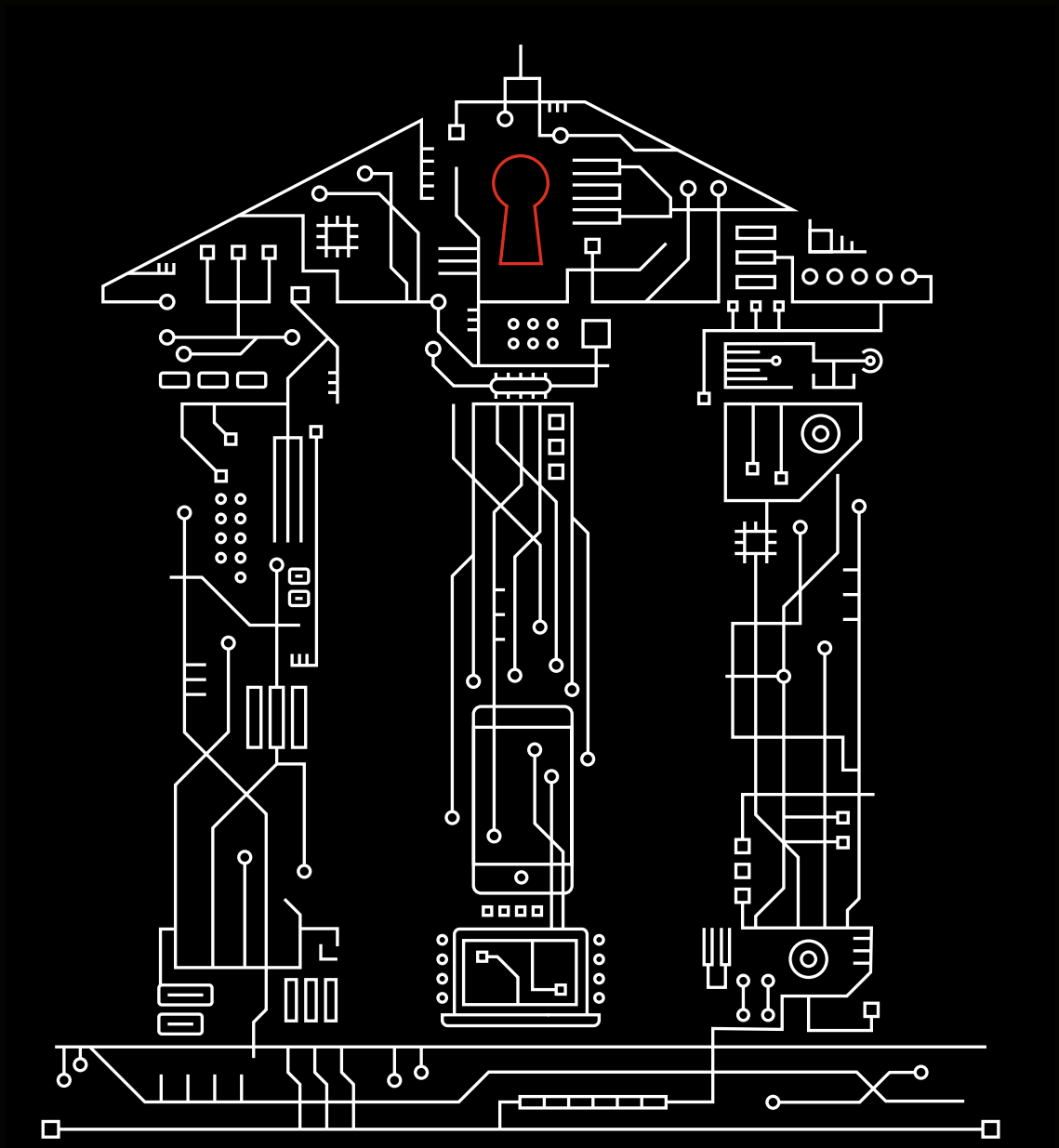
Mobile Security Index 2020

Financial services spotlight

A deep dive into mobile security in the banking, insurance, credit and financial industries



verizon

Could your mobile devices help a cybercriminal get their next payday?

