The State of Application Security:
Is Your Company at Risk?

PreEmptive Solutions

April 2017

The State of Application Security: Is Your Company at Risk?

PreEmptive Solutions

Introduction

The risks of reverse engineering applications to uncover intellectual property or search for vulnerabilities to exploit are the highest they've ever been. And organizations that release apps with unprotected binary code are at risk because it is quite easy for hackers and criminals to reverse-engineer binary code back to source code using freely available tools. Leaving binary code unprotected provides unfettered access to the information inside, including intellectual property and security controls. Additionally, hackers are motivated by increasing social and financial incentives, which show no sign of decreasing.

Many companies still don't have official policies or guidelines for dealing with application risk. We surveyed individuals across a variety of industries and development platforms about their companies' approach to application and IP risk management. Despite the sheer amount of threats that could impact these companies, a majority of those surveyed do not have formal programs or regular coordination to address such threats.

To further explore these trends and their impact on application development, PreEmptive Solutions surveyed 161 individuals, comprised of developers and company leadership, about their companies' approach to application risk management.

This white paper explores the following:

- Trends in application risks and security
- The state of corporate application risk management
- How companies can better manage their risk moving forward

Trends in Application Security

Risks to applications and intellectual property are at all-time high, due in large part to almost a "perfect storm" of circumstances where expanding customer demands creates a "rush-to-release" phenomenon which may cause teams to overlook security vulnerabilities. In addition, hacking is becoming more rewarding, and regulations are becoming more complex.

Mobile Apps

More and more line of business mobile apps are being released daily. For those deploying applications to mobile, there's an increasing focus in Android and cross-platform uses, with iOS remaining ever popular.

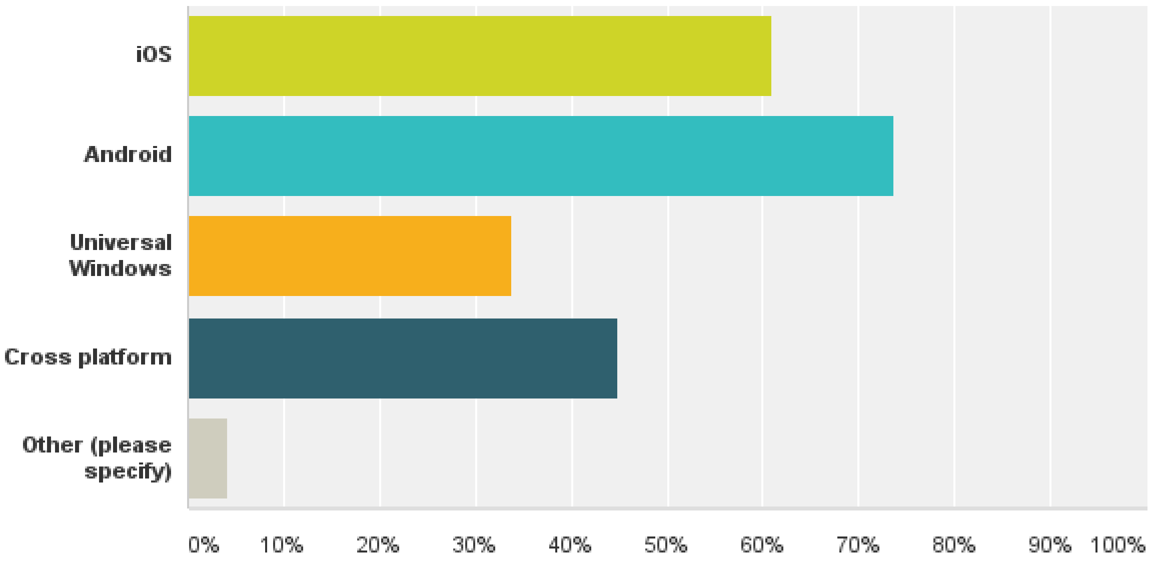


Figure 1- Mobile Targeted Platforms

An increased focus on Android development has subsequently triggered a rise in the number of Android malware families[1]. This growth within Android and cross-platform development means that developers and company leaders need to take appropriate steps to protect the code and intellectual property within their apps, especially if they are deploying publicly.

