2014: A Year of Mega Breaches

Sponsored by Identity Finder

Independently conducted by Ponemon Institute LLC

Publication Date: January 2015

2014: A Year of Mega Breaches

Ponemon Institute, January 2015

Part 1. Introduction

2014 will long be remembered for a series of mega security breaches and attacks starting with the Target breach in late 2013 and ending with Sony Pictures Entertainment. In the case of the Target breach, 40 million credit and debit cards were stolen and 70 million records were stolen that included the name, address, email address and phone number of Target shoppers. Sony suffered a major online attack that resulted in employees' personal data and corporate correspondence being leaked. The financial consequences and reputation damage of both breaches have been widely reported.

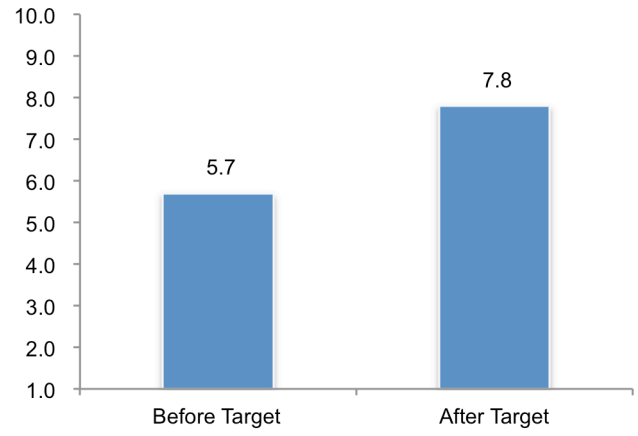
Other well-publicized mega breaches in 2014 in order of magnitude were:

- eBay (145 million people affected)
- JPMorgan Chase & Co. (76 million households and 7 million small businesses affected)
- Home Depot (56 million unique payment cards)
- CHS community Health Systems (4.5 million people affected)
- Michaels Stores (2.6 million people affected)
- Nieman Marcus (1.1 million people affected)
- Staples (point-of-sales systems at 115 of its more than 1,400 retail stores)

2015 is predicted to be as bad or worse as more sensitive and confidential information and transactions are moved to the digital space and become vulnerable to attack. Will companies be prepared to deal with cyber threats? Are they taking steps to strengthen their cyber security posture? Ponemon Institute, with sponsorship from Identity Finder, conducted *2014: A Year of Mega Breaches* to understand if and how organizations have changed their data protection practices as a result of these breaches.

Figure 1. Management's concern about breach

Percentage concern level on a 10-point scale



As noted in Figure 1, respondents believe security incidents such as Target and other mega breaches raised senior managements' level of concern about how cyber crimes might impact their organizations.

We surveyed 735 IT and IT security practitioners about the impact of the Target and other mega breaches on their IT budgets and compliance practices as well as data breaches their companies experienced. The participants in this study are knowledgeable about data or security breach incidents experienced by their companies. They are also very informed about the facts surrounding the Target and other mega breaches.

Following are key steps companies have taken because of mega breaches:

- **More resources are allocated to preventing, detecting and resolving data breaches**. According to respondents, the Target breach did have a significant impact on the their

organizations' cyber defense. Sixty-one percent of respondents say the budget for security increased by an average of 34 percent. Most was used for SIEM, endpoint security and intrusion detection and prevention.

- **Senior management gets a wake up call and realizes the need for a stronger cyber defense posture**. More companies have the tools and personnel to do the following: prevent the breach (65 percent of respondents), detect the breach (69 percent of respondents), contain and minimize the breach (72 percent of respondents) and determine the root cause of the breach (55 percent of respondents). Sixty-seven percent of respondents say their organization made sure the IT function had the budget necessary to defend it from data breaches.

- **Operations and compliance processes are changing to prevent and detect breaches.** Sixty percent of respondents say they made changes to operations and compliance processes to establish incident response teams, conduct training and awareness programs and use data security effectiveness measures.

- **Many companies fail to prevent the breach with the technology they currently have.** With new investments, companies will hopefully prevent more data breaches. However, 65 percent of respondents say the attack evaded existing preventive security controls. Forty-six percent say the breach was discovered by accident.

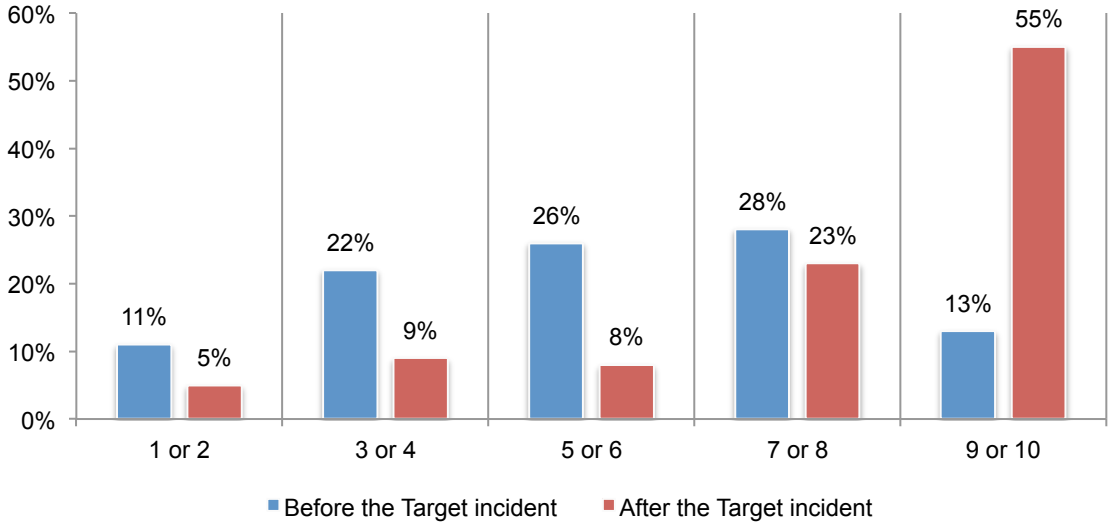
- **Companies confident of understanding the root cause of the breach had incident response teams in place**. They also had the right security management tools and the expertise of a security consultant to help determine the root cause. After knowing the root cause, these companies stepped up their security training and enhanced their security monitoring practices.

Part 2. Key findings

In this section, we provide an analysis of the findings. The complete audited findings are presented in the appendix of the report. The study covers two topics: how mega breaches influenced companies' efforts to strengthen their security posture and how companies represented in this study responded to their own data breaches in 2014.

The Target breach was a wake up call for senior management. Before the Target breach, respondents rate their companies' level of concern as average, as shown in Figure 2. After the Target incident, respondents say it became much more of a concern for senior management. Fifty-five percent of respondents rate senior management's concern as extremely high. Prior to the Target breach, only 13 percent of respondents believed senior management was extremely concerned.

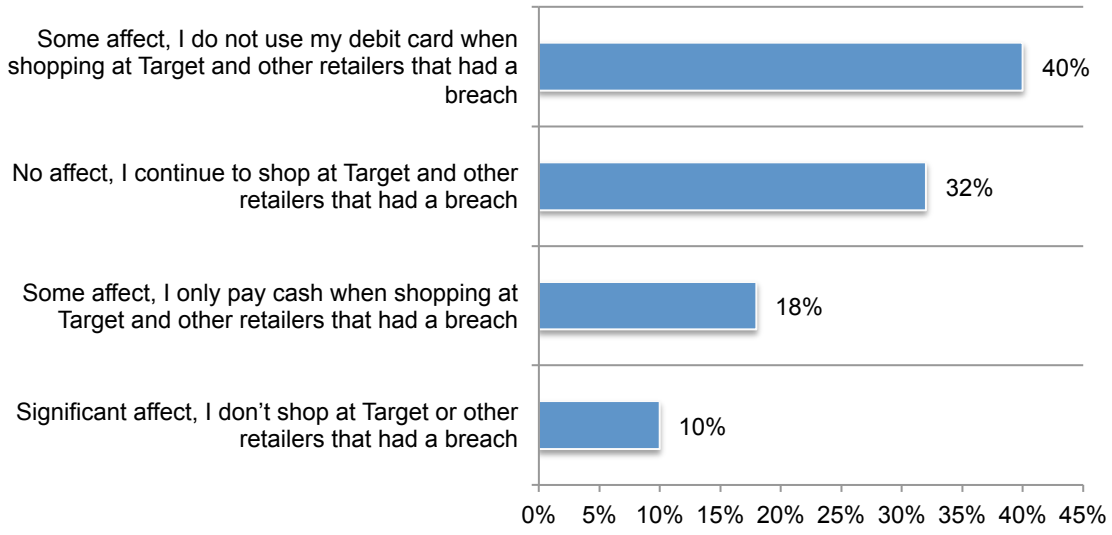
Figure 2. Senior management's concerns about a data breach rose dramatically
Extrapolated value before the Target incident = 5.7, after the Target incident = 7.8
Percentage concern level on a 10-point scale



As consumers, how did IT practitioners respond to mega breaches? Our respondents are more knowledgeable than the average consumer about the security practices of retailers. In the aftermath of the Target breach, we asked respondents if they changed their shopping habits because of concerns about having personal information stolen.

Approximately 90 percent of IT practitioners/consumers (40 percent + 32 percent + 18 percent) say they did not stop shopping at Target and other retailers that experienced a data breach. However, many did change how they paid for the items they purchased. Forty percent of respondents say they stopped using their debit card when shopping and 18 percent say they now only pay cash.

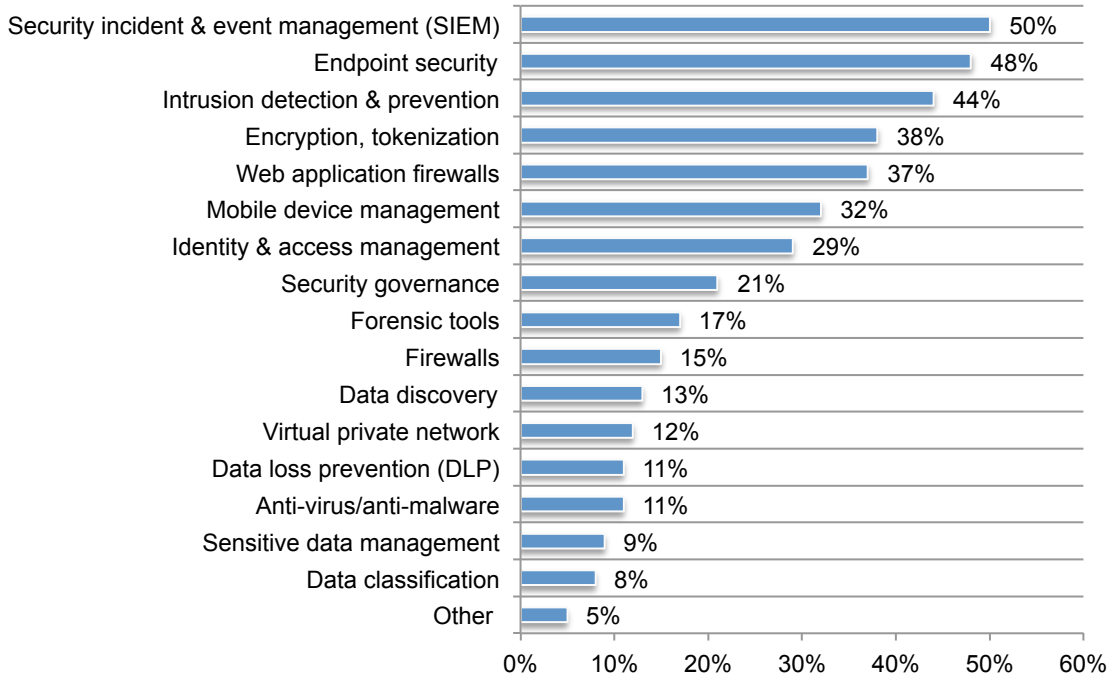
Figure 3. How mega breaches affected respondents' shopping habits



More resources were allocated to preventing, detecting and resolving data breaches. According to respondents, mega breaches did have a significant impact on the their organizations' security posture. Sixty-one percent of respondents say the budget for security increased by an average of 34 percent. Sixty-three percent of respondents say this increase in budget resulted in investments in enabling security technologies to prevent and/or detect breaches.

According to Figure 4, the top five technology investments are: security incident & event management (SIEM), endpoint security, intrusion detection and prevention, encryption/tokenization and web application firewalls. Only 9 percent of respondents say they invested in sensitive data management and 8 percent invested in data classification. This suggests that companies are not taking steps to make sure their information is properly managed to minimize the damage from future data breaches.

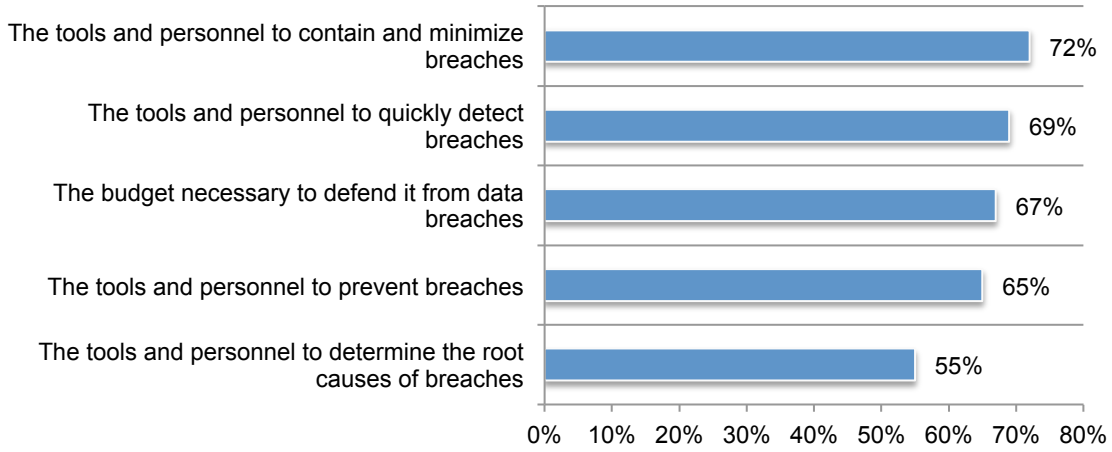
Figure 4. Technology investments made in response to mega breaches



Senior management realizes the need for a stronger cyber defense posture. As shown in Figure 5, the majority of respondents say well-publicized mega breaches resulted in providing tools and personnel to deal with data breaches.

The tools and personnel to improve their companies' security posture include the following: contain and minimize the breach (72 percent of respondents), detect the breach (69 percent of respondents), prevent the breach (65 percent of respondents), and determine the root cause of the breach (55 percent of respondents). Sixty-seven percent of respondents say their organization made sure the IT function had the budget necessary to defend it from data breaches.

Figure 5. Following mega breaches my company provided tools and personnel to prevent and detect data breaches
Strongly agree and agree responses combined



Companies have changed their operations and compliance processes. Sixty percent of respondents say they made changes to operations and compliance processes to improve their ability to prevent and detect breaches.

The most common changes, as shown in Figure 6, were the following: creation of an incident response team (56 percent of respondents), conduct training and awareness activities (50 percent of respondents), new policies and procedures (48 percent of respondents) and use of data security effectiveness metrics (48 percent of respondents).

Figure 6. Most significant changes to operations and compliance
Four choices permitted

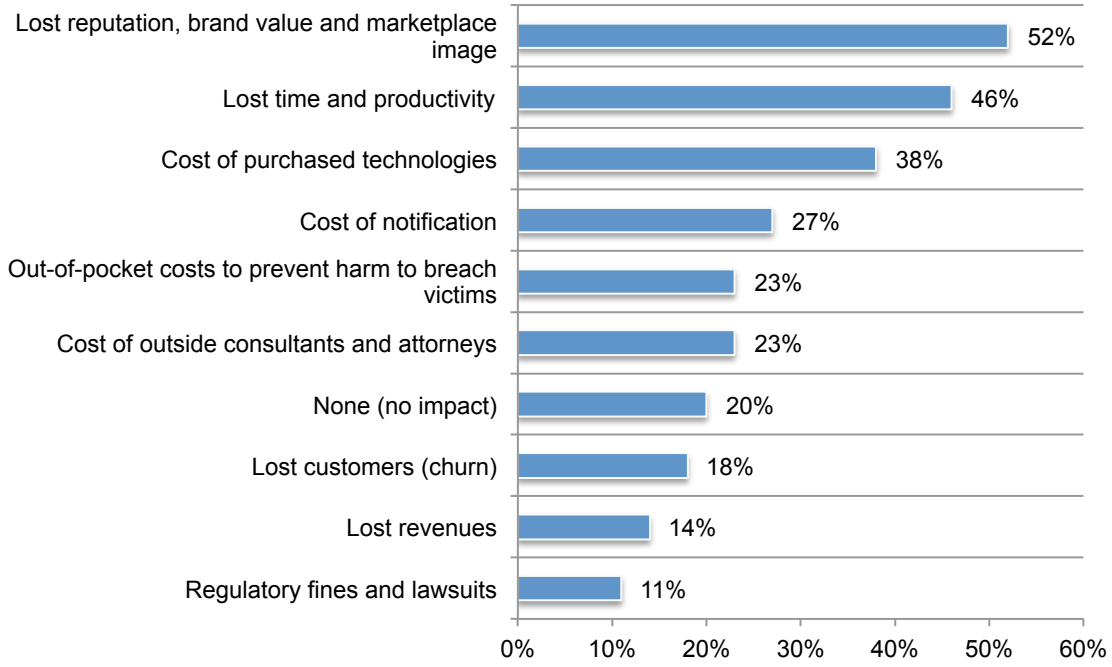
How companies responded to their own data breaches

In the context of this survey, we defined a data breach as the loss or theft of information assets including intellectual property such as trade secrets, contact lists, business plans and source code. Data breaches happen for various reasons including human errors and system glitches. They also happen as a result of malicious attacks, hactivism, or criminal attacks that seek to obtain valuable data (a.k.a. exfiltration).

Forty-five percent of respondents report their company had one or more data breaches in the past 24 months. We asked these respondents a series of questions about the one data breach that had the most serious economic impact on their companies. These findings are presented below. While these were not mega breaches, the study illustrates the difficulty all companies have in preventing and detecting a data breach.

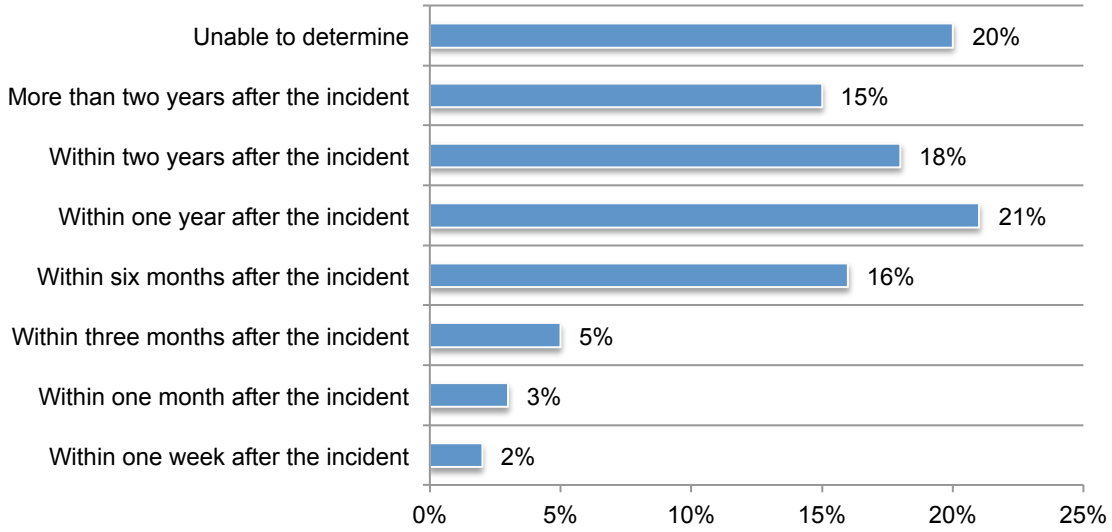
Lost reputation is the number one consequence of the data breaches experienced by companies in this study. Companies in this study can identify with the Target and Sony breaches. According to Figure 7, 52 percent of respondents say reputation loss, brand value and marketplace image was the biggest impact of the data breach. This is followed by lost time and productivity to deal with the data breach (46 percent of respondents). Only 20 percent say there was no impact on the company.

Figure 7. How did the data breach affect your company?
More than one response permitted



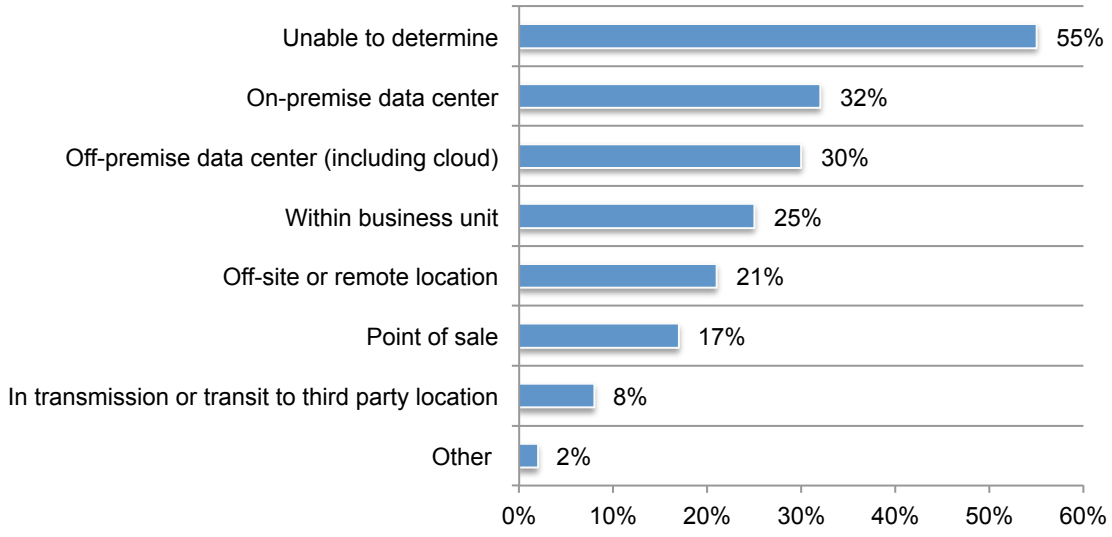
Organizations are not able to detect a breach in a timely manner. As shown in Figure 8, it took one-third of the organizations (18 percent + 15 percent) represented in this research to discover the breach two or more years after the incident. Twenty percent are not able to determine when the breach was discovered making it difficult to determine the extent of the breach and the root cause.

Figure 8. When was the breach discovered?



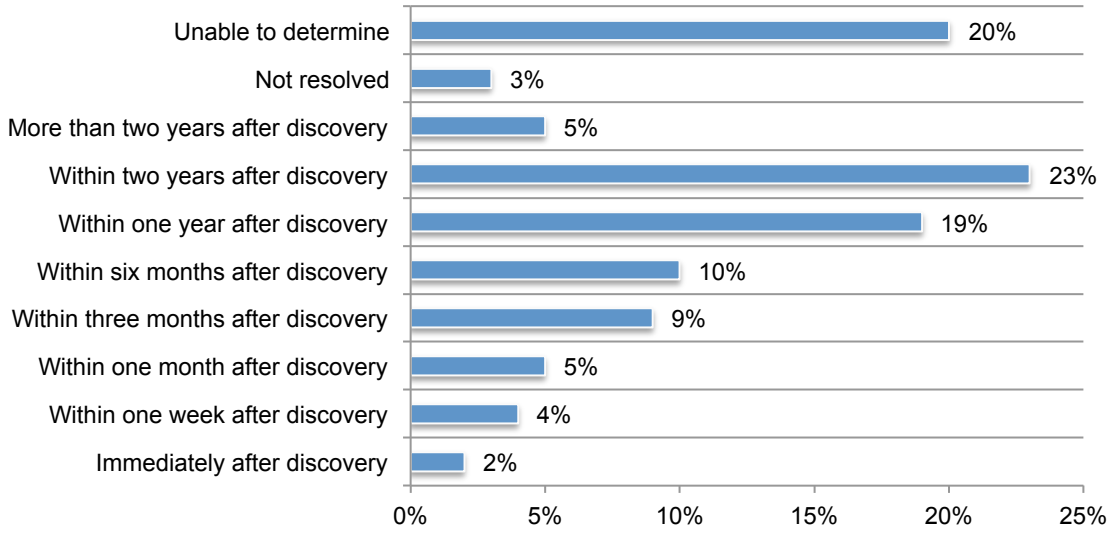
Many organizations were not able to determine where the breach occurred. As shown in Figure 9, 55 percent of respondents say they were unable to determine the location of the breach. If they did it was the on-premise data center (32 percent of respondents) and 30 percent say it was at an off-premise data center (including cloud).

Figure 9. Where did the breach happen?
Select all that apply



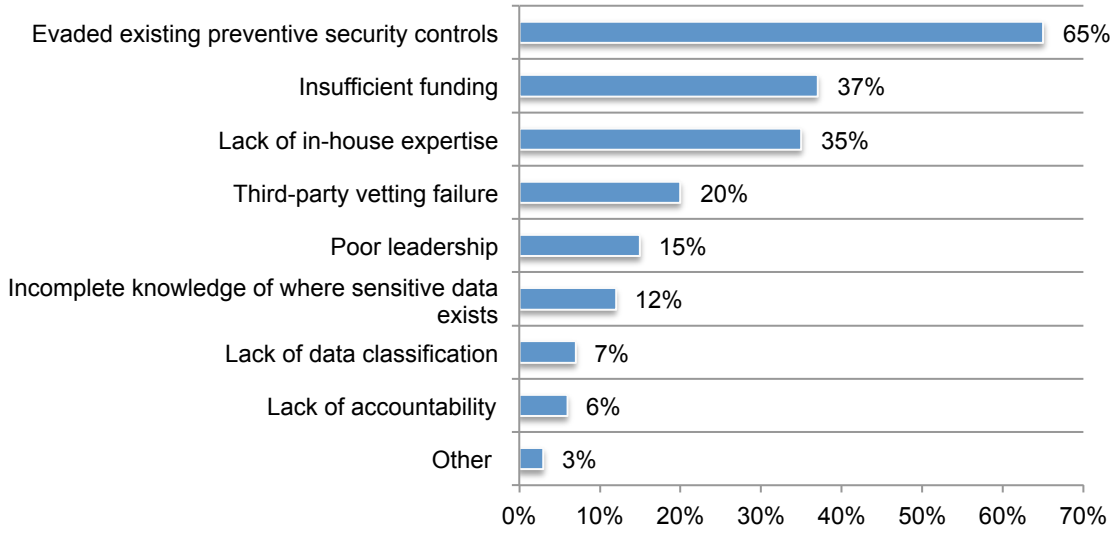
Organizations are not able to quickly resolve the data breach. As shown in Figure 10, it can take years to resolve the consequences of a data breach and 20 percent of respondents say they are not able to determine if the breach was ever resolved.

Figure 10. When was the breach resolved?



