OWASP Security Spending Benchmarks Project Report

March 2009

Project Leader: Boaz Gelbord
Executive Director of Information Security
Wireless Generation

Project Partners:

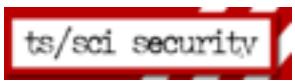


Table of Contents

Executive Summary

How much security spending is enough? Security - whether processes, policies, or technical measures- imposes a real cost on organizations. The Security Spending Benchmarks Project seeks to establish an industry accepted benchmark for justifying overall Web application security spending. We want to quantify how many dollars and human resources should be allocated towards the software development life-cycle, security training, security software/tools, independent third-party reviews, Web application firewalls, etc.

This project is motivated by the fact that there are few, if any, industry standard benchmarks for executive management to consider when deciding what is a reasonable amount of resources to spend on Web application security in or out of the software development processes. Although some industry regulations like PCI are more technical in nature, most state and federal regulations are based on the idea of taking reasonable measures to secure data. Until now, there has been very little data as to how this translates into monetary terms.

The survey was conducted through a network of 17 partner organizations that included security research and consultancy companies and industry associations. There were a total of 51 valid responses to our survey that were procured through our 17 project partners.

Key findings of this study are:

- Organizations that have suffered a public data breach spend more on security in the development process than those that have not.
- Web application security spending is expected to either stay flat or increase in nearly two thirds of companies.
- Half of respondents consider security experience important when hiring developers, and a majority provide their developers with security training.
- 38% have a third party firm conduct a security review of outsourced code.
- At least 61% of respondents perform an independent third party security review before deploying a Web application while 17% do not (the remainder do not know or do so when requested by customers).
- Just under half of the surveyed organizations have Web application firewalls deployed for at least some of their Web applications.

1 Introduction

The Security Spending Benchmarks Project started as a simple conversation[1] between myself and Jeremiah Grossman about how much organizations should spend on security in the development process. As we dug deeper, we realized that there was little pre-existing data on this topic. How are organizations to know what the right level of security spending is?

This question led us to the OWASP Security Spending Benchmarks Project. This report contains our first results from what is intended to become a quarterly effort.

All surveys produce data that needs to be taken with a certain grain of salt. Particularly with security related surveys that offer participants some anonymity, it is virtually impossible to guarantee that participants are answering questions truthfully. There are however a number of principles that can be applied to increase the general quality of the data and to increase community confidence in the results. We believe that we have taken these steps by basing The OWASP Security Spending Benchmarks Project on a number of key principles:

- *Transparency of process*. The current status of the project and analysis can always be found on the website.[2]
- *Open participation and independence*. Organizations that can demonstrate a willingness and ability to volunteer their time are welcome to take part. The project is purely voluntary and has not been funded by any entity.
- *Open availability of survey results*. All raw survey results are open to project partners, allowing any one to draw their own conclusions or take issue with the report findings.
- *Industry credibility*. Assembling of a team of high quality partners from amongst leaders in the field and soliciting advice from the community.

This project would not have been possible without our project partners, who provided invaluable help in formulating, promoting, and analyzing the survey. All participation in this effort has been purely voluntary. I would like to thank all our partners for their contributions.

Particular thanks are due to Jeremiah Grossman (CTO and Founder of WhiteHat) who played an instrumental role in the planning and execution of this project.

Boaz Gelbord

Project Leader

1 http://www.boazgelbord.com/2008/12/owasp-security-spending-benchmarks.html and http://jeremiahgrossman.blogspot.com/2008/12/budgeting-for-web-application-security.html

2 http://www.owasp.org/index.php/Category:OWASP_Security_Spending_Benchmarks

2 Survey Results

Participant Profiles

A total of 51 companies completed the survey questionnaire. The respondents have different roles within their organizations, with the two largest groups being technical security professionals (53%) and executives (25%). A large range of industries are represented with finance being the largest group at 24%. The breakdown by size and revenue is as follows:

Figure 1: Number of Employees:

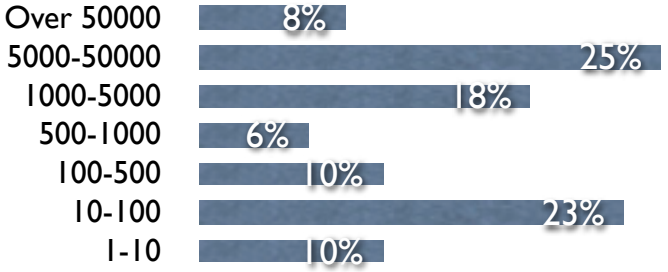
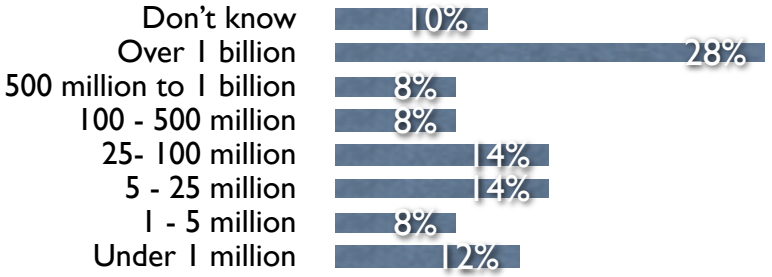


Figure 2: Annual Revenue



Motivations For Security Spending

Although 50% of companies state that they use security as part of their branding strategy, companies overwhelmingly do not rank competitive advantage as a factor driving security spending decisions. 61% of respondents list competitive advantage last amongst a group of five factors. Compliance is cited most frequently (40%) as the most important driver behind security spending.

Security Spending

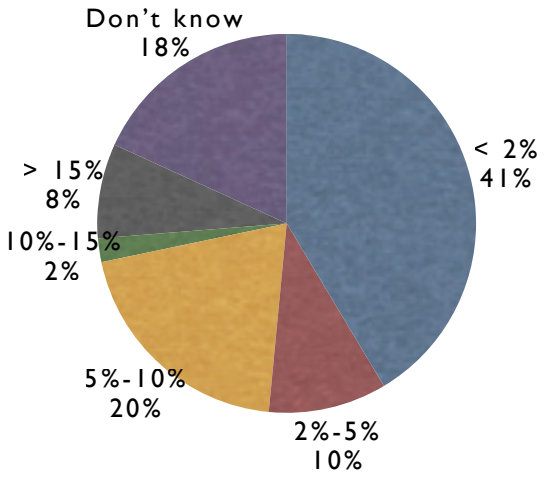
67% of companies have a specific IT security budget. Out of companies with 1000 employees or more, that figure rises to 89%. Companies that have suffered a public data breach in the last two years were more likely (86% vs. 52%) to have a specific IT security budget.

Web application security forms less than 10% of overall security spending in 36% of companies, and a further 33% do not know what portion of security spending is on Web applications.

Despite the economic downturn, over a quarter of respondents expect Web application security spending to increase in 2009 and 36% expect it to remain flat.

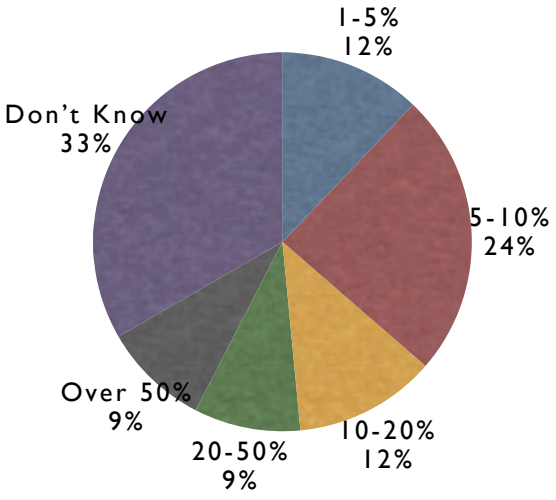
The specific development budget or headcount dedicated to security is low in most organizations:

Figure 3: Percentage of Development Budget or Headcount Dedicated to Security



There are a wide range of responses from organizations regarding the percentage of their IT security budget that is dedicated towards Web application security. Organizations with a greater percentage of their revenue passing through their website report a higher rate of spending. A third of organizations do not know what portion of their IT security budget is dedicated towards Web application security:

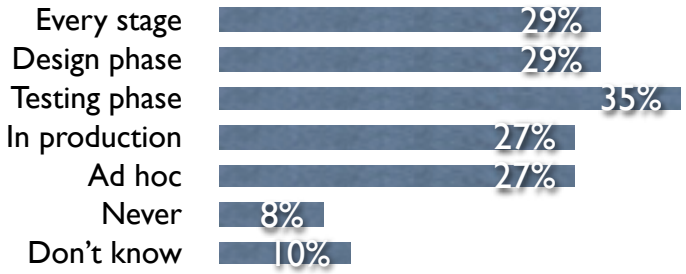
Figure 4: Percentage of IT Security Budget dedicated towards Web application security



Security in Software Development Lifecycle

There is no uniform point at which security checkpoints are present during the Web application software development lifecycle.

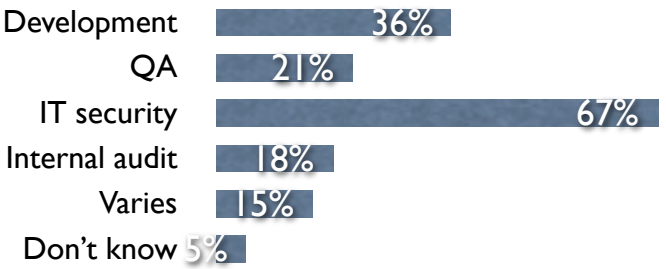
Figure 5: Security Checkpoint Reviews in the Software Development Lifecycle (multiple responses possible)



Responsibility for Security Checkpoints

Organizational responsibility for the development security reviews in the software development lifecycle is spread around different departments, with multiple departments sharing responsibility:

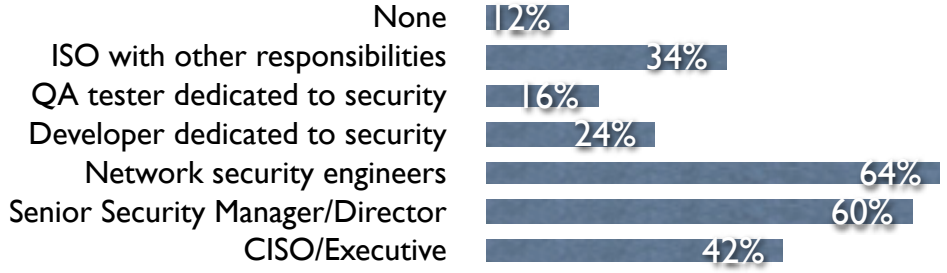
Figure 6: Organizational Responsibility for Development Security Reviews (multiple responses possible)



Security Personnel

Organizations employ a variety of security-related personnel. For each of the dedicated security professionals, larger organizations report having more of each type of employee.

Figure 7: Security Related Personnel in Organizations



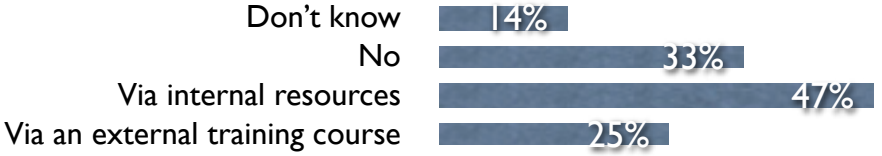
Organizations that had reported a public security breach in the last two years were more likely by a margin of 71% to 26% to have a Chief Information Security Officer.

Security Training

About half of respondents consider security experience as at least somewhat important in hiring new developers.

For existing employees, the majority of organizations provide software security training, using either internal resources, external courses, or both:

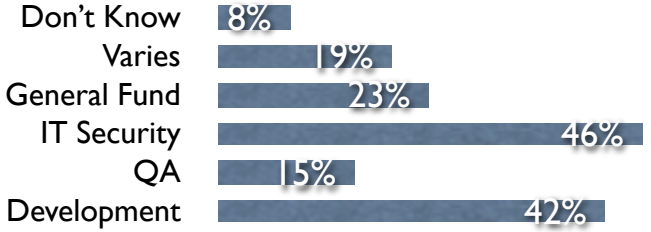
Figure 8: Software Security Training Provided to Developers (multiple responses possible)



Of those organizations providing training, 69% give training to more than half of their developers.

Developer training costs are allocated from several budgets within the same organization, with IT security and development budgets being the most frequent source:

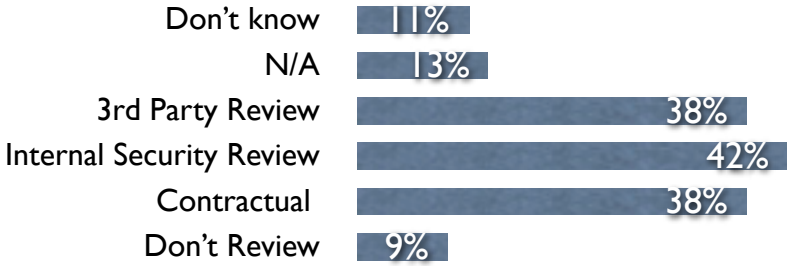
Figure 9: Budget From Which Developer Training Costs Are Allocated (multiple responses possible)



Outsourcing

Just under a quarter of respondents outsource half of more of their Web application development. Organizations take the following steps to review outsourced code:

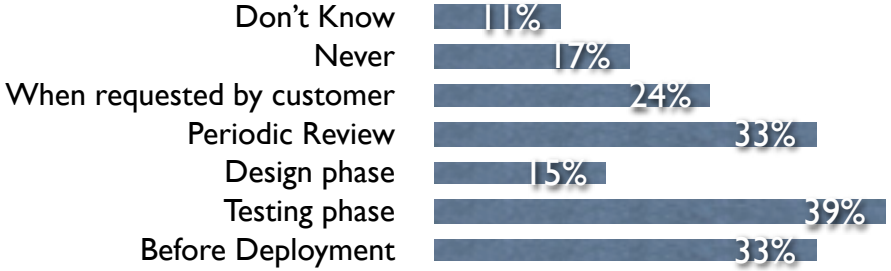
Figure 11: Methods for Reviewing the Security of Outsourced or Subcontracted Code (multiple responses possible)



Third Party Security Reviews

The survey measured at what point third party reviews are conducted. A total of 61% of respondents perform an independent third party security review before deploying a Web application while 17% do not and the remainder do not know or do so when requested by the customer. The point at which these reviews are performed:

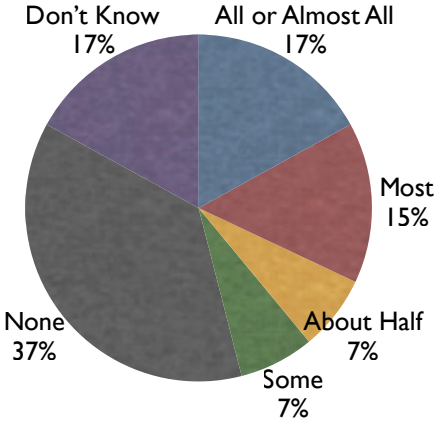
Figure 12: Points at Which Third Party Security Reviews are Conducted Prior to Deploying a Web Application (multiple responses possible)



Web Application Firewalls

Over a third of organizations do not use Web application firewalls at all to monitor or defend applications. Out of those organizations that use Web application firewalls, in 57% of cases the cost is allocated from the IT security budget. The survey also measured the portion of deployed web applications with a Web application firewall:

Figure 10: Percentage of Deployed Web Applications with Web Application Firewalls Monitoring or Defending Them



3 Methodology

The goal of the survey was to measure as accurately as possible security spending on Web applications and related areas. While we recognize the inherent limitations of Web-based surveys, the goal of the survey was to collect useful data that can stimulate a conversation on this topic. The survey was created with the principles that:

- The process should be transparent for all partners and for the community at large.
- The questions should be formulated neutrally so as not to affect results.
- All responses should be anonymous
- All raw survey results should be made available to the community.

To allow respondents to candidly describe their organizations, no identifiable information was collected, including IP address.

Data Cleansing

65 respondents filled in the survey. Out of these, 14 responses were discarded for having spent less than 2 minutes on the survey and not completing more than one third of the answers. The remaining 51 responses were almost entirely complete. The average response time was 8 minutes, with 90% of respondents taking between 5 and 15 minutes to answer the survey.

Potential Causes for Inaccurate Results

- For privacy reasons IP addresses were not collected. It is therefore possible that a respondent could have filled out multiple versions of the survey. This risk was mitigated by assigning separate IP addresses and passwords to each partner.
- The supporting partners that distributed the survey are mostly security research and consultancy organizations. As a result the surveyed organizations do not form a completely random group, and there is possibly a bias towards companies that are contacts of security research organizations or consultancies.
- Different understanding of what constitutes “security spending” could also influence the final results.
- The relatively small number of valid responses (51) makes classical statistical modelling and correlations difficult.

4 Future Work

The OWASP Security Spending Benchmarks Project intends to continue to collect benchmark data through our partners. We hope that this project will contribute substantially to the field by providing a collaborative community space for discussing, collecting, and analyzing data on actual information security spending, particularly as it relates to software and Web applications.

We will be reaching out to the community to choose thematic priorities for our next survey to complement and improve on the results contained in this report.

The current status of the project can always be found on the project Web page[1].

1 http://www.owasp.org/index.php/Category:OWASP_Security_Spending_Benchmarks