THE NUTS AND BOLTS OF MAKING BYOD WORK

Mobile technology is changing at an astonishing rate, and employees are increasingly using their personally owned devices for business purposes – sanctioned or not. Organizations, therefore, need to create **bring-your-own-device (BYOD)** policies that will help them mitigate the risks related to having their corporate information stored on employee-owned devices.

Brent Gatewood, CRM

The days of employees using organization-supplied devices for company business are going the way of the Dodo. The bring-your-own-device (BYOD) trend is rapidly being adopted by organizations of all sizes and in all industries. This means that as business information makes its way to personal devices, information governance policies and practices need to be created or revised to ensure the organization's critical assets are properly managed.

BYOD Trend Drivers

For those organizations that had previously adopted standards for their mobile work force using company-owned devices, those standards typically involved a bench of tools (two or three devices) running a particular operating system (e.g., BlackBerry or Windows) that relied on a dedicated backend server environment. Individuals were given devices depending on their needs, and configuration was generally straightforward. Then, the smartphone market exploded.

The proliferation of Apple iOS and Android devices started to create headaches for the IT group. Individuals who didn't want to carry two different devices to access e-mail and information commonly asked, "Why can't I just use my personal device to access corporate e-mail?" Because they had already chosen and purchased the personal devices that best met their needs, those are the devices they preferred to use for their professional lives, too.

The device, however, was not the main concern; there were still challenges back in the server room. How would these new devices interact with the approved and standard systems of the corporate environment? For a brief time, the answer to the request to use personal devices was easy. The infrastructure integrations were not strong enough; therefore, the answer was "no"; an organization's information and e-mail had to be accessed on a company device.

Then, device manufacturers and third-party vendors ascertained that the corporate market could be very lucrative; they quickly adapted their products to work in that environment. The expectation was that systems would work together better and many information services questions could be put at ease. But, as it turns out, connecting devices to information repositories was not the hard part. There were many other issues to be addressed. And, this is where the BYOD conundrum is today.

BYOD Security Challenges

Although the technologies are in place to facilitate a BYOD environment, organizations must now readdress their corporate policies to ensure that their greatest asset – information – is being safeguarded on these mobile devices that are outside of their direct control. This requires them to understand the challenges, the players within (and outside of) the organization, and the tools that must be utilized.

Addressing Device Security

Protecting the organization's information becomes more difficult as it is allowed to become resident on an employee's personally owned smartphone or tablet. Smartphones, for example, are more than "just phones." Many organizations have smartphone applications for their enterprise solutions to allow their mobile workforce to access saved e-mail, documents, and business intelligence or analytics. As such, smartphones can provide a view into the systems that run an organization.

So, what happens when a phone or a tablet is lost, along with all of its contact information, corporate e-mail, and documents? Without proper safeguards in place, the information on these devices is accessible by people who should not have it. That information can be taken out of context and cast into questionable light or used in a competitive situation against the organization. So, it is imperative that this issue be thought through from the beginning.

A mobile device must have a minimum set of protections:

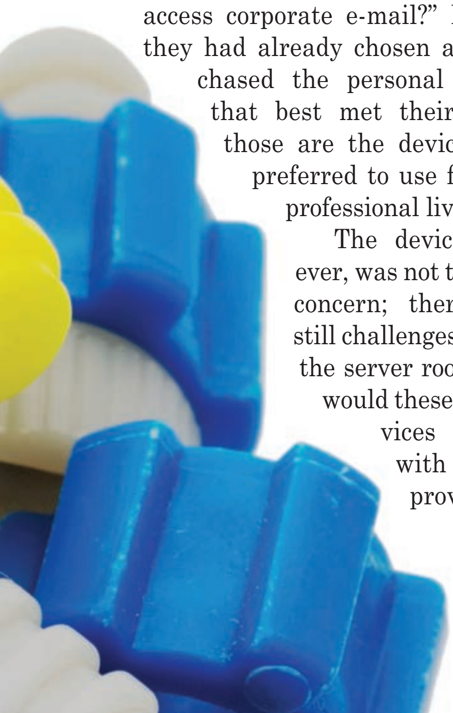
- Passcode – The device needs to be protected with a passcode, preferably one that automatically erases the data after a predefined number of failed attempts to access it.
- Remote lock – The device must be able to be locked remotely, disabling all features except allowing an emergency call to be dialed or allowing an incoming call that would be helpful in effecting the device's return.
- Remote wipe – The device must have remote erase capability.

The organization must also be prepared with a clearly defined protocol for the individual and the organization to follow in the event of a lost or stolen device. It should spell out:

- Who to contact if the device has system access
- What applications on the device interact with what corporate systems
- How the device can be remotely locked or wiped
- What system passwords need to be changed or access temporarