severity and frequency in the past 24 months, according to the majority of respondents. However, less than half of respondents say their organizations have the tools, personnel and funding to prevent, quickly detect and contain data breaches.

Figure 1: Perceptions about organizations' breach experiences
Strongly agree and agree response combined



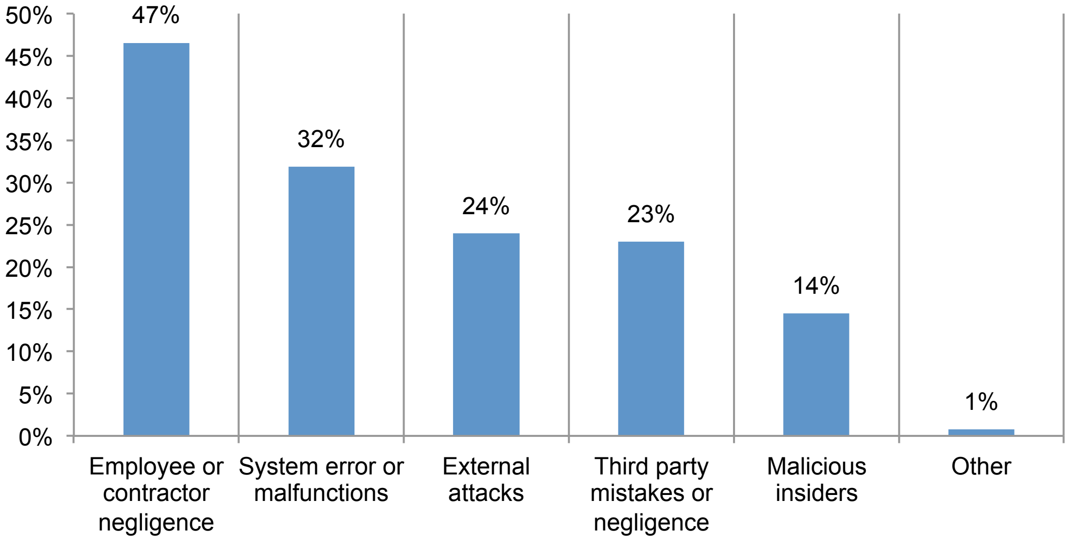
As shown in Figure 2, 63 percent of respondents believe understanding the root causes of breaches has strengthened their organization's security posture but only 40 percent say they have tools, personnel and funding to determine the root causes.

Figure 2: Perceptions about root causes
Strongly agree and agree response combined



Insider risk is the main cause of breaches. Employee or contractor negligence and system error or malfunctions are the two primary types of data and security breach incidents experienced by organizations. As discussed previously, breaches caused by human errors are typically less costly and faster to resolve than premeditated acts. In contrast, malicious insiders and external attacks are much less prevalent, as shown in Figure 3.

Figure 3: Types of data breaches experienced over the past 24 months
More than one response permitted

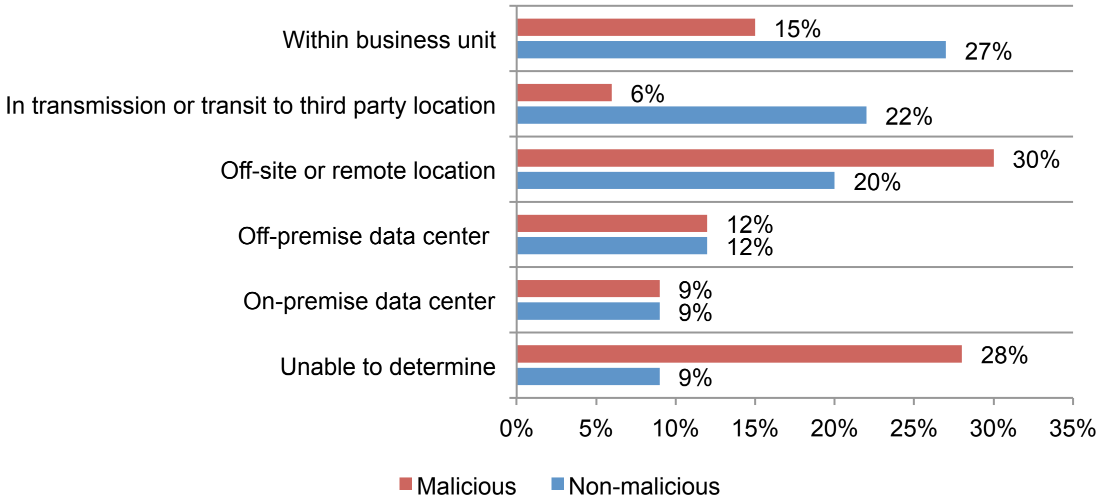


Significant differences exist between a non-malicious and malicious data breach.

In this section we analyze how very different these two types of breaches are. Understanding such differences can help organizations improve their ability to respond in the post breach boom.

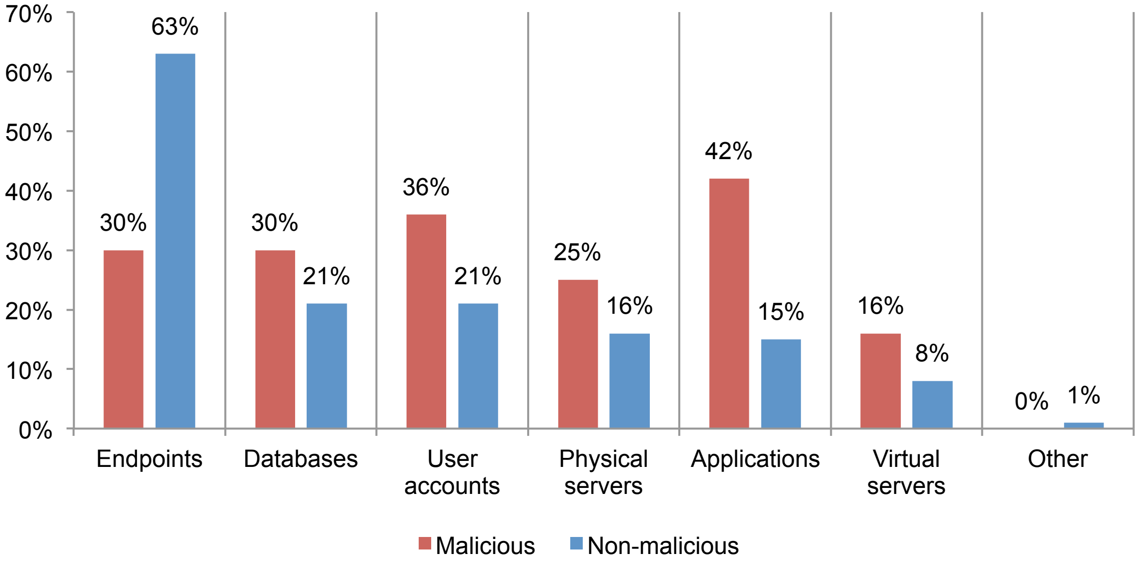
Location of the incident. According to Figure 4, non-malicious data breaches are more likely to occur within the business unit or in transmission or transit to a third party. In contrast, malicious incidents are more likely to occur in an off-site or remote location. It is interesting to note that 28 percent of respondents are unable to determine the location of malicious breaches. Only nine percent said they were unable to determine the location of non-malicious breaches.

Figure 4: Where the breach occurred



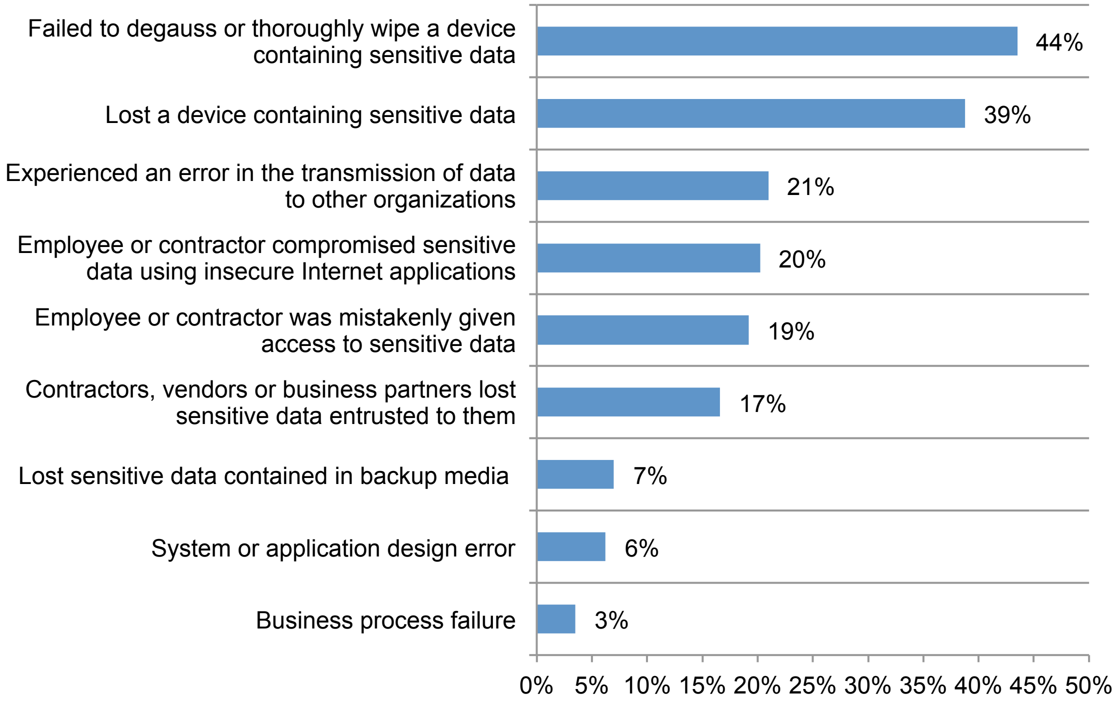
Assets compromised. According to Figure 5, endpoints (63 percent) followed by databases (21 percent) were most often compromised in the non-malicious data breach. In the case of malicious incidents, it was applications (42 percent) followed by user accounts (36 percent).

Figure 5: Compromised assets
More than one response permitted



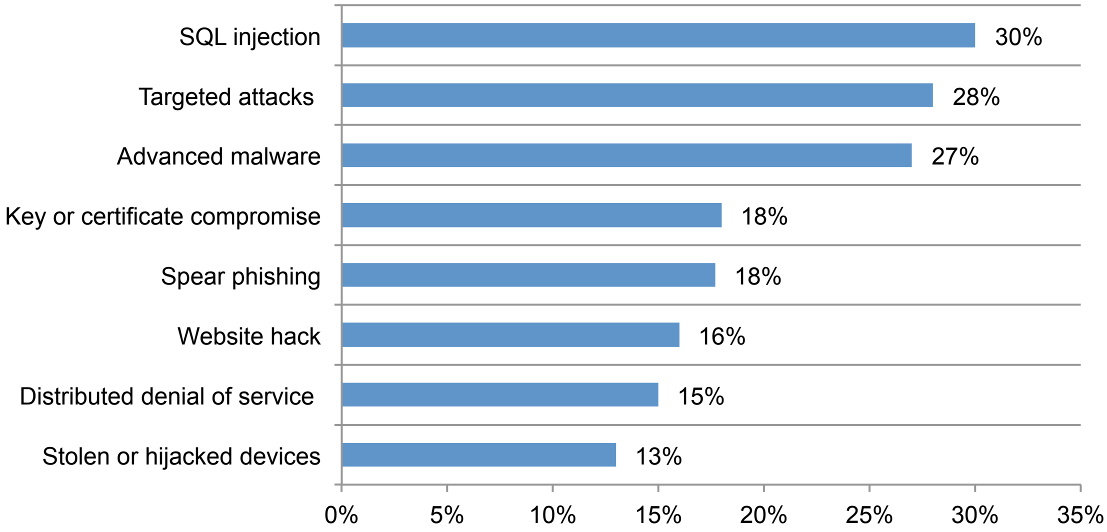
How it happened. Figure 6 reveals that failure to degauss or thoroughly wipe a device containing sensitive or confidential data (44 percent) and an employee or contractor losing a device containing sensitive or confidential data (39 percent) were the primary reasons the breach occurred.

Figure 6: How the non-malicious breach occurred
More than one response permitted



As shown in Figure 7, SQL injections, targeted attacks and advanced malware (30 percent, 28 percent and 27 percent) caused the malicious breach.

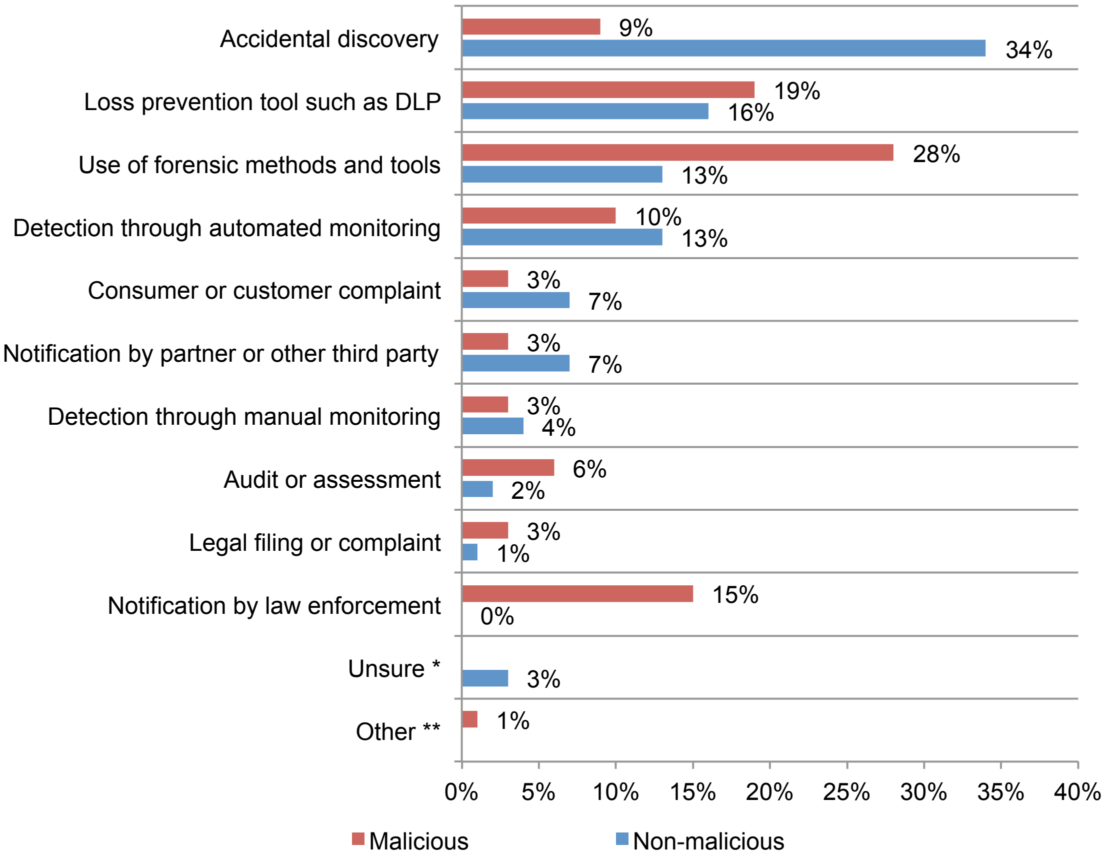
Figure 7: How the malicious or criminal breach occurred
More than one response permitted



Detection of the breach. In the non-malicious breach the discovery was most often accidental (34 percent) followed by a loss prevention tool such as DLP (16 percent), as revealed in Figure 8.

There is a significant difference between non-malicious and malicious breaches in how the incident was discovered. Very few malicious breaches are discovered by accident. Rather malicious breaches were most often discovered through the use of forensic methods and tools (28 percent) and DLP or other loss prevention tools (19 percent).

Figure 8: How the breach was detected



* This was not a choice for malicious breach
** This was not a choice for non-malicious breach

Time to discover and resolve the breach. As shown in Figure 9**,** non-malicious breaches were discovered an extrapolated average of 49 days and for malicious breach 80 days.

Figure 9: When the breach was discovered

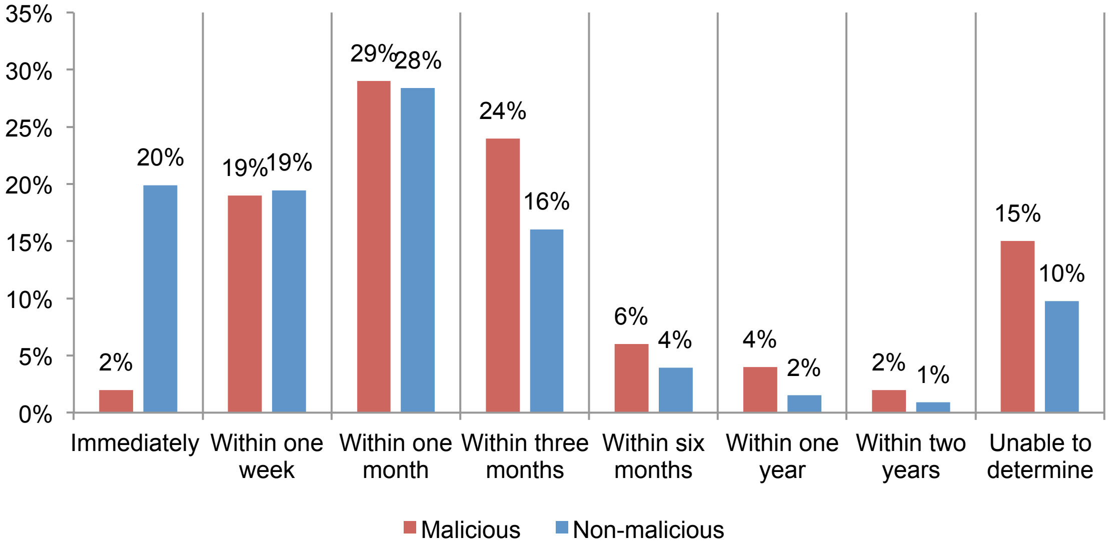
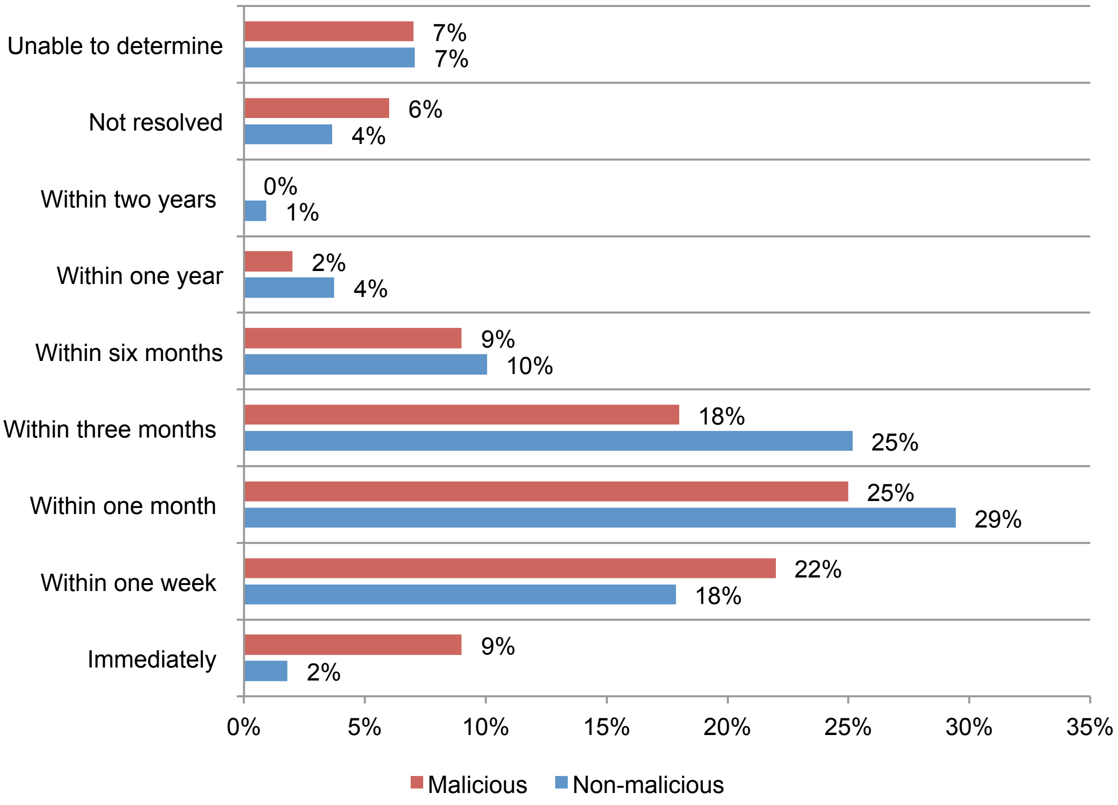


Figure 10 shows that resolution was also shorter on average for non-malicious breaches at 83 days and malicious breaches took an average of 123 days.

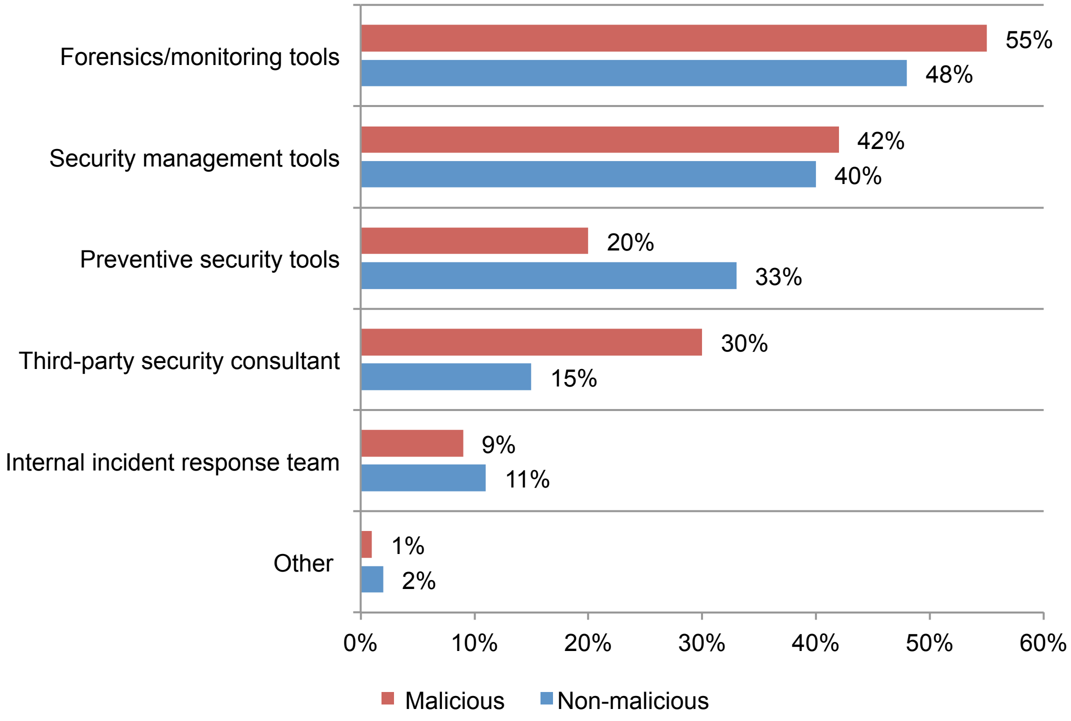
Figure 10: When the breach was resolved



Confidence in understanding the root cause. There is more confidence that organizations understand the root cause of a non-malicious breach. Forty-six percent of respondents in organizations that had a non-malicious breach say they are very confident or confident they understand the root cause. Only 39 percent of respondents that had to deal with a malicious breach are very confident or confident they know the root cause.

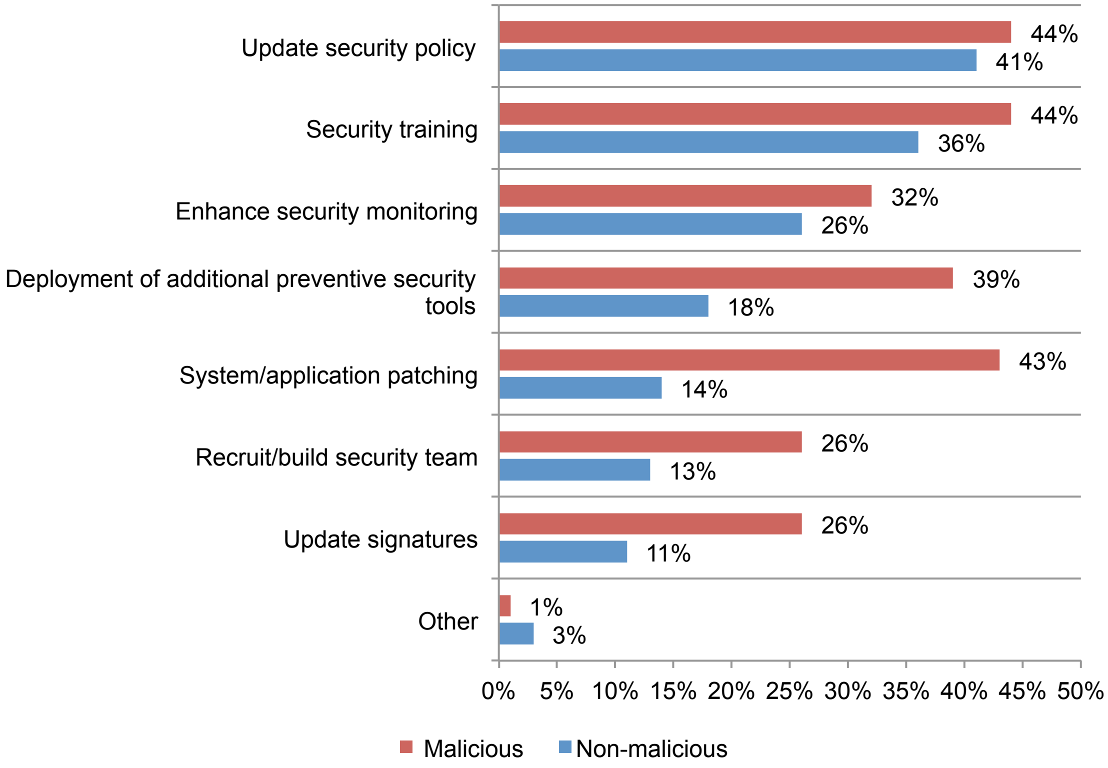
In the case of both non-malicious and malicious breaches, the most common method used to find the root cause was existing forensics/monitoring tools (48 percent and 55 percent, respectively) and existing security management tools (40 percent and 42 percent of respondents, respectively), as revealed in Figure 11.

