Ponemon INSTITUTE

State of Web Application Security

Sponsored by Imperva & WhiteHat Security

Independently conducted by Ponemon Institute LLC

Publication Date: 26 April 2010

State of Web Application Security

Ponemon Institute, 26 April 2010

Part 1: Executive Summary

Ponemon Institute conducted this study to better understand the risk of insecure websites and how organizations' are addressing internal and external threats.[1] Sponsored by Imperva and WhiteHat Security, the study reveals that despite having mission-critical applications accessible via their websites, many organizations are failing to provide sufficient resources to secure and protect Web applications important to their operations. This is particularly alarming given that the Web application layer is the number one attack target of hackers.[2]

We surveyed 638 IT and IT security practitioners with approximately 13 years IT experience in large US-based organizations with an average headcount of about 10,000. They most often are in network, data and application security, including quality assurance for development and testing. More than half are involved in setting priorities, managing budgets and selecting vendors and contractors.

While participants in this study consider the biggest threat to their websites is theft of data, they do not believe that their organizations are viewing Web security as a strategic initiative. They also believe their organizations are not allocating sufficient resources to protecting critical Web applications. Further, the IT practitioners surveyed are divided on whether the Web application security program is threat-based (41 percent) or compliance-based (40 percent).

Website risks are being ignored despite evidence that malicious and criminal attacks most often compromise databases or applications.[3] While there is no clear accountability for Web application security, the largest percentage of respondents (23 percent) report the information security officer or leader followed by IT operations are the most accountable.

As revealed in this study, websites are at risk for the following reasons:

- 70 percent of respondents do not believe their organizations (allocate) sufficient resources to secure and protect critical Web applications.
- 34 percent of urgent vulnerabilities are not fixed.
- 38 percent believe it would take more than 20 hours of developer time to fix one vulnerability.
- 55 percent of respondents believe developers are too busy to respond to security issues.

In addition to these findings, crosstab analysis revealed interesting differences between those organizations that are proactive in managing Web application security threats than those that are not proactive (and possibly reactive). Following are the main differences:

- Proactive organizations spend more than twice the amount on application security than non-proactive organizations (25 percent vs. 12 percent of the total IT security budget).
- Proactive organizations are much more likely to use Web application firewalls (43 percent vs. 21 percent) and SaaS (or Cloud) based security solutions (25 percent vs. 13 percent) than non-proactive organizations.
- Proactive organizations are much more likely to fix the most urgent vulnerabilities in a timely fashion than non-proactive organizations (50 percent vs. 19 percent).

---

[1] In this paper, website security and Web application security are terms used interchangeably.
[2] 2009 Verizon Business Data Breach Investigations Report, April 15, 2009
[3] A review of Privacy Rights Clearinghouse (www.privacyrights.org) chronology of data breaches that occurred in 2009 indicates 93 percent of all data breaches involving malicious or criminal attacks concerned compromised databases or applications.

Part 2: Key Findings

Most of the key findings are shown in bar chart format. The actual data utilized in each figure and referenced in the paper are shown in percentage frequency tables attached as an appendix to this paper.

There is a mismatch between the risk to Web application security and the budget allocated to address the risk. Web applications, which are considered by respondents as the most vulnerable, are not receiving as much budget as the least vulnerable areas of a website, according to respondents. Forty-three percent of the IT security budget is devoted to the network layer (considered one of the least vulnerable) while only 18 percent is allocated to applications.

Pie Chart 1: Q. In your opinion, is the level of your website security budget sufficient?

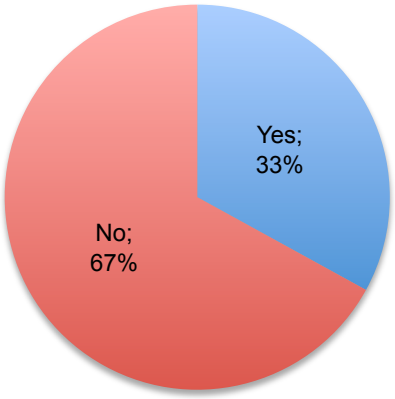
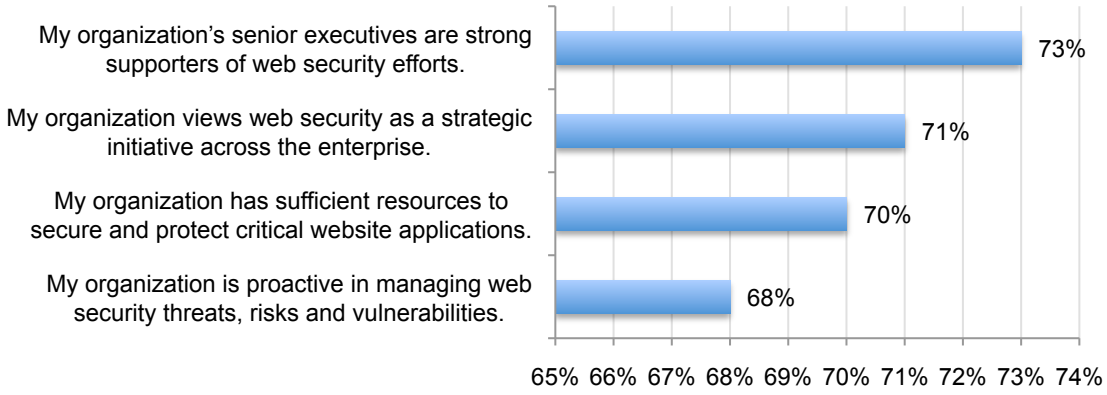


Table 1: IT security budget allocated by layer

Application security	18%
Data security	30%
Host security	9%
Infrastructure/network security	43%

