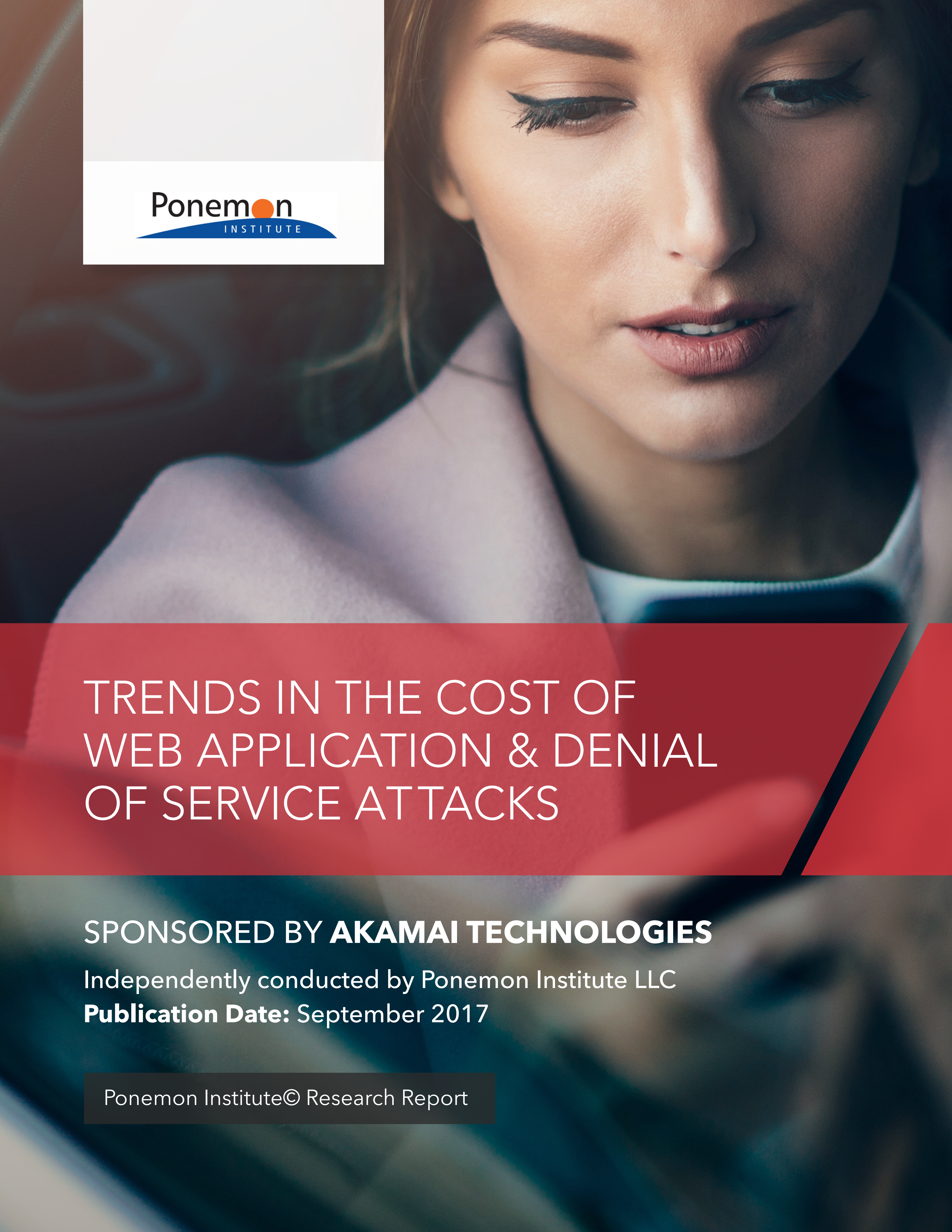


Ponemon INSTITUTE

TRENDS IN THE COST OF WEB APPLICATION & DENIAL OF SERVICE ATTACKS

SPONSORED BY **AKAMAI TECHNOLOGIES**

Independently conducted by Ponemon Institute LLC
Publication Date: September 2017

Ponemon Institute© Research Report

Trends in the Cost of Web Application and Denial of Service Attacks

Ponemon Institute, September 2017

Part 1. Introduction

We are pleased to present the *Cost of Web Application and Denial of Service Attacks,* sponsored by Akamai Technologies. The purpose of this research is to understand changes in the cost and consequences of web application and denial of service attacks since the study was first conducted in 2015. For this study, Ponemon Institute surveyed 621 individuals in IT operations, IT security, IT compliance or data center administration.

Figure 1. Cost of web application security & DoS attacks
US $ thousands

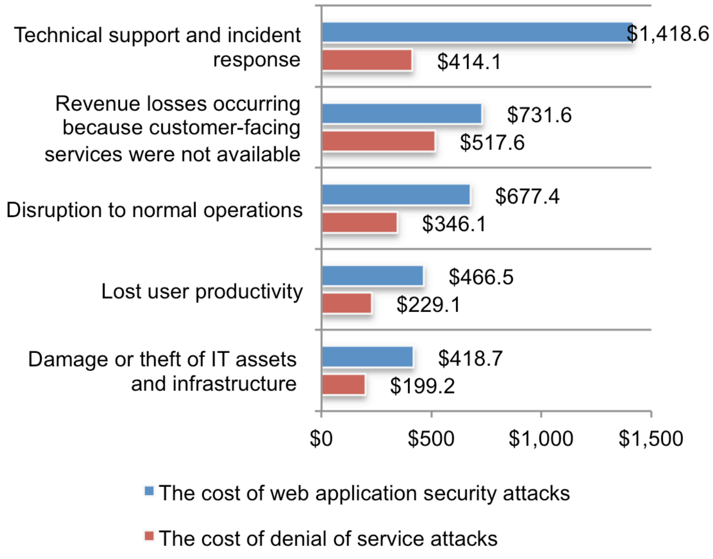


Figure 1 presents five areas of cost that are the consequence of web application security and DoS attacks. The total average cost of web application attacks over the past 12 months increased from $3.1 million to $3.7 million. The total average cost of a DoS attack increased from an average of $1.5 million to $1.7 million.

As shown in Figure 1, web application security attacks are far costlier than DoS attacks. Specifically, companies spent much more on technical support and incident response activities when they faced a web application attack than when they faced a DoS attack ($1,418.6 vs. $414.1). In the case of DoS attacks, revenue losses are the worst financial consequence because customer-facing services are not available.

This report is divided into two sections. The first section (2a) addresses web application security, and the second section (2b) focuses on DoS attacks.

Key takeaways from this study include the following.

- Since the 2015 study, compromises and costs increased, making web application security more critical than ever, according to respondents. However, most companies are testing less than 50 percent of their web applications for vulnerabilities.
- Revenue losses stemming from customer-facing services being unavailable increased from an average of $517.6 million in 2015 to $731.6 million in this year's research.
- It takes just as long to fix one compromised web application in 2017 as it did in 2015.

- Seventy-three percent of companies represented in this research use a web application firewall (WAF) to stop attackers' access to sensitive data. According to these respondents, web-borne malware has bypassed their WAF frequently (8 percent) or sometimes (42 percent).

- Ideally, most companies want a WAF that supports both security and performance. In fact, 40 percent of those respondents who have a WAF believe both security and performance are equally important.

- Most companies in this study (82 percent of respondents) rate themselves as ineffective in preventing DoS attacks.

- In the past year, companies experienced approximately 5 DoS attacks, an increase from 4 in 2015's research.

- System downtime due to DoS attacks increased from an average of 9 hours to almost 11 hours.

- It now takes significantly longer to mitigate just one DoS attack compared to the year 2015 (from 62 minutes to 74 minutes).

- A lack of qualified security personnel is much more of a barrier to preventing DoS attacks than a lack of resources.

- Revenue losses and the need to allocate more resources to technical support are the most significant financial consequences of a DoS attack.

