The 2013 eCommerce Cyber Crime Report: Safeguarding Brand And Revenue This Holiday Season

Sponsored by

RSA Security

Independently conducted by Ponemon Institute, LLC

Publication Date: October 2013

The 2013 eCommerce Cyber Crime Report:
Safeguarding Brand And Revenue This Holiday Season

A Study of US & UK IT Security Practitioners

Part 1. Introduction

During the holiday shopping season, a company's inability to safeguard its ecommerce websites and keep customers loyal comes with a high price tag. While shoppers on Cyber Monday can significantly boost sales, just one hour of downtime as a result of an attack could mean an average loss of almost $500,000. Or, about $8,000 for every minute a purchase is prevented or the integrity of the website compromised.

It gets worse when you consider what the cost could be to customer loyalty if it becomes impossible to make a purchase or there is perception that the website is not secure. According to the companies in our study, an average of $3.4 million is what reputation and brand damage can cost as a result of the loss of customers.

Conducted by Ponemon Institute and sponsored by RSA Security, the study surveyed more than 1,100 experienced IT practitioners in the United States and United Kingdom.[1] To ensure a knowledgeable respondent, all participants say they are familiar with their organization's website security and anti-fraud activities. The majority has either full responsibility or some responsibility for the security of their organization's websites and believes that prevention of internet fraud is a high priority for their company during high traffic days such as Cyber Monday.

In this study, we asked companies to estimate the number of customer-facing websites they have, ranging from 1 to more than 100. On average, companies represented in this study have 44 ecommerce websites. These companies estimate that just on Cyber Monday revenues from these websites can increase an average of 55 percent or more than $600,000.

Top findings from this study include:

- The financial stakes are high on Cyber Monday and during the holiday shopping season. The estimated brand damage could average $3.4 million for one hour of downtime.
- Beware of Botnet and DoS attacks. In this research, we asked respondents to identify the types of attacks most likely to occur during the holiday shopping season. Botnet and DoS are not only expected to be the most prevalent, they are considered very difficult to detect.
- Cyber Monday precautions are often ignored. Sixty-four percent of respondents say their organizations have seen an increase in Internet fraud and/or attempted website attacks on high traffic days such as Cyber Monday. However, only one-third say they take special precautions to ensure high availability and integrity of their websites.
- Detection of fraud is difficult because of the lack of real time visibility. More than half of respondents (51 percent) say their organization does not have real time visibility into its website to detect the presence of a criminal.
- Only 36 percent or respondents say their organizations use automated forensic tools that detect business logic abuses.

[1] The average respondent has approximately 11 years experience in their field.

Part 2. Key Findings

The analysis of key findings is presented in this section. The complete audited findings are presented in the appendix of this report. The findings are organized according to the following topics:

- Financial stakes are high during the holiday shopping season
- Methods used to attack ecommerce websites
- Why companies are vulnerable to attack

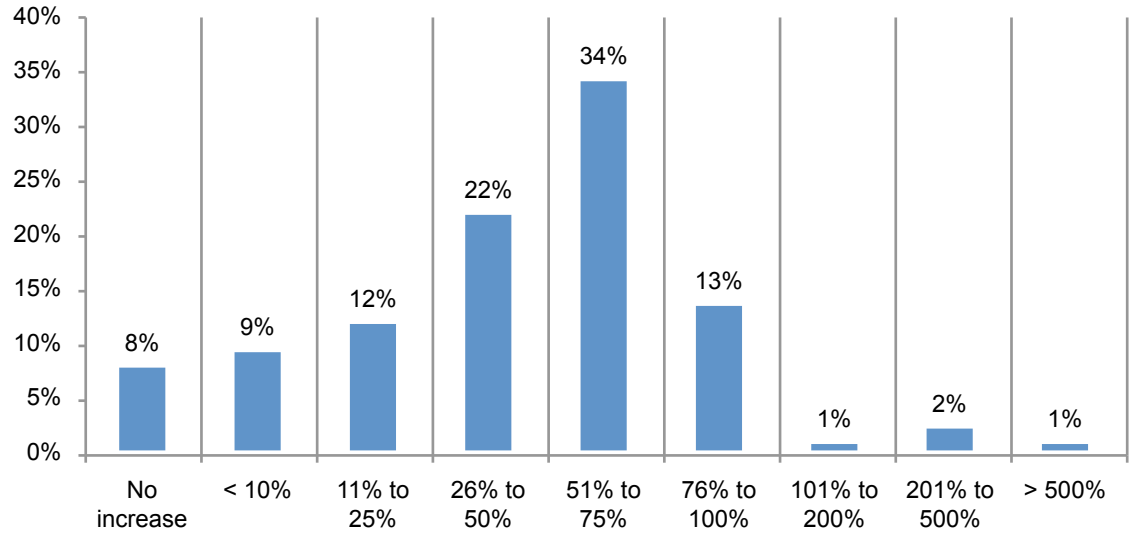
Financial stakes are high during the holiday shopping season

Companies invest heavily in website marketing only to realize significant losses if they are not ready to deal with the potential threat of attacks on Cyber Monday. Understanding the cost of downtime and more important the cost to reputation and brand, can help make the business case for investing in the resources necessary to stop fraud and preserve the integrity of customer facing websites.

The economics of ecommerce. On average, organizations have about 44 customer-facing websites and on a typical day sales from internet and mobile channels average $800,000.

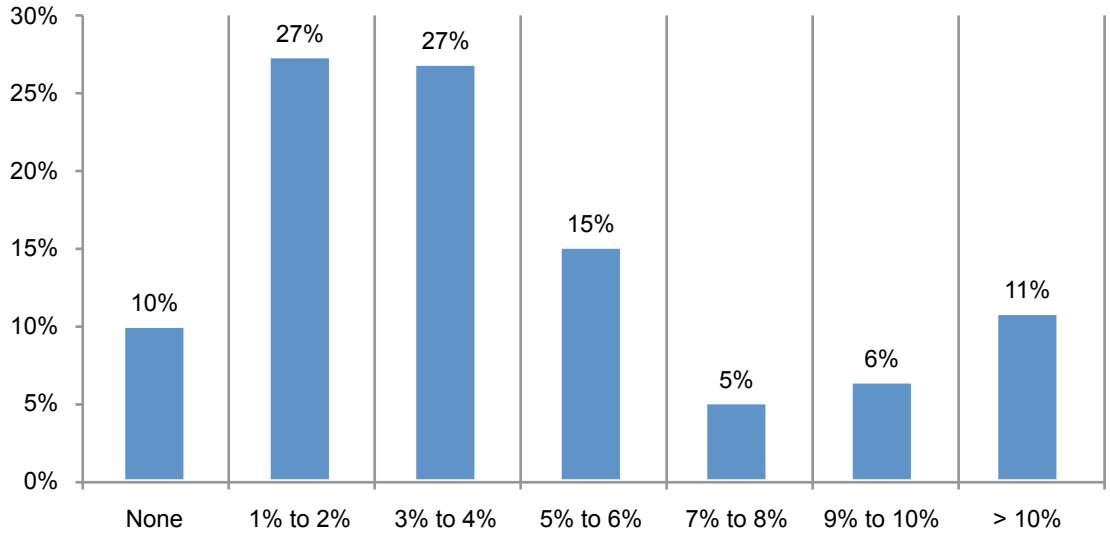
Figure 1 shows the percentage increase in revenues on Cyber Monday. As shown, 51 percent of respondents (34 percent + 13 percent + 1 percent + 2 percent + 1 percent) estimate that revenues just on Cyber Monday will increase more than 50 percent. Based on all responses, the average increase is 55 percent or $665,115.

Figure 1. The Cyber Monday revenue boost
Extrapolated average increase is 55 percent



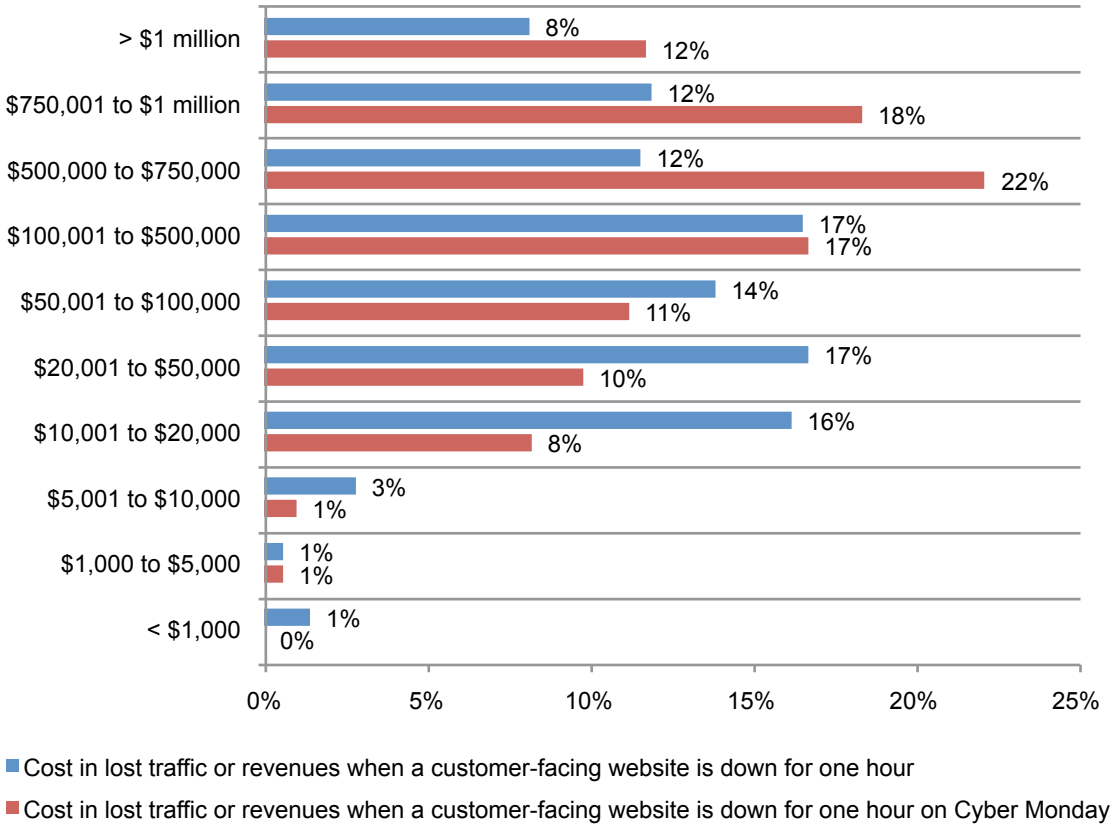
Internet fraud is costly and affects brand. According to organizations in our study the amount of revenue lost due to internet fraud can do measurable harm to the bottom line. As shown in Figure 2, an average of almost 5 percent of total revenues (gross sales) were lost due to the financial and brand impact of internet fraud during the past 12 months. They also report an average of 19 separate internet fraud incidents during the same period.

Figure 2. The financial & brand impact of Internet fraud as a percentage of total revenues



The economics of downtime. According to Figure 3, on a typical day the average cost if a primary customer-facing website went down for just one hour is estimated to be $336,729. As discussed, respondents anticipate an average revenue boost of 55 percent on Cyber Monday and downtime is expected to cost an average of almost $500,000.

Figure 3. The cost of losing one customer-facing website for one hour
Extrapolated average loss is $336,729



If customers become frustrated and disgruntled when they are prevented from making a purchase and vow never to return, the estimated brand damage could be on average $3.4 million, as shown in Figure 4.

Figure 4: The economic impact to reputation & brand
Extrapolated average of brand & reputation damage is $3,372,616

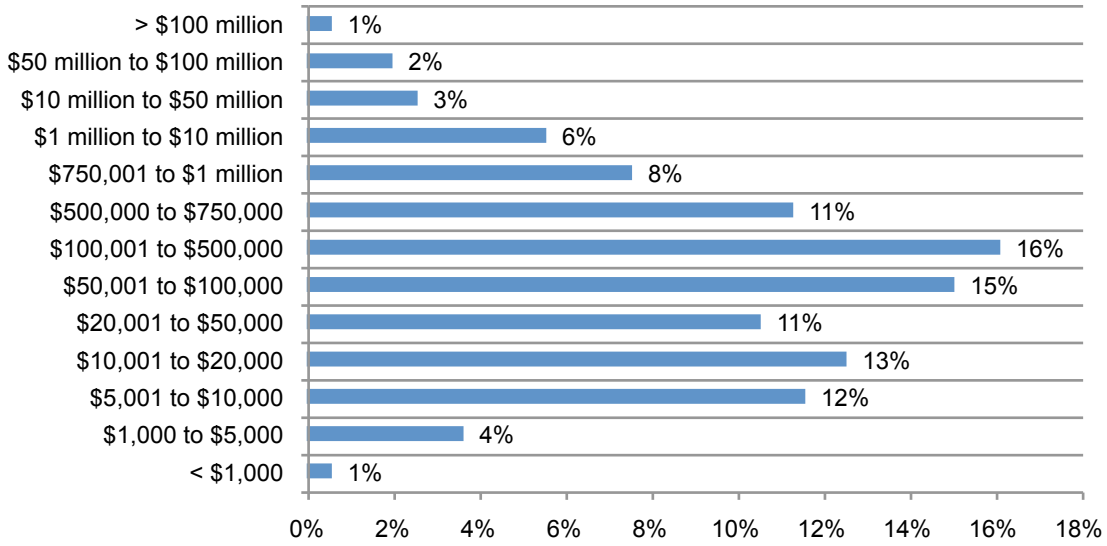
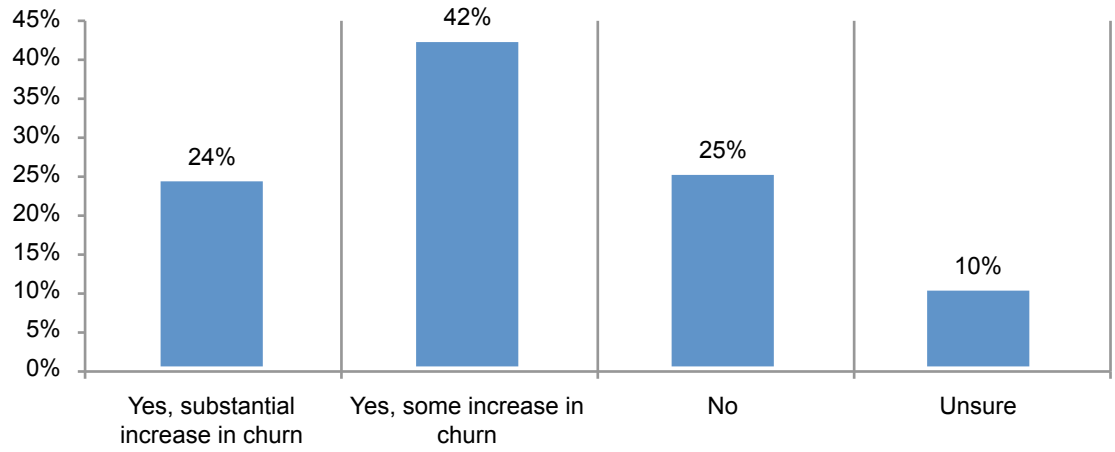


Figure 5 reveals that 66 percent of respondents say there would be a substantial or at least some loss of customers as a result of the website shutting down.

Figure 5. Will companies lose customers because of downtime?

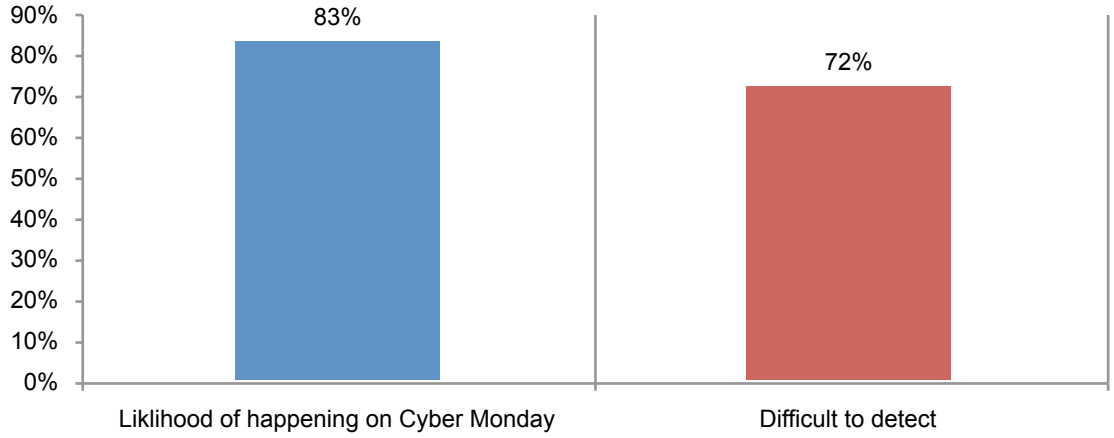


Methods used to attack ecommerce websites

The majority of respondents believe the nine types of attacks are more likely to occur during the holiday shopping season than on other days. The findings reveal that not only can the attacks be economically disastrous, the majority of respondents believe they are difficult to detect. The types of attacks are presented in the order they are most likely to occur.

