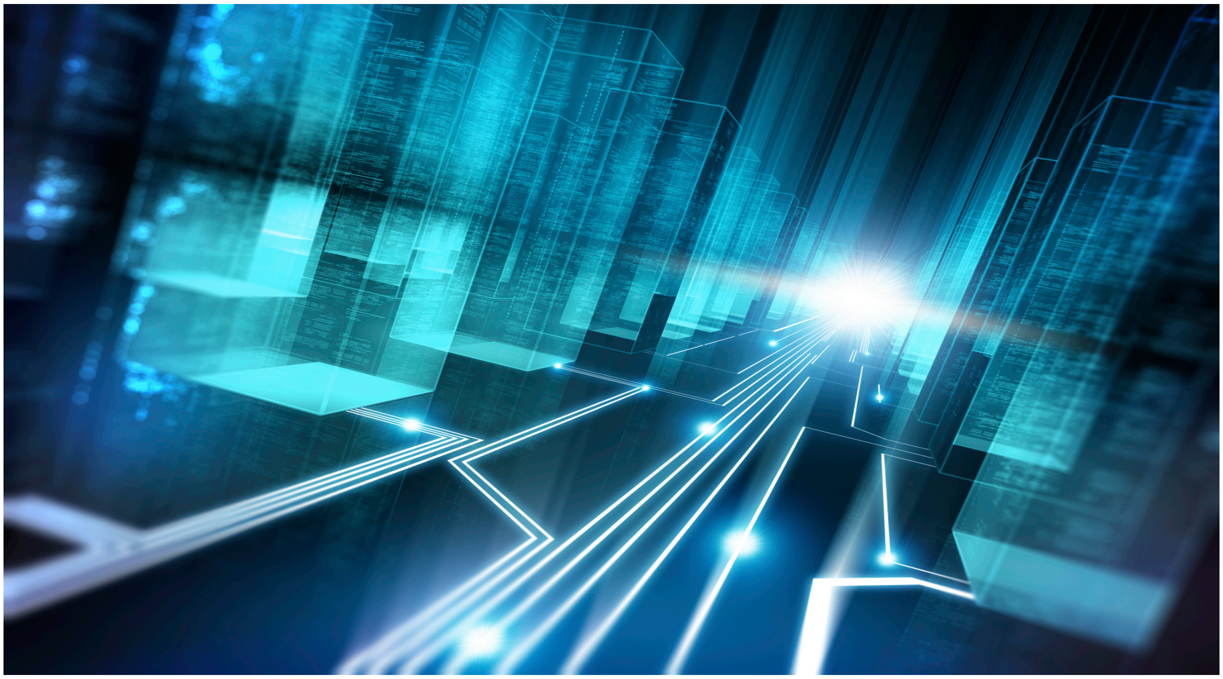


Security Beyond the Traditional Perimeter Executive Summary

Sponsored by BrandProtect™

Independently conducted by Ponemon Institute LLC

Publication Date: July 2016

Security Beyond the Traditional Perimeter

Ponemon Institute: July 2016

Executive summary

Ponemon Institute is pleased to present the findings of *Security Beyond the Traditional Perimeter,* sponsored by BrandProtect^{TM}. The purpose of this study is to understand companies' ability to analyze and mitigate online incidents and cyber attacks that are beyond the traditional security perimeter.

In the context of this survey, external threats are those that arise outside the company's traditional firewall/security perimeter, and use online channels – email, social media, mobile apps, or domains, as their primary attack technology. These threats may or may not cross the firewall as they are perpetrated. Examples of external threats include socially engineered attacks, executive impersonations, brand-based attacks with ransomware, malware, or other payloads, rogue social domain activity, hactivism/activism and activities which violate compliance or regulatory requirements.

In this study, we surveyed 591 IT and IT security practitioners in the United States. Sixty-five percent of these respondents are either CISOs (20 percent) or IT security operations (45 percent). Participants in this study agree external threats put companies' ability to continue their operations in peril.

