


Application Risk Management Survey Summary Report

In June of 2017, 397 developers completed an Application Risk Management survey. The respondents represented 55+ industries and 100+ countries. The survey gathered information about their development organizations' risk management priorities and mitigation strategies.

How to use this report

Development organizations can use the survey results to benchmark their own practices by industry, application type, development organization size, etc.

The summary information presented here identifies application, organizational, and industry-specific considerations that can – *and should* – be considered by every development organization serious about sustaining an effective application risk management program.

 **For organizations interested in comparing their own specific practices against the full data set,** please contact solutions@preemptive.com. You will be provided with a link to an online questionnaire and a benchmark analysis will be delivered to your attention following the completion of the questionnaire.

Key survey results

Risk Profiles

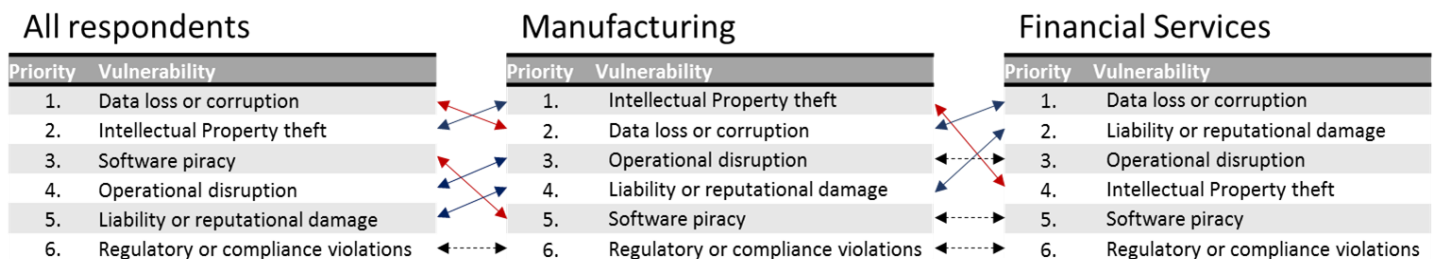
1. PROFESSIONAL APPLICATION DEVELOPMENT ORGANIZATIONS GENERALLY AGREE ON THE “SHORT LIST” OF COMMON APPLICATION DEVELOPMENT VULNERABILITIES.

The top 6 application development vulnerabilities

Application Development Vulnerabilities
Data loss or corruption
Intellectual Property theft
Liability or reputational damage
Operational disruption
Regulatory or compliance violations
Software piracy

2. ...BUT DIVERGE QUICKLY ON THEIR RELEVANCE, PRIORITIZATION, AND MITIGATION STRATEGIES.

The top 6 application development vulnerabilities prioritized by materiality (severity & relevance)



Vulnerability priority ranking compared across all developers, manufacturing, and financial services



Manufacturers rank IP theft as a greater threat than the general development community did and significantly higher than financial service company developers.

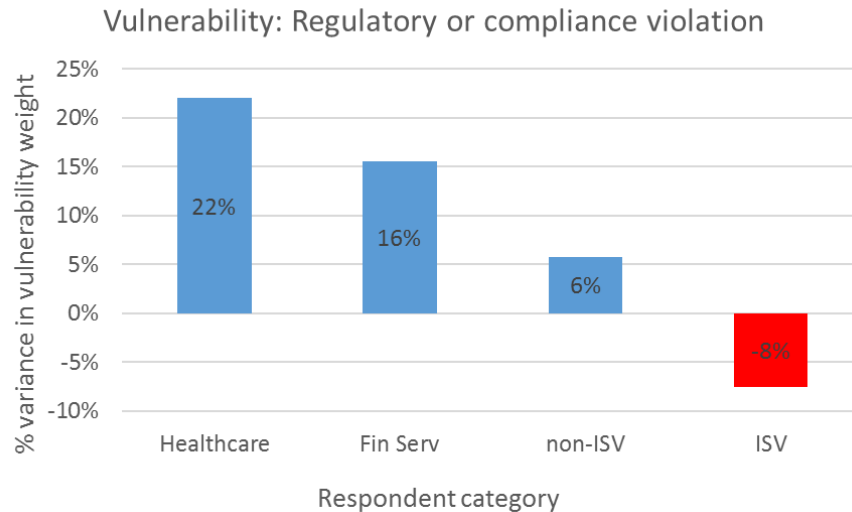


Financial Service companies placed data loss or corruption as the highest priority vulnerability with liability or reputational damage as the second highest priority vulnerability to manage.

