2021 SURVEY RESULTS

The State of Mobile Banking App Security

verimatrix
DRIVING TRUST

iSMG
INFORMATION SECURITY
MEDIA GROUP

Table of Contents

The survey, conducted in early 2021, generated more than 150 responses from security professionals working in the financial services industry throughout the U.S., Canada and EMEA.

Letter from the Editor

NICK HOLLAND
Director of Editorial, ISMG
editorial@ismg.io

Holland, an experienced security analyst, has spent the last decade focusing on the intersection of digital banking, payments and security technologies. He has spoken at a variety of conferences and events, including Mobile World Congress, Money2020, Next Bank and SXSW, and has been quoted by The Wall Street Journal, CNN Money, MSNBC, NPR, Forbes, Fortune, BusinessWeek, Time Magazine, The Economist and the Financial Times. He holds an MSc degree in information systems management from the University of Stirling, Scotland.

Our survey examined how decision makers in financial services approached application security, primarily in mobile banking.

This survey, sponsored by Verimatrix, aims to determine the challenges of developing and securing the increasingly critical mobile channel for financial institutions.

This report showcases valuable and actionable research findings:

- Banking security teams' greatest concerns relating to mobile banking application security;
- What types of mobile attacks are most prevalent today;
- How today's banking security executives are mitigating risk in the mobile channel.

Among some of the key findings from financial services security professionals:

- **Almost 70% of survey participants** perceive the mobile channel to be critical or very critical for their financial institution.
- **Just 60% of survey respondents** are confident about the level of security on their mobile apps, and only 8% of those are extremely confident.
- **A quarter of survey respondents** state that they spend less than $50,000 per year on mobile security, and nearly half spend under $200,000 per year.

Explore the full survey results below, and get expert analysis about how to put this information to use to improve your organization's ability to enhance mobile security.

Best,

Executive Summary

KEY AREAS

This research showcases three key areas:

- Fraud and Security Concerns for Financial Institutions
- Mobile Banking Security Threats and Mitigation
- Mobile Banking Security Management and Execution

Fraud and Security Concerns for Financial Institution

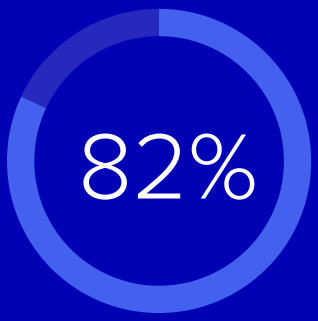
Survey results show there is a high level of concern about security in the financial services sector, especially regarding the mobile channel, with 93% of respondents stating that they are concerned or very concerned about security in the financial services sector.

The greatest concern is for malware and ransomware, with 43% of survey respondents stating that they are worried or very worried about this threat. The least concerning area is application/API hacks, although over one-third of respondents see these as worrying or very worrying.

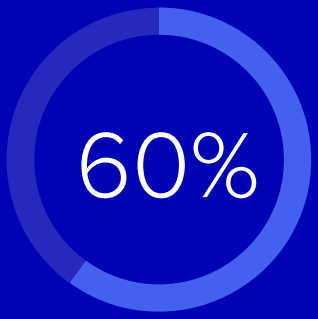
The survey responses reflect the degree of criticality that the mobile channel has for digital banking, with 69% of respondents saying they perceive it to be critical or very critical.

About 82% of respondents see mobile security as being important or very important, and just 5% consider it to be of low importance.

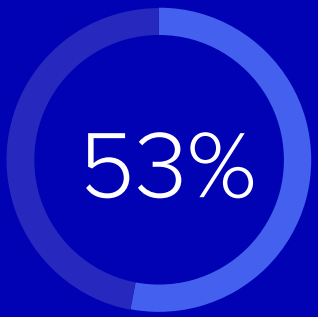
BY THE NUMBERS



82% of respondents consider securing the mobile channel to be important or very important for their financial institution.



60% of survey respondents are confident about the level of security on their mobile apps, and only 8% of those are extremely confident.



53% of CISOs are involved in evaluating, influencing and deciding on mobile security for financial institutions.

The greatest area of concern if a data breach occurs in the mobile channel is for reputational loss, with 60% of respondents considering it to be of significant concern. That is 20 percentage points higher than the second category – financial losses directly related to fraud.

Mobile Banking Security Threats and Mitigation

About 42% of survey respondents believe that they have had no fraud incidents in the mobile channel.

The most common form of increased security via the mobile channel is the addition of multifactor authentication, or MFA, which 83% of institutions either have in place or plan to have in place within the next 18 months. Other anti-fraud tools that banks are using include fraud detection and monitoring systems (51%), device identity (40%), out-of-band verification (36%), DDoS mitigation (34%) and cross-channel fraud detection (29%).

Just 60% of survey respondents are confident about the level of security on their mobile apps, and only 8% of those are extremely confident.

Just over half of CISOs are involved in evaluating, influencing and deciding on mobile security for financial institutions.

Mobile Banking Security Management and Execution

Half of survey respondents have their mobile banking apps and mobile websites developed externally through a vendor. Another 19% purchase a white label solution.

Three-quarters of respondents state they have a strong understanding of the data that flows through their mobile apps. Just 61% of respondents state that they are currently running vulnerability analysis and penetration tests on mobile channels.

Over one-third of respondents state that they don't know what the annual spend on security is for mobile applications. Just over half of CISOs are involved in evaluating, influencing and deciding on mobile security for financial institutions.

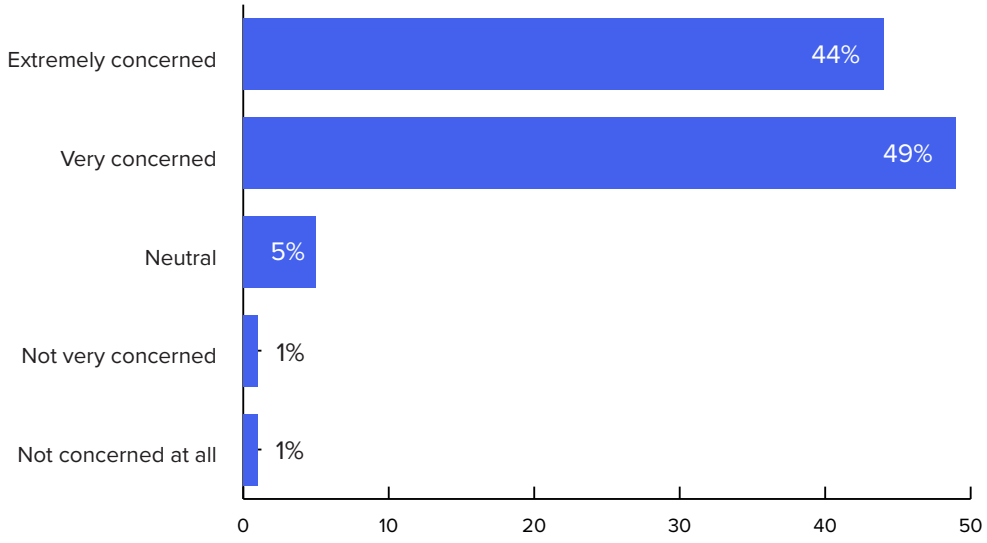
Fraud and Security Concerns for Financial Institutions