Part 2a. Key findings on trends in web application attacks

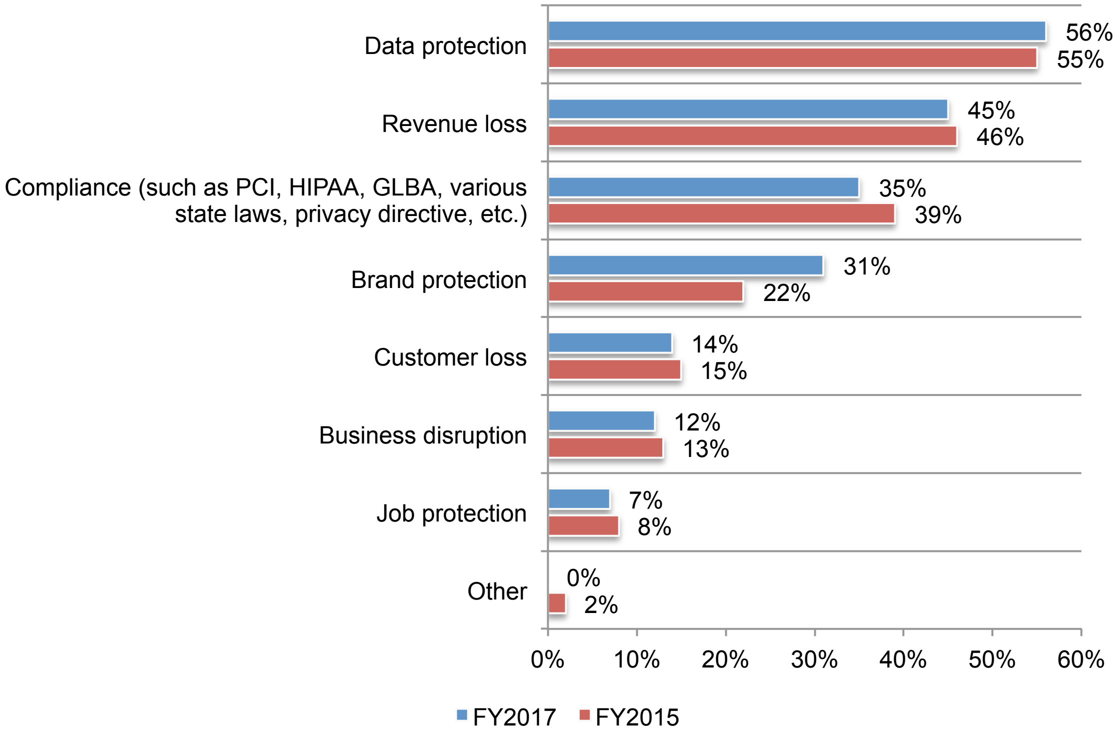
In this section, we present an analysis of the web application findings. This section is organized according to the following topics:

- The importance of safeguarding web applications
- If companies have a web application firewall (WAF), is it effective?
- The cost of web application attacks

The importance of safeguarding web applications

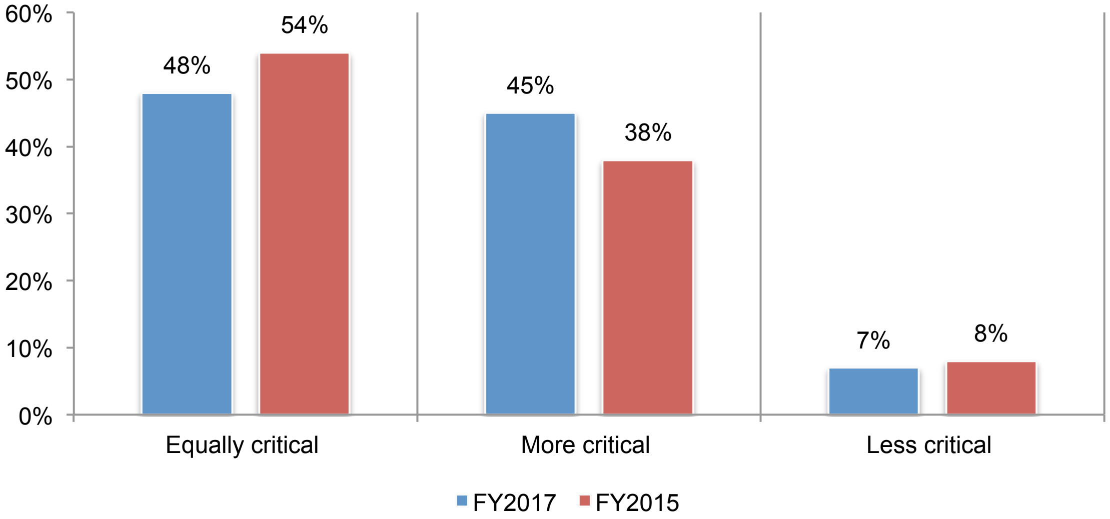
The protection of data continues to be the most important reason for securing web applications. As shown in Figure 2, similar to the findings of the 2015 study, 56 percent of respondents say their organizations secure web applications to protect the sensitive data they contain and to prevent a data breach. This is followed by 45 percent of respondents who want to prevent loss of revenue. Only 35 percent say compliance with regulations is a reason to improve web application security.

Figure 2. Reasons to secure web applications
Two responses allowed



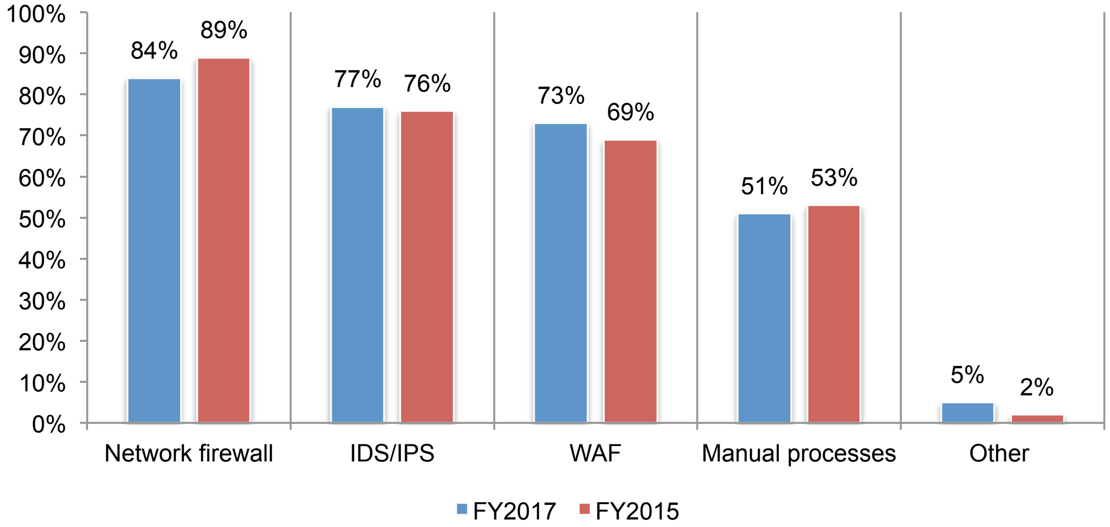
Since 2015, web application security has become more critical for organizations. Web application attacks are a constant threat for companies. As shown in Figure 3 reveals, 45 percent of respondents say web application security is more critical than other security issues faced by their organizations. This is a significant increase from 38 percent of respondents in 2015. Many companies represented in this study (57 percent of respondents) believe that web-hosting providers should assume responsibility for the security of their companies' web applications.

Figure 3. How critical is web application security compared to other security issues?



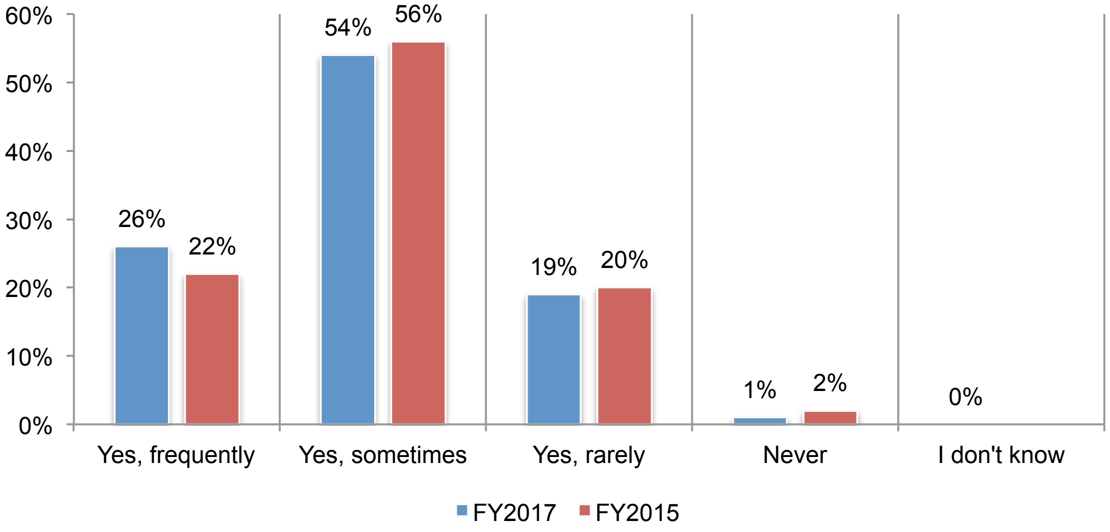
Network firewalls are mostly used to protect web infrastructure. As shown in Figure 4, while network firewalls continue to be the most likely control to be used to protect the web infrastructure until known vulnerabilities are fixed, more WAFs are being used, an increase from 69 percent of respondents.

