The Cost of Web Application Attacks

Sponsored by

Akamai Technologies

Independently conducted by Ponemon Institute LLC

Publication Date: May 2015

The Cost of Web Application Attacks

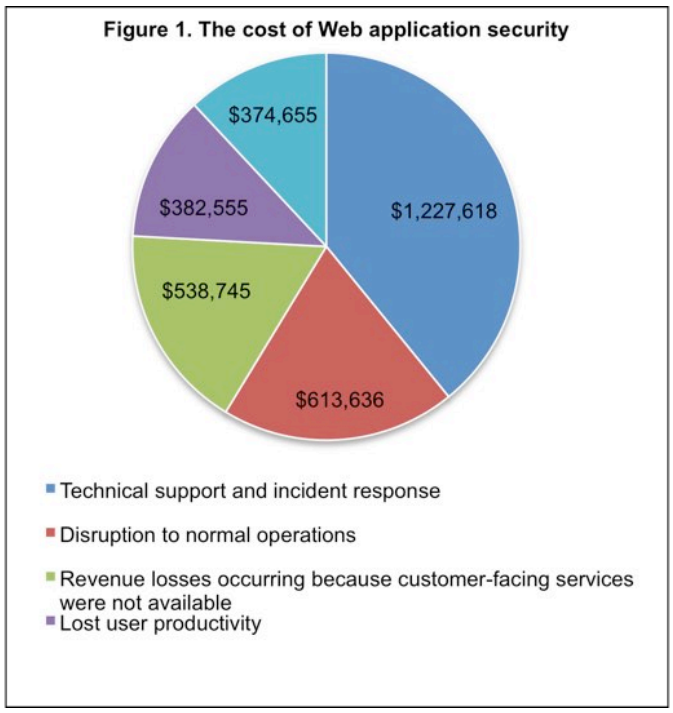
Ponemon Institute, May 2015

Part 1. Introduction

We are pleased to present the *Cost of Web Application Attacks,* sponsored by Akamai Technologies. The purpose of this research is to understand how organizations are protecting Web applications and how web application attacks affect both an organization's security posture and bottom line.

Ponemon Institute surveyed 594 individuals who are familiar with the Open Web Application Security Project (OWASP), an organization responsible for increasing awareness of and highlighting risks to web applications. Participants in this research work in IT operations, IT security, IT compliance or data center administration.

According to the findings, Web application security is considered equally critical or more critical than other security issues faced by organizations. With Web application security incidents becoming increasingly common, respondents believe Web application attacks have cost their organizations approximately $3.1 million in the past 12 months. As shown in Figure 1, most of that cost is due to necessary technical support and incident response.



Other key findings:

Most organizations have had their Web applications compromised with the past 12 months. Only 2 percent of respondents say their organizations have not been compromised.

Protection of data is the most important reason for securing Web applications. Revenue loss and compliance are also considered important.

The need for a WAF is widely recognized. Sixty-nine percent of respondents say a WAF is a necessary or critical piece of their organizations' security arsenal.

WAFs require significant management overhead. On average, respondents say that it requires 4.4 FTEs to properly manage their WAF.

For a WAF, performance is as important as security. Twenty-two percent of respondents say that performance is more important than security. Forty-five percent say both performance and security are equally important.

Despite how frequent Web applications are compromised, on average less than half are tested. Primary reasons for not testing more Web applications are: uncertainty over how much to test, senior management doesn't understand application security or see its need, no budget and no expertise.

Part 2. Key findings

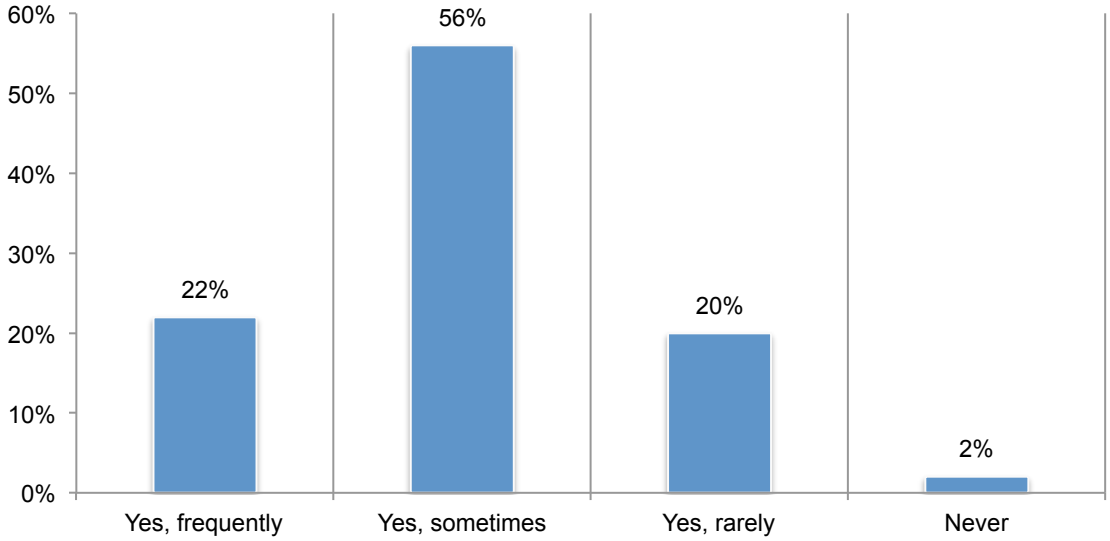
This report is organized according to the following topics:

- The importance of WAF to safeguarding Web applications
- Deploying a WAF
- Performance
- Testing Web applications
- Cost of Web application attacks