SUMMARY

This survey begins by asking security professionals in the financial services industry about their concerns relating to the mobile channel if a breach or other significant cybersecurity event occurs. Some notable findings:

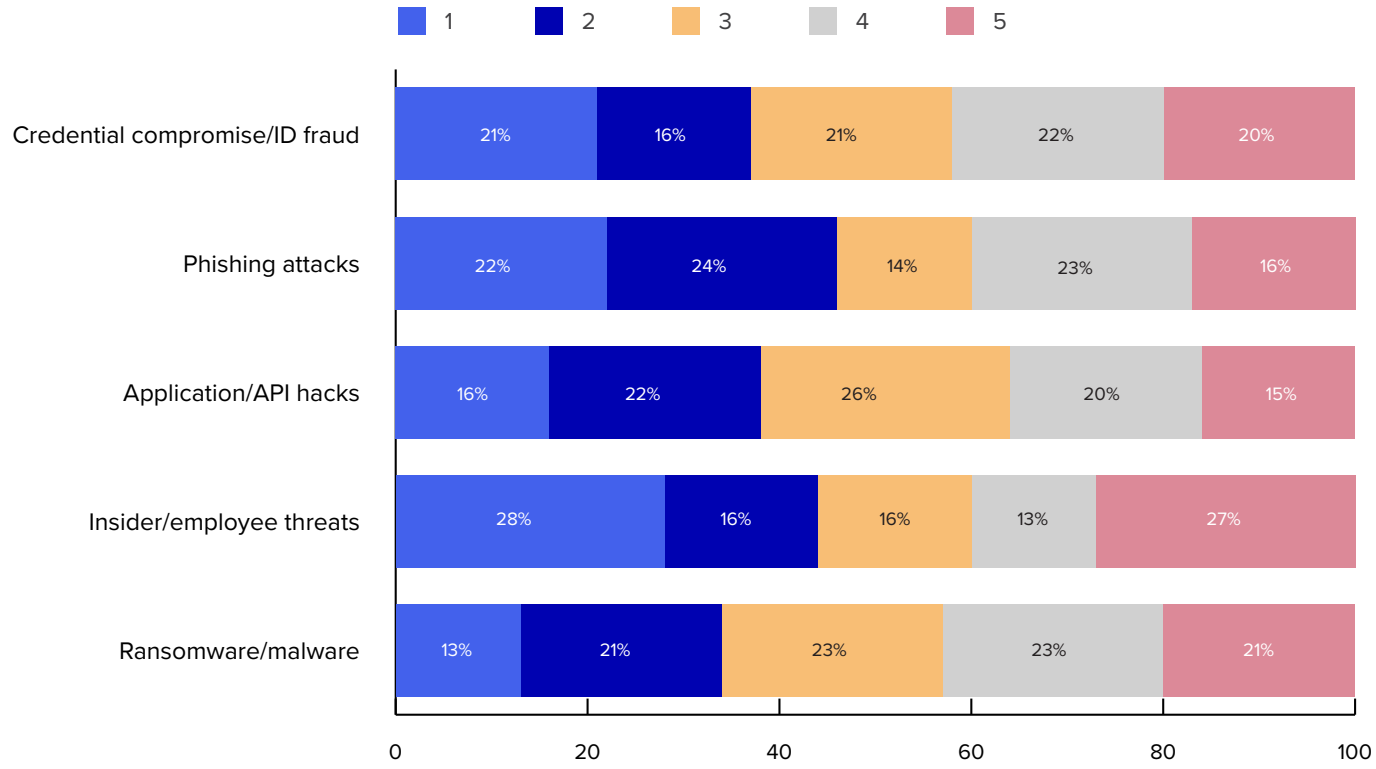
- 93% of respondents say they are concerned or extremely concerned about security in the financial services sector.
- 82% of respondents consider securing the mobile channel to be important or very important.
- 60% of respondents state that reputational losses are their greatest concern should there be a significant cybersecurity incident via the mobile channel.

How concerned are you about security in the financial services sector?



Given that the survey was sent to security professionals in the financial services industry, the response to how concerned they were about security was not a great surprise. About 93% stated that they were concerned or very concerned about security in the financial services sector. Financial institutions always have a bull's-eye on their back for cybercriminals and fraudsters, and this is likely to be more pronounced than ever via remote channels that are still somewhat nascent for many banks and credit unions.

What security threats are you worried about the most? (1 = least important, 5 = most important)



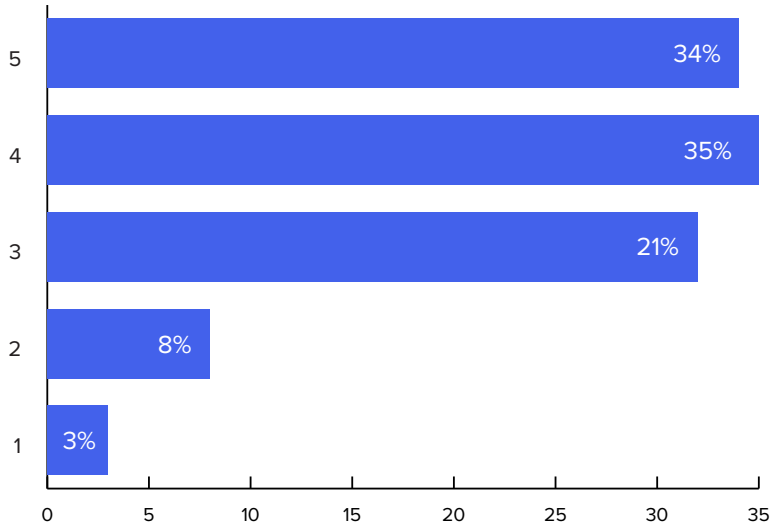
While all security threats are seen as worrying, the greatest concern is for malware and ransomware – 43% of survey respondents are worried or very worried about this threat. The least concerning area is application/API hacks, although this is still seen as worrying or very worrying by over one-third of respondents.

