

Intelligence on the Intractable Problem of Insecure Software

The Security Scoreboard In The Sky

OWASP Ireland Conference
September 17, 2010

VERACODE

GUINNESS[®]

Proud Sponsor of Irish Rugby

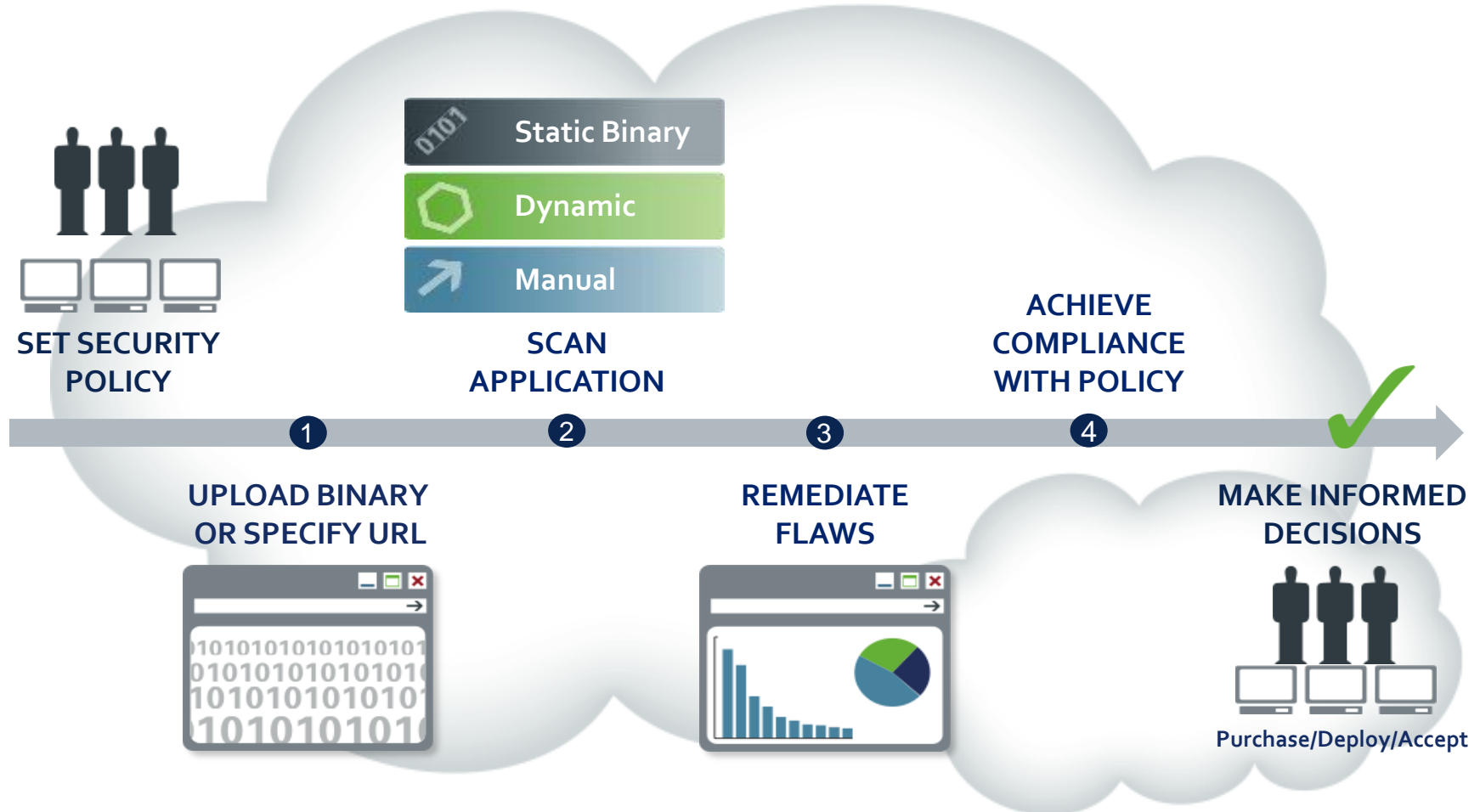
Ireland 43

England 13

Bio

- Tyler Shields
 - Senior Security Researcher at Veracode
 - Responsible for researching and incorporating security intelligence into Veracode's offerings
- Previously
 - Security Consultant Symantec (through acquisition)
 - Security Consultant at @stake
 - Incident Response and Forensics Handler U.S. Government
- Industry Involvement
 - Frequent speaker at security conferences
 - Author of numerous security advisories and open source tools
 - Creator of txsBBSpy - Blackberry Mobile Spyware

Application Risk Management Services Platform: Automating Security Acceptance Testing



Data Set and Available Metrics

Application Data

- Industry vertical
- Application supplier (internal, purchased, outsourced, open source)
- Application type
- Assurance level
- Language
- Platform