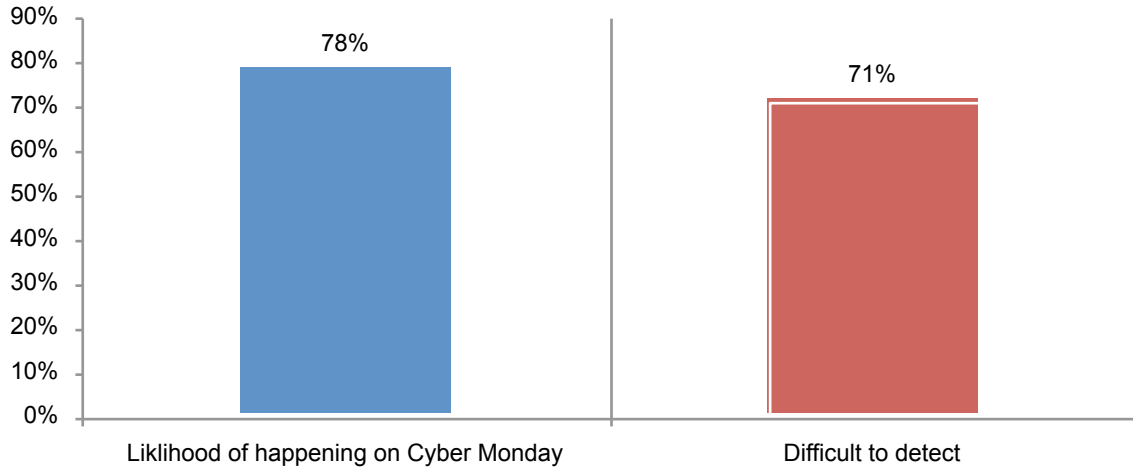
Attack 1: Botnet and DoS. This type of attack tops the list. We define this scenario as occurring when a cyber criminal targets a botnet against a company and this results in a denial of Service (DoS) attack that ultimately brings down its websites. *Eighty-three percent say it is more likely to occur on high traffic days and 72 percent say it would be very difficult or difficult to detect.*

Figure 6. Botnet and DoS



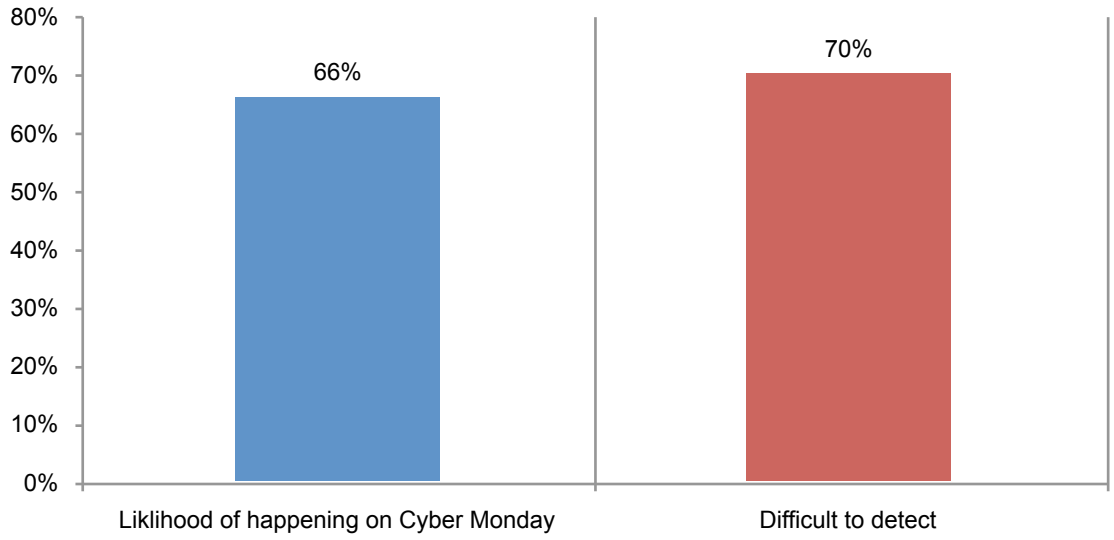
Attack 2: Mobile app store fraud. The likelihood of this type of fraud taking place on Cyber Monday is also high. Companies that are vulnerable have an app store/market place that provides access to products and instant rebates. Criminals masquerading as a merchant and a buyer manipulate the open platform for financial gain, cashing in on rebates and earning points from credit card incentive programs. *Seventy-eight percent say it is more likely to occur on Cyber Monday than other times and 71 percent say it would be difficult to detect.*

Figure 7. Mobile app store fraud



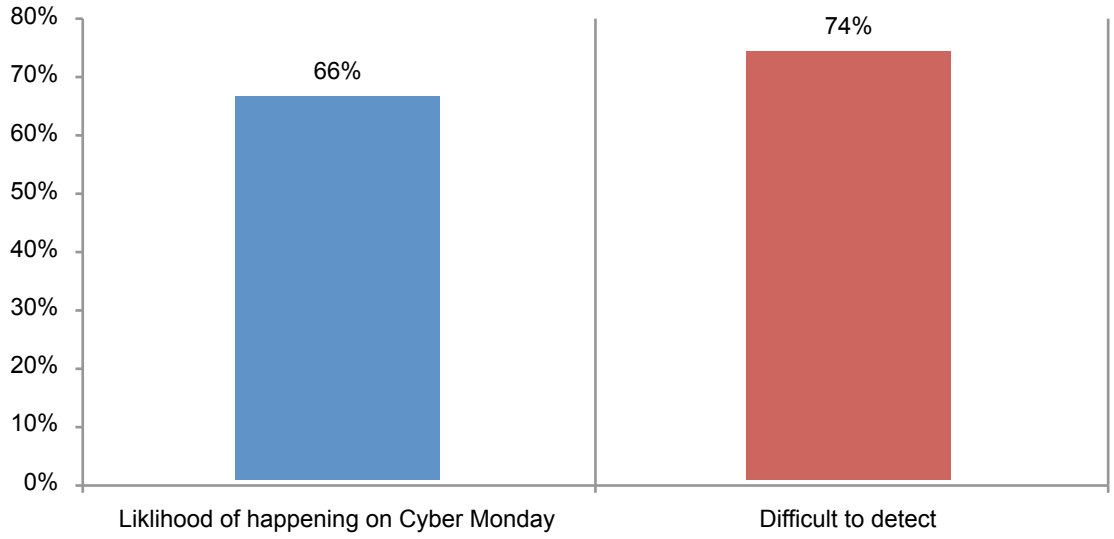
Attack 3. Mobility use case. A company expanded its consumer reach using a mobility platform that allows customers to access its websites using smart phones and other mobile devices. Cyber criminals infiltrate these devices with malware that captures customers' account access credentials. The criminals harvest this information to takeover accounts using a laptop or desktop computer. *Sixty-six percent say it is more likely to occur and a higher percentage (70 percent) say it would be very difficult or difficult to detect.*

Figure 8. Mobility use case



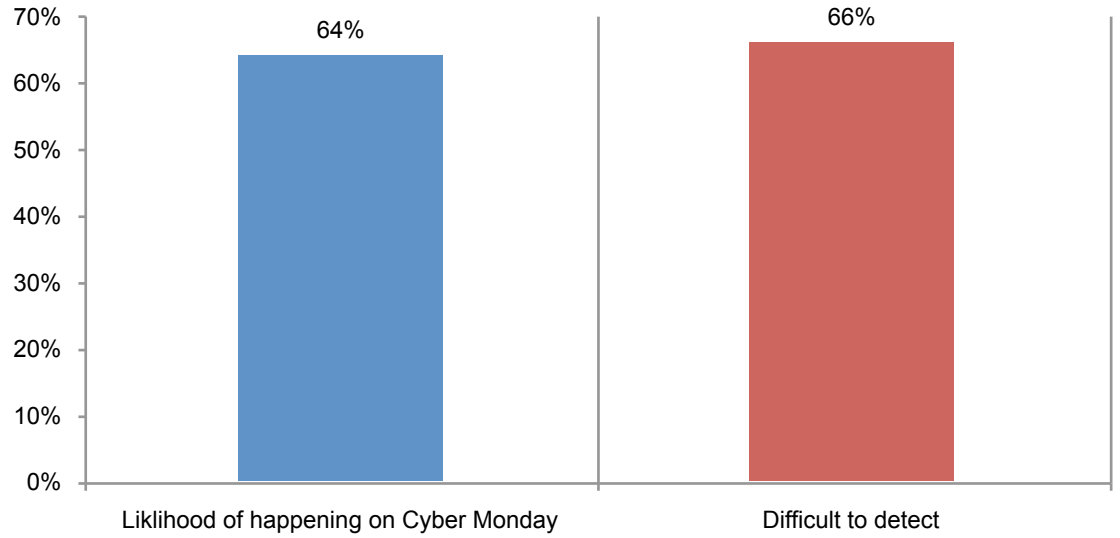
Attack 4: Click fraud. A company hires an agency to conduct an online advertising campaign. The agency is paid on a "per click" basis. In reality, many of the paid "per clicks" are not authentic (i.e. not involving an interested consumer). *Sixty-six percent say it is more likely to occur and a higher percentage (74 percent) say it would be very difficult or difficult to detect.*

Figure 9. Click fraud



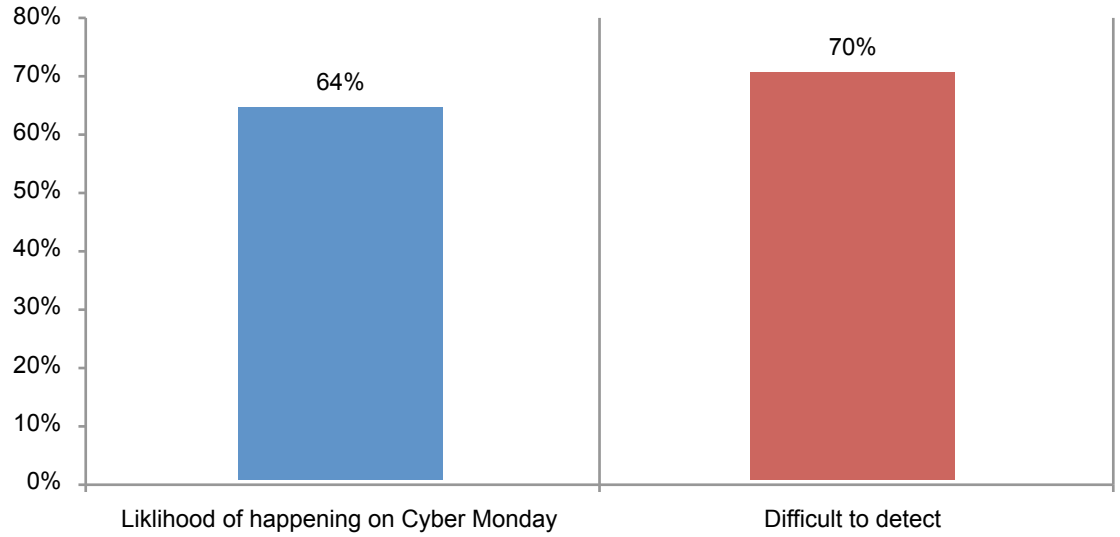
Attack 5: Testing stolen credit cards. A cyber criminal steals hundreds of credit card numbers and uses a company's credit or debit card payments function to validate active credit cards. *Sixty-four percent of respondents say this is more likely to happen and 66 percent say it would be very difficult or difficult to detect.*