One interesting finding was the polarizing nature of insider/employee threats. About 27% of respondents say they are the most worrying, and 28% say they are the least worrying. This bifurcation shows the subjectivity of this topic, as some financial institutions had a more progressive approach to remote work before the pandemic began while others had a more traditional office-based culture. This polarization may be a barometer of attitudes to current remote work environments and the ability for security professionals to keep a close eye on human (mis)behavior outside of a traditional security perimeter. It is likely that financial institutions that embarked on their digital transformation journey before the pandemic began are more apt to be prepared for remote work environments that are secure and preplanned.

Other areas of concern captured in the survey are DDoS attacks and attacks on the supply chain, possibly stemming from the recent SolarWinds attack that has significantly raised awareness of threats via third parties.

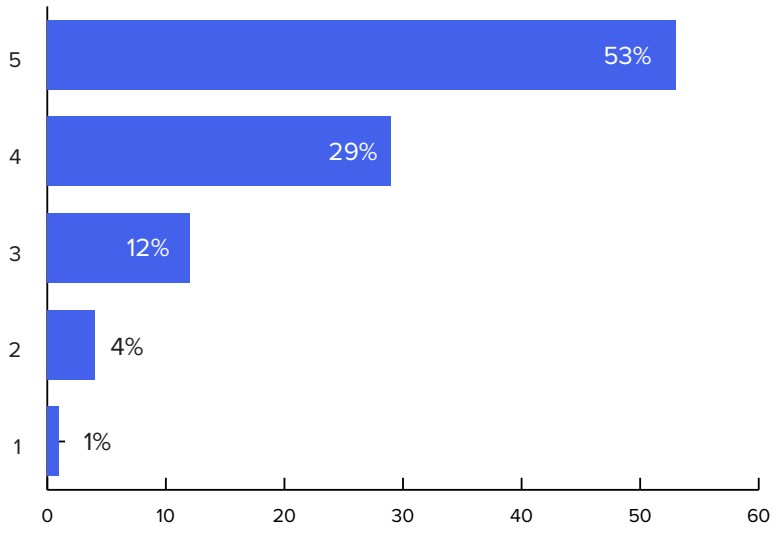
On a 1-5 scale (1 = not critical, 5 = very critical), how critical is the mobile channel to your financial institution?

The survey responses reflect the degree of criticality that the mobile channel has for digital banking. About 69% of respondents perceive it to be critical or very critical. But nearly one-quarter of respondents are neutral about the criticality of mobile, and 11% see it as not being critical or as having a low level of criticality. Clearly, there is still a sizeable number of institutions that have not yet fully embraced how important the mobile channel is to their customer base.

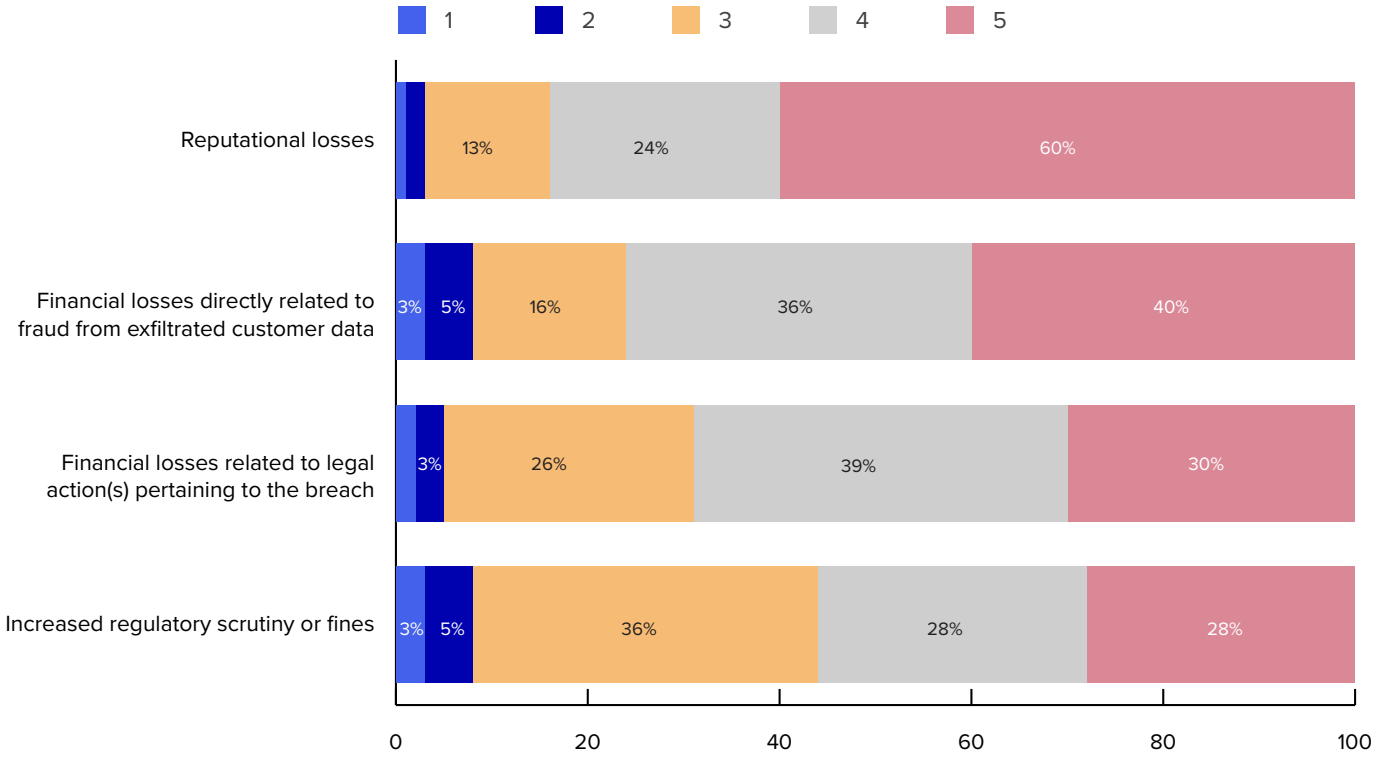


On a 1-5 scale (1 = not important, 5 = very important), how important is mobile application security to your financial institution?

Survey respondents care a lot about the security of their mobile apps. About 82% of respondents see mobile security as important or very important. Just 5% consider it of low importance. This is a good sign that financial institutions understand how important securing the mobile channel is for an increasingly remote customer base.



On a 1-5 scale (1 = little concern, 5 = significant concern), how concerned are you about the following actions occurring due to a data breach of the mobile channel resulting in loss of customer PII?



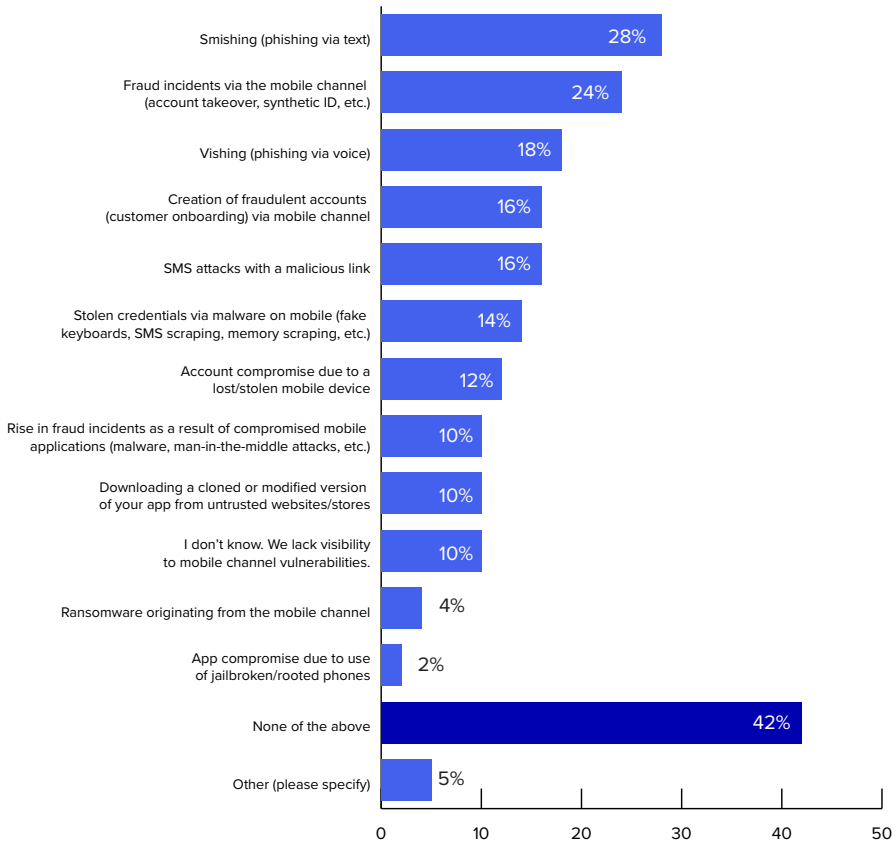
The greatest area of concern if a data breach occurs in the mobile channel is for reputational loss. About 60% of respondents consider it to be of significant concern. That is 20 percentage points higher than the second category – financial losses directly related to fraud. This reflects the fact that, in the mobile channel, reputation is critical to customer retention, and jeopardizing it could be catastrophic, causing customer defections to other financial institutions. The digital transformation of banking has significantly lowered the barriers to moving accounts elsewhere.

The area of least concern was increased regulatory scrutiny or fines. That may be a result of the somewhat abstract nature of this concern compared with more direct financial or reputational damages that could occur. Yet the majority of survey respondents (57%) see this as an area of high concern.

Mobile Banking Security Threats and Mitigation

In the past year, have you experienced any of the following fraud incidents specifically related to the mobile channel? (check all that apply)

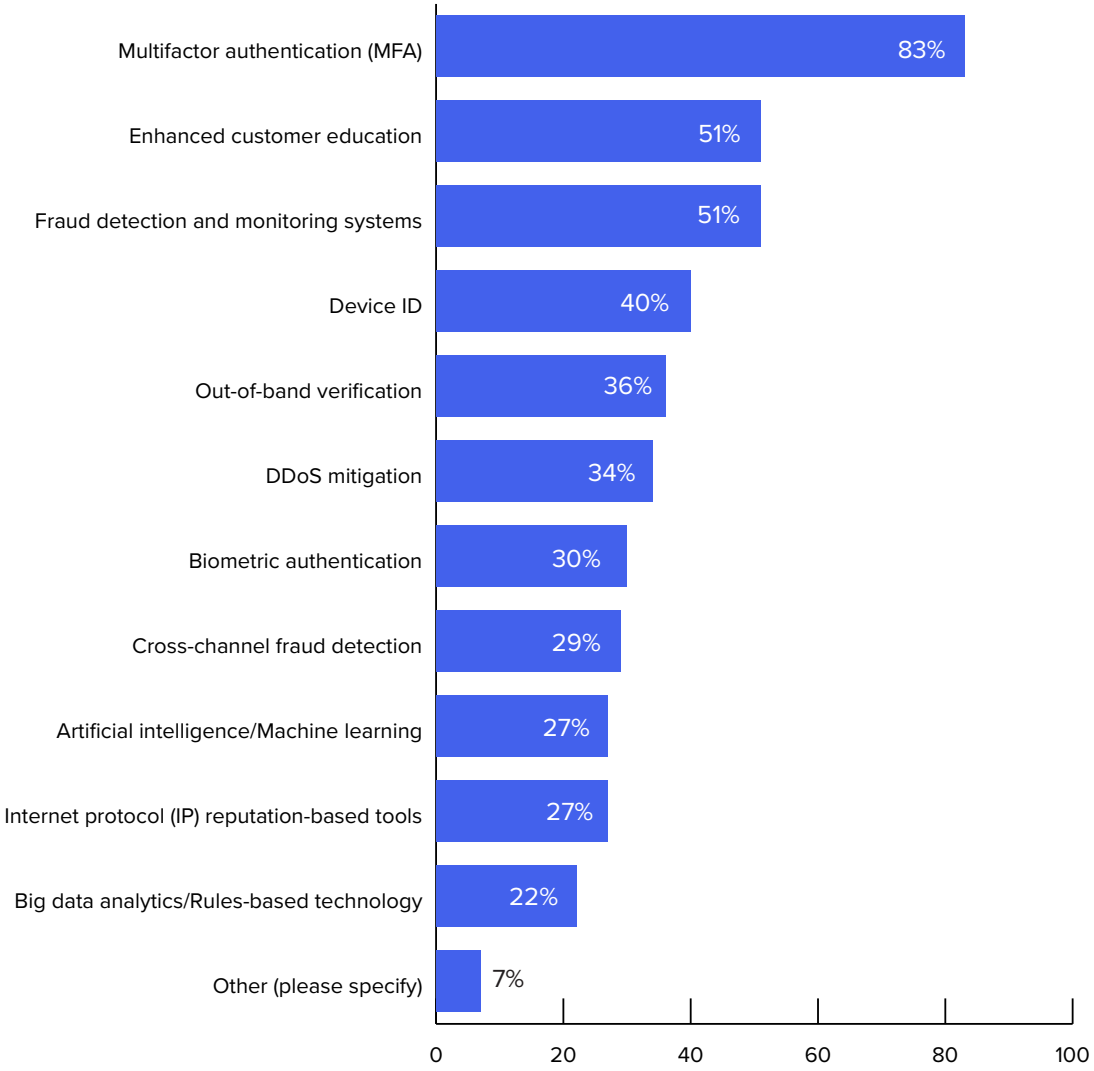
The most common form of fraud that occurs over the mobile channel is via SMS phishing, or smishing. About 28% of respondents note that this fraud incident occurred within the previous year. Another notable area of fraud via mobile were incidents such as account takeover and synthetic identity fraud. While these may have originated in the mobile channel, they are fraud incidents that occur via all banking channels and are not unique to mobile.