Figure 11: How the root cause(s) were determined
More than one response permitted



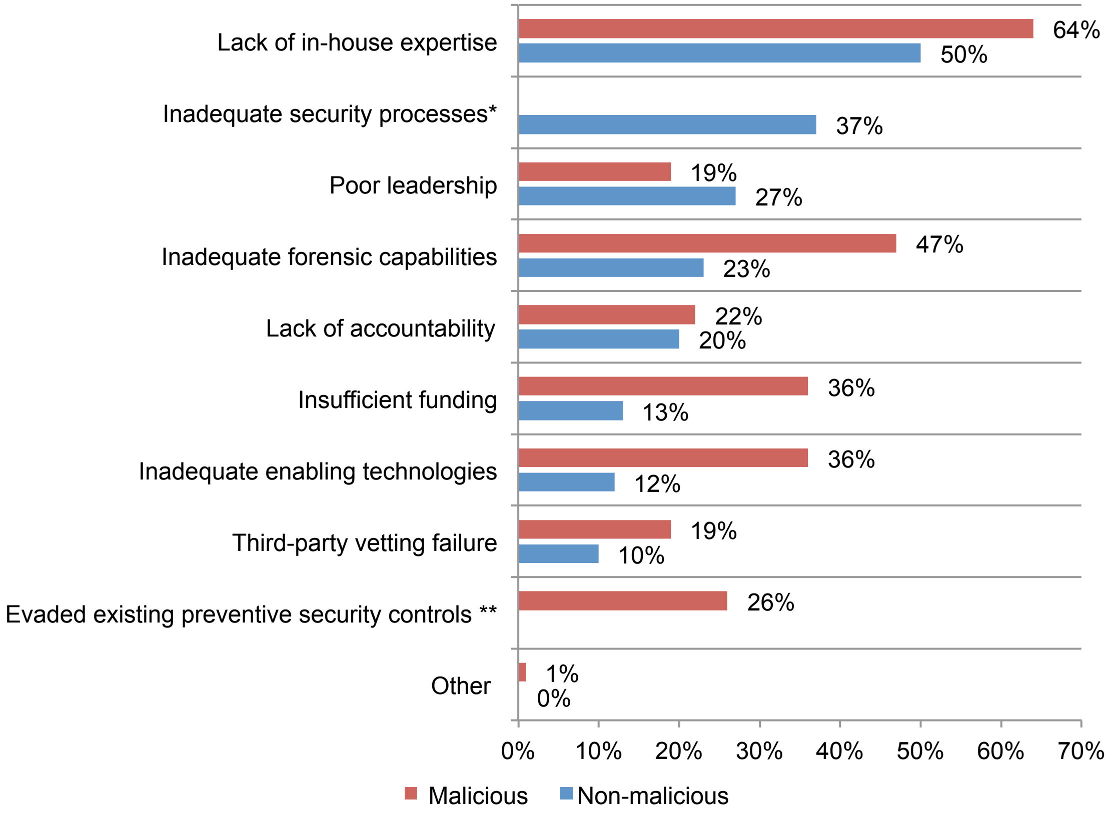
Remediation following the breach was to update security policies and training for both types of breaches, as shown in Figure 12.

Figure 12: Appropriate mitigation/remediation actions taken
More than one response permitted



Reasons for failing to stop the breach. Figure 13 shows that respondents cite the lack of in-house expertise (50 percent) and inadequate security processes (37 percent) as reasons for not preventing the non-malicious breach. This is similar for malicious breaches. Sixty-four percent of respondents blame a lack of expertise followed by inadequate forensic capabilities (47 percent).

Figure 13: Reasons for failing to prevent the breach
Three responses permitted



* This was not an option for non-malicious breach
** This was not an option for mailicous breach

Impact and cost of the breach. In the case of the non-malicious breach, lost reputation, brand value and market place image was the most serious consequence followed by no impact. With the malicious breach, organizations suffered lost time and productivity followed by loss of reputation. See Figure 14.

Figure 14: Impact of the breach
More than one response permitted

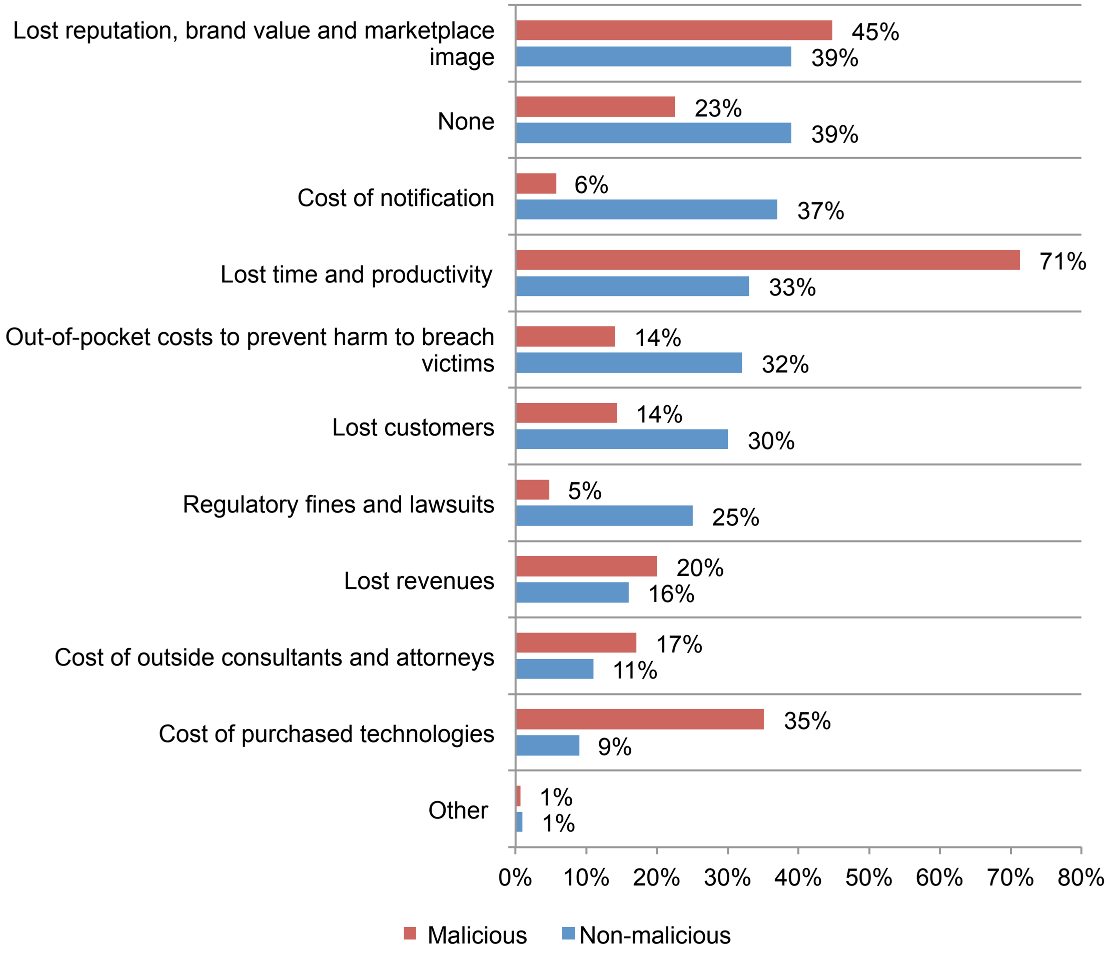
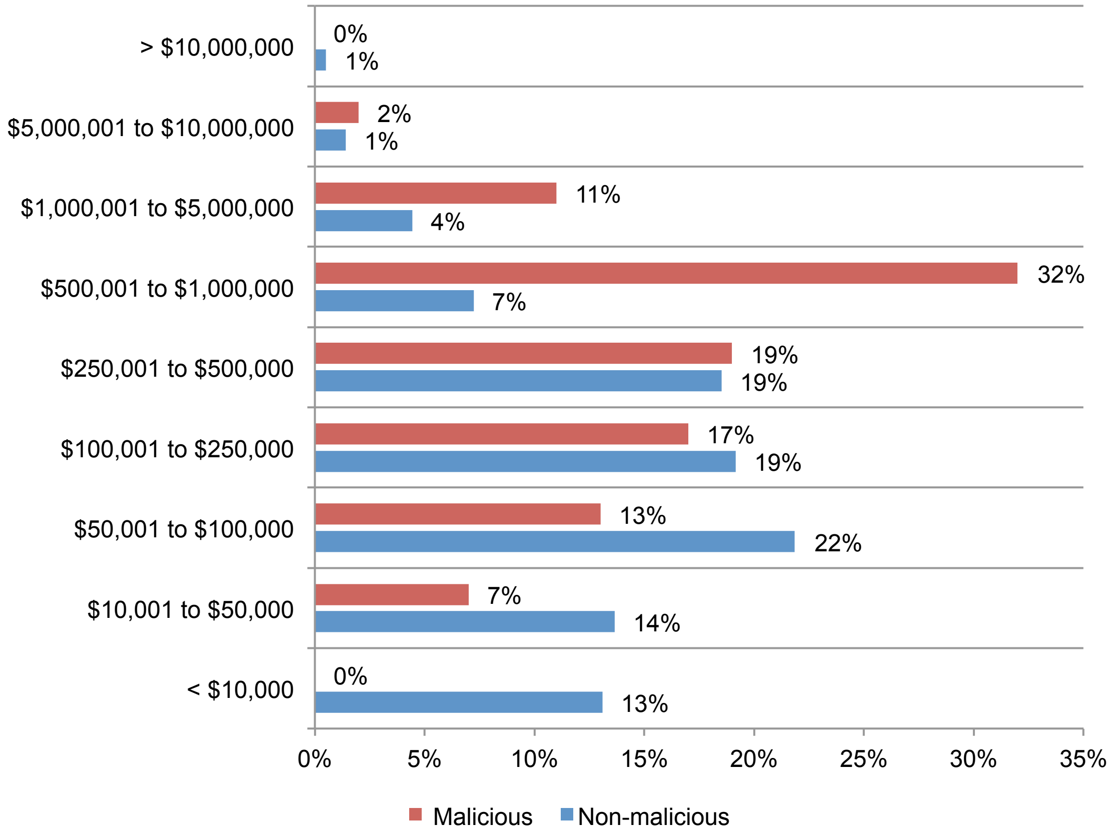


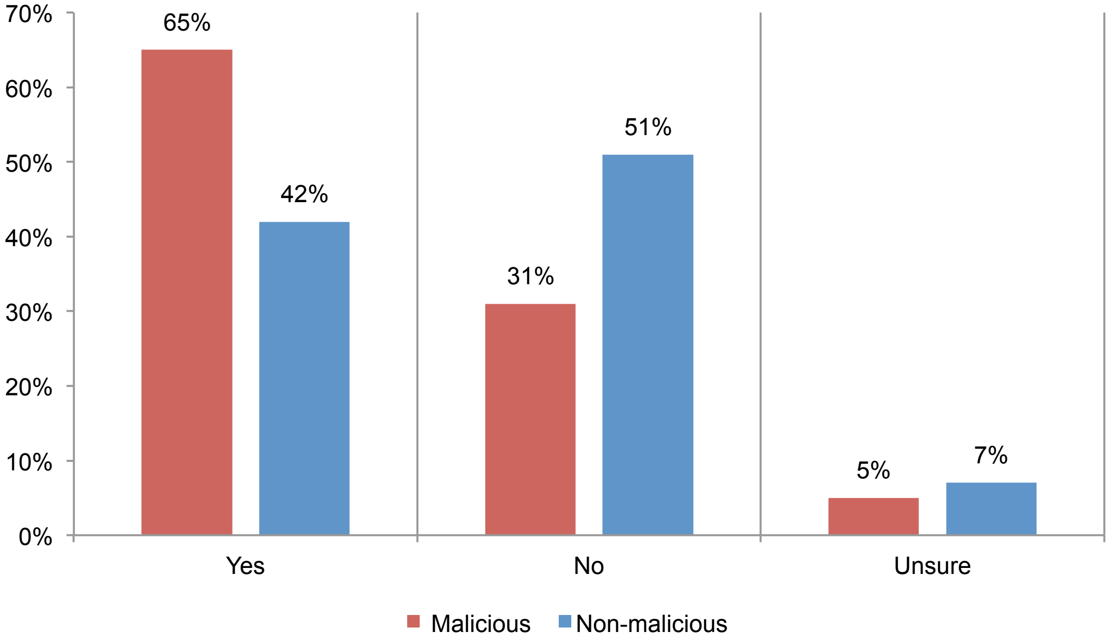
Figure 15 shows the differences in what a non-malicious data breach vs. a malicious data breach costs on average. An extrapolation of cost with conversion into US dollars revealed non-malicious breaches are far less costly than malicious breaches ($500,000 vs. $840,000 on average).

Figure 15: Extrapolated cost of the breach



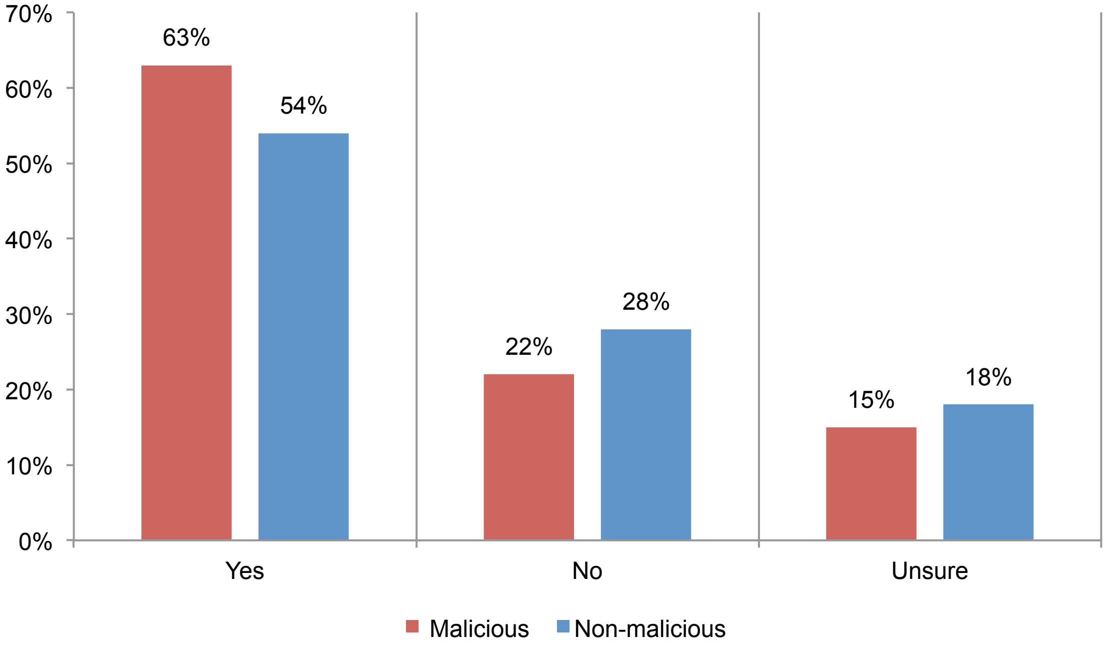
Investment in the post breach boom. According to Figure 16**,** following a malicious breach, organizations more often invested in enabling security technologies (65 percent vs. 42 percent).