3. THE MATERIALITY OF EACH VULNERABILITY ALSO VARIED WIDELY ACROSS DEVELOPMENT SEGMENTS.

Development organizations may align on the relative prioritization of vulnerabilities within a group, but they can still place markedly different weights on any individual vulnerability.

As an example, regulatory or compliance violations were typically placed at the bottom of the prioritized vulnerability lists. However, the relative importance of regulatory compliance across different development communities varied significantly.

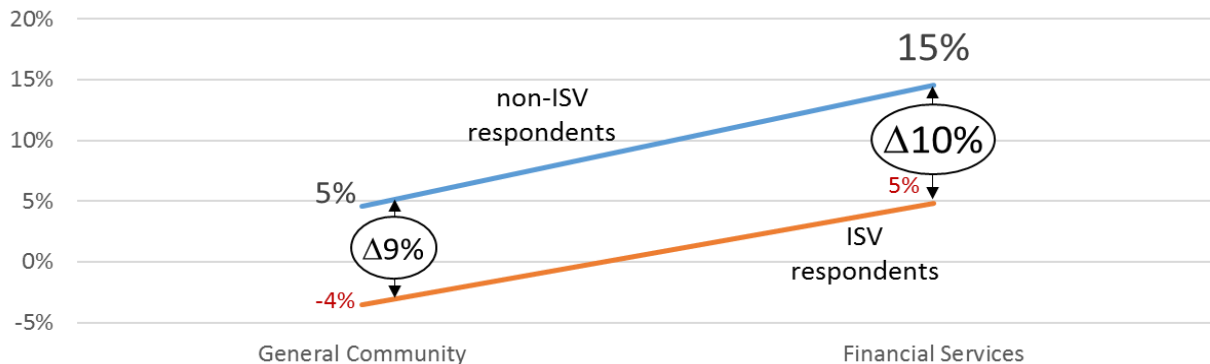


Healthcare and financial services development teams placed a greater weight on regulatory and compliance risk versus the general development community.



ISVs (independent Software Vendors) placed a lower emphasis on regulator risk than did the general non-ISV development community.

4. ISVs SHARE SOME UNIQUE TRAITS AMONGST THEMSELVES, BUT THEY ARE OFTEN MOST INFLUENCED BY THE CUSTOMERS THEY SERVE.



Comparing ISV and non-ISV Risk Tolerance (Appetite)



Non-ISV's have a 9% higher investment in mitigating risks than their ISV counterparts (which is 5% higher than the overall average investment).



Financial Services development organizations have a 10% higher investment in mitigating risks than the general non-ISV community.



ISV's whose applications are specifically developed for the Financial Services industry, like the financial industry developers themselves, have a ~10% higher than the general ISV community.

