# OWASP Security Spending Benchmarks Project Report

June 2009

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

Project Partners:



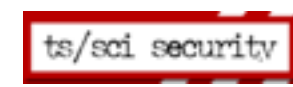


















# Table of Contents

# Executive Summary

The focus of the Q2 OWASP Security Spending Benchmarks Project is on the effect of cloud computing on security resource allocation.

The term cloud computing means different things to different people. The survey defined three different types of cloud computing for respondents - Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service. The survey gathered information on resource allocation for each cloud area, as well as legal, compliance, and contractual issues related to each type of cloud activity.

As in the past, the focus of the OWASP Security Spending Benchmarks Project is on the quality rather than the quantity of respondents. Our 46 responses were obtained through the contacts of our 20 partner organizations.

Below are the key findings of the Q2 study:

- ***Software-as-a-Service is in much greater use than Infrastructure-as-a-Service or Platform-as-a-Service.*** Over half of respondents make moderate or significant use of SaaS. Less than a quarter of all respondents make any use of either IaaS or PaaS.
- ***Security spending does not change significantly as a result of cloud computing***. Respondents did not report significant spending changes in the areas of network security, third party security reviews, security personnel, or identity management.
- ***Organizations are not doing their homework when it comes to cloud security.*** When engaging a cloud partner, only half of organizations inquire about common security-related issues, and only a third require documentation of security measures in place.
- ***The risk of an undetected data breach is the greatest concern with using cloud computing, closely followed by the risk of a public data breach.***
- ***Compliance and standards requirements related to cloud computing are not well understood.*** Respondents report having the greatest understanding of PCI requirements relating to cloud computing and the least understanding of HIPAA cloud requirements.

# 1 Introduction

The OWASP Security Spending Benchmarks Project was launched in late 2008 to address the lack of consensus on the appropriate level of security spending within the development process.

The current Q2 version of this survey focuses on the topic of cloud computing. The survey seeks to measure the extent to which the awareness of, planning for, or use of systems commonly associated with cloud computing has affected, or is expected to affect, spending in both the development and deployment of web applications. It also gathers data on the legal, compliance, and risk aspects companies are considering in their use of cloud computing.

Cloud computing has many definitions and the survey results are undoubtedly influenced by respondents' interpretation of various terms. We have tried to minimize the effect of divergent understandings of the cloud by including definitions within the survey text. We understand the cloud to mean some meaningful use of computing resources that are not directly owned or managed by an organization. We use the SPI terminology - Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) - to differentiate between various types of cloud computing. The definition of these terms was presented to survey respondents and is reproduced in this report.

As usual I would like to thank all of our project partners - OWASP is a volunteer organization and without their efforts this survey would not have been possible. Through the help of our partner network we are able to provide data to help the community of security practitioners in benchmarking security spending. Special thanks go out to Jeremiah Grossman of WhiteHat for his contributions to the project.

Boaz Gelbord
Project Leader
(boaz.gelbord@owasp.org)

# 2 Definitions Relating to Cloud Computing

In this survey we used the terminology of Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service.

- Infrastructure-as-a-Service refers to the renting of raw computing power with no additional services. One example is Amazon EC2.
- Platform-as-a-Service goes one step further and involves the provision of a computing platform where customers can build applications. Google's App Engine is an example of this.
- Software-as-a-Service refers to the provision of a full software application online. Examples include Google Docs and Salesforce's customer management software.

# 3 Survey Results

## Participant Profiles

A total of 46 companies completed the survey questionnaire. The respondents have different roles within their organizations, with the two largest groups being technical security professionals (40%) and executives (30%). A large range of industries are represented with technology being the largest group at 32%. Just over three quarters of respondents are based in North America with the majority of the remainder from Europe. The breakdown by size was similar to the Q1 survey and broke down as follows:

**Figure 1: Number of Employees**

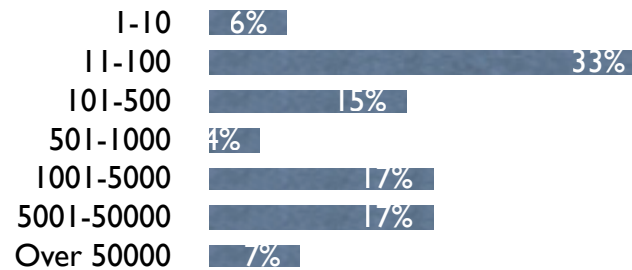
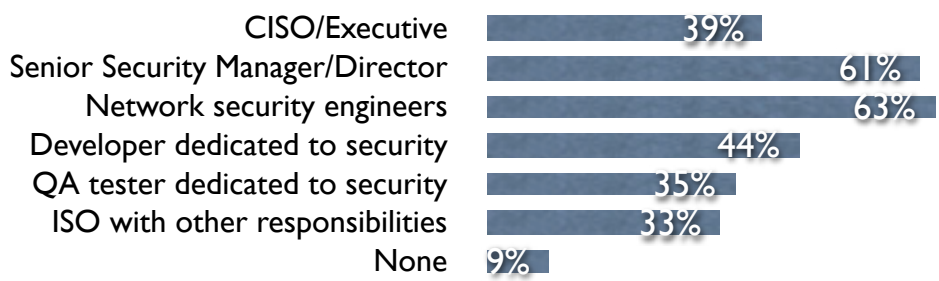


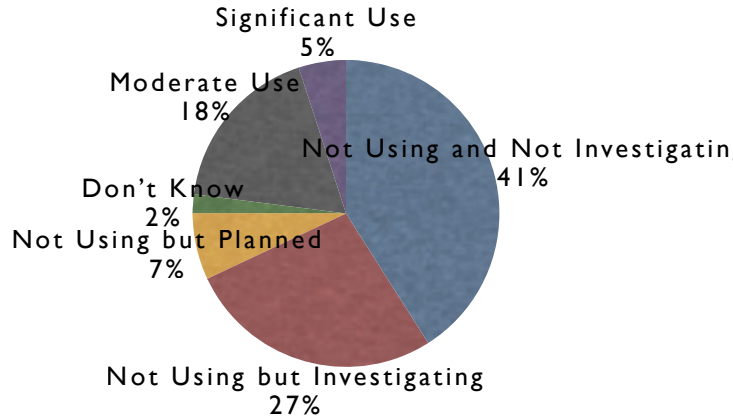

**Figure 2: Security Personnel Employed at Surveyed Organizations**



## Use of Infrastructure-as-a-Service

Only 23% of respondents report making use of IaaS, and over 40% have no plans to use it in the future:

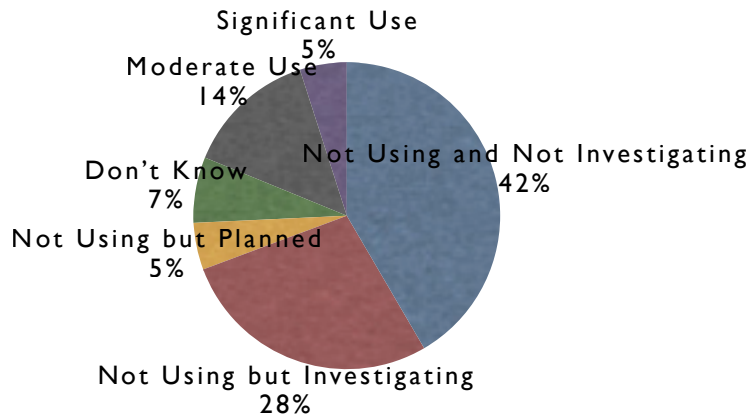
**Figure 3: Use of IaaS (Infrastructure-as-a-Service)**




## Use of Platform-as-a-Service

Platform-as-a-Service is the least used of the three cloud computing methods. Only 19% of respondents report current use of Platform-as-a-Service:

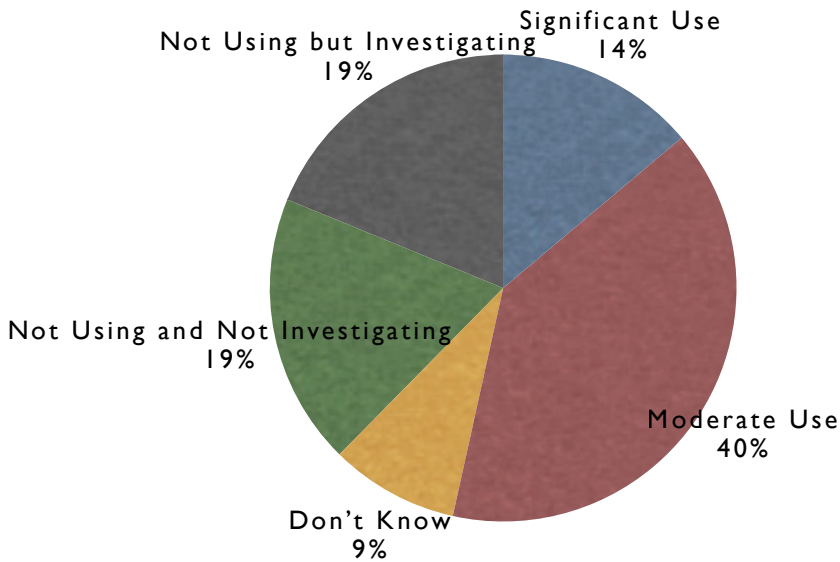
**Figure 4: Use of PaaS (Platform-as-a-Service)**



## Use of Software-as-a-Service

Software-as-a-Service is by far the most prevalent of the cloud computing modes used by respondents of the survey. Over half of respondents report some use of SaaS:

**Figure 5: Use of SaaS (Software-as-a-Service)**



## Spending Changes as a Result of Cloud Computing

Participants were asked what spending changes resulted from their adoption of different cloud models. There are not enough companies currently using either Infrastructure-as-a-Service or Platform-as-a-Service to make a significant statement about spending changes for those cloud components. Below are the spending changes resulting from SaaS:

**Figure 6.1: Spending Changes on Network Security Resulting from SaaS**

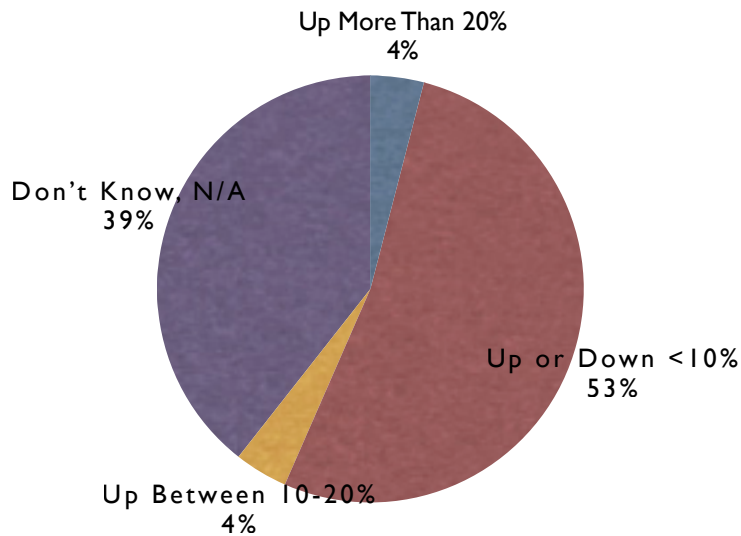



**Figure 6.2: Spending Changes on Third Party Security Reviews Resulting from SaaS**

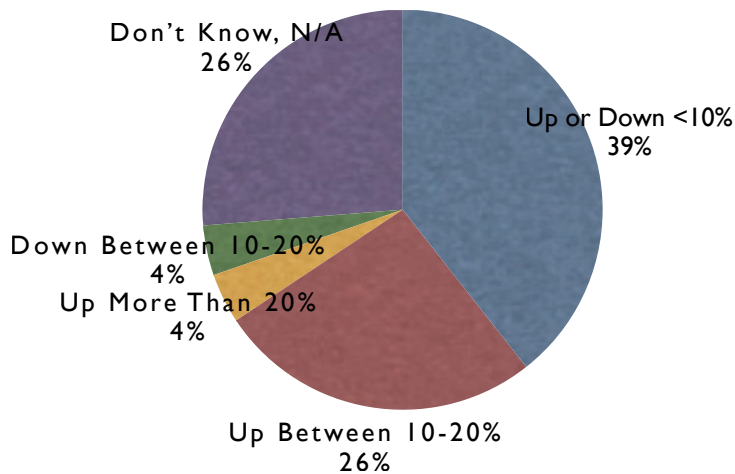


**Figure 6.3: Spending Changes on Security Personnel Resulting from SaaS**

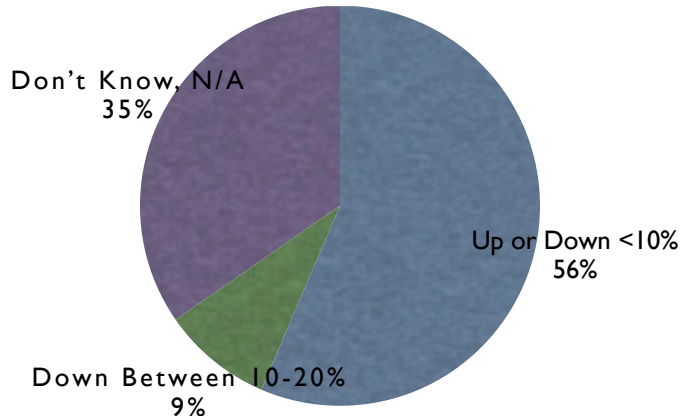
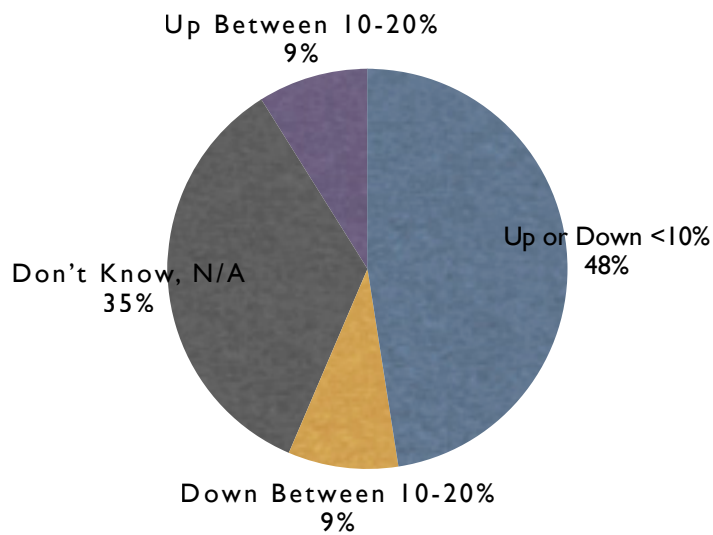