Figure 4. Until you fix your known vulnerabilities, what controls does your organization put in place to protect web infrastructure?



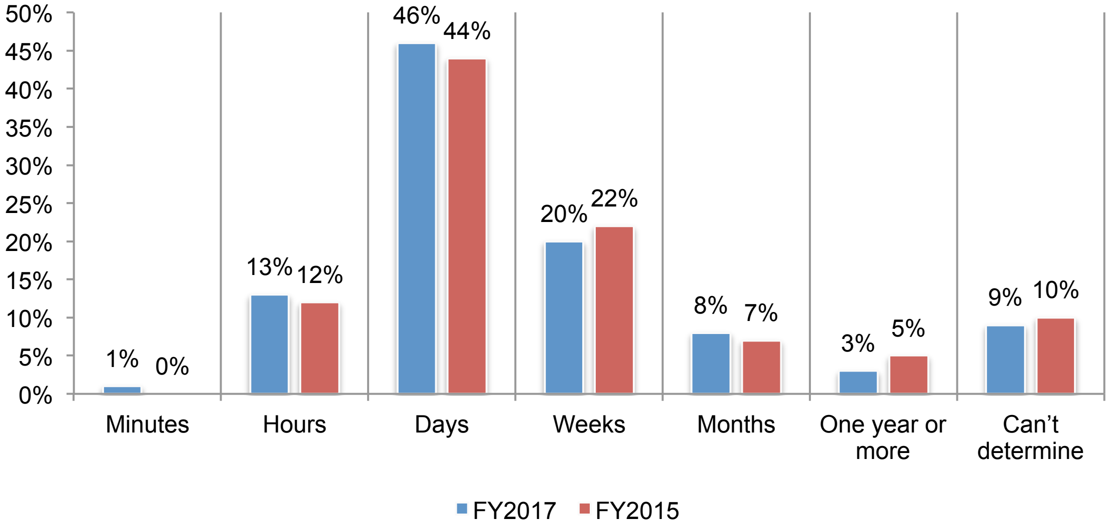
Most organizations continue to have their web applications compromised. As shown in Figure 5 illustrates, 80 percent of respondents say their organizations' web applications have been compromised in the past year (26 percent frequently and 54 percent sometimes), a slight increase from 2015.

Figure 5. Have web applications been compromised in the past 12 months?



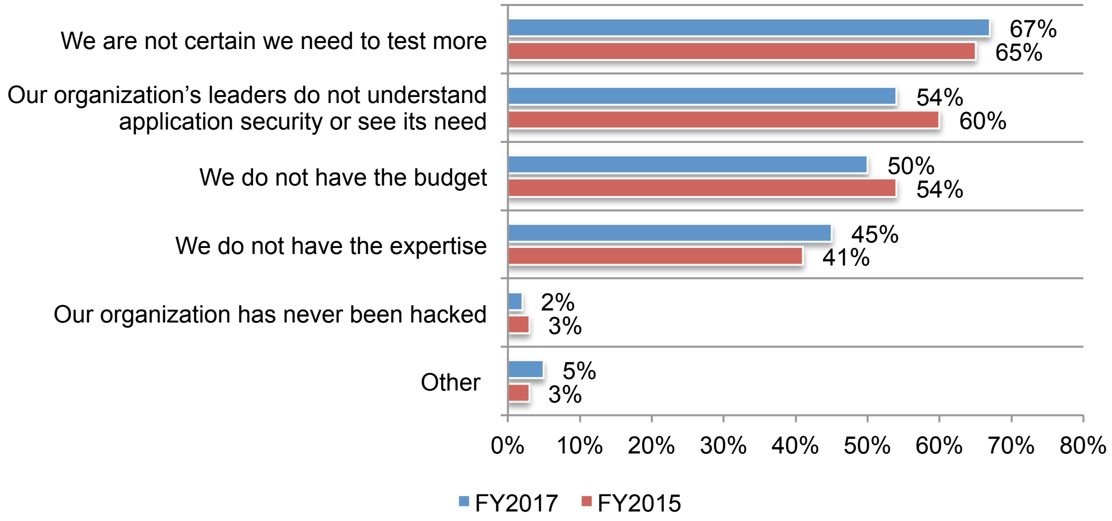
Fixing compromised web applications can take days or weeks. On average, 66 percent of respondents say it takes days (46 percent of respondents) or weeks (20 percent of respondents) to fix one compromised web application whenever vulnerabilities are found, as shown in Figure 6.

Figure 6. How long does it take to fix one compromised web application?



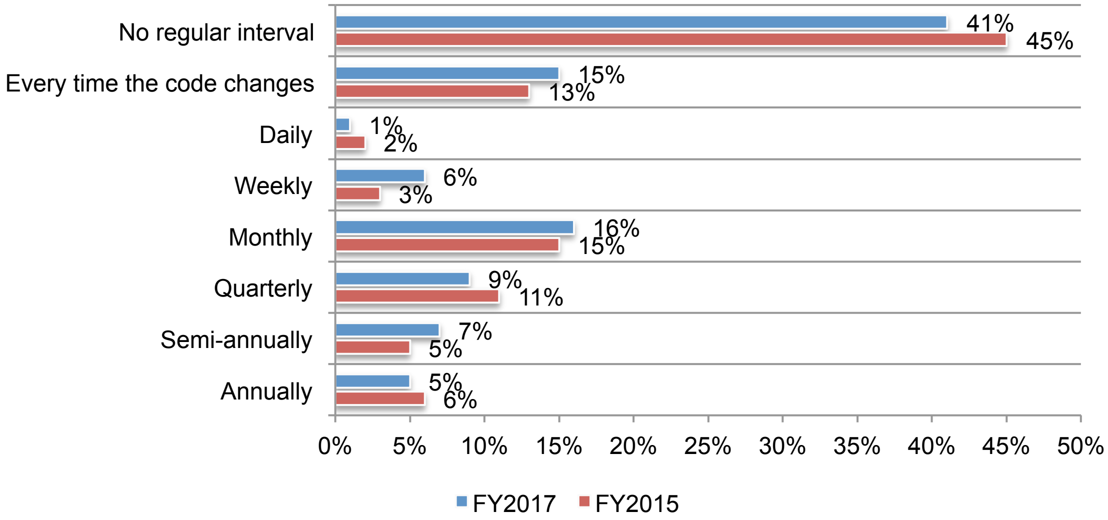
Less than half of web applications are tested for vulnerabilities. On average, 45 percent of web applications are tested for vulnerabilities. There are many obstacles to the comprehensive testing of web applications. According to Figure 7, the top three reasons for not testing at least 50 percent of web applications are: uncertainty whether more web applications need to be tested (67 percent of respondents), leaders do not understand applications security or see its need (54 percent of respondents) or a lack of budget (50 percent).

