VansonBourne

GUARDSQUARE
Mobile application protection

Survey results: Nearly 90% of respondents have experienced a mobile app security incident in the past 12 months.

Are your mobile apps as secure as you think?

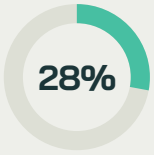
Introduction

Mobile applications are used by nearly everyone. The number of mobile apps continues to grow to keep pace with business needs and consumer expectations. Survey responders report that they release 10 unique mobile apps per year, on average.

Organizations understand the risk of an unprotected mobile app

There's a strong understanding that attacks on mobile apps are becoming increasingly sophisticated.

In fact, within the last year, 88% of organizations have experienced an attack on their mobile applications.



28% of respondents claim an increase in attempts to reverse engineer/ modify apps is driving their organization to consider or purchase mobile app security products.

While organizations may understand the risk of an unprotected app, few organizations are fully protecting their mobile applications. Many believe operating system (OS)-level protections are sufficient when these defaults alone are not enough to defend against sophisticated attacks from bad actors. A lack of a comprehensive, multi-layered security approach has the potential of opening a myriad of risks. Within the last twelve months, respondents reported their organizations suffered from mobile app downtime, negative user experiences, data leakage, and financial loss due to unprotected mobile apps.

It's essential that organizations building, launching, and managing mobile apps are aware of the risks of releasing an unsecured mobile app and understand the best practices to protect them. Contrary to popular belief, it is possible to balance security considerations with the rapid development and iteration pressures of the mobile app development process.

This executive summary is based on a global research study consisting of 500 software developers and security professionals from organizations releasing at least 5 different end-user facing mobile applications in the past 12 months.

This summary provides insights into the following:

The challenges mobile development teams are facing when securing their mobile apps

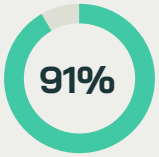
How organizations worldwide are protecting their mobile apps, and how that may (or may not) vary by region

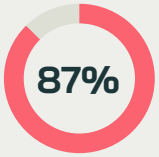
Whether organizations are doing enough to keep their mobile apps secure

The risks associated with releasing an unprotected mobile app

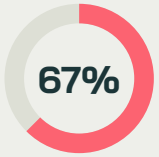
Key Findings

Mobile app developers and engineers are overestimating the level of security of their mobile apps.





Despite 91% of responding organizations feeling they do not release unprotected mobile apps, 87% reported a mobile app security incident in the last twelve months.



What's more, 93% of organizations believe they understand the risks of releasing unprotected mobile apps; however, 67% report that using the OS only (e.g. Android or iOS) is sufficient in keeping mobile apps secure.

In the last twelve months as a result of unprotected or less protected mobile apps:

32%
of users were estimated to be directly affected by a security incident, on average.

26%
of surveyed organizations experienced mobile app downtime due to a security incident.

25%
experienced attacks that bypassed their security measures.

25%
experienced data loss or data theft.

$4.97 million

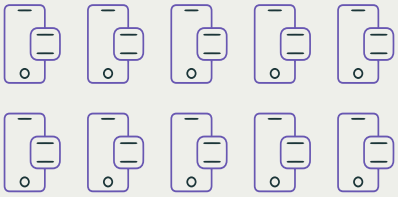
Organizations report the average cost of a mobile application security incident is just under 5 million USD.

Organizations acknowledge that there is room for improvement in their current mobile app security processes. However, they are often constrained by pressures to continuously release new features for their applications.

98%
of organizations reported **room for improvement** in the level of security incorporated in their mobile application development process.

27%
report a **need for significant improvement** indicating their current level of security needs to be prioritized to protect their mobile apps from attacks.

Organizations reported the biggest challenge with implementing and maintaining mobile application protection was the pressure to continuously release new features (41% of organizations ranked this concern highest). Nearly 30% believe that investing in mobile app security will delay their time to market.