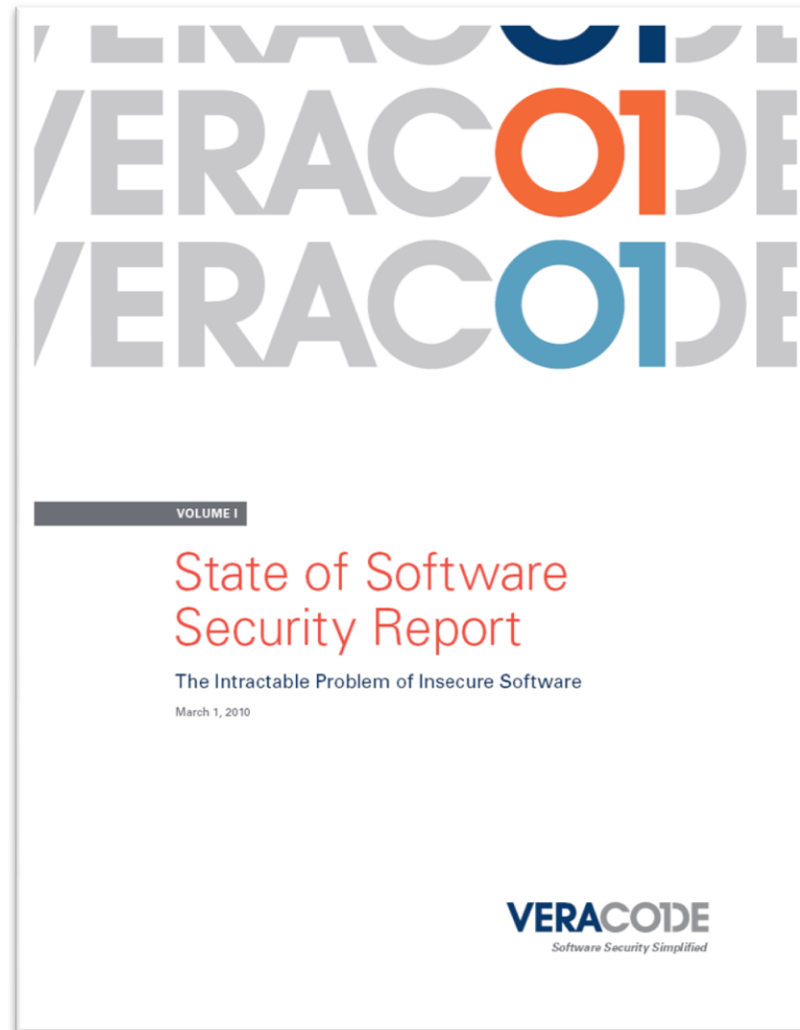
Scan Data

- Scan number
- Scan date
- Lines of code

Enterprise Metrics

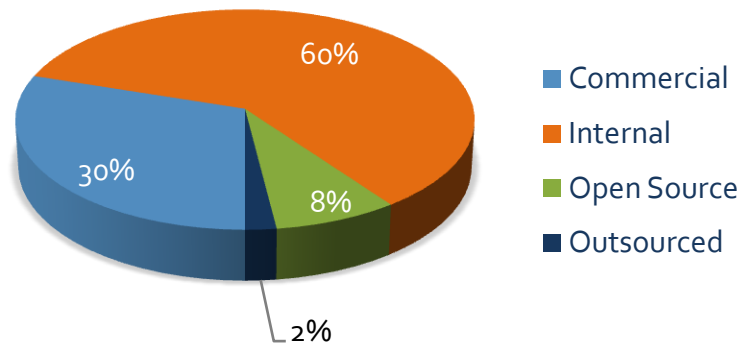
- Flaw counts
- Flaw percentages
- Application count
- Risk-adjusted rating
- First scan acceptance rate
- Mean time between scans
- Days to remediation
- Scans to remediation
- PCI-DSS (pass/fail)
- CWE/SANS Top25 (pass/fail)
- OWASP Top Ten (pass/fail)

State of Software Security, Volume 1

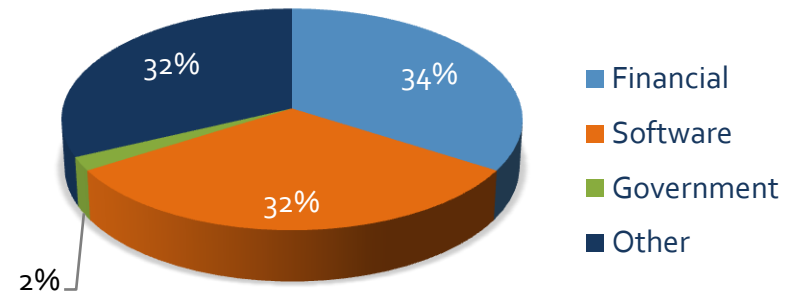


Sample Distribution

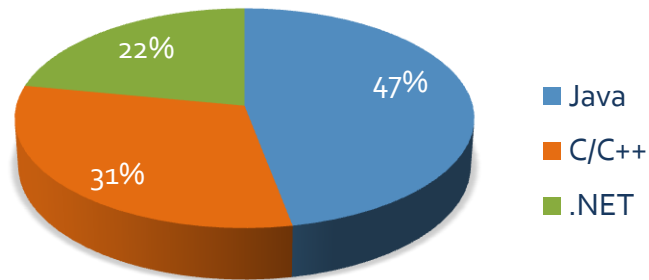
Applications by Supplier



Applications by Industry



Applications by Language



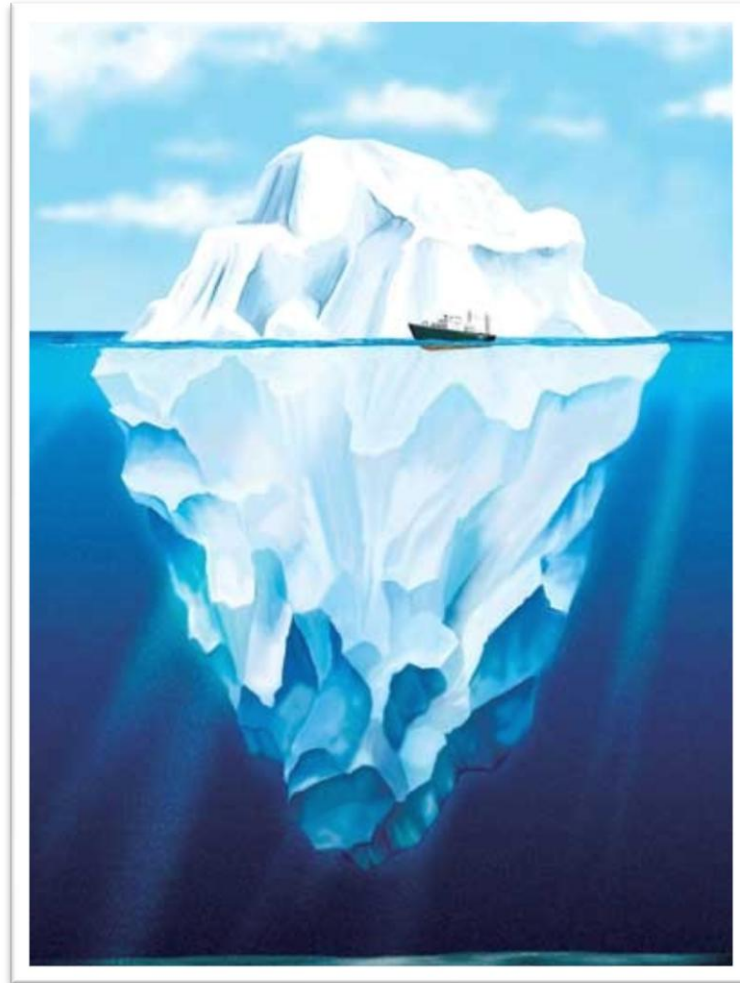
Statistically Significant Sample Size

- Sample size this large enable us to report findings with a reasonable degree of confidence:
- Type I Error
 - Probability of stating that something is FALSE when it is in fact TRUE: < 5%
- Type II Error
 - Probability of stating that something is TRUE when it is in fact FALSE: < 20%
- Margins of error for estimates of various metrics:
 - Flaw count: 10%
 - First scan acceptance rate: 15%
 - Veracode risk-adjusted rating: 10%
 - Remediation time: 10%