Figure 16: Investments in security technologies to prevent or detect future breaches



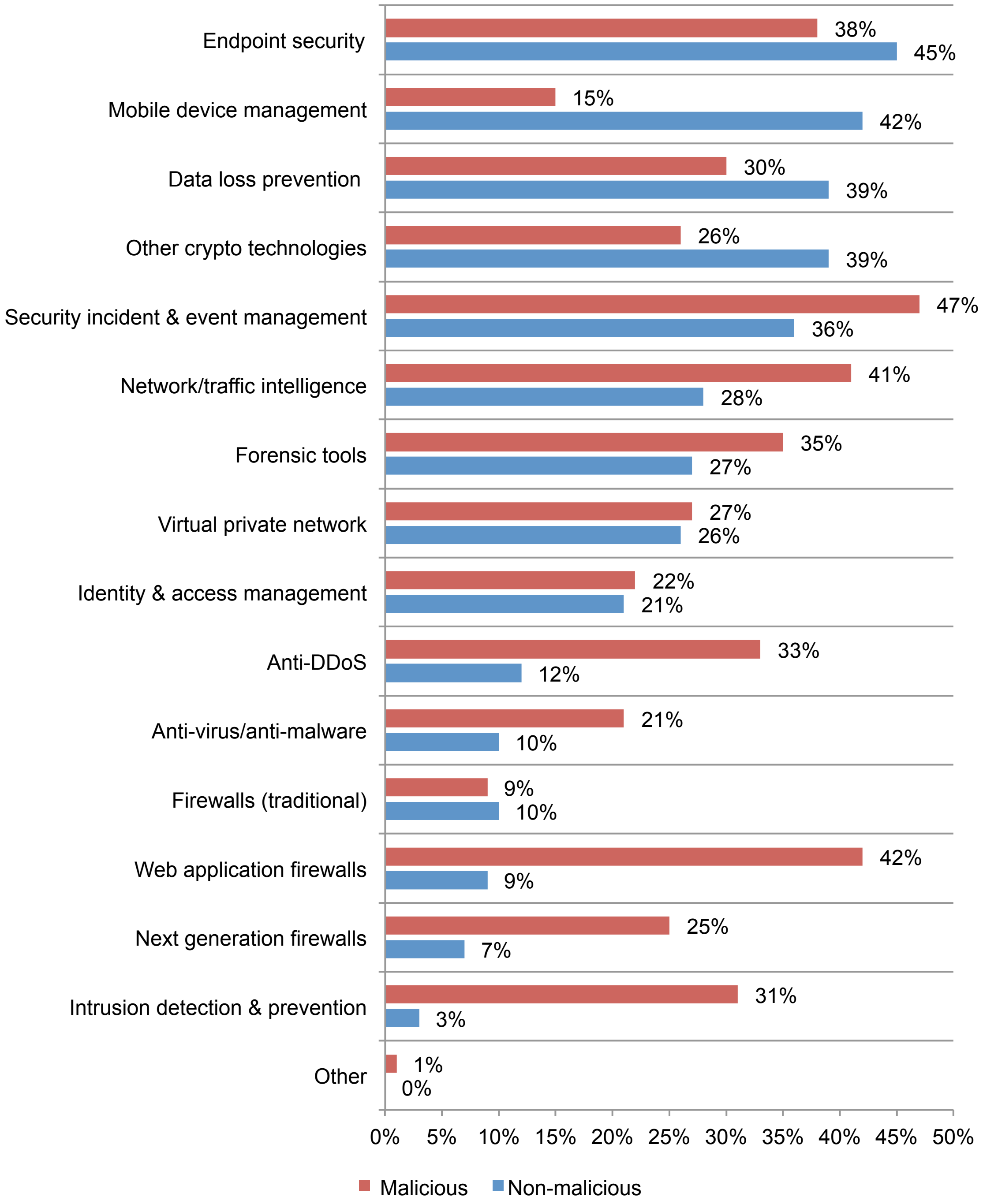
According to Figure 17, more often they also made changes to its operations and compliance processes to better prevent and detect future breaches (63 percent vs. 54 percent).

Figure 17: Changes to operations and compliance processes to prevent or detect future breaches



Endpoint security and encryption tools were the most popular following a non-malicious breach and SIEM and encryption tools were most frequently purchased following a malicious breach. See Figure 18.

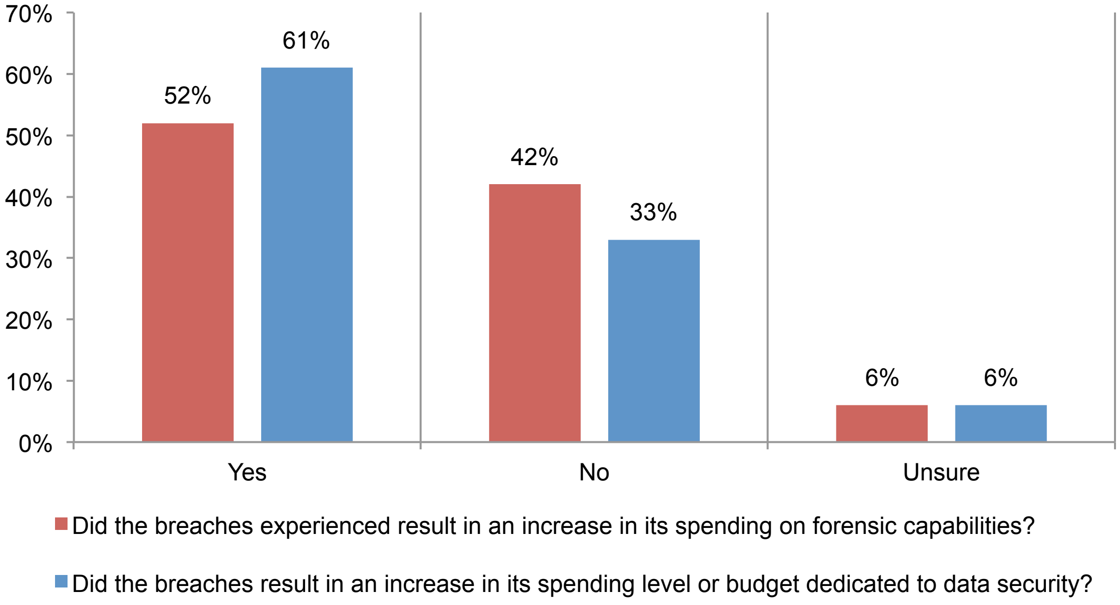
Figure 18: Technology investments made post breach to prevent or detect future breaches
Five choices permitted



Lessons Learned

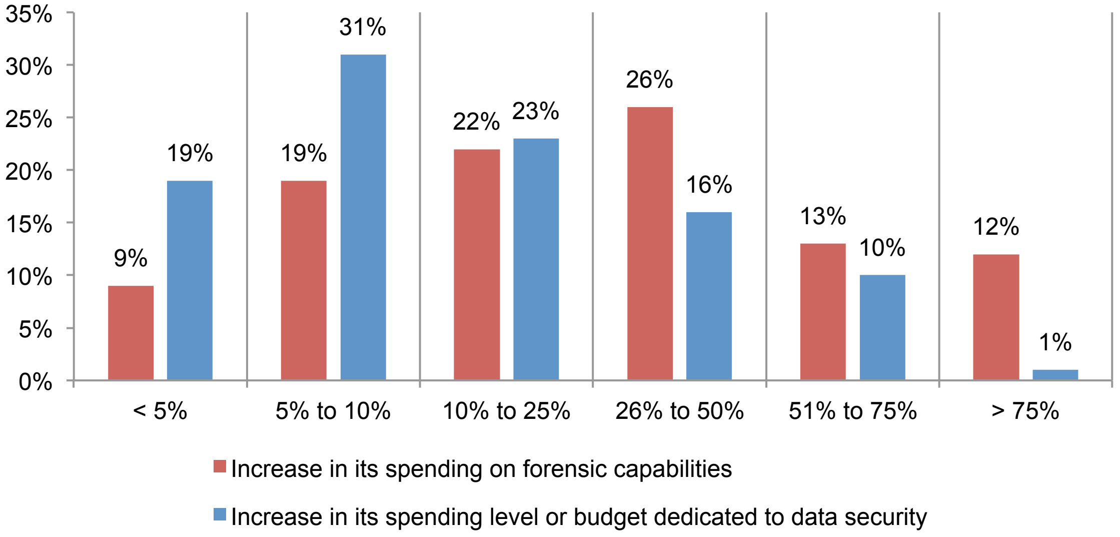
Organizations spend more on data security in the post breach boom. Data breaches drive increased spending on data security, according to 61 percent of respondents. The average increase is 20 percent. See Figure 19.

Figure 19: Increase in spending level dedicated to data security or forensic capabilities



A smaller percentage (52 percent) of respondents say the breach resulted in an increase in spending on forensics capabilities. However, among those organizations that spent more the increase was an average of 33 percent. This represents 13 percent more than the increase in data security funding. See Figure 20.

Figure 20: How much of an increase in spending levels?



Part 3. Comparison of country samples

Figures 21 to 28 show the country-level results for eight survey attributions. Each percentage shows the average “strongly agree” and “agree” response (combined) for each country. The dotted line indicates the global average for all countries.

This figure shows Singapore and Japan are more likely to perceive their organizations as ready to prevent breach incidents. Respondents in Brazil are least ready to prevent breaches.

Figure 21: Readiness to prevent breaches

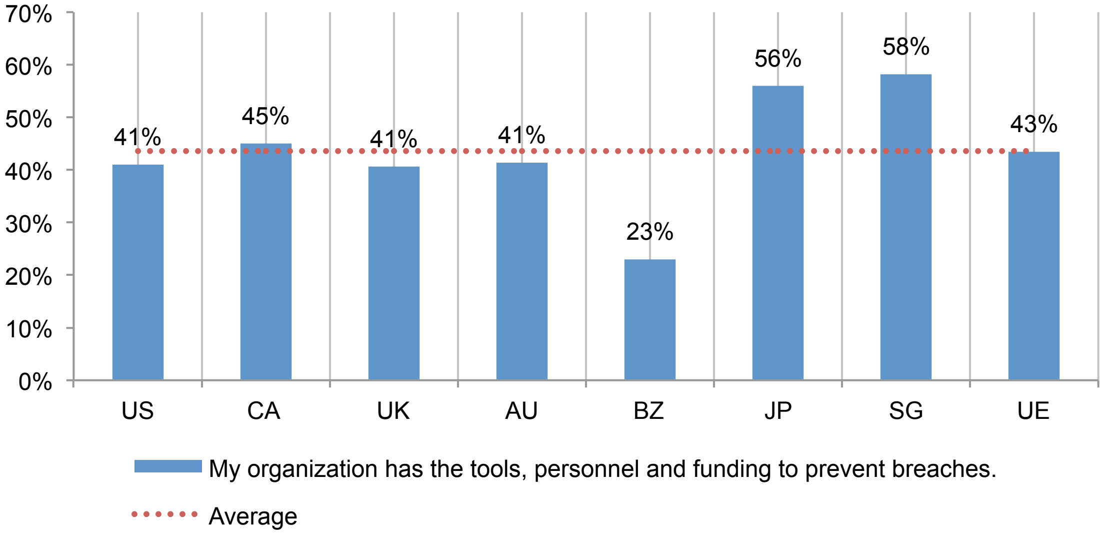


Figure 22 again shows Singapore and Japan are more likely to perceive their organizations as ready to quickly detect breaches. Respondents in Brazil perceive their organizations as least able or ready to quickly detect breaches.

Figure 22: Readiness to quickly detect breaches

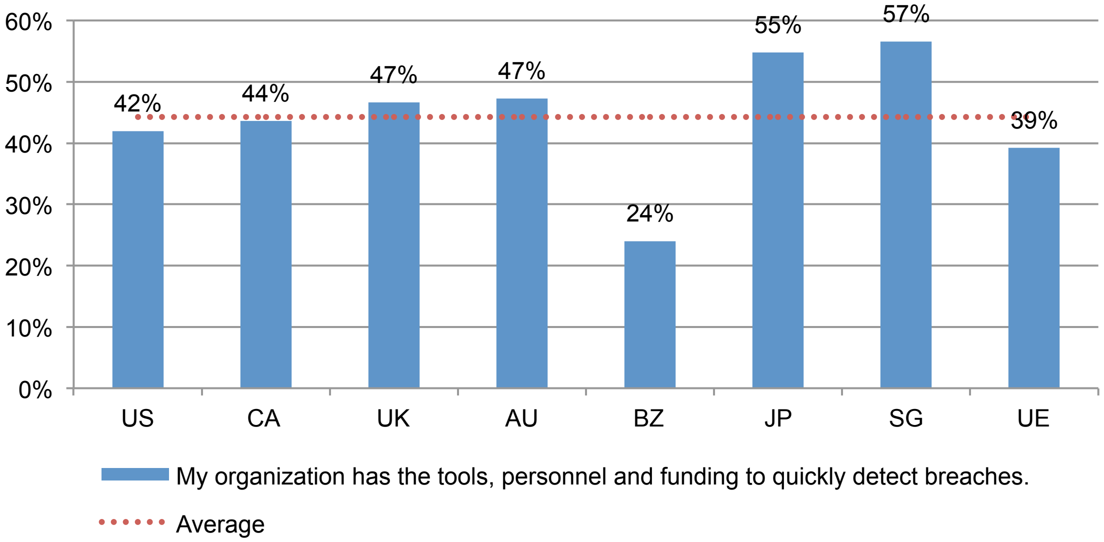
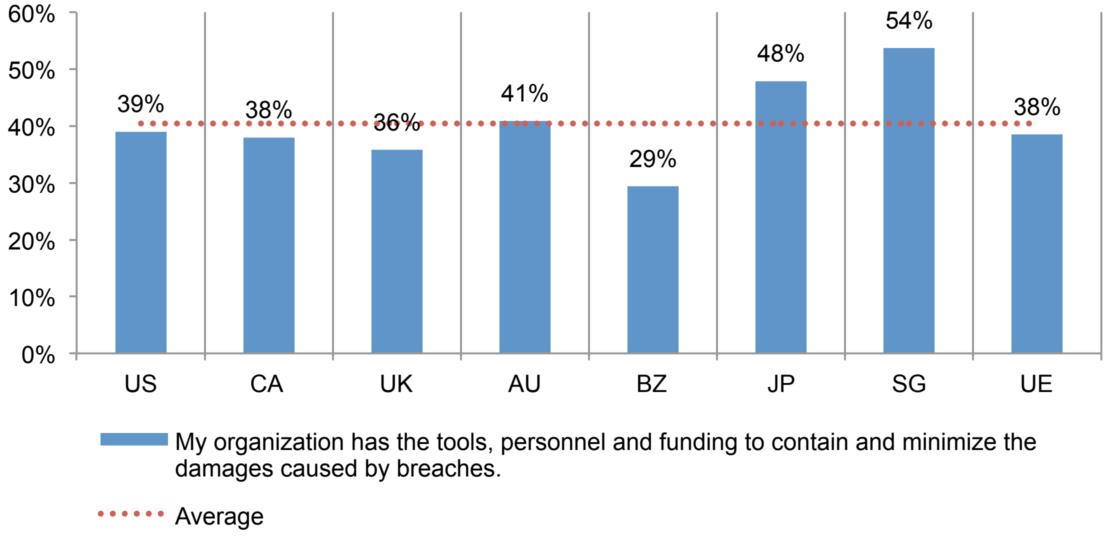


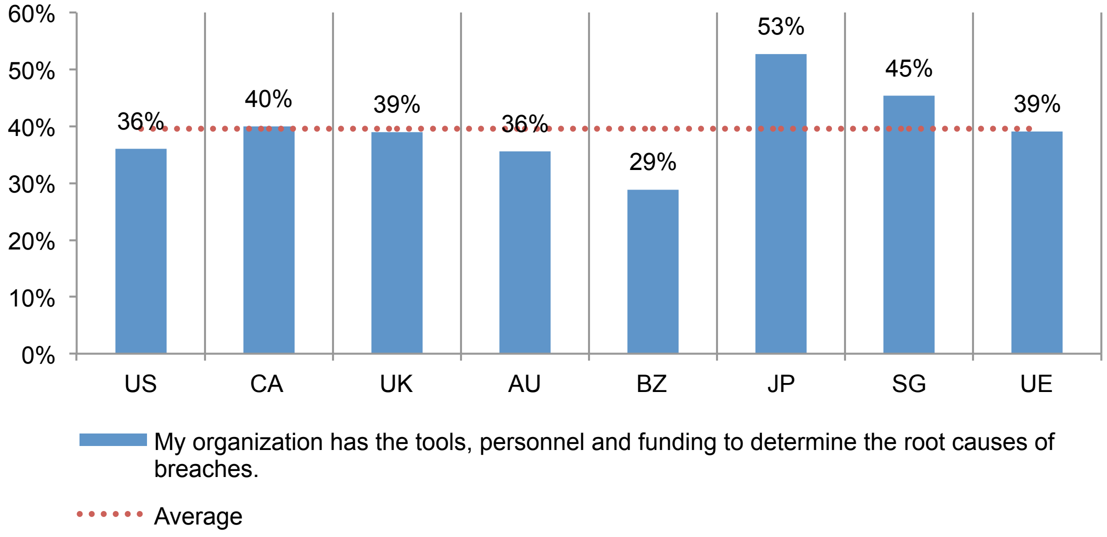
Figure 23 again shows respondents in Singapore and Japan are more likely to perceive their organizations as being capable of minimizing the damages caused by breaches. Once again, respondents in Brazil are least likely to perceive their organizations as having the ability to minimize breach damages.

Figure 23: Capable of minimizing damages



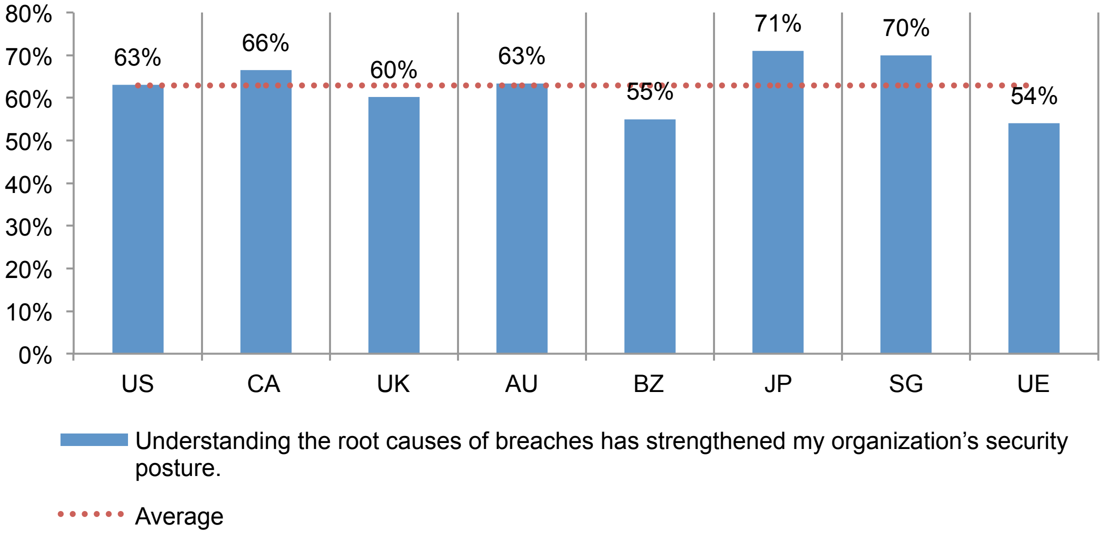
The next figure once again shows respondents in Japan and Singapore as having the most favorable views about their organization's resources to assess root causes of beach incidents. Respondents in Brazil once again has the least favorable view.

Figure 24: Adequacy of funding to determine root causes



According to figure 25, respondents in Japan and Singapore are most likely to see root cause analysis as a way to strengthen or improve their organizations' security effectiveness. Respondents in the United Arab Emirates and Brazil are least likely to hold this view.

Figure 25: Understanding the root cause strengthens security



Respondents in Japan and Singapore are most likely to perceive their organizations' leaders as supportive of data protection activities. Brazil and the United Arab Emirates are least likely to hold this perception.

Figure 26: Organizational leaders view data protection as a top priority

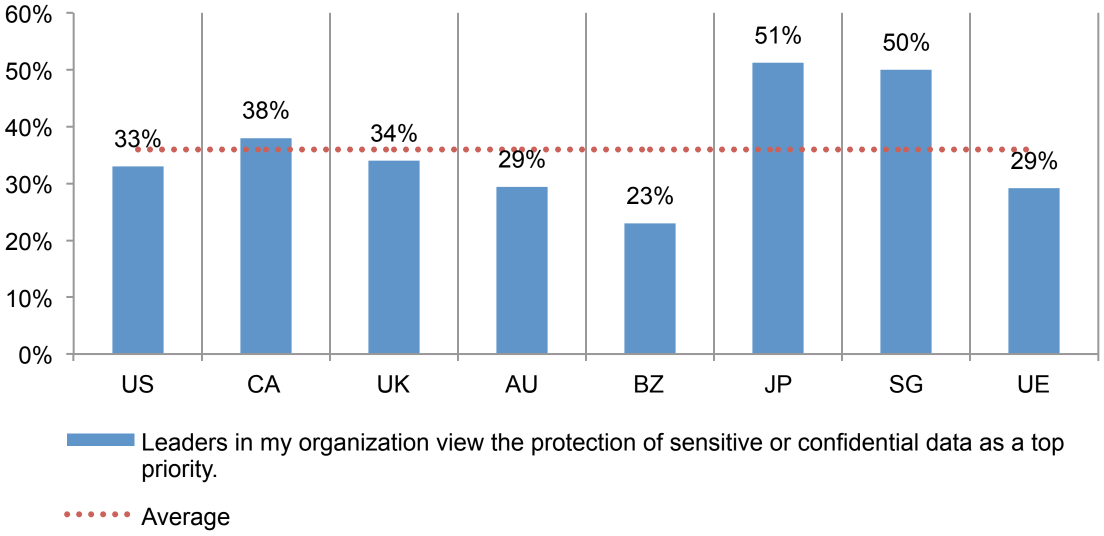
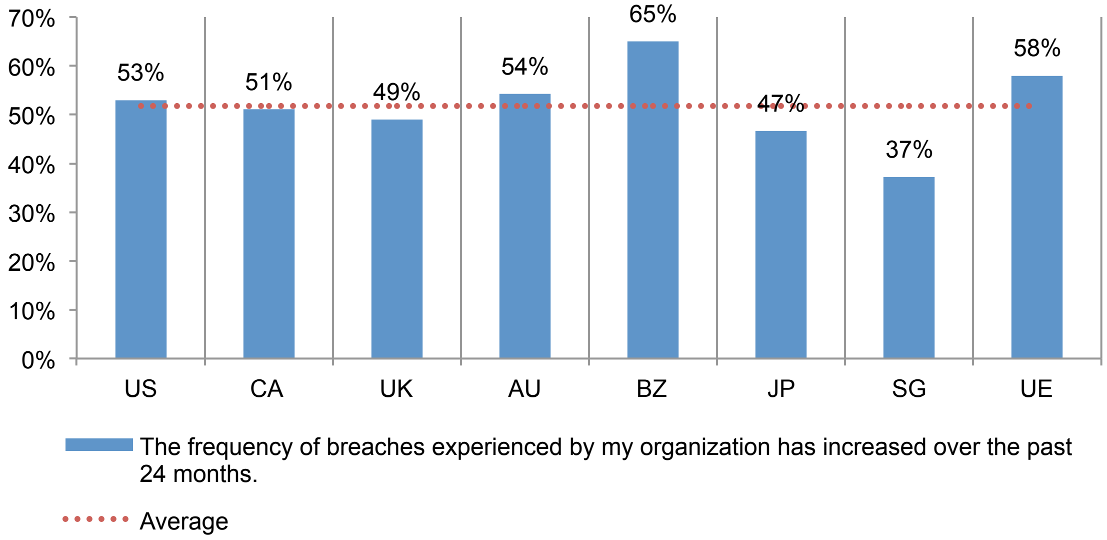


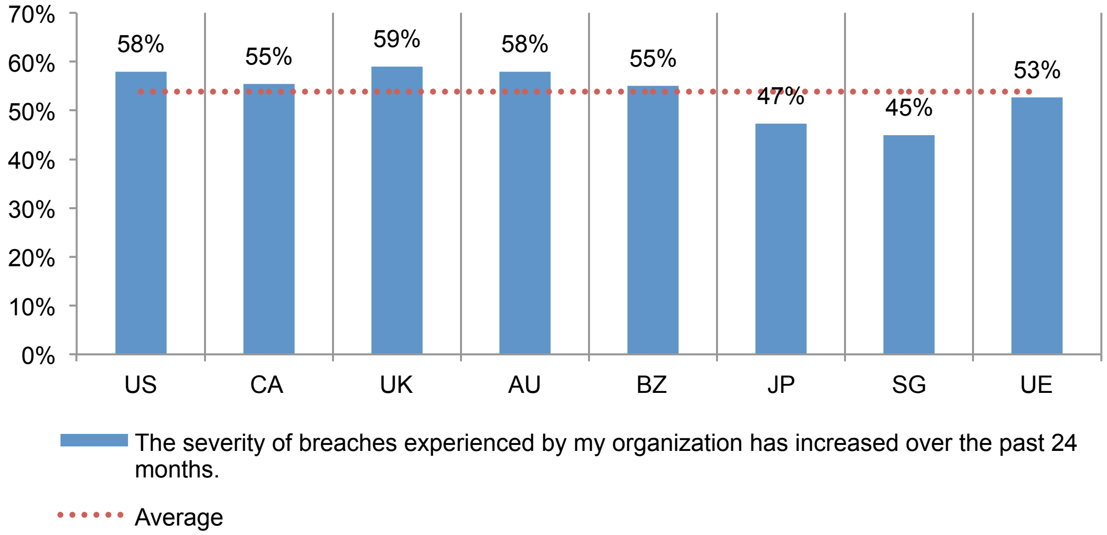
Figure 27 shows the percentage of respondents who believe breach incidents have increased over the past two years. Given the pattern shown above, it is interesting to see Brazil with the highest rate of agreement and Singapore and Japan with the lowest rates of agreement.

Figure 27: Increased frequency of breach incidents



With the exception of Japan, all countries perceive a higher increase in the severity of breach incidents than frequency.   Here again, respondents in Singapore and Japan have the lowest rates of agreement to the issue of increasing severity of breaches.

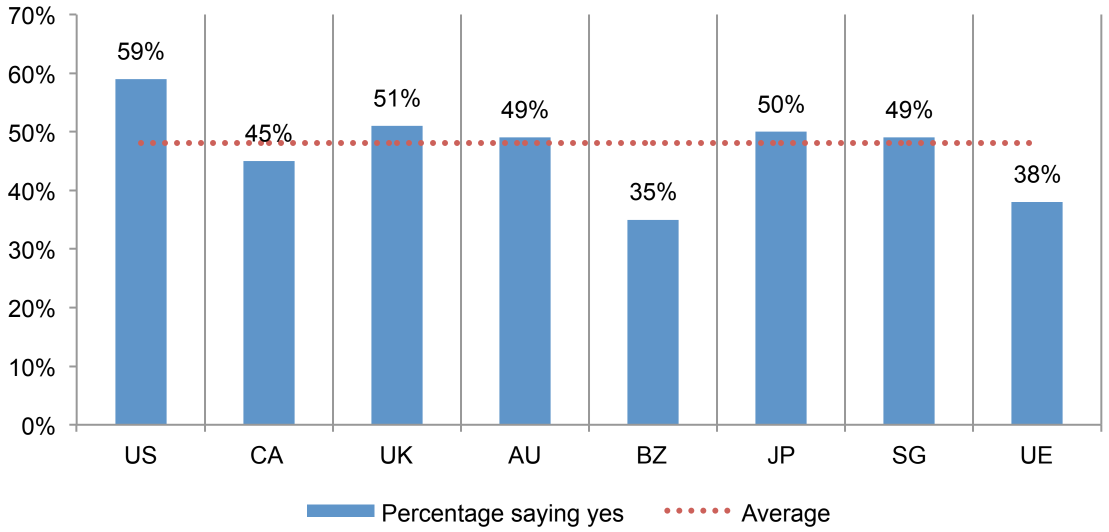
Figure 28: Increased severity of breach incidents



Taken together, the above figures strongly suggest that respondents in Singapore and Japan are most likely to hold favorable perceptions about their organizations' readiness for breach prevention and quick detection. These respondents are also more likely to value root cause analysis and see their leaders as strongly supportive of data protection and security initiatives. In sharp contrast, respondents in Brazil appear to hold the least favorable opinion on the same attributes. Respondents in all other countries appear to be relatively similar on most attributes.