Perhaps the most notable finding from this question is that 42% of survey respondents believe that they had no fraud incidents in the mobile channel. This is somewhat surprising given that mobile banking is now commonplace in the majority of financial institutions and the fraud types that were identified cover a wide spectrum of schemes. It is highly unlikely that financial institutions today are experiencing no fraud in mobile apps and web channels, so a far more likely scenario is that fraud is simply not being recognized or is being miscategorized as having originated in other channels.

Finally, 10% of respondents admit that they don't know if fraud occurred since they lack visibility into mobile channel vulnerabilities.

What security measures have you put in place or do you plan to put in place within the next 18 months to mitigate mobile cybersecurity threats? (check all that apply)

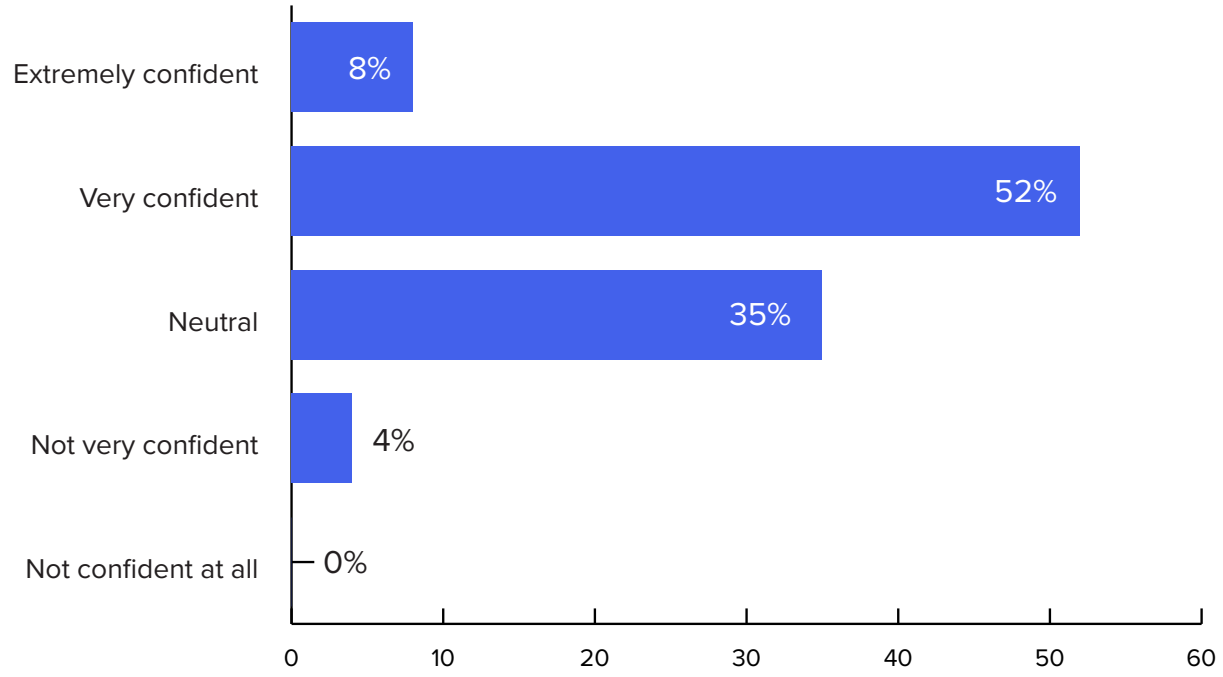


The most common form of increased security via the mobile channel is the addition of multifactor authentication, or MFA, which 83% of institutions either have in place or plan to put in place within the next 18 months. While this is a significant step up from more traditional authentication approaches such as passwords, it is still by no means robust, particularly when sent over insecure channels such as SMS. This security measure may not be so much a result of a bank's desire to increase mobile security as it is to meet regulatory mandates, such as PSD2, that require financial institutions to provide strong authentication to their customers.

Other anti-fraud tools that banks are using include fraud detection and monitoring systems (51%), device identity (40%), out-of-band verification (36%), DDoS mitigation (34%) and cross-channel fraud detection (29%). Note that, with the exception of fraud detection and monitoring systems, all other forms of fraud mitigation are being used by a minority of financial institutions for mobile.

One final area of note: About 51% of financial institutions are relying on enhanced customer education as an anti-fraud tool.

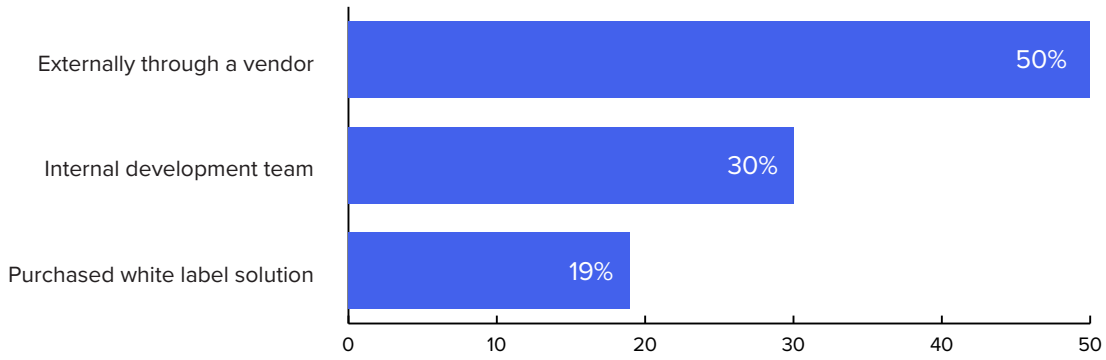
How confident do you feel about the security level on your mobile apps today?