The importance of WAF to safeguarding Web applications

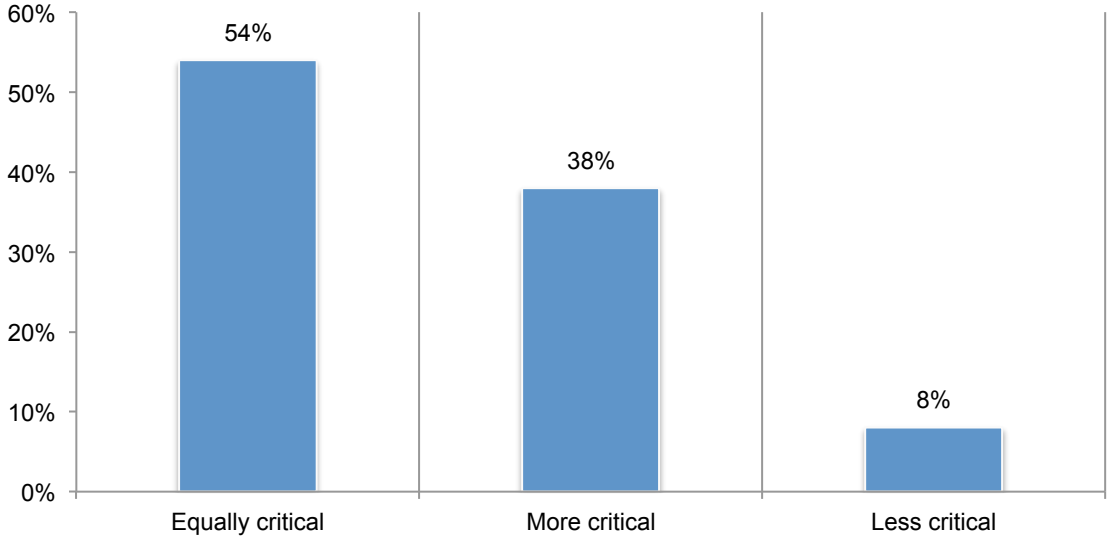
Most organizations have had their Web applications compromised. As shown in Figure 2, 78 percent of respondents say their organizations' Web applications have been compromised in the past year. Only 2 percent say they have never been compromised.

Figure 2. Have Web applications been compromised in the past 12 months?



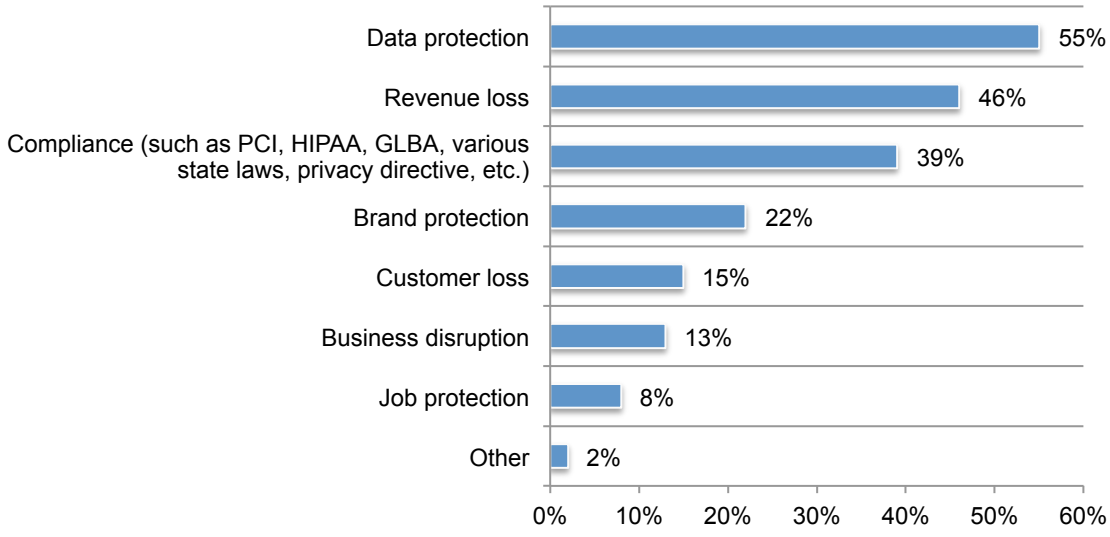
Web application security is equally or more critical than other security issues. As shown in Figure 3, 92 percent of respondents say Web application security is equal to or more critical than other security issues faced by their organizations. Only 8 percent say it is less critical.

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



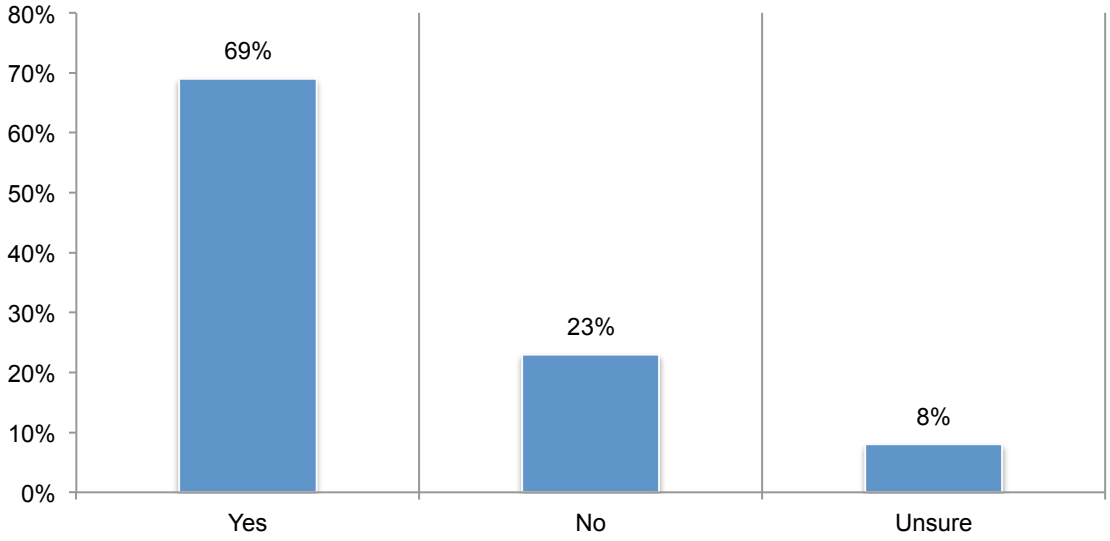
The protection of data is the most important reason for securing Web applications. As shown in Figure 4, 55 percent of respondents say their organizations secure Web applications to protect the sensitive data they contain. This is followed by 46 percent of respondents who want to prevent loss of revenue. Only 39 percent say Web application security is important because of compliance with regulations.