According to Figure 29, US organizations (59 percent) are most likely to experience a breach involving the loss of information assets than all other countries. Brazil (35 percent) and the United Arab Emirates (38 percent) are least likely to experience breaches involving information losses.

Figure 29: Did your organization experience a breach incident resulting in the loss of information assets?



The following figure shows the extrapolated time in days for organizations to recover from a breach incident. As can be seen, the total time for malicious incidents are substantially higher than non-malicious incidents in all country samples. Respondents in the United Arab Emirates report the longest timeframe for both malicious and non-malicious breach incidents. Singapore reports the shortest time frame to resolve a malicious breach incident and Japan reports the shortest time to resolve a non-malicious incident.

Figure 30: Time to recover from a breach (in days from discovery to resolution)

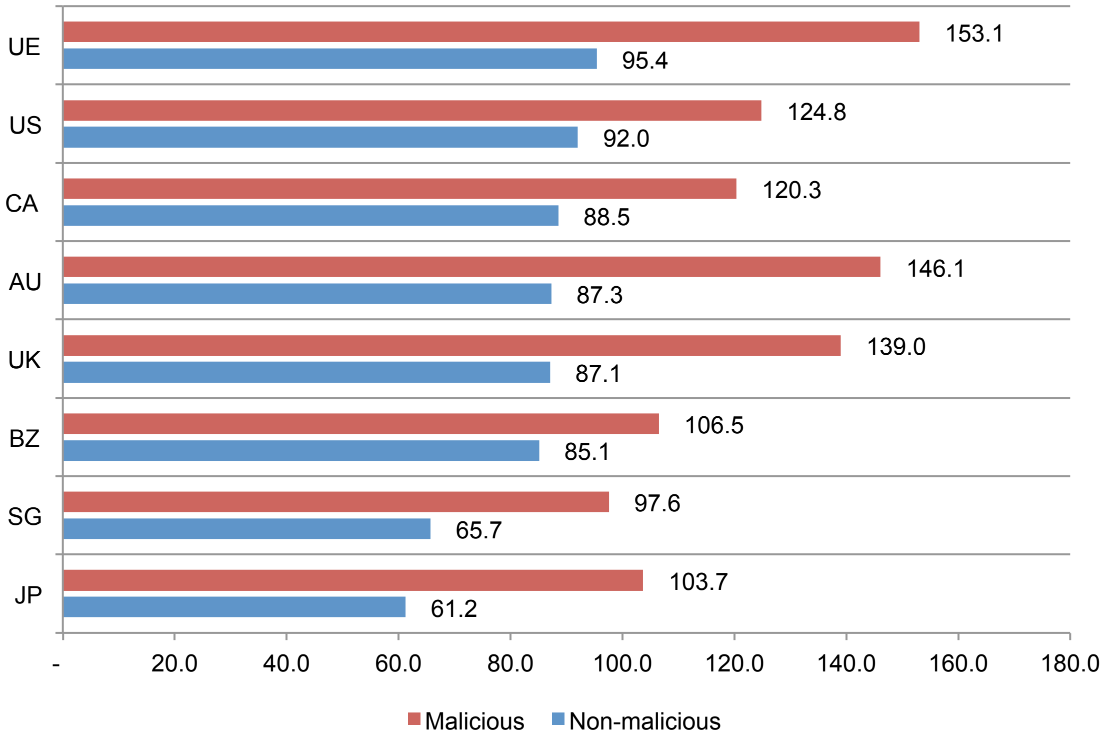


Figure 31 shows respondents' level of confidence in their organizations' ability to determine the root causes of malicious and non-malicious breach incidents. Respondents in Singapore and Japan hold the highest level of confidence, while respondents in Brazil and the US hold the lowest level of confidence. With the exception of Singapore and Japan, respondents appear to hold a higher level of confidence in their ability to uncover root causes of non-malicious versus malicious incidents.

Figure 31: How confident are you that the investigation revealed the root cause(s) of this breach incident?

Very confident and confident response combined

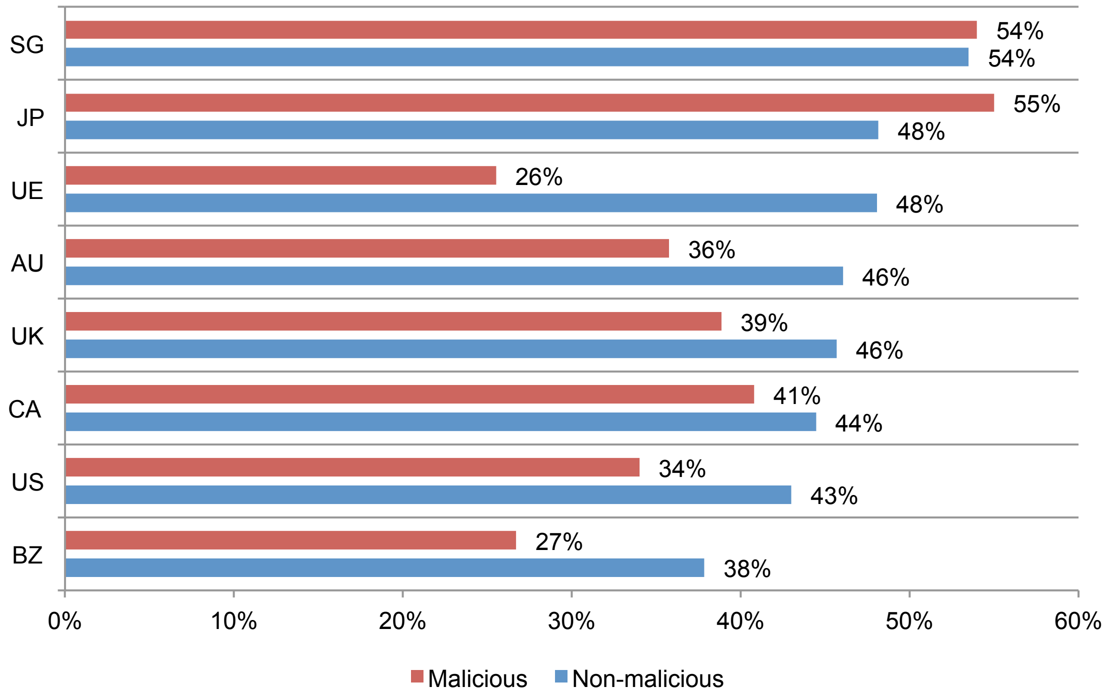
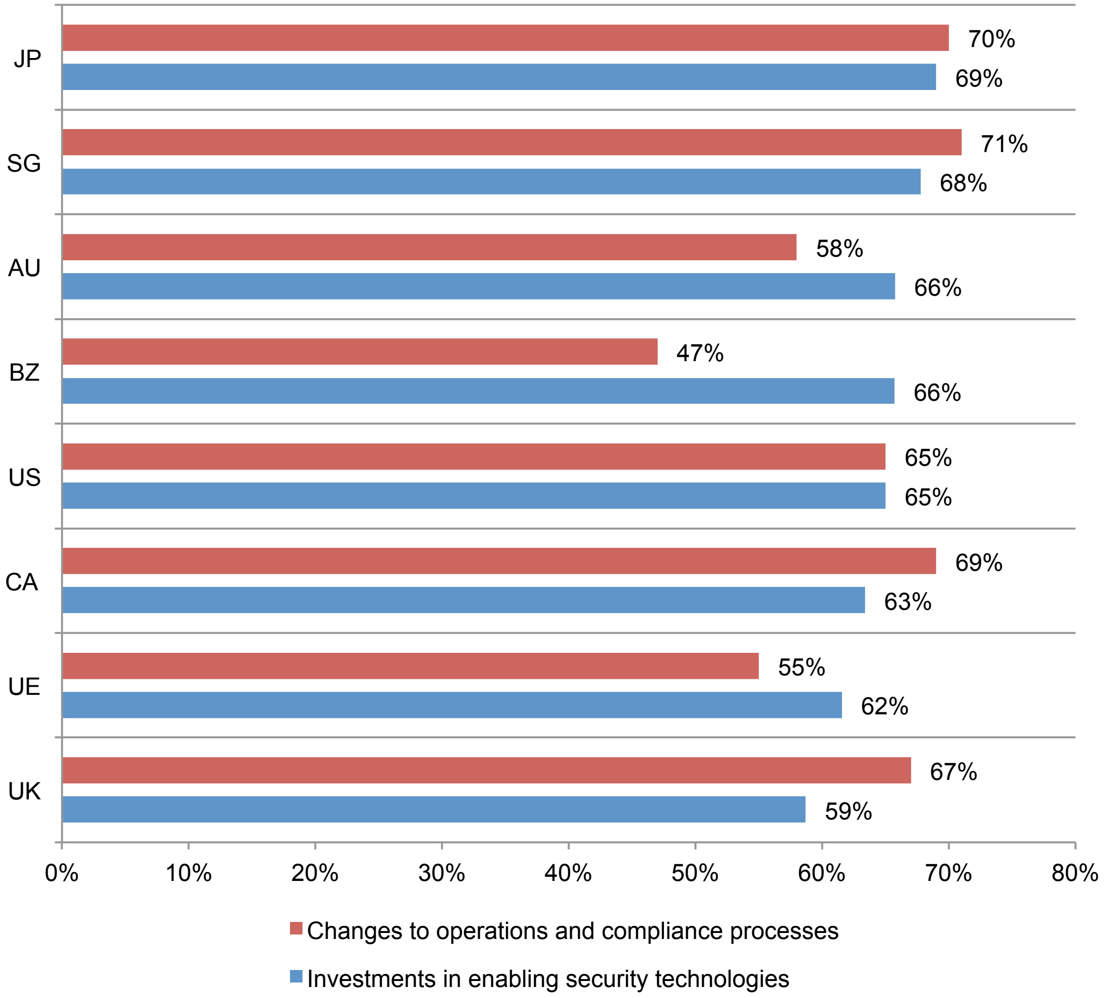


Figure 32 shows the percentage of respondents who say their organization implemented positive changes to strengthen its security posture. As can be seen, a majority of respondents in all countries say their organizations invested in enabling security technologies following the breach. With the exception of Brazil, a majority of respondents say their organizations made changes to operations and compliance processes following the breach.

Figure 32: Investments and changes made to operations and compliance operations after the breach incident



Part 4. Methods

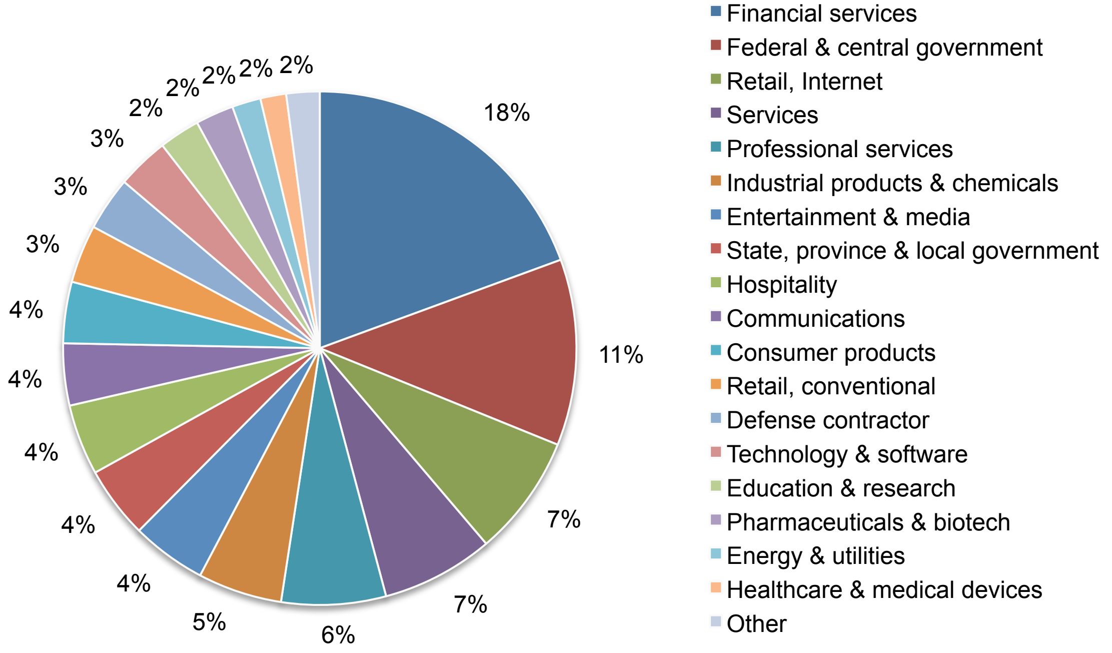
Table 1 reports the sample response in eight countries. A total of 107,195 IT or IT security practitioners located in eight countries were targeted to participate to this survey. As shown, 4,437 respondents returned the survey. Tests for reliability and screening removed 908 surveys. The final combined sample was 3,529 surveys (or a 3.3 percent response rate).