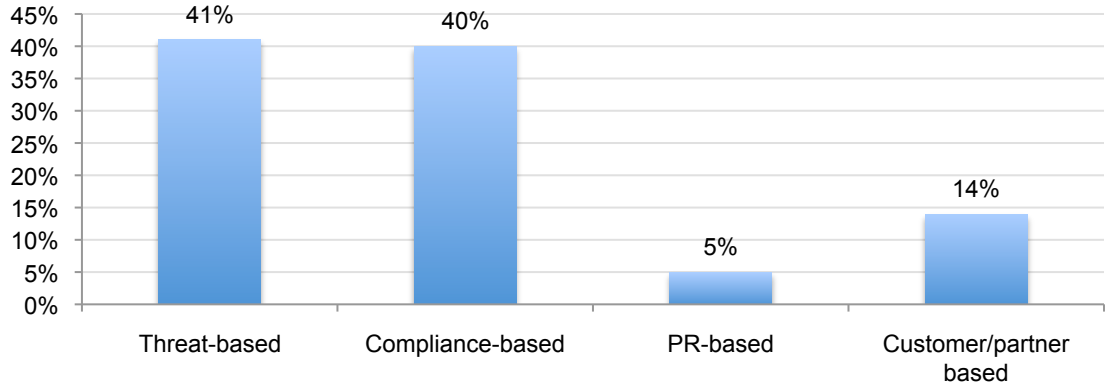
Lack of senior-level support for Web application security puts organizations at risk. Bar Chart 1 reports respondents' combined strongly disagree, disagree or unsure response (a.k.a. unfavorable views) to five statements about their organization. Seventy percent of respondents do not believe their organizations have sufficient resources to secure and protect critical Web applications. Seventy-three percent disagree that their senior executives are strong supporters of Web application security efforts or that the organization views it as a strategic initiative across the enterprise (71 percent). It is not surprising that 68 percent of respondents believe that their organizations are not proactive in managing Web application security threats and vulnerabilities.

Bar Chart 1: Attributions about Web application security
Combined strongly disagree, disagree and unsure combined



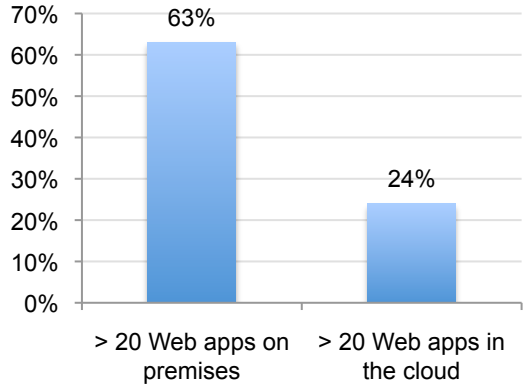
Respondents are evenly divided as to whether their Web application security programs are mostly threat-based or compliance-based. As shown in Bar Chart 2**,** 41 percent believe security is focused on thwarting attacks and 40 percent say it is focused on compliance with PCI, SOX, HIPAA and general audit requirements.

Bar Chart 2: Classification of Web application security program

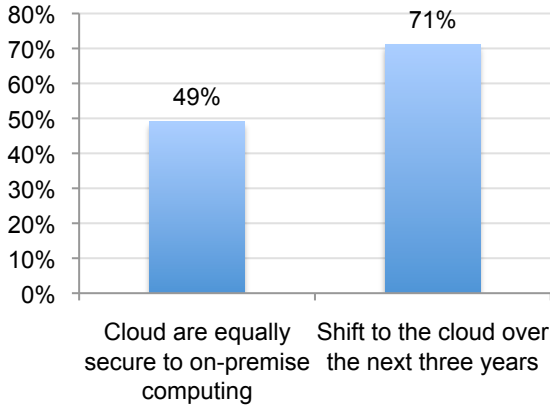


Web applications are moving to the cloud. On average, 63 percent of respondents say their organizations have more than 20 Web applications hosted on premises and 24 percent stay their organizations have more than 20 Web applications in the cloud. Seventy-one percent see a significant or slight shift to applications in the cloud. Only 16 percent believe cloud computing applications are more secure than on-premise applications and 49 percent believe cloud computing and on-premise applications are equally secure. See Bar Charts 3 and 4.

Bar Chart 3: Percent that 20 or more Web apps are hosted on premises or it the cloud



Bar Chart 4: Percentage yes response to two questions about cloud computing



The findings indicate that solutions in place today may not enable prompt remediation of vulnerabilities. Pie Chart 2 shows only 31 percent of respondents strongly agree or agree that vulnerabilities are resolved in a timely fashion. Table 2 reports the primary reasons these vulnerabilities may not be resolved quickly is that organizations do not have the resources secure coding requires (70 percent), developers are not responsible (56 percent) or are too busy with other activities to respond to security issues (55 percent). The least cited reason is not having access to the source code in order to perform code changes (16 percent).

Pie Chart 2: [Attribution] In my organization, fixing vulnerabilities in code is always done in a timely fashion

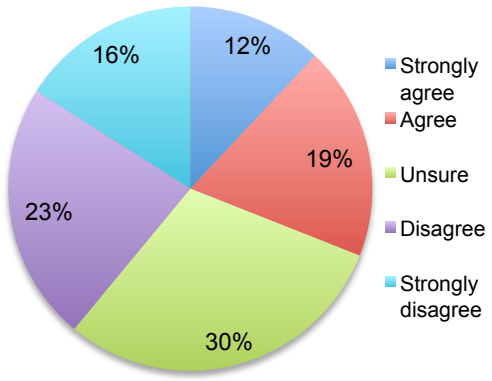
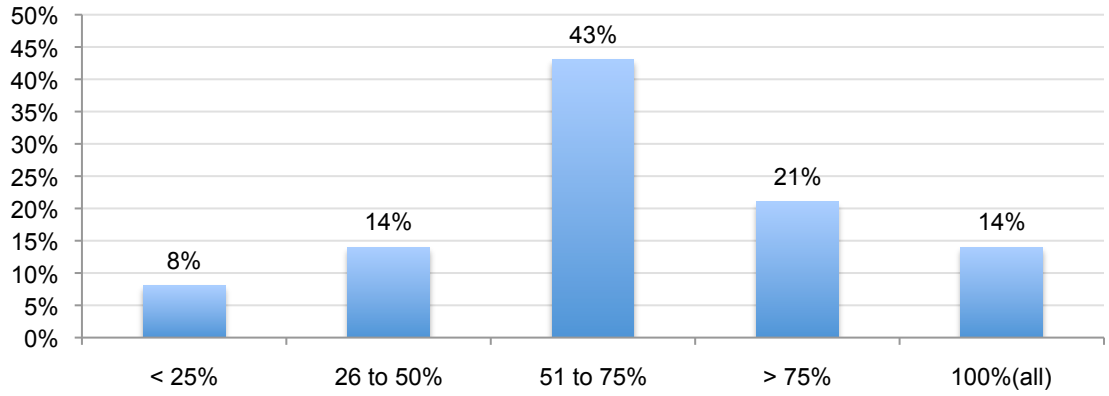