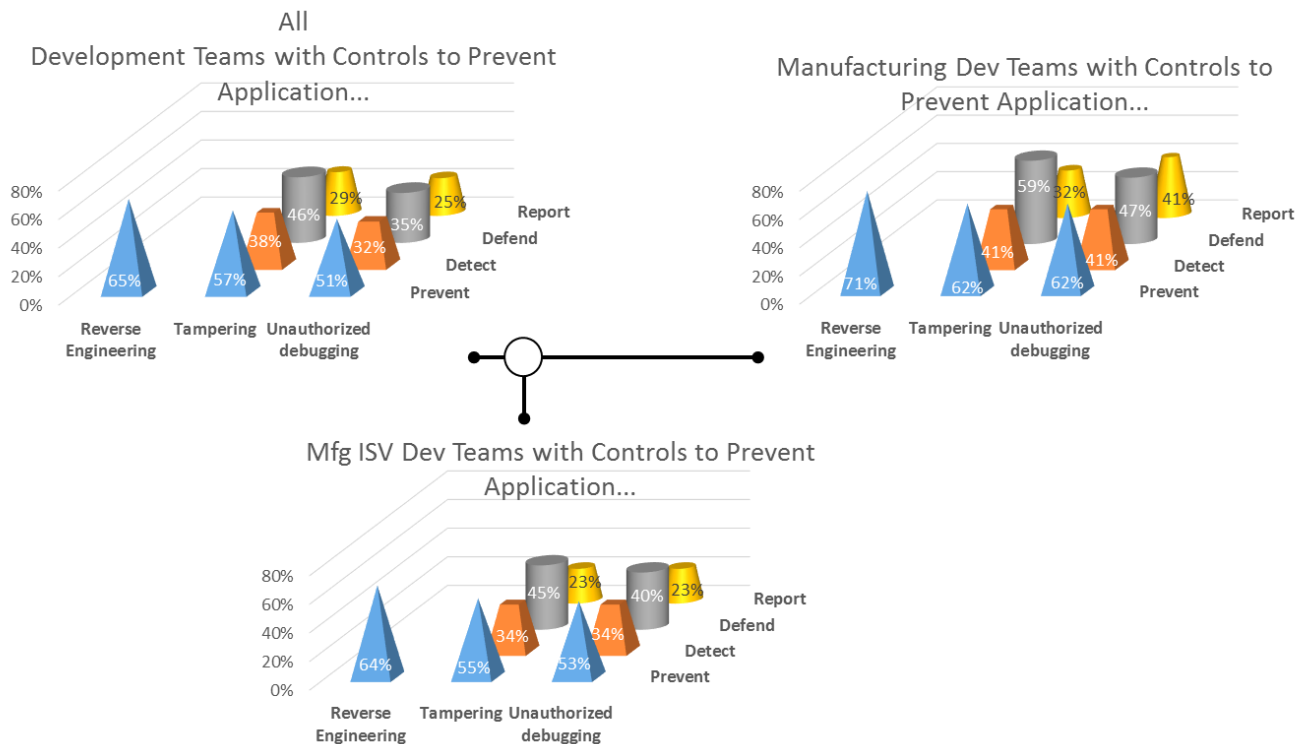
Financial Services ISV's have assumed the risk mitigation profile of their target users' risk profile.

Risk Mitigation Controls and Technologies

Survey respondents also indicated to what extent their development organizations have implemented specific controls to mitigate their application development risk.

Three gaps were assessed; Reverse engineering, tampering, and unauthorized debugging (to view and modify data, logic, and privileges).

Four classes of controls were measured; preventative, detective, active defense, and reporting.



Application control adoption comparison between all respondents, manufacturers, and ISVs developing software for manufacturers.



The majority of development organization have controls to prevent reverse engineering, application tampering, and unauthorized debugging. Preventative controls are a well-understood, common practice.



Manufacturers are most likely to implement application risk management controls across all classes and, in addition to preventative controls, defending against application tampering is also a common, well-understood practice.



ISVs developing software for manufacturers, as a group, appear to be out of step with the priorities of their target industry. As supplier risk management grows in importance, many of these ISVs may find themselves squeezed out but more security conscious competitors.

Have questions about this research? Want to learn more about your peers and how you measure-up? Contact solutions@preemptive.com and we will be delighted to work with you.

Demographics

Some more information about the 397 respondents.

Applications being developed (multiple selections permitted)

For internal business use	47.86%
To support our partners and supply chain	22.42%
For sale and/or subscription use	53.65%
Embedded inside or in support of some form of equipment	15.11%

Development organization size

Answer Choices	Responses
▼ 1-5 developers	59.32%
▼ 6-15 developers	14.70%
▼ 16-50 developers	13.91%
▼ 51+ developers	12.07%

Development platform and language (multiple selections permitted)

.NET desktop	81.11%
.NET backend server components	53.90%
Modern .NET surfaces including UWP, .NET Core	29.97%
Xamarin for Android	15.87%
Xamarin for iOS	14.11%
Other Xamarin	7.05%
Cloud-based apps and services	21.16%
Non-mobile Java	7.30%
Android	22.42%
iOS objective C	10.33%
JavaScript	28.46%
Other (please specify)	Responses 6.80%

Risk management maturity (risk priorities and controls are established...)

In an ad hoc and occasionally reactive manner	40.86%
Within a framework approved by management	30.35%
Within a framework formally established as organizational policy	16.34%
Within a framework formally established as organizational policy that is regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.	12.45%