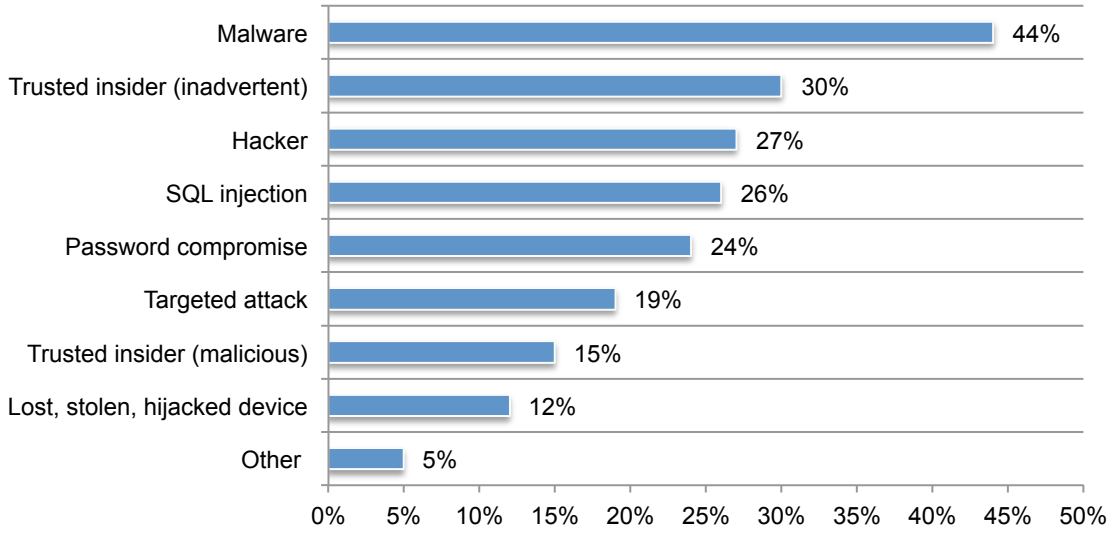
Could IT have stopped the data breach? Fifty percent say they should have been able to prevent the breach with the technology they currently have. Figure 11 reveals the main reasons why the organization failed to stop the breach: the attack evaded existing preventive security controls (65 percent), insufficient funding (37 percent) and lack of in-house expertise (35 percent).

Figure 11. Why did IT fail to stop the data breach?
Two responses permitted



Most breaches were caused by malware (44 percent of respondents). Figure 12 shows the other root causes: a trusted but negligent insider (30 percent) and hacker (27 percent). This is followed by SQL injection (26 percent) and password compromise (24 percent).

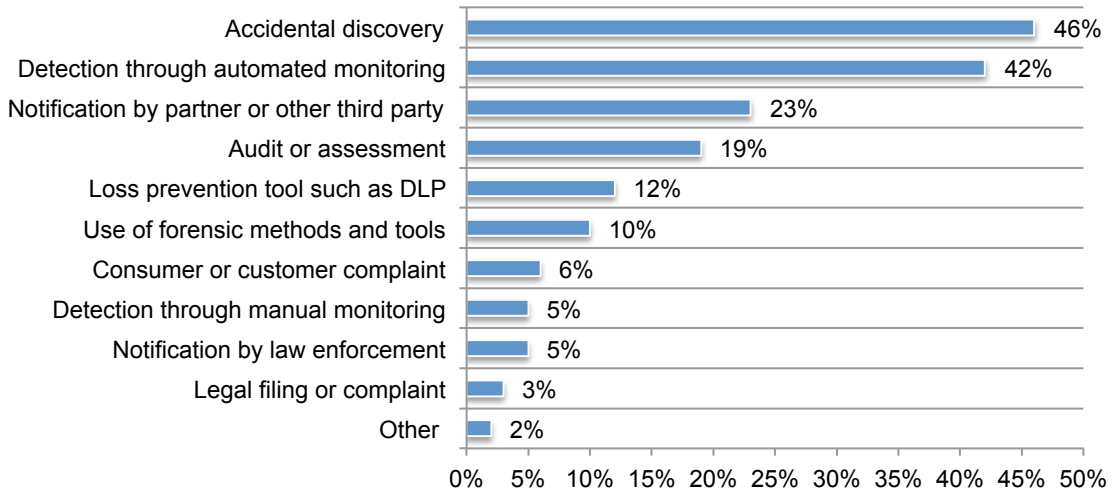
Figure 12. What was the root cause of the breach?
More than one response permitted



Most breaches are difficult to detect, resolve and determine the root cause. On a positive note, mega breaches have driven an increase in budgets, technologies and tools to prevent, detect and contain the impact of breaches. However, the companies in this study reveal the problems they have mitigating the risk and consequences of a data breach.

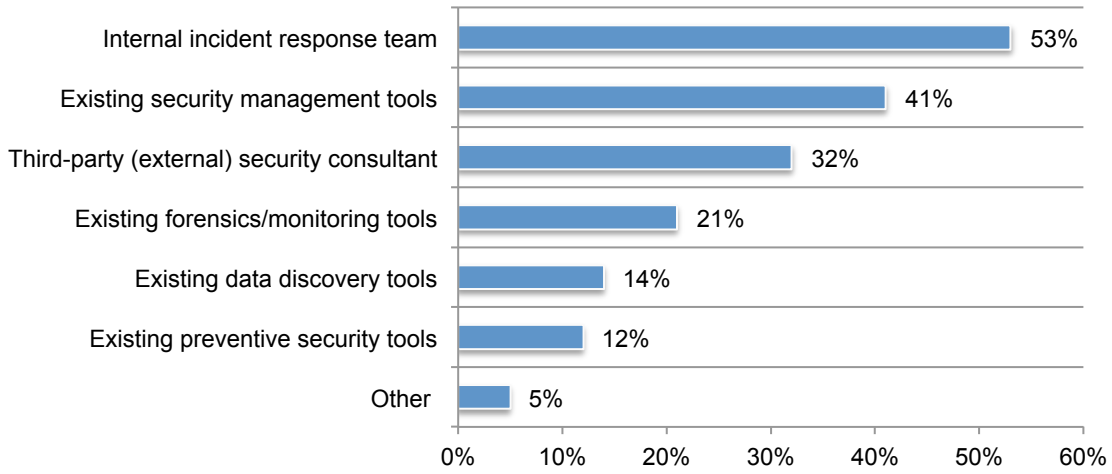
Specifically, as shown in Figure 13, most respondents (46 percent) say the breach was discovered accidentally. Forty-two percent say it was through the use of automated monitoring.

Figure 13. How was the breach detected?
More than one response permitted



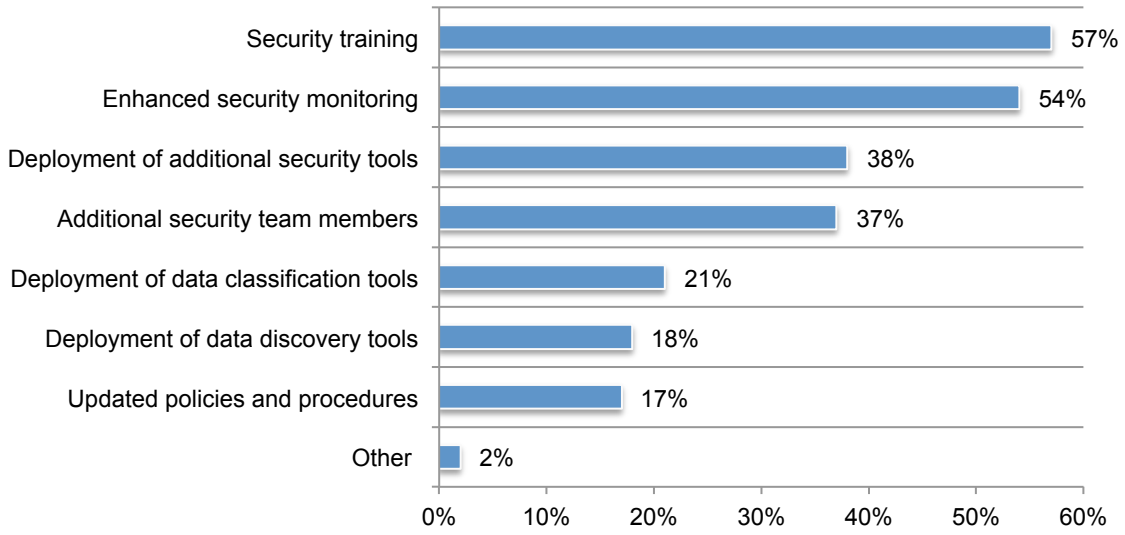
Forty-six percent of respondents say they are not confident that their investigations revealed the root cause of the breach. If they are confident or very confident (31 percent of respondents), it was because of an internal incident response team (53 percent), existing security management tools (41 percent) or a third-party security consultant (32 percent), as shown in Figure 14.