Figure 10. Testing stolen credit cards



Attack 6. eCoupons. Fraudsters do an end-run around a company's pricing policy. They select a heavily discounted item and place it in the "shopping cart." They delay the checkout in order to obtain and apply an eCoupon to the final purchase price, thus obtaining the item well below the company's cost. *Again, 64 percent say this is more likely to happen and a significant percentage (70) say this would be very difficult or difficult to detect.*

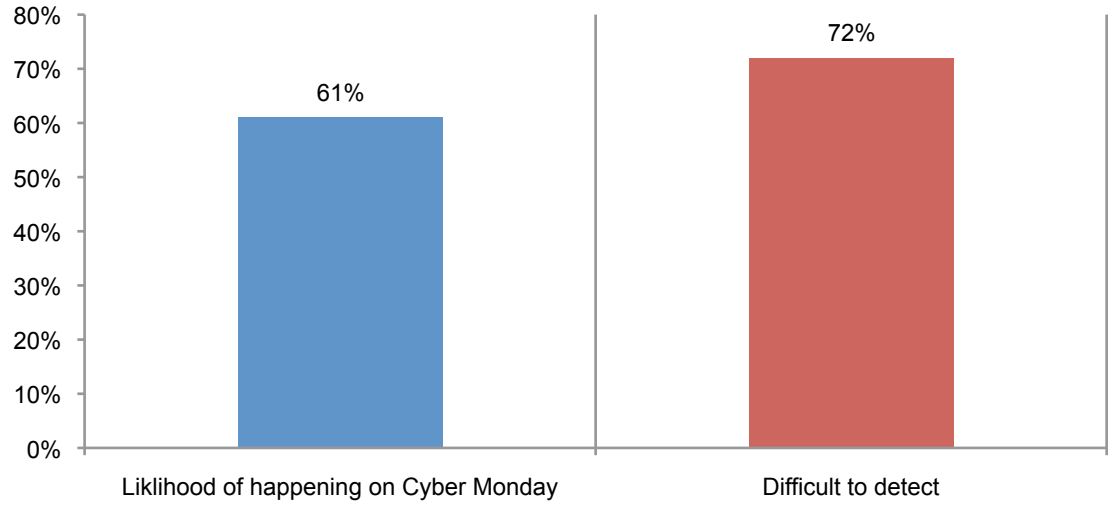
Figure 11. eCoupons



The following three types of attack are considered less likely to occur but are still considered very difficult or difficult to detect.

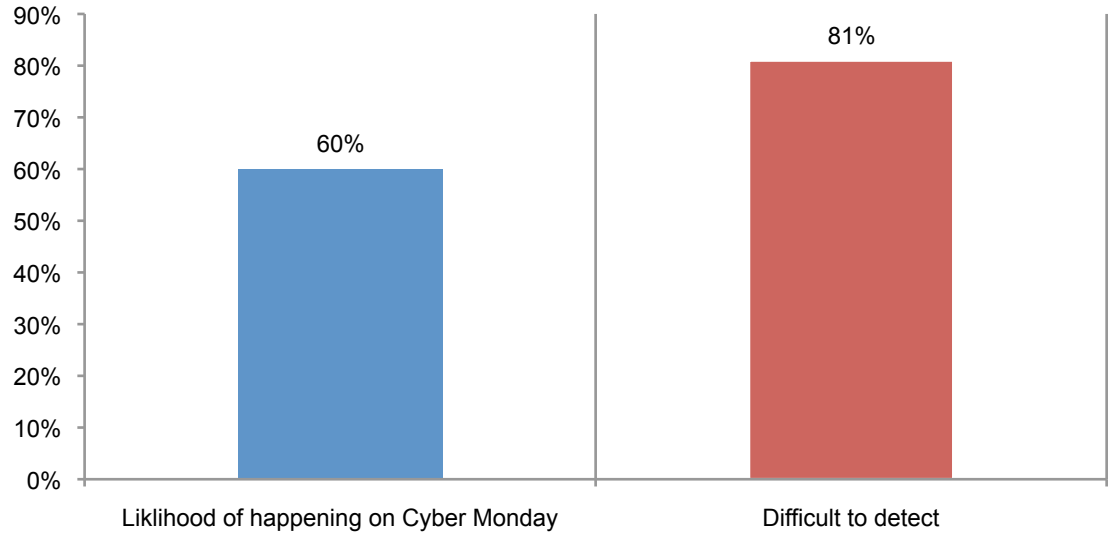
Attack 7: Account hijacking. A successful spear phishing scam resulted in cyber criminals obtaining the user names and passwords of customers. The leakage of customer account information occurred because employees were duped by what appeared to be a legitimate internal company email communication. The crime originated when the criminal obtained key employee email addresses directly from the website. *Sixty-one percent say it is more likely to occur and 72 percent say it would be very difficult or difficult to detect.*

Figure 12. Account hijacking



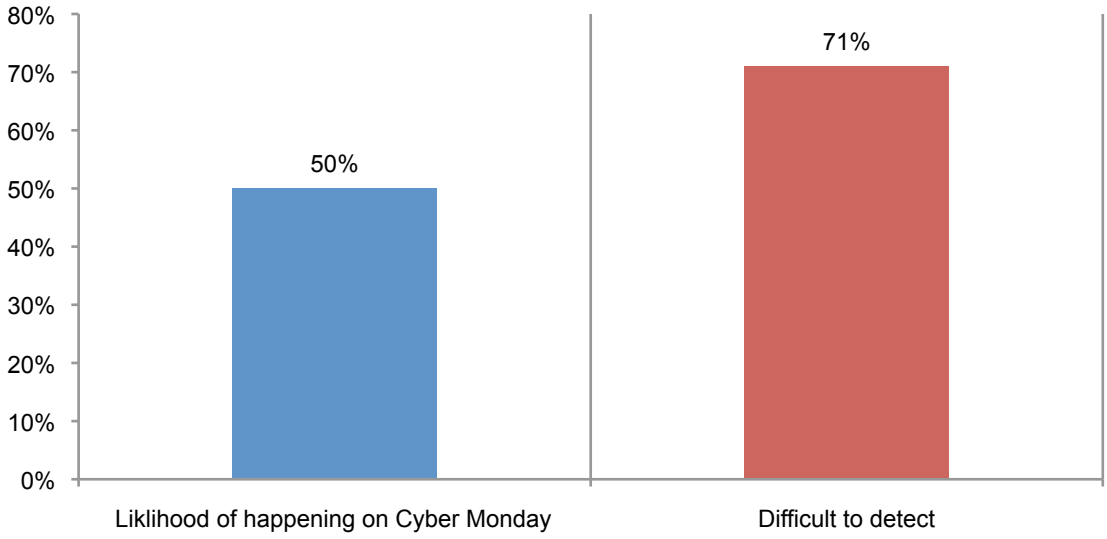
Attack 8. Electronic wallet. A company has expanded customer payment options to include Internet payment methods such as PayPal, Google Wallet, Amazon Checkout and others. A criminal looking for sites that have recently added internet payment processes identifies its site and exploits the lack of fully implemented security controls. *Sixty percent say this is more likely to happen and a much higher percentage (81 percent) say it would be very difficult or difficult to detect.*

Figure 13. Electronic wallet



Attack 9. Mass registration. A cyber criminal creates a fake website that imitates your company's website. Loyal and prospective customers are lured to this bogus website, which asks them to provide personal information in order to register for a promotion or offer. This results in the theft of sensitive information. *In this case, 50 percent say it is more likely to occur but a much higher percentage (71 percent) says it would be very difficult or difficult to detect.*

