PURPOSE
To discover how large, complex organizations manage application security.

WHO
Most respondents were large multinational companies earning >$1 billion USD in annual earnings (n = 28).

THE RESULT
Aggregated insights, industry trends, and best practices that illuminate how large corporations manage application security.
THREE KEY BUSINESS TRENDS

INCREASING SPEED OF BUSINESS

INCREASING SOPHISTICATION OF RISK MANAGEMENT

INCREASING PRESSURE ON COST CONTROL
IMPORTANCE OF APPLICATION SECURITY

- 73% of respondents stated that application security is a high or critical priority within their organization.
- 50% stated it is a critical/always a top priority.
- 15% currently a high priority (e.g., because of an audit deficiency).
- 12% the same priority as other parts of information security (e.g., incident management, network security, etc.).
- 23% not particularly important compared to other areas.

73% of respondents stated that application security is a high or critical priority within their organization.
79% of respondents stated that general risk management was the key driver for their organization’s application security.
HOW BROAD IS YOUR ORGANIZATIONAL SUPPORT FOR APPLICATION SECURITY?

FINANCIAL INSTITUTIONS

1 2 3 4 5

INDEPENDENT SOFTWARE VENDORS

1 2 3 4 5

OIL & GAS

1 2 3 4 5

ALL OTHERS

1 2 3 4 5

1 = NO SUPPORT
5 = SUPPORT ACROSS THE BOARD
SECURITY AWARENESS TRAINING ADOPTION BY DEVELOPERS ACROSS THE ORGANIZATION

(1 = NO TRAINING, 5 = ALL DEVELOPERS ARE TRAINED)

Average Rating by Industry:
- Financial Institutions: 3.5
- Independent Software Vendors: 3.5
- Oil & Gas: 3.3

Average Rating: 3.4
In general, respondents with a higher level of support for AppSec across the organization show a broader adoption rate of security awareness training, although a larger sample size can confirm this.
### Tracking the Effectiveness of an Application Security Program

<table>
<thead>
<tr>
<th>Metric</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Vulnerabilities Found</td>
<td>75%</td>
</tr>
<tr>
<td>Compliance/Adherence to Company Policies/Standards</td>
<td>68%</td>
</tr>
<tr>
<td>Length of Remediation</td>
<td>39%</td>
</tr>
<tr>
<td>Number of Development Teams Using Tools/Tool Adoption</td>
<td>32%</td>
</tr>
<tr>
<td>Completion of Security Requirements</td>
<td>25%</td>
</tr>
<tr>
<td>We Do Not Track the Effectiveness of Our Application Security Program</td>
<td>14%</td>
</tr>
<tr>
<td>Delays to Deadlines Due to Security Fixes</td>
<td>11%</td>
</tr>
<tr>
<td>Money Spent on Patching in Production</td>
<td>7%</td>
</tr>
<tr>
<td>Money Spent on Remediation</td>
<td>4%</td>
</tr>
</tbody>
</table>

75% of respondents stated that the number of vulnerabilities found was a key metric used to track the effectiveness of their application security program.

Only 4% of respondents stated that they used the amount of money spent on remediating vulnerabilities as a key metric to track the effectiveness of their application security program.
RISK REDUCTION

SOFTWARE PROJECT PROGRESS

IDENTIFY CONTROL
IMPLEMENT CONTROL
VALIDATE CONTROL

RISK

SOFTWARE PROJECT PROGRESS
VALIDATE CONTROL

- Number of vulnerabilities found: 75%
- Compliance/adherence to company policies/standards: 68%
- Length of remediation: 39%
- Number of development teams using tools/tool adoption: 32%
- Completion of security requirements: 25%
- We do not track the effectiveness of our application security program: 14%
- Delays to deadlines due to security fixes: 11%
- Money spent on patching in production: 7%
- Money spent on remediation: 4%
46% of Application-level Risks are not covered by SAST & DAST tools.

- 54% of risks are not found.
- 46% of risks are found and remediated.
- 30% of risks found and fixed.
- Average time to remediation: 316 days.
- 24% of risks found but not fixed.
- 70% of risks remain unaddressed.
KEY SECURITY ACTIVITIES PERFORMED

What activities are you doing that are not listed here?
DO YOU PRIMARILY BUILD IN-HOUSE OR BUY THIRD-PARTY SOFTWARE?

- 47% BUILD IN-HOUSE
- 23% BUY & CONFIGURE COTS
- 15% (ROUNGLY) EQUAL MIX OF ALL THREE
- 15% (ROUNGLY) EQUAL MIX OF BUILD IN-HOUSE AND COTS
of respondents stated that they provide detailed application security requirements as part of their contracts with third-party software vendors.

ONLY

19%

of respondents stated that they perform threat modelling or other design-level analysis of third-party software.
A FRAMEWORK FOR APPLICATION SECURITY

STRATEGY
DRIVERS & GOALS
METRICS & GOVERNANCE
ORGANIZATIONAL STRUCTURE

EXECUTION
IN-HOUSE
TRAINING
REQUIREMENTS & DESIGN
TESTING

THIRD PARTY
PROCUREMENT
SECURITY QUESTIONNAIRES
REQUIREMENTS
TESTING

KEY
● RESPONDENTS NEED IMPROVEMENT
● RESPONDENTS ARE AVERAGE
● RESPONDENTS ARE STRONG
KEY TAKEAWAYS

1. Require your vendors to have a higher standard for secure SDLC (e.g. ISO 27034 or vBSIMM or Microsoft's SDL)

2. Data about vulnerabilities is being unaddressed - keep this data in mind, communicate this to emphasize secure SDLC

3. Follow 3 steps for assurance - identify, implement & validate
Application Security at the Speed Of Business

Our goal is to help you build secure software by seamlessly unifying your application security needs through eLearning, Security Requirements and Verification.

= EXPERT PERFORMANCE
Our Secure Software Professional Suites provide business relevant security courses to help your staff champion security and defend your organization’s most valuable software.

SD Elements automates software security requirements based on your project’s technology, business and compliance drivers. SD Elements eliminates security vulnerabilities in the most cost effective way, before scanning begins.

Our advisors understand your unique business requirements and provide services that advise on unique needs while focusing on driving strategic security goals.
For a copy of the full report, please visit: https://www.securitycompass.com/managingapplicationsecurity2017/

Or email us at info@securitycompass.com
Security Compass is a leading application security firm specializing in solving root application security problems for Fortune 500 companies. Our goal is to help clients build secure software by seamlessly unifying their application security needs through advisory services, training products, and security requirement software.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com