The success of financial services companies depends on their ability to build and maintain a trustworthy reputation. But they're also a naturally lucrative target for cybercriminals. If these companies don't take urgent measures to strengthen their mobile security, they could lose their customers for good.

80%

Eighty percent of financial services companies said that mobile devices are critical to their business.

Mobile technology is helping financial services companies deliver better customer experiences and offer innovative new products. Combined with cloud-based services, mobile is helping give companies the edge. Businesses of all sizes are benefiting—from large banks and payments providers to emerging financial technology companies.

We contracted an independent research company to survey senior professionals responsible for the procurement, management and security of mobile devices. In total, 876 people responded—12% of whom were from financial services organizations. Unless stated otherwise, all data in this report is from this survey.

verizon

Almost half were hit.

Almost half (47%) of financial services companies admitted to having suffered a compromise involving a mobile device in the past year. That's up from 42% in our previous report. These companies know that their business depends on maintaining a good reputation, yet they're not doing enough to protect themselves.

Customers put a lot of trust in financial services providers—they let them guard their money, assets, sensitive data and credentials. But cybercriminals go where the cash is, which makes the sector a lucrative target for attacks. And as the numbers show, often the criminals succeed.

87%

Eighty-seven percent of financial services companies said that cybercriminals see them as a more lucrative target than other sectors.

There's a veritable treasure trove of data at stake. In 2019, a major bank holding company was breached. The hacker gained access through a misconfigured web application firewall and got hold of account numbers, Social Security numbers and credit card applications from more than 100 million customers.[1]

Despite the potential damage to customer loyalty and brand value, 48% of financial services companies admitted they had sacrificed mobile security to "get the job done." As in other sectors, this was shown to have consequences. Financial services companies that said they'd sacrificed mobile security were 2.1 times as likely to have suffered a compromise.

91%

Ninety-one percent of financial services companies said that a good reputation for cybersecurity helps to attract new customers.

48%

Forty-eight percent of financial services companies sacrificed security.

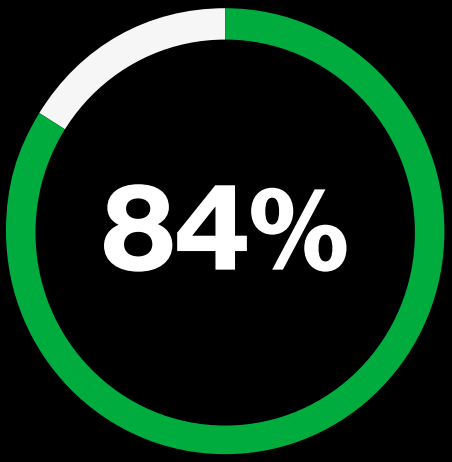
47%

Forty-seven percent of financial services companies suffered a security compromise.

Figure 1. Has your financial services company experienced a security compromise involving mobile or Internet of Things (IoT) devices during the past year? Has your financial services company ever sacrificed the security of mobile devices (including IoT devices) to "get the job done"?

Mobile is transforming finance.

There's no disputing the importance of mobile technology in the financial services sector. It's helping companies transform the customer experience with mobile payment apps, e-wallets and highly tailored insurance policies. It's empowering employees with the data they need to serve customers better, such as easily accessible comparisons of loan, interest and mortgage rates. It's also helping to secure crucial services with two-factor authentication.



Eighty-four percent of financial services companies said that within five years, mobile will be their primary means of access to cloud-based services.

The risks of mobile and the cloud

Mobile and the cloud are becoming more intertwined. In fact, 84% of financial services companies said that within five years, mobile will be their primary means of accessing cloud-based services. For most, the cloud is now the default choice for building and running apps. Sixty-eight percent said that over half the new business information they create is stored in the cloud.

Most financial services companies massively underestimate the number of apps being used in their organization. Thirty-eight percent said the number was under 100. Just 8% said that they use over 1,000. The average is actually much higher.