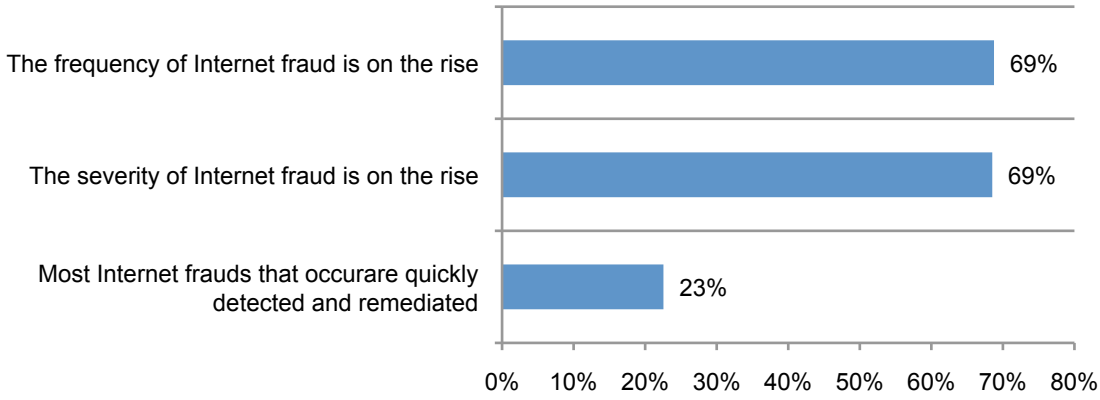
Figure 14. Mass registration



Why companies are vulnerable

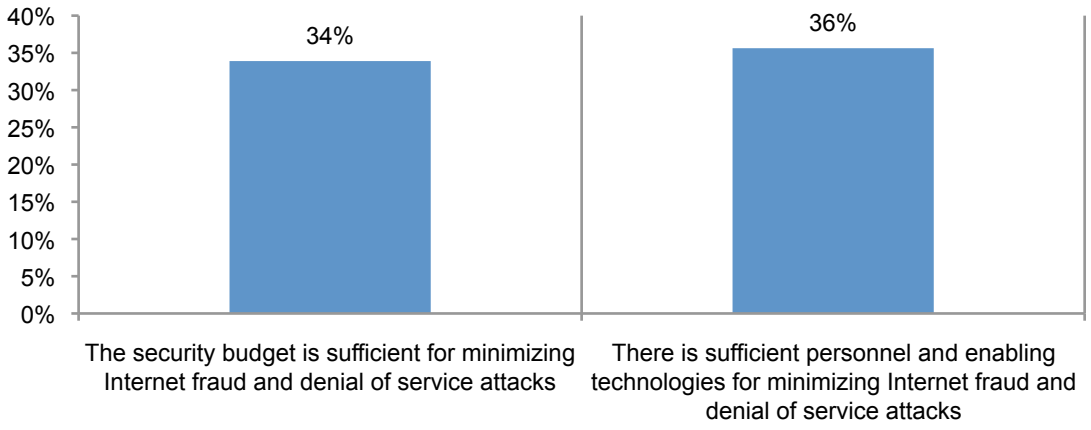
The severity and frequency of internet fraud is on the rise but budgets and resources are not. As shown in Figure 15, 69 percent of respondents believe Internet fraud is becoming frequent and severe. Only 23 percent of respondents say most internet fraud that occurs on their company's websites are quickly detected and remediated.

Figure 15. Attributions regarding Internet fraud
Strongly agree and agree response combined



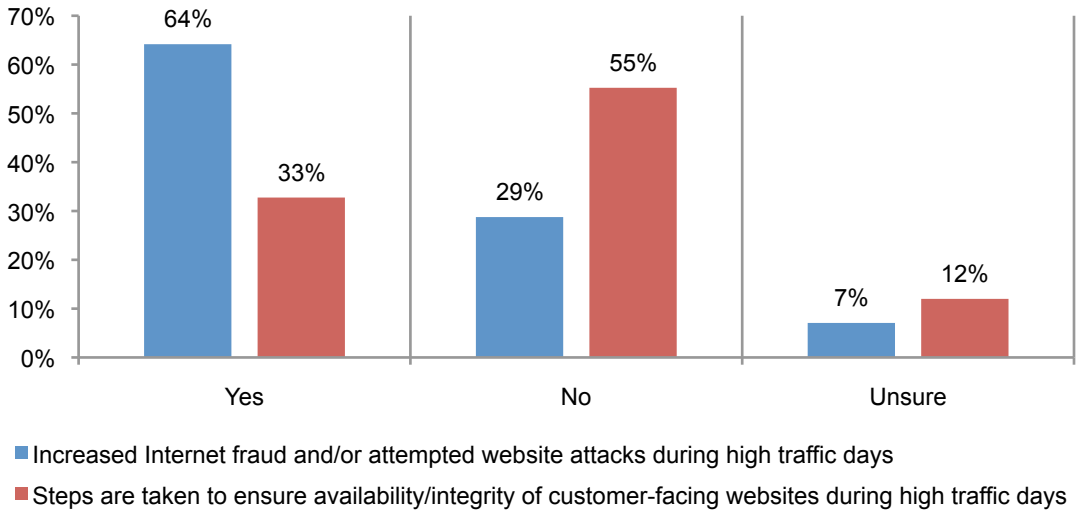
Despite understanding the importance of data center availability on high traffic days and the business risk of internet fraud, it seems as if the resources necessary to deal with potential threats are not available. Only 34 percent say the budget is sufficient, as shown in Figure 16. Thirty-six percent say their organizations have the personnel and enabling technologies to reduce Internet fraud and denial of service attacks.

Figure 16. Attributions regarding internet fraud



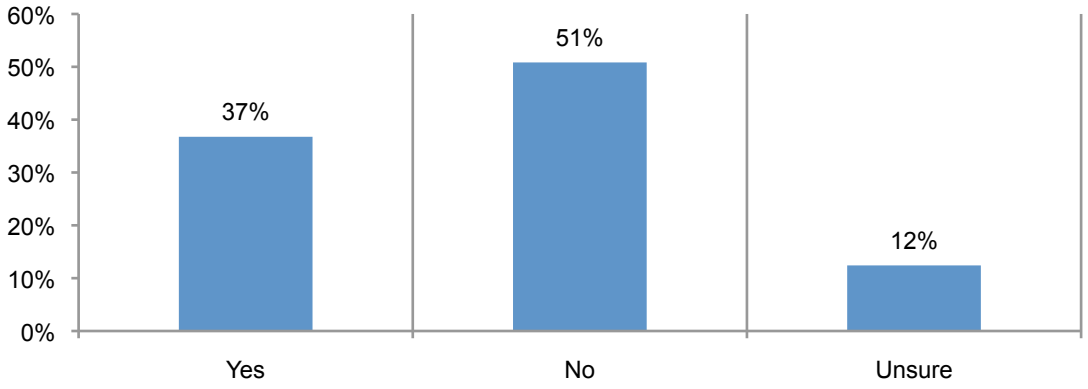
Holiday shopping season precautions are not taken by most organizations. As revealed in Figure 17, 64 percent of respondents say their organizations have seen an increase in internet fraud and/or attempted website attacks during high traffic days such as Cyber Monday. However, only one-third say they are taking special precautions to ensure high availability and integrity of customer-facing websites during high traffic days such as Cyber Monday. That is why most rate their companies as not being sufficiently prepared for the increased traffic and likelihood of an attack.

Figure 17. Internet fraud during high traffic days



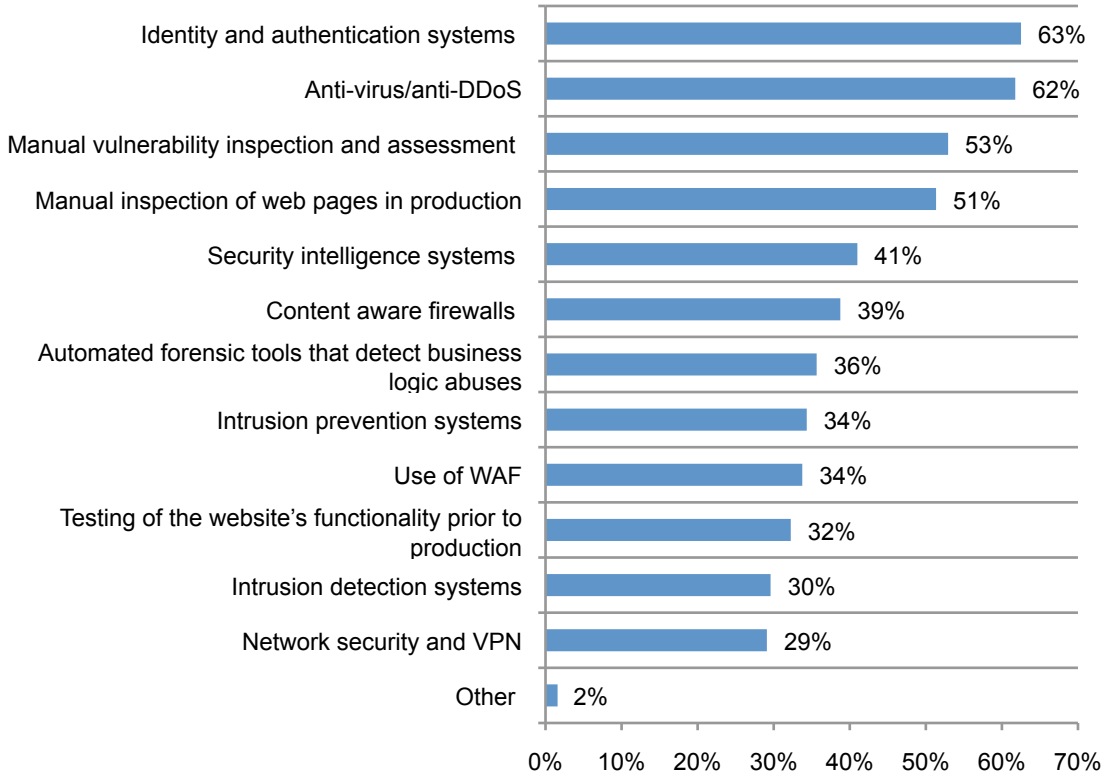
Detection of fraud is difficult because of the lack of real time visibility. Figure 18 indicates that more than half (51 percent) say their organization does not have real time visibility into its website traffic to make it possible to immediately detect the presence of a criminal or fraudster and 12 percent are unsure. This lack of visibility leads to the problem 46 percent of respondents have in understanding the root cause of an attack.