Table 2: Q. What are the main reasons why fixing vulnerabilities in code is not done in a timely fashion?

Secure coding requires resources we don't have	70%
Developers are not responsible for security	56%
Developers are too busy to respond to security issues	55%
Its not a corporate priority and developers do not care	43%
Source code is outsourced to developers	28%
We do not have the source code	16%

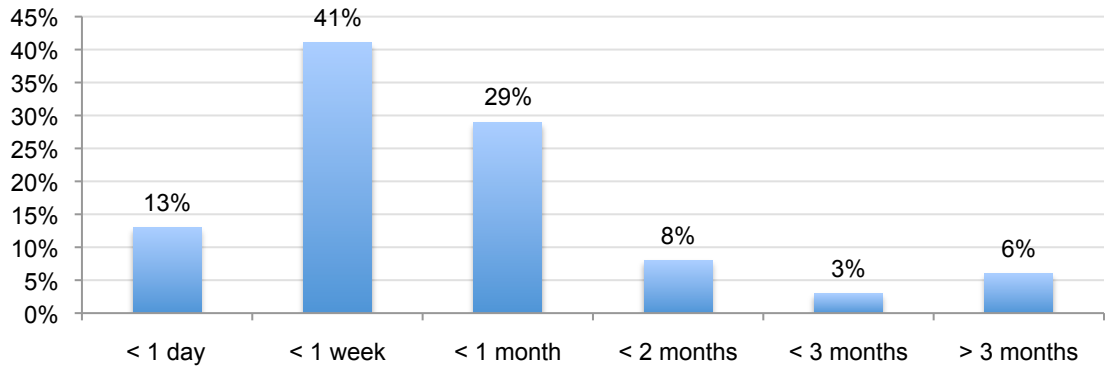
Bar Chart 5 shows the frequency of vulnerabilities resolved. Accordingly, more than 78 percent of respondents say their organizations resolve, on average, more than half of all urgent vulnerabilities affecting Web applications.

Bar Chart 5: Frequency of all urgent vulnerabilities that are fixed



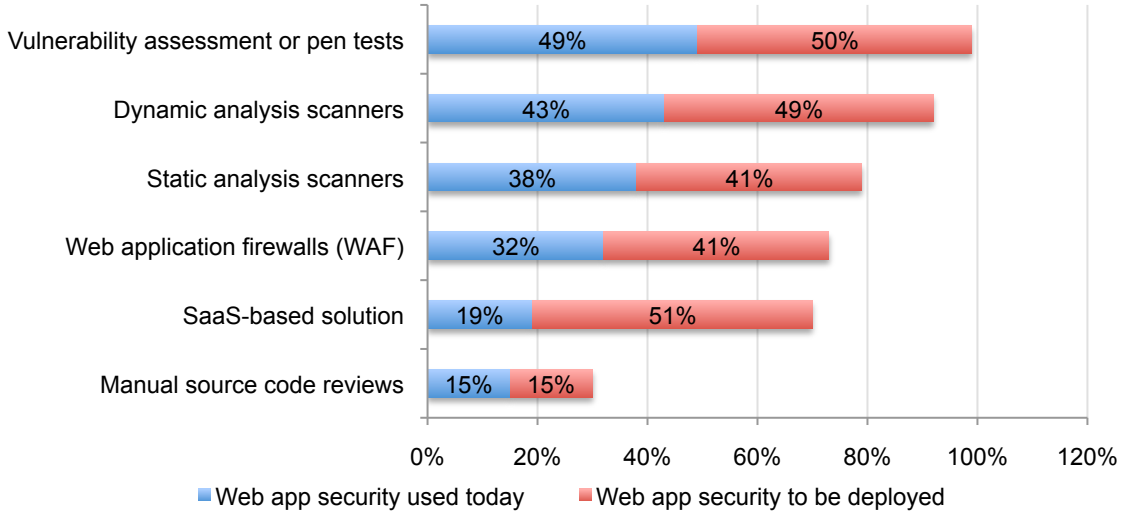
As reported in Bar Chart 6, 54 percent of respondents say vulnerabilities can be fixed in less than one week. Only 17 percent of respondents say vulnerabilities take more than one month to resolve.

