The Cost of Denial-of-Services Attacks

Sponsored by
Akamai Technologies

Independently conducted by Ponemon Institute LLC

Publication Date: March 2015

Ponemon Institute© Research Report

The Cost of Denial-of-Service Attacks

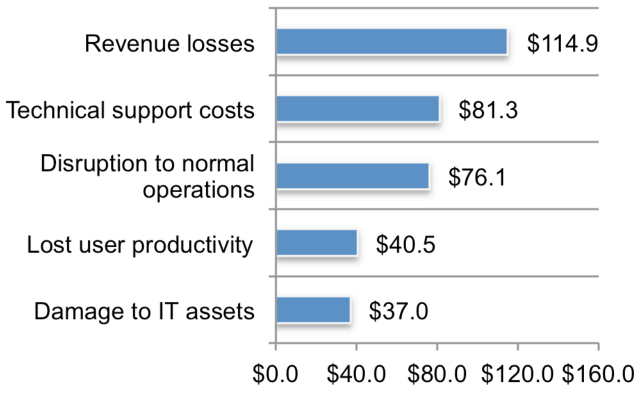
Ponemon Institute, March 2015

Part 1. Introduction

We are pleased to present the findings of *The Cost of Denial-of-Service Attacks* sponsored by Akamai Technologies. The purpose of this research is to understand the cost and consequences of these security threats. Ponemon Institute surveyed 641 individuals involved in preventing, detecting and/or containing denial-of-service attacks against their organizations. Most participants in this research work in IT operations, IT security, IT compliance or data center administration.

Figure 1. Average per attack costs of DoS

$1,000 omitted



A denial-of-service (DoS) attack occurs when the criminal prevents legitimate users from accessing information or services. By targeting a company's computers and its network connection an attacker can cause costly disruptions to operations and damage to its reputation and trustworthiness. The following is a summary of the cost and consequences of DoS attacks:

- **DoS attacks are costly.** Companies in this study reported an average of $1.5 million in costs related to DoS over the past 12 months. On average, these companies had four DoS attacks in the past 12 months. The average costs for each DoS attack is summarized in Figure 1. As shown, the most expensive cost component concerns customer–facing revenue losses because of IT availability gaps or downtime.

- **Data center downtime due to a denial-of-service attack happens frequently.** Eighty-two percent of respondents say the denial-of-service attack shut down the entire data center (34 percent) or part of the data center (48 percent). On average, during the past 12 months respondents say their systems were shut down 9 hours.

- **The number one consequence of a DoS attack is reputation damage**. Sixty-four percent of respondents say reputation damage is the main consequence of a denial-of-service attack. This is followed by diminished productivity for IT staff (35 percent) and revenue losses (33 percent).

- **Denial-of-service attacks will increase**. Forty-four percent of respondents say denial-of-service attacks increased over the past year and 49 percent say they will increase over the next 12 months. The most critical barriers to preventing these threats are insufficient budget resources, lack of qualified security personnel (46 percent) and lack of C-level support.

- **Denial-of-service is in the top three of security threats facing companies.** When asked to indicate which security threats worry them most, 56 percent say it is zero-day attacks, malware (45 percent of respondents) and denial-of-service (38 percent).