Figure 7. Why organizations do not test web applications
More than one response permitted



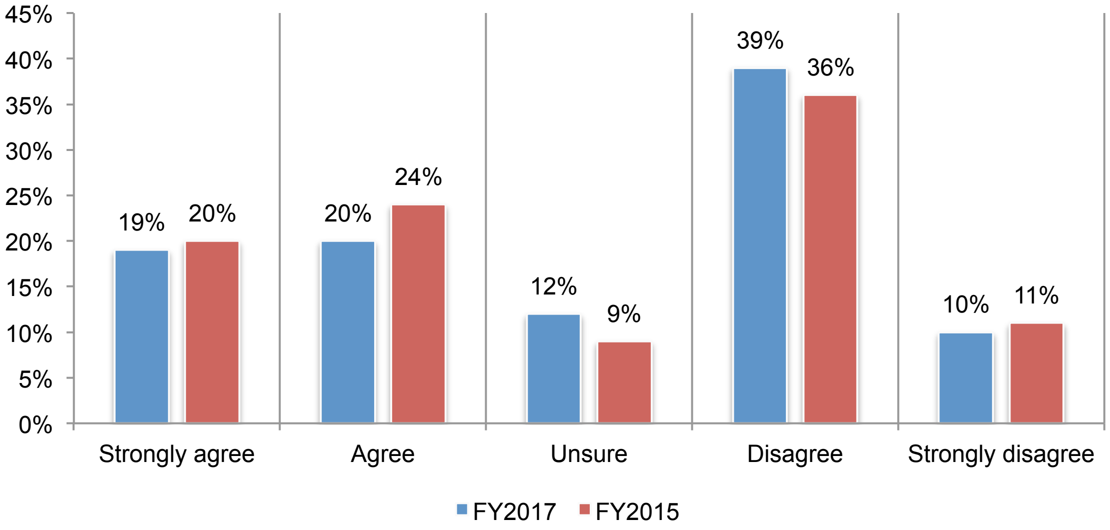
More organizations are testing web applications regularly. Fifty-nine percent of respondents say their organizations are testing web applications on a regular basis, as shown in Figure 8. Those respondents who say they **do not test** on a regular basis declined from 45 percent to 41 percent. Sixteen percent of respondents say their companies test web applications monthly and 15 percent of respondents say their companies test web applications every time the code changes.

Figure 8. How often does your organization test its web applications?



Expectations are low that WAFs will stop all web-borne malware. All respondents in this research were asked if they expect a WAF to stop **all** web-borne malware, including malware without a known signature. As shown in Figure 9, only 39 percent of respondents strongly agree (19 percent) or agree (20 percent) that WAFs are capable of stopping all such malware.

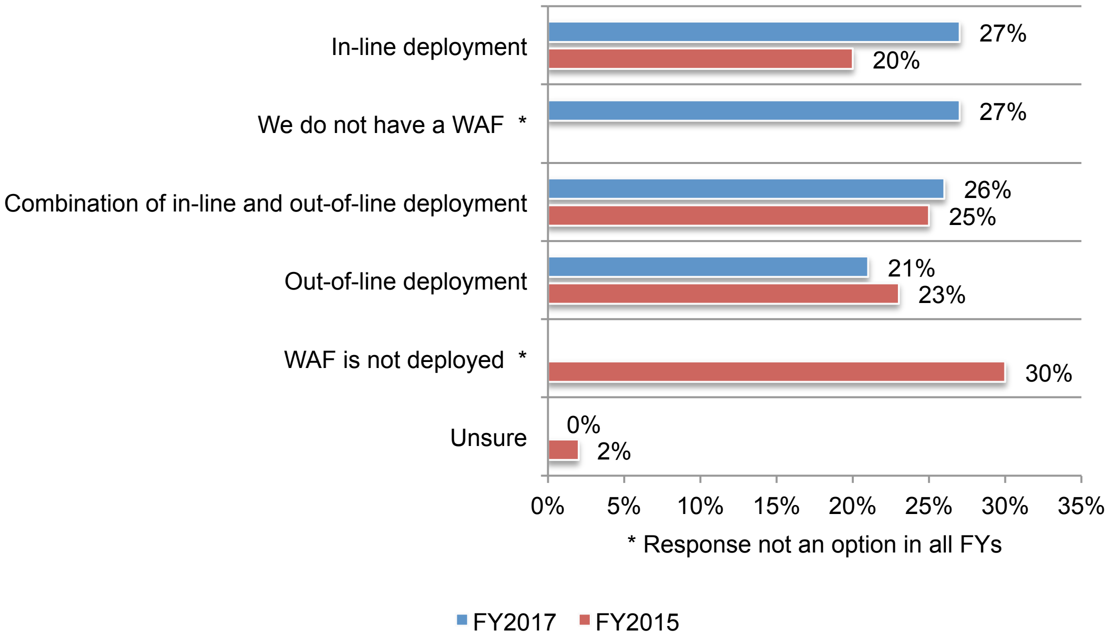
Figure 9. Expectations regarding WAFs



A WAF can be an effective technology for preventing attacks on web applications. A WAF can be deployed in several ways with the goal of preventing application attacks from compromising web servers and their corresponding databases. Only 27 percent of respondents say their organizations do not have a WAF. Seventy-three percent of respondents say their organizations do have a WAF.

Of the 73 percent of respondents who say their organizations have a WAF, 27 percent have an in-line deployment and 21 percent of respondents say their organizations have an out-of-line deployment, as can be seen in Figure 10. In this year's study, we did not ask if they had a WAF that was not deployed.

Figure 10. What best describes your organization's approach to WAF?

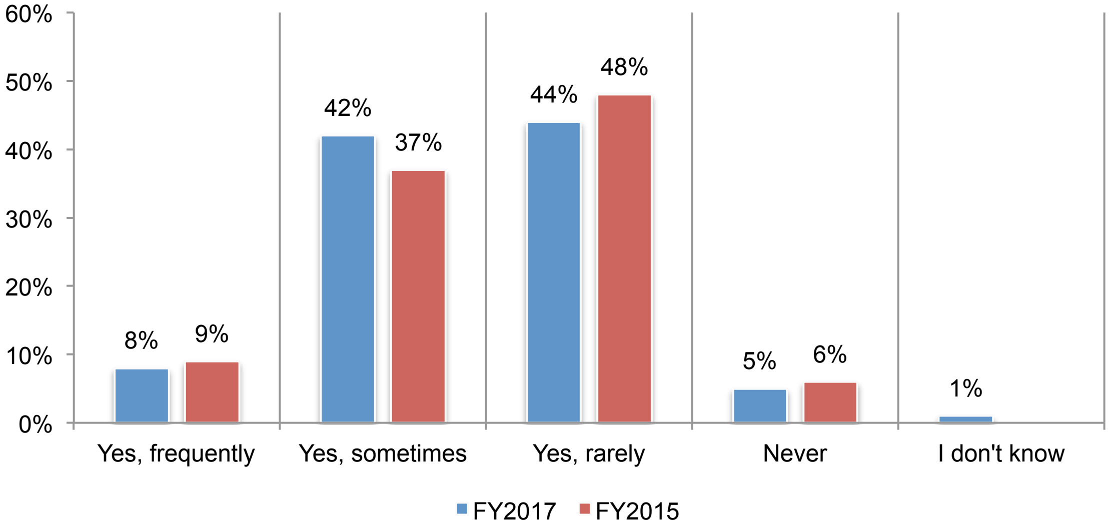


If companies have a web application firewall (WAF), is it effective?

In this section, only responses from participants whose organizations have a WAF are shown (73 percent of respondents).

Web-borne malware continues to bypass WAFs. As discussed above (see Figure 10), respondents do not expect WAFs to stop all web-borne malware. As Figure 11 illustrates, 50 percent of respondents say web-borne malware has bypassed their WAF frequently (8 percent) or sometimes (42 percent). This is a slight increase from 46 percent of respondents in 2015.

Figure 11. In the past 12 months, has web-borne malware ever bypassed your WAF?