Figure 18. Real time visibility into website traffic



Steps taken to detect fraud may not be the most effective. According to respondents, organizations are using identity and authentication systems such as IAM, anti-virus/anti-DDoS, manual inspection and assessment of vulnerabilities, manual inspection and assessment of web pages in production and security intelligence systems. Only 36 percent of respondents say their organizations use automated forensic tools that detect business logic abuses.

Figure 19. Steps taken to prevent/detect internet fraud
Very important and important response combined



Part 3. Conclusion & recommendations

It is important that companies do not think narrowly about this issue. When making the business case for investing in website security, emphasize the economics of reputation damage.

The following are technology, governance and assessment recommendations to make a website ready for Cyber Monday:

Technologies. Invest in technology that improves the ability to prevent downtime or outages and detect fraud occurring in real time. Do not wait until the holiday shopping season to take the necessary precautions.

Governance. Centralize resources under one function to improve accountability for preventing and detecting internet fraud and cyber attacks. Too many organizations say no one function is accountable for stopping internet fraud and threats. Have a business continuity and disaster recovery plan in place to minimize downtime and data center availability in the event of an attack.

Assessment. Based on your business model, assess what threats are most likely to target your websites. Prevent future fraud by understanding the root cause of the attack.

Part 4. Methods

A random sampling frame of 34,614 IT and IT security practitioners located in the United States and United Kingdom were selected as participants to this survey. As shown in Table 1, 1,338 respondents completed the survey. Screening removed 177 surveys. The final sample was 1,161 surveys (or a 3.4 percent response rate).

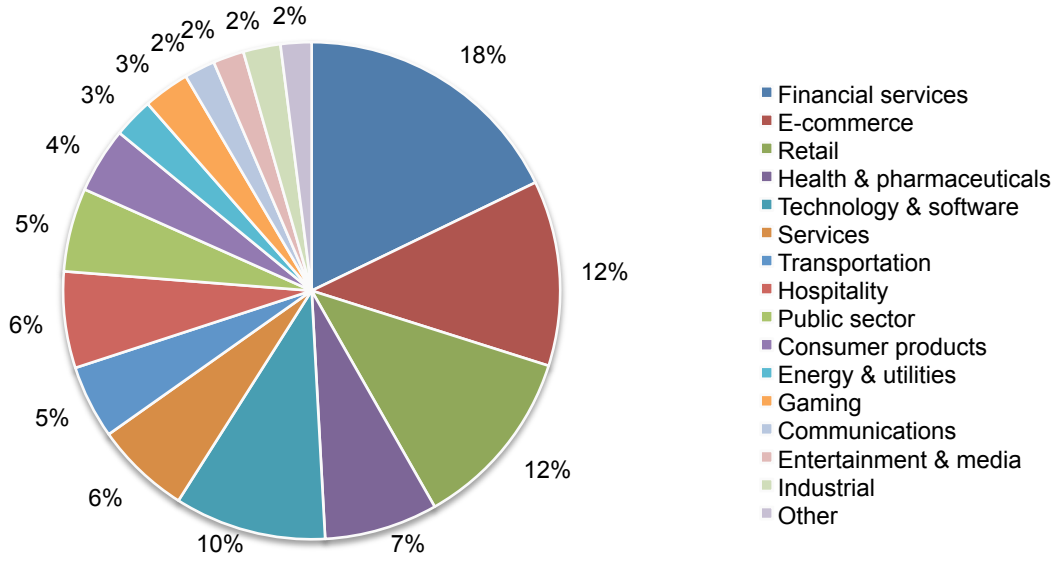
Table 1. Sample response	Freq.	Pct%
Total sampling frame	34,614	100.0%
Total returns	1,338	3.9%
Screened or rejected surveys	177	0.5%
Final sample	1,161	3.4%

As noted in Table 2, the respondents' average (mean) experience in IT, IT security or related fields is 10.8 years.

Table 2. Other characteristics of respondents	Mean
Total years of IT or IT security experience	10.8
Total years in your current position	5.9

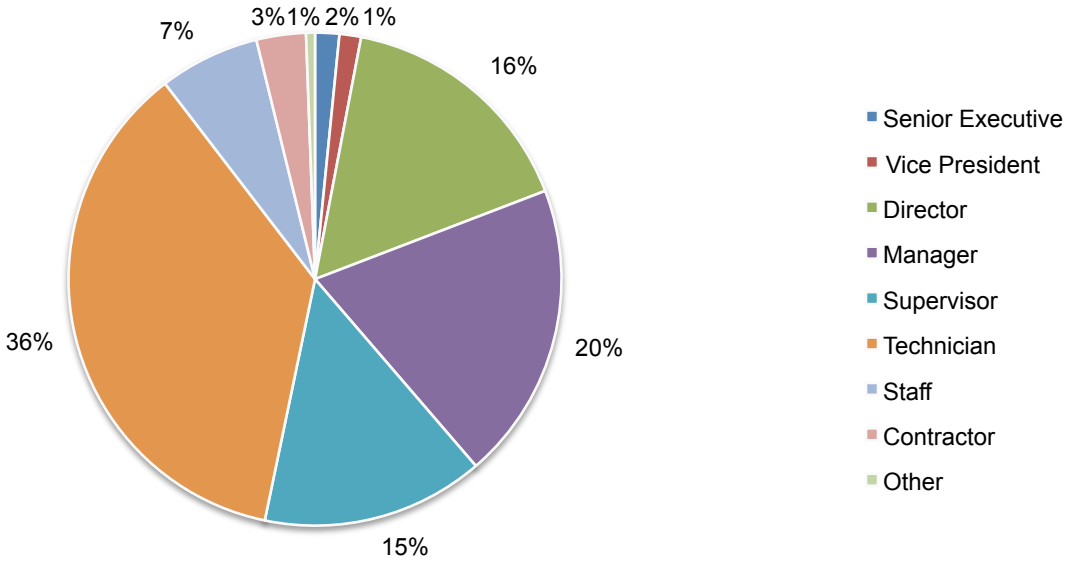
Pie Chart 1 reports the industry segments of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by e-commerce (12 percent) and retail (12 percent).

Pie Chart 1. Industry distribution of respondents' organizations



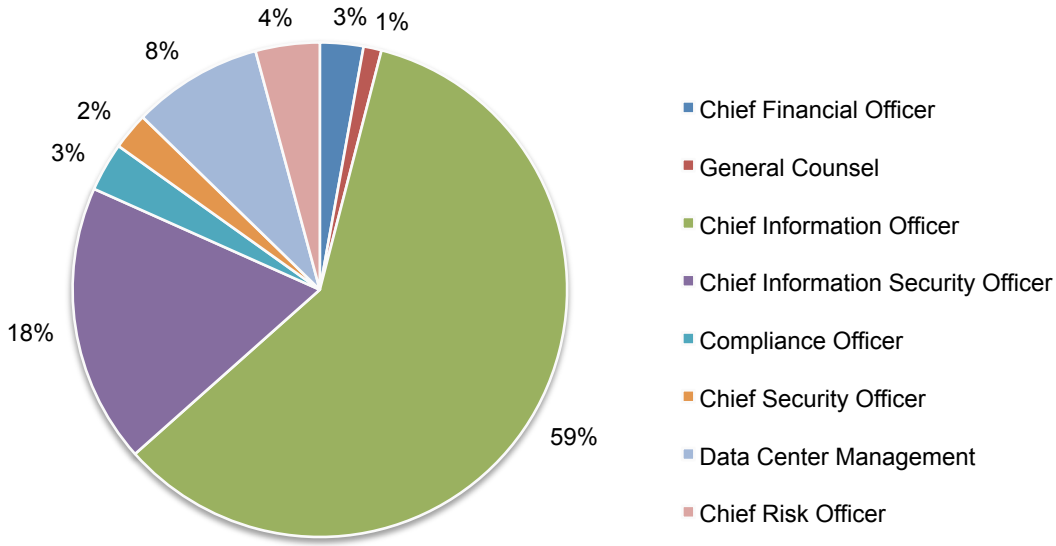
Pie Chart 2 reports the respondent's organizational level within participating organizations. By design, 54 percent of respondents are at or above the supervisory levels.

Pie Chart 2. What organizational level best describes your current position?