Figure 4. Reasons to secure Web applications
Two responses permitted



The need for a WAF is widely recognized. As shown in Figure 5, 69 percent of respondents say a WAF is a necessary or critical piece of their security arsenal. Only 23 percent say it is not and 8 percent are unsure.

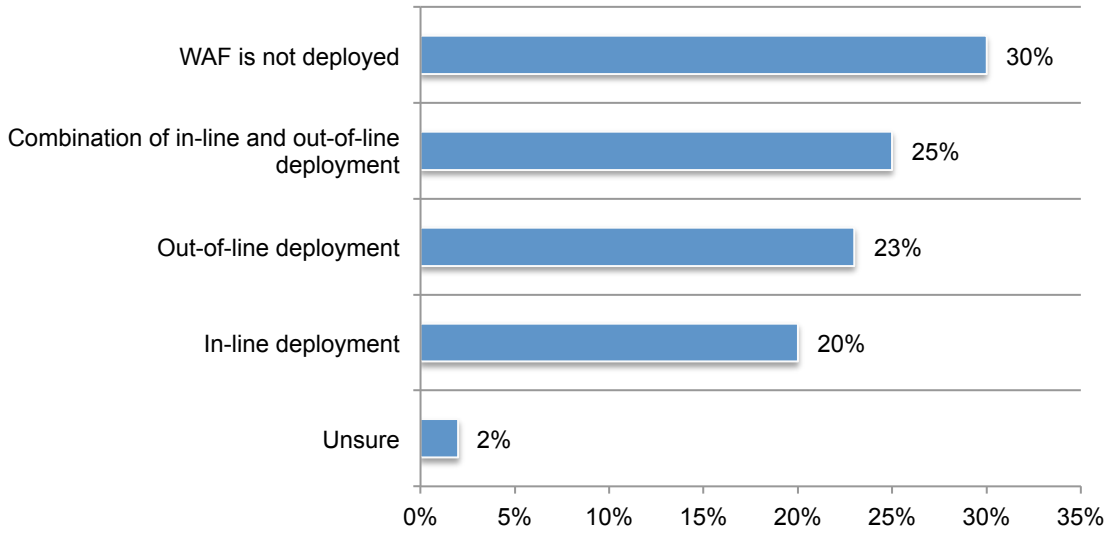
Figure 5. Do you consider Web application firewalls (WAF) to be a necessary or critical piece of your security arsenal and infrastructure?



Deploying a WAF

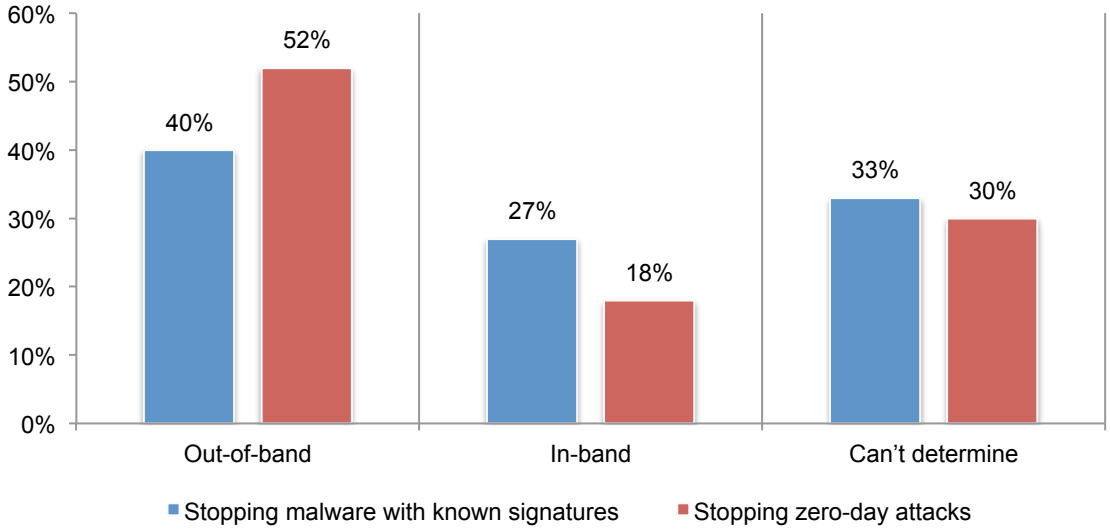
Most organizations have not deployed their WAF in a manner that allows them to stop attacks. Sixty-eight percent of respondents say their organizations deploy WAF. Among these organizations that have a WAF, only 20 percent have an in-line deployment that would allow them to stop attacks. Twenty-three percent of respondents say their organizations have an out-of-line deployment, according to Figure 6. Thirty percent of respondents say their organizations have yet to deploy a WAF.

Figure 6. What best describes your organization's approach to WAF?