Just 60% of survey respondents are confident about the level of security on their mobile apps, and only 8% of those are extremely confident. This is concerning, given that the mobile channel has a high degree of importance for these institutions. Over one-third of respondents state that they are neutral in regard to confidence about mobile app security.

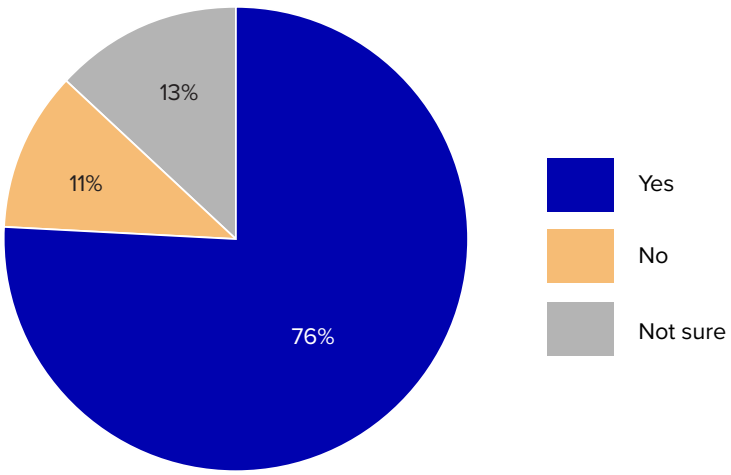
Mobile Banking Security Management and Execution

How do you develop your banking apps/mobile website?



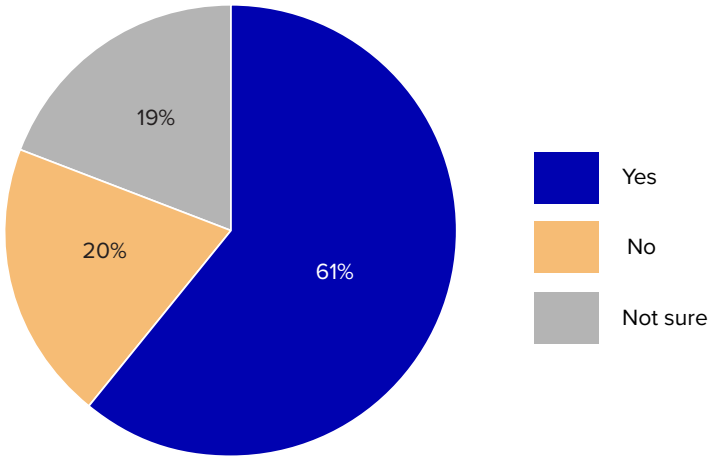
Half of survey respondents have their mobile banking apps and mobile websites developed externally through a vendor, which may explain the respondents' lack of clarity about the security of the mobile channel. Another 19% purchase a white label solution. For many banks and credit unions, it is probably too expensive to have an internal development team dedicated purely to mobile. But security professionals in financial institutions must have concerns about not knowing what third-party vendors are doing in relation to securing mobile.

Data protection is a key component in the compliance of any financial system. Does your organization have a strong understanding of the data that flows through your mobile apps?



Drilling down a little further on the previous question, attendees were asked if they had a strong understanding of the data that flows through their mobile apps. Over three-quarters state that they do, with 11% stating that they don't and 13% not sure. As a security fundamental, security professionals working in mobile banking would be expected to have a thorough understanding of data flow in the mobile channel.

Are you currently running vulnerability analysis and penetration tests for your mobile apps?

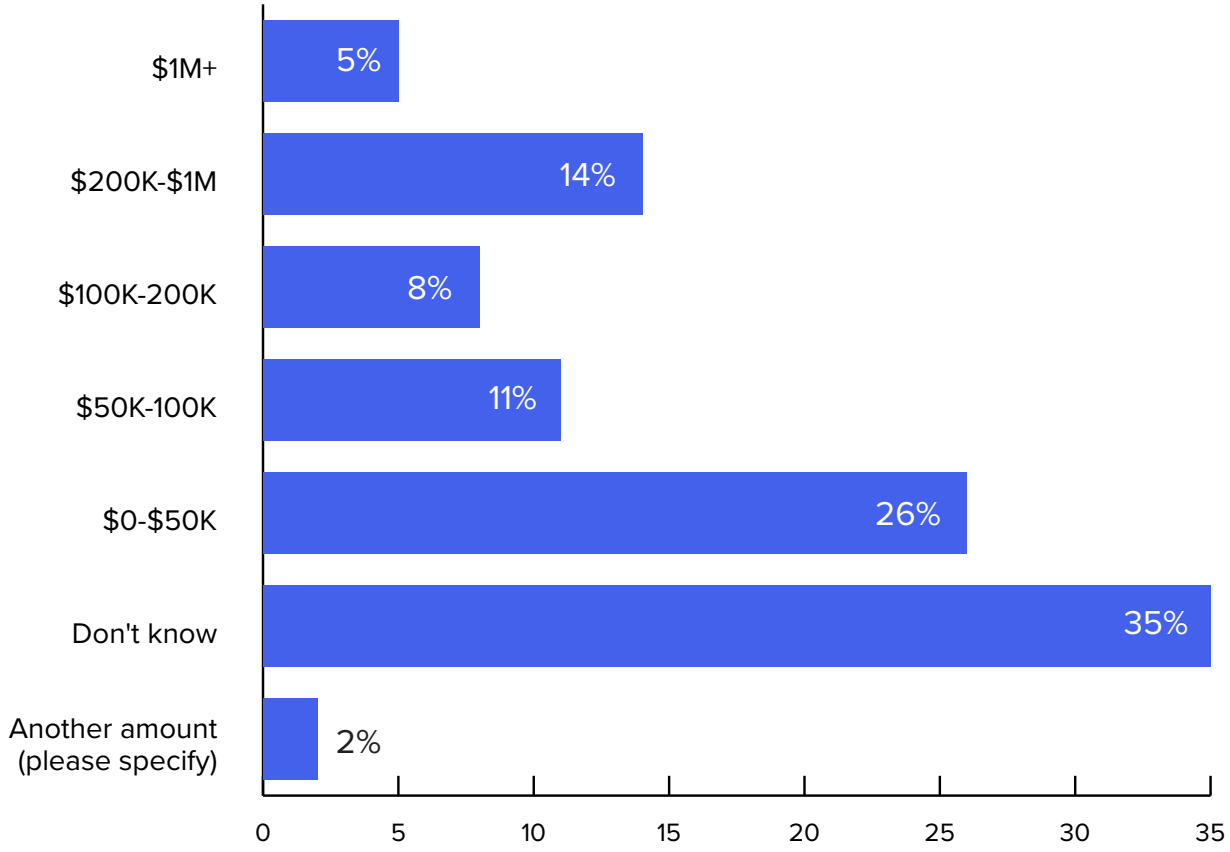


Respondents were also asked about vulnerability analysis and penetration tests of their mobile apps. Just 61% of respondents state that they are currently running these tests on mobile channels, with 20% stating that they are not and 19% stating that they are not sure. Again, banking security teams would be expected to take a more direct role in testing the critical mobile channel.

