OWASP Security Spending Benchmarks Report

OWASP AppSec DC Nov 13th, 2009

Boaz Gelbord
Executive Director of Information Security, Wireless Generation
Project Leader, OWASP Security Spending Benchmarks Project
Personal Ruminations on Info Security: www.boazgelbord.com
A quick straw poll...
A quick straw poll...

Does it cost more to produce a secure product than an insecure product?
A quick straw poll...

Does it cost more to produce a secure product than an insecure product?

The correct answer is YES
One More Question...
One More Question...

Do any of you not shop somewhere/not go to a hospital/not enroll in a university because they have had a data breach?
One More Question...

Do any of you not shop somewhere/not go to a hospital/not enroll in a university because they have had a data breach?

The correct answer is NO (even if you think it is YES)
Hmmm...

So why do we spend on security?

And how much should we be spending?
Security imposes extra costs on organizations.

The “security tax” is relatively well known for network and IT security – 5 to 10% (years of Gartner, Forrester, and other studies).

No comparable data for development or web apps.

Regulations and contracts usually require “reasonable measures”. What does that mean?
OWASP Security Spending Benchmarks Project

- 20 partner organizations, many contributors.
- Open process and participation.
- Raw data available to community.
Reasons For Investing in Security

- Contractual and Regulatory Compliance
- Incident Prevention, Risk Mitigation
- Cost of Entry
- Competitive Advantage

Technical and Procedural Principles

- Managed and Documented Systems
- Business-need access
- Minimization of sensitive data use
- Security in Design and Development
- Auditing and Monitoring
- Defense in Depth

Specific Activities and Projects

- Security Policy and Training
- DLP-Type Systems
- Internal Configurations Management
- Credential Mgmt
- Security in Development
- Locking down internal permissions
- Secure Data Exchange
- Network Security
- App Security Programs
The 10000’ View For Most Organizations

- Legal and Regulatory Compliance
  
  **Because We Have To**

- Incident Prevention, Risk Mitigation
  
  **Because This is What Everyone Else Does**

- Cost of Entry

- Competitive Advantage
  
  **Really?**
Regulations, contracts, and RFPs are usually based on the notion of “reasonable effort” - state regulations, HIPAA, FTC, SEC, Red Flags Rule.

When regulations do get technical, they focus on old school security fetishes like firewalls, SSL, encryption, biometric passes in server rooms.
A Few Examples

- PCI Prioritized Approach
- Massachusetts 201 CMR 17.00
- The encryption exemption in state data breach notification laws
- HIPAA Notification Form
- Recent SEC Action
- Most of the contracts/RFPs/Vendor security whitepapers I have seen...
A Real World Example of Where Your PII Lives...

Small company with a few dozen employees sells widgets over the Internet.

They pay an outsourced team to develop a Joomla/Drupal/whatever site to build a widget-lovers community where users can connect. All sorts of PII involved in the app.

They deploy their site on a shared hosting/VPS model and basically only interact with the App from a web admin interface.

They know a bit about the technical details of their app but not much. Actually, no actual web developers were really involved in the building or deployment of the app.
Here is What Company A Did...

 Asked their developer team in India to develop code securely. Referenced OWASP Top 10 or similar list.

 Told their development team that services and database users needed to run with minimum privilege. Dev team balked. Company A agreed to pay a bit extra.

 Did a bit of reading on best practices for Joomla/Drupal/whatever security and tried to implement as much of this as possible. Maybe even hired someone to lock down their server.

 Configured their servers so admin interfaces are only available from their IP range.
And Here is What Company B Did...

- Installed anti-virus on all employee machines.
- Bought a firewall for the corporate network.
- Maybe even got two-factor tokens for network access.
- Made sure everything is going over SSL everywhere.
- Put a biometric reader on the entrance to the local data center.
- Encrypted all laptops.
One more poll question...
One more poll question...

Which company is more likely to be in compliance with state laws and other regulations?
One more poll question...

Which company is more likely to be in compliance with state laws and other regulations?

The correct answer is Company B
And one final question...
And one final question...

Which company is more likely to suffer a data breach?
And one final question...

Which company is more likely to suffer a data breach?

The correct answer is Company B
So the only think left to finance your app sec program is the “reasonable spend” argument...
As a community we need to get some consensus on what constitutes reasonable spend...
First survey focussed on general web application spending.

Second survey focussed on cloud computing.

Responses currently being gathered for third survey.

Approximately 50 companies profiled in each case.
We do not collect IP addresses

Most of the partners are security vendors

Relatively small respondent base

Meant to stimulate a discussion on security spending benchmarks.
<table>
<thead>
<tr>
<th>Annual Revenue</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 1 million</td>
<td>12%</td>
</tr>
<tr>
<td>1 - 5 million</td>
<td>8%</td>
</tr>
<tr>
<td>5 - 25 million</td>
<td>14%</td>
</tr>
<tr>
<td>25- 100 million</td>
<td>14%</td>
</tr>
<tr>
<td>100 - 500 million</td>
<td>8%</td>
</tr>
<tr>
<td>500 million to 1 billion</td>
<td>8%</td>
</tr>
<tr>
<td>Over 1 billion</td>
<td>28%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>10%</td>
</tr>
</tbody>
</table>
Percentage of Development Headcount Spent On Security