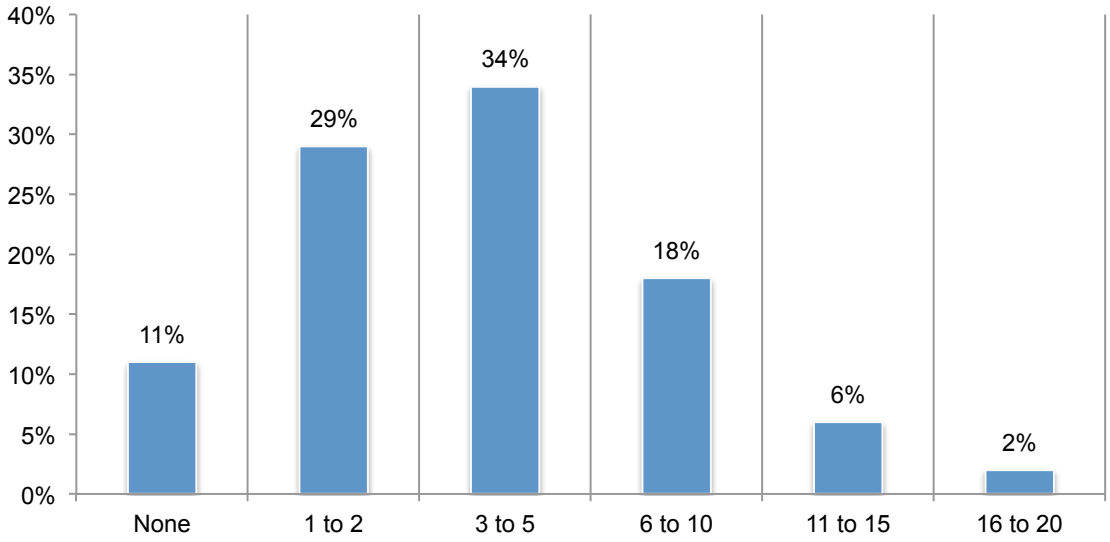
There is a lack of understanding about how a WAF stops attacks. While only an in-line deployment can actually stop attacks, respondents believe an out-of-line deployment is most effective in stopping malware with known signatures (40 percent of respondents) and zero-day attacks (52 percent of respondents). Only a minority of respondents believes an in-line deployment is most effective in stopping malware with known signatures (27 percent) and zero-day attacks (18 percent).

Figure 7. Which WAF is most effective? Change to Out-of-line and In-line



WAFs require significant management overhead. As shown in Figure 8, 60 percent of respondents say that three or more employees (on a full-time equivalent basis) are required to properly manage a WAF. Twenty-nine percent say only 1 to 2 employees were required, while 11 percent say non were required.

Figure 8 How many FTEs are needed to properly manage a WAF?

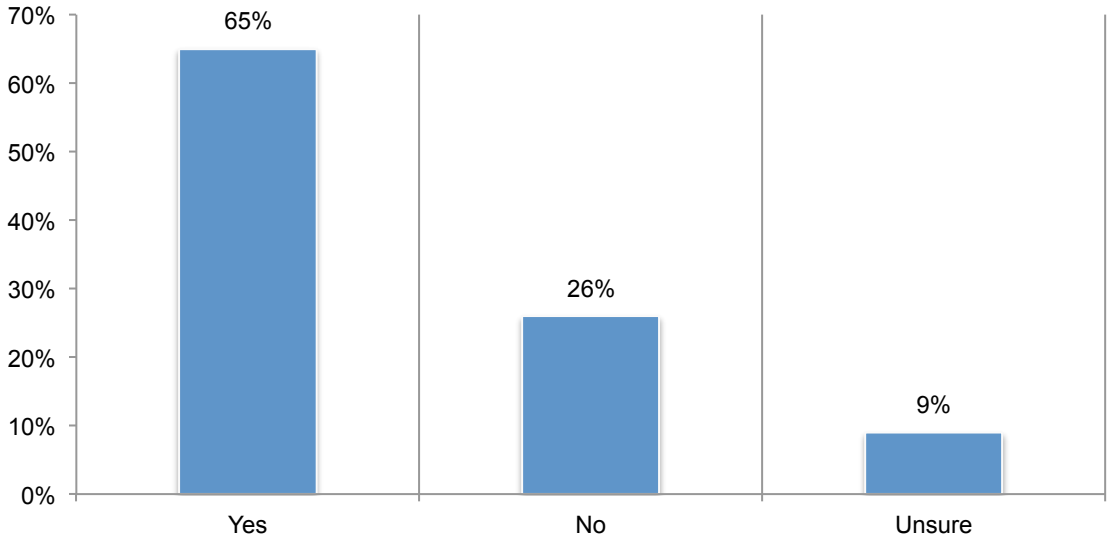


Performance

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.

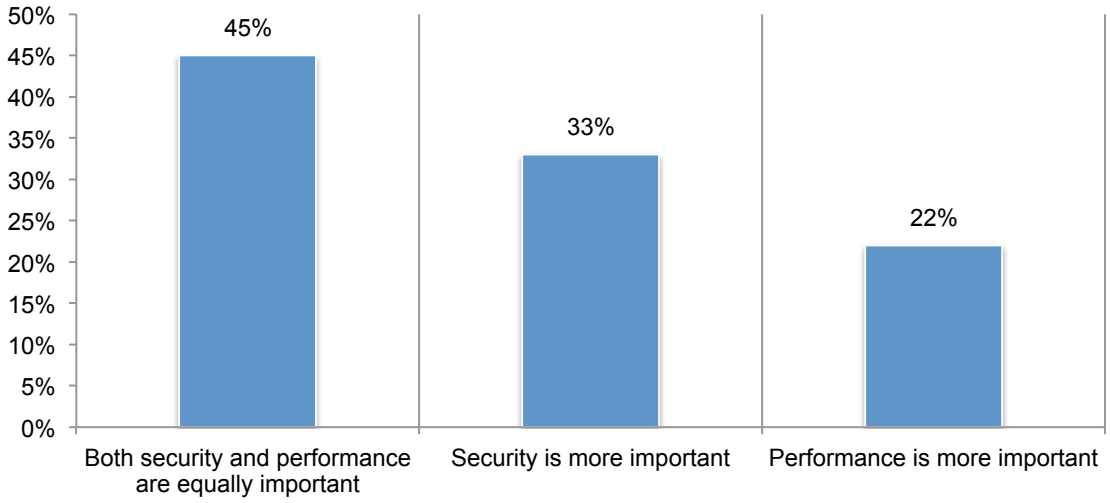
A WAF should support both security and performance. As shown in Figure 9, 65 percent of respondents say a fully functional WAF is one that optimizes both performance and security. Only 26 percent say performance was not important and nine percent are unsure.