Fear of being held to ransom

Financial services companies are concerned about mobile device threats—85% rated the risk to their business as moderate to significant. They said they're worried about a wide range of threats, including emerging ones like "cryptojacking." But the threat they felt the least prepared to deal with was ransomware (23%); although these attacks have been around for years, they're getting more sophisticated. Financial services companies also felt unprepared for threats related to employee behavior, like staff using devices to access adult or illegal content (20%).

Financial services companies said they are worried about a wide range of potential security breach consequences, including the loss of intellectual property (57%), damage to the company's reputation (56%) and being hit with regulatory fines (53%). But their biggest concern was the potential exposure or theft of data (60%), particularly customers' personal details or bank account information.

Hackers aren't the only danger.

Financial services companies know they're a target for cybercriminals looking to make a quick buck. But "insider threats" were also a significant concern. Seventy-nine percent of financial services companies said they think their employees are the greatest risk when it comes to mobile devices. Despite this, only 41% of financial services companies said they gave their employees ongoing training on IT security.

It's true that employee actions, even if inadvertent, can expose companies to greater risk. These range from installing unapproved apps to connecting to insecure public Wi-Fi hotspots. But with so many companies knowingly sacrificing security and those responsible for setting mobile policies breaking the rules themselves, is it fair, or good risk management, to expect better from employees?

Financial companies could be doing more.

Despite the high stakes, many financial services companies are failing to take basic precautions. Less than half (49%) said they changed all default and vendor-supplied passwords. And only 46% restricted access to data on a need-to-know basis. These are two of the most fundamental security measures, along with regular security testing and encrypting data sent over public networks. Only 16% of financial services companies had all four of these basic precautions in place.

And despite growing use of the cloud, many financial services companies are failing to secure their cloud-based apps and services. Less than half (48%) said they restricted the use of cloud apps without a proven security rating. And only 51% said they restricted the functionality of cloud apps when accessed from unknown networks or locations. Failing to take basic precautions like these can put customer, employee and business data at greater risk.

1,300

According to Netskope, enterprises use an average of almost 1,300 apps and cloud services, 95% of which are unmanaged, with no IT administration rights or even visibility.[2]

95%

Ninety-five percent of financial services companies said that even a few minutes of downtime could have a lasting impact on their reputation.

79%

Seventy-nine percent of financial services respondents said that they personally used public Wi-Fi for work tasks, even though it was explicitly prohibited by company policy for 32% of them.

92%

Ninety-two percent of financial services companies said they think organizations need to take mobile device security more seriously.

20%

According to NetMotion, 20% of mobile workers list a restrictive IT security policy as their most frustrating issue at work—"cumbersome authentication" came fifth overall.[3]

43%

Forty-three percent of financial services companies that had experienced a compromise said that their mobile security spend had increased significantly in the coming year.

91%

Ninety-one percent of financial services companies that experienced a mobile-related compromise said that the effects were major, and 51% said that it had lasting repercussions.

Financial services organizations' biggest mobile security concerns

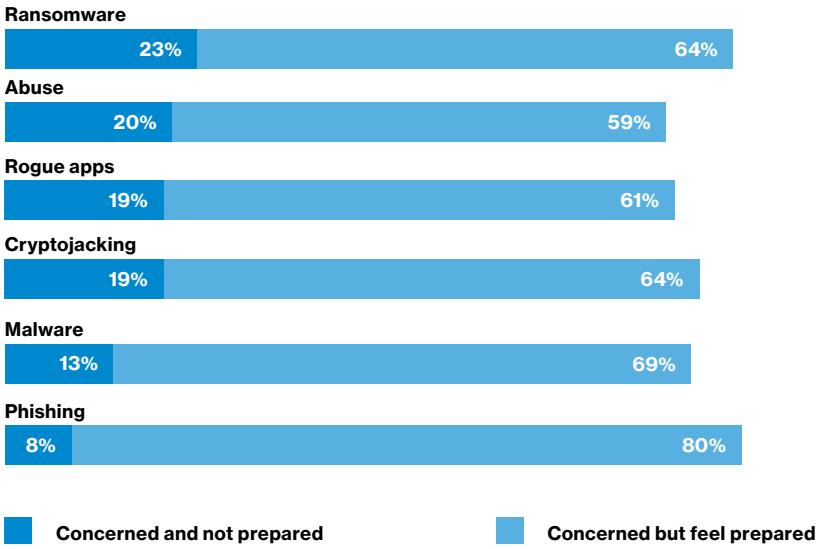


Figure 2. Please indicate how you feel about the following threats/vulnerabilities.

