SURVEY REPORT

Security Testing Practices and Priorities

An Osterman Research Survey Report

Published August 2016

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

This report presents the results of a survey that was conducted by Osterman Research for Trustwave. The survey was conducted during July 2016 with qualified members of the Osterman Research survey panel. To qualify for the survey, respondents had to be knowledgeable about and/or responsible for security testing in their organizations.

Our focus in this research was security testing – the process of testing database, network and application systems for vulnerabilities that could allow bad actors to penetrate them and steal sensitive or confidential information, encrypt data, disable the intended functionality, or otherwise cause harm.

KEY TAKEAWAYS

- **Most organizations are not proactive about security testing**
  Our research revealed that fewer than one in four organizations considers themselves to be "very proactive" in the context of security testing, while nearly one-half are "somewhat proactive". However, nearly one-third of organizations consider themselves "somewhat" to "very" reactive about security testing, or that their security testing posture is "non-existent".

- **Many organizations do no security testing**
  Most organizations conduct security testing using a combination of in-house resources and third-party testing services, although two in five organizations manage security testing only in-house. However, we found that one in five organizations has not conducted security testing of any kind during the past six months; among those that do conduct security testing, 66% do so only monthly or less frequently and most do not perform regular security testing after every infrastructure change.

- **Even so, most find security testing to be valuable best practice**
  Despite the fact that many organizations do not perform security testing for either their internally developed or procured IT assets and product offerings, two-thirds believe that security testing is a valuable best practice.

- **Security testing and reviews are infrequent in many organizations**
  Both security testing and reviews of these tests are not commonplace: only 5% perform detailed reviews of security tests to assess vulnerabilities on a daily basis and only 24% do so weekly or multiple times during the week. However, 25% of the organizations surveyed perform these reviews only quarterly or annually, and 20% do so only when they perceive the need.

- **Security testing challenges abound**
  Among the leading security testing challenges discovered in the survey, the most commonly cited are inadequate staffing, insufficient time to perform the security tests, and the shortage of skills to support regular testing.

- **Using third parties will be more common**
  To address these issues, a large proportion of those surveyed are open to the idea of using third parties, like managed security services providers, to conduct security testing for them. Thirty-five percent of those surveyed already do so and another 21% plan to do during the next year. Only 9% of those surveyed don't plan to use third-party security testing services.

- **No one is immune to cyber attacks**
  Our research revealed that 71% of survey respondent organizations had experienced a phishing and/or social engineering attack during the previous 12 months, 59% had been victims of malware infiltrations, and 28% had experienced a distributed denial-of-service (DDoS) attack. Ninety-five percent of survey respondents reported encountering one of the dozen common security issues associated with security vulnerabilities that were listed in the survey.

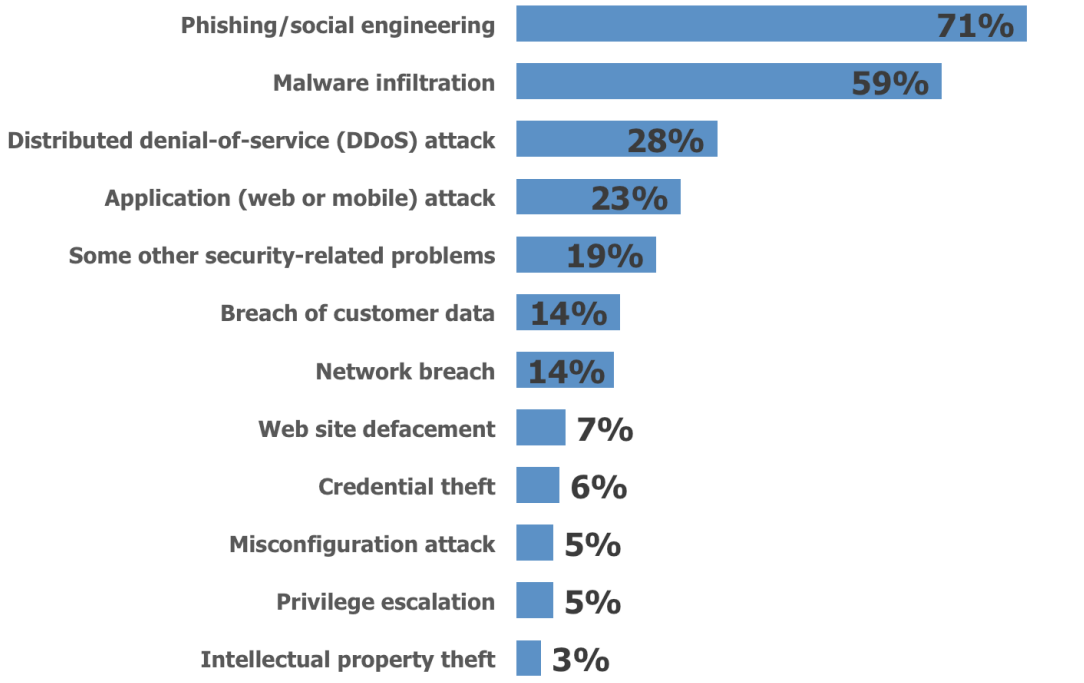
- **The cloud is increasingly the focus of corporate applications**
  Eighty-seven percent of the organizations surveyed have either released new projects or updated existing projects during the past 12 months. The most common delivery platform for these applications is the cloud.