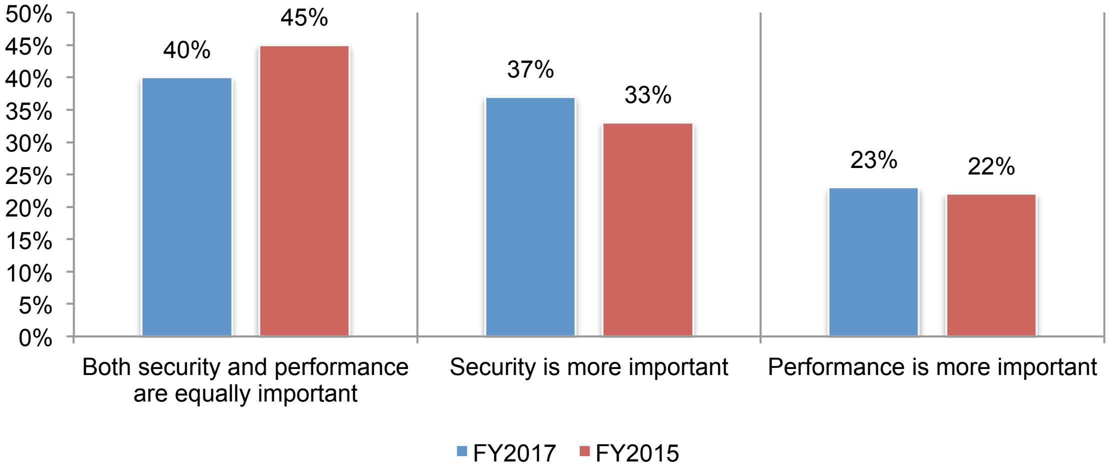


A WAF should support both security and performance. While performance is an attribute often overlooked for security solutions, the majority of respondents place a high value on performance for a WAF solution. This is likely due to the number of different respondent roles either responsible for managing the WAF or whose responsibilities may be impacted by the slow performance of a WAF.

Seventy-three percent of respondents say a fully functional WAF is one that optimizes both performance and security. This is an increase from 65 percent of respondents in 2015.

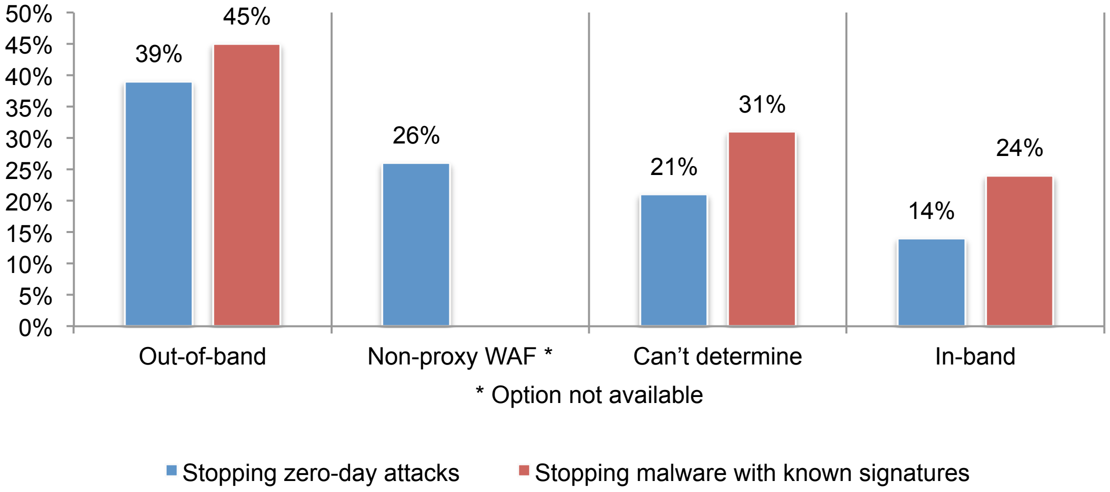
According to Figure 12, when asked if security or performance is more important when deploying a WAF, 40 percent of respondents say both are equally important. Only 37 percent say security is more important, a slight increase from 2015's data, while even fewer respondents (23 percent) say performance is more important.

Figure 12. What is more important for WAF deployment: security or performance?



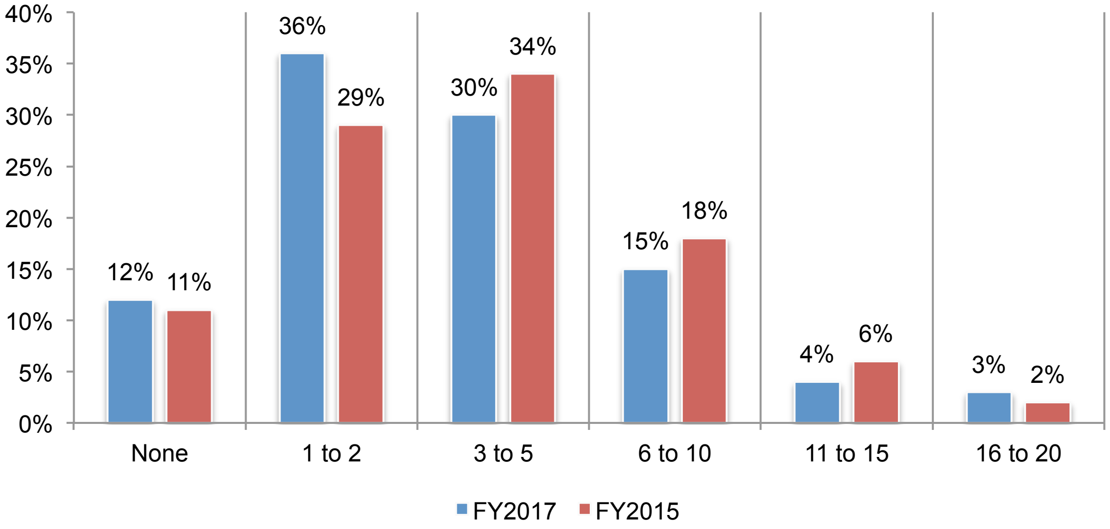
When asked what type of WAF is most effective at stopping zero-day attacks and malware with known signatures, more respondents believe out-of-band WAFs are most effective in stopping malware with known signatures and zero-day attacks, as shown in Figure 13.

Figure 13. Which WAF is most effective?



Companies are becoming more efficient at managing WAFs. As shown in Figure 14, slightly more than a third (36 percent) of respondents say only 1 or 2 employees (on a full-time equivalent basis) are required to properly manage a WAF. This is a significant increase from 30 percent who said they only needed 1 or 2 employees in 2015.

Figure 14. How many employees (on a full-time equivalent basis) are needed to properly manage a WAF?



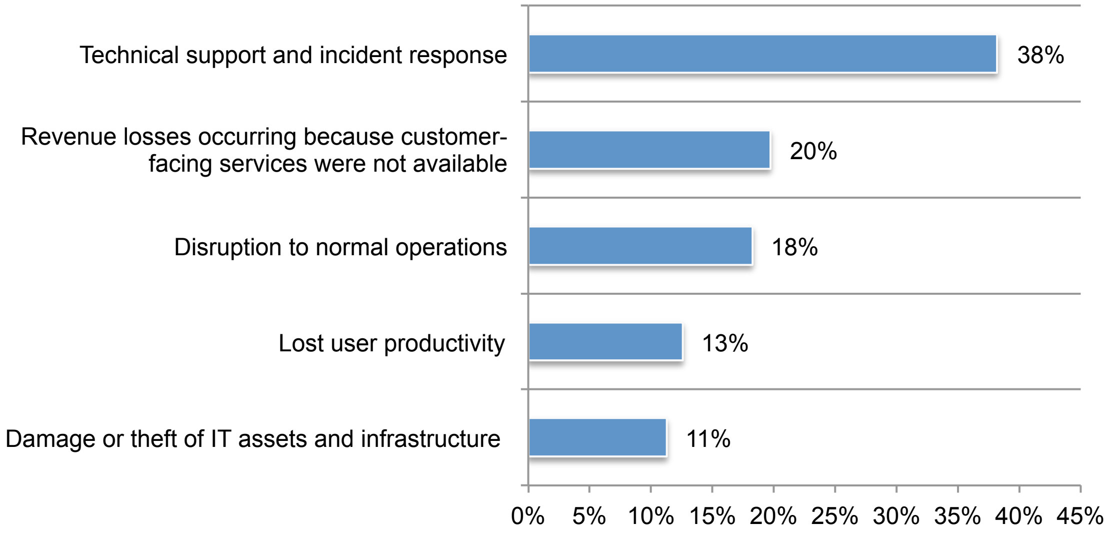
The cost of web application attacks

Companies face growing revenue losses from web application attacks because customers are unable to purchase goods and services. The average total cost per year to deal with attacks against web applications is approximately $3.7 million. As shown in Table 1, this includes technical support and incident response ($1.4 million), lost user productivity ($466,500), disruption to normal operations ($677,411), damage or theft of IT assets and infrastructure ($418,712) and revenue losses due to customer-facing services not being available ($538,745).