- < 2%: 20%
- 2%-5%: 10%
- 5%-10%: 18%
- 10%-15%: 8%
- > 15%: 2%
- Don't know: 2%
Percentage IT Budget on Web App Security

- 33%
- 24%
- 12%
- 12%
- 9%
- 9%
Security Checkpoints

- Every stage: 29%
- Design phase: 29%
- Testing phase: 35%
- In production: 27%
- Ad hoc: 27%
- Never: 8%
- Don’t know: 10%
Organizational Responsibility For Security Reviews

- Development: 36%
- QA: 21%
- IT security: 67%
- Internal audit: 18%
- Varies: 15%
- Don’t know: 5%
### Personnel

- None: 12%
- ISO with other responsibilities: 34%
- QA tester dedicated to security: 16%
- Developer dedicated to security: 24%
- Network security engineers: 64%
- Senior Security Manager/Director: 60%
- CISO/Executive: 42%
Provide developers with training

Don’t know: 14%
No: 33%
Via internal resources: 47%
Via an external training course: 25%
Budget for training costs

- Don’t Know: 8%
- Varies: 19%
- General Fund: 23%
- IT Security: 46%
- QA: 15%
- Development: 42%
Percentage of Applications Organizations Defend with Web Application Firewalls

- Don't Know: 17%
- None: 37%
- Some: 7%
- About Half: 7%
- Most: 15%
- All or Almost All: 17%
Third Party Security Reviews

Don’t Know: 11%
Never: 17%
When requested by customer: 24%
Periodic Review: 33%
Design phase: 15%
Testing phase: 39%
Before Deployment: 33%
Ways of Reviewing Outsourced Code

- Don’t know: 11%
- N/A: 13%
- 3rd Party Review: 38%
- Internal Security Review: 42%
- Contractual: 38%
- Don’t Review: 9%
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.
Significant Use: 5%
Moderate Use: 18%
Don't Know: 2%
Not Using but Planned: 7%
Not Using but Investigating: 27%
Not Using and Not Investigating: 41%
SaaS – Spending Changes on Network Security

- Don’t Know, N/A: 39%
- Up More Than 20%: 4%
- Up or Down <10%: 53%
- Up Between 10-20%: 4%
- Down Between 10-20%: 4%
- Down More Than 20%: 4%

Legend:
- Yellow: Up More Than 20%
- Blue: Up or Down <10%
- Purple: Up Between 10-20%
- Pink: Down Between 10-20%
- Green: Down More Than 20%
- Orange: Don’t Know, N/A
SaaS Spending Changes - Third Party Security Reviews

- Don’t Know, N/A: 26%
- Up or Down <10%: 39%
- Down Between 10-20%: 4%
- Up Between 10-20%: 26%
- Up More Than 20%: 4%
SaaS Spending Changes - Security Personnel

- Up or Down <10%: 56%
- Down Between 10-20%: 9%
- Don’t Know, N/A: 35%
SaaS Spending Changes - Identity Management

- Up Between 10-20%: 9%
- Don't Know, N/A: 35%
- Down Between 10-20%: 9%
- Up or Down <10%: 48%
Inquire About Issue With Third Party

- Internal Security Policies: 35% Yes, 53% Yes - Require Documentation
- Disaster Recovery: 31% Yes, 49% Yes - Require Documentation
- Encryption: 29% Yes, 54% Yes - Require Documentation
- Data Segregation: 29% Yes, 40% Yes - Require Documentation
- Data Location: 34% Yes, 51% Yes - Require Documentation
- Compliance: 39% Yes, 44% Yes - Require Documentation
Concerns with Cloud Computing

- **Risk of Public Data Breach**: 58% IaaS, 62% PaaS, 62% SaaS
- **Risk of Undetected Data Breach**: 27% IaaS, 29% PaaS, 69% SaaS
- **Getting Locked Into Provider**: 17% IaaS, 17% PaaS, 29% SaaS
- **Legal and Compliance Concerns**: 41% IaaS, 52% PaaS, 52% SaaS
- **Reliability, SLA, and Availability**: 44% IaaS, 58% PaaS, 58% SaaS
- **Doesn’t Make Business Sense**: 15% IaaS, 23% PaaS, 24% SaaS
- **No Concerns**: 3% IaaS, 3% PaaS, 12% SaaS
Level of Understanding Cloud Computing

- PCI: 15% Low, 18% Medium, 24% High, 21% Don't Know or N/A
- HIPAA: 6% Low, 24% Medium, 30% High, 33% Don't Know or N/A
- US State Regulations: 15% Low, 21% Medium, 33% High, 30% Don't Know or N/A
- SOX: 21% Low, 21% Medium, 30% High, 27% Don't Know or N/A
Cloud Summary

- Software-as-a-Service is in much greater use than Infrastructure-as-a-Service or Platform-as-a-Service.

- Security spending does not change significantly as a result of cloud computing.

- Organizations are not doing their homework when it comes to cloud security.

- 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.
Currently collecting responses for the third survey.

Partners assist in promoting survey, analyzing results, and providing strategic input.

Current status of project can always be found on OWASP website.

New partners are always welcome.