Bar Chart 6: Average frequency for time to remediate one vulnerability



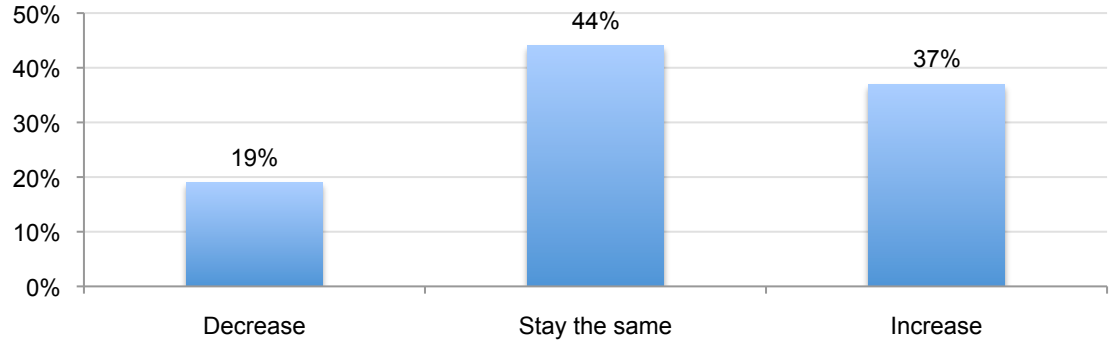
Respondents deploy different technologies to secure websites. Today, according to Bar Chart 7, the top two products or services used to secure websites are vulnerability assessment/penetration tests by third-party consultants (49 percent) followed by dynamic analysis scanners (43 percent). More than half are considering a SaaS-based solution (51 percent) or vulnerability assessment/penetration tests by third-party consultants (50 percent).

Bar Chart 7: Solutions used to secure Web applications



Spend on consulting services is expected to increase slightly. On average, organizations spent $338,000 on consulting services for Web application security in 2009. Fifty-eight percent expect their organization's consulting services budget to stay the same (38 percent) or increase slightly (20 percent). See Bar Chart 8.

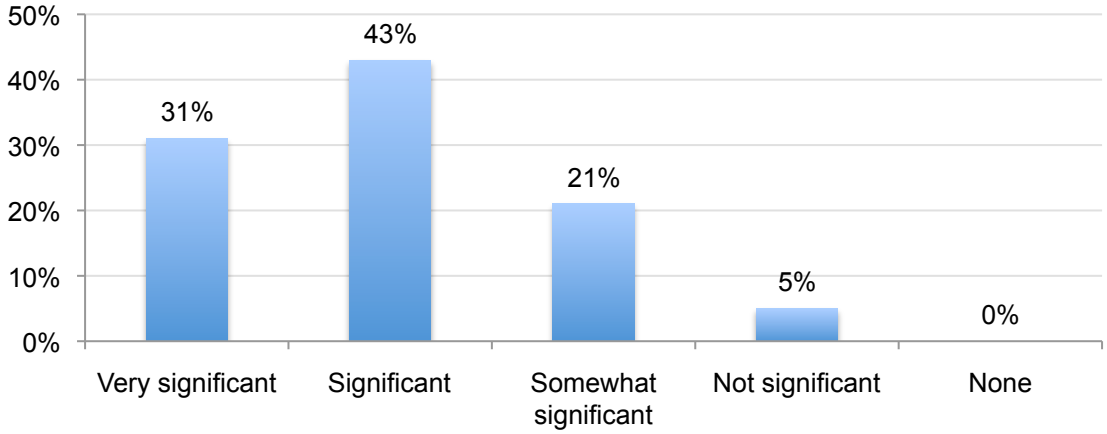
Bar Chart 8: Expected change in consulting services from 2009 to 2010



Fifty-nine percent allocate the IT security budget based on internal headcount. The average headcount of these organizations is about 10,000. Thirty percent allocate according to external service provider and 11 percent according to the number of consultants. As noted previously (see Pie Chart 3), only 33 percent of respondents say their organization's Web application security budget is sufficient.

Downtime can be costly. Disruption of service for one hour in accessing an organization's primary Web property would result in a very significant or significant loss of revenues, according to 74 percent of respondents.

Bar Chart 9: Significance of revenue loss resulting from website downtime for one hour



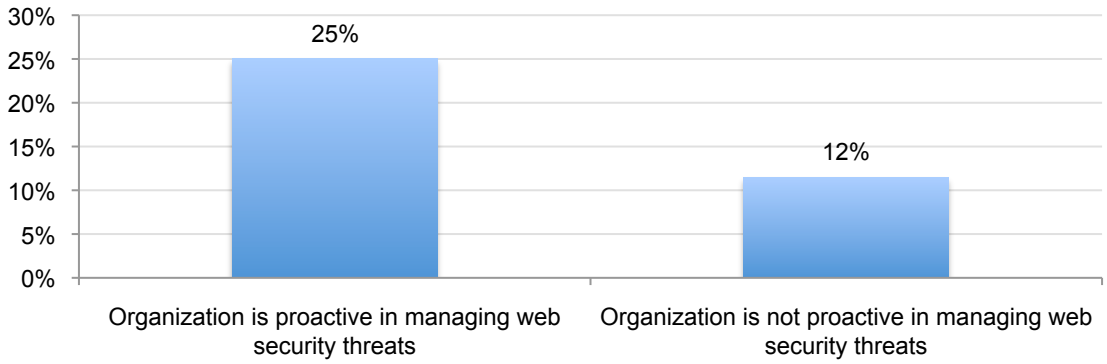
Additional Analysis

At the outset of the survey, we asked respondents to rate four attributions about their organization's Web application security. One of these questions expressly asked respondents to rate whether they believed their organizations are proactive in managing Web application security threats, risks and vulnerabilities (using a five-point scale from strongly agree to strongly disagree).

Approximately 32 percent of respondents agree or strongly agree that their organizations are proactive in managing Web application security. In contrast, 30 percent disagree or strongly disagree that their organizations are proactive. The remaining 38 percent of the sample provided ambiguous responses and, hence, were omitted from this additional analysis.