Table 1. Survey responses in eight countries

Country	Sampling frame	Total returns	Rejected & screened	Final sample	Response rate
United States (US)	20,967	816	157	659	3.1%
Canada (CA)	13,993	533	110	423	3.0%
United Kingdom (UK)	13,891	549	118	431	3.1%
Australia (AU)	9,986	473	78	395	4.0%
Brazil (BZ)	15,830	578	133	445	2.8%
Japan (JP)	17,649	707	141	566	3.2%
Singapore (SG)	7,919	398	89	309	3.9%
United Arab Emirates (UE)	6,960	383	82	301	4.3%
Total	107,195	4,437	908	3,529	3.3%

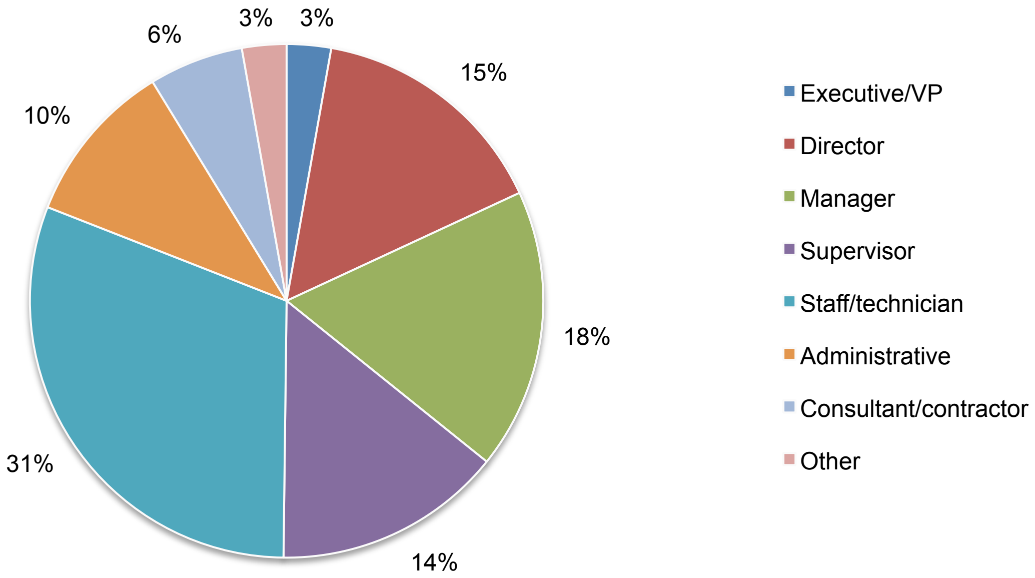
Pie Chart 1 reports the industry segments of respondents' organizations for the consolidated sample composed of eight individual country samples. This chart identifies financial services (18 percent) as the largest segment, followed by federal and central government (11 percent) and retail, Internet (7 percent) and services (7 percent).

Pie Chart 1: Industry distribution of respondents' organizations
Consolidated view (n = 3,529)



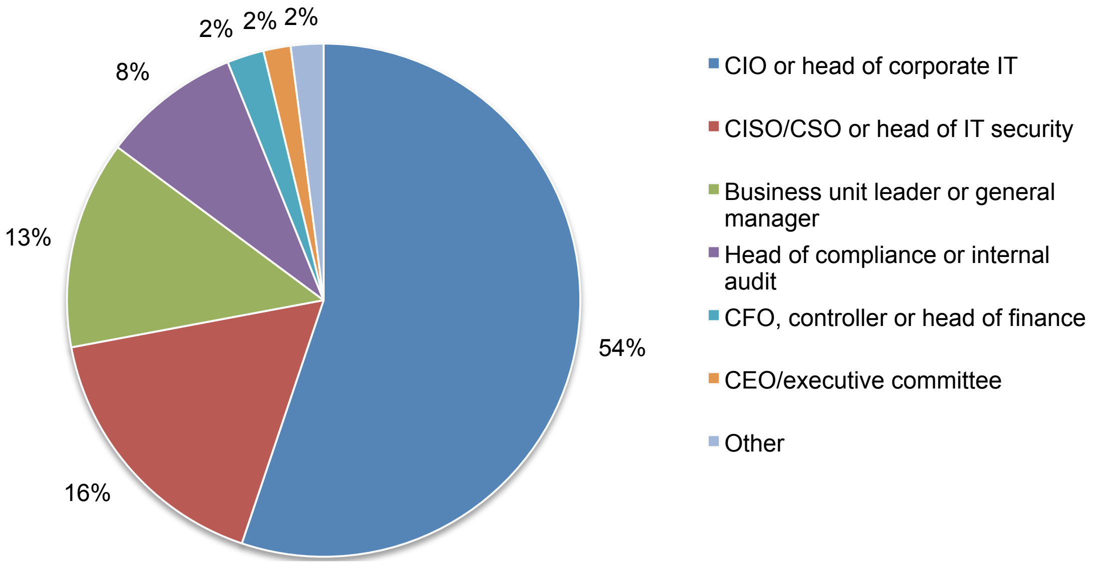
Pie Chart 2 reports the respondent's organizational level within participating organizations for the consolidated sample. Half (50 percent) of the respondents are at or above the supervisory levels. The largest segment at 31 percent is composed of respondents who self report being technicians or staff level employees.

Pie Chart 2: What organizational level best describes your current position?
Consolidated view (n = 3,529)



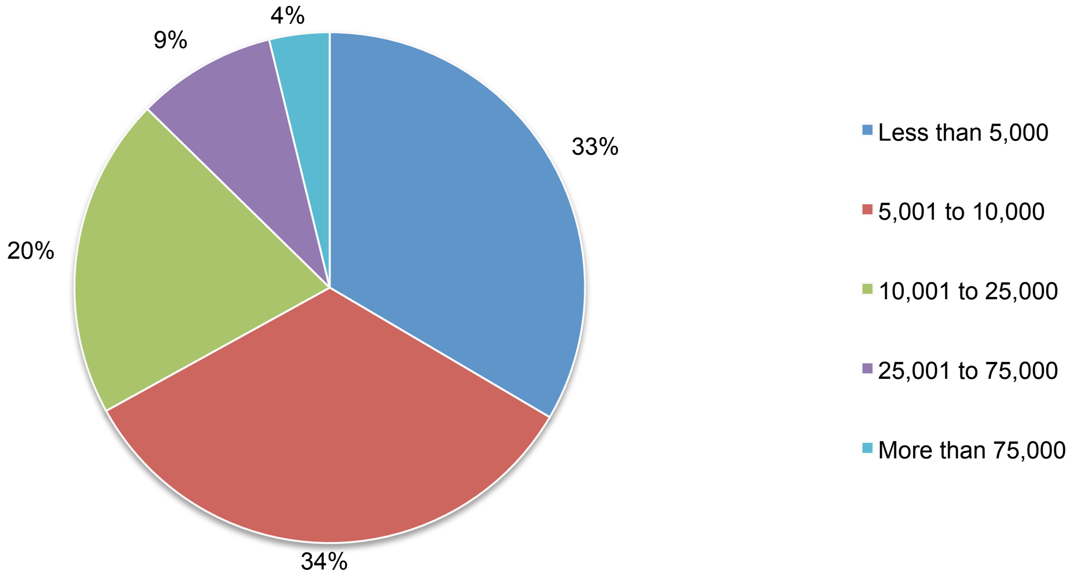
Pie Chart 3 reports the chain of command or reporting channel for respondents in the consolidated sample. As shown, 54 percent of respondents report to the chief information officer or head of corporate IT. Sixteen percent report to the chief information security officer, chief security officer or head of IT security.

Pie Chart 3: The primary person you or the IT security practitioner reports to within the organization
Consolidated view (n = 3,529)



The next pie chart shows the full time equivalent headcount or size of participating organizations in the consolidated sample containing eight separate country samples. As shown in Pie Chart 4, one third (33 percent) of respondents are located in companies with less than 5,000 employees worldwide. Another third are located in companies with more than 10,000 employees.

Pie Chart 4: Worldwide headcount
Consolidate view (n = 3,529)



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 surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals in eight countries, 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 their underlying beliefs from those who responded to our survey request.

Sampling-frame bias: The accuracy of our sample is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by our methods for compensating respondents as an incentive to complete this research.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from participants. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide an accurate or truthful response. We also acknowledge the possibility of a halo effect to questions requiring respondents to rate their organization relative to others.

Appendix: Detailed Survey Results

The following tables summarize the frequency or percentage frequency of responses to all survey questions contained in this report. Survey responses in eight countries were captured over 55 days concluding in January 2013.

Survey response	Combined
Sampling frame	107,195
Total returns	4,437
Rejected surveys	214
Screened surveys	694
Final sample	3,529
Response rate	3.3%
Sample weights	100.0%

Part 1. Screening

S1. Has your organization suffered one or more data or security breaches in the past 24 months?	Combined
Yes	3,780
No or Unsure (stop)	443
Total	4,223

S2. What best describes your level of knowledge about data or security breach incidents experienced by your organization?	Combined
Very knowledgeable	1,170
Knowledgeable	1,453
Somewhat knowledgeable	906
Minimal or no knowledge (stop)	251
Total	3,780

Part 2. Background. Strongly agree and Agree responses combined.	Combined
Q1a. My organization has the tools, personnel and funding to prevent breaches.	43%
Q1b. My organization has the tools, personnel and funding to quickly detect breaches.	44%
Q1c. My organization has the tools, personnel and funding to contain and minimize the damages caused by breaches.	40%
Q1d. My organization has the tools, personnel and funding to determine the root causes of breaches.	40%
Q1e. Understanding the root causes of breaches has strengthened my organization's security posture.	63%
Q1f. Leaders in my organization view the protection of sensitive or confidential data as a top priority.	36%
Q1g. The frequency of breaches experienced by my organization has increased over the past 24 months.	52%
Q1h. The severity of breaches experienced by my organization has increased over the past 24 months.	54%

Q2. Following are the types of data and security breach incidents experienced by many organizations. Please select the types of breach incidents experienced by your organization over the past 24 months.	Combined
System error or malfunctions	32%
Employee or contractor negligence	47%
Third party mistakes or negligence	23%
Malicious insiders	14%
External attacks (exfiltration)	24%
Other	1%
Total	141%

Q3. Please select the most significant security technologies deployed by your organization at the time of the incident to detect and/or prevent breaches? Please select the top five from the list provided below.	Combined
Anti-virus/anti-malware	15%
Anti-DDoS	14%
Data loss prevention (DLP)	45%
Firewalls (traditional)	26%
Next generation firewalls	11%
Intrusion detection & prevention	19%
Web application firewalls	12%
Virtual private network	27%
Network/traffic intelligence	44%
Security incident & event management (SIEM)	32%
Encryption technologies	48%
Forensic tools	47%
Other	2%
Total	341%

Q4. What best describes the frequency of breach incidents experienced by your organization over the past 24 months?	Combined
No change or decrease	47%
1 to 25% increase	30%
26 to 50% increase	11%
51 to 75% increase	5%
76 to 100% increase	3%
100%+ increase	4%
Total	100%
Extrapolated value	19%

Part 3. Non-malicious breach incidents

Q5. Did the breach incident result in the loss (not theft) of information assets?	Combined
Yes	48%
No (Go to Part 4)	41%
Unsure (Go to Part 4)	11%
Total	100%

Q6. Where did this breach happen?	Combined
On-premise data center	9%
Off-premise data center (including cloud)	12%
In transmission or transit to third party location	22%
Within business unit	27%
Off-site or remote location	20%
Unable to determine	9%
Total	100%

Q7. Which assets were compromised? Please select all that apply.	Combined
Physical servers	16%
Virtual servers	8%
Endpoints	63%
Databases	21%
Applications	15%
User accounts	21%
Other (please specify)	1%
Total	145%

Q8. How did the breach happen? Please check more than one if this incident involved multiple occurrences.	Combined
Employee or contractor lost a device containing sensitive or confidential data	39%
Employee or contractor was mistakenly given access to sensitive or confidential data	19%
Employee or contractor compromised sensitive or confidential data using insecure Internet applications	20%
Organization lost sensitive or confidential data contained in backup media (such as a tape)	7%
Organization experienced an error in the transmission of data to other organizations	21%
Contractors, vendors or business partners lost sensitive or confidential data entrusted to them	17%
Organization lost sensitive or confidential data because of a system or application design error	6%
Organization lost sensitive or confidential data because of a business process failure	3%
Organization failed to degauss or thoroughly wipe a device containing sensitive or confidential data	44%
Total	176%

Q9. How did your organization detect the breach?	Combined
Accidental discovery	34%
Loss prevention tool such as DLP	16%
Use of forensic methods and tools	13%
Consumer or customer complaint	7%
Notification by law enforcement	0%
Notification by partner or other third party	7%
Legal filing or complaint	1%
Detection through manual monitoring	4%
Detection through automated monitoring	13%
Audit or assessment	2%
Unsure	3%
Total	100%

Q10. From the time of the incident, when was the breach discovered? In the context of this survey, discovery occurred when the organization recognized the potential loss or theft of information assets.	Combined
Immediately after the incident	20%
Within one week after the incident	19%
Within one month after the incident	28%
Within three months after the incident	16%
Within six months after the incident	4%
Within one year after the incident	2%
Within two years after the incident	1%
More than two years after the incident	0%
Unable to determine	10%
Total	100%
Extrapolated value (days to discovery)	48.7

Q11. From the time of discovery, when was the breach adequately resolved? In the context of this survey, resolved means all investigations have been completed and the incident case closed.	Combined
Immediately after discovery	2%
Within one week after discovery	18%
Within one month after discovery	29%
Within three months after discovery	25%
Within six months after discovery	10%
Within one year after discovery	4%
Within two years after discovery	1%
More than two years after discovery	0%
Not resolved	4%
Unable to determine	7%
Total	100%
Extrapolated value (days to resolution)	82.6

Q12a. How confident are you that the investigation revealed the root cause(s) of this breach incident?	Combined
Very confident	20%
Confident	26%
Somewhat confident	19%
Not confident	36%
Total	100%

