# State of Software Security Report, Volume 3
# Report Publish Date: April 19th 2011

## BRIEFING DECK
## (Under Embargo till April 19th)

VERACODE

# SOSS Volume 3 Data Distribution

Application Development by Supplier Type

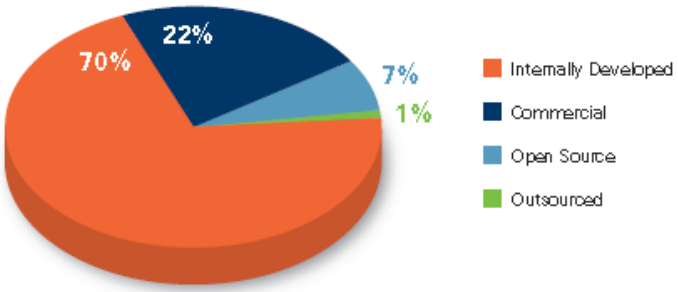



Figure 1: Application Development by Supplier Type

Applications by Language Family

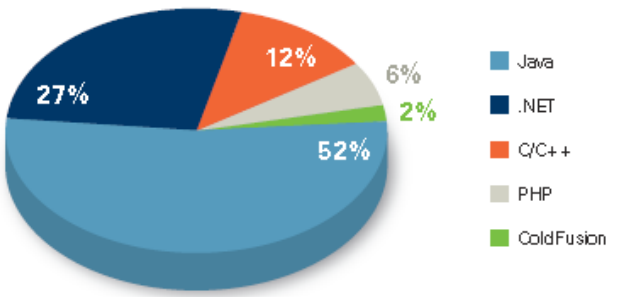



Figure 16: Applications by Language Family

Distribution of Software Sub-segment by Software Purpose

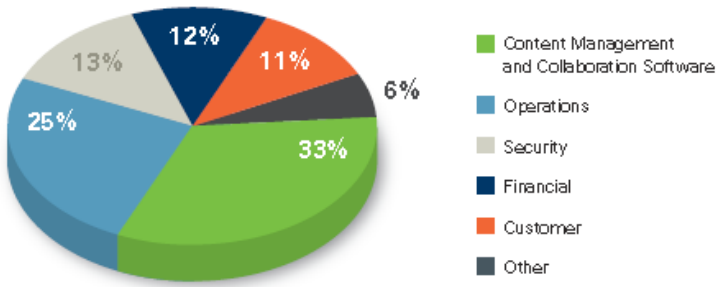



Figure 30: Distribution of Software Sub-segment by Software Purpose

- 4,835 applications (as compared to 2,922 in Volume 2)

# New in Volume 3

- Deep dive on Software Industry
- Study of Remediation Behavior and Time to Acceptable Security Quality
- Developer Education and Training Statistics
- Quarterly Trending information (e.g. for XSS, SQL Injection prevalence)

# Executive Summary Findings

1. When first tested, more than half of all applications fail to meet acceptable security quality, and more than 8 out of 10 web applications fail OWASP Top 10
2. Cross-site scripting prevalence remains constant over time, while SQL injection is trending slightly down
3. Finance and Software industries lead the charge on holding software suppliers accountable; Aerospace and Defense are following suit
4. Most developers are in dire need of additional application security training and knowledge
5. The software industry, including security products and services, have significant gaps in their security posture
6. While static analysis finds orders of magnitude more flaws than dynamic analysis, both techniques are required for comprehensive coverage
7. Building secure software or requiring it from your suppliers does not have to be time consuming

# When first tested, more than half of all applications fail to meet acceptable security quality, and more than 8 out of 10 web applications fail OWASP Top 10