State of Software Security, Vol. 1: Observations

1. Most software is indeed very insecure
2. Third-party software is a significant percentage of the enterprise software infrastructure, and third-party components are a significant percentage of most applications
3. Open source projects have comparable security, faster remediation times, and fewer Potential Backdoors than Commercial or Outsourced software
4. A significant amount of Commercial and Open Source software is written in C/C++ making it disproportionately susceptible to vulnerabilities that allow attackers to gain control of systems
5. The pervasiveness of easily remedied vulnerabilities indicates a lack of developer education on secure coding
6. Software of all types from Finance and Government sectors was relatively more secure on first submission to Veracode for testing
7. Outsourced software is assessed the least, suggesting the absence of contractual security acceptance criteria

Most Software is Insecure



42%

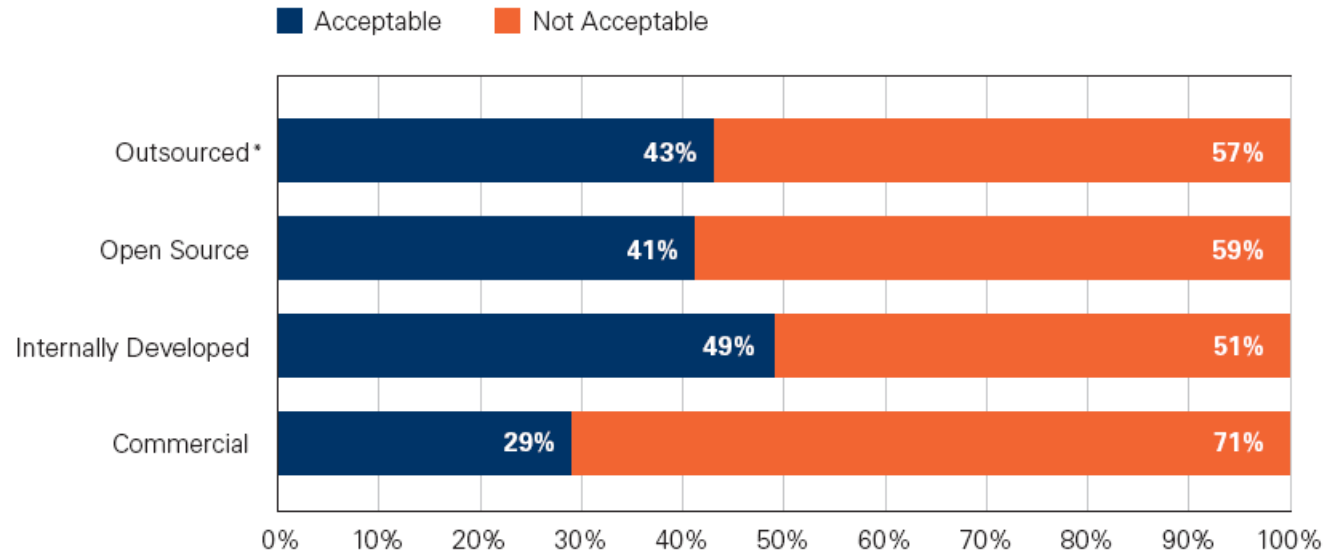
58%

Veracode Risk-Adjusted Ratings

Assurance Level	Rating Based on Analysis Score
VERY HIGH (AL ₅)	90-100 (no VH, H, M) A
	80-89 (no VH, H) B
	70-79 (no VH) C
	60-69 D
HIGH (AL ₄)	80-100 (no VH, H) A
	70-79 (no VH) B
	60-69 C
	50-59 D
MEDIUM (AL ₃)	70-100 (no VH) A
	60-69 B
	50-59 C
	40-49 D
LOW (AL ₂)	60-100 A
	50-59 B
	40-49 C
	30-39 D