SURVEY FINDINGS

SECURITY ATTACKS AND BREACHES ARE COMMON

The vast majority of organizations surveyed have been the victims of a significant number of different types of attacks, including phishing/social engineering and malware infiltration of various kinds, as shown in Figure 1. Our research also found that attacks like distributed denial-of-service (DDoS) attacks, attacks against applications, and breaches of customer data and corporate networks were fairly common.

Figure 1
Security Issues That Organizations Have Experienced During the Past 12 Months



Source: Osterman Research, Inc.

The potential success of phishing attempts and other infiltrations varies based on a number of factors, including the victim's gullibility, their training, the vulnerability of their applications, their organization's security infrastructure and other factors. However, there are four key reasons that phishing is so successful today:

- Many applications in common use have one or more security vulnerabilities and the number of these vulnerabilities is increasing, meaning criminals are finding easier success in introducing malware through social engineering and phishing attacks. Osterman Research has discovered that security awareness training in most organizations is not adequate to help users defend against phishing attacks[1].

- Users share an enormous amount of information through social media channels, providing cybercriminals with information they can use to craft personalized and more believable messages.

- Cybercriminals are getting better at penetrating corporate defenses, including vulnerable applications. For content that makes it past security defenses, professionally crafted messages

[1] Osterman Research survey of end users conducted July 2016.

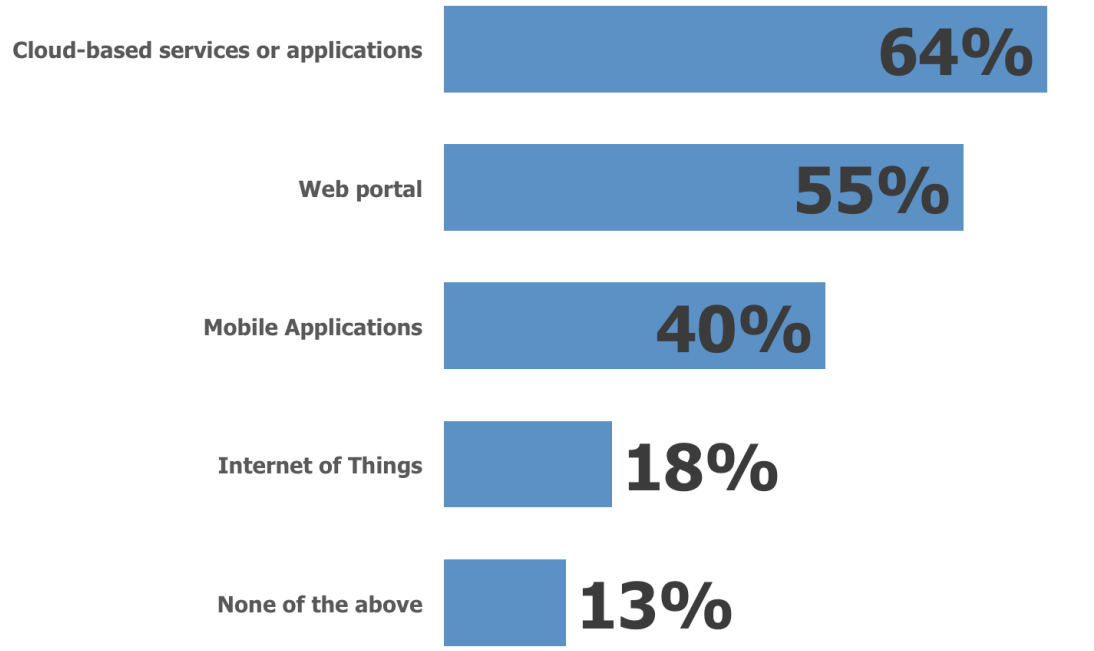
and personalization of content makes phishing attempts more believable, and so prospective victims are more likely to click on the links and attachments contained within them.

- Some anti-phishing solutions are not supported with a robust database of real-time intelligence, often making them less useful and effective than solutions that are supported by real-time intelligence capabilities.

CLOUD DOMINATES NEW SERVICE OFFERINGS

Seven out of eight of the organizations we surveyed have released new IT-related projects or updated existing projects. Not surprisingly, nearly two-thirds of the organizations surveyed have released new or updated existing cloud projects, while most have also released or updated Web portals, as shown in Figure 2.

Figure 2
Technology Areas in Which Organizations Have Released New Projects or Updated Existing Projects



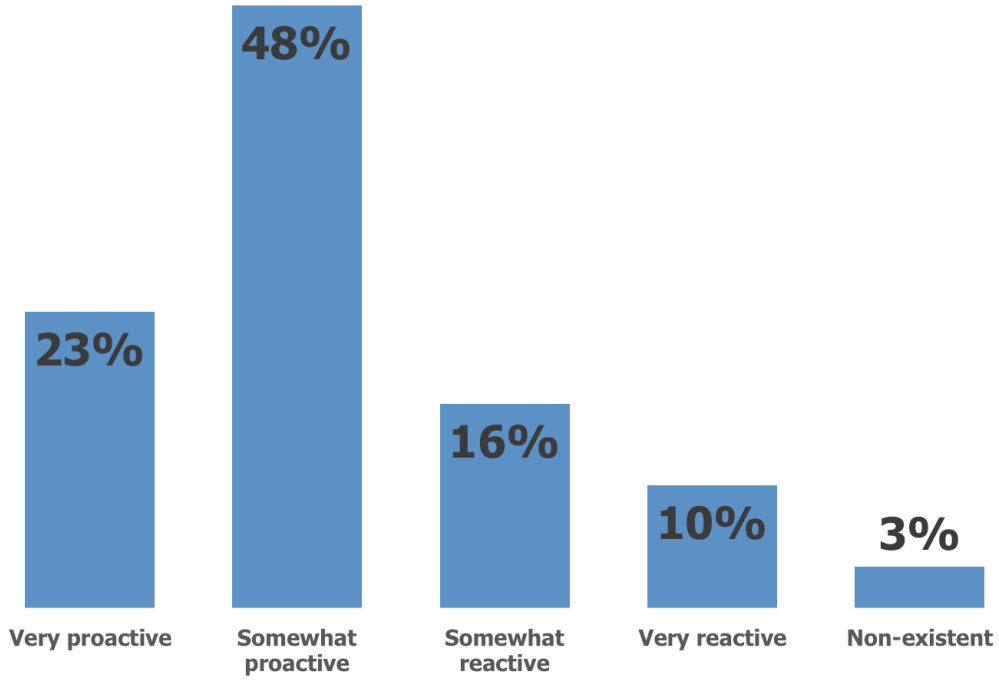
Source: Osterman Research, Inc.