Part 2. Key findings

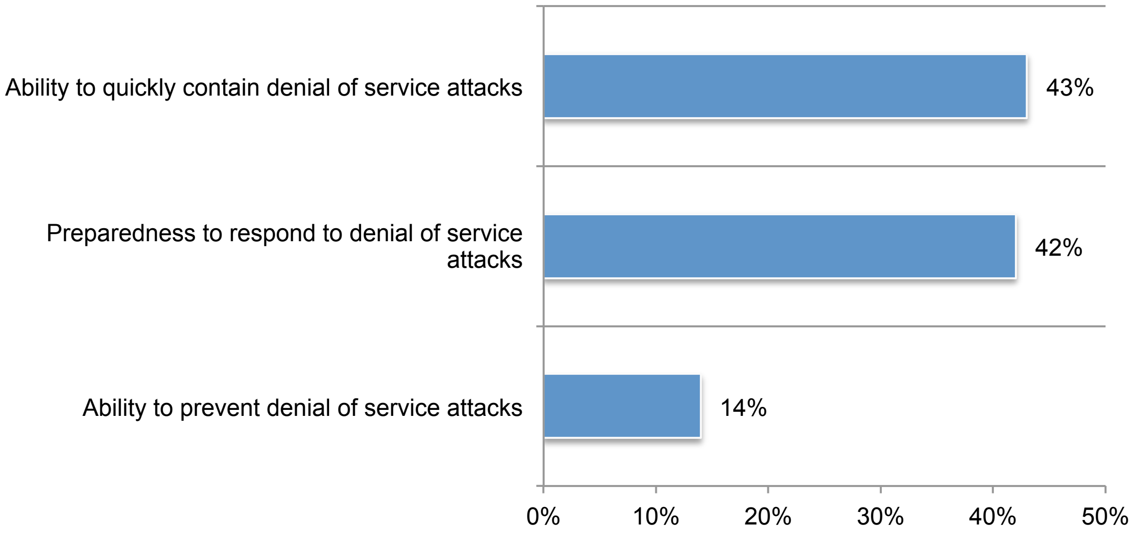
In this section we present an analysis of the key findings.

The following is a summary of key takeaways.

What is the state of denial-of-service attacks in organizations? On average, organizations experienced approximately 4 denial-of-service attacks in the past 12 months. The majority of respondents do not have confidence in their organizations ability to deal with a DoS attack.

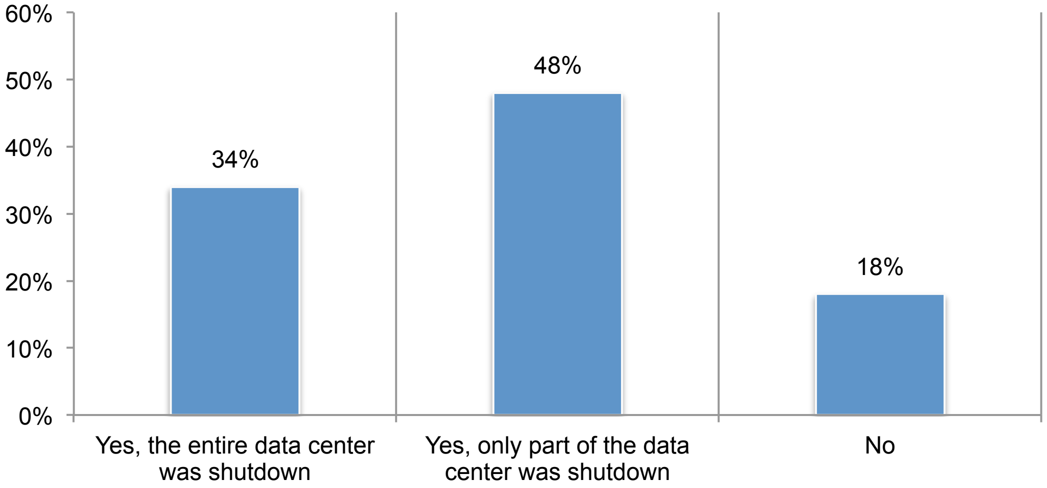
As Figure 2 reveals, only 43 percent rate their organizations highly effective in quickly containing denial-of-service attacks and only 14 percent of respondents rate their ability to prevent denial-of-service attacks as highly effective. Forty-three percent believe they are effective in responding to denial-of-service attacks.

Figure 2. Can organizations deal with a DoS Attack?
Percentage of respondents who rate their organization as high (7+ on a scale of 1 = low to 10 = high)