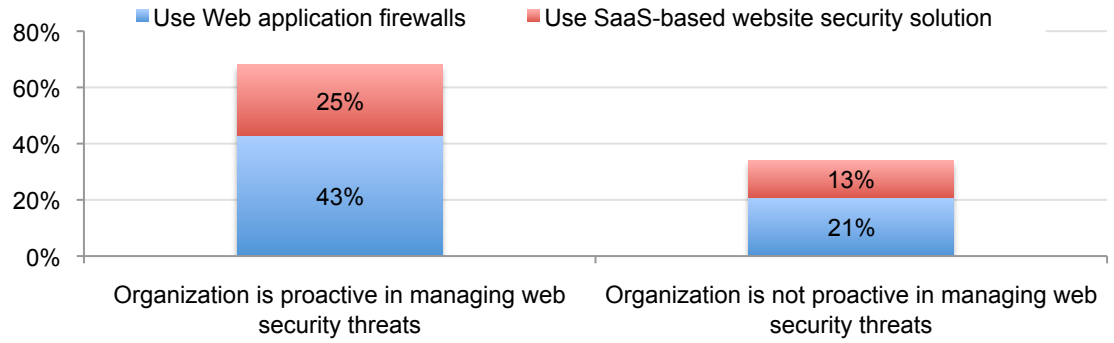
Proactive organizations spend more resources on application security. Respondents who believe their organizations are proactive in managing Web application security spend more than twice the amount (relative to the total IT security budget) on application security than those organizations that are not proactive (25 percent vs. 12 percent). See Bar Chart 10.

Bar Chart 10: Percentage of IT security budget allocated to the application security layer



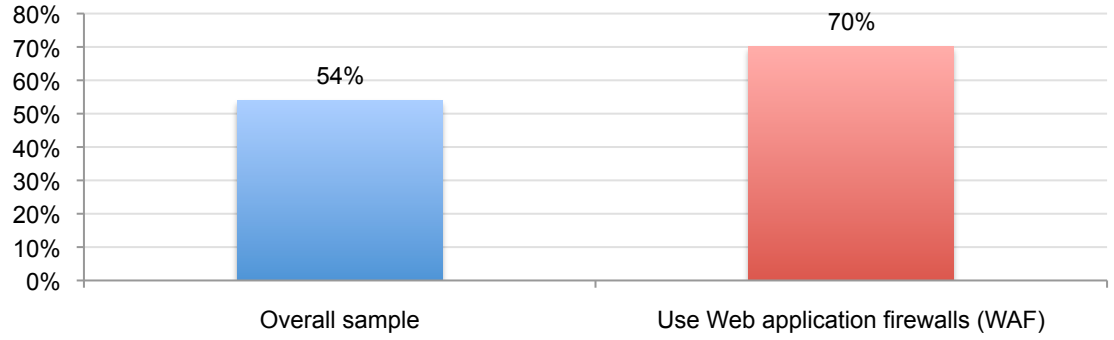
Proactive organizations are more likely to use leading Web application security technologies. Respondents who believe their organizations are proactive are much more likely to utilize Web application firewalls (WAF) and SaaS-based Web application security solutions than those respondents who view their organizations as non-proactive. See Bar Chart 11.

Bar Chart 11: Percentage use of WAF and SaaS-based Web application security



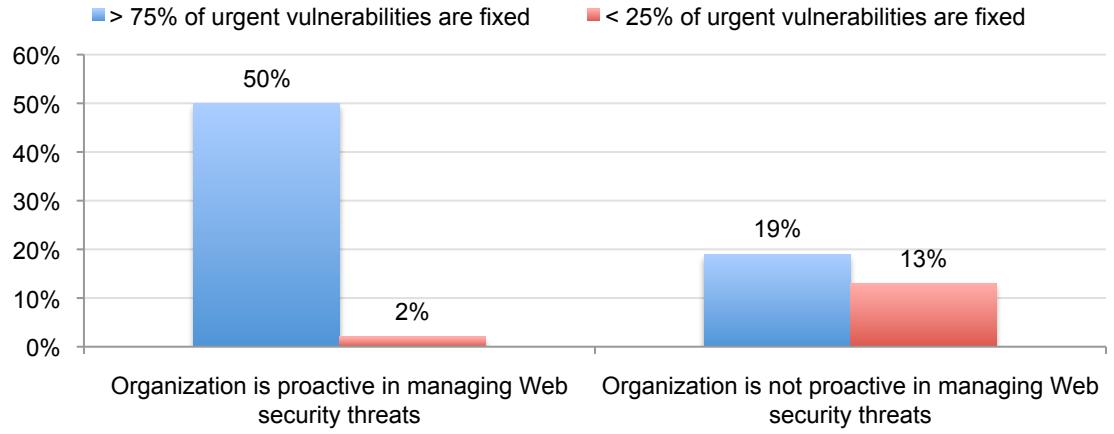
Organizations deploying WAF are more likely to fix urgent vulnerabilities faster than non-users. Bar Chart 12 shows the percentage of respondents who say their organizations typically remediate urgent vulnerabilities in less than one week. As shown, 70 percent of WAF users as opposed to 54 percent, say their organizations remediate vulnerabilities quickly.

Bar Chart 12: Percentage of WAF users that fix urgent vulnerabilities in less than one week



Proactive organizations are more responsive in fixing known vulnerabilities. Bar Chart 13 shows that proactive organizations are much more likely to fix 75 percent or more of all urgent vulnerabilities than non-proactive organizations (50 percent vs. 19 percent).

Bar Chart 13: Percentage of urgent vulnerabilities fixed
Greater than 75% and less than 25%



Part 3: Methods

A sampling frame of more than 11,000 adult-aged individuals who reside within the United States was used to recruit and select participants to this survey. Our randomly selected sampling frame was built from several proprietary lists of experienced IT and IT security practitioners. In total, 758 respondents completed the survey. Of the returned instruments, 120 surveys failed reliability checks. A total of 638 surveys were used as our final sample, which represents a 5.8 percent response rate.

Table 3: Sample and response statistics	Freq.	Pct%
Sampling frame	11,016	100.0%
Invitations sent	10,002	90.8%
Bounce back	1,873	17.0%
Returns	758	6.9%
Rejections	120	1.1%
Final sample	638	5.8%

Pie Chart 3 reports the primary industry sector of respondents' organizations. As shown, the largest segments include financial services, government, services, retail, and healthcare.

Pie Chart 3: Industry distribution of respondents' organizations

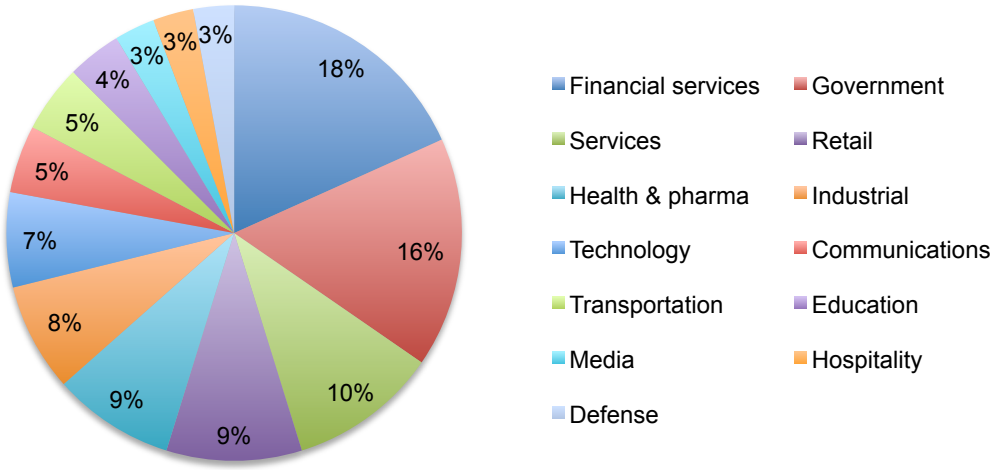


Table 4 reports the respondent organization's global headcount. As shown, a majority of respondents work within companies with more than 1,000 employees. Over 31 percent of respondents are located in larger-sized companies with more than 5,000 employees.

Table 4: The worldwide headcount of respondents' organizations	Pct%
Less than 500 people	7%
500 to 1,000 people	32%
1,001 to 5,000 people	30%
5,001 to 25,000 people	21%
25,001 to 75,000 people	8%
More than 75,000 people	2%
Total	100%

Table 5 reports the respondent's primary reporting channel. As can be seen, 51 percent of respondents are located in the organization's IT department (led by the company's CIO). Twenty-five percent report to the company's security officer or CISO.

Table 5: Respondent's primary reporting channel.	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	6%
General Counsel	3%
Chief Information Officer	51%
Compliance Officer	6%
Human Resources VP	0%
CSO/CISO	25%
Chief Risk Officer	8%
Other	1%
Total	100%

Table 6 reports the respondent organization's global footprint. As can be seen, a large number of participating organizations are multinational companies that operate outside the United States, Canada and Europe.

Table 6: Geographic footprint of respondents' organizations	Pct%
United States	100%
Canada	61%
Europe	59%
Middle east	21%
Asia-Pacific	49%
Latin America	34%
Average	54%

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. 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 holdout period. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- 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 a truthful response.

Part 5: Conclusion & Recommendations

The findings from this study reveal the challenges organizations are facing in their efforts to protect their websites from malicious and criminal attacks. IT practitioners in our study seem to be frustrated with the lack of an appropriate governance structure within their organization that would help ensure enough resources are allocated to protect their websites and to hold the appropriate individuals accountable for vulnerabilities.

Further contributing to the problem is the lack of an industry standard to determine who should be responsible for assessing and securing websites. Corporate security should join forces with business leaders to make Web application security an integral part of business operations. Otherwise, organizations will remain unable to address Web application vulnerabilities and prevent costly data breaches, lost productivity and downtime.

In addition to a serious misalignment between the risk to Web application security and the budget allocated to address the risk, we also found that developers do not have an incentive to respond to vulnerabilities in a timely fashion. For many, security is not considered as much a priority as other responsibilities they have. Further, they may not be rewarded for efforts to protect their organization's websites.

We believe in addition to increasing developer time and resources, there should be shift to the use of solutions that protect corporate websites until remediation takes place. Organizations should make Web application security the responsibility of the security team and direct them to address the problems where they occur on production websites. In addition, they should consider holding developer teams or business units accountable that fail to resolve Web application vulnerabilities.

Most important, the risk to websites should be recognized by senior executives as a real threat to an organization's information assets. Instead, as is shown in this study, organizations are ignoring this risk at their own possible peril.

Appendix I: Survey Details

Sample and response statistics	Freq.	Pct%
Sampling frame	11,016	100.0%
Invitations sent	10,002	90.8%
Bounce back	1,873	17.0%
Returns	758	6.9%
Rejections	120	1.1%
Final sample	638	5.8%

I. Attributions. Please rate each one of the following four statements using the scale provided below each item.	Strongly agree	Agree
Q1a. My organization has sufficient resources to secure and protect critical Web applications.	9%	21%
Q1b. My organization's senior executives are strong supporters of Web security efforts.	8%	19%
Q1c. My organization views Web security as a strategic initiative across the enterprise.	11%	18%
Q1d. My organization is proactive in managing Web security threats, risks and vulnerabilities.	12%	20%

II. Questions

Q2a. How is your IT security budget allocated by layer? Please assign an approximate percentage for each layer (which must sum to 100%)	Points
Application security	18%
Data security	30%
Host security	9%
Infrastructure/network security	43%
Total	100%

Q2b. Please rank the following layers with respect to the **significance of security threats** your organization faces today, where 1 = most significant to 4 = least significant.	Forced rank	Rank order
Application	1.93	1
Data	2.18	2
Host	2.95	4
Infrastructure/network	2.54	3
Average	2.40	

Q3. Approximately how many public-facing Web applications does your organization have?	Pct%	Extrapolated value
1 to 10	15%	1
11 to 50	32%	10
51 to 100	29%	22
101 to 500	14%	42
More than 500	4%	24
I don't know	6%	-
Total	100%	98