Many believe that the use of cloud-based solutions to deal with phishing attempts and other malicious content from reaching endpoints can be an important best practice in either bolstering an existing, on-premises security solution or adding another layer of defense to a cloud solution. Many organizations have enough to deal with when it comes to phishing and malware, and so the use of cloud-based solutions is viewed by some as an important supplement to their existing defenses. This is part of a larger trend toward moving key functionality to the cloud, as exemplified by the rapid growth of business productivity applications, CRM, ERP, HR and other applications moving from on-premises delivery to the cloud.

ARE ORGANIZATIONS PROACTIVE IN THEIR SECURITY TESTING?

In the context of security testing, decision makers and influencers do not believe their organizations are highly proactive. As shown in Figure 3, fewer than one-quarter of these decision makers and influencers rate themselves "very proactive", while about one-half believe that their organizations are "somewhat proactive". However, nearly one in three organizations consider themselves to be either "somewhat reactive" or "very reactive," or they take absolutely no steps with regard to security testing.

Figure 3
Perceived Proactivity/Reactivity to Security Testing



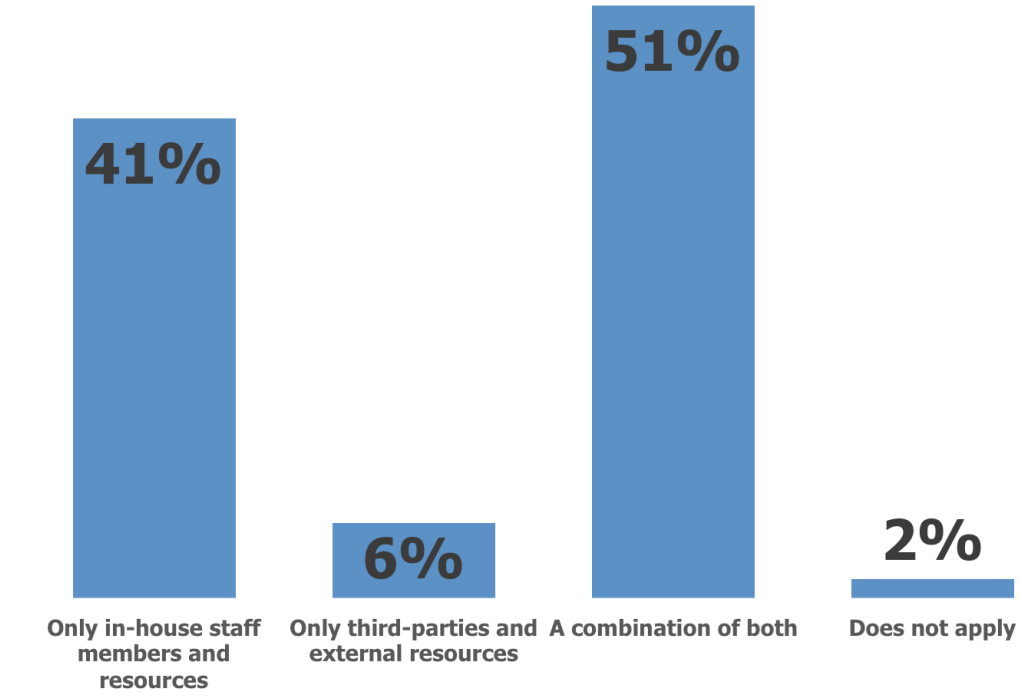
Source: Osterman Research, Inc.

The data in the figure above reveals one of the fundamental reasons that security breaches of various kinds are so common: Despite record numbers of vulnerabilities in recent years, fewer than one in four security decision makes and influencers believes that their organizations are highly proactive in the context of security testing.

HOW DO ORGANIZATIONS CONDUCT SECURITY TESTING?

When organizations test the security capabilities of new and existing IT assets and product offerings, about one-half use a combination of in-house staff members and third-party resources, like managed security services providers, as shown in Figure 4. However, about two in five organizations employ only in-house staff members and resources, while few use third parties exclusively for testing purposes.