Figure 14. How was the root cause determined?
More than one response permitted



The following are the mitigation or remediation actions in those companies confident they know the root cause of the data breach: security training (57 percent), enhanced security monitoring (54 percent), deployment of additional security tools (38 percent) and additional security team members (37 percent), as revealed in Figure 15.

Figure 15. After knowing the root cause, what actions did the company take?
More than one response permitted



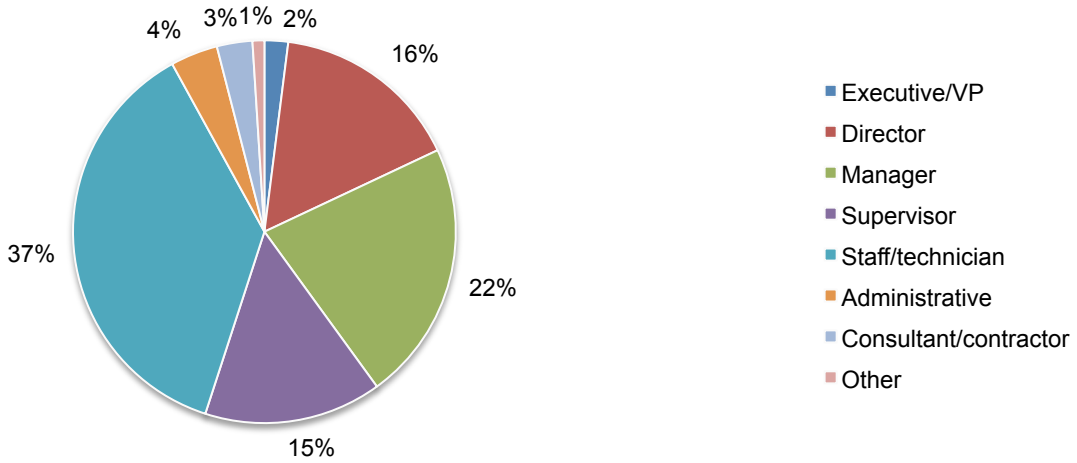
Part 3. Methods

A sampling frame composed of 20,003 IT and IT security practitioners located in the United States and who are familiar with data or security breach incidents experienced by their companies were selected for participation in this survey. As shown in Table 1, 798 respondents completed the survey. Screening removed 63 surveys. The final sample was 735 surveys (or a 3.7 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	20,003	100.0%
Total returns	798	4.0%
Rejected or screened surveys	63	0.3%
Final sample	735	3.7%

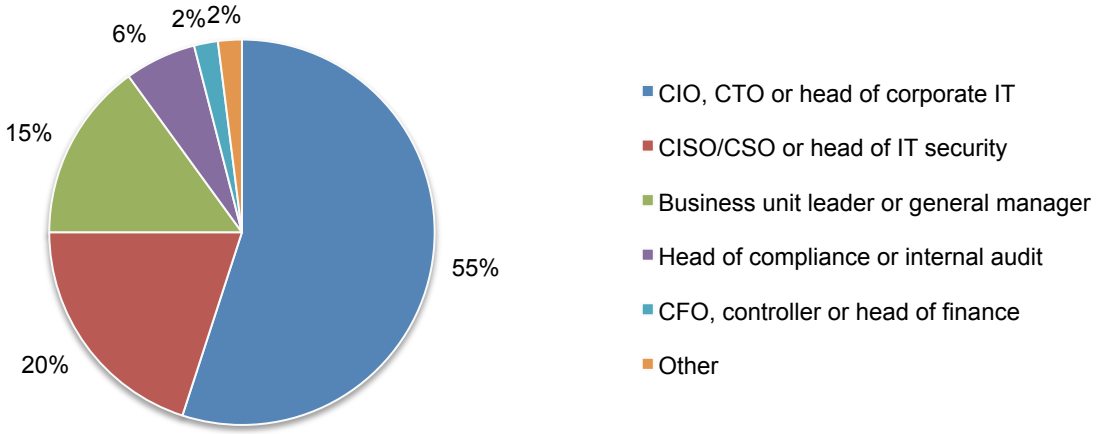
Pie chart 1 reports the current position or organizational level of the respondents. As shown in Pie Chart 1, more than half of respondents (55 percent) reported their position as supervisory or above.

Pie Chart 1. Current position or organizational level



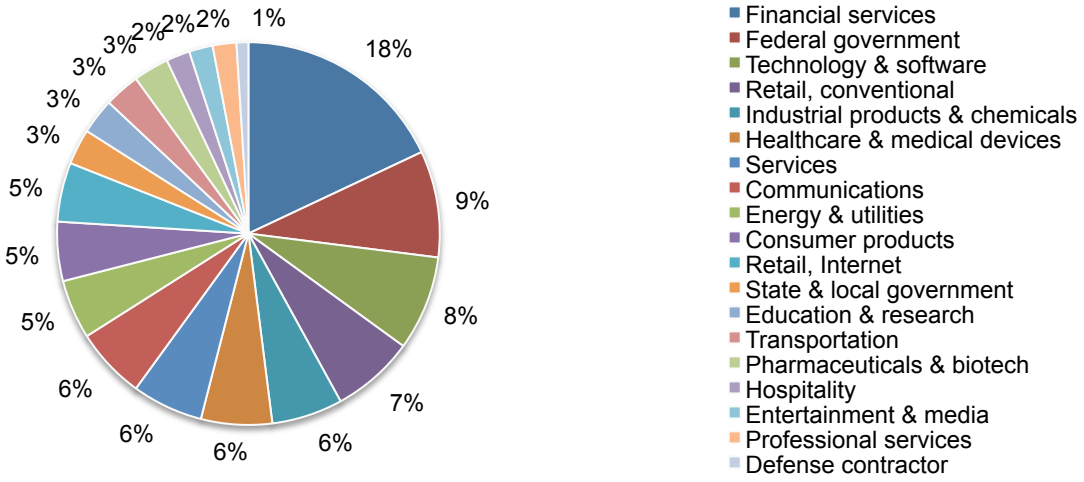
Pie Chart 2 identifies the primary person the respondent reports to. Fifty-five percent of respondents identified the chief information officer or head of corporate IT as the person they report to. Another 20 percent indicated the CISO/CSO or head of IT security.