Q4. Approximately how many internal-facing Web applications does your organization have?	Pct%	Extrapolated value
1 to 10	21%	1
11 to 50	49%	15
51 to 100	13%	10
101 to 500	9%	27
More than 500	2%	12
Don't know	6%	-
Total	100%	65

Q5. In percentage terms, how many of your organization's mission-critical business processes are accessible via the Web?	Pct%	Extrapolated value
Less than a 25%	8%	2%
Between 26 and 50%	32%	12%
Between 51 and 75%	23%	16%
More than 75%	18%	14%
All (100%)	10%	10%
Don't know	9%	0%
Total	100%	54%

Q6. What products and services are you currently using to secure your organization's website(s)? Please check all that apply.	Total
Dynamic analysis scanners (such as HP WebInspect, IBM Rational Appscan, Cenzic Hailstorm and others)	43%
Static analysis scanners (such as Foritfy SCA, Ounce, Veracode and others)	38%
Web Application Firewalls (such as Imperva SecureSphere, F5 Application Security Manager, Breach ModSecurity and others)	32%
SaaS-based solution (such as WhiteHat Sentinel vulnerability management services)	19%
Vulnerability Assessment / Penetration Tests by third-party consultants	49%
Manual source code reviews by third-party consultants	15%
None of the above	39%
Total	235%

Q7. From the previous question, how much of a role did industry analysts, such as Gartner, Forrester, IDC, and others, contribute to your procurement decisions?	Pct%	
Very significant	9%	
Significant	11%	Significant
Somewhat significant	38%	58%
Not significant	30%	
None	12%	
Total	100%	

Q8. What products and services are you considering to deploy in 2010 to protect your organization's website(s)? Please check all that apply.	Total
Dynamic analysis scanners (such as HP WebInspect, IBM Rational Appscan, Cenzic Hailstorm and others)	49%
Static analysis scanners (such as Foritfy SCA, Ounce, Veracode and others)	41%
Web Application Firewalls (such as Imperva SecureSphere, F5 Application Security Manager, Breach ModSecurity and others)	41%
SaaS-based solution (such as WhiteHat Sentinel vulnerability management services)	51%
Vulnerability Assessment / Penetration Tests by third-party consultants	50%
Manual source code reviews by third-party consultants	15%
None of the above	23%
Total	270%

Q9. How many full-time staff within your organization are dedicated to website security?	Pct%	Extrapolated value
No full-time staff	4%	-
Between 1 and 5	40%	1.0
Between 5 and 10	42%	3.2
Between 11 and 15	9%	1.2
Between 16 and 25	3%	0.6
More than 25	2%	0.6
Total	100%	6.5

Q10. How much did you spend on consulting services for website security in 2009?	Pct%	Extrapolated value
Nothing	19%	-
Less than $50,000	11%	4,400
$50,000 to $100,000	18%	13,500
$100,001 to $500,000	19%	47,500
$500,001 to $1,000,000	13%	97,500
More than $1,000,000	16%	176,000
I don't know	4%	-
Total	100%	$338,900

Q11. How is your consulting services budget for website security going to be affected in 2010?	Pct%	
Significant decrease (more than 50%)	0%	
Decrease (about 20 to 50%)	9%	Decrease
Slight decrease (about 1 to 10%)	10%	19%
Stay the same	38%	
Slight increase (about 1 to 10%)	20%	
Increase (about 20 to 50%)	14%	Increase
Significant increase (more than 50%)	3%	37%
I don't know	6%	
Total	100%	

Q12. How is your IT security budget allocated by service provider? Please assign an approximate percentage for each service provider (which must sum to 100%)	Points
External Service Provider	30%
Internal Headcount	59%
Consultant	11%
Total	100%

Q13. In your opinion, is the level of your organization's website security budget sufficient?	Pct%
Yes	33%
No	67%
Total	100%

Q14. Does your organization apply punitive repercussions for developer teams or business units who fail to resolve website vulnerabilities according to policy?	Pct%
Yes	19%
No	81%
Total	100%

Q15. If your organization's primary Web property were completely disrupted for one hour, how significant would the potential revenue loss be?	Pct%	
Very significant	31%	Significant
Significant	43%	74%
Somewhat significant	21%	
Not significant	5%	
None	0%	
Total	100%	

Q16. Please rank the following eight (8) costs of a data breach, where 1 = most significant cost and 8 = least significant cost.	Forced rank	Rank order
Legal	5.40	6
Consultants	3.51	4
Lost productivity	1.40	1
Cost of notification	7.09	8
Free or subsidized services to breach victims	7.70	9
Customer or consumer churn (turnover)	3.54	5
System or process remediation	1.71	2
Diminished brand	2.49	3
Fines and penalties	6.51	7

Q17. Typically, how long does it take your organization to remediate urgent vulnerabilities?	Pct%
Less than a day	13%
Less than a week	41%
Less than a month	29%
Less than two months	8%
Less than three months	3%
More than three months	6%
Total	100%

Q18. Typically, what percent of all urgent vulnerabilities do you and organization fix?	Pct%	Extrapolated value
Less than 25%	8%	1%
Between 26 and 50%	14%	5%
Between 51 and 75%	43%	27%
More than 75%	21%	18%
All (100%)	14%	14%
Total	100%	66%

Q19a. In my organization, fixing vulnerabilities in code is always done in a timely fashion.	Pct%	
Strongly agree	12%	Agreement
Agree	19%	31%
Unsure	30%	
Disagree	23%	
Strongly disagree	16%	
Total	100%	

Q19b. [If unsure or disagree] What are the main reasons why fixing vulnerabilities in code is not done in a timely fashion?	Total
We do not have the source code	16%
We have the source code, but it is outsourced to developers that are not in-house	28%
Developers are not responsible for security	56%
Developers are too busy to respond to security issues	55%
Its not a corporate priority and developers do not care	43%
Secure coding requires resources we don't have	70%
Other (please specify)	3%
Total	271%