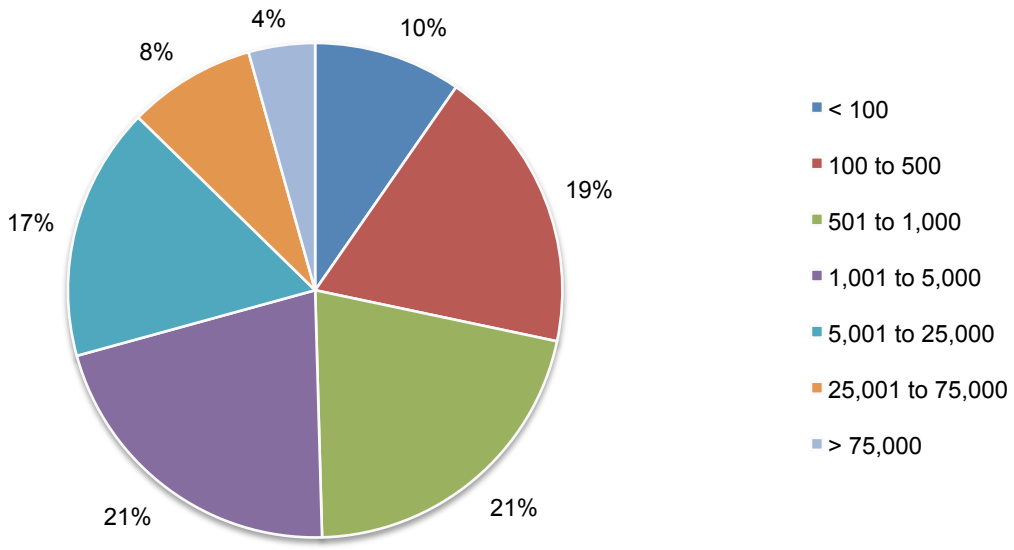
According to Pie Chart 3, 59 percent of respondents report directly to the Chief Information Officer and 18 percent report to the Chief Information Security Officer.

Pie Chart 3. The primary person you or the IT security leader reports to within the organization



More than half of the respondents (55 percent) are from organizations with a global headcount of over 1,000 employees, as shown in Pie Chart 4.

Pie Chart 4. Global headcount



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 IT or IT security leaders. 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 holdout 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 a truthful response.

Ponemon INSTITUTE

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 August 2013.

Sample response	Combined
Total sampling frame	34,614
Total returned surveys	1,338
Screened or rejected surveys	177
Final sample	1,161
Response rate	3.4%
Sample weights	100%

Part 1. Screening questions

S1. How familiar are you with organization's website security and anti-internet fraud activities?	Combined
Very familiar	25%
Familiar	41%
Somewhat familiar	34%
No knowledge (Stop)	0%
Total	100%

S2. Approximately, how much of your organization's revenues (gross sales) are from internet channels?	Combined
None (Stop)	0%
1 to 10%	12%
11 to 20%	26%
21 to 30%	23%
31 to 40%	14%
41 to 50%	11%
51 to 60%	7%
61 to 70%	2%
71 to 80%	2%
81 to 90%	2%
91 to 100% (virtually all)	1%
Total	100%
Extrapolated values	29%

S3. Approximately, how much of your organization's revenues (gross sales) are from mobile channels?	Combined
None (Stop)	0%
1 to 10%	39%
11 to 20%	27%
21 to 30%	20%
31 to 40%	9%
41 to 50%	3%
51 to 60%	1%
61 to 70%	0%
71 to 80%	1%
81 to 90%	1%
91 to 100% (virtually all)	0%
Total	100%
Extrapolated values	17%

S4. Do you have any responsibility for the security of your organization's websites?	Combined
Yes, full responsibility	30%
Yes, some responsibility	61%
Yes, minimum responsibility	10%
No responsibility (Stop)	0%
Total	100%

Part 2. Attributions. Strongly agree and agree combined.	Combined
Q1a. Internet fraud represents a significant business risk for my company.	66%
Q1b. Data center availability is my company's highest priority above all other IT priorities.	52%
Q1c. The prevention of internet fraud is a priority for my company during high traffic days such as Cyber Monday.	67%
Q1d. Most internet frauds that occur on my company's websites are quickly detected and remediated.	23%
Q1e. My company is vigilant in monitoring websites for internet fraud and other abuses.	41%
Q1f. My company is vigilant in monitoring threats that seek to shutdown our websites (such as denial of service attacks).	39%
Q1g. My company's security budget is sufficient for minimizing Internet fraud and denial of service attacks.	34%
Q1h. My company has sufficient personnel and enabling technologies for minimizing Internet fraud and denial of service attacks.	36%
Q1i. The frequency of Internet fraud experienced by my company is on the rise.	69%
Q1j. The severity of Internet fraud experienced by my company is on the rise.	69%

Part 3. Background

Q2. Approximately, how many customer-facing websites does your company have in production today?	Combined
Between 1 and 5	7%
Between 6 and 10	12%
Between 10 and 20	19%
Between 21 and 30	16%
Between 31 and 40	6%
Between 41 and 50	9%
Between 51 and 100	11%
More than 100	20%
Total	100%
Extrapolated values	44.4

Q3. On a typical day, how much revenue does you earn from internet and mobile channels?	Combined
Less than $100,000	13%
$100,001 to $200,000	16%
$200,001 to $300,000	16%
$300,001 to $400,000	15%
$400,001 to $500,000	12%
$500,001 to $1,000,000	9%
$1,000,001 to $2,000,000	7%
$2,000,001 to 5,000,000	5%
More than $5,000,000	7%
Total	100%
Extrapolated values	$823,079

Q4. In percentage terms, how much of a revenue boost or increase do you anticipate this coming Cyber Monday?	Combined
No increase	8%
Less than 10%	9%
11% to 25%	12%
26% to 50%	22%
51% to 75%	34%
76% to 100%	13%
101% to 200% (1 to 2X)	1%
201% to 500% (2 to 5X)	2%
More than 500% (> 5X)	1%
Total	100%
Extrapolated value	55%
Net increase (Cyber Monday revenue boost)	$665,115

Q5. In a 12-month period, what percent of your company's total revenues (gross sales) were lost due to the financial and brand impact of internet fraud?	Combined
None	10%
1% to 2%	27%
3% to 4%	27%
5% to 6%	15%
7% to 8%	5%
9% to 10%	6%
More than 10%	11%
Total	100%
Extrapolated value	4.7%

Q6. In the past 12 months, how many separate internet fraud incidents did your company experience?	Combined
None	18%
1 to 5	25%
6 to 10	20%
10 to 20	12%
21 to 30	7%
31 to 40	2%
41 to 50	6%
51 to 100	6%
More than 100	5%
Total	100%
Extrapolated value	19.2

Q7a. Have you experienced any unplanned data center outages in the past 12 months most likely caused by internet fraud, denial of services or other cyber attacks?	Combined
Yes	55%
No	35%
Unsure	10%
Total	100%

Q7b. If yes, what was the frequency of unplanned data center outages in the past 12 months most likely caused by internet fraud, denial of services or other cyber attacks?	Combined
1 and 2	31%
3 and 5	43%
6 and 10	11%
11 and 15	5%
16 and 20	7%
More than 20	3%
Total	100%
Extrapolated value	5.7

Q7c. If yes, what was the average duration of unplanned data center outages most likely caused by internet fraud, denial of services or other cyber attacks in the past 12 months?	Combined
Less than 1 minute	12%
1 to 5 minutes	36%
5 to 20 minutes	35%
20 minutes to 2 hours	8%
2 hours to one day	4%
More than one day	5%
Total	100%
Extrapolated value	51.5

Q8. How confident are you in knowing the root causes of most Internet frauds or cyber attacks that seek to shutdown your company's data centers?	Combined
Very confident	17%
Confident	37%
Not confident	46%
Total	100%

Q9. On a typical day, how much would it cost your company in lost traffic or revenues when a primary customer-facing website is down for just one hour?	Combined
None	0%
Less than $1,000	1%
$1,000 to $5,000	1%
$5,001 to $10,000	3%
$10,001 to $20,000	16%
$20,001 to $50,000	17%
$50,001 to $100,000	14%
$100,001 to $500,000	17%
$500,000 to $750,000	12%
$750,001 to $1 million	12%
More than $1 million	8%
Total	100%
Extrapolated value	$336,729

Q10. On high traffic days such as Cyber Monday, how much would it cost your company in lost traffic or revenues when a primary customer-facing website is down for just one hour?	Combined
None	0%
Less than $1,000	0%
$1,000 to $5,000	1%
$5,001 to $10,000	1%
$10,001 to $20,000	8%
$20,001 to $50,000	10%
$50,001 to $100,000	11%
$100,001 to $500,000	17%
$500,000 to $750,000	22%
$750,001 to $1 million	18%
More than $1 million	12%
Total	100%
Extrapolated value	$494,882

Q11. What is the total economic impact to reputation or brand damage in the event your company suffered just one hour unplanned shutdown during a high traffic day such as Cyber Monday?	Combined
None	0%
Less than $1,000	1%
$1,000 to $5,000	4%
$5,001 to $10,000	12%
$10,001 to $20,000	13%
$20,001 to $50,000	11%
$50,001 to $100,000	15%
$100,001 to $500,000	16%
$500,000 to $750,000	11%
$750,001 to $1 million	8%
$1 million to $10 million	6%
$10 million to $50 million	3%
$50 million to $100 million	2%
More than $100 million	1%
Total	100%
Extrapolated value	$3,372,616

Q12. Do you believe your company's customer churn (turnover) rate would increase in the event its primary customer-facing website was shutdown just **one hour** during a high traffic day such as Cyber Monday?	Combined
Yes, substantial increase in churn	24%
Yes, some increase in churn	42%
No	25%
Unsure	10%
Total	100%