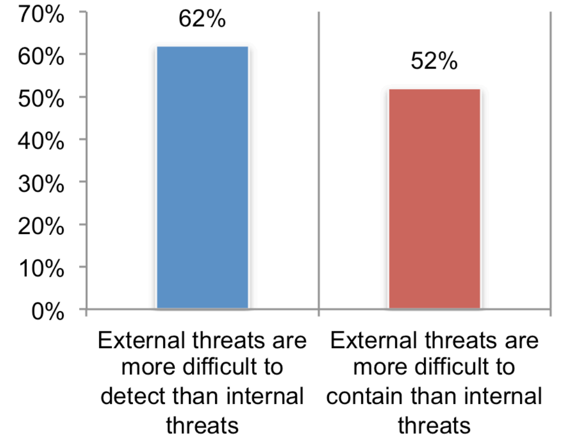
As shown in Figure 1, 62 percent of respondents say external threats are more difficult to detect than internal threats within the security perimeter and 52 percent of respondents say they are more difficult to contain than internal threats within the security perimeter.

The following are four important takeaways from this study.

1. Security processes for Internet and social media monitoring are non-existent, partially deployed or inconsistently deployed, according to 79 percent of respondents.

2. The protection of intellectual property from external threats is essential or very important to the sustainability of their companies, according to 59 percent of respondents.

Figure 1. Perceptions about the difficulty in detecting and containing external threats



3. External attacks are frequent and the financial costs of external attacks are significant. The 505 enterprises and financial institutions surveyed experienced an average of more than one cyber attack each month and spent an average of almost $3.5 million to deal with the attack. This is consistent with other Ponemon Institute research.[1]

[1] *2016 Cost of Data Breach: United States,* sponsored by IBM, May 2016,revealed the average total cost paid to resolve a data breach involving lost or stolen records is $7.01 million. *The State of Cybersecurity in Healthcare Organizations in 2016, sponsored by ESET* February 2016, found that healthcare organizations experience an average of almost one cyber attack per month and spend $1.32 million on DDoS attacks per year.

4. A lack of necessary tools and resources diminishes the ability to respond to external threats. Sixty-one percent of respondents do not believe their company has the tools to mitigate external threats. The lack of tools also affects the ability to monitor, analyze and understand external threats. Specifically, 58 percent of respondents do not believe their companies have tools to monitor external threats and 59 percent of respondents say they do not have the tools and resources necessary to analyze and understand external threats.

The key findings of the study are organized according to the following topics.

- Understanding the threat
- Monitoring of external threats
- Impact of external threats
- Ability to deal with external threats
- Special analysis: Industry differences
- Special analysis: Position level differences

Understanding the threat

Companies in this study experience an average of more than one external attack each month. Respondents say their companies have experienced an average of 32 material attacks against employees, executives, physical assets, locations and IP or brand/reputation over the past 24 months. The 505 enterprises and financial institutions surveyed report that an average of 30 percent of these attacks were perpetrated via the Internet or social media.

Cyber exploits and data loss are most likely to occur. When asked to rank nine external threat vectors in terms of the likelihood of occurrence in their organizations, cyber threats and incidents and data loss or theft are the primary threats. Also likely to occur are branded exploits against customers and the public, compliance/regulatory incidents and phishing/social engineering attacks.

The number one worry about an external attack is reputational damage. Fifty-one percent of respondents say they worry most about reputational damage following an external attack. Forty percent of respondents say they are concerned about branded exploits and 33 percent say compliance/regulatory incidents are a concern.

Monitoring of external threats

Monitoring the Internet and social media is critical to gaining intelligence about external threats, but few companies have a formal process in place. Thirty-eight percent of respondents say their companies do not monitor the Internet and social media to determine external threats their companies face. Only 17 percent of respondents say they have a formal process in place that is applied consistently across the entire enterprise. As mentioned above, an average of 30 percent of external attacks are carried out through the Internet or social media.

Monitoring for social engineering activity and cyber incidents is considered critical. While many companies represented in this study are not monitoring the Internet or social media, certain activities are considered essential or very important to detecting and containing external threats against a company.

The most important activities are: monitoring mobile apps (62 percent of respondents), monitoring for social engineering activity or reconnaissance (61 percent of respondents), monitoring cyber incidents (60 percent of respondents), monitoring branded exploits (59 percent of respondents), monitoring for spear-phishing infrastructure (58 percent of respondents) and monitoring phishing scams (57 percent of respondents).

To strengthen security posture, companies should collect phishing IP address data. Sixty percent of respondents say phishing IP addresses are considered essential or very important to reducing external threats. Also important are malicious mobile app details (59 percent of respondents), rogue domain data (54 percent of respondents) and malicious twitter handles (52 percent of respondents).

Cyber threat monitoring is forecasted to increase within the next 24 months. Respondents were asked what security services are implemented for the perimeter, infrastructure and outside the perimeter today and what services will be implemented in the next two years. These services included those in-house and outsourced.

Services outside the perimeter are expected to increase both in house and outsourced. The most significant increase is in cyber threat monitoring according to 51 percent of respondents. The outsourcing of social media monitoring is expected to increase significantly. Today 11 percent of respondents say social media monitoring is outsourced and this is expected to increase, according to 39 percent of respondents.

Insufficient risk awareness is the main barrier to having an effective monitoring approach. Eighty-three percent of respondents believe their organizations are not effective in monitoring the Internet and social media. The main barriers to achieving a more effective monitoring approach are insufficient risk awareness (50 percent of respondents), lack of knowledgeable staff (45 percent of respondents) and lack of technologies and tools (43 percent of respondents).

Despite the lack of in-house expertise and technologies (as shown above), 40 percent of respondents say their organizations are not looking to outsource the monitoring of Internet and social media. Currently, 35 percent of respondents outsource this activity.

Impact of external threats

External attacks have a revenue, operational and reputational impact on companies. Respondents were asked to rate the impact of external attacks on revenue, operations and reputation on a scale of 1 = most significant to 9 = least significant.

External attacks that have the greatest **reputational** impact are branded exploits against customers and the public and hacktivism/activism/physical threats (1.88 and 2.34, respectively). External attacks that have the greatest **revenue** impact are data loss or theft, branded exploits against customers and the public and denial of service (1.67, 2.22 and 2.79, respectively). External attacks that have the greatest **operational** impact are data loss or theft and denial of service (1.90 and 2.17, respectively).

Over the past two years, an average of almost $7 million was spent as a result of material attacks against employees, executives, physical assets, locations, IP or brand/reputation.

Senior executives recognize the risk of external threats to reputation. Sixty percent of respondents say their organizations' leaders recognize that external threats could affect reputation. Fifty-two percent of respondents say their leaders agree revenues could be affected by external threats and 47 percent say these threats could affect the safety and well being of key employees.

Ability to respond to external threats

Actionable intelligence is vital to the detection and containment of external threats. Respondents were asked what factors help companies quickly detect and contain external attacks from 1 = most important to 7 = least important. To respond to external threats, the factors most critical are actionable intelligence, resilience and a strong security posture.

The CIOs' and CISOs' responsibility for threats stops at the perimeter. Responsibility for directing efforts to minimize exposure to business risk stemming from threats on the network or at the security perimeter is concentrated in the chief information officer and chief information security officer function (36 percent and 21 percent of respondents, respectively). In contrast, responsibility for external threats is most often given to the lines of business or no one person.

Only 36 percent of respondents say their companies' security leader (CISO) is very involved (12 percent of respondents) or has some involvement (24 percent of respondents) in the collection and evaluation of intelligence obtained from the Internet and social media.

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

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.