2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)

Sponsored by Keeper Security

Independently conducted by Ponemon Institute LLC

Publication Date: September 2017

2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB)

Ponemon Institute, September 2017

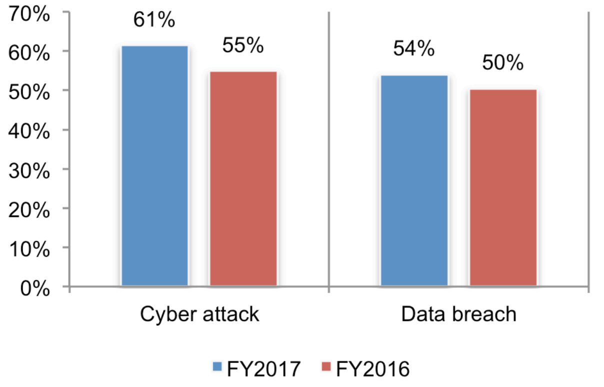
Part 1. Introduction

Cyber attacks, ransomware and disruptive technologies, such as the Internet of Things (IoT), challenge the ability of small businesses to safeguard their information assets. In fact, only 21 percent of the companies represented in this study rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective. Moreover, more than half (51 percent) have experienced either a successful or unsuccessful ransomware attack.

Ponemon Institute is pleased to present the results of the second annual study on *the State of Cybersecurity in Small and Medium-Sized Businesses* sponsored by Keeper Security*.* The goal of the study is to track how smaller companies are addressing the same threats larger companies face. Approximately 600 individuals in companies with a headcount from less than 100 to 1,000 participated in this research.

Figure 1. Our organization experienced a cyber attack and data breach in the past 12 months

Yes responses



As shown in Figure 1, 61 percent of these respondents say their companies have experienced a cyber attack in the past 12 months, and 54 percent report they had data breaches involving customer and employee information in the past 12 months. In the aftermath of these incidents, these companies spent an average of $1,027,053 because of damage or theft of IT assets. In addition, disruption to normal operations cost an average of $1,207,965.

The following are the top 10 trends in the state of cybersecurity in SMBs

1. Cyber attacks affected more SMBs in the past 12 months, an increase from 55 percent to 61 percent of respondents. The most prevalent attacks against smaller businesses are phishing/social engineering and web-based (48 percent and 43 percent of respondents, respectively). More respondents in this year's study say cyber attacks are more targeted, severe and sophisticated.

2. The rise of ransomware is affecting SMBs. In last year's research, only two percent of respondents described the cyber attacks they experienced as ransomware. This year, 52 percent of respondents say their companies experienced a ransomware attack and 53 percent of these respondents say they had more than two ransomware incidents in the past 12 months. Seventy-nine percent of respondent say the ransomware was unleashed through a phishing/social engineering attack.

3. SMBs are having slightly more data breaches involving personal information and the size of data breaches is larger. In the past 12 months, 54 percent of respondents report they had a breach involving sensitive information about customers, target customers or employees, an increase from 50 percent in last year's study. The average size of the breach involved 9,350 individual records, an increase from an average of 5,079 records.

4. Of the respondents who say their organization had a data breach, 54 percent say negligent employees were the root cause of data, an increase from 48 percent of respondents in last year's study. However, similar to last year, almost one-third of companies in this research could not determine the root cause.

5. While only 23 percent of respondents report their organization had a data breach or security incident due to the use of the Internet of Things (IoT), 67 percent of respondents say their organizations are very concerned or concerned about the security of IoT devices in the workplace. Moreover only 29 percent of respondents say they have confidence in their ability to contain or minimize the risk of insecure IoT. In fact, 56 percent of respondents say IoT and mobile devices are the most vulnerable endpoint their organization's networks and enterprise systems.

6. More SMBs are experiencing situations when exploits and malware have evaded their intrusion detection system (an increase from 57 percent of respondents to 66 percent of respondents) and anti-virus solutions (an increase from 76 percent of respondents to 81 percent of respondents).

7. Strong passwords and biometrics continue to be an essential part of the security defense. However, 59 percent of respondents say they do not have visibility into employees' password practices such as the use of unique or strong passwords and sharing passwords with others. This has not improved since last year.

8. Password policies are still not strictly enforced. If a company has a password policy (43 percent of respondents), 68 percent of respondents say they do not strictly enforce it or are unsure. However, more SMBs are requiring employees to use password or biometric to secure access to mobile devices, an increase from 42 percent of respondents to 51 percent of respondents.

9. Personnel, budget and technologies continue to be insufficient to have a strong security posture. As a result, some companies engage managed security service providers to support an average of 36 percent of their IT security operations. The services most often used are monitored or managed firewalls or intrusion prevention systems and intrusion detection systems and security gateways for messaging or Web traffic.

10. Cyber attacks are more costly. The average cost due to damage or theft of IT assets and infrastructure increased from $879,582 to $1,027,053. The average cost due to disruption to normal operations increased from $955,429 to $1,207,965.