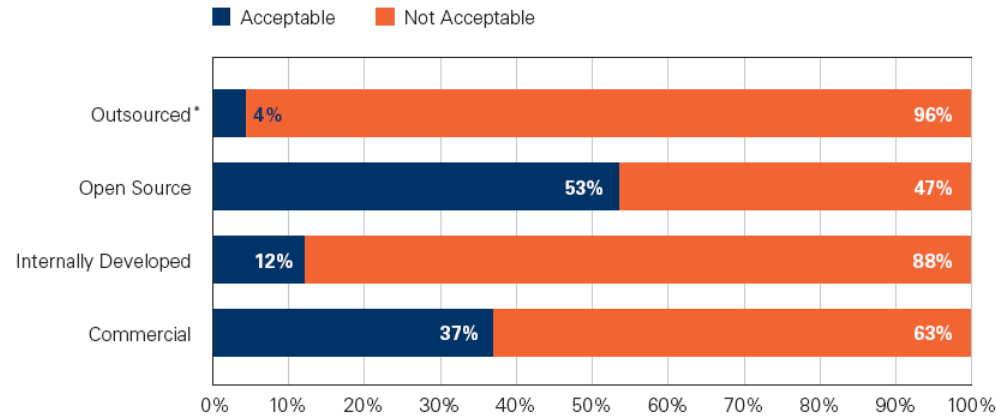
Most Software is Insecure

**Supplier Performance on First Submission
(Adjusted for Business Criticality)**

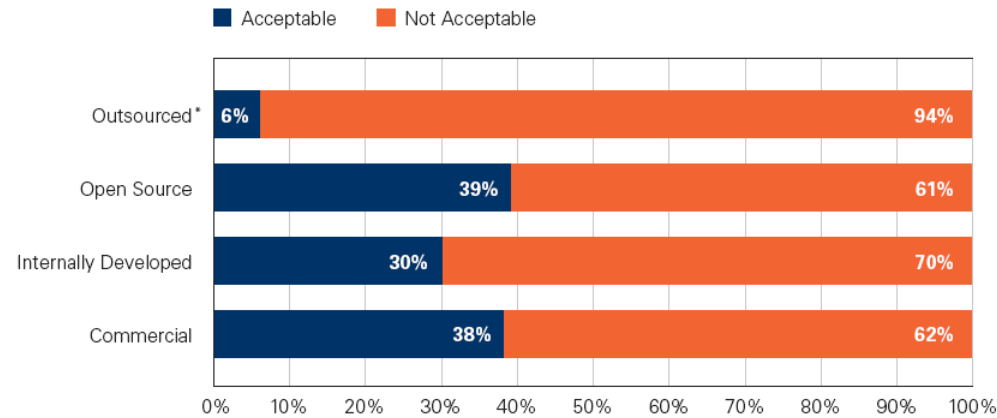


Most Software is Insecure

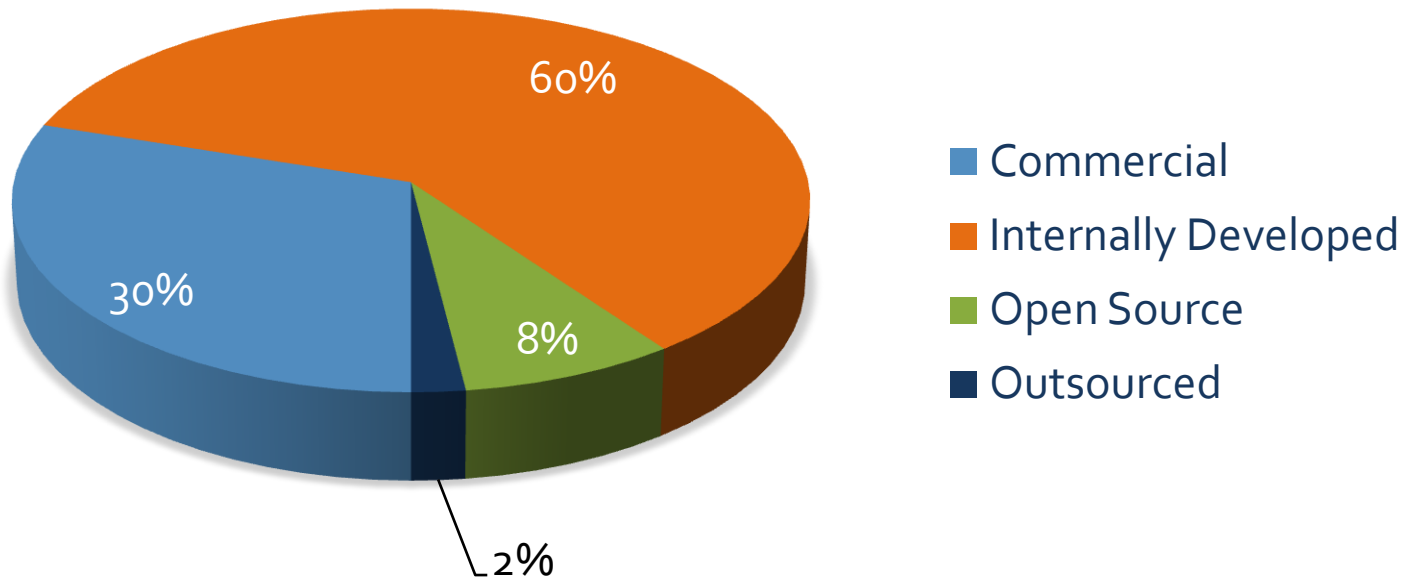
OWASP Top 10 Compliance by Supplier on First Submission (2007 List)



CWE/SANS Top 25 Compliance by Supplier on First Submission (2009 List)