Pie Chart 2. Direct reporting channel



Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by federal government (9 percent) and technology and software (8 percent).

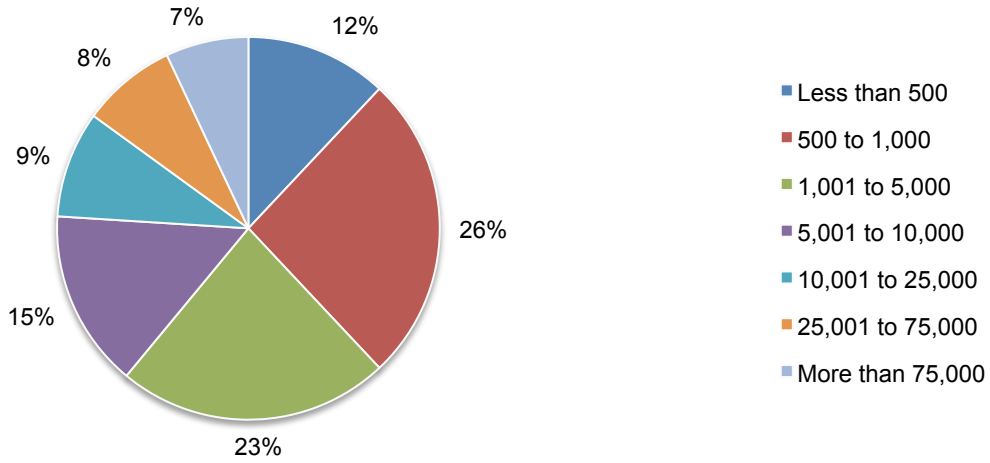
Pie Chart 3. Primary industry classification



According to Pie Chart 4, more than half of the respondents (62 percent) are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 4. Worldwide headcount of the organization

Extrapolated value = 13,233



Part 4. 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 IT or IT security practitioners in various organizations in the United States. 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 November 2014.

Survey response	Freq	Pct%
Total sample frame	20,003	100.0%
Total survey returns	798	4.0%
Rejected or screened surveys	63	0.3%
Final sample	735	3.7%

Part 1. Screening

S1. What best describes your level of knowledge about data or security breach incidents experienced by your organization?	Pct%
Very knowledgeable	54%
Knowledgeable	34%
Somewhat knowledgeable	12%
Minimal or no knowledge (stop)	0%
Total	100%

S2. What best describes your level of knowledge about the Target breach that occurred approximately one year ago?	Pct%
Very knowledgeable	43%
Knowledgeable	46%
Somewhat knowledgeable	11%
Minimal or no knowledge (stop)	0%
Total	100%

Part 2. Background.

Q1. As a consumer, how did the Target breach affect your shopping habits?	Pct%
No affect, I continue to shop at Target and other retailers that had a breach	32%
Some affect, I do not use my debit card when shopping at Target and other retailers that had a breach	40%
Some affect, I only pay cash when shopping at Target and other retailers that had a breach	18%
Significant affect, I don't shop at Target or other retailers that had a breach	10%
Other (please specify)	0%
Total	100%

Q2. Please rate the impact that the Target breach had on your company's cyber security defense using the following 10-point scale, where 1 = no impact to 10 = significant impact.	Pct%
1 or 2	5%
3 or 4	12%
5 or 6	19%
7 or 8	26%
9 or 10	38%
Total	100%
Extrapolated value	7.10

Q3. In your opinion, how concerned were your organization's leaders about data breaches **before** the Target incident? Please rate their level of concern using the 10-point scale from 1 = none to 10 = significant concern.	Pct%
1 or 2	11%
3 or 4	22%
5 or 6	26%
7 or 8	28%
9 or 10	13%
Total	100%
Extrapolated value	5.70

Q4. In your opinion, how concerned are your organization's leaders about data breaches **after** the Target incident? Please rate their level of concern using the 10-point scale from 1 = none to 10 = significant concern.	Pct%
1 or 2	5%
3 or 4	9%
5 or 6	8%
7 or 8	23%
9 or 10	55%
Total	100%
Extrapolated value	7.78

Attributions: Following are statements pertaining to the Target breach and subsequent large retail breaches. Please rate each statement using the five-point scale provided below each item.	
Q5. Following the Target breach, my organization made sure it had the tools and personnel to **prevent** breaches.	Pct%
Strongly agree	33%
Agree	32%
Unsure	18%
Disagree	14%
Strongly disagree	3%
Total	100%

Q6. Following the Target breach, my organization made sure it had the tools and personnel to **quickly detect** breaches.	Pct%
Strongly agree	40%
Agree	29%
Unsure	16%
Disagree	13%
Strongly disagree	2%
Total	100%

Q7. Following the Target breach, my organization made sure it had the tools and personnel to **contain and minimize breaches.**	Pct%
Strongly agree	43%
Agree	29%
Unsure	15%
Disagree	11%
Strongly disagree	2%
Total	100%

Q8. Following the Target breach, my organization made sure it had the tools and personnel to **determine the root causes of breaches.**	Pct%
Strongly agree	30%
Agree	25%
Unsure	21%
Disagree	16%
Strongly disagree	8%
Total	100%

Q9. Following the Target breach, my organization made sure it had the budget necessary to defend it from data breaches.	Pct%
Strongly agree	33%
Agree	34%
Unsure	15%
Disagree	13%
Strongly disagree	5%
Total	100%

Q10a. After the Target breach, did your organization increase its investments in enabling security technologies to prevent and/or detect breaches?	Pct%
Yes	63%
No	30%
Unsure	7%
Total	100%

Q10b. If yes, please select the most significant technology investments made by your organization after the Target breach. Please provide your top 4 choices.	Pct%
Anti-virus/anti-malware	11%
Data discovery	13%
Data classification	8%
Data loss prevention (DLP)	11%
Firewalls	15%
Sensitive data management	9%
Intrusion detection & prevention	44%
Web application firewalls	37%
Encryption, tokenization	38%
Security governance	21%
Virtual private network	12%
Security incident & event management (SIEM)	50%
Endpoint security	48%
Mobile device management	32%
Forensic tools	17%
Identity & access management	29%
Other (please specify)	5%
Total	400%

Q11a. After the Target breach, did your organization make changes to its operations and compliance processes to prevent and/or detect breaches?	Pct%
Yes	60%
No	35%
Unsure	5%
Total	100%

Q11b. If yes, please select the most significant changes to operations and compliance made by your organization after the Target breach. Please provide your top 4 choices.	Pct%
Incident response team	56%
Policies & procedures	48%
Monitoring & enforcement activities	41%
Data inventory and classification	12%
Communications to senior leadership (including CEO and board)	36%
External audits and assessment	11%
Customer or consumer redress program	8%
Data security effectiveness metrics	48%
Training & awareness activities	50%
Specialized education for the IT security staff	47%
Privacy and data protection leadership	30%
Reducing sensitive enterprise data	8%
Other (please specify)	5%
Total	400%

