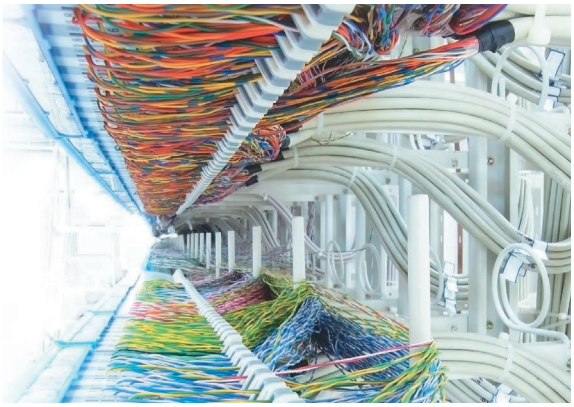
Today's Mobile Security Requires a New Approach



Neal Leavitt

Companies are looking for new ways to secure their data and networks now that many employees are using their own mobile devices in the workplace.

Employees bringing their personal mobile devices to work—a practice known now as BYOD (bring your own device)—is no longer a trend but instead is a model that's here to stay.

In fact, market research firm Gartner Inc. predicts that half of employers worldwide will stop providing devices by 2017 and require employees to bring their own.

While workers might enjoy using a personal device that they're familiar with, BYOD can also result in potential security breaches and risks because these devices access company data and networks outside the control of corporate security directors.

Last June, security vendor Check Point Software Technologies unveiled its second annual mobile-security report, based on a poll of about 800 IT professionals worldwide.

Of responding businesses, about 80 percent had a mobile-security problem in the past year and 42 percent suffered a breach—including information losses, and hackers downloading malware onto or otherwise compromising networks—costing more than $100,000.

The study found that about two-thirds of companies let personal mobile devices connect to their networks, but 63 percent don't manage corporate-information use on those smartphones, tablets, or laptops.

"It's worrying to see such a high proportion of businesses burying their head in the sand when it comes to planning adequately for BYOD," said Richard Absalom, senior analyst at market research firm Ovum.

Many companies are continuing to use traditional approaches—such as passwords, firewalls, and intrusion-detection and -prevention systems—to manage this risk.

However, these approaches are designed to protect against external threats and thus don't completely address BYOD-related issues, which present a problem from within an organization, noted Carnegie Mellon University professor Patrick Tague.

In addition, many of these technologies require companies to control the device they want to protect—as they do with their servers and PCs—and this is not the case with employees' personal devices, said North Carolina State University associate professor Xuxian Jiang.

Instead, stated Matt Bancroft, president and chief operations officer of enterprise applications for security vendor Mobile Helix, companies should focus on encrypting and thus protecting important data, regardless of the device that accesses it.

"Authentication would then be required before decryption of the data could proceed," added Andrew Borg, research director for enterprise mobility and collaboration with the Aberdeen Group, a market research firm.

"Three years ago, it was about protecting the device. Two years ago, it was all about protecting the application. Now, companies are trying to protect the data. Each approach is necessary on some level," said Jonathan Dale, marketing director of mobile-device management vendor Fiberlink Communications.

BYOD SECURITY ISSUES

BYOD began to surface in 2003 but really took off in 2011.

Managed-services provider Logicalis commissioned—and market-research firm Ovum conducted—a 2012 survey of 3,796 consumers in 17 countries

Published by the IEEE Computer Society
0018-9162/13/$31.00 © 2013 IEEE

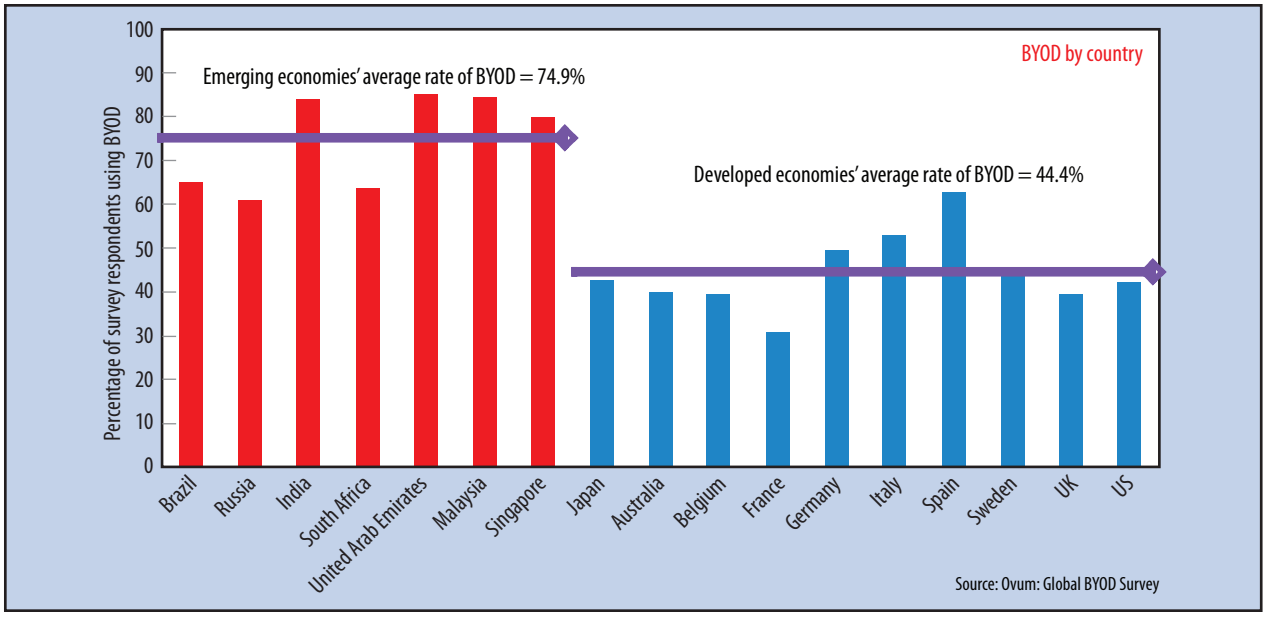


Figure 1. A recent survey showed that many smartphone owners, particularly in countries with emerging economies, use their devices at work.

(www.us.logicalis.com/PDF/LogicalisBYODWhitePaperOvum.pdf).

As Figure 1 illustrates, the survey showed that about 75 percent of users in countries with emerging, high-growth economies such as Brazil, India, Malaysia, and Russia used their own mobile devices at work, as did 44 percent of workers in countries with developed economies like France, the UK, and the US.

Mobile devices have greater capabilities than in the past, which has encouraged workers to use them for some complex tasks at work, said North Carolina State's Jiang.

In addition, proponents say that BYOD increases employee productivity and morale, and makes employers appear more flexible and attractive.

However, BYOD can cause security headaches for employers.

Device vulnerabilities

Tests this year by security vendor Trustwave found that 90 percent of vulnerabilities common in desktop computers were also present in mobile devices, regardless of operating system. This lets hackers conduct many of the same types of attacks on mobile devices that they launch against PCs.

And almost 90 percent of mobile applications tested had one or more security flaws.

Also, the amount of mobile malware, particularly for Android devices, has increased considerably in recent years, said Eric Skinner, security vendor Trend Micro's vice president of solutions marketing.

Smartphones, added Carnegie Mellon's Tague, have a broader attack surface than PCs because they use so many third-party applications and connect to networks in multiple ways.

Mobile Helix's Bancroft said BYOD environments can be easy to hack because employees often use them on insecure public—as well as secure corporate—networks. Workers also frequently employ weak or no passwords.

Some users jailbreak or root their devices—removing OS-based limitations via software or hardware exploits—to add functionality such as the ability to run otherwise prohibited software or overclock their processors.

However, this can also disable OS-level security, said Adam Ely, cofounder and COO of Bluebox Security.

Potential threats

Vulnerabilities could enable hackers to compromise mobile devices and, for example, infiltrate corporate networks, said Berk Veral, vendor RSA Security's senior product marketing manager.

They could also intercept passwords, steal credentials, collect sensitive personal or corporate data, or install malware to take over devices.

Hackers could use malware to monitor and log victims' keystrokes, as well as cause other problems, said John Dasher, mobile-security vendor Good Technology's vice president of product marketing.

Hackers, added Trend Micro's Skinner, could even access a device's microphone and camera to eavesdrop on its owner.

Another problem, he noted, is that employees could lose devices containing corporate

data or leak information via public clouds and networks.

And problems could occur when workers leave a company with sensitive information on their device.

Despite these threats, many organizations don't prioritize the securing of important data, said the Aberdeen Group's Borg.

PROVIDING SECURITY

The approaches to mobile security typically have been the same ones used for years with desktop computers, said Rob Bamforth, principal analyst for business communications with market research firm Quocirca.

Previous mobile-security approaches alone won't protect BYOD environments.

However, this has not adequately solved BYOD-related problems.

Passwords for accessing corporate networks alone don't work because legitimate users with compromised devices could still sign into company systems.

In some cases, organizations have tried to provide security by establishing employee policies—such as enforced corporate-network access via VPNs—for utilizing devices on the job.

However, this doesn't always work, as employees using devices for personal purposes sometimes connect to insecure networks that expose them to hackers and malware that could then affect corporate systems.

And, noted North Carolina State's Jiang, setting policies doesn't guarantee employees will follow them.

Mobile-device management

MDM lets companies inventory, monitor, manage, secure, and apply various policies to employee- or corporate-owned mobile devices used in the workplace, explained Mike Johnson, Logicalis' director of communication and collaboration.

The policies, noted Carnegie Mellon's Tague, could enforce the use of encryption with corporate data, disable sensors to prevent information leakage, and mandate complex passwords.

MDM also enables IT departments to, for example, distribute applications to devices, lock and wipe data from them, and establish and enforce configuration settings.

MDM approaches work via a management application or agent that a company uploads to devices. A corporate server then sends commands to the application or agent.

Examples of MDM products include Fiberlink's MaaS360 and MobileIron's Advanced Mobile Management.

Mark Bermingham, security vendor Kaspersky Lab's director of global product marketing, said an MDM shortcoming is that it uses reactive security approaches, such as remotely wiping data from a device after a problematic event occurs.

He stated that companies also need proactive measures such as data encryption and antimalware software.

MDM doesn't prevent either a hacker from attacking an employee's device, or a thief from stealing it and accessing sensitive data.

And in some cases, a hacker could turn off network access while compromising a device, making it impossible for a company to transmit the erase-data command.

MDM also restricts what workers could do with their devices, which could make it unattractive and reduce productivity.

Unlike the PC world, the mobile environment uses multiple operating systems and platforms. This makes device management too difficult to be the only approach to BYOD security.

"Any security model that relies on device security as its foundation is fundamentally flawed," said Mobile Helix's Bancroft.

Mobile-application management

MAM focuses on managing and limiting mobile users' access to applications, as well as protecting the permitted programs and data they use.

This approach lets companies limit employee access to unapproved mobile programs, manage access to approved applications, securely deploy them to devices, and set policies for software behavior, noted the Aberdeen Group's Borg.

MAM, noted Quocirca's Bamforth, allows only secured mobile applications to access corporate networks and data.

Companies can accomplish this by operating an enterprise store from which employees can access acceptable applications or by isolating untrusted programs from corporate resources.

However, placing a virtual wall around applications can keep them from communicating with one another.

In addition, MAM doesn't protect data or provide fine-grained control that would, for example, enable employees to access corporate information in some settings but not in others.

MAM products include Citrix Systems' XenMobile, Symantec's App Center, and Good Technology's Good Dynamics Secure Mobility Platform.

Cloud storage

Trend Micro's Skinner said some companies have adopted cloud storage, which provides mobile

access to work data and applications, while still providing some information security via encryption.

However, problems can occur if access to corporate information is not properly managed and limited.

And once users download corporate files, a company loses control of them unless it implements technology that isolates them from other parts of a device.

NEW SECURITY APPROACH: DATA SECURITY

Data-centric security is not new. What is different, noted the Aberdeen Group's Borg, is companies' growing awareness of problems caused by unmanaged corporate data on personal mobile devices and vendors releasing products to address this issue.

Elements

According to Mobile Helix's Bancroft, data-security systems include several elements, including a secure enterprise browser for delivery of and access to corporate applications, the isolation of data and applications from other parts of a device, and strong online- and offline-access credentials.

Users could thus do what they want with their devices, but their interactions with corporate data would be secure.

Containerization

In the past 18 months, the concept of *containerization* has become more popular as companies realize the value of separating corporate and personal data on employee's personal devices, noted Fiberlink's Dale.

Containerization creates a separate encrypted storage application or secure virtual storage on a mobile device. According to Mobile Helix's Bancroft, all application and security processes function within the container, independently of OS-based capabilities.

A company-supplied browser also operates within the container, with all traffic to the enterprise network secured via HTTPS, he added.

Workers could still use their personal data and applications without restriction. In addition, companies could wipe corporate information from a device while leaving personal data intact.

Potential challenges include the difficulty of implementing and integrating strong cryptography within the system, said Ray Potter, CEO of encryption vendor SafeLogic.

Most experts agree that a multilayered BYOD-security approach is most effective.

"Organizing a BYOD risk-management plan around a single technical solution can be restrictive," said Steve Durbin, global vice president of the nonprofit Information Security Forum.

The multilayered approach should include steps such as device management, the use of containers, the establishment and enforcement of security policies, access controls, and encryption, according to SafeLogic's Potter.

In the future, more companies will adopt the data-security approach because it will be the most practical way to solve BYOD issues, said Scott Emo, Check Point Software Technologies' head of endpoint product marketing.

"By protecting the data and not the device, the organization can control what's important to the business," he continued. "The approach also won't infringe on the phone owners' ability to do what they want on their device."

In addition, by focusing on securing the data, companies will experience better, more consistent protection in an environment with numerous types of mobile devices.

"Companies are just beginning to understand the need for a data-focused approach to mobile security" said Mobile Helix's Bancroft. "The BYOD trend is here to stay, and so we will see data-focused security solutions gain traction."

Neal Leavitt *is president of Leavitt Communications (www.leavcom.com), a Fallbrook, California-based international marketing communications company with affiliate offices in Brazil, Hong Kong, France, India, and the UK. He writes frequently on technology topics and can be reached at neal@leavcom.com.*

Editor: Lee Garber, *Computer*; l.garber@computer.org

Selected CS articles and columns are available for free at http://ComputingNow.computer.org.

IEEE Intelligent Systems

THE #1 ARTIFICIAL INTELLIGENCE MAGAZINE!

IEEE Intelligent Systems delivers the latest peer-reviewed research on all aspects of artificial intelligence, focusing on practical, fielded applications. Contributors include leading experts in

• Intelligent Agents • The Semantic Web
• Natural Language Processing
• Robotics • Machine Learning

Visit us on the Web at
www.computer.org/intelligent