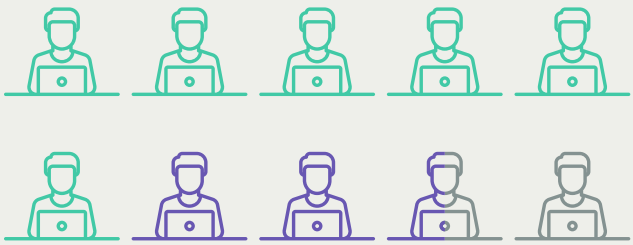


Surveyed organizations are producing an average of 10 unique mobile apps per year, with 70% of organizations reporting they update their mobile apps at least once a month. With this volume and pace of mobile app releases, it is important organizations balance security with speed. Leveraging third-party tools and best practices can address the risks associated with unprotected mobile apps such as loss of IP, revenue, brand trust, and more.

Organizations understand the importance of mobile application security; however, many are facing a security skills gap which is hindering what can be achieved.

As mentioned, organizations are producing 10 unique mobile applications a year, on average, with 70% of organizations updating their mobile apps at least once a month. This works out to be one new mobile app released every 37 days on top of updates to existing apps. This amount of work requires large investments in resources including human capital and budgets. These investments become even more challenging when organizations are struggling with internal security skills gaps and a lack of trained security professionals available in the market for organizations to hire. This begs the question - is there a way to effectively deliver mobile app security without having to invest in expensive training or expanding teams?

On average, organizations with at least 200 employees may have as many as 120 people on average contributing to the development of their mobile apps...



...and testing teams with as many as 44 people.

However, with 71% of organizations reporting their organization is facing a skills gap, there's clearly a gap in available skilled mobile app security resources leading to a lack of ability to implement mobile app security tools. What's more, there's a misalignment between departments, with those working in mobile application development or software engineering/development departments more likely to report a security skills gap than those working in IT security (Figure 1). This misalignment is likely the result of those in the IT/information security department being further removed from the mobile app development process and perhaps overlooking some of the complex tasks developers and software engineers are tackling.

"There is a skills gap within my organization"

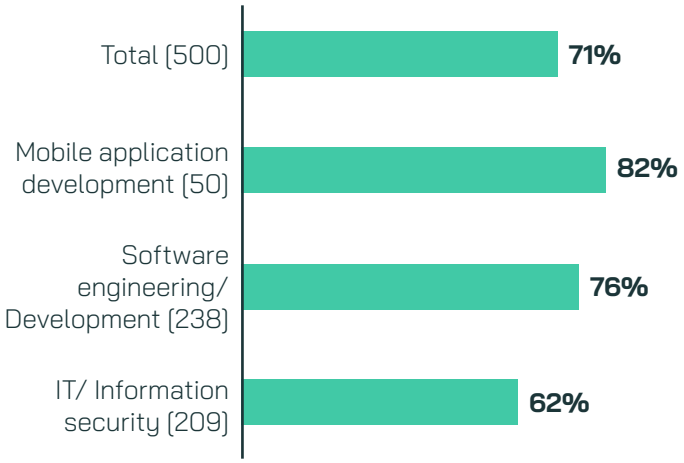


Figure above: To what extent do you agree or disagree with the following statements? – There is a security skills gap within my organization. (Base shown in chart), data split by respondent department.

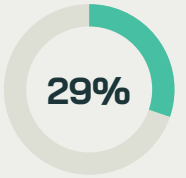
IT security and mobile app development teams will need to work together to identify the best measures they can take to overcome these skills gaps. One approach is for organizations to look for robust tools and solutions that don't require deep security knowledge and training or a vast amount of time to implement and manage, while continuing to deliver the best possible mobile app protection and user experience.

Organizations are relying on additional protection solutions to stay ahead of potential attacks.

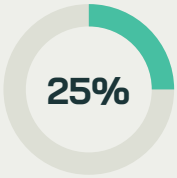
Positively, nearly all (98%) organizations report purchasing or considering purchasing additional protection solutions to augment limitations with time and talent. This added layer of security helps mitigate any possible mobile app vulnerabilities and ensures a secure and safe mobile app is developed.

With 98% of organizations considering or having purchased additional protection solutions for their mobile apps, purchasing from external vendors is the favored approach worldwide. However, it's not uncommon for organizations to protect their mobile apps using tools built in-house (20%), or a combination of internal and external products and tools (14%). The source of protection solutions also varies by market with individual markets having varying preferences. Before purchasing additional products, it's essential organizations are aware of their markets current trends, constraints and driving forces to ensure the best solution is chosen.