Table 1. The cost of web application attacks (over the past 12 months)	**Extrapolated value FY2017**	**Extrapolated value FY2015**
Technical support and incident response costs	$1,418,555	$1,227,618
Lost user productivity	$466,500	$382,555
Disruption to normal operations	$677,411	$613,636
Damage or theft of IT assets and infrastructure	$418,712	$374,655
Revenue losses because customer-facing services were not available	$731,609	$538,745
Total	$3,712,787	$3,137,209

As shown in Figure 15, the largest percentage of cost related to web application attacks is technical support and incident response (38 percent). Damage or theft of IT assets and infrastructure is the smallest (11 percent).

Figure 15. Breakdown of the cost of web application attacks



Part 2b. Key findings on trends in denial of service attacks

In this section, we present an analysis of DoS attacks. This section is organized according to the following topics:

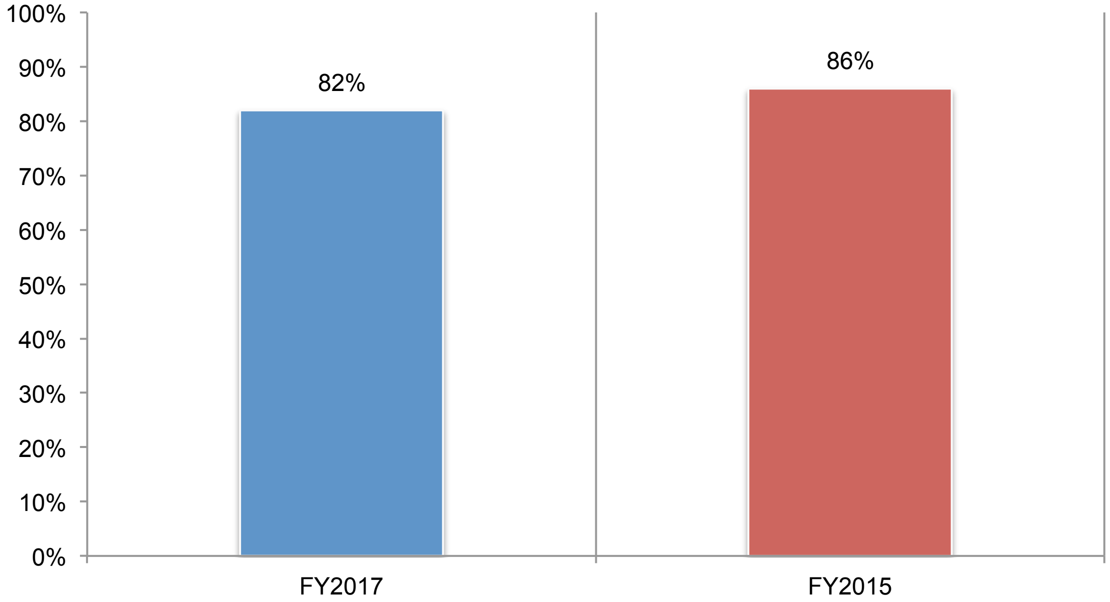
- The growing threat of DoS attacks
- The financial consequences of a DoS attack

The growing threat of DoS attacks

Eighty-two percent of respondents say their companies are ineffective at preventing DoS attacks. Companies are experiencing more DoS attacks. On average, in the past year, organizations experienced approximately 5 DoS attacks, an increase from 4 in 2015's research. Moreover, system downtime increased from an average 9 hours to almost 11 hours. Further, it is taking significantly longer to mitigate just one DoS attack. The time has increased from just over one hour (62 minutes) to 74 minutes.

As a consequence, when asked to rate their organization's effectiveness at preventing DoS attacks on a scale from 1 = low effectiveness to 10 = high effectiveness, 82 percent of respondents rate their organizations as ineffective (less than 6 on the scale of 1 to 10), as shown in Figure 16.

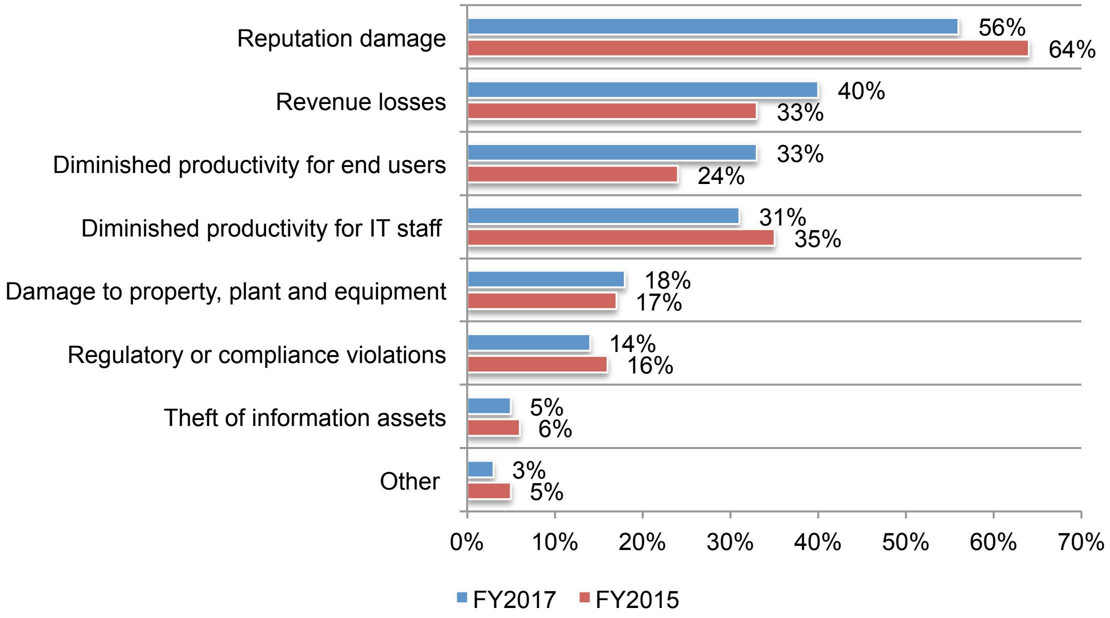
Figure 16. Our organization is not effective at preventing DoS attacks
Percentage of respondents who rate their organization as low (1-6 ratings on a scale of 1 = low to 10 = high)



The number one consequence of a DoS attack is reputation damage. In light of the significant increase in downtime and the time it takes to mitigate one DoS attack, companies suffer reputation damage loss of revenues.

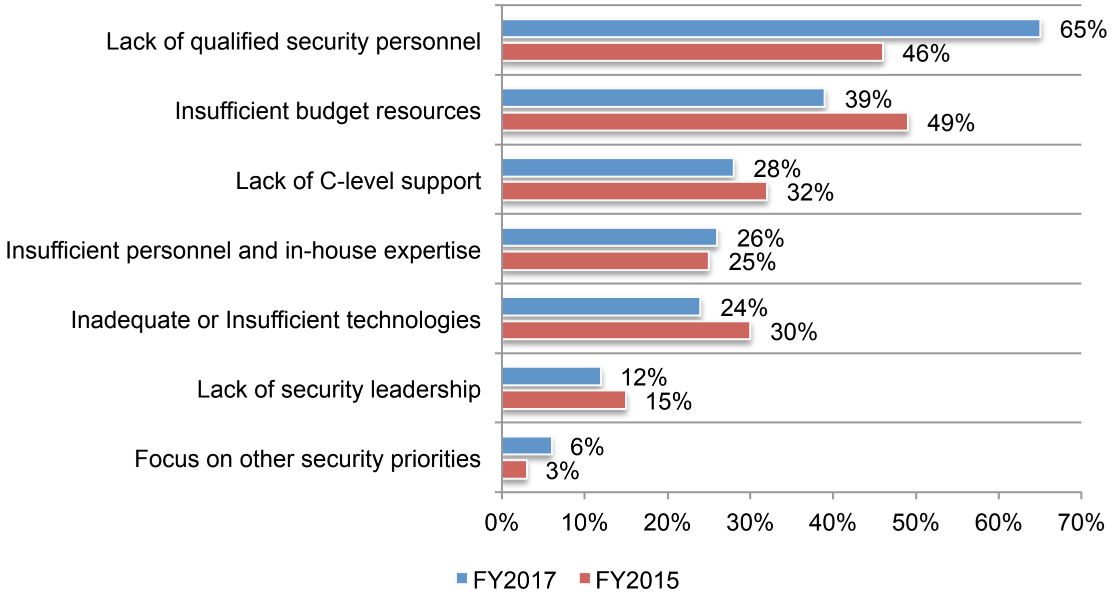
As Figure 17 reveals, 56 percent of respondents say reputation damage is the main consequence of a DoS attack, a decrease from 64 percent in the 2015 study. Diminished productivity for end users increased significantly from 24 percent to 33 percent of respondents in this year's study.