**Figure 6.4: Spending Changes on Identity Management Resulting from SaaS**

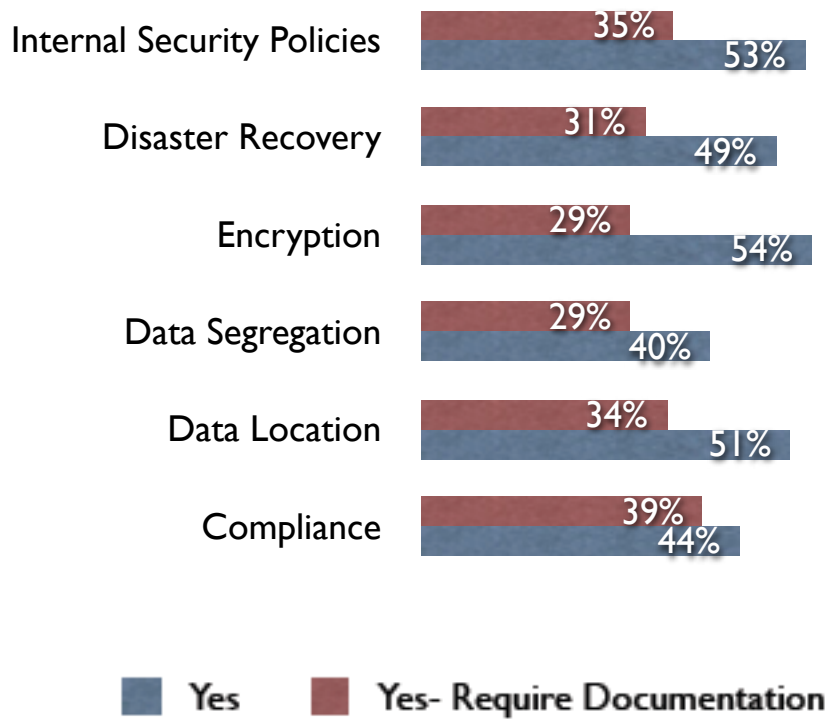


## Legal Arrangements and Vetting Cloud Partners

Just over half of respondents have a security-specific SLA in place with their SaaS, PaaS, or IaaS partner. Most respondents did not know whether security indemnification was in place. On the other hand, a full 60% of respondents have security language in the contract of their cloud (SaaS, PaaS, or IaaS) partner.

Many organizations do not inquire about basic security issues with their cloud partners and even fewer require documentation of security measures in place:

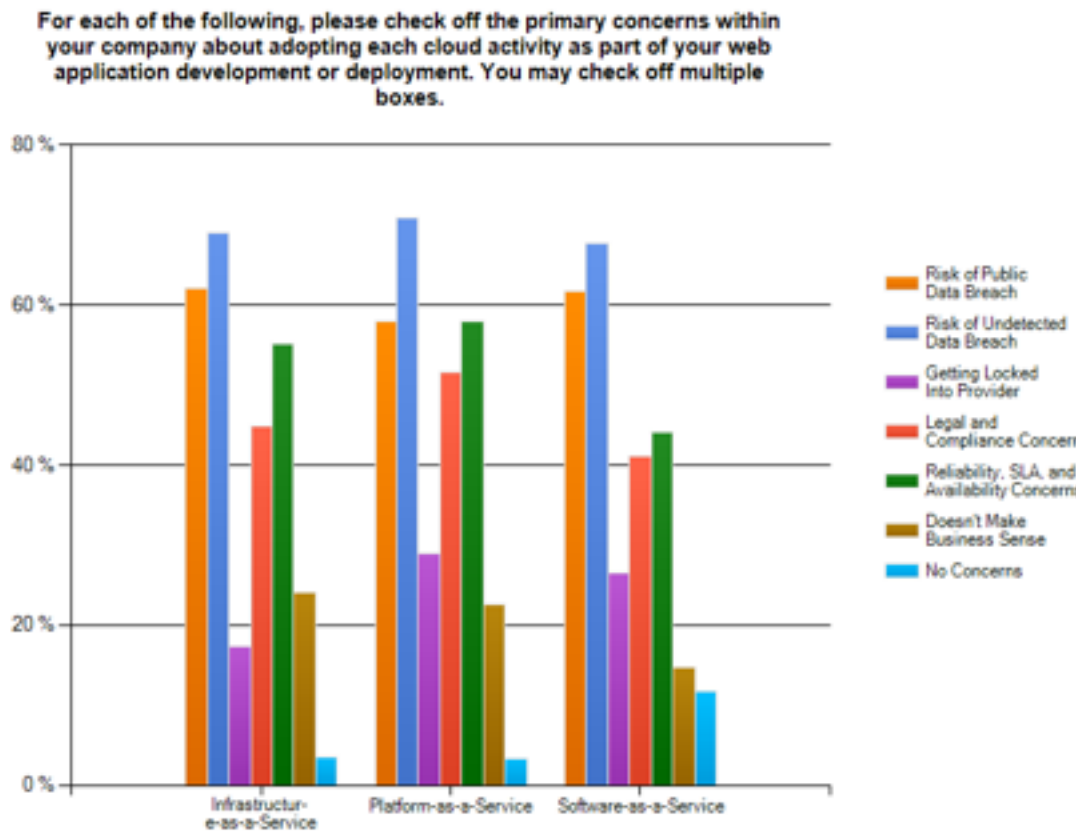
**Figure 7: Inquiries of Third Parties on Cloud Security Issues**