[1] Symantec, April 2016, "Internet Security Threat Report"

Strategic State-Based Hacking

As we've seen with the recent election cycle rumors, the use of state-backed hacking may become a more substantial threat as international conflicts are increasingly played out in the digital arena. IBTimes predicts that "in 2017 there will be an increase in 'strategic state-backed hacking' operations" looking to exploit companies and influence foreign populations.[2] As state-based actors become more emboldened, we expect their reach to extend into both public and private applications, creating unprecedented risk scenarios.

Intellectual Property Theft

Of the application risk categories recognized by our survey respondents, the highest perceived risk is that of intellectual property theft. This is followed by information theft and data loss or corruption.

Risk area	1- High	2	3- Low	N/A	Weighted Avg. Risk
Intellectual Property theft	41%	30%	20%	10%	1.77
Piracy	36%	25%	19%	19%	1.79
Information theft	39%	25%	22%	14%	1.81
Data loss or corruption	37%	28%	25%	10%	1.86
Interruption of service	27%	33%	21%	19%	1.93
Regulatory compliance breach	19%	24%	20%	37%	2.01
Public health or safety	13%	15%	14%	57%	2.02
Financial loss or theft	24%	24%	28%	24%	2.06
Identity theft	22%	17%	31%	30%	2.13
Service level breach	15%	29%	31%	25%	2.21

Figure 2- Application risk categories (1 is highest risk and 3 is the lowest). Any category that is not a material risk is marked as NA.

This data is not surprising. The very nature of "intellectual property" indicates that something unique and significant has been developed, thus making it a top concern for those involved in its creation.

Additionally, the Defend Trade Secrets Act of 2016 (DTSA)[3] and the European Union directive on trade secrets[4] have introduced new regulatory frameworks regarding the protection of intellectual property, or trade secrets. The evolution and fracturing of regulations domestically and internationally have increased the penalties for making mistakes and multiplied the confusion around what compliance actually looks like for managing corporate risk, giving malicious parties greater opportunities to expose mistakes and take advantage of regulatory loopholes.

[2] http://www.ibtimes.co.uk/russian-hacking-ransomware-what-experts-say-about-cybersecurity-2017-1597644

[3] https://www.congress.gov/bill/114th-congress/senate-bill/1890/text

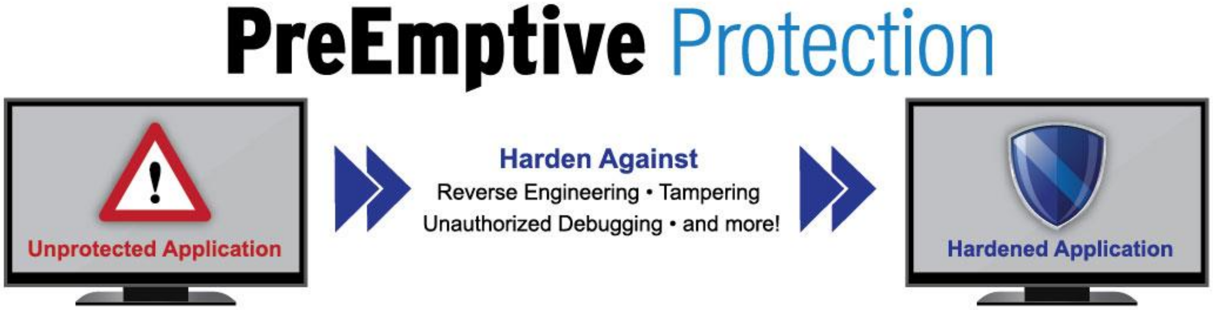
[4] http://ec.europa.eu/growth/industry/intellectual-property/trade-secrets_en

Worth Protecting: Corporate Application Risk Management

With such significant threats to applications, devices, and intellectual property, one would think that companies with even a minimal exposure to these risks would be investing substantial amounts of time and money on protecting themselves. However, this isn't always the case. A surprising 30% of survey respondents do not have adequate controls to mitigate these risks, while 41% don't include 3rd party application risks in their company's risk management framework. Even in companies with formal or informal risk management programs, 53% do not include app protection controls in their considerations.