Why are they failing to act?

The top three reasons respondents gave for sacrificing security were expediency (69%), pressure to meet profitability targets (47%) and convenience (42%). This suggests that it's not just budget considerations that are holding financial services companies back—decision makers are also concerned about the impact that security measures can have on efficiency.

Badly designed or implemented security policies can be bad for the employee experience and company performance. Something as simple as a password policy could impede employees' productivity, increase support costs (due to more resets) and potentially increase risk (by driving employees to circumvent the rules).

Security shouldn't be a burden.

On the other hand, well-implemented security solutions can dramatically reduce risk while remaining largely transparent to users. For example, secure mobile gateways, adaptive authentication and zero-trust services can actually reduce the number of intrusive login prompts without putting systems and data at greater risk.

Effective tools can also help reduce the burden on IT teams, improve reporting and increase visibility.

Increase of threat?

The volume and variety of devices using wireless connectivity has grown massively. Smart IoT devices are transforming the finance and insurance sectors. Eighty-six percent of respondents said that IoT devices are crucial to digital transformation.

Financial services companies are using IoT devices to monitor equipment or productivity (82%), the physical security of buildings (68%) and the location of people, vehicles or other assets (61%). For example, IoT-enabled surveillance systems are helping to keep cash machines and bank branches secure. And IoT sensors in homes and cars are helping insurers to improve underwriting accuracy and offer hypertailored insurance policies.

To investigate the security dangers of IoT, we interviewed an additional group of financial services professionals responsible for the procurement, management and security of these devices. Seventy-five percent of them said their business is at risk from attacks targeting IoT devices, rating the risk as moderate to significant. And 29% said they had already suffered a compromise involving an IoT device.

Despite their fears, 54% said they'd sacrificed IoT security to "get the job done." Why are they cutting corners? Expediency. Fifty-three percent said that time pressure was behind the decision. In the drive to get to market quickly, security often takes a back seat. Twenty-seven percent said IoT device security isn't a priority for version 1.0; it's something they can "worry about later."

Securing your IoT devices

Fortunately, there's a lot that can be done to improve IoT security. As well as following our recommendations for all mobile devices, implementing these four IoT-specific best practices could help you protect your organization:

1. Review security before you buy anything.
Whether you are buying off-the-shelf solutions or components to build your own IoT devices, ask potential vendors to supply details of the security measures they take and review them for robustness. Pay particular attention to their authentication, encryption and patching policies. Seventy-six percent of respondents said they had IoT devices in remote or difficult-to-access locations. Use over-the-air (OTA) updates to help keep these devices secure.

2. Harden all devices before attaching them to your network.
First make sure that the device itself is tamper-resistant and tamper-evident. Then make sure you change all default or vendor-supplied passwords. Also, reduce exposure by shutting down anything you don't need—if you're not using a port or protocol, block it.

3. Encrypt data in transit and at rest.
Eighty-three percent of respondents said that they are collecting personally identifiable information (PII), and 25% of those weren't encrypting it. Encrypting data can make it useless to hackers and help you mitigate the risk of a reputation-destroying data breach.

4. Use an IoT platform.
Choose an IoT platform that enables you to monitor and manage all your devices easily. This can help you reduce vulnerabilities by implementing digital certificates and other security features. An IoT platform can also help mitigate attacks by limiting the potential damage of SIM theft by binding SIMs to devices.

72%

Seventy-two percent of financial services companies said they think IoT devices are the greatest security risk facing organizations.