Q12. What percentage of your IT security budget is dedicated to the detection and containment of data breaches?	Pct%
Less than 1%	0%
1 to 10%	10%
11 to 20%	25%
21 to 40%	38%
41 to 60%	15%
61 to 80%	8%
More than 80%	4%
Total	100%
Extrapolated value	32%

Q13a. Did your organization's budget or spending level on security increase after the Target breach?	Pct%
Yes	61%
No	34%
Unsure	5%
Total	100%

Q13b. If yes, please estimate the percentage increase in the budget or spending level as a result of the Target breach.	Pct%
Less than 1%	0%
1 to 5%	2%
6 to 10%	5%
11 to 20%	11%
21 to 30%	20%
31 to 40%	23%
41 to 50%	29%
More than 50%	10%
Total	100%
Extrapolated value	34%

Part 3. Data breach incidents experienced by your organization

Q14. Did the breach incident result in the theft (or attempted theft) of data or technology assets?	Pct%
Yes	45%
No	43%
Unsure	12%
Total	100%

Q15. Where did this breach happen? Please select all that apply.	Pct%
On-premise data center	32%
Off-premise data center (including cloud)	30%
In transmission or transit to third party location	8%
Within business unit	25%
Off-site or remote location	21%
Point of sale	17%
Unable to determine	55%
Other (please specify)	2%
Total	190%

Q16. Which IT assets were compromised? Please select all that apply.	Pct%
Physical servers	15%
Virtual servers	2%
Desktops	25%
Databases	36%
Applications	34%
User accounts	41%
Cloud storage	18%
Files	29%
Emails	13%
Laptops	15%
Mobile devices	13%
Websites	34%
SharePoint	5%
Removable storage devices (USB drive)	8%
Other (please specify)	2%
Total	290%

Q17. How did the breach happen? Please check more than one if this incident involved multiple occurrences.	Pct%
Trusted insider (malicious)	15%
Trusted insider (inadvertent)	30%
Hacker	27%
Password compromise	24%
Targeted attack	19%
Malware	44%
Lost, stolen, hijacked device	12%
SQL injection	26%
Other (please specify)	5%
Total	202%

Q18. Do you have technology that should have prevented the data breach?	Pct%
Yes	50%
No	35%
Unsure	15%
Total	100%

Q19. How did your organization detect the breach?	Pct%
Accidental discovery	46%
Loss prevention tool such as DLP	12%
Use of forensic methods and tools	10%
Consumer or customer complaint	6%
Notification by law enforcement	5%
Notification by partner or other third party	23%
Legal filing or complaint	3%
Detection through manual monitoring	5%
Detection through automated monitoring	42%
Audit or assessment	19%
Other (please specify)	2%
Total	173%

Q20. 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.	Pct%
Immediately after the incident	0%
Within one week after the incident	2%
Within one month after the incident	3%
Within three months after the incident	5%
Within six months after the incident	16%
Within one year after the incident	21%
Within two years after the incident	18%
More than two years after the incident	15%
Unable to determine	20%
Total	100%

Q21. 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.	Pct%
Immediately after discovery	2%
Within one week after discovery	4%
Within one month after discovery	5%
Within three months after discovery	9%
Within six months after discovery	10%
Within one year after discovery	19%
Within two years after discovery	23%
More than two years after discovery	5%
Not resolved	3%
Unable to determine	20%
Total	100%

Q22a. How confident are you that the investigation revealed the root cause(s) of this breach incident?	Pct%
Very confident	13%
Confident	18%
Somewhat confident	23%
Not confident	46%
Total	100%

Q22b. [If confident or very confident] How did your organization determine the root cause(s)? Please select all that apply.	Pct%
Existing preventive security tools	12%
Existing data discovery tools	14%
Existing forensics/monitoring tools	21%
Existing security management tools	41%
Internal incident response team	53%
Third-party (external) security consultant	32%
Other (please specify)	5%
Total	178%

Q22c. [If confident or very confident] What appropriate mitigation/remediation actions did your organization take? Please select all that apply.	Pct%
Security training	57%
Updated policies and procedures	17%
Deployment of additional security tools	38%
Deployment of data discovery tools	18%
Deployment of data classification tools	21%
Enhanced security monitoring	54%
Additional security team members	37%
Other (please specify)	2%
Total	244%

Q23. Why did the organization fail to prevent this breach? Please select the top two reasons.	Pct%
Incomplete knowledge of where sensitive data exists	12%
Lack of data classification	7%
Evaded existing preventive security controls	65%
Lack of in-house expertise	35%
Lack of accountability	6%
Poor leadership	15%
Insufficient funding	37%
Third-party vetting failure	20%
Other (please specify)	3%
Total	200%

Q24. What types of sensitive or confidential information was compromised by this breach incident?	Pct%
Customer accounts	68%
Consumer data	65%
Employee/HR data	18%
Patient data	6%
Intellectual property	28%
Financial information	13%
Non-financial information	25%
Source code	9%
Other proprietary information	7%
None (information was not compromised)	13%
Other (please specify)	4%
Total	256%

Q25. What best describes the nature of sensitive or confidential information compromised by this breach incident?	Pct%
Structured data (such as records or files in a database program)	34%
Unstructured data (such as Word documents, spreadsheets, emails, presentations and others)	30%
Combination of both structured and unstructured data	19%
None (information was not compromised)	13%
Unsure	4%
Total	100%

Q26. How did this breach impact your organization? Please select all that apply.	Pct%
Lost revenues	14%
Lost customers (churn)	18%
Lost time and productivity	46%
Regulatory fines and lawsuits	11%
Cost of outside consultants and attorneys	23%
Cost of purchased technologies	38%
Cost of notification	27%
Out-of-pocket costs to prevent harm to breach victims	23%
Lost reputation, brand value and marketplace image	52%
None (no impact)	20%
Total	272%

Part 4. Organization and respondents' demographics

D1. What best describes your position level within the organization?	Pct%
Executive/VP	2%
Director	16%
Manager	22%
Supervisor	15%
Staff/technician	37%
Administrative	4%
Consultant/contractor	3%
Other	1%
Total	100%

D2. What best describes your direct reporting channel?	Pct%
CEO/executive committee	1%
COO or head of operations	1%
CFO, controller or head of finance	2%
CIO, CTO or head of corporate IT	55%
Business unit leader or general manager	15%
Head of compliance or internal audit	6%
CISO/CSO or head of IT security	20%
Other	0%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Pct%
Less than 500	12%
500 to 1,000	26%
1,001 to 5,000	23%
5,001 to 10,000	15%
10,001 to 25,000	9%
25,001 to 75,000	8%
More than 75,000	7%
Total	100%
Extrapolated value	13,233

D4. What best describes your organization's primary industry classification?	Pct%
Financial services	18%
Federal government	9%
State & local government	3%
Energy & utilities	5%
Education & research	3%
Transportation	3%
Consumer products	5%
Industrial products & chemicals	6%
Pharmaceuticals & biotech	3%
Healthcare & medical devices	6%
Defense contractor	1%
Hospitality	2%
Entertainment & media	2%
Technology & software	8%
Services	6%
Professional services	2%
Retail, Internet	5%
Retail, conventional	7%
Communications	6%
Other	0%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

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

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