Figure 9. Do you consider a fully functional WAF one that optimizes for both performance and security?



Performance is as important as security. As shown in Figure 10 when asked what is more important, only 33 percent say security is more important. Twenty-two percent of respondents say performance is important. Forty-five percent of respondents say both security and performance are equally important.

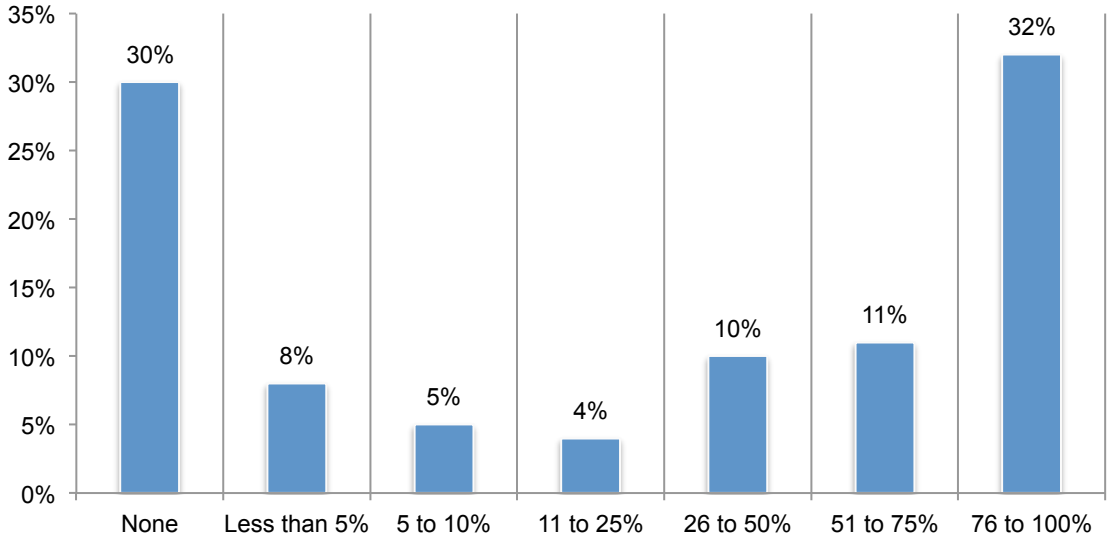
Figure 10. What is more important: security or performance?



Testing Web Applications

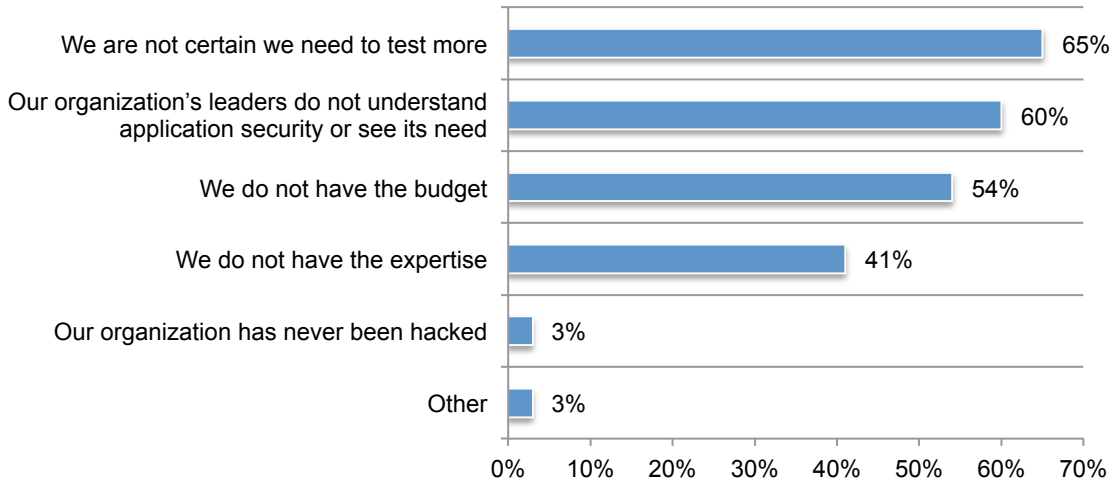
Less than half of Web applications are tested for vulnerabilities. As shown in Figure 11, 57 percent of respondents test less than half of their Web applications. Only 32 percent of respondents say their organizations test more than 76 percent of their Web applications.

Figure 11. What percentage of Web applications is tested for vulnerabilities?



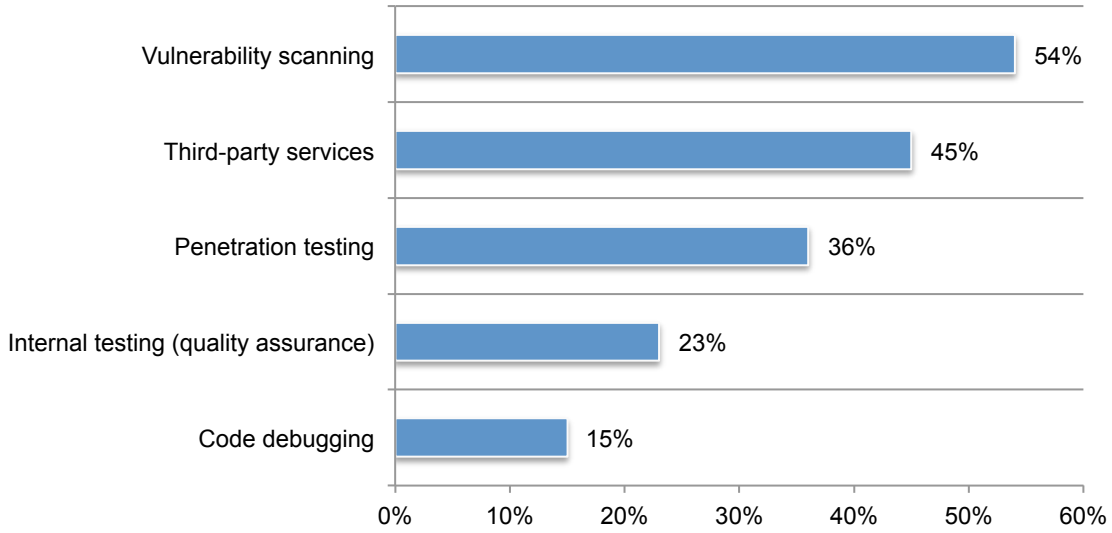
Many obstacles to comprehensive testing of Web applications exist. According to Figure 12, the three top reasons for not testing at least 50 percent of Web applications are: uncertainty whether more Web applications need to be tested (65 percent of respondents), leaders do not understand applications security or see its need (60 percent of respondents) or a lack of budget (54 percent).

