Mobile devices could put your agency at risk. Are you ready?

Report

Mobile Security Index 2019 — Public Sector

82% of government organizations said the risks associated with mobile devices are serious and growing. Our research suggests they're right.

When organizations experience a data breach, they typically only share details when they have to – when customers need to be notified about payment card details or other personal information being exposed. Organizations rarely make public facts like how the attack started. Our latest research shows that mobile-related compromises are a growing problem.

The public sector hasn't seen any improvement

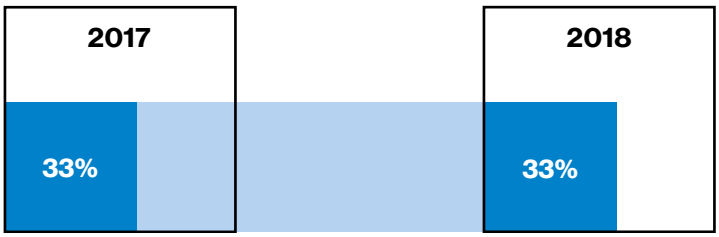

Figure 1. [Have you] experienced a security breach involving mobile devices during the past year?

In the previous Mobile Security Index, 27% of companies admitted they'd suffered a compromise that involved a mobile device. Our latest survey found that number has risen to 33%.

Looking at government organizations (including federal, state and local), there has been no increase in the proportion of organizations experiencing a compromise since last year. But there has been no improvement either. A third (33%) of public sector organizations reported being compromised, putting it in line with the all-sectors figure.

Malware (59%) and phishing (45%) ranked as the two biggest causes of mobile-related compromises affecting public sector organizations.

Are mobile devices an open door for cybercriminals?

Mobile devices might not hold much proprietary data, but they are increasingly used to access core business systems holding citizens' and employees' personal data and other sensitive information. All of this could be at risk if a mobile device is compromised.

Mobile breaches led to other devices being compromised

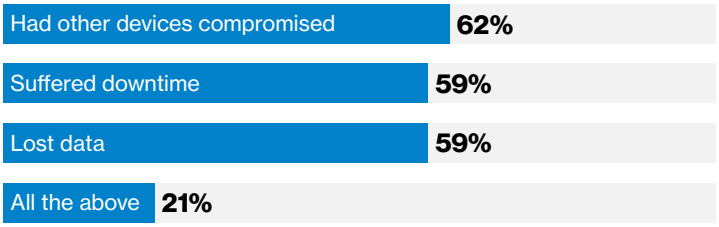

Figure 2. Which of the following consequences did your organization experience as a result of that security breach?

More than just data is at risk – compromises involving mobile devices affected other devices in government. Of those government organizations that experienced a mobile-related compromise, a third (36%) reported Internet of Things (IoT) devices were compromised too. A mobile security breach could unknowingly bring critical services to a halt. This could result in a city in gridlock or emergency services unable to respond to an incident. A fifth of government organizations that were compromised said the consequences were "major."

Mobile Security Index 2019
Verizon contracted an independent research company to survey over 600 US professionals responsible for the procurement, management and security of mobile devices. This included tablets, laptops enabled with Wi-Fi or cellular connectivity, and connected devices, as well as mobile phones. We teamed up with leading mobile security and management companies – IBM, Lookout, MobileIron and Wandera – to provide additional insight.

Most organizations are confident. Over confident.

Like all the industries we looked at, the public sector was pretty confident that its defenses were effective (81%) and that it would be able to spot a compromised device quickly (76%). Despite this, a third of government organizations suffered a mobile-related compromise.

> Organizations are still leaving mobile devices exposed to a degree they'd never tolerate for other IT systems. 57% of public sector respondents said they are less confident about the security of their mobile devices than other IT assets, including desktops and servers.

That's hardly surprising given that many government organizations don't have solutions in place that could help them mitigate the risks. Of the industries surveyed, the public sector was least likely to rate its employees as highly knowledgeable in mobile security – only one in eight (12%).

A strong starting point would be setting out a clear acceptable use policy (AUP) – only 51% of government organizations have one in place. Solutions like unified endpoint management (UEM) could also help – just 27% reported having this.

Legislation is driving action.

Public bodies are already required to disclose information. But new legislation on data privacy is proving a driving factor in organizations doing more about mobile security.

Increased regulatory penalties forced public sector organizations to reassess security spending

Figure 3. Do you agree with the statement "The threat of increased regulatory penalties has been a major driver of increased security spending over the past year"?

General Data Protection Regulation (GDPR) was clearly the big regulation news of 2018. While this applies to organizations trading in the European Union, it's already proving to be a catalyst for tighter legislation in the US. For example, the California Consumer Privacy Act, introduced in the second half of 2018, gives people the right to know what personal information is being collected. As more states introduce their own legislation, both public and private sector organizations are going to have to continually reassess their approaches to data privacy and security.

Many public sector organizations also have to comply with the Payment Card Industry Data Security Standard (PCI DSS). This regulation provides a solid framework for building strong security policies and procedures. But our annual Payment Security Report has found that the majority of organizations struggle to maintain compliance between annual assessments.

Legislation requires organizations to meet minimum standards. And regulations, like PCI DSS, can provide organizations with a useful basis for building effective security programs. But with the threat landscape changing so quickly and the stakes so high, it's crucial that organizations don't wait to be forced to act.

It's time to act: Find out more about mobile security.

Mobile Security Index 2019
Read the Mobile Security Index 2019 to help you assess your own environment and calibrate your mobile defenses.

Read the full report >

Executive Summary
Short on time? Get the key findings of the main report in our Executive Summary.

Read our summary >

Other Verizon security publications.

Data Breach Investigations Report
For over a decade, our Data Breach Investigations Report (DBIR) has been one of the IT industry's most respected security publications. Based on analysis of thousands of confirmed data breaches and hundreds of thousands of security incidents, it offers unparalleled insight to help you understand the threats and prepare your defenses.

Download the latest edition >

Payment Security Report
Almost half of organizations that achieve PCI DSS compliance fail to maintain it until their next annual assessment. Read the Payment Security Report to discover which controls they didn't have in place, and how you can avoid the same fate.

Download the latest edition >

enterprise.verizon.com