Those who responded "no" to the previous question were asked why they are not running these tests. Responses included that they expect the third-party vendor who developed their mobile solutions to do this testing or, in a number of instances, that they do not have a mobile channel.

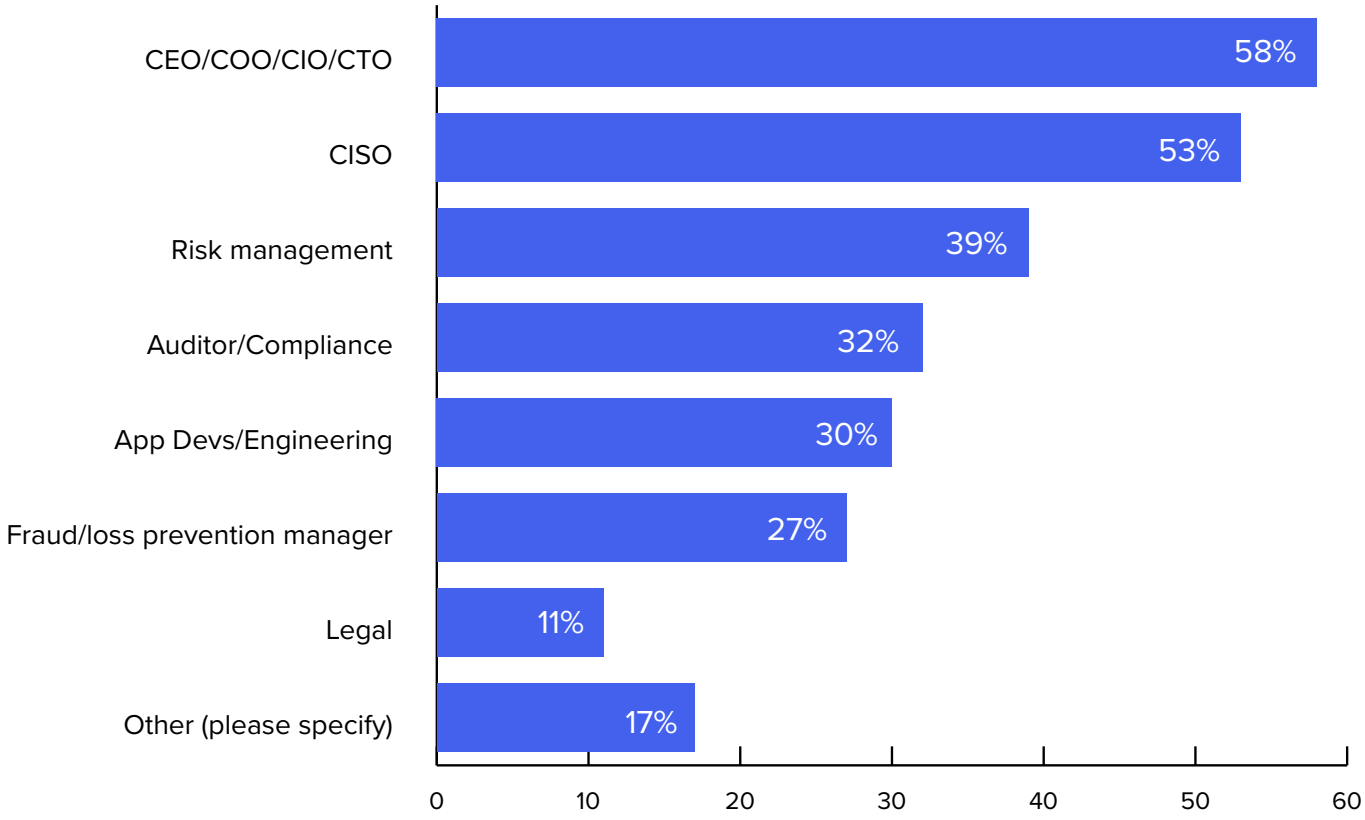
Just 61% of respondents state that they are currently running vulnerability analysis and penetration tests on mobile channels.

In your best estimation, what is your annual spend on security measures for your mobile applications?



Over one-third of respondents state that they don't know what the annual spend on security is for mobile applications. This reflects just how little visibility there is in mobile security for financial institutions. Further, where spend is allocated, it may be insufficient to deal with current-generation threats to mobile. One-quarter of respondents state that they spend less than $50,000 per year on mobile security, and nearly half spend under $200,000 per year.

Who in your organization evaluates, influences or decides on the security needed for the mobile applications? (check all that apply)



The survey shows that the role of evaluating, influencing and deciding on mobile security for financial institutions is not necessarily centralized around the security practice. Just over half of CISOs are involved in this important role, coming second to C-level executives who are not specifically charged with security. Other departments involved in deciding on security requirements for mobile apps include application development and engineering (30%), auditing and compliance (32%), risk management (39%) and fraud and loss prevention (27%). Again, these positions are not typically associated with cybersecurity and fraud mitigation.

Conclusions

SUMMARY

In reaching conclusions about the survey results, it's important to reflect upon the goals of this study, which were to help determine:

- What banking security teams' greatest concerns relating to mobile banking application security are today;
- What types of mobile attacks are most prevalent today;
- How today's banking security executives are mitigating risk in the mobile channel.

Through this research, we learned that:

- The mobile channel and mobile security are seen as critical.
- Financial and reputational risks would be highly damaging to financial institutions if a significant incident occurred to the mobile channel.

However ...

- Over one-third of security professionals in financial services are neutral about the level of security in their mobile apps.
- Nearly half don't think that there have been any significant fraud or cyber incidents in the mobile channel.
- Over one-third don't know what amount is spent on mobile security.
- Just over half of CISOs are involved in the process of evaluating, influencing or deciding on the security needed for the mobile applications.