Figure 12. Why organizations don't test Web applications
More than one response permitted



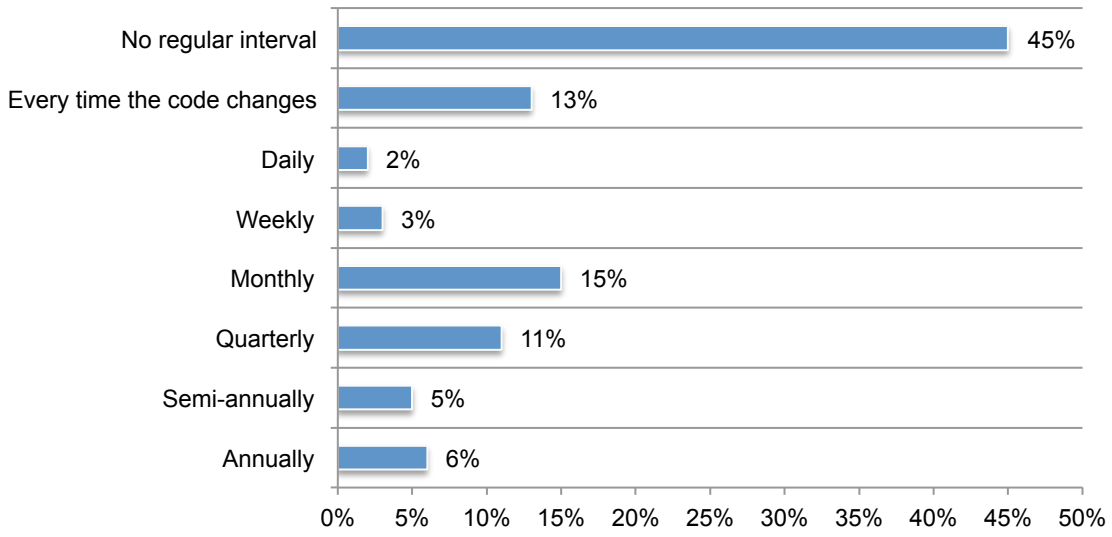
Most organizations use vulnerability scanning to test Web applications but not on a regular basis. According to Figure 13, 54 percent of respondents say they use vulnerability scanning and 45 percent use third-party services. Forty-five percent of respondents say testing occurs at no regular interval. Only 15 percent of respondents say their organization test monthly and 13 percent say they do it every time the code changes.

Figure 13. How does your organization test Web applications?
More than one response permitted



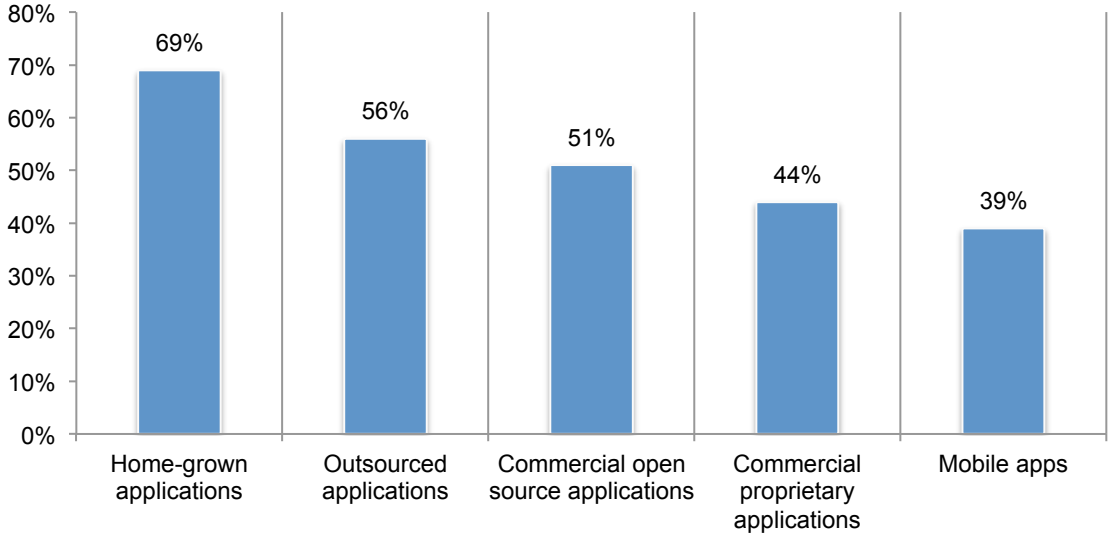
Organizations do not test Web applications enough. As mentioned above, less than half test their Web applications for vulnerabilities. Figure 14 reveals only 13 percent of organizations in this research test their Web applications every time the code changes. Forty-five percent do not regularly test their applications.

Figure 14. How often does your organization test its Web applications?



