The Growing Case for Corporate-Liable Mobile Devices over "BYOD" in Financial Services

Sponsored by verizon

Presented by AMERICAN BANKER

Financial services firms are raising an alarm about mobile device security as federal regulators continue to crack down on improper record keeping at a number of banks and brokerages. Some executives are questioning whether Bring Your Own Device (BYOD) practices — and the consumer apps that frequently accompany them — are sufficiently airtight from a risk and compliance perspective. "Mobile security is part and parcel of a company's overall security posture. As security practitioners, we have noticed mobile devices contributing to mission-critical operations," says Jude Fils-Aimé, Managing Partner of Enterprise Security for Verizon Business Group.

Recently, the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) once again levied hefty fines on a group of financial institutions for failing to keep proper records of business communications, ordering them to pay a combined $549 million[1]. In an even larger action last year, regulators fined several top-tier Wall Street brokerages and banks a collective $1.8 billion for violations related to widespread use of consumer messaging apps and poor business recordkeeping[2].

A relatively lax attitude toward personal devices at work has been a lingering side effect of the pandemic era. During the national emergency, the abrupt shift to remote work required some enterprises to be unusually flexible about allowing employees to use their own mobile phones for business as they quickly pivoted to working out of makeshift home offices.

BYOD Became Routine — But Remains Risky

"Expediency made BYOB the flavor of the day. During COVID, when people suddenly moved to working from home, some requirements were relaxed. In particular, many people started using consumer messaging apps, bypassing their firm's chosen message archive system," says Fils-Aimé.

Even before the pandemic, a trend toward "the consumerization of IT" caused work and personal functions to become increasingly intertwined on employees' computers and phones. As the line between business and personal is increasingly blurred, particularly for younger workers, BYOD was extremely popular with employees for the flexibility and freedom of using personal phones for work. This opened the door to increasing use of consumer communications apps in the work setting. Employees on their own devices at work easily revert to favorite communications apps instead of strict corporate protocols.

Still, in a tight labor market, companies remained lenient about using personal phones. "During the Great Resignation, people tended to leave or migrate to organizations that allowed them to do what they wanted with their devices," says Fils-Aimé. After all, consumer apps were beneficial in corporate environments in some ways — they raised the bar for user experience and empowered employees to meet customer needs during a crisis period. "But within a highly regulated industry like finance, consumer apps must be able to produce communications that can be logged and retained to create records of interactions — and retried later, if they're needed," according to an August article from *Insider Intelligence*[3]. In recent years, cases of financial crimes or scandals have been discovered because of digital messages preserved in chat rooms. It remains critical for business communications to be handled according to protocols.

How Threat Actors Can Leverage Personal Phones

There are multiple ways for threat actors to leverage a mobile device and jeopardize an individual or enterprise. They may be able to "jailbreak" a device by unlocking the operating system to bypass security features in order to load applications. By loading malware on a device, they can often enable location-based services or push notifications that provide opportunities to intercept communications. Criminals can also hijack a device's connected network and cloud sessions. If an employee goes to a coffee shop and joins an unsecure hotspot, a threat actor could launch a man-in-the-middle attack to impersonate the user by stealing their credentials and sending emails or messages to the individual's employer.

Increasingly, C-level executives are being targeted with phishing, smishing and vishing attacks. For example, bad actors can deploy SMS phishing to hijack an executive's personal phone number. "From there they are able to hijack

[1] Insider Intelligence | eMarketer, "Regulatory crackdown on bankers' use of WhatsApp and texts enters its second round with another $549 million in fines," August 11, 2023.
[2] Barrons, "Wall Street's Biggest Banks Fined $1.8 Billion Over Use of Banned Messaging Apps," September 28, 2022.

your credentials or lure you to a 'watering hole' website built specifically around your business segment," says Fils-Aimé. They can combine personal data obtained from the dark web or past data breaches to manipulate not only the individual's financial accounts, but their corporate accounts — including sending messages to the financial institution that appear to be from the executive, leading to the potential for corporate intellectual property to be exfiltrated. Corporate-liable devices preempt many headaches, because they can be set up with controls to allow only compliant communications apps and message archiving.