## Concerns with Cloud Computing

The survey measured the level of concern that companies have with various aspects of cloud computing. The most prevalent concern for all three types of cloud computing defined in the survey (IaaS, PaaS, and SaaS) was the risk of an undetected data breach, closely followed by the risk of a public data breach.

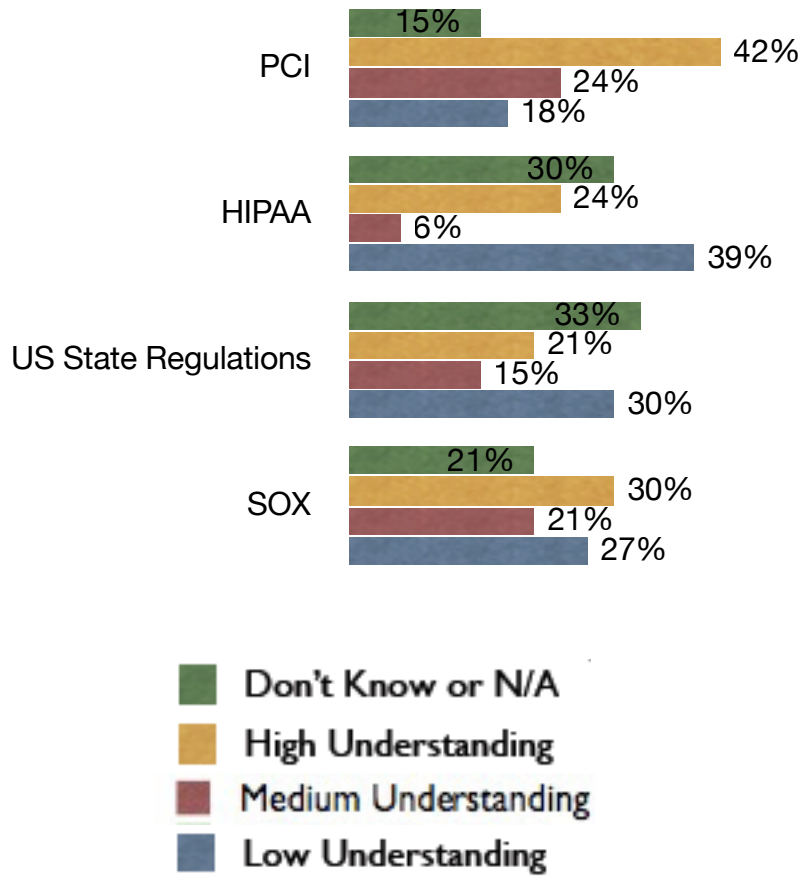
**Figure 8: Concerns with Cloud Computing**



## Compliance and Cloud Computing

The survey measured the level of understanding that companies have of the various compliance and standards requirements relating to cloud computing. Respondents report having the greatest understanding of PCI requirements relating to cloud computing and the least understanding of HIPAA cloud requirements.

**Figure 9: Understanding of Compliance and Standards Issues in Cloud Computing**



# 3 Methodology

The goal of the survey was to measure as accurately as possible the effect of cloud computing use on security spending and related challenges in Web applications. 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 is conducted with the following principles:

- *Transparency of process*. The current status of the project and analysis can always be found on the website.[1]
- *Anonymity*. To allow respondents to candidly describe their spending, no identifiable information including IP addresses is collected.
- *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 a team of high quality partners from amongst leaders in the field and soliciting advice from the community.

## 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" and "cloud computing" could also influence the final results.
- The relatively small number of valid responses (46) makes classical statistical modelling and correlations difficult.

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

# 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].

Questions about the project may be directed to the project leader at boaz.gelbord@owasp.org.

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