Figure 4
Resources Employed to Test the Security of New and Existing IT Assets and Product Offerings

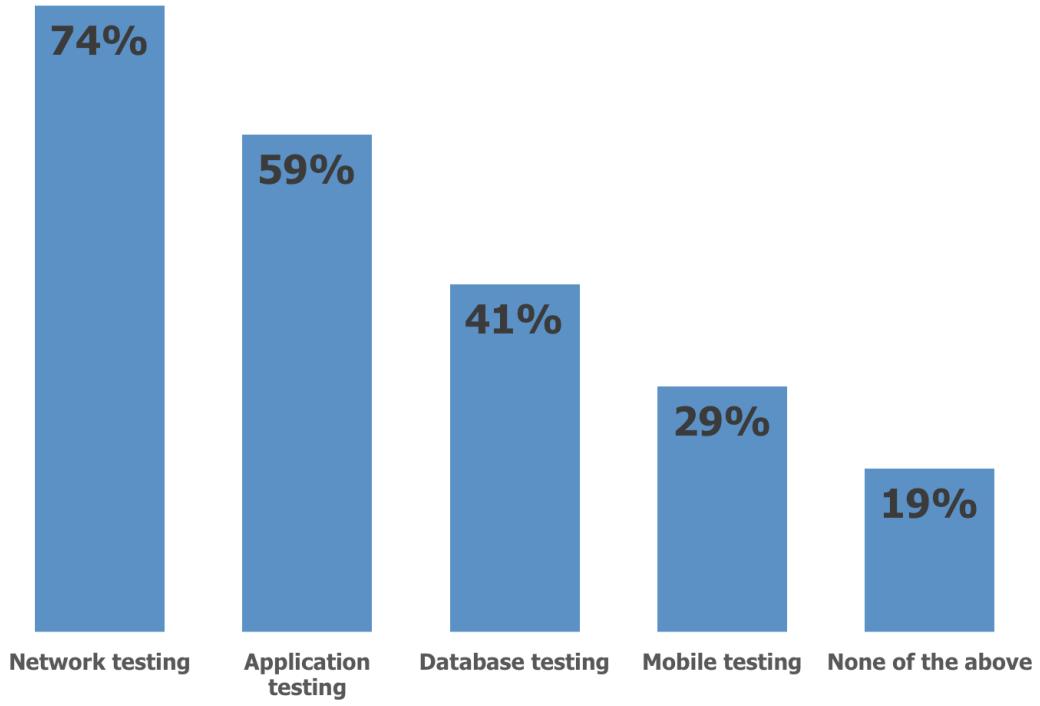


Source: Osterman Research, Inc.

ONE IN FIVE DOES NO SECURITY TESTING

Our research found that the vast majority of organizations have performed network testing during the past six months, while three in five have performed application testing and about two in five have performed database testing, as shown in Figure 5. However, about one in five organizations reports that they have not performed any type of security testing during the past half-year.

Figure 5
Types of Security Testing That Organizations Have Conducted During the Past Six Months



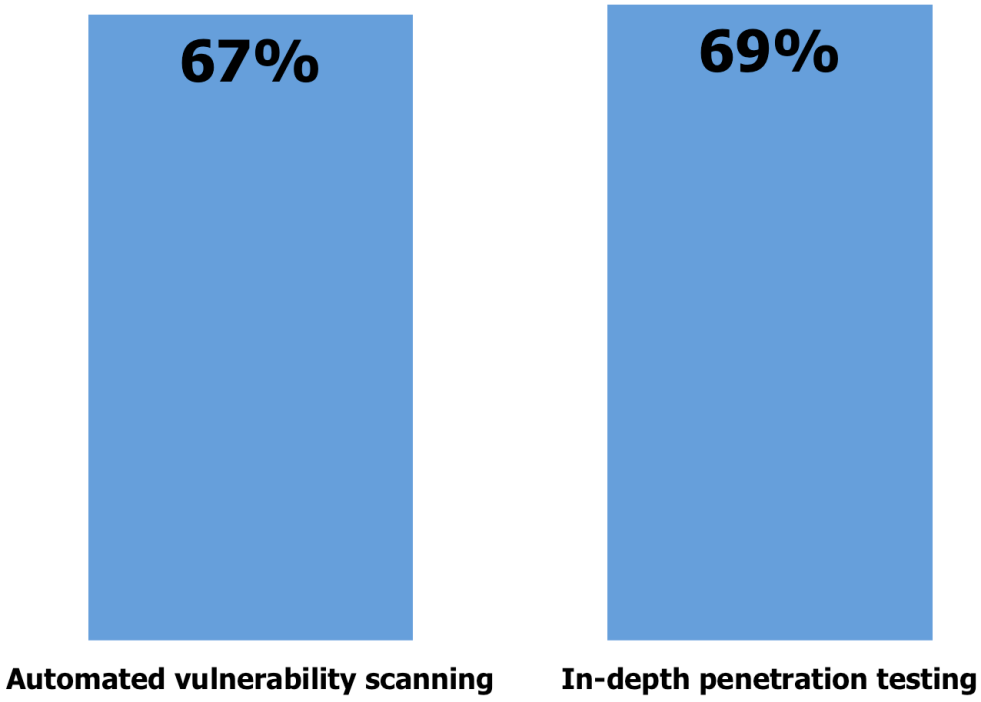
Source: Osterman Research, Inc.

It is important to note the fairly significant drop-off between network testing and other types of testing and the vulnerabilities this can create in an organization. Since corporate applications, databases and mobile apps serve as gateways to sensitive data, such as email stores and customer information, it is imperative that all potential areas of vulnerability be tested.

MOST SEE VALUE IN KEY SECURITY TESTING PRACTICES

Despite the relative infrequency of security testing or reviews of these tests, the vast majority of organizations finds both automated vulnerability scanning and in-depth penetration testing to be either valuable or extremely valuable, as shown in Figure 6. In fact, if we combine the top three ratings from our survey ("somewhat valuable", "valuable" or "extremely valuable"), we find that automated vulnerability scanning jumps to 91% of those surveyed, while in-depth penetration testing increases to 89%.