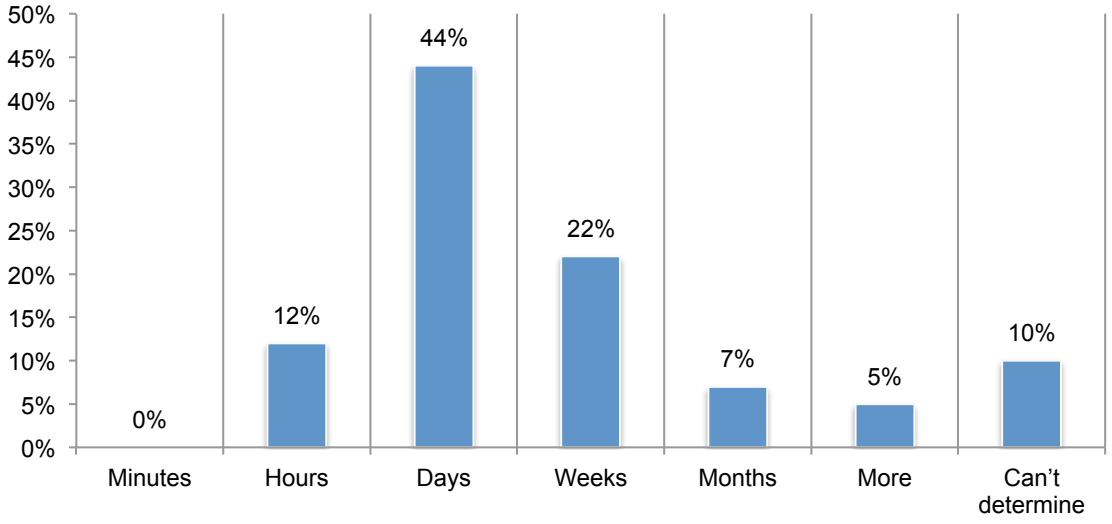
Externally sourced and mobile applications are not tested as much as they should be. As shown in Figure 15 respondents place a higher emphasis on testing home-grown applications (69 percent of respondents). This is higher than for outsourced applications (56 percent), commercial open source applications (51 percent), commercial proprietary applications (44 percent)) or mobile apps (39 percent).

Figure 15. Do you test Web applications in the following categories?
More than one response permitted



Fixing compromised Web applications can take days or weeks. On average, 66 percent of respondents say it takes days (44 percent of respondents) or weeks (22 percent of respondents) to fix one compromised Web application whenever a vulnerability is found.

Figure 16. How long does it take to fix one compromised Web application?



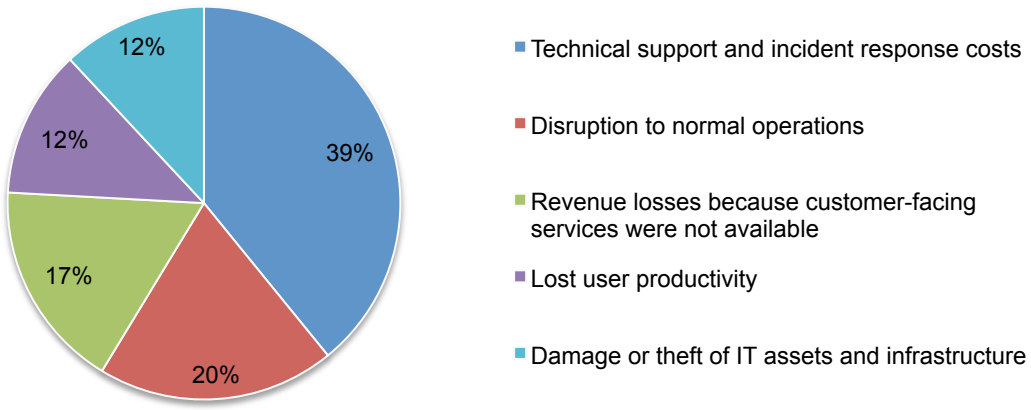
The cost of Web application security

How costly are attacks against an organization's Web applications? The average total cost per year to deal with attacks against Web applications is approximately $3.1 million. As shown in Table 1, this includes technical support and incident response ($1.2 million), lost user productivity ($382,555), disruption to normal operations ($613,636), damage or theft of IT assets and infrastructure ($374,655) 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
Technical support and incident response costs	$1,227,618
Lost user productivity	$382,555
Disruption to normal operations	$613,636
Damage or theft of IT assets and infrastructure	$374,655
Revenue losses because customer-facing services were not available	$538,745
Total	$3,137,209

According to Pie Chart 1, the largest percentage of cost is technical support and incident response. Damage or theft of IT assets and infrastructure is the smallest.

Chart 1. Breakdown of the cost of Web application attacks



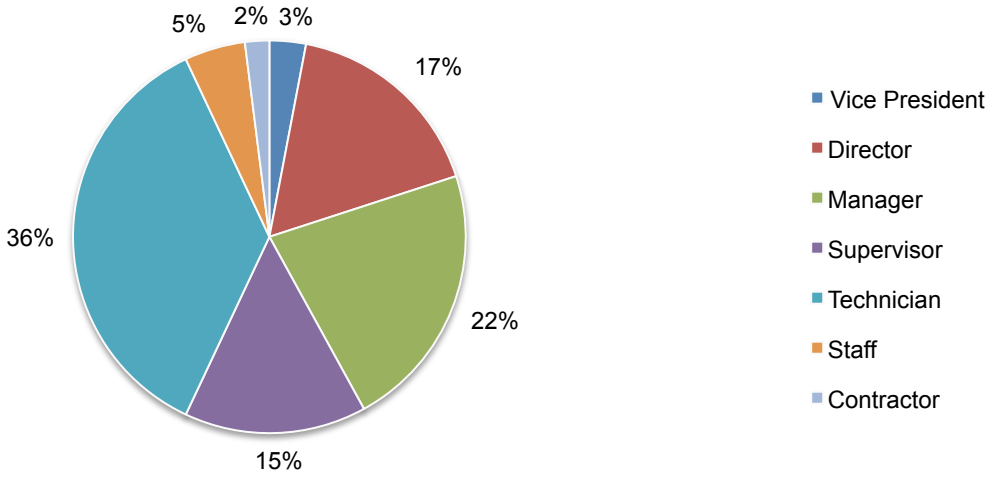
Part 3. Methods

The sampling frame is composed of 17,402 IT and IT security practitioners located in the United States and who are familiar with the Open Web Application Security Project (OWASP). As shown in Table 1, 657 respondents completed the survey. Screening removed 63 surveys. The final sample was 594 surveys (or a 3.4 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	17,402	100.0%
Total returns	657	3.8%
Rejected or screened surveys	63	0.4%
Final sample	594	3.4%