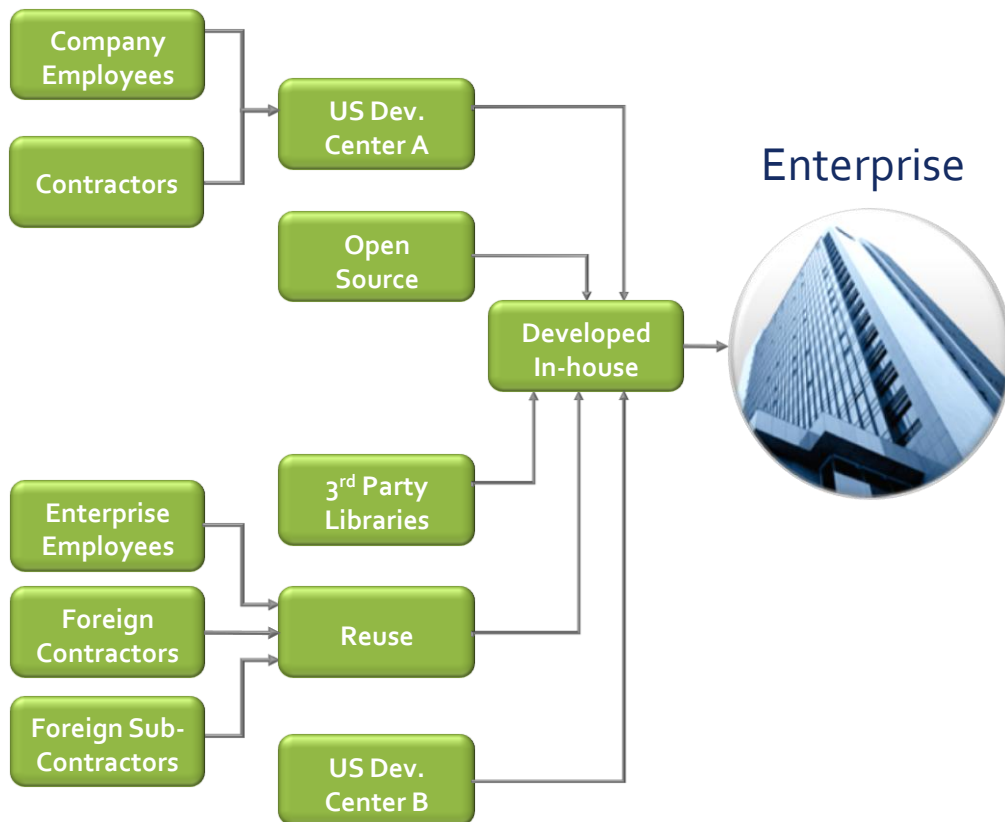


Third-Party Software Cannot Be Ignored

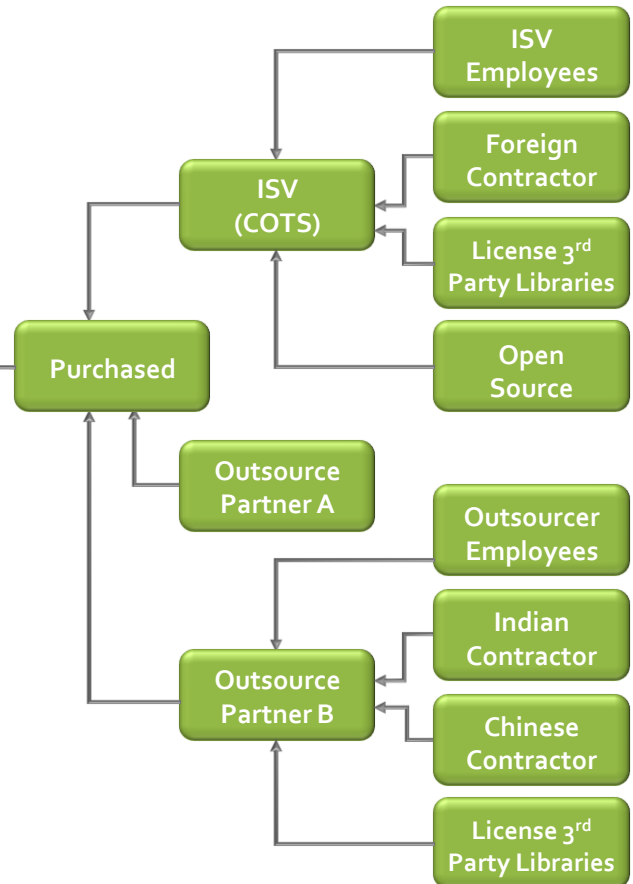


Third-Party Software Cannot Be Ignored

Development Process

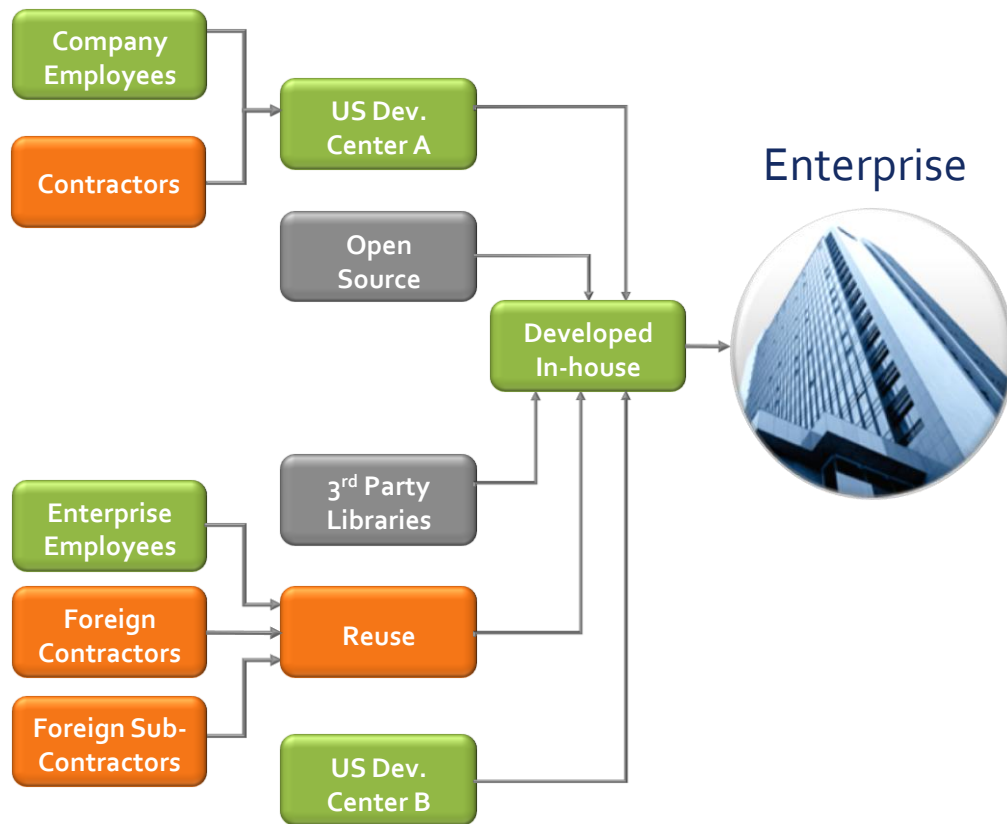


Procurement Process

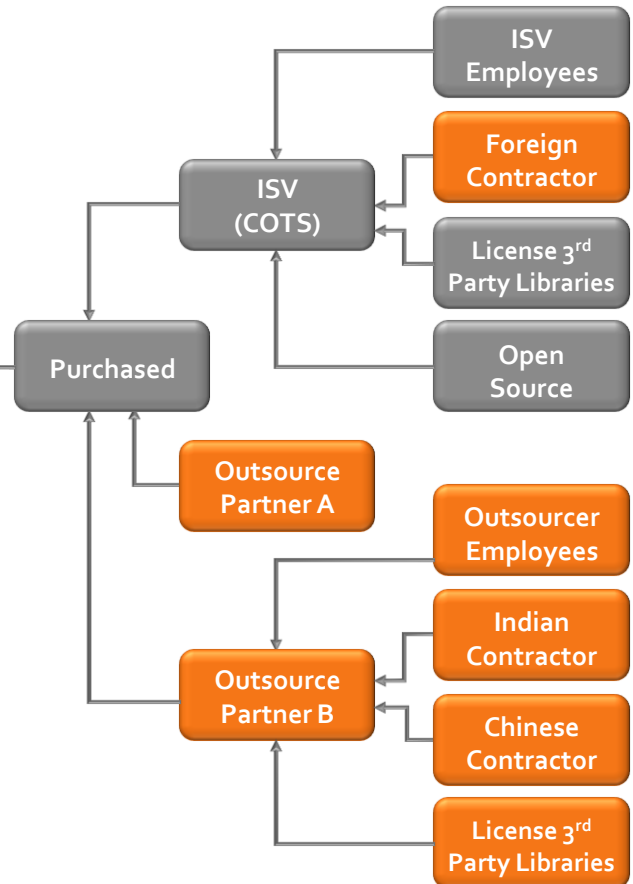


Third-Party Software Cannot Be Ignored

Development Process

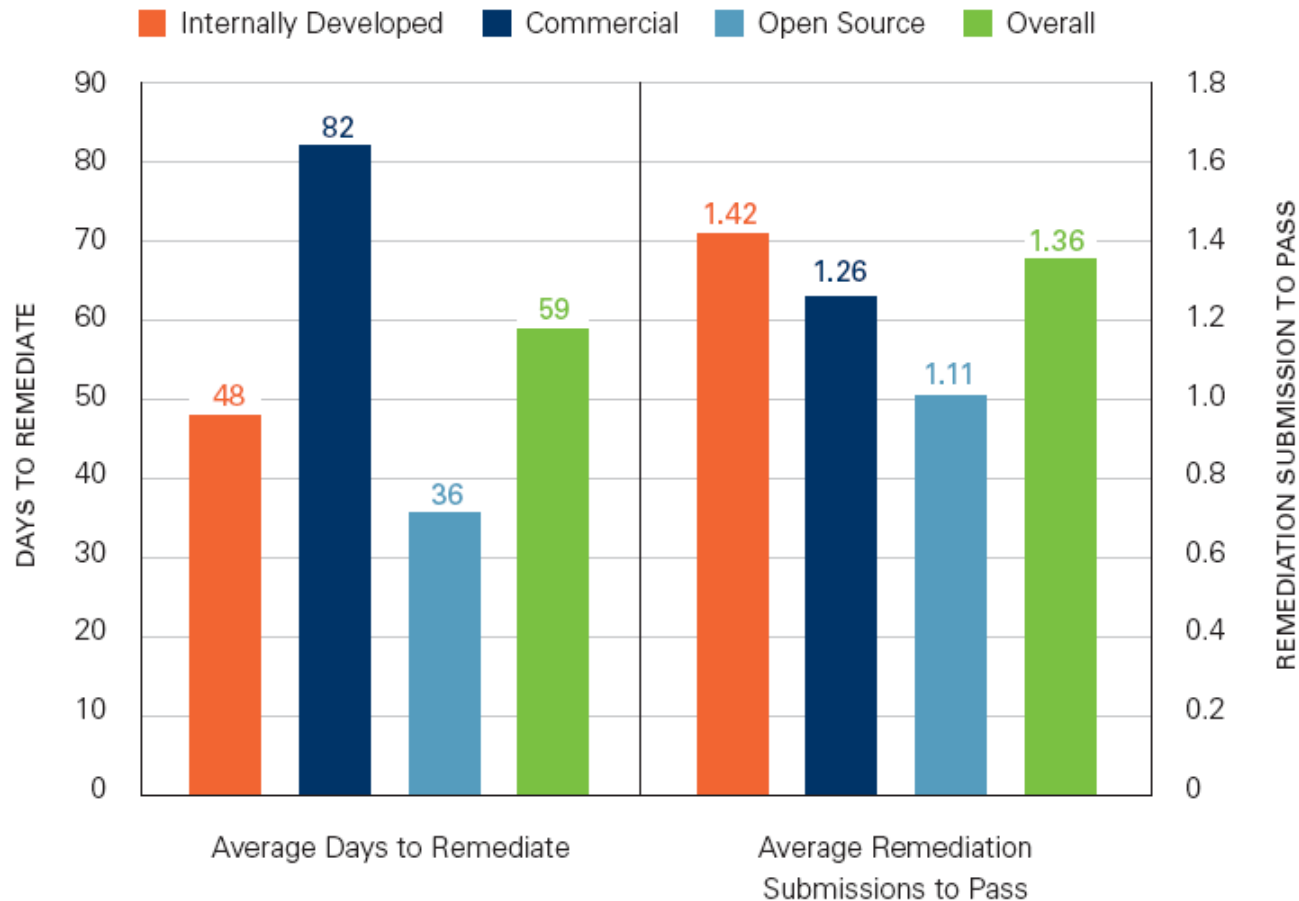


Procurement Process