"We've observed this evolve for our customers, where shifting to corporate devices reduces the risk of enabling a richer set of communication options for employees. This bridges the mobile modalities for text, voice, enterprise collaboration and even consumer applications...." says Blane Warrene, Vice President of Product Management at Smarsh, a provider of message archiving and compliance solutions for financial services companies.[4] "This model enables an organization to leverage efficiencies of automating devices and services — while their employees can move fluidly from office to home and beyond with the right tools to serve customers."

Pendulum Swinging Toward Corporate-Liable Devices

In the wake of the regulatory actions, many financial institutions are reexamining their risks and liabilities around messaging and communications. Companies have become less confident in their defenses around mobile security. "After Goldman, J.P. Morgan and others were levied fines, many firms are slowly but surely realizing the lack of visibility they have on mobile security from a risk posture," says Fils-Aimé.

At this point, the market appears to be beginning to favor corporate-liable device programs versus BYOD. Risk officers are reverting to the more conservative position that regulated firms are safer when they deploy regulated mobile device solutions. When personal devices and messaging apps are widely used in a corporate environment, enterprises lose the ability to control costs and ensure compliance.

Risk and compliance officers are reconsidering the dangers associated with employee-owned smartphones and other connected devices. When personal phones are widely used in a business setting and there are no controls over usage, "It's impossible for IT departments to enforce governance with corporate and legal requirements," according to *Insider Intelligence*.

There are also legal risks. "Who is responsible for company data versus employee privacy? What if a breach or attack is spawned from a personal mobile device?" says Fils-Aimé.

As companies note the increase of malicious apps, phishing and other cybercrimes, some have shifted back to corporate-liable phones. "In the financial sector, corporate-liable phones are becoming more of the protocol," says Fils-Aimé. In the past, all verticals—including financial—took a ham-handed, draconian approach," says Fils-Aimé. Employers were given devices strictly for business use and were forbidden to check personal texts or their own financial accounts. Unlike with past rounds of corporate-issued mobile phones, there are now more employee-friendly variations available.

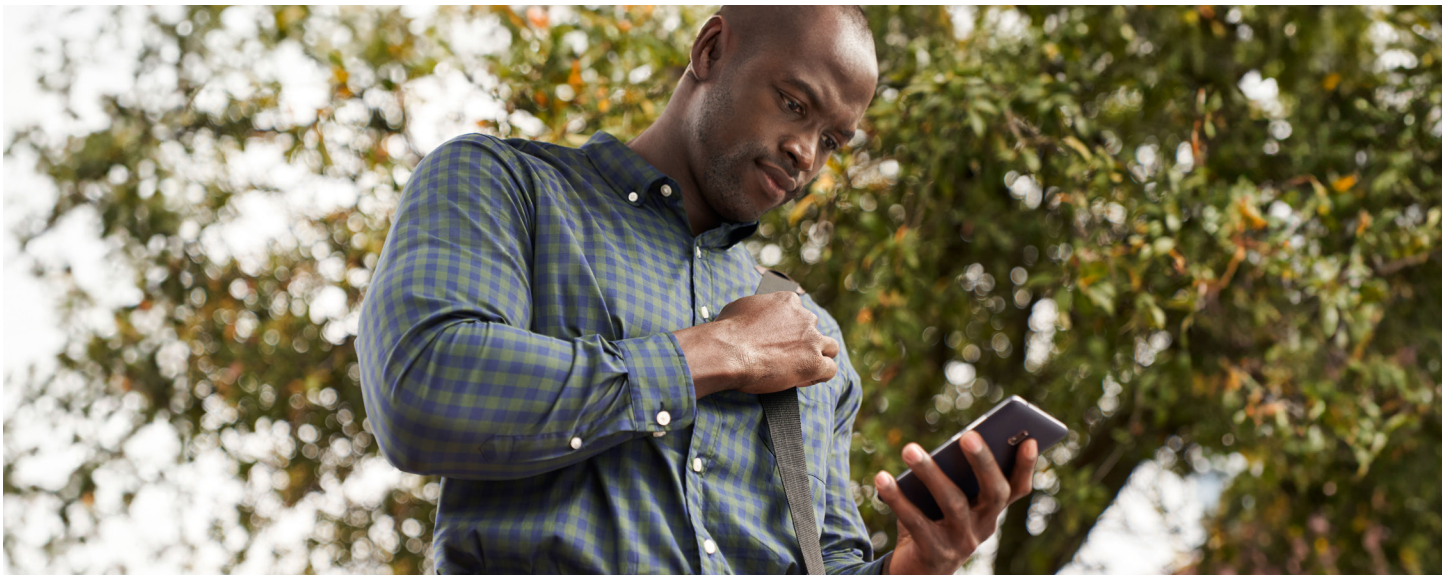
A New Happy Medium – Corporate-owned, Personally-Enabled