Figure 6
Value of Key Security Testing Practices
% Responding Valuable or Extremely Valuable



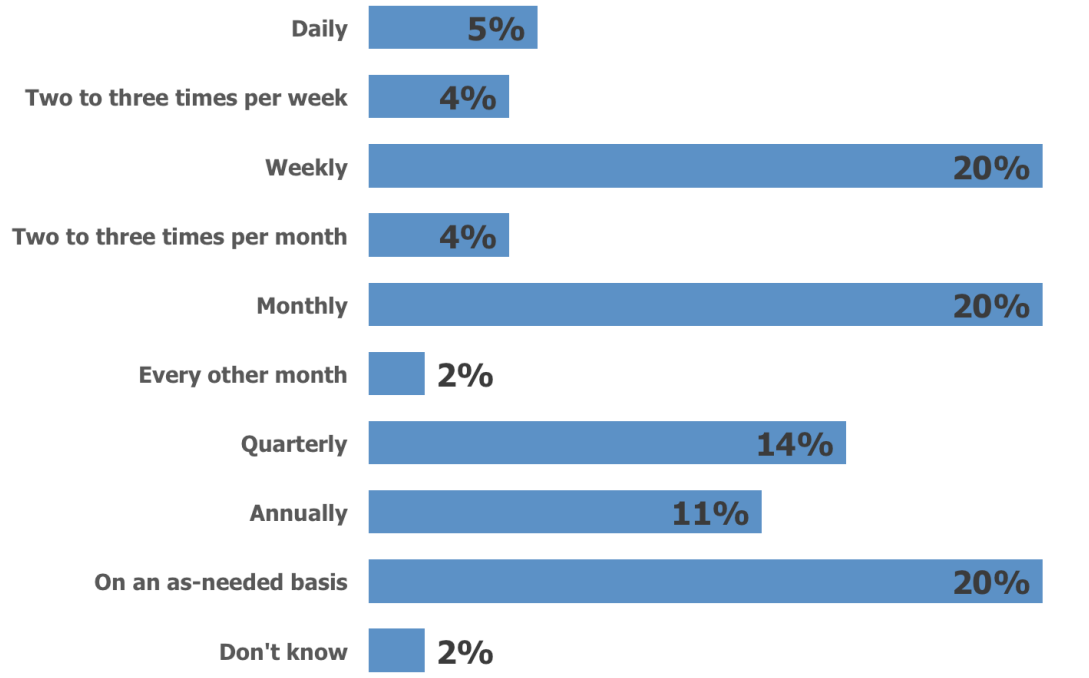
Source: Osterman Research, Inc.

The data in the figure above reveals that while security-focused decision makers find significant value in things like automated vulnerability scanning and in-depth penetration testing, they are constrained by other factors that often prevent adequate testing of their own networks or the applications and databases they build internally or those they procure from third parties.

SECURITY TESTING IS SPORADIC: FREQUENT REVIEWS OF SECURITY TESTS ARE EVEN LESS COMMON

While most organizations conduct security testing only on a monthly or less frequent basis, detailed reviews of security tests in order to assess vulnerabilities are even less common. As shown in Figure 8, only 5% of the organizations surveyed conduct daily security reviews, while nearly two-thirds do so no more frequently than once each month.

Figure 8
Frequency of Detailed Review of Security Tests to Assess Vulnerabilities

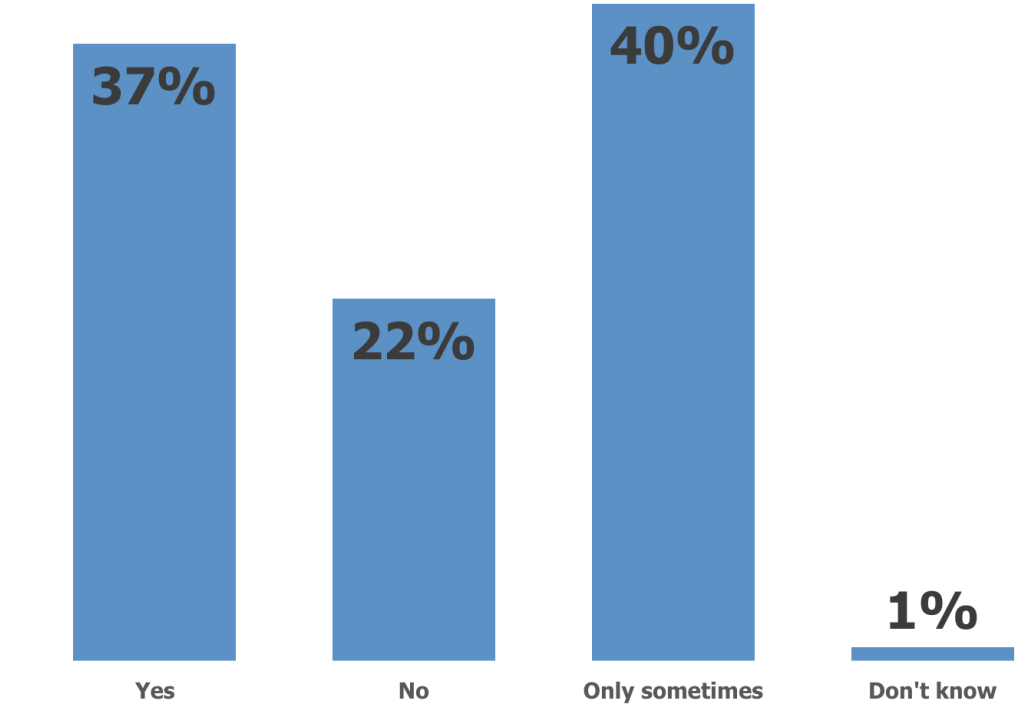


Source: Osterman Research, Inc.