ISVs Slowest to Remediate; Open Source Fastest

Remediation Performance by Supplier



C/C++ Less Prevalent in Enterprises

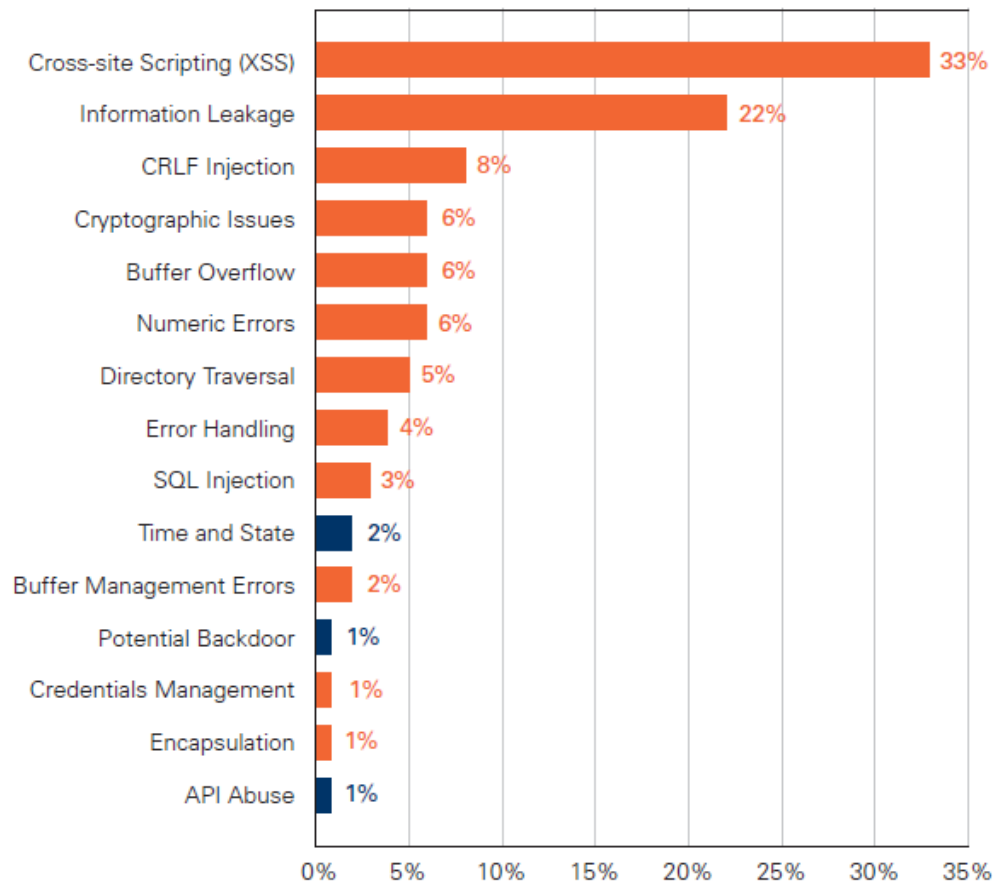
Supplier Application Profiles

	C/C++	Java	.NET
Internally Developed	22%	53%	25%
Commercial	44%	35%	21%
Open Source	45%	54%	1%
Outsourced* (Low sample size)	0%	67%	33%

Easily Remedied Vulnerabilities Remain Pervasive

Top Vulnerability Categories (Overall Prevalence)