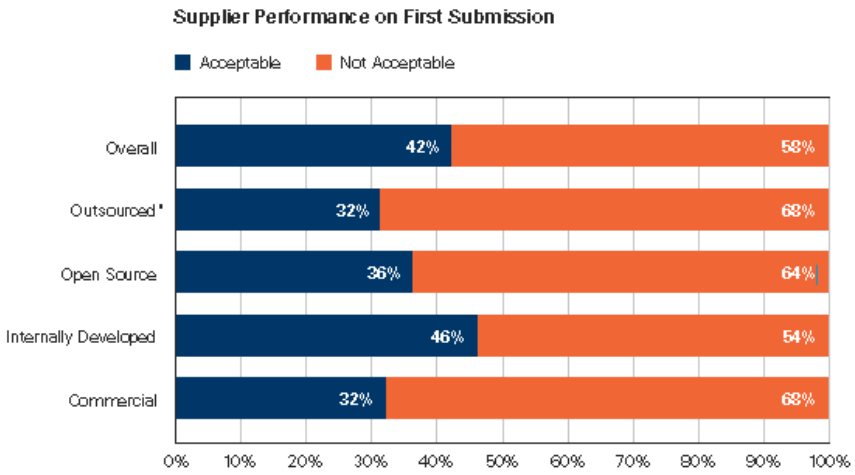



Figure 3: Supplier Performance on First Submission
(*Small sample size)

**58% unacceptable (57% in Volume 2)**

**Commercial acceptability dipped from 35% to 32%**

**More than 8 out of 10 fail OWASP (and likely PCI too!)**

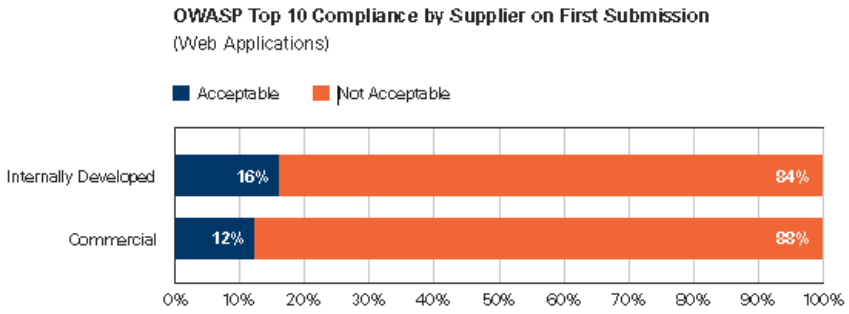



Figure 10: OWASP Top 10 Compliance by Supplier on First Submission (Web Applications)

# Cross-site scripting prevalence remains constant over time, while SQL injection is trending slightly down

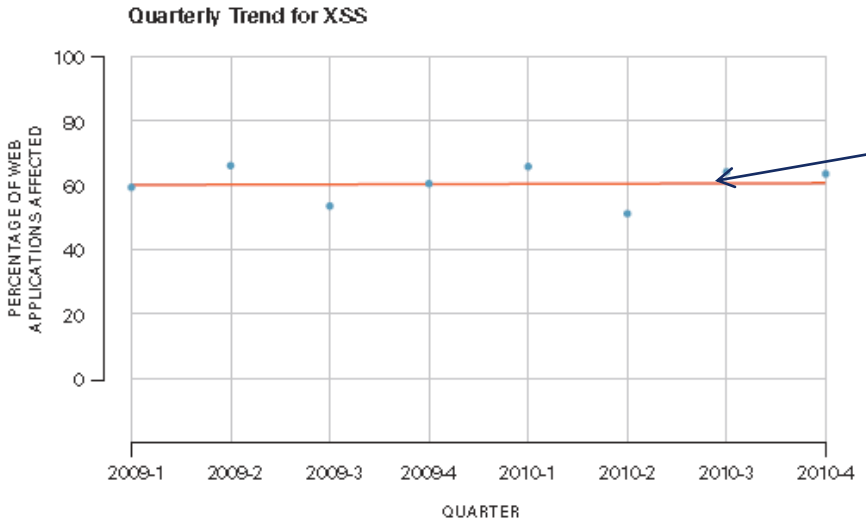



Figure 20: Quarterly Trend for XSS

**XSS prevalence (measured by % of web applications affected) remaining constant since 2009. Discouraging!**

**SQL Injection has gradually decreased by 2.4% per quarter since 2009. Easy to understand & fix. Need faster reduction to outpace the threat environment.**