While many companies recognize the importance of preempting and addressing such risks, oftentimes these efforts are led by single developers or teams, which in turn are not adopted throughout the enterprise. It is imperative that these threats to applications are understood by all parties with a vested interest in their security, and yet for many businesses this cross-departmental alignment does not currently exist. Of those surveyed, 58% do not have a well-defined, regularly scheduled coordination between development, legal and risk personnel while 60% think legal and executive management would benefit from a better understanding of their company's dependence on technology. A shocking 70% believe that development and IT personnel, the very individuals who are building apps and intellectual property that merits protecting, should have a deeper understanding of their company's approach to risk management.

The significant range of threats to application development have made it even more complex for companies to understand and address the risks – so what should companies do to mitigate these threats and protect their intellectual property?



Is it Worth Protecting? Determine Risks. Establish Controls.

Unprotected binary distribution holds varying degrees of risk that can be segmented by industry segment. Software vendors, financial service providers, telecommunications companies, manufacturers and other businesses that rely on applications to generate revenue, assure business continuity and whose applications represent unique intellectual property have a greater risk with proportionately higher requirements and more severe penalties for failure.

Yet most corporations and governments have a high degree of dependency on applications. Companies developing applications need to make sure there is clear, aligned corporate directive and cross-departmental understanding of application risk in addition to ensuring the right tools are in place to protect their information. Risks stemming from application failure, compromise or disclosure must be assessed and managed as a first-class category of risk within/across financial and operational and reputational risk categories.

This is amplified for organizations that develop their own software or have software developed specifically to meet their own needs; additional risks stemming from development practices, embedded intellectual property and/or trade secrets – whether embedded in the code itself or in the data that flows through those applications, must be carefully evaluated.

Determining risk for developed software is more than a technical exercise - it must be reflected within higher order categories of risk; broad financial, operation and reputational categories and can no longer be treated as a highly-specialized niche set of controls. Executive and risk management must enhance their understanding of their dependency on applications even as application developers must take the time to appreciate the follow-up implications of application failure, compromise or disclosure.

IS YOUR APP WORTH PROTECTING?
Contact us to see if we can help.

About the Survey

PreEmptive Solutions surveyed a total of 161 individuals at a wide variety of companies, 128 of which provided complete responses.