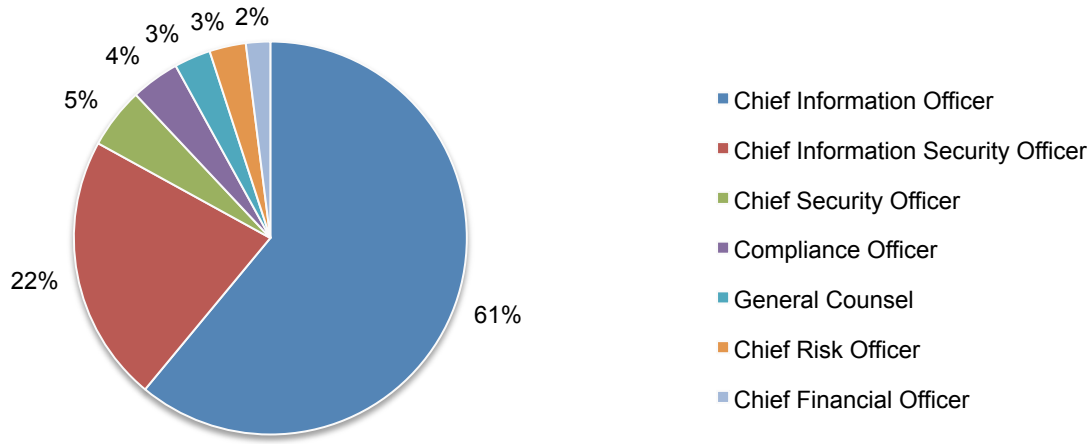
Pie Chart 2 reports the current position or organizational level of the respondents. More than half of respondents (57 percent) reported their current position as supervisory or above.

Pie Chart 2. Current position or organizational level



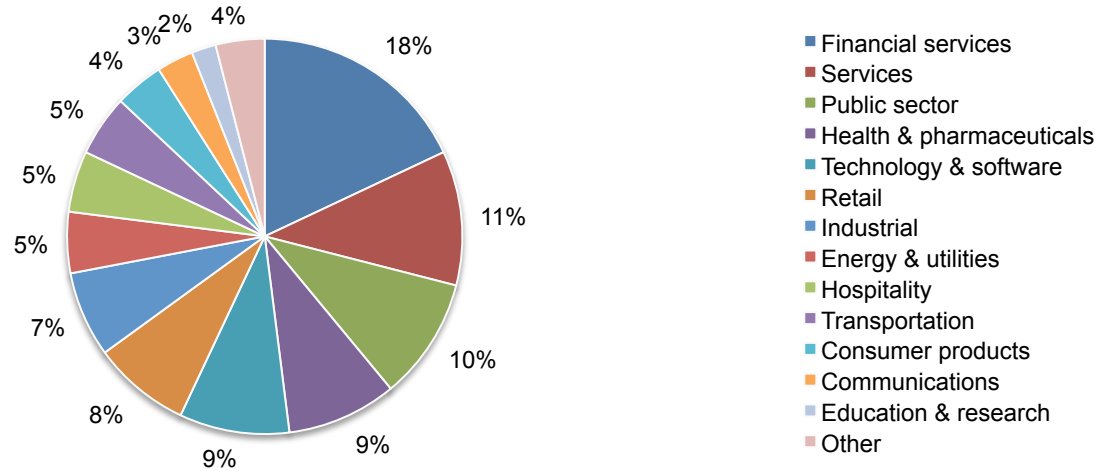
Pie Chart 3 identifies the primary person the respondent reports to. Sixty-one percent of respondents identified the chief information officer as the person they report to. Another 22 percent indicated they report directly to the CISO.

Pie Chart 3. Direct reporting channel



Pie Chart 4 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by services (11 percent) and public sector (10 percent).

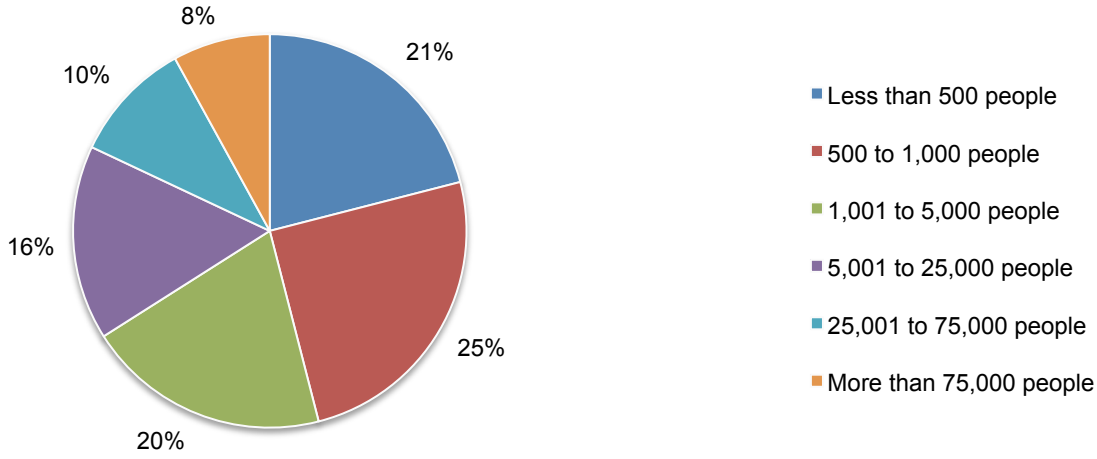
Pie Chart 4. Primary industry focus



According to Pie Chart 5, more than half of the respondents (54 percent) are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 5. Worldwide headcount of the organization

Extrapolated value = 14,672



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.