Other factors include the desire to demonstrate a security-first mindset (34%), to keep in line with regulatory / compliance requirements (29%), and to address the increase in attempts to reverse engineer and modify / clone mobile apps (28%).



Report purchasing from one third-party vendor

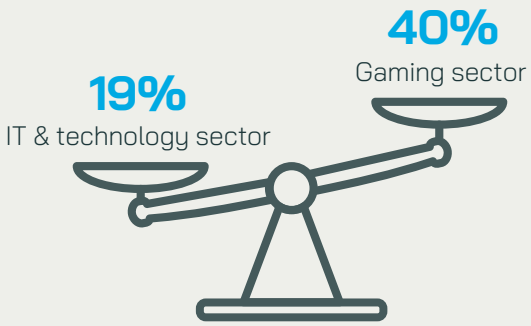


Report purchasing from multiple third-party vendors

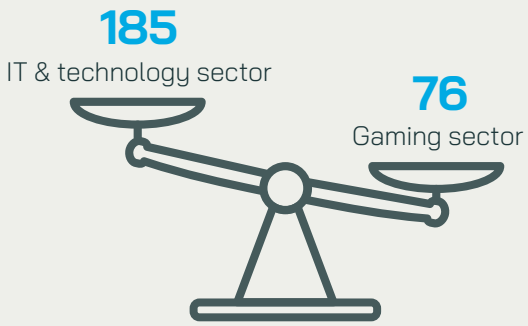
Out of the global respondents, the desire to stay ahead of potential attacks (36%) is the top driving factor pushing organizations to consider, or purchase, robust protection solutions.

Approaches to mobile app security vary by industry and department.

From the source of their protection solutions to the number of people contributing to the development of mobile applications, approaches to mobile app security vary by industry and department. It's important organizations keep this in mind, one size definitely does not fit all with mobile application security and approaches should be tailored to specific needs and constraints.



The gaming sector is more likely to utilize one third-party provider compared to the IT & technology sector perhaps due to the specialized nature of the gaming industry.



The number of people contributing to the development of mobile apps varies significantly by sector, ranging from 185, on average, for IT and technology, to just 76 for gaming.

In addition to the need to release and update mobile apps frequently, there may be additional perceived barriers that restrict investments into mobile application security. For instance, 31% of organizations report creating a good user experience as a barrier in the next twelve months impacting further investment. This is especially true for the retail, distribution, and transport sector, where 49% expect the challenge to remain.

Organizations are struggling to ensure they are balancing a good user experience with strong mobile application security; many acknowledge inadequate security will likely end in a damaged user experience – as reported by one in four (25%) in the last twelve months.

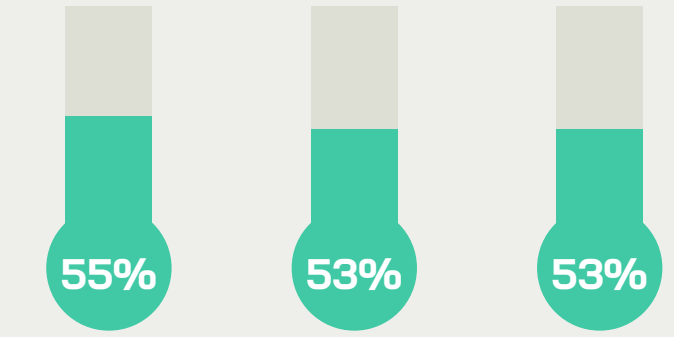
Security best practices elevate global organizations, recognizing security as a key comeptitive advantage

Surprisingly, only 48% of organizations reported having up-to-date company policies outlining security requirements. Organizations may be focusing on the minimum requirements due to a lack of time and available skills to create their desired security process for mobile apps.

However, there is disparity across departments, with security professionals more likely to say there are up-to-date company policies (52%) than the mobile app development or software engineering/development teams (40% and 45%, respectively). This makes sense given security professionals have likely taken a larger role in the creation of the policies. Ensuring alignment between the security and IT teams will be essential to ensure the app security in place meets best practices and allows for emerging threats, whilst remaining customer and user focused.