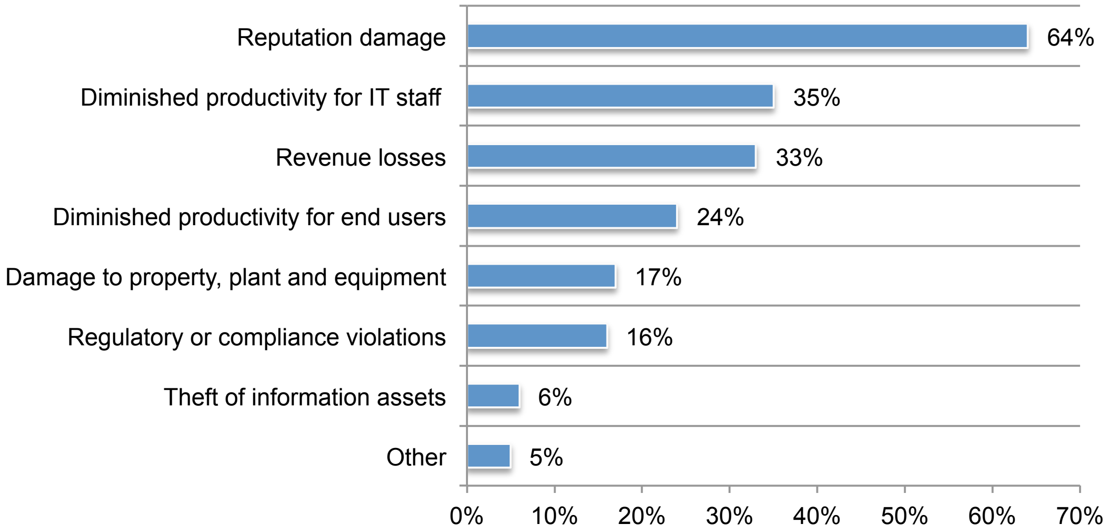
Data center downtime due to a denial-of-service attack happens frequently. According to Figure 3, 82 percent of respondents say the denial-of-service attack shut down the entire data center (34 percent) or part of the data center (48 percent). On average, during the past 12 months respondents say their systems were shut down 9 hours.

Figure 3. Did the DoS attack result in downtime of the data center



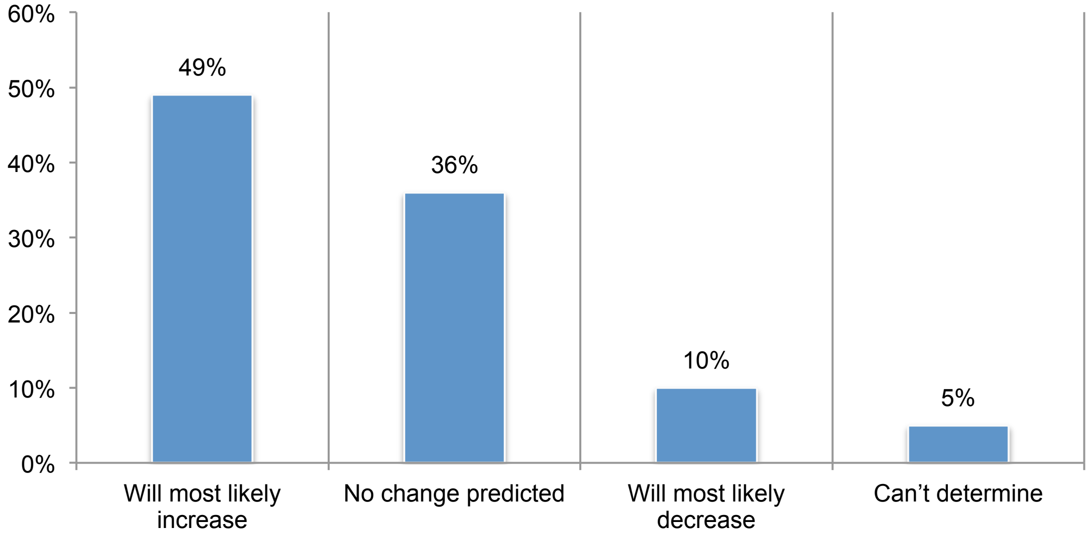
The number one consequence of a DoS attack is reputation damage. As shown in Figure 4, reputation damage, according to 64 percent of respondents is the main consequence of a denial-of-service attack. This is followed by diminished productivity for IT staff (35 percent) and revenue losses (33 percent).