Figure 17. Consequences of a DoS attack
Two responses permitted



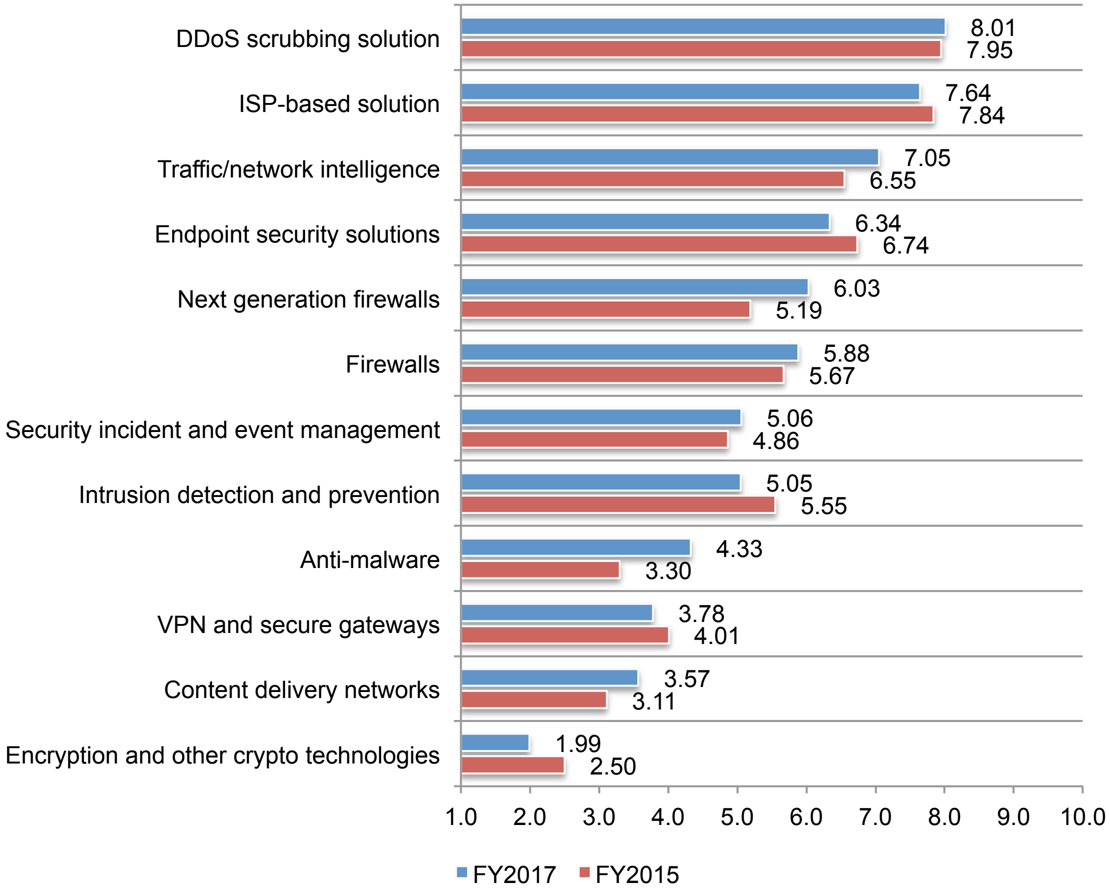
A lack of qualified security personnel is more of a barrier than a lack of resources. The most critical barriers to preventing these threats are lack of qualified security personnel (65 percent). The problem of not having sufficient resources decreased significantly from 49 percent to 39 percent of respondents in this year's research, as shown in Figure 18.

Figure 18. Barriers to preventing DoS attacks
Two responses permitted



Respondents were asked to rank the effectiveness of security technologies considered the most effective at preventing, detecting and containing DoS attacks. Similar to 2015, DDoS scrubbing solutions, ISP-based solutions, endpoint security solutions and traffic/network intelligence are considered the most effective technologies as shown in Figure 19. The effectiveness of next generation firewalls and anti-malware increased the most since 2015.

Figure 19. Most effective technologies to deal with DoS attacks
1 = low to 10 = high



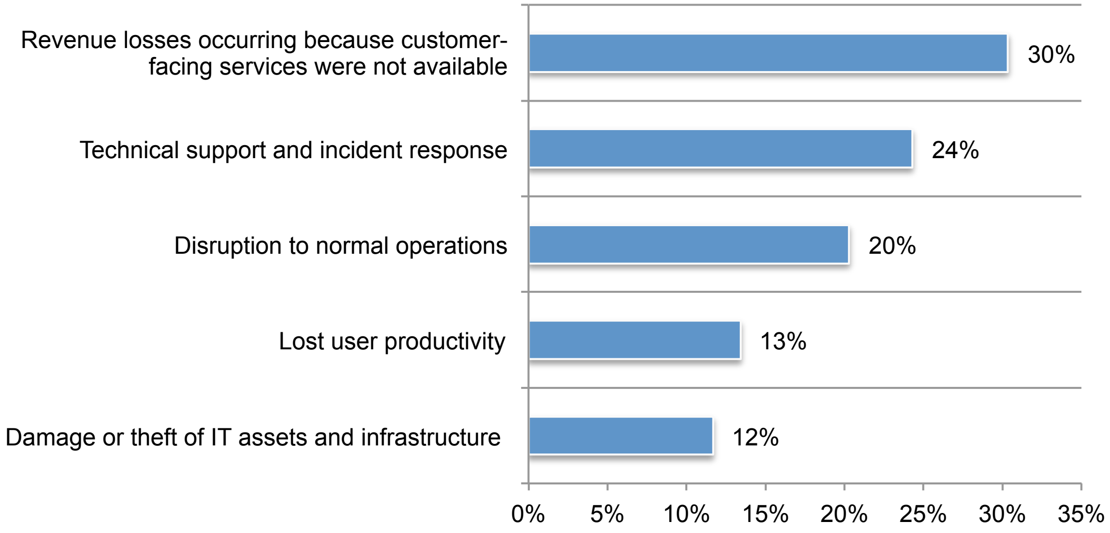
The cost of Dos attacks

Revenue losses and the need to allocate resources to technical support are the most significant financial consequences of a DoS attack. The average total cost per year to deal with a DoS attack is approximately $1.7 million. As shown in Table 2, this includes technical support ($414,128), lost productivity ($229,071), disruption to normal operations ($346,062), damage or theft of IT assets and infrastructure ($199,201) and revenue losses due to customer-facing services not being available ($517,599).

Table 2. The financial consequences of a DoS attack	Extrapolated value FY2017	Extrapolated value FY2015
Revenue losses occurring because customer-facing services were not available	$517,599	$491,152
Technical support	$414,128	$347,685
Disruption to normal operations	$346,062	$325,180
Lost user productivity	$229,071	$173,169
Damage or theft of IT assets and infrastructure	$199,201	$158,320
Total	$1,706,061	$1,495,506

According to Figure 20, the largest percentage of cost is the loss of revenue because customer-facing services were unavailable (30 percent), whereas damage or theft of IT assets and infrastructure is the smallest (12 percent).

Figure 20. Breakdown of the financial consequences of a DoS attack



Part 3. Methods

The sampling frame is composed of 17,651 IT and IT security practitioners located in the United States. As Table 3 demonstrates, 669 respondents completed the survey. Screening removed 48 surveys. The final sample consisted of 621 surveys (for a 3.4 percent response rate).

Table 3. Sample response	Freq	Pct%
Total sampling frame	17,651	100.0%
Total returns	669	3.8%
Rejected or screened surveys	48	0.4%
Final sample	621	3.4%

Figure 21 reports the current position or organizational level of the respondents. More than half of respondents (57 percent) reported their current position as supervisory or above.