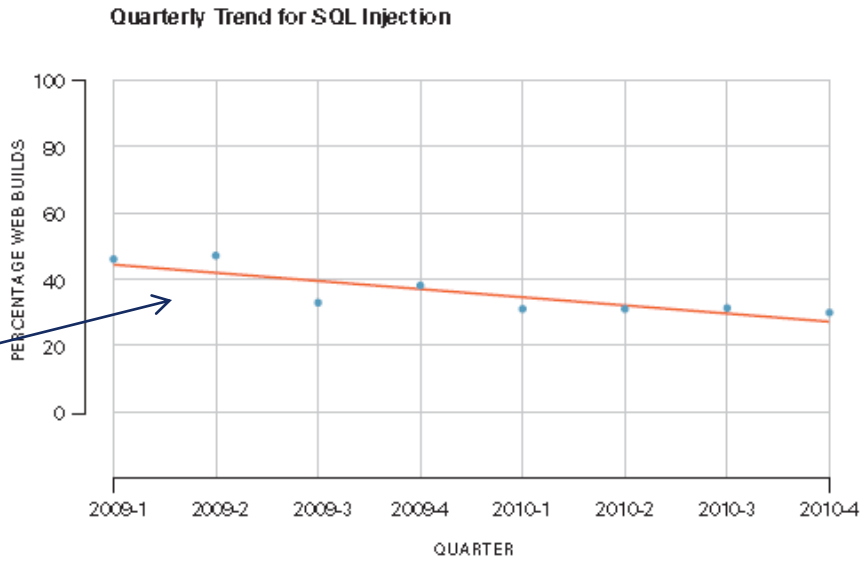



Figure 21: Quarterly Trend for SQL Injection

# Finance and Software industries lead the charge on holding software suppliers accountable; Aerospace and Defense are following suit

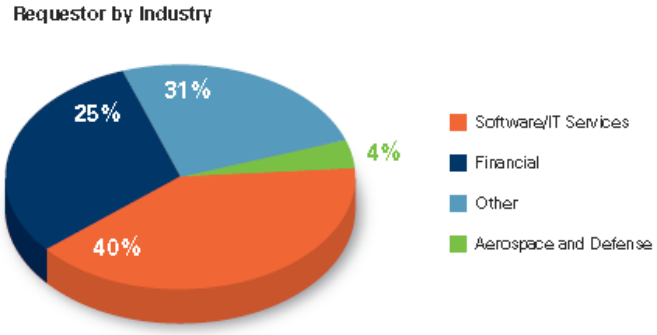



Figure 12: Requestor by Industry

**Finance & Software represent over 75% of enterprises requesting independent verification of third-party software**

**Types of applications being analyzed: Sensitivity of data and processes determining factor in selection**

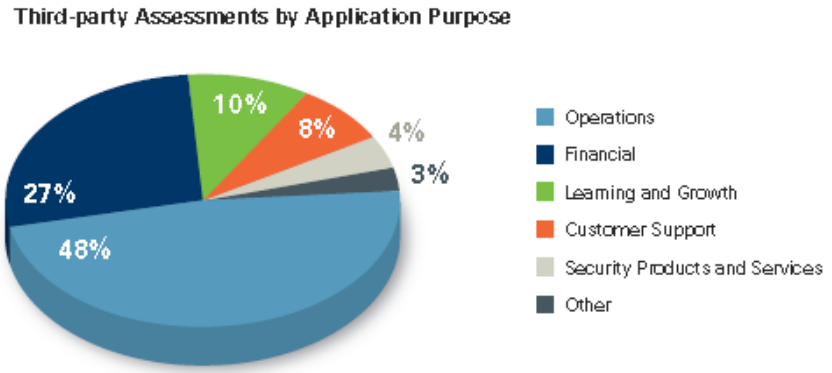



Figure 13: Third-party Assessments by Application Purpose

**Small improvement in acceptability rate of third-party software upon initial submission – 25% acceptable upon initial submission in Volume 3 as compared to 19% in Volume 2.**