When it comes to the driving force behind consideration of mobile app protection solutions, alongside wanting to stay ahead of potential threats (36%) – an expected finding – organizations also want to be seen as having a security-first mindset thus increasing positive brand association (figure 2). The perception of a security-first mindset indicates security is woven into the security development lifecycle, which, in turn, will increase a positive brand reputation. If users perceive the mobile app to be secure, they are likely to be more willing to use the app for sensitive transactions. Indeed, 95% of respondents believe that prioritizing mobile app security acts as a unique selling point for their mobile applications.

The security approaches most likely to be followed by self-identified digital leaders are:



The driving forces in why an organization considers/purchases additional protection solutions

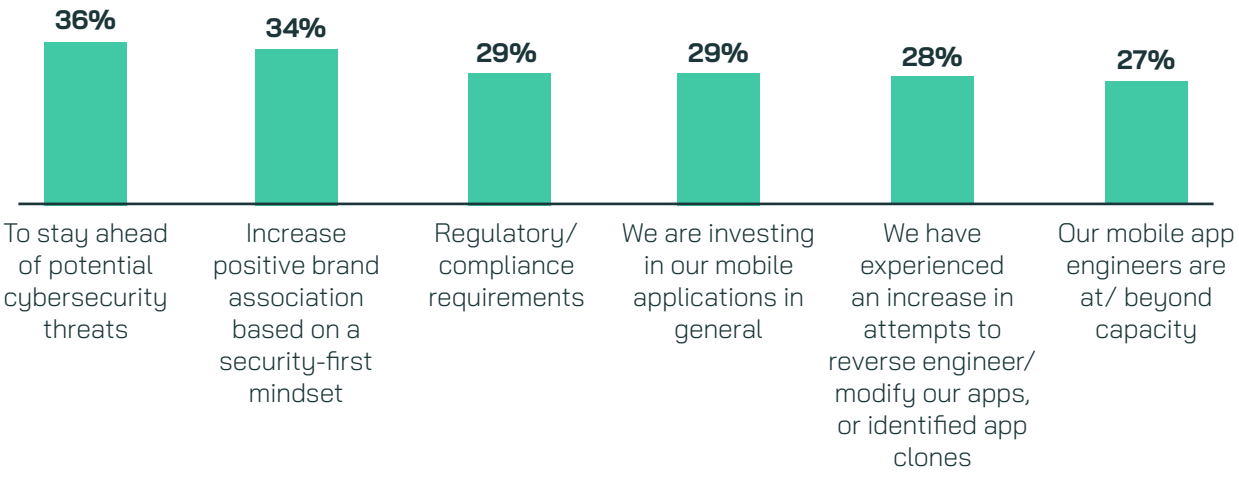


Figure above: What is driving your organization to consider/ purchase protection solutions for your mobile applications? (500) Not showing all answer options.

Despite the need and desire for improvement, organizations recognize clear risks with third-party libraries and a lack of resources.

Mobile app attacks are constantly evolving and becoming more sophisticated. Organizations understand that they need to keep their mobile app security approaches under continuous review to prevent negative customer or business impacts from mobile app security gaps.

Of the 98% of responders reporting their current organization's level of protection has room for improvement, there was remarkable consistency across industry sectors, individual departments, and the varying seniority levels.

One-way organizations can improve their mobile app security posture is to implement best practices and proven mobile app security tools and protections at the code level. They must also ensure that third-party libraries and open-source solutions are utilized effectively and securely. Although they can speed up development, and reduce the resources needed, few feel that those tools are secure. In fact, 47% report they feel there are significant risks associated with third-party libraries.

To address issues discussed above, such as developer capacity and security talent shortages, it's encouraging to see major investments are being made to increase security training for all engineers and developers (51%) as well as increasing the size of security (44%) and mobile app testing teams (44%) (figure 3). Organizations are enabling their security and app development teams with proper and effective training on best practices, and with tools that provide a deep level of protection with a lower administrative/managerial burden. This should help ensure that these increased investments are maximized to the fullest extent possible. An increase in staffing resources would allow mobile application developers more bandwidth to evolve their security processes and tools.