MOST DO NOT DO REGULAR SECURITY TESTING AFTER INFRASTRUCTURE CHANGES

Our research found that most organizations implement security testing after they make changes to their infrastructure, but a plurality of organizations do so only occasionally, as shown in Figure 9. More than one in five organizations do not perform security testing after making infrastructure changes.

Figure 9
Security Testing Following Infrastructure Changes

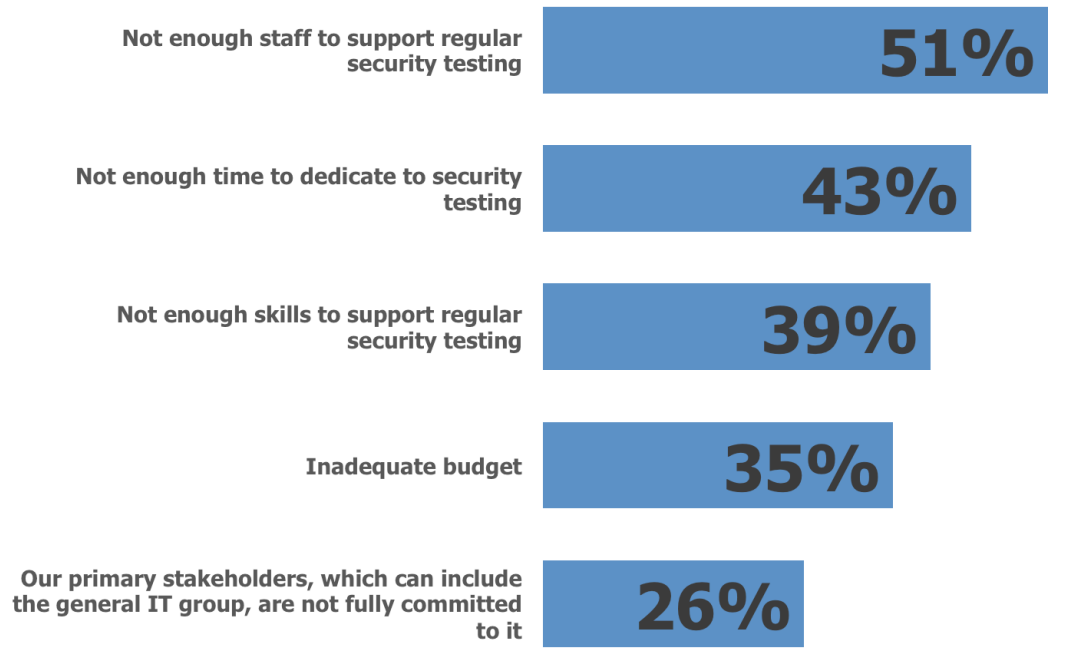


Source: Osterman Research, Inc.

THERE ARE SEVERAL SECURITY TESTING CHALLENGES

Organizations face a variety of challenges in the context of security testing. As shown in Figure 10, about one-half of decision makers and influencers report that they simply do not have enough staff members available to support regular security testing, while roughly two in five do not have enough time to dedicate to security testing, nor do they possess the skills internally to support regular security testing. Interestingly, about one in four organizations report that one of their chief challenges is that the key stakeholders in the organization are not fully committed to security testing.

Figure 10
Organizational Security Testing Challenges
% Responding "Challenging" or "Extremely Challenging"



Source: Osterman Research, Inc.

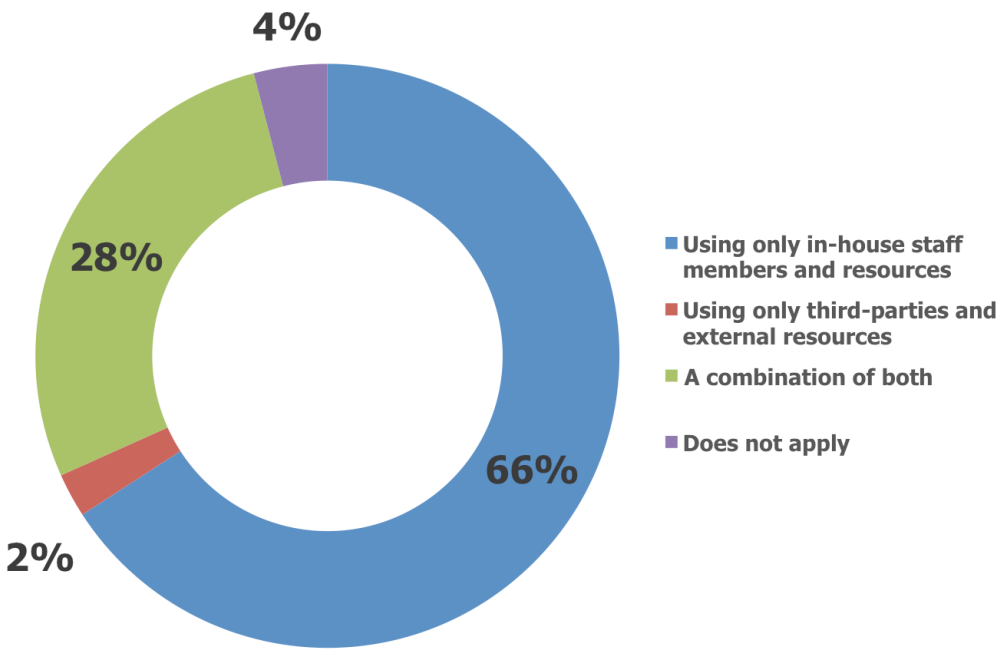
The survey also asked respondents about the security testing capabilities they wish they had available to them, but do not have today. The top five capabilities that decision makers and influencers wish they had available to them are:

- Automatic security testing capabilities
- Additional staff with deep application security assessment skill sets and/or more expertise
- Better tools
- More in-depth and faster analysis of security vulnerabilities
- More time to do security testing.