# Most developers are in dire need of additional application security training and knowledge

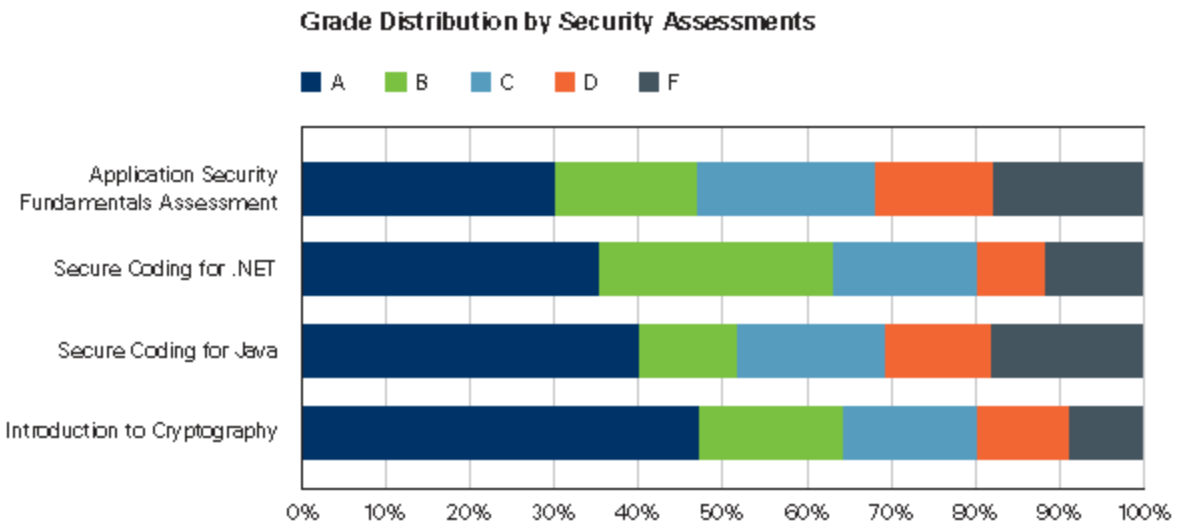
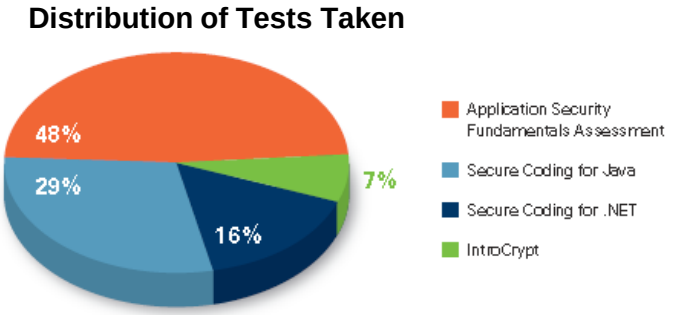



Figure 31: Grade Distribution by Security Assessments

**Over 50% of users taking an application security fundamentals exam got a grade of C or lower. Over 30% got a failing grade of D or F. Much room for additional training!**



# The software industry, including security products and services, have significant gaps in their security posture

**Overall, 66% of software industry applications were found to be of unacceptable security quality upon initial submission (lower than the 58% unacceptable rate when applications from all industries are taken into account).**