The latest trend is COPE: corporate-owned, personally enabled. With a COPE policy, "the company purchases the device, but it gives employees a choice of devices. Personal use is allowed, but it is 'sandboxed' in its own container," says Fils-Aimé.

"Both profiles [business and personal] are using the same 'bare metal' device, but it is bifurcated at a software layer so you have access to both your corporate view and your personal view. You can see both profiles seamlessly, without having the chore of logging in and out," he says.

A COPE strategy ensures that enterprises can keep visibility and control over the mobile devices for security purposes, without being intrusive about innocent employee actions such as checking their personal email account or logging in to their bank. "But, if we see that the user clicked on a malicious link, we can prevent any exposure to malware before it is

[3] Insider Intelligence | eMarketer, "Regulatory crackdown on bankers' use of WhatsApp and texts enters its second round with another $549 million in fines," August 11, 2023.
[4] Blane Warrene, "Employee or Corporate Owned Devices: The Tough Choice for Organizations in Regulated Industries," July 19, 2023.



downloaded and pushed to the device. If someone clicks on a known bad site, or there is a phishing campaign underway that is known, we will stop that connection before it can spawn within the organization," says Fils-Aimé.

"Theoretically, if a firm issues a corporate liable phone, they can better control the apps that can be loaded on it. If a firm permits a BYOD phone, the firm can segment off part of the phone for business, but they can't control the rest of the phone," he says. IT departments have greater controls and ability to ensure mobile security by managing access to the apps that employees need, keeping apps updated to the latest and most secure versions, and providing backup for devices in case of loss or breakage.

Learn more about how your financial institution can enhance mobile device security while providing flexible and positive experiences for employees with Verizon solutions by reviewing these two documents:

- Improve your strategy for archiving key communications
- How Verizon Mobile for Microsoft Teams can help with compliance call recording and archiving needs

Or contact your Verizon Client Partner.

DISCLAIMER: Verizon continues to work on improving its capabilities and thought leadership in areas where we can support our customers with challenges around mobile device security. There is no silver bullet. In order to solve these challenges, enterprises should take a programmatic approach involving collaboration with IT and security operations, finance, legal and human resources.

Mobile Device Use: Regulations and Acronyms

COBO: Corporate-Owned, Business Only. The phone is selected and owned by the enterprise, and personal use is not supported.

BYOD: Bring Your Own Device. The employee chooses and owns the device, and the primary use of the device is personal.

COPE: Company-Owned, Personally-Enabled. A newer trend in which the employer distributes company-owned devices but employees are able to use them for personal business within established parameters.

CYOD: Choose Your Own Device. Employers offer employees a selection of company-owned mobile phones to choose from.

1934 Securities Exchange Act: Proper recordkeeping is part of this regulation governing financial institutions.

Rule 17a-4: The SEC updated this rule to include recordkeeping requirements for electronic customer records and communications.

Rule 18a-6: This SEC rule was also modernized to govern recordkeeping for electronic records, which must be properly stored and able to be promptly furnished when requested.

PCI-DSS: An information security standard for credit card payments from the Payment Card Industry Security Standards Council.