Q13a. In the past few years have you seen an increase in internet fraud and/or attempted website attacks during high traffic days such as Cyber Monday?	Combined
Yes	64%
No	29%
Unsure	7%
Total	100%

Q13b. If yes, in percentage terms, what is the relative increase in internet fraud and/or attempted websites attacks during high traffic days such as Cyber Monday?	Combined
Less than 5%	14%
5% to 10%	14%
11% to 25%	23%
26% to 50%	21%
51% to 75%	17%
76% to 100%	5%
More than 100%	5%
Total	100%
Extrapolated value	34%

Q14. Does your company take special steps or precautions to ensure high availability and integrity of customer-facing websites during high traffic days such as Cyber Monday?	Combined
Yes	33%
No	55%
Unsure	12%
Total	100%

Q15. Is your company ready to deal with internet frauds and other cyber attacks that seek to shutdown its primary customer-facing websites during high traffic days such as Cyber Monday? Please use the following 10-point scale to rate your opinion from 1 = not ready to 10 = fully prepared.	Combined
1 to 2	20%
3 to 4	33%
5 to 6	16%
7 to 8	12%
9 to 10	18%
Total	100%
	5.0

Q16. What steps does your organization take to prevent or detect internet fraud and other attacks that seek to shutdown websites? Please rate each one of the following steps in terms of its importance using the following scale: Very important and Important combined.	Combined
Manual inspection and assessment of vulnerabilities	53%
Manual inspection and assessment of web pages in production	51%
Thorough testing of the website's functionality prior to production	32%
Identity and authentication systems such as IAM	63%
Automated forensic tools that detect business logic abuses	36%
Content aware firewalls (including next generation firewalls)	39%
Security intelligence systems such as SIEM	41%
Intrusion detection systems	30%
Intrusion prevention systems	34%
Anti-virus/anti-DDoS	62%
Network security and VPN	29%
Use of WAF	34%
Other (please specify)	2%
Average	39%

Q17. Does your organization have real time visibility into its website traffic? In other words, can you detect the presence of a criminal or fraudster in real time (immediately)?	Combined
Yes	37%
No	51%
Unsure	12%
Total	100%

Q18. Who is **most responsible** for curtailing internet fraud and threats that seek to shutdown your organization's websites?	Combined
Chief information officer (CIO)	22%
Chief technology officer (CTO)	1%
Chief information security officer (CISO)	16%
Chief security officer (CSO)	2%
Chief risk officer (CRO)	1%
Head, data center management	3%
Business unit management	16%
Website development leader/manager	8%
Fraud prevention leader/manager	9%
Corporate compliance or legal department	1%
Web hosting service provider	1%
No one person or function has overall responsibility	19%
Other (please specify)	1%
Total	100%

Part 4. Cyber Monday scenarios

Testing stolen credit cards. A cyber criminal steals hundreds of credit card numbers and uses your credit or debit card payments function to validate active credit cards.	Combined
Q19a. How likely could this happen to your company? Already happened or very likely to happen.	50%
Q19b. How difficult would it be to detect this situation? Very difficult or difficult.	66%

Q19c. Do you believe this scenario is more likely to occur on high traffic days such as Cyber Monday?	Combined
Yes	64%
No	31%
Unsure	6%
Total	100%

Click fraud. Your company hires an agency to conduct an online advertising campaign. The agency is paid on a "per click" basis. In reality many of the paid "per clicks" are not authentic (i.e., not involving an interested consumer).	Combined
Q20a. How likely could this happen to your company? Already happened or very likely to happen.	65%
Q20b. How difficult would it be to detect this situation? Very difficult or difficult.	74%

Q20c. Do you believe this scenario is more likely to occur on high traffic days such as Cyber Monday?	Combined
Yes	66%
No	28%
Unsure	7%
Total	100%

Account hijacking. A successful spear phishing scam resulted in cyber criminals obtaining the user names and passwords of customers. The leakage of customer account information occurred because employees were duped by what appeared to be a legitimate internal company email communication. The crime originated when the criminal obtained key employee email addresses directly from the website.	Combined
Q21a. How likely could this happen to your company? Already happened or very likely to happen.	62%
Q21b. How difficult would it be to detect this situation? Very difficult or difficult.	72%

Q21c. Do you believe this scenario is more likely to occur on high traffic days such as Cyber Monday?	Combined
Yes	61%
No	35%
Unsure	5%
Total	100%

Botnet and DDoS. A cyber criminal targets a botnet against your company and this results in a denial of service (DoS) attack that ultimately brings down your websites.	Combined
Q22a. How likely could this happen to your company? Already happened or very likely to happen.	54%
Q22b. How difficult would it be to detect this situation? Very difficult or difficult.	72%

Q22c. Do you believe this scenario is more likely to occur on high traffic days such as Cyber Monday?	Combined
Yes	83%
No	15%
Unsure	2%
Total	100%

Mass registration. A cyber criminal creates a fake website that imitates your company's website. Loyal and prospective customers are lured to this bogus website, which asks them to provide personal information in order to register for a promotion or offer. This results in the theft of sensitive information.	Combined
Q23a. How likely could this happen to your company? Already happened or very likely to happen.	43%
Q23b. How difficult would it be to detect this situation? Very difficult or difficult.	71%

Q23c. Do you believe this scenario is more likely to occur on high traffic days such as Cyber Monday?	Combined
Yes	50%
No	47%
Unsure	3%
Total	100%

App store fraud. Your company has an app store/market place, providing access to products and instant rebates. Criminals masquerading as a merchant and a buyer manipulate the open platform for financial gain, cashing in on rebates and earning points from credit card incentive programs.	Combined
Q24a. How likely could this happen to your company? Already happened or very likely to happen.	45%
Q24b. How difficult would it be to detect this situation? Very difficult or difficult.	71%

Q24c. Do you believe this scenario is more likely to occur on high traffic days such as Cyber Monday?	Combined
Yes	78%
No	13%
Unsure	10%
Total	100%

Mobility use case. Your company has expanded its consumer reach using a mobility platform that allows customers to access its websites using smart phones and other mobile devices. Cyber criminals infiltrate these devices with malware that captures customers' account access credentials. The criminals harvest this information to takeover accounts using a laptop or desktop computer.	Combined
Q25a. How likely could this happen to your company? Already happened or very likely to happen.	60%
Q25b. How difficult would it be to detect this situation? Very difficult or difficult.	70%

Q25c. Do you believe this scenario is more likely to occur on high traffic days such as Cyber Monday?	Combined
Yes	66%
No	24%
Unsure	10%
Total	100%

eCoupons. Fraudsters do an end-run around your company's pricing policy. They select a heavily discounted item and place it the "shopping cart." They delay the check out in order to obtain and apply an eCoupon to the final purchase price, thus obtaining the item well below your company's cost.	Combined
Q26a. How likely could this happen to your company? Already happened or very likely to happen.	51%
Q26b. How difficult would it be to detect this situation? Very difficult or difficult.	70%

Q26c. Do you believe this scenario is more likely to occur on high traffic days such as Cyber Monday?	Combined
Yes	64%
No	31%
Unsure	5%
Total	100%

Electronic wallet. Your company has expanded customer payment options to include Internet payment methods such as PayPal, Google Wallet, Amazon Checkout and others. A criminal looking for sites that have recently added Internet payment processes identifies your site and is able to exploit the lack of fully implemented security controls.	Combined
Q27a. How likely could this happen to your company? Already happened or very likely to happen.	54%
Q27b. How difficult would it be to detect this situation? Very difficult or difficult.	81%

Q27c. Do you believe this scenario is more likely to occur on high traffic days such as Cyber Monday?	Combined
Yes	60%
No	30%
Unsure	10%
Total	100%

Part 5. Your role and organization

D1. What organizational level best describes your current position?	Combined
Senior Executive	2%
Vice President	1%
Director	16%
Manager	20%
Supervisor	15%
Technician	36%
Staff	7%
Contractor	3%
Other	1%
Total	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	Combined
CEO/Executive Committee	0%
Chief Financial Officer	3%
General Counsel	1%
Chief Information Officer	59%
Chief Information Security Officer	18%
Compliance Officer	3%
Human Resources VP	0%
Chief Security Officer	2%
Data Center Management	8%
Chief Risk Officer	4%
Other	0%
Total	100%

D3. Total years of relevant experience	Combined
Total years of IT or security experience (mean value)	10.8
Total years in current position years (mean value)	5.9

D4. What industry best describes your organization's industry focus?	Combined
Agriculture & food services	1%
Communications	2%
Consumer products	4%
E-commerce	12%
Education	0%
Energy & utilities	3%
Entertainment & media	2%
Financial services	18%
Gaming	3%
Health & pharmaceuticals	7%
Hospitality	6%
Industrial	2%
Public sector (including non-profits)	5%
Retail	12%
Services	6%
Technology & software	10%
Transportation	5%
Other	1%
Total	100%

D5. Where are your employees located? (Check all that apply):	Combined
United States	86%
Canada	65%
Europe	81%
Middle East & Africa	50%
Asia-Pacific	58%
Latin America (including Mexico)	52%

D6. What is the worldwide headcount of your organization?	Combined
< 100	10%
100 to 500	19%
501 to 1,000	21%
1,001 to 5,000	21%
5,001 to 25,000	17%
25,001 to 75,000	8%
> 75,000	4%
Total	100%
Extrapolated value	10,995

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.