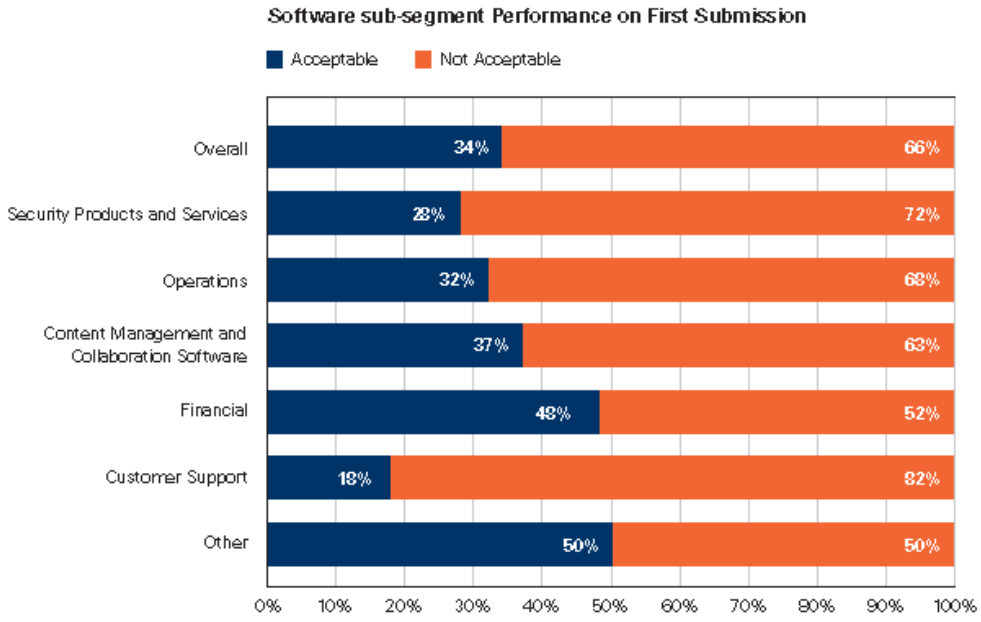



Figure 28: Software sub-segment Performance on First Submission

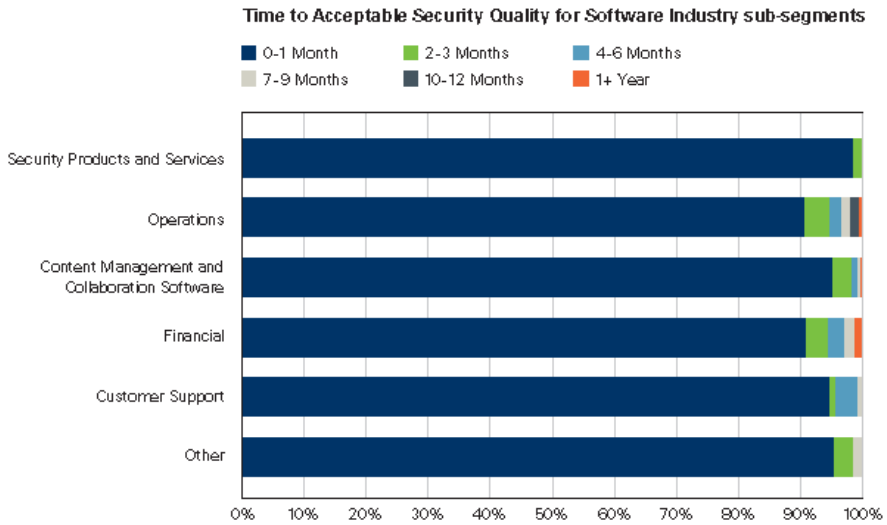



Figure 29: Time to Acceptable Security Quality for Software Industry sub-segments

**Two worst performers within the software industry were the categories of customer support (82% unacceptable) and most surprisingly security products and services (72% unacceptable)!**

**Over 90% of applications across all sub-categories achieved acceptable security quality within 1 month The average for security products and services was an impressive 3 days!**

# The software industry, including security products and services, have significant gaps in their security posture (Continued)

**No discernable difference in security quality score on first submission of applications from public and private software companies. Contrary to expectation!**