What does this mean?

The people who should be controlling the security of the increasingly mission-critical mobile channel are not in control. The task is seen as someone else's job, which means there is potential for gaps in mobile security to occur. This situation urgently needs to be addressed.

Trust and safety are big drivers in customers' decision-making process. In a world where the security of a financial institution is no longer determined by visual factors such as the thickness of safe doors and the imposing nature of the branch architecture, bank clients need to see tangible examples of how their hard-earned money is being protected in the digital domain.

Clearly, banks and financial institutions are concerned about security, but they are unsure about how to proceed. Those who are learning about application security and deploying it are gaining the competitive edge. Security will be the driving force in determining which companies will gain customers and grow and which companies will be left behind.

So what's the solution?

- **Security professionals working for financial institutions need to control ownership of mobile security**. Ultimately, if a security incident occurs, the buck stops with them, not with external developers or other internal departments.
- **Financial institutions need to articulate the security measures that they offer in the mobile channel and sell them proactively to the customer base**. Customer churn is increasingly straightforward via digital channels, and financial institutions that think historical loyalty is transposable to the digital domain are naive. Yes, user experience is important, but security and trust are intertwined, and financial institutions are all about trust.
- **Mobile security needs to be treated with the gravity that it deserves**. This is particularly important in the pandemic era when people remain reluctant to visit physical branches. Reputational losses due to a significant security incident will equate to actual losses of banking customers and will tarnish the institution for a long time.

The call to action is simple. The status quo of security isn't cutting it anymore. Treat mobile security with at least the same importance as branch security. Be proactive, and set yourself apart by doing everything possible to prevent mobile security threats.

For more analysis on how to put the survey results to work, see the interview that follows.

SURVEY ANALYSIS

The State of Mobile Banking App Security

Insights From Neal Michie, Director of Product Management at Verimatrix

NOTE: In preparing this report, ISMG's Nick Holland discussed the findings with Neal Michie from survey sponsor Verimatrix. Following is an excerpt of that conversation.

Key Takeaways

NICK HOLLAND: What was your gut reaction to the survey results, and what surprised you the most?

NEAL MICHIE: What surprised me the most was the differential between organizations identifying mobile as their primary channel for interacting with their customers, the primary channel for engagement going forward … and the level of importance they put on security of their mobile channel, whether that was investments and money or even knowing who was responsible for the security of the mobile channel. Mobile is important. Mobile is the future. But we're not focusing in on the security of the mobile channel.

The Mobile Security Gap

HOLLAND: Do you think financial institutions are denying the threats to the mobile channel, or do they just not have the ability to see threats that are occurring?


Neal Michie

MICHIE: The cliche that goes around cybersecurity a lot is that there are two types of organizations: Those that are under attack, and those that don't know they're under attack. These organizations are always under attack. They're big targets with lots of return on investment for the criminals going after them. It's wrong to describe it as denial or naivete. That misses the point. The reality is: Mobile security is falling into a gap between the IT security teams, which are very good at locking down servers and IT infrastructure, and the mobile development teams, which are very good at developing the product and the applications. The IT teams think mobile is the responsibility of the mobile development teams, and they hand it over, and the mobile development teams believe security is the responsibility of the IT security teams.

Security Layers

HOLLAND: In terms of authentication within the mobile apps, the survey shows that most financial institutions have put multifactor

authentication in place or plan to put it in place in the next 18 months. Is that sufficient, given the shifting threat landscape that they’re experiencing?

MICHIE: One of the drivers for that is legislation, like PSD2 in Europe, which is forcing two-factor authentication on payments and money transfers. When security is applied in layers, it’s known to work best, but to do that well, each layer has to serve a purpose. Otherwise, the layers just add bloat and complication for no benefit. Also, the layers need to complement each other in the security solution. You get strength in depth, but you have to be smart about what layers you’re building to get that strength in depth without adding unnecessary complication.

Security Spending

HOLLAND: Over one-third of respondents don’t know their mobile security spend. Why do you think that is, and does it worry you?

MICHIE: It’s an illustration of the gap we were discussing earlier. Not knowing the spend, not knowing the budget or even who’s responsible for that budget is a sign that no one is taking direct responsibility for the mobile security. No one in the organization is saying, “I own this, and I will make sure that it’s safe.”

The Need for Trust

HOLLAND: With the pandemic and remote work, customer onboarding and customer interaction are becoming less about the branch

and more about remote digital channels. Is security going to be more of a customer selling point for financial services apps now than it was prior to the pandemic and the shift to remote channels?

MICHIE: Indirectly, security becomes the selling point, but it is perceived by the customers as trust. Trust and security aren't the same thing, but they are linked. Financial institutions are selling trust. Banking ads on TV present the bank as your trusted companion on the journey of life. Trust is very important to the sale the bank is making to its customers. Trust is an emotional attachment earned through demonstrating over a long time that things work, things don't go wrong, and things progress smoothly. Trust is lost, and lost very quickly, when things go wrong. And a perfect example of throwing away your trust is to have a big, public cybersecurity breach.

The pandemic has accelerated the shift of focus to digital channels – to mobile and web. That means trust in these interaction points is more important than ever for the financial institutions. Security is the foundation that maintains trust and gives consumers an emotional attachment.

Taking Responsibility

HOLLAND: What should security professionals in the financial space be doing, based on the survey findings?

MICHIE: They should find out who in their organization is responsible for the security of the mobile apps and the mobile ecosystem they're building. If they can't find anyone responsible, the CISO or whoever is ultimately responsible for the cybersecurity of the organization needs to know that. Once the CISO finds out who's responsible, the CISO should make sure that those people have the resources to do the job properly – whether that's the right skill set within the organization, the right suppliers or the budgets to plug in vendors who have the knowledge and the products that they need and to make sure that the people are resourced properly to do the job. If not, ultimately, the whole organization suffers once that hard-earned trust is lost.

If a mobile app is valuable to the bank, that's valuable to the customers, and it's going to be valuable to the bad guys. Banks should make sure the bad guys can't get a return on any investment they put in attacking. ■

verimatrix
DRIVING TRUST

Protect Financial Transactions *at SaaS Speed.*

Verimatrix application shielding solutions have been proven through countless security lab pentests and deployed in hundreds of millions of apps – that's why we're trusted by some of the largest financial institutions and payment networks in the world. We protect content, applications, and devices with intuitive, people-centered and frictionless security.

APPLICATION SHIELDING
WHITEBOX
MOBILE PAYMENT

Learn more at
verimatrix.com/fintech

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io