64%

Sixty-four percent of financial services companies said they think the risk associated with IoT devices has increased in the past year.

43%

Forty-three percent of financial services companies that were using IoT said they had at least one full-scale deployment.

Don't wait until you get bitten.

Forty-three percent of financial services companies that had experienced a compromise said that their mobile security spend had increased significantly in the past year, and 57% said they expected it to increase significantly in the coming year. The corresponding numbers for those that hadn't suffered a breach were just 28% and 20%.

While it's good to see that companies are taking steps to rectify mobile security issues, it's worrying that so many seem to wait until they personally suffer a compromise.

The consequences of a mobile-related security breach can be serious and the repercussions lasting. Financial services companies are often hit particularly hard. Ninety-one percent of those that suffered a compromise said the effects were major—a bigger proportion than in any other sector. And 40% said remediation was difficult and expensive.

Don't wait until you discover a breach to rethink your mobile security. It's time to act.

Next steps

MSI 2020 main report
This spotlight is an offshoot of the full Mobile Security Index (MSI) 2020 report. The extended report provides more detailed statistics and analysis of the threats facing mobile devices. It includes interviews with security experts, including an FBI Unit Chief and Verizon's Chief Information Security Officer (CISO).

MSI 2020 security assessment tool
This online assessment tool uses insight from the MSI report to rate your organization's mobile security maturity in four key areas: understanding, perception of risk, exposure and preparedness. Use it to identify where to focus to improve your security posture.

MSI 2020 acceptable use policy guide
This 10-step guide can help you build a comprehensive acceptable use policy (AUP) that helps your employees understand what is, and isn't, acceptable when using mobile devices. This can help mitigate the risk of threats like malware and phishing.

Recommendations

Users:

- Establish a formal AUP that specifies responsibilities for bring-your-own device users, what networks can be used and what apps users can install
- Adopt a security-first focus, give all employees regular training and make sure users know how to report anything suspicious
- Set and communicate a password policy covering strength, reuse and two-factor authentication

Apps:

- Restrict access to data on a need-to-know basis
- Limit employees to installing apps from vetted sources, and block those downloaded from the internet
- Ensure that all patches are installed promptly

Devices:

- Change all default and vendor-supplied passwords—and avoid reusing the same ones
- Implement policies to lock down and isolate vulnerable, infected, and lost or stolen devices
- Use a mobile device management solution to simplify patch management and enforce your AUP, including authentication policies
- Deploy mobile threat detection software to regularly scan for vulnerabilities

Networks:

- Encrypt all data sent over unsecured networks
- Educate users on the dangers of public Wi-Fi, and block the use of unknown or insecure Wi-Fi networks
- Consider adopting a zero-trust approach

Cloud services:

- Restrict the use of unvetted cloud apps, especially file-sharing ones
- Limit access to cloud services to devices that use trusted networks or VPNs

For more information, visit enterprise.verizon.com/msi

About the Verizon Mobile Security Index

Now in its third edition, the MSI is a leading source of information on mobile security. This year, we commissioned an independent survey of 876 professionals responsible for buying, managing and securing mobile and IoT devices for their organization. To add further insight, we worked with Asavie, IBM, Lookout, MobileIron, NetMotion, Netskope, Symantec, VMware and Wandera, all leaders in mobile device security. They provided additional information, including incident and usage data. We also worked with the FBI and the U.S. Secret Service. We'd like to thank all of our contributors for their valuable contributions in helping us present a more complete picture of the threats impacting mobile devices and what is being done to mitigate them.

verizon

1 "A hacker gained access to 100 million Capital One credit card applications and accounts," CNN, July 30, 2019
2 Netskope Cloud Report, Netskope, August 2019, https://resources.netskope.com/cloud-reports/netskope-cloud-report-august-2019
3 Employee Frustration Index, a survey of 285 individuals covering a wide range of age groups and device types across North America, NetMotion, September 2019, https://www.netmotionsoftware.com/blog/connectivity/mobile-frustration-index