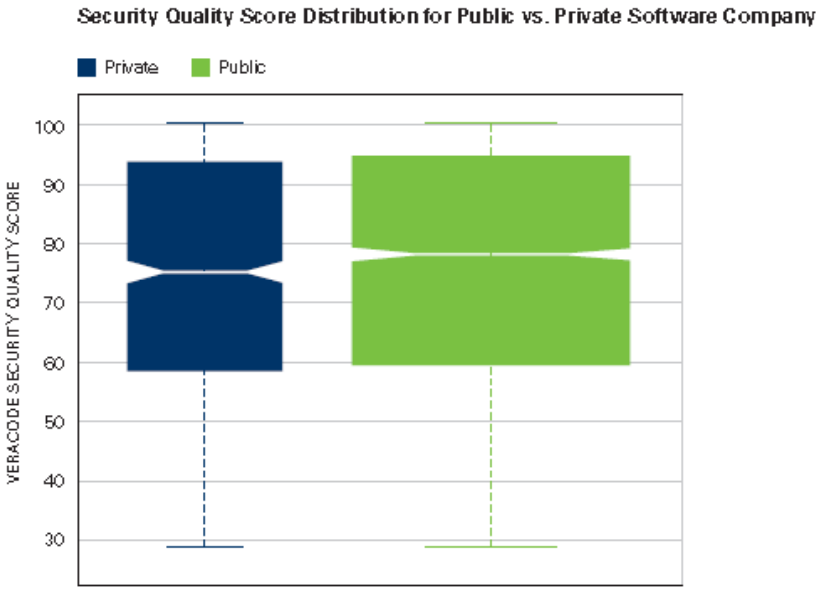



Figure 25: Security Quality Score Distribution for Public vs. Private Software Company

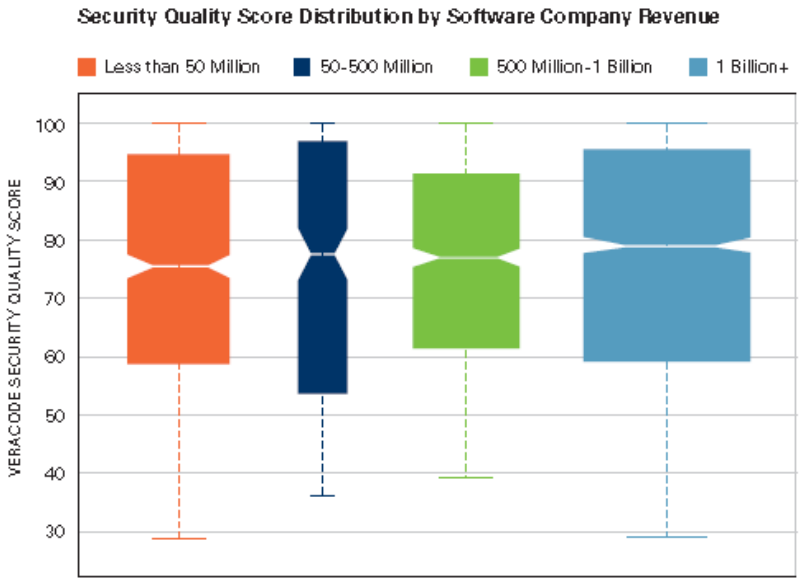



Figure 26: Security Quality Score Distribution by Software Company Revenue

**No discernable difference in security quality score on first submission of applications from software companies in different revenue brackets.**

# While static finds orders of magnitude more flaws than dynamic in important vulnerability categories, both techniques still required for comprehensive coverage