Q12b. [If confident or very confident] How did your organization determine the root cause(s)? Please select all that apply.	Combined
Existing preventive security tools	33%
Existing forensics/monitoring tools	48%
Existing security management tools	40%
Internal incident response team	11%
Third-party (external) security consultant	15%
Other (please specify)	2%
Total	149%

Q12c. [If confident or very confident] What appropriate mitigation/remediation actions did your organization take? Please select all that apply.	Combined
Update signatures	11%
Security training	36%
Update security policy	41%
System/application patching	14%
Deployment of additional preventive security tools	18%
Enhance security monitoring	26%
Recruit/build security team	13%
Other (please specify)	3%
Total	162%

Q13. Why did the organization fail to prevent this breach? Please select the top three reasons.	Combined
Inadequate enabling technologies	12%
Inadequate security processes	37%
Inadequate forensic capabilities	23%
Lack of in-house expertise	50%
Lack of accountability	20%
Poor leadership	27%
Insufficient funding	13%
Third-party vetting failure	10%
Other (please specify)	0%
Total	194%

Q14. What types of sensitive or confidential information was compromised by this breach incident?	Combined
Customer accounts	56%
Consumer data	23%
Employee records	11%
Financial information	1%
Non-financial information	3%
Source code	3%
Other proprietary information	1%
None (information was not compromised)	0%
Other (please specify)	0%
Total	100%

Q15. What best describes the nature of sensitive or confidential information compromised by this breach incident?	Combined
Structured data (such as records or files in a database program)	50%
Unstructured data (such as Word documents, spreadsheets, emails, presentations and others)	23%
Combination of both structured and unstructured data	19%
None (information was not compromised)	0%
Unsure	7%
Total	100%

Q16. How did this breach impact your organization? Please select all that apply.	Combined
Lost revenues	16%
Lost customers (churn)	30%
Lost time and productivity	33%
Regulatory fines and lawsuits	25%
Cost of outside consultants and attorneys	11%
Cost of purchased technologies	9%
Cost of notification	37%
Out-of-pocket costs to prevent harm to breach victims	32%
Lost reputation, brand value and marketplace image	39%
None (no impact)	39%
Other (please specify)	1%
Total	273%

Q17a. After the breach, did your organization make investments in enabling security technologies to prevent and/or detect future breaches?	Combined
Yes	42%
No	51%
Unsure	7%
Total	100%

Q17b. If yes, please select the most significant technology investments made by your organization after the incident to prevent and/or detect future breaches. Please select the top five from the list provided below.	Combined
Anti-virus/anti-malware	10%
Anti-DDoS	12%
Data loss prevention (DLP)	39%
Firewalls (traditional)	10%
Next generation firewalls	7%
Intrusion detection & prevention	3%
Web application firewalls	9%
Encryption	47%
Other crypto technologies (including tokenization)	39%
Virtual private network	26%
Network/traffic intelligence	28%
Security incident & event management (SIEM)	36%
Endpoint security	45%
Mobile device management	42%
Forensic tools	27%
Identity & access management	21%
Other (please specify)	0%
Total	401%

Q18a. After the breach, did your organization make changes to its operations and compliance processes to prevent and/or detect future breaches?	Combined
Yes	54%
No	28%
Unsure	18%
Total	100%

Q18b. If yes, please select the most significant areas of change made by your organization after the incident to prevent and/or detect future breaches. Please select the top five from the list provided below.	Combined
Incident response plan	57%
Incident response team	44%
Policies & procedures	52%
Monitoring & enforcement activities	32%
Data inventory and classification	9%
Communications to senior leadership (including CEO and board)	6%
Training & awareness activities	48%
Specialized education for the IT security staff	17%
Privacy and data protection leadership	12%
Cross-functional team to oversee data protection activities	28%
External audits and assessment	6%
Program certification (such as ISO 27001 or SOC 2/3)	9%
Customer or consumer redress program	9%
Data security effectiveness metrics	6%
Vendor assessments and vetting procedures	14%
Organizational restructuring	3%
Other	2%
Total	355%

Q19. In your opinion (best guess), what best describes the total economic impact of this breach incident experience by your organization?	Combined
Less than $10,000	13%
$10,001 to $50,000	14%
$50,001 to $100,000	22%
$100,001 to $250,000	19%
$250,001 to $500,000	19%
$500,001 to $1,000,000	7%
$1,000,001 to $5,000,000	4%
$5,000,001 to $10,000,000	1%
More than $10,000,000	1%
Total	100%
Extrapolated value	$0.47

Part 4. Malicious or criminal data or security breach incidents

Q20. Did the breach incident result in the theft (or attempted theft) of information assets?	Combined
Yes	91%
No (Go to Part 5)	3%
Unsure (Go to Part 5)	6%
Total	100%

Q21. Where did this breach happen?	Combined
On-premise data center	9%
Off-premise data center (including cloud)	12%
In transmission or transit to third party location	6%
Within business unit	15%
Off-site or remote location	30%
Unable to determine	28%
Total	100%

Q22. Which assets were compromised? Please select all that apply.	Combined
Physical servers	24%
Virtual servers	16%
Endpoints	30%
Databases	30%
Applications	42%
User accounts	36%
Other (please specify)	0%
Total	179%

Q23. How did the breach happen? Please check more than one if this incident involved multiple occurrences.	Combined
Targeted attacks (advanced persistent threats)	28%
Advanced malware	27%
Distributed denial of service (including botnet attacks)	15%
Spear phishing	18%
SQL injection	30%
Stolen or hijacked devices	13%
Key or certificate compromise	18%
Website hack (including business logic abuses)	16%
Total	166%

Q24. How did your organization detect the breach?	Combined
Accidental discovery	9%
Loss prevention tool such as DLP	19%
Use of forensic methods and tools	28%
Consumer or customer complaint	3%
Notification by law enforcement	15%
Notification by partner or other third party	3%
Legal filing or complaint	3%
Detection through manual monitoring	3%
Detection through automated monitoring	10%
Audit or assessment	6%
Other (please specify)	1%
Total	100%

Q25. From the time of the incident, when was the breach discovered? In the context of this survey, discovery occurred when the organization recognized the potential loss or theft of information assets.	Combined
Immediately after the incident	2%
Within one week after the incident	19%
Within one month after the incident	29%
Within three months after the incident	24%
Within six months after the incident	6%
Within one year after the incident	4%
Within two years after the incident	2%
More than two years after the incident	0%
Unable to determine	15%
Total	100%
Extrapolated value (days to discovery)	79.7

Q26. From the time of discovery, when was the breach adequately resolved? In the context of this survey, resolved means all investigations have been completed and the incident case closed.	Combined
Immediately after discovery	2%
Within one week after discovery	9%
Within one month after discovery	22%
Within three months after discovery	25%
Within six months after discovery	18%
Within one year after discovery	9%
Within two years after discovery	2%
More than two years after discovery	0%
Not resolved	6%
Unable to determine	7%
Total	100%
Extrapolated value (days to resolution)	122.7

Q27a. How confident are you that the investigation revealed the root cause(s) of this breach incident?	Combined
Very confident	17%
Confident	22%
Somewhat confident	20%
Not confident	40%
Total	100%

Q27b. [If confident or very confident] How did your organization determine the root cause(s)? Please select all that apply.	Combined
Existing preventive security tools	20%
Existing forensics/monitoring tools	55%
Existing security management tools	42%
Internal incident response team	9%
Third-party (external) security consultant	30%
Other (please specify)	1%
Total	156%

Q27c. [If confident or very confident] What appropriate mitigation/remediation actions did your organization take? Please select all that apply.	Combined
Update signatures	26%
Security training	44%
Update security policy	44%
System/application patching	43%
Deployment of additional preventive security tools	39%
Enhance security monitoring	32%
Recruit/build security team	26%
Other (please specify)	1%
Total	253%

Q28. Why did the organization fail to prevent this breach? Please select the top three reasons.	Combined
Inadequate enabling technologies	36%
Inadequate forensic capabilities	47%
Evaded existing preventive security controls	26%
Lack of in-house expertise	64%
Lack of accountability	22%
Poor leadership	19%
Insufficient funding	36%
Third-party vetting failure	19%
Other (please specify)	1%
Total	270%

Q29. What types of sensitive or confidential information was compromised by this breach incident?	Combined
Customer accounts	33%
Consumer data	6%
Employee records	7%
Financial information	8%
Non-financial information	24%
Source code	11%
Other proprietary information	8%
None (information was not compromised)	1%
Other (please specify)	0%
Total	100%

Q30. What best describes the nature of sensitive or confidential information compromised by this breach incident?	Combined
Structured data (such as records or files in a database program)	24%
Unstructured data (such as Word documents, spreadsheets, emails, presentations and others)	39%
Combination of both structured and unstructured data	28%
None (information was not compromised)	0%
Unsure	8%
Total	100%

Q31. How did this breach impact your organization? Please select all that apply.	Combined
Lost revenues	20%
Lost customers (churn)	14%
Lost time and productivity	71%
Regulatory fines and lawsuits	5%
Cost of outside consultants and attorneys	17%
Cost of purchased technologies	35%
Cost of notification	6%
Out-of-pocket costs to prevent harm to breach victims	14%
Lost reputation, brand value and marketplace image	45%
None (no impact)	23%
Other (please specify)	1%
Total	250%

Q32a. After the breach, did your organization make investments in enabling security technologies to prevent and/or detect future breaches?	Combined
Yes	65%
No	31%
Unsure	5%
Total	100%

Q32b. If yes, please select the most significant technology investments made by your organization after the incident to prevent and/or detect future breaches. Please select the top five from the list provided below.	Combined
Anti-virus/anti-malware	21%
Anti-DDoS	33%
Data loss prevention (DLP)	30%
Firewalls (traditional)	9%
Next generation firewalls	25%
Intrusion detection & prevention	31%
Web application firewalls	42%
Encryption	47%
Other crypto technologies (including tokenization)	26%
Virtual private network	27%
Network/traffic intelligence	41%
Security incident & event management (SIEM)	47%
Endpoint security	38%
Mobile device management	15%
Forensic tools	35%
Identity & access management	22%
Other (please specify)	1%
Total	490%

Q33a. After the breach, did your organization make changes to its operations and compliance processes to prevent and/or detect future breaches?	Combined
Yes	63%
No	22%
Unsure	15%
Total	100%

Q33b. If yes, please select the most significant areas of change made by your organization after the incident to prevent and/or detect future breaches. Please select the top five from the list provided below.	Combined
Incident response plan	28%
Incident response team	16%
Policies & procedures	16%
Monitoring & enforcement activities	55%
Data inventory and classification	3%
Communications to senior leadership (including CEO and board)	7%
Training & awareness activities	37%
Specialized education for the IT security staff	49%
Privacy and data protection leadership	7%
Cross-functional team to oversee data protection activities	9%
External audits and assessment	12%
Program certification (such as ISO 27001 or SOC 2/3)	29%
Customer or consumer redress program	3%
Data security effectiveness metrics	18%
Vendor assessments and vetting procedures	35%
Organizational restructuring	6%
Other (please specify)	1%
Total	331%

Q34. In your opinion (best guess), what best describes the total economic impact of this breach incident experience by your organization?	Combined
Less than $10,000	0%
$10,001 to $50,000	7%
$50,001 to $100,000	13%
$100,001 to $250,000	17%
$250,001 to $500,000	19%
$500,001 to $1,000,000	32%
$1,000,001 to $5,000,000	11%
$5,000,001 to $10,000,000	2%
More than $10,000,000	0%
Total	100%
Extrapolated value (US$ millions)	$0.84

Part 5. Lessons learned

Q35a. Did the breaches experienced by your organization result in an increase in its spending level or budget dedicated to data security?	Combined
Yes	61%
No	33%
Unsure	6%
Total	100%

Q35b. If yes, how much is this increase in percentage terms?	Combined
< 5%	19%
5% to 10%	31%
10% to 25%	23%
26% to 50%	16%
51% to 75%	10%
> 75%	1%
Total	100%
Extrapolated value	20%

Q36a. Did the breaches experienced by your organization result in an increase in its spending on forensic capabilities?	Combined
Yes	52%
No	42%
Unsure	6%
Total	100%

Q36b. If yes, how much is this increase in percentage terms?	Combined
< 5%	9%
5% to 10%	19%
10% to 25%	22%
26% to 50%	26%
51% to 75%	13%
> 75%	12%
Total	100%
Extrapolated value	33%

	Combined
Q37a. How important is a thorough post-breach analysis and forensic investigation to minimizing the negative consequences of a non-malicious breach? Essential and Very important responses combined.	57%

	Combined
Q37b. How important is a thorough post-breach analysis and forensic investigation to minimizing the negative consequences of a malicious or criminal breach?	64%

Part 6. Organization and respondents' demographics

D1. What best describes your position level within the organization?	Combined
Executive/VP	3%
Director	15%
Manager	18%
Supervisor	14%
Staff/technician	31%
Administrative	10%
Consultant/contractor	6%
Other	3%
Total	100%

D2. What best describes your direct reporting channel?	Combined
CEO/executive committee	2%
COO or head of operations	1%
CFO, controller or head of finance	2%
CIO or head of corporate IT	54%
Business unit leader or general manager	13%
Head of compliance or internal audit	8%
CISO/CSO or head of IT security	16%
Other	1%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Combined
Less than 5,000	33%
5,001 to 10,000	34%
10,001 to 25,000	20%
25,001 to 75,000	9%
More than 75,000	4%
Total	100%
Extrapolated value (headcount)	14,389

D4. What best describes your organization's primary industry classification?	Combined
Financial services	18%
Federal & central government	11%
State, province & local government	4%
Energy & utilities	2%
Education & research	2%
Transportation	1%
Consumer products	4%
Industrial products & chemicals	5%
Pharmaceuticals & biotech	2%
Healthcare & medical devices	2%
Defense contractor	3%
Hospitality	4%
Entertainment & media	4%
Technology & software	3%
Services	7%
Professional services	6%
Retail, Internet	7%
Retail, conventional	3%
Communications	4%
Other	1%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

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.