Predicted investments to be made in the next twelve months

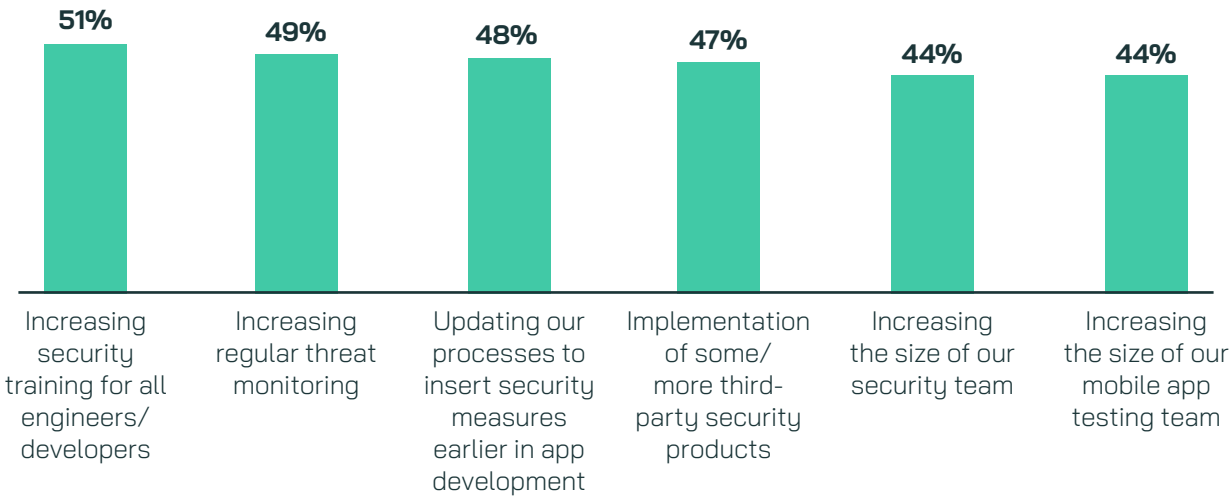


Figure above: Which of the following investments do you think your organization will make over the next twelve months, to improve your mobile application security? (500) Not showing all answer options.

What does this mean for mobile application security?

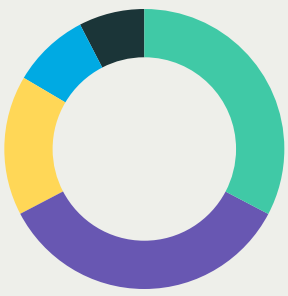
It's clear that improving mobile app security is not just an option - it is vital. With risks including app downtime, security circumvention, data loss/theft, intellectual property theft, and malware insertion, among many others, organizations are at risk of experiencing significant repercussions. Surveyed organizations reported losing an estimated US$5 million to mobile app security incidents in the past 12 months alone. Many of these incidents could have been avoided if organizations implemented strong mobile application protection.

First, organizations must understand that OS-level security protections alone are not enough. Organizations should embrace a multi-layered approach to mobile app security which starts at the code level before an app is released and continues throughout the development lifecycle with ongoing testing and real-time security threat monitoring.

In addition, security doesn't have to come at the expense of development time-to-market. It's positive to see organizations begin to embrace third-party tooling to extend the capabilities of their team. It's important to note that a security solution should expand the development team's capacity, rather than adding additional burden. As mobile app attacks increase in volume and sophistication, incorporating secure coding best practices, in addition to the right tooling, can help organizations improve their overall security posture.

Research scope and methodology

Guardsquare commissioned independent market research specialist Vanson Bourne to undertake the quantitative research, which this report relies upon. A total of 500 software engineers and developers were interviewed in November and December 2023. There was representation from the following markets (number of interviews in brackets):



- Europe (150) – Made up from UK (76) and Germany (74)
- North America (200) – US (150) and Canada (50)
- Brazil (75)
- Singapore (40)
- UAE (35)

Respondents were from various private sectors – excluding private education.

Vanson Bourne conducted interviews online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

This executive summary is based on all respondents, with some department or market differences referenced where applicable.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit *www.vansonbourne.com*

About Guardsquare

Guardsquare offers the most complete approach to mobile application security on the market. Guardsquare's software integrates seamlessly across the development cycle: from app security testing to code hardening to real-time visibility into the threat landscape, Guardsquare products provide enhanced mobile application security from early in the development process through publication. More than 900 customers worldwide across all major industries rely on Guardsquare to help them identify security risks and protect their mobile applications against reverse engineering and tampering.