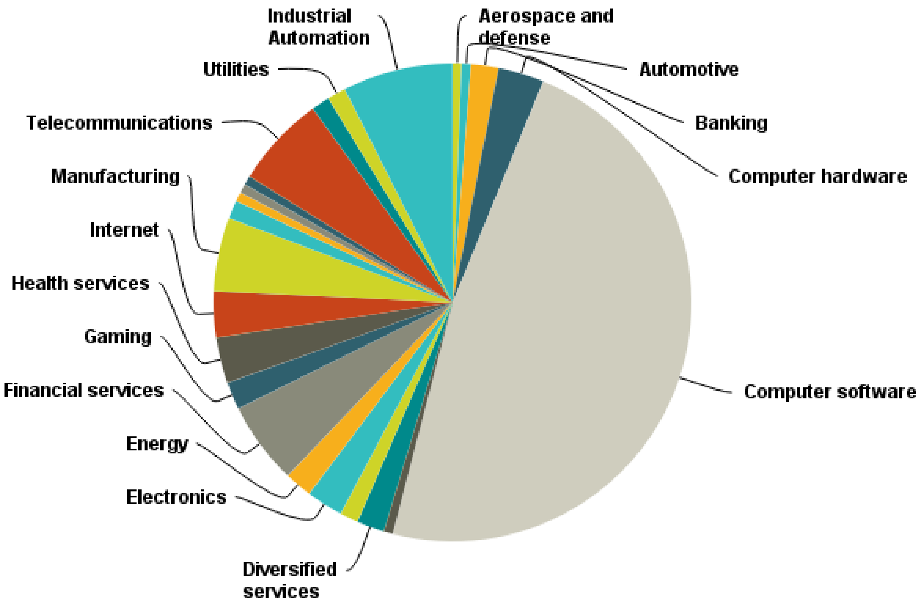


Figure 3- Primary Industry

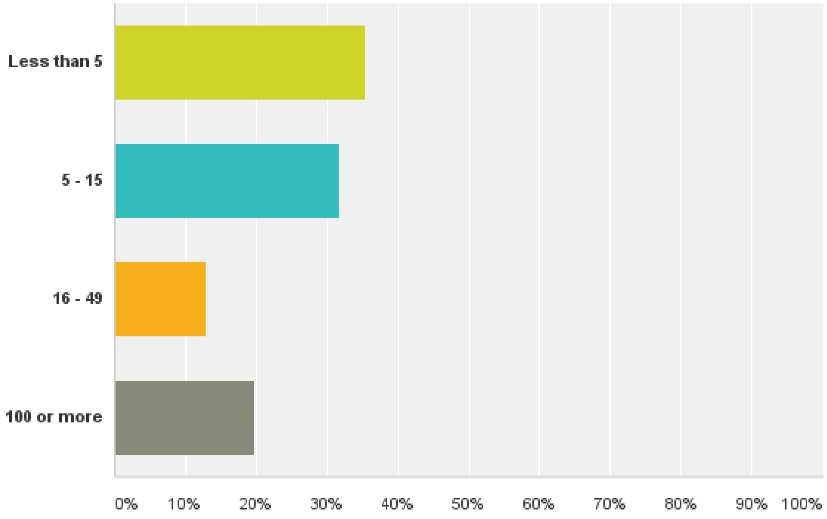


Figure 4- Size of combined developer, test and support organization

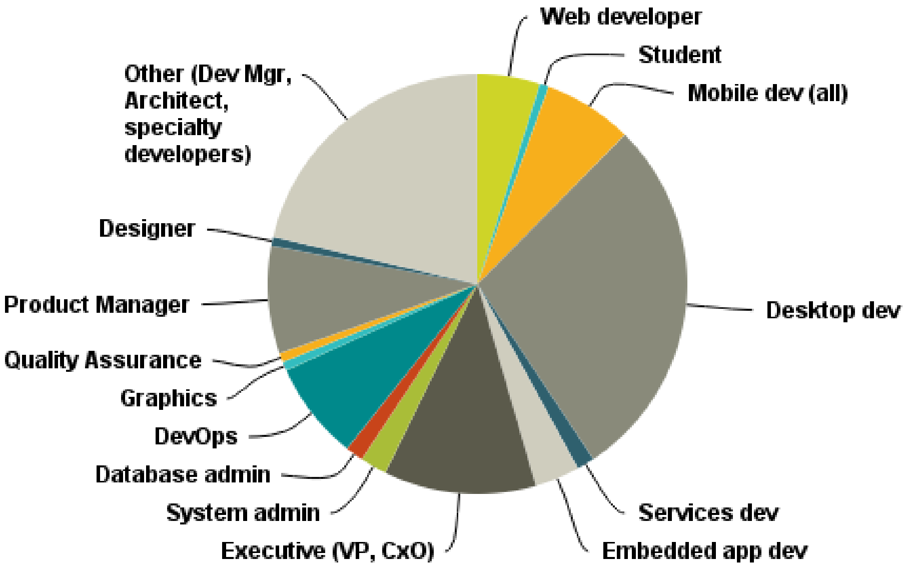


Figure 5- Role of respondent

About PreEmptive Solutions

PreEmptive Solutions is a trusted global leader of application self-protection tools for Desktop, Mobile, Cloud, Internet of Things (IoT) and other Applications used by over 5,000 corporate clients spanning virtually every industry in over 100 countries.

PreEmptive Protection hardens all flavors of .NET, Java, Android, iOS, Xamarin and UWP apps through a combination of binary obfuscation, encryption, suspicious activity detection, defense and alert controls that are directly infused into software applications before they are released.

For more information, visit www.preemptive.com or call +1 440.443.7200.