Figure 21. Current position or organizational level

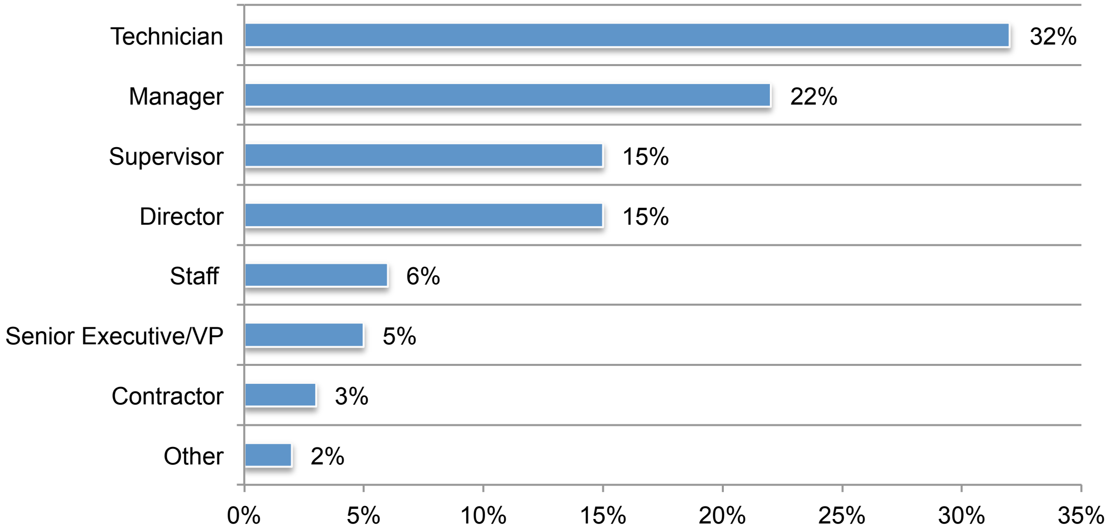


Figure 22 identifies the primary person to whom the respondent reports to. Fifty-three percent of respondents identify the chief information officer as the person to whom they report to. Another 21 percent indicate the chief information security officer as the person to whom they directly report.

Figure 22. Direct reporting channel

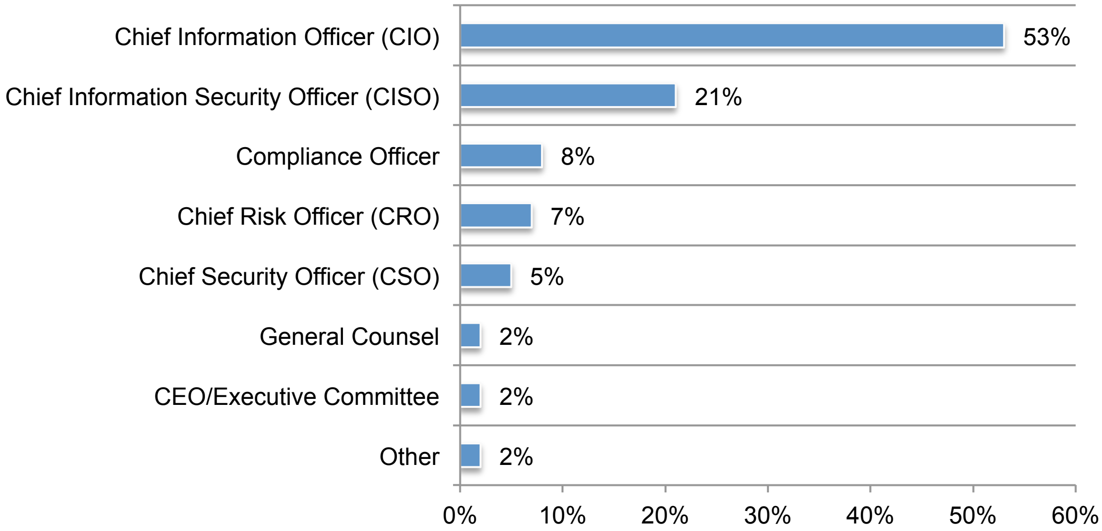
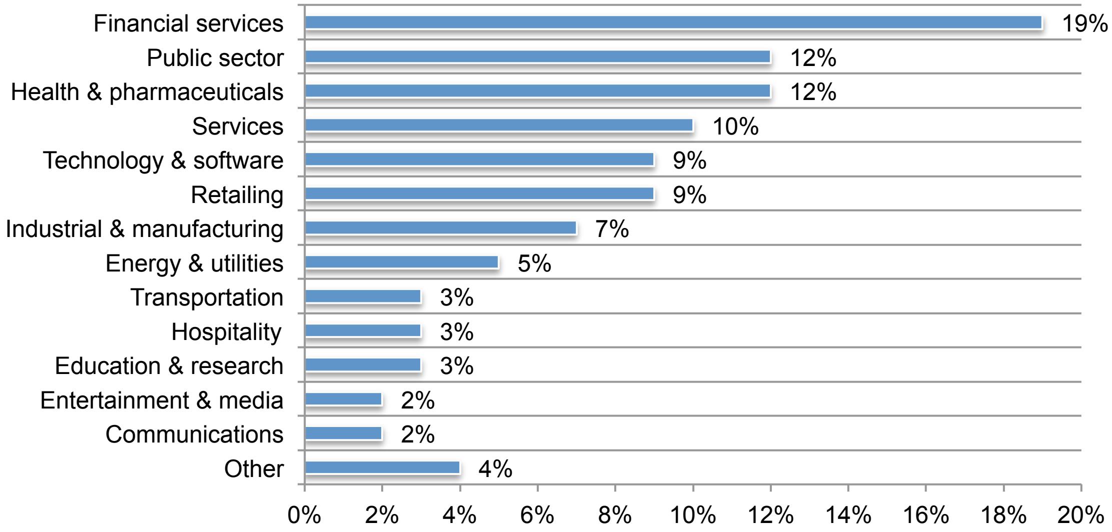


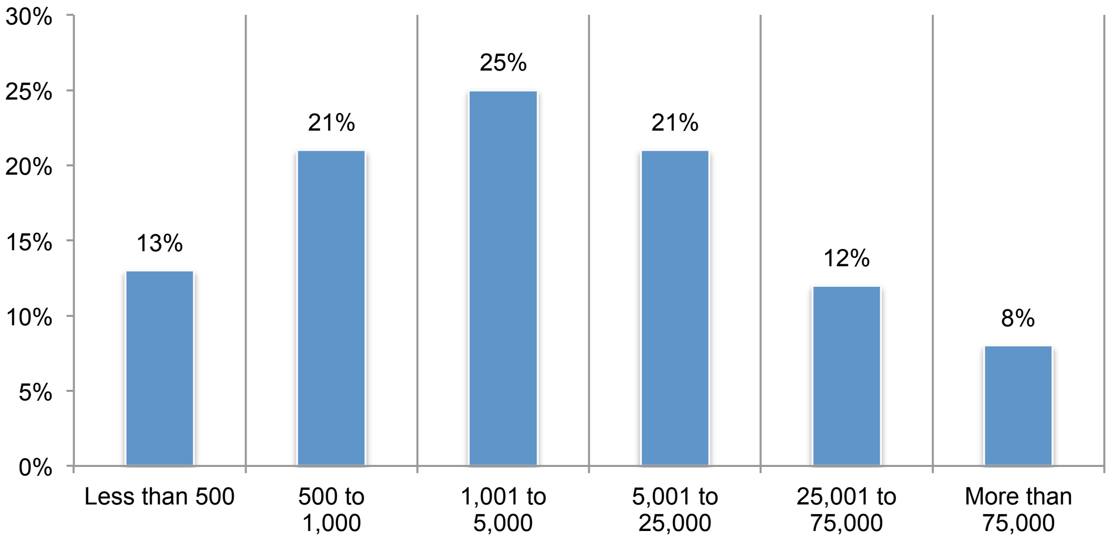
Figure 23 reports the primary industry classification of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by health and pharmaceuticals (12 percent) and public sector (12 percent).

Figure 23. Primary industry focus



According to Figure 24, more than half of the respondents (66 percent) are from organizations with a global headcount of more than 1,000 employees.

Figure 24. Worldwide headcount of the organization
Extrapolated value = 16,510



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.

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.