Ensuring secure and **accessible resources**

Mobile phones and IoT devices require a combination of vigilance and automation

Charles Eagan
CTO, BlackBerry

SECURING DIGITAL DEVICES, including mobile phones and internet-of-things sensors, requires organizations to perform a difficult balancing act. They need to make information easy to share while keeping it safe. If security measures are too cumbersome, employees may try to bypass them.

The ideal solution facilitates secure information sharing without friction. Two key strategies are digital rights management, which involves knowing what users are allowed to do, and authentication, which gives administrators the confidence that users are who they say they are.

As we gather more data on users and their behavior, we can use multiple attributes to increase that confidence. Behavioral analysis and machine learning can build a model of what's normal for users, and when behavior does not align with that model, they could be locked out of the organization's systems or asked to provide another factor of authentication beyond a password.

Preventing users from sidestepping security

Mobile phones have an enormous amount of information on their users — including location, habits and passwords — making them highly desirable targets. Therefore, it's important for organizations to adopt an external management system for mobile devices. For instance, organizations could prevent users from copying and pasting sensitive information from a work email into a personal email account. Or organizations can make it impossible for a user to opt out of having a device password.

Furthermore, organizations need to continuously monitor mobile devices. A potential compromise could show up as any unusual activity — for example, an app that is performing a calculation and suddenly tries to access the device's camera or microphone.

A certain amount of user education is involved, but employees should be able to do their jobs without having to understand the underlying security structure.

Preparing for the IoT tsunami

The internet of things is rapidly changing the security landscape. Wherever possible, organizations should focus their efforts on the IoTs that need to be trusted and avoid having single points of failure. In some cases, organizations might need to overlay permissions or user profiles on devices.

Developing best practices now is essential because a tsunami of connected things is coming. According to Gartner, the number of connected devices is expected to reach 75 billion in 2025. At BlackBerry, we're working on ways to interconnect IoT systems so that they can be secure, private and not vendor-specific. That way, we can make sure the devices' software is updated as needed, and we can detect when security has been compromised. Then, organizations can use unified endpoint management to set and enforce security policies across the IoT environment. ■

Charles Eagan is CTO at BlackBerry.