MOST CURRENTLY USE ONLY IN-HOUSE CAPABILITIES TO DEAL WITH SECURITY INCIDENTS

About two-thirds of the organizations surveyed employ only in-house IT staff members and various other resources to deal with security incidents, while more than one-quarter of those surveyed use a combination of both in-house staff/resources and third-party capabilities, such as a managed security services provider, as shown in Figure 7.

Figure 7
Resources Employed to Deal With the Most Recent Security Incident



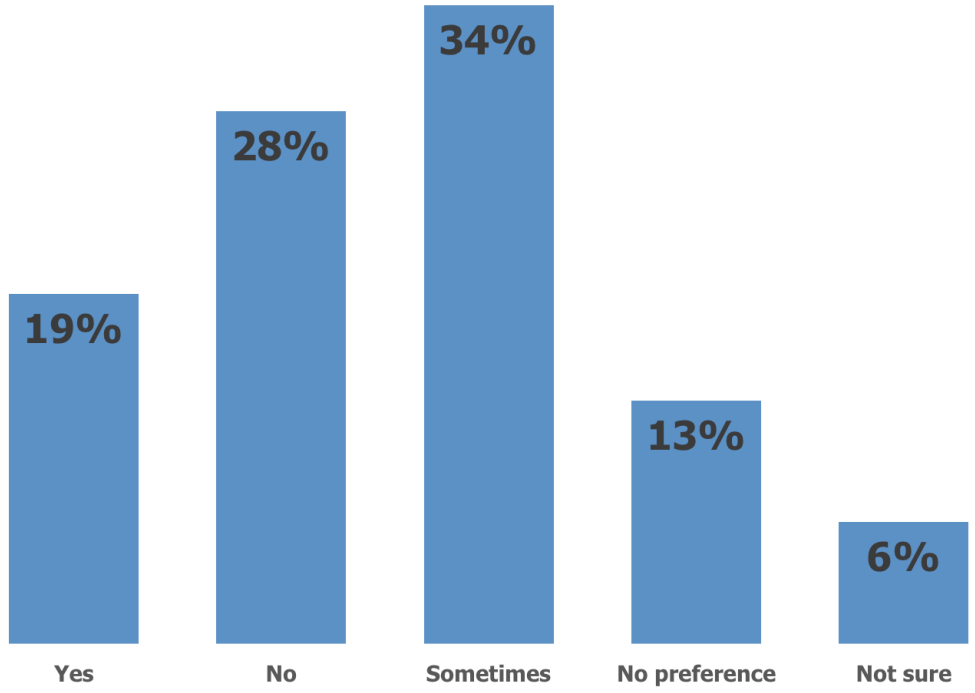
Source: Osterman Research, Inc.

While the data in the figure above appears to be a bit of a non sequitur in the context of security testing, it actually reveals that the heavy reliance on internal staff and other resources to deal with security incidents may be part of the larger problem of not having enough resources to perform adequate security testing. For example, as shown in Figure 9, many organizations do not have enough staff members, time or internal expertise to do security testing. This results in a greater likelihood that untested and undiscovered vulnerabilities will lead to security breaches, part of the larger problem of lacking adequate internal resources and not relying on external expertise, whether in part or entirely, to deal with both security testing and breach remediation.

WHAT ABOUT USING JUST ONE THIRD-PARTY TESTING VENDOR?

About one in five decision makers and influencers would prefer to use a single third-party vendor to conduct their security testing, while another one-third would prefer to do so on a case-by-case basis, as shown in Figure 11. About one in five organizations either have no preference about who performs their security testing or has not yet come to a decision.

Figure 11
Preferences for Use of a Single Third-Party Vendor to Conduct Security Testing

