Developers and Application Security: Who is Responsible?

SURVEY RESULTS, November 2014
Survey Sponsors
Q5 - In what industry does your business operate?

- Technology / ISV: 41%
- Consulting / SI: 20%
- Financial Services & Insurance: 17%
- Media / Entertainment: 14%
- Public Sector: 10%
- Telecommunications: 10%
- Consumer Goods / Retail: 6%
- Other: 6%
Q1 – What is your role within your current organization?

- DevOps: 30%
- Development: 26%
- Operations: 25%
- Security: 16%
- Other: 3%
Q3 – What is your responsibility level?

- Practitioner: 46%
- Manager: 40%
- Senior Management: 8%
- Executive Management: 6%
Q9 - Percentage of open source software?

- 0% open source: 13%
- 20% open source: 14%
- 40% open source: 15%
- 60% open source: 15%
- 80% open source: 15%
- 100% open source: 5%

What people estimate they are doing:

- 67% >5000 employees
- 50% in FSI
- 41% in Consulting
- 31% in Government
- 27% in Tech
- 44% for Java developers
Q9 - Percentage of open source software?

- 0% open source: 13%
- 20% open source: 40%
- 40% open source: 14%
- 60% open source: 15%
- 80% open source: 5%
- 100% open source: 67% >5000 employees

People estimate they are doing:
- What app scans reveal:
  - 67% >5000 employees
  - 50% in FSI
  - 41% in Consulting
  - 31% in Govt
  - 27% in Tech
  - 44% for Java developers
Q10 - For custom development, what languages are used?

- **Java**: 57%
- **PHP**: 31%
- **.NET**: 30%
- **Ruby**: 25%
- **C/C++**: 21%

83% with > 5000 employees
FSI: 82.5%
Banking/Finance: 88%
Government: 74%
Q11 - Who is the primary driver behind AppSec initiatives?

- 40% say dev (Q14) 76% say dev spends less than 15% time on AppSec
- (Q15) 42% say dev knows its important but does not have time to spend on it
Q11 - Who primarily drives AppSec initiatives? (filtered for developers only)

- Development: 67%
- IT Architecture: 33%
- Security Architecture: 26%
- DevOps: 20%
- Design and Planning: 16%
- Operations: 13%
- Legal: 10%

Observations:
- 67% devs think they are the primary driver;
- (Q15) 26% say security is not their focus,
- 40% say they have no time to spend on it;
- (Q17) 74% state we have no policies or policies are not effectively enforced

84% w/ >5000 employees think it's compliance / risk management
### Q12 – Your role in AppSec? (1=not at all, 10 = highest priority)

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>3.13%</td>
<td>0%</td>
<td>0%</td>
<td>3.13%</td>
<td>6.25%</td>
<td>12.50%</td>
<td>9.38%</td>
<td>28.13%</td>
<td>37.50%</td>
<td>32</td>
</tr>
</tbody>
</table>

**w/ >5000 employees, 75% rank security 8+ priority**

- Q17 – 58% of >5000 employees feel there is no clear security policy or that policy is not effectively enforced.
- Q13 - 74% state adherence to internal security policies is a top concern

**Conclusion:**

"App Sec is important to me but we lack corporate policies so I'll determine my own."

**w/ 101 – 1000 employees, 76% rank security 8+ priority**

- Q17 – 67% employees feel there is no clear security policy or that policy is not effectively enforced.
- Q13 - 74% state adherence to internal security policies is a top concern

**Conclusion:**

"App Sec is important to me but we lack corporate policies so I'll determine my own."

**81% state Adherence to internal security policies is a top concern**

**Conclusion:**

Strong personal sense of responsibility, but little to no policies to enforce security standards; people make up their own standards.
Q13 - Are any of these security concerns?

- **Open Source Security**: 65.03%
  - #2 overall issue but only 31% test it
  - #1 issue for government
Q14 - How much time do developers spend on security?
Q15 - Interest of in-house developers in regard to AppSec

41% in FSI know it's important but don't spend time
42% in tech
Q16 - When does App Dev spend time with security group?

<table>
<thead>
<tr>
<th>Observation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>At the end of the development cycle</td>
<td>42.31%</td>
</tr>
<tr>
<td>During the design phase as a security review</td>
<td>33.97%</td>
</tr>
<tr>
<td>During the development phase</td>
<td>30.13%</td>
</tr>
<tr>
<td>The security team does not work with our developer team</td>
<td>29.49%</td>
</tr>
<tr>
<td>Security checks are embedded throughout the entire process</td>
<td>23.72%</td>
</tr>
</tbody>
</table>

Observations:
23% say security checks happen, but (Q17) Only 12% have automated
End of development cycle - 62% in government (#1 answer), 47% in financial services
Historically, ‘end of development cycle’ is the most expensive option
Q17 - Describe your current app security policies (Overall)

Observations:
67.05% do not have clear, well defined, enforced policies
12.5% have well defined, automated policies

<table>
<thead>
<tr>
<th>Answer Choices</th>
<th>Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>We do not have clear policies in place</td>
<td>35.23%</td>
</tr>
<tr>
<td>We have policies that are not effectively enforced</td>
<td>31.82%</td>
</tr>
<tr>
<td>We have well defined policies that are manually enforced across the software lifecycle</td>
<td>23.86%</td>
</tr>
<tr>
<td>We have well-defined policies that are manually enforced late in the development lifecycle</td>
<td>17.61%</td>
</tr>
<tr>
<td>We have well defined policies that are enforced through automation across the software lifecycle</td>
<td>12.50%</td>
</tr>
<tr>
<td>We have well-defined policies that are enforced through automation late in the development lifecycle</td>
<td>9.66%</td>
</tr>
</tbody>
</table>

Total Respondents: 176
Q17 - Describe your current app security policies (filtered for government)

59% policies not enforced compared to:
- 40% in FSI
- 28% in Tech

24% don’t have policies in place compared to:
- 20% in FSI
- 30% in Tech

- 18% Automated late in Development
- 12% Automated across SW lifecycle
Q17 - Describe your current app security policies (Developers only)

- **42%** Do not have clear policies
- **9%** Automation across lifecycle
- **7%** Automation late in development cycle

**Observations:**
“`I am responsible, but I have:
- No tools
- No policy
- No time`
Q20 - If doing CI, how often is code compiled?

Observations:
If there is continuous integration, the percentage of automated testing increases.
Q23 - Where is security testing automated?

- Post deployment: Highest Cost
- During continuous integration: Lower Cost
- During Q&A: Lower Cost
- During development: High Cost
- During deployment: Lower Cost
- During the design phase: Lower Cost
Q18 - What are you testing?

Observations:
- 80%+ of app composition is open source
- 30% of companies test open source
  - 37% tech
  - 20% in FSI
  - 29% in government
Summary
Get the deck right now, within seconds

Community@Sonatype.com
Survey Sponsors
Developers and Application Security: Who is Responsible?

SURVEY RESULTS, November 2014