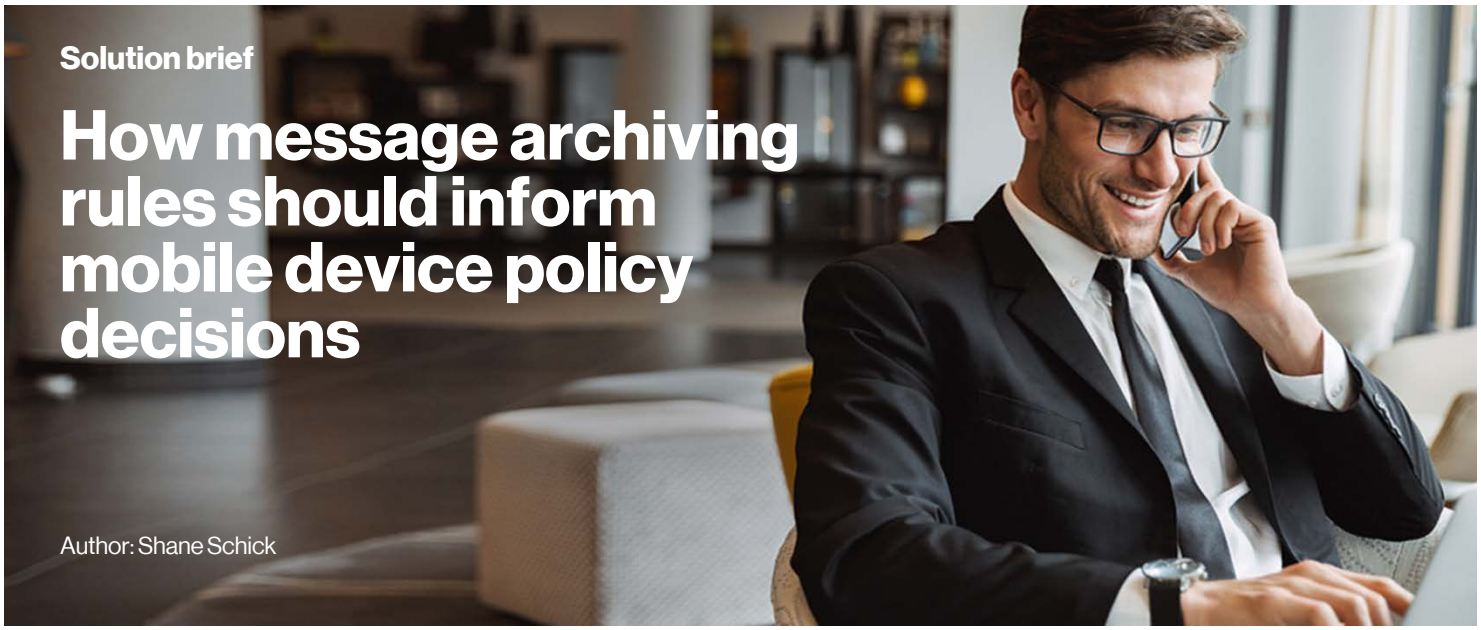

Solution brief

How message archiving rules should inform mobile device policy decisions

Author: Shane Schick

The commercial and consumer communications tools and solutions have changed how people share information. But for the financial services sector, while technology may have changed, the requirement to comply with regulations such as message archiving rules has not.

Message archiving requirements

The SEC regulations require financial companies to securely archive all business communications related to certain regulated activities. Many finance employees have been using their own phones, known as Bring Your Own Device (BYOD) to communicate and send text messages to exchange sensitive information. This practice is placing financial services companies at risk of non-compliance and subject to heavy fines.

Each company establishes its own record retention policy that defines rules that addresses what information needs to be retained, under what circumstances a record is to be made, when that record is to be accessible and how long the record should be archived.

How sensitive information increases the risk of exposure

Given changing trends in communications tools and solutions, workplace location, and employee preferences to use their own personal devices, it is understandable why some companies decided to adopt the BYOD policy, where employees use their personally owned devices to connect to their company's corporate network and access company data and sensitive information.

Organizations need to pair their desire for increased collaboration, production and efficiency through mobile devices with a communications policy that avoids the risks of noncompliance.

Advantages of a corporate-liable communication policy

Unlike BYOD programs, which allow employees greater freedom to use personal apps and messaging tools, corporate-liable programs provide IT with increased security and control to protect sensitive information. This includes the ability to configure devices based on business and regulatory requirements and to enroll them in a mobile device management (MDM) platform. That means employees aren't able to bypass security protocols and communicate in ways they shouldn't. It also helps to capture data properly to meet message archiving requirements.

Some possible benefits from adopting a corporate-liable approach may include:

- The IT department, rather than the employee, is responsible for keeping customer, company or employee data out of the wrong hands when devices are lost or stolen.
- Business continuity is less likely to be impacted as IT can back up devices in the event they break down.
- Corporate-liable devices can help boost productivity as they're more easily integrated with back-end systems and apps that ensure they perform as expected. IT management can also ensure employees are kept on the latest versions of the apps they need.
- Corporate-liable devices make it easier to comply with other industry regulations such as the Payment Card Industry Data Security Standard.

verizon

Mitigation best practices

Whether your organization is ready to adopt corporate-liable programs or wants to continue offering BYOD, they can mitigate security risks by creating basic best practices. A few examples are:

- Clearly communicating to employees which devices and apps are permitted and your monitoring policies over sensitive information for such usage.
- Turn to trusted advisers, such as a managed services provider, to explore options, including potential integrations with third-party message archiving solutions and other mechanisms to ensure data can't be changed or erased.

Learn more:

Read more about how to give your employees the reliable mobile connectivity they need to stay productive while keeping your data protected.

For more information, reach out to Mark Bubar (mark.bubar@verizon.com), Verizon's strategy leader for the global financial services sector.

The author of this content is a paid contributor for Verizon.