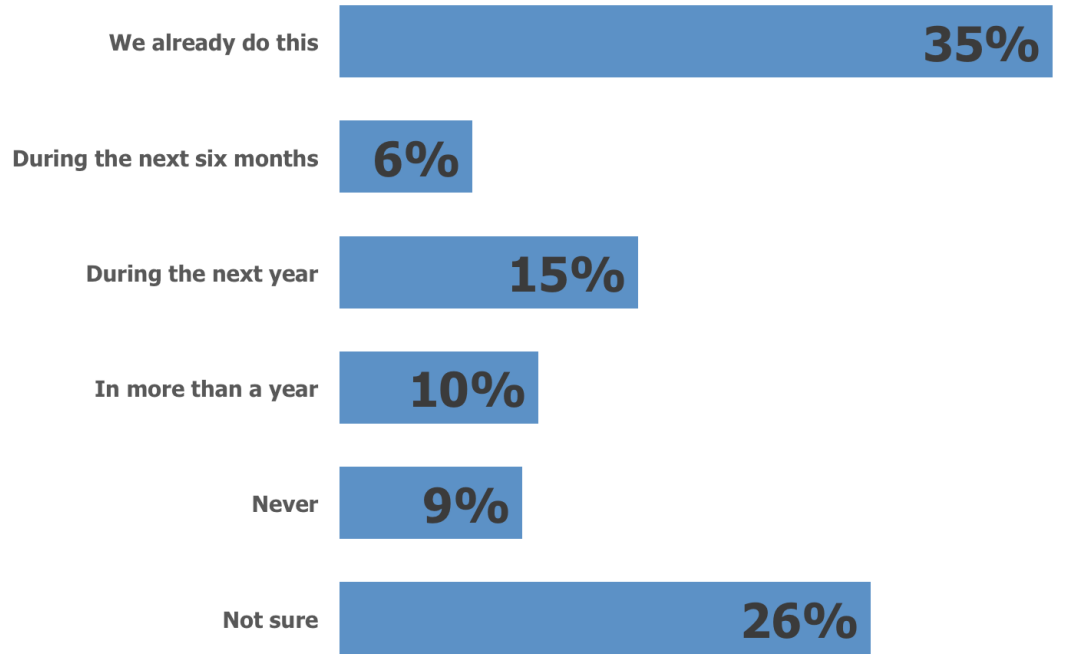


Source: Osterman Research, Inc.

WILL ORGANIZATIONS USE THIRD PARTIES IN THE FUTURE?

Currently, about one-third of organizations use third parties, like managed security services providers, for security testing, as shown in Figure 12. However, another 21% plan to begin using third parties within the next year, while another 36% will either do so in more than a year or are not yet sure of their plans. Only one in 11 decision makers or influencers indicated any sort of opposition to the use of third parties for security testing purposes.

Figure 12
Plans for Partnering With a Third-Party for Security Testing



Source: Osterman Research, Inc.

SUMMARY AND KEY ISSUES TO CONSIDER

Based on the research findings in this survey report, there are some key takeaways that we recommend organizations consider in the context of their security testing:

- Organizations should consider partnering with an established managed security services provider to address the staffing, skills and resource constraints identified by the majority of respondents to this survey. While internal resources should be used, our research clearly demonstrated that internal staff members and other resources are being strained in their ability to provide adequate security testing and breach remediation for their organizations.

- Consider testing platforms that can test databases, networks and applications. It is essential that organizations test their networks, every application and every repository of sensitive or confidential information for vulnerabilities that could result in loss of data or a failure to meet its compliance objectives.

- Consider testing platforms that do both automated vulnerability scanning and offer in-depth penetration testing to discover as many vulnerabilities as possible, including after even minor updates.

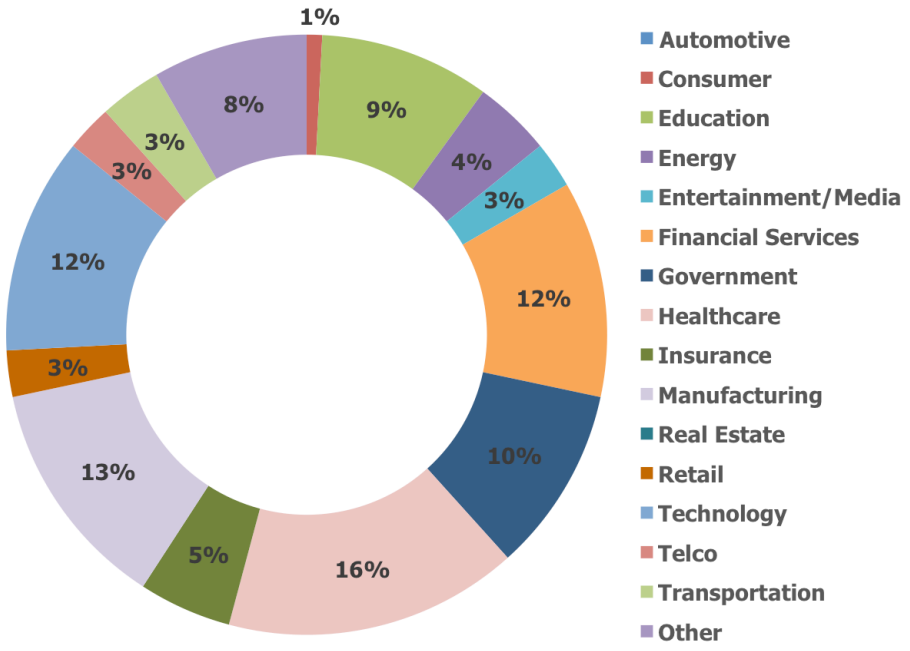
- Finally, application, database, network and other vulnerability must be a very high priority for any organization, not an afterthought once a solution has been deployed or updated. By

addressing vulnerabilities before solutions are rolled out, organizations can prevent many security breaches and substantially reduce overall corporate risk in the process.

ABOUT THE SURVEY

On behalf of Trustwave, Osterman Research conducted this survey in July 2016 with members of its survey panel, the majority of whom are located in the United States. In order to qualify for the survey, respondents had to be knowledgeable about and/or responsible for security testing in their organizations. The mean number of employees at the organizations surveyed was just under 14,700 and the mean number of email users was 12,130. A wide range of industries were included in the survey, as shown in Figure 13. A total of 126 surveys were completed, providing a maximum margin-of-error of ±8.7%.

Figure 13
Industries Surveyed



Source: Osterman Research, Inc.