Static vs. Dynamic: Mean Flaws Detected per Application by Vulnerability Category

| Vulnerability | Static | Dynamic |
|---|---|---|
| Cross-site Scripting (XSS) | 354 | 5 |
| CRLF Injection | 133 | 0 |
| Information Leakage | 41 | 20 |
| SQL Injection | 32 | 4 |
| Cryptographic Issues | 18 | <1 |
| Encapsulation | 16 | 0 |
| Directory Traversal | 14 | 0 |
| Insufficient Input Validation | 8 | 0 |
| Race Conditions | 5 | 0 |
| Potential Backdoor | 4 | 0 |
| Time and State | 4 | 0 |
| Credentials Management | 3 | 0 |
| API Abuse | 2 | 0 |
| OS Command Injection | 1 | <1 |
| Error Handling | <1 | 0 |

Table 5: Static vs. Dynamic: Mean Flaws Detected per Application by Vulnerability Category

**Static analysis found 22 times as many flaws as dynamic analysis overall (8 times as many for SQL Injection but only twice as many for information leakage)**

**Both techniques are required for comprehensive coverage!**

# Building secure software or requiring it from your suppliers does not have to be time consuming

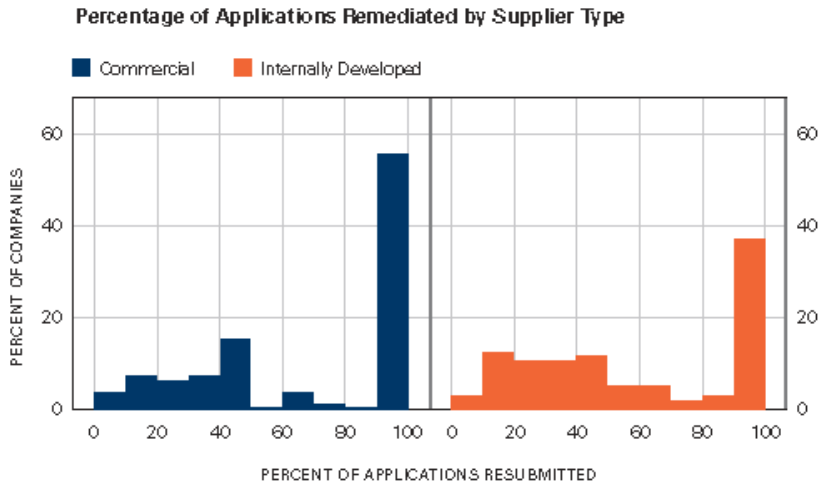



Figure 4: Percentage of Applications Remediated by Supplier Type

**Over 50% of commercial suppliers resubmitted 90-100% of their applications and slightly under 40% of companies developing applications internally resubmitted 90-100% of their applications.**

**Resubmission rates indicate moderate remediation activities across supplier types and industry verticals.**

**More than 80% of applications across all supplier types achieved acceptable security quality within 1 month.**

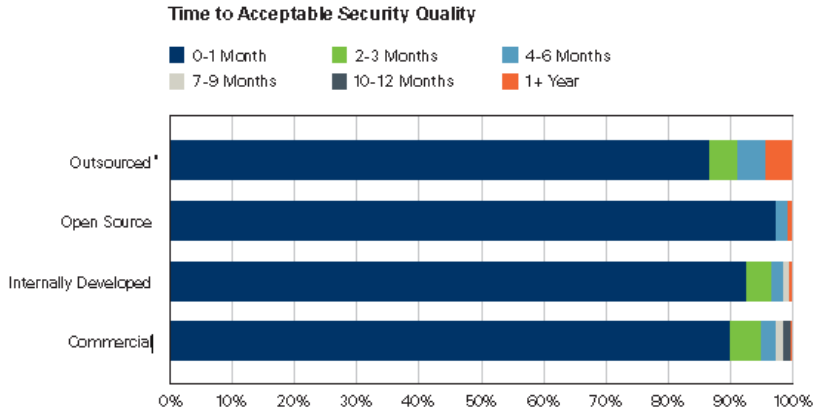



Figure 9: Time to Acceptable Security Quality

**Data indicates that once security and development professionals are made aware of security weaknesses in their applications they are quick to take action.**

# Thank You

Questions?

VERACODE