Q20. On average, how many developer hours does it take in to fix one vulnerability?	Pct%	Extrapolated value
Less than 1 hour	0%	-
Between 1 to 5 hours	15%	0.38
Between 6 to 10 hours	34%	2.72
Between 11 to 20 hours	13%	1.95
Between 21 to 50 hours	18%	6.30
More than 50 hours	11%	6.60
Don't know	9%	-
Total	100%	17.95

Q21. Approximately, what percentage of security vulnerabilities did you and your organization fix in the last version?	Pct%	Extrapolated value
Less than a 25%	6%	1%
Between 26 and 50%	15%	6%
Between 51 and 75%	49%	31%
More than 75%	19%	17%
All (100%)	5%	5%
Don't know	6%	0%
Total	100%	59%

Q22. How would you classify your website security program? Please assign an approximate percentage for each choice listed (which must sum to 100%).	Points
Threat-based (designed to thwart the attack as currently understood)	41%
Compliance-based (PCI, SOX, HIPAA, general audit)	40%
PR-based (concern over publicly disclosed breaches)	5%
Customer/partner based (require certain level of measurable security policies/procedures)	14%
Total	100%

Q23. Please rank the criticality of the following three threats from 1 = most critical to 3 = least critical.	Forced rank	Rank order
Automated attacks	2.15	2
Fraud	2.57	3
Data theft	1.28	1
Average	2.00	

Q24. In your organization, how many applications are currently hosted on premises?	Pct%	Extrapolated value
None	3%	0
Between 1 to 10	10%	0.5
Between 11 to 20	24%	3.6
Between 21 to 50	26%	9.1
Between 51 to 100	21%	15.75
More than 100	16%	19.2
Total	100%	48.15

Q25. In your organization, how many applications are currently hosted in the cloud?	Pct%	Extrapolated value
None	32%	0
Between 1 to 10	23%	1.15
Between 11 to 20	21%	3.15
Between 21 to 50	15%	5.25
Between 51 to 100	9%	6.75
More than 100	0%	0
Total	100%	16.3

Q26. In your opinion, how will the ratio of on-premise applications versus cloud computing applications change in the next one to three years?	Pct%	
Significant shift to applications in the cloud	23%	Increase cloud
Slight shift to applications in the cloud	48%	71%
No change	21%	
Slight shift to applications on premises	8%	
Significant shift to applications on premises	0%	
Total	100%	

Q27. How do you perceive the level of security for the applications in the cloud versus on-premises?	Pct%
Cloud computing applications are more secure than applications on-premises	16%
Cloud computing and on-premise applications are equally secure	49%
On-premise applications are more secure than cloud computing applications	35%
Total	100%

Q28a. Who in your organization is **most responsible** for Web application security?	Pct%
Security officer or leader	8%
Information security officer or leader	23%
Quality assurances	6%
Chief information officer	11%
Chief technology officer	4%
Website administrator	13%
Compliance	8%
IT operations	18%
Systems development and testing	5%
Internal audit	3%
Risk management	1%
Other (please specify)	0%
Total	100%

Q28b. Does your organization have a dedicated Web application security team?	Pct%
Yes	26%
No	74%
Total	100%

Q29a. For application security, which of the following technology combinations do you use?	Pct%
Pen testing plus code analysis to identify code flaws uncovered by pen tests	20%
Pen testing plus WAF to shield vulnerabilities uncovered by pen tests	33%
WAF plus code analysis to fix code flaws found in production by the WAF	37%
None of the above	10%
Total	100%

Q29b. Even if you do not use any of the above technology combinations, please rank from 1 = most important to 3 = least important for ensuring application security?	Forced rank	Rank order
Pen testing plus code analysis to identify code flaws uncovered by pen tests	2.61	3
Pen testing plus WAF to shield vulnerabilities uncovered by pen tests	1.88	2
WAF plus code analysis to fix code flaws found in production by the WAF	1.47	1
Average	1.99	

III. Your role

D1. What organizational level best describes your current position?	Pct%
Senior Executive	0%
Vice President	3%
Director	25%
Manager	40%
Supervisor	15%
Technician	9%
Staff	8%
Contractor	0%
Total	100%

D2. Is this a full time position?	Pct%
Yes	98%
No	2%
Total	100%

D3. Check the **Primary Person** you or your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	6%
General Counsel	3%
Chief Information Officer	51%
Compliance Officer	6%
Human Resources VP	0%
CSO/CISO	25%
Chief Risk Officer	8%
Other	1%
Total	100%

Experience	Mean	Median
D4a. Total years of relevant experience	13.48	12.5
D4b. Total years of IT or security experience	12.88	12
D4c. Total years in current position years	5.46	5

D5. Gender	Pct%
Female	34%
Male	66%
Total	100%

D6. What industry best describes your organization's industry focus?	Pct%
Airlines	2%
Automotive	1%
Brokerage & Investments	3%
Communications	4%
Chemicals	1%
Credit Cards	3%
Defense	3%
Education	4%
Energy	2%
Entertainment and Media	3%
Federal Government	11%
Food Service	2%
Healthcare	6%
Hospitality	3%
Manufacturing	5%
Insurance	2%
Internet & ISPs	1%
State or Local Government	6%
Pharmaceuticals	3%
Professional Services	5%
Research	2%
Retailing	8%
Retail Banking	11%
Services	4%
Technology & Software	7%
Transportation	2%
Total	100%

D7. Where are your employees located? (check all that apply):	Pct%
United States	100%
Canada	61%
Europe	59%
Middle east	21%
Asia-Pacific	49%
Latin America	34%
Average	54%

D8. What is the worldwide headcount of your organization?	Pct%	Extrapolated value
Less than 500 people	7%	28
500 to 1,000 people	32%	240
1,001 to 5,000 people	30%	750
5,001 to 25,000 people	21%	3,150
25,001 to 75,000 people	8%	4,000
More than 75,000 people	2%	1,650
Total	100%	9,818

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 organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.