Figure 4. Consequences of a DoS attack
Two responses permitted



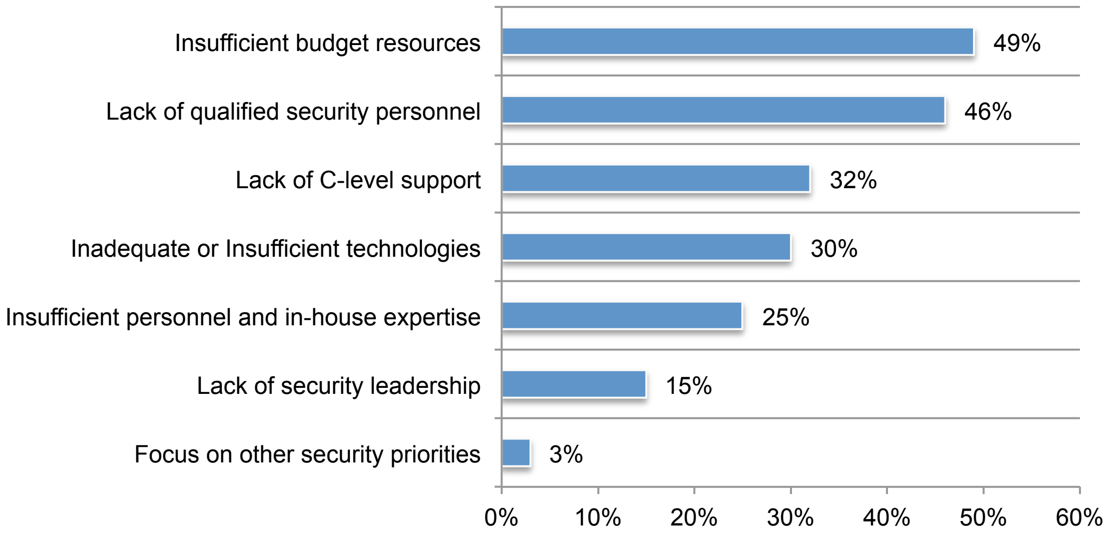
Denial-of-service attacks will increase. According to Figure 5, the DoS threat will continue to plague companies. Forty-four percent of respondents say denial-of-service attacks increased over the past year and 49 percent say they will increase over the next 12 months.

Figure 5. DoS attacks predicted to increase



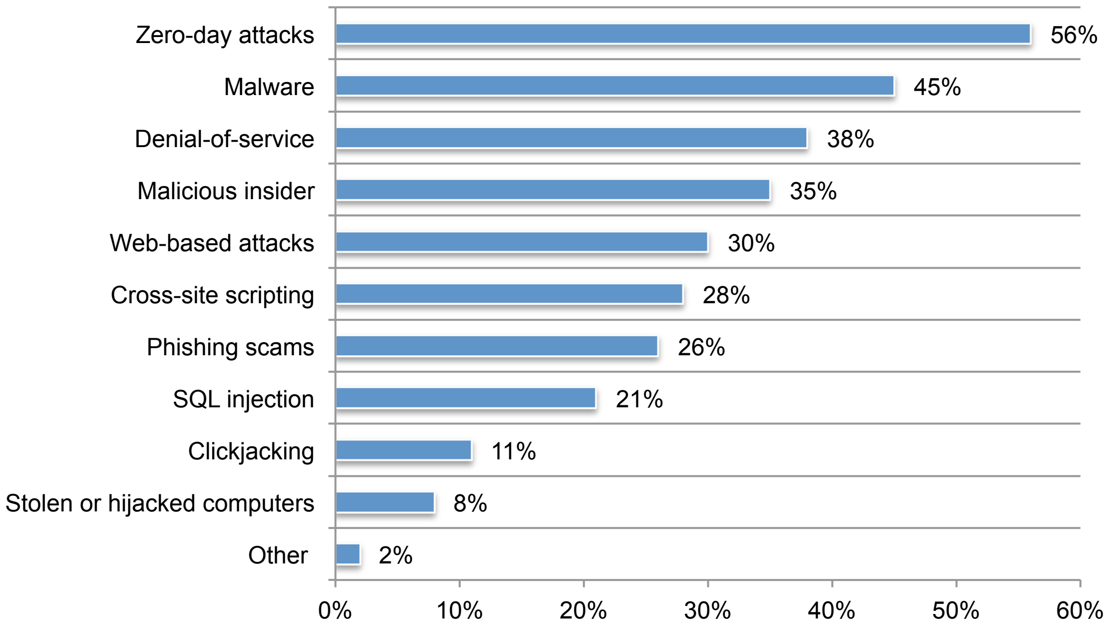
A barrier to stopping DoS attacks is the lack of resources. The most critical barriers to preventing these threats are insufficient budget resources, lack of qualified security personnel (46 percent) and lack of C-level support, as shown in Figure 6.

Figure 6. Barriers to preventing DoS attacks
Two responses permitted



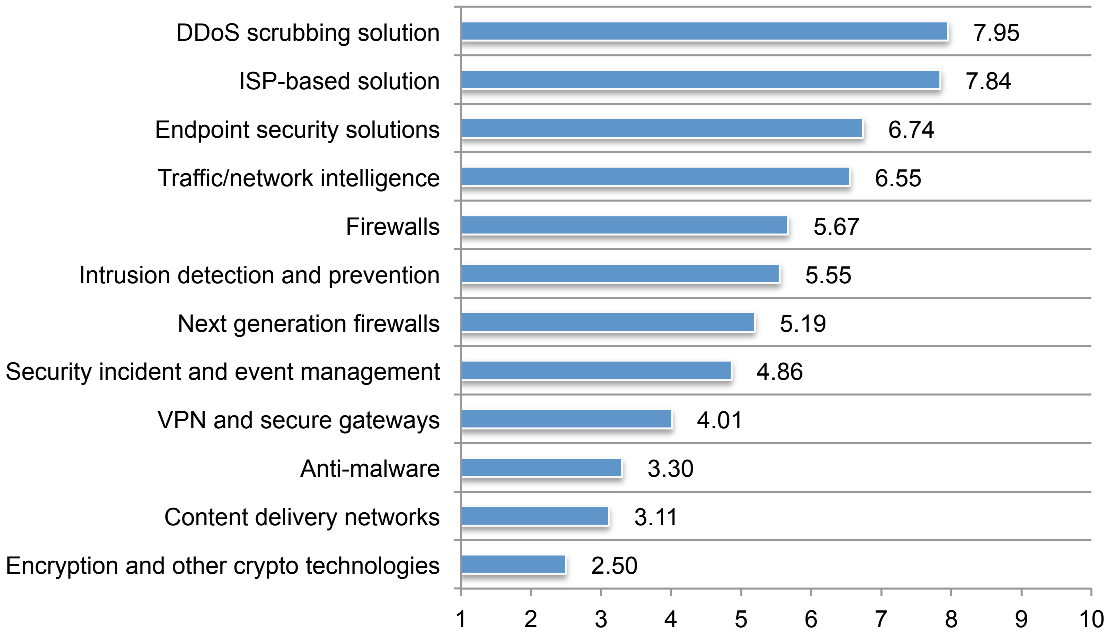
Denial-of-service is in the top three of security threats facing companies. When asked to indicate which security threats worry them most, 56 percent say it is zero-day attacks, malware and denial-of-service, as shown in Figure 7.

Figure 7. Security threats that worry IT
Three responses permitted



The solutions used most often to prevent, detect and contain denial-of-service attacks are: DDoS scrubbing solutions, ISP-based solutions, endpoint security solutions and traffic/network intelligence.

Figure 8. Most effective technologies to deal with DoS attacks
1 = low to 10 = high

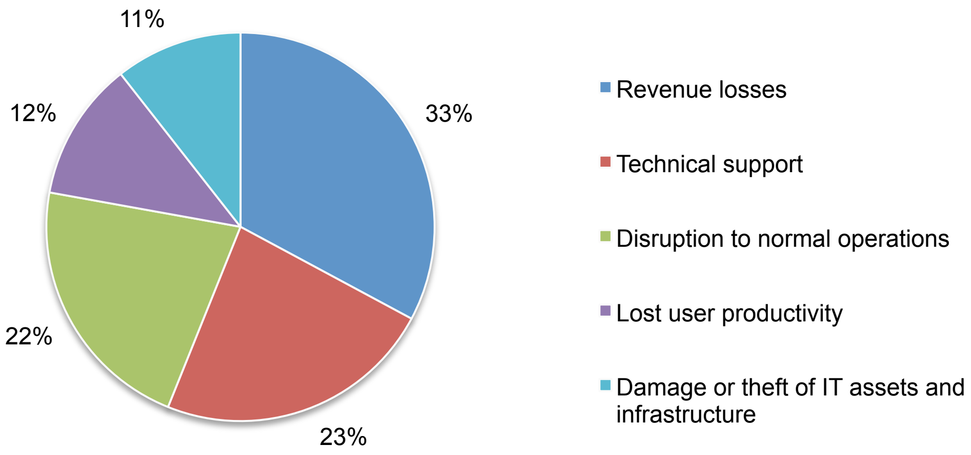


How costly are denial-of-service attacks? The average total cost per year to deal with DoS is approximately $1.5 million. As shown in Table 1, this includes technical support ($347,685), lost productivity ($173,169), disruption to normal operations ($325,180), damage or theft of IT assets and infrastructure ($158,320) and revenue losses due to customer-facing services not being available ($491,152).

Table 1. The financial consequences of a DoS attack	**Extrapolated value**
Revenue losses occurring because customer-facing services were not available	$491,152
Technical support	$347,685
Disruption to normal operations	$325,180
Lost user productivity	$173,169
Damage or theft of IT assets and infrastructure	$158,320
Total	$1,495,506

According to Pie Chart 1, the largest percentage of cost is the loss of revenue because customer-facing services were not available. Damage or theft of IT assets and infrastructure is the smallest.

Pie Chart 1. Breakdown of the financial consequences of a DoS attack



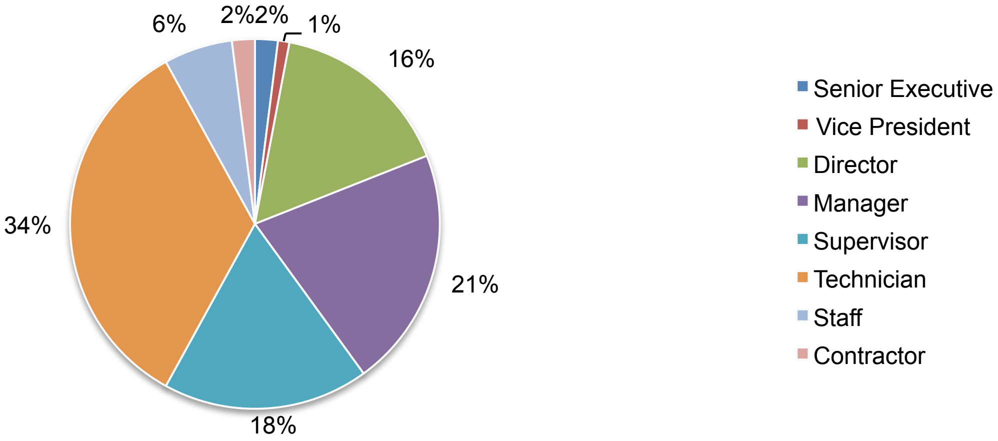
Part 3. Methods

The sampling frame is composed of 16,880 IT and IT security practitioners located in the United States and who are involved in preventing, detecting and/or containing denial-of-service attacks against their organizations. As shown in Table 1, 697 respondents completed the survey. Screening removed 56 surveys. The final sample was 641 surveys (or a 3.8 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	16,880	100.0%
Total returns	697	4.1%
Rejected or screened surveys	56	0.3%
Final sample	641	3.8%

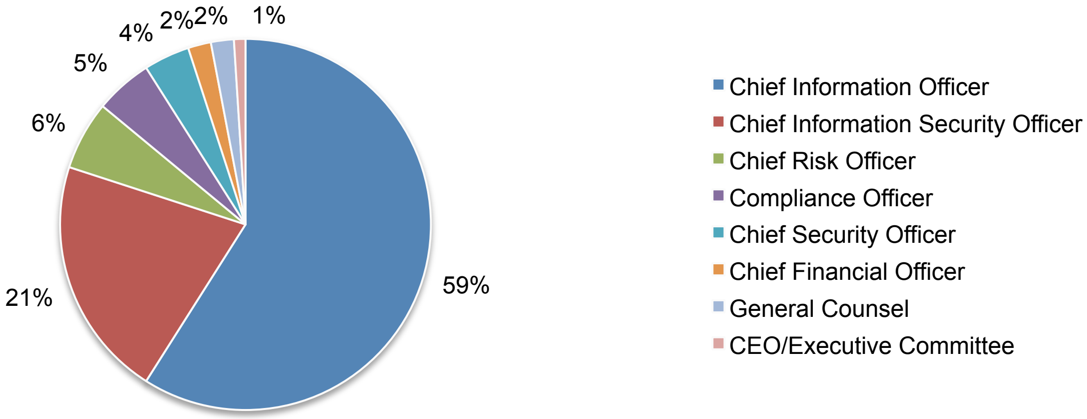
Pie Chart 2 reports the current position or organizational level of the respondents. More than half of respondents (58 percent) reported their current position as supervisory or above.

Pie Chart 2. Current position or organizational level



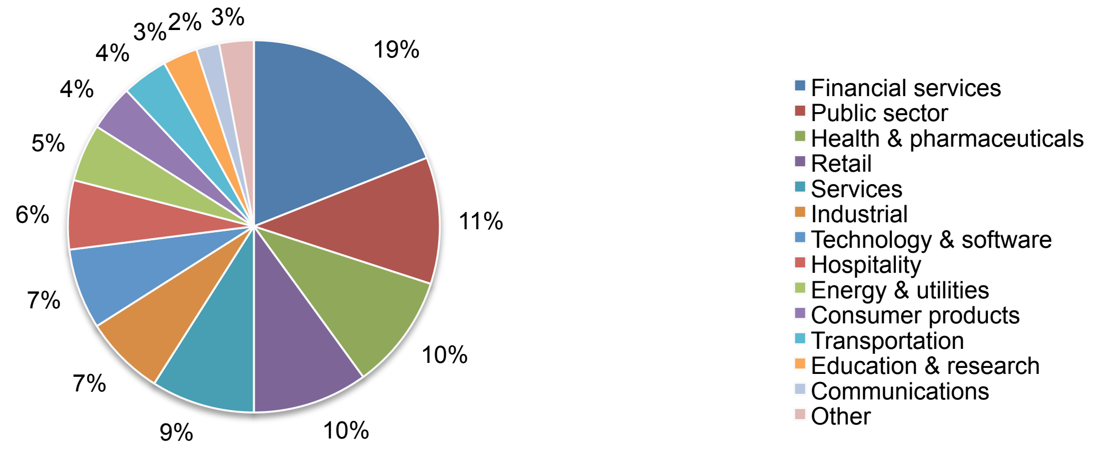
Pie Chart 3 identifies the primary person the respondent reports to. Fifty-nine percent of respondents identified the chief information officer as the person they report to. Another 21 percent indicated they report directly to the CISO.

Pie Chart 3. Direct reporting channel



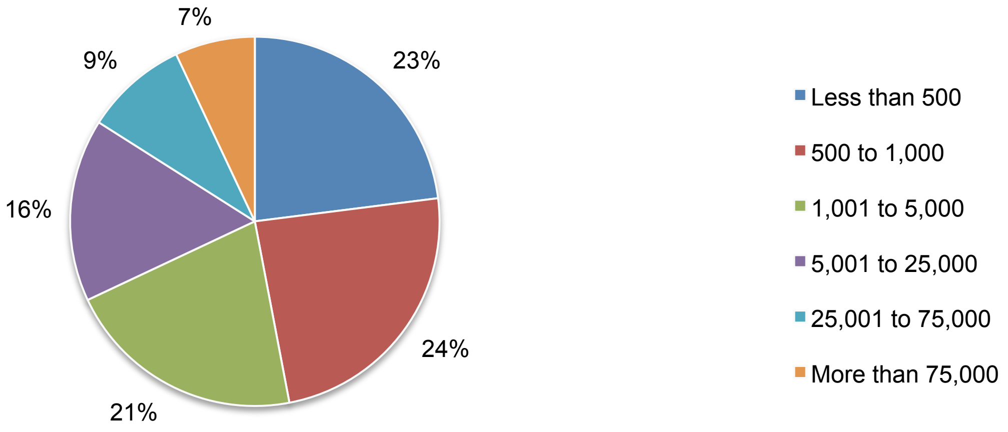
Pie Chart 4 reports the primary industry classification of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by public sector (11 percent), health and pharmaceuticals (10 percent) and retail (10 percent).

Pie Chart 4. Primary industry focus



According to Pie Chart 5, more than half of the respondents (53 percent) are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 5. Worldwide headcount of the organization
Extrapolated value = 13,402



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.