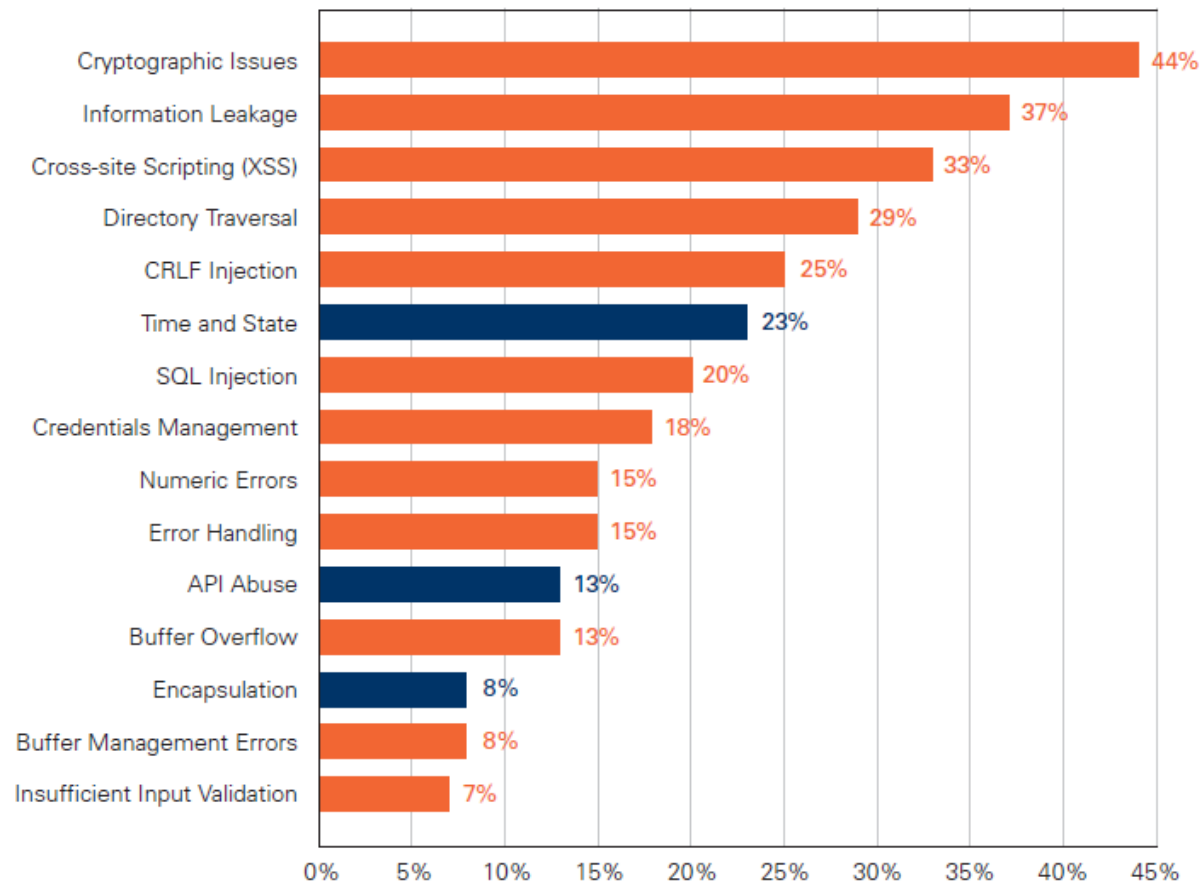
■ Indicate categories that are in the OWASP Top 10 or CWE/SANS Top 25



Easily Remedied Vulnerabilities Remain Pervasive

Top Vulnerability Categories (Percent of Application Affected)

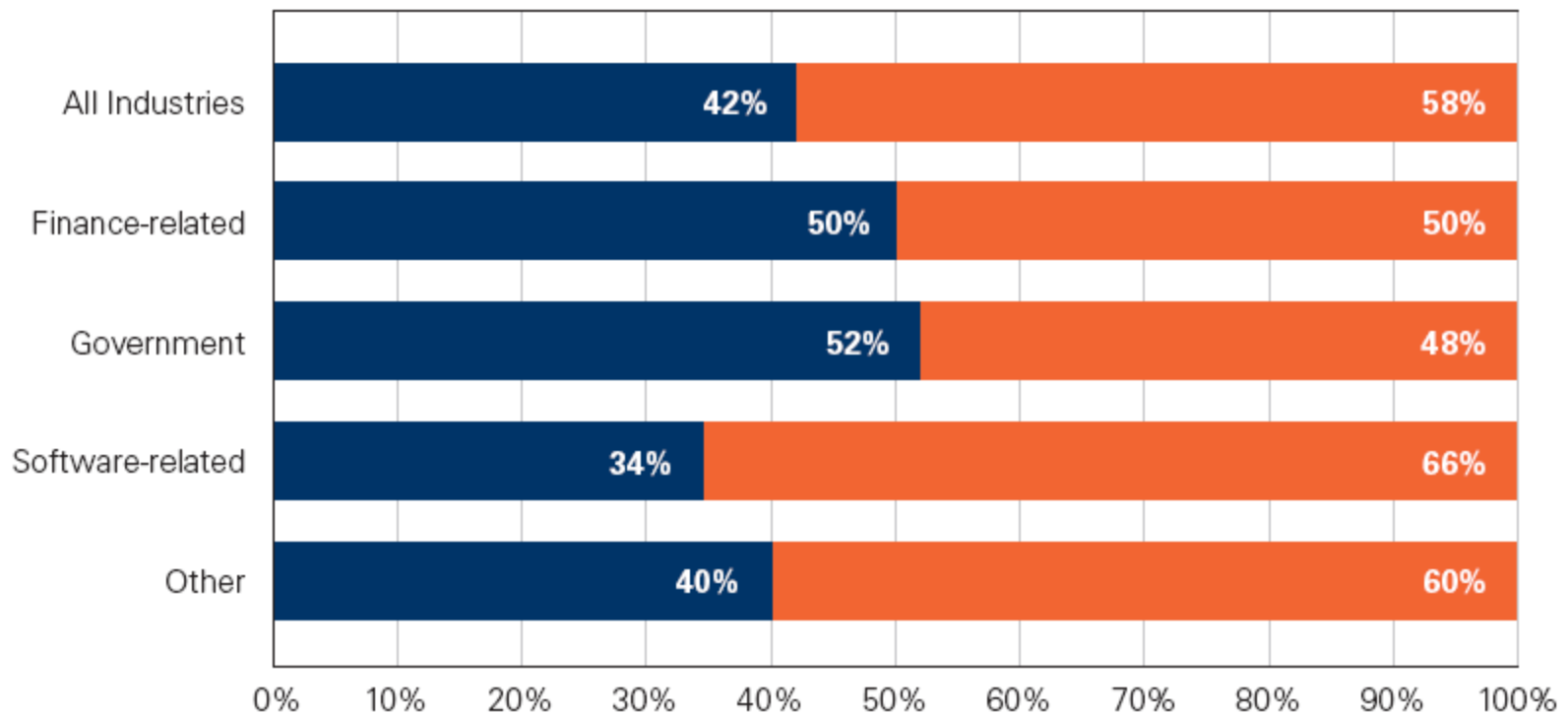
■ Indicate categories that are in the OWASP Top 10 or CWE/SANS Top 25



Finance and Government are Better

**Application Performance by Industry on First Submission
(Adjusted for Business Criticality)**

■ Acceptable ■ Not Acceptable



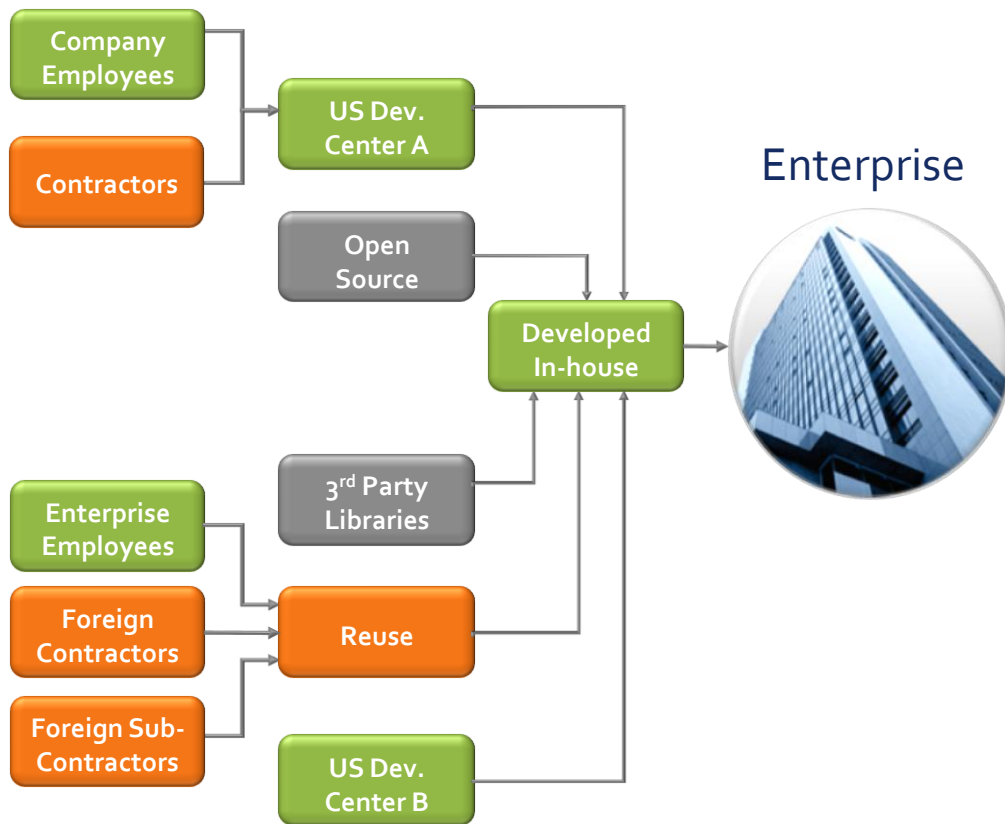
Finance and Government are Better?!

Vulnerability Distribution by Industry

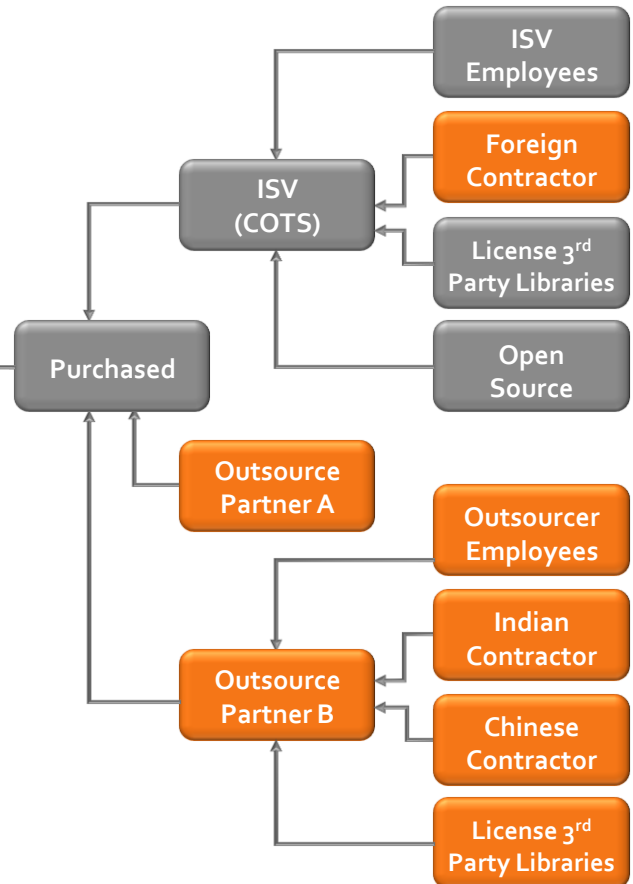
Finance-related		Software-related		Government	
Cross-site Scripting (XSS)	35%	Cross-site Scripting (XSS)	19%	Cross-site Scripting (XSS)	53%
Information Leakage	21%	Information Leakage	17%	Information Leakage	12%
CRLF Injection	5%	Numeric Errors	11%	CRLF Injection	6%
Cryptographic Issues	5%	Buffer Overflow	8%	Buffer Mgmt Errors	4%
Directory Traversal	3%	Cryptographic Issues	6%	SQL Injection	3%

Outsourced Software is Assessed the Least

Development Process



Procurement Process



State of Software Security, Vol. 2: Observations

1. ...
2. ...
3. Third-party applications found to have lowest security quality.
4. ...
5. Suppliers of Cloud/Web applications were the most requested third-party assessments.
6. No single method of application security testing is adequate by itself.
7. ...

New In Volume 2

- Deep dive on Financial Sector to explore differences between Banks, Insurance and Financial Services
- Study on multiple testing techniques (static, dynamic, manual)
- Language Flaw density across C/C++, .NET, Java and ColdFusion
- Investigation of Third-party risk assessments market (buyers, sellers, performance etc.)

More Resources

- Download the report, plus other whitepapers, webcasts, and educational resources
 - <http://veracode.com/resources>

- Veracode ZeroDay Labs Blog
 - <http://veracode.com/blog>

- Contact info
 - Email: tshields@veracode.com
 - Twitter: @txs
 - Phone: (USA) 304.YO.TYLER