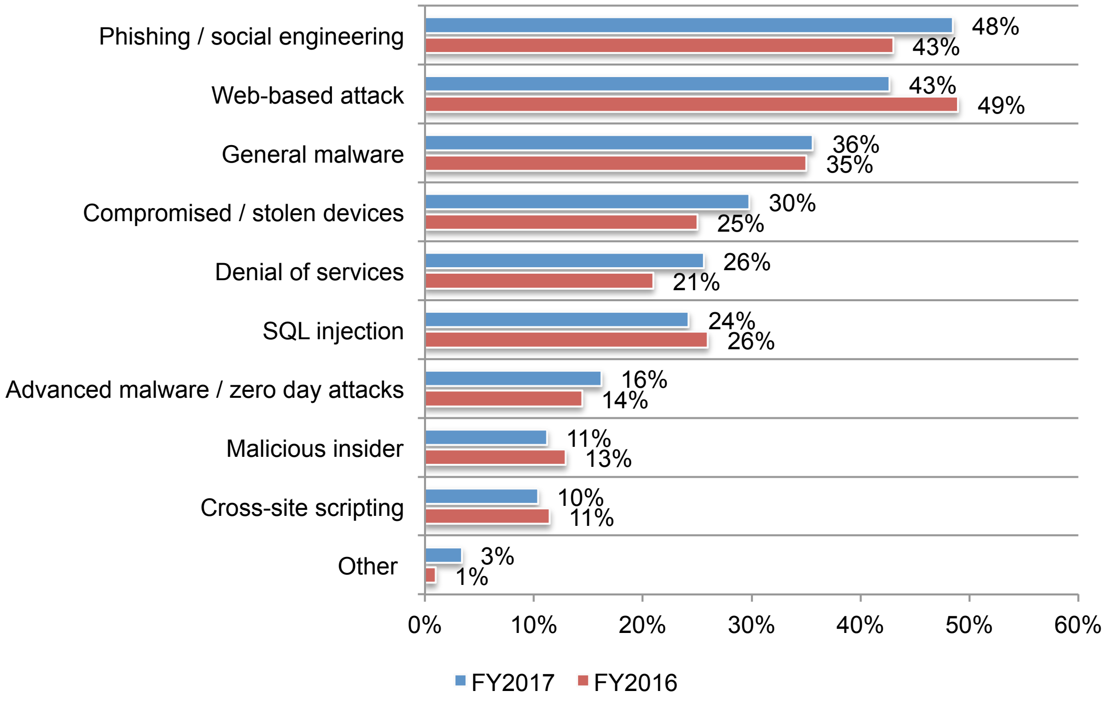
Part 2. Key findings

- Trends in SMB cyber attacks and data breaches
- The rise of SMB ransomware attacks
- IT security posture and governance
- Technologies in place to address the threat
- The impact of the Cloud and mobile on IT security posture

Trends in SMB cyber attacks and data breaches

Cyber attacks and data breaches target SMBs. As discussed, most businesses represented in this study experienced a cyber attack and data breach with severe financial consequences (61 percent and 54 percent, respectively). Since last year, phishing/social engineering has replaced web-based attacks (48 percent and 43 percent of respondents, respectively) as the most frequent type of attack, as shown in Figure 2. Compromised/stolen devices and denial of services attacks increased from last year's study (30 percent and 26 percent, respectively).

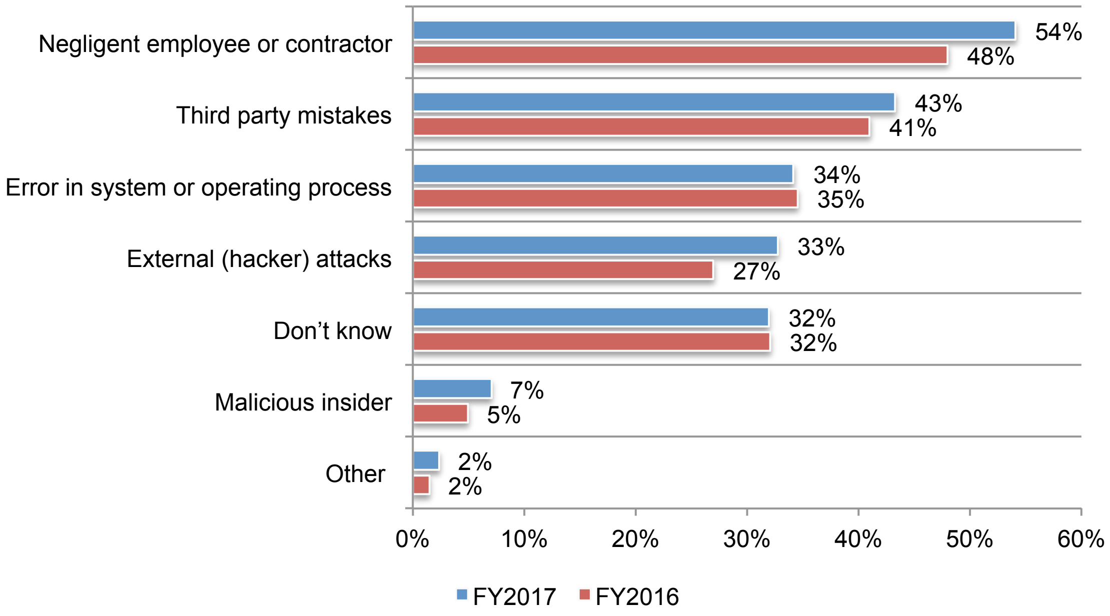
Figure 2. What types of attacks did your business experience?
More than one choice allowed



Businesses are losing more records in a data breach. Companies represented in this research lost an average of more than 9,350 individual records as a result of the data breach, a significant increase from an average of 5,079 in last year's study.

As shown in Figure 3, data breaches due to negligent employees or contractors (54 percent of respondents) increased significantly from 48 percent in 2016. This is followed by third party mistakes (43 percent of respondents) and errors in system or operating processes (34 percent of respondents). However, almost one-third of respondents say their companies could not determine what caused the incident.

Figure 3. What was the root cause of the data breaches your business experienced?
More than one choice allowed


Negligent employee or contractor
Third party mistakes
Error in system or operating process
External (hacker) attacks
Don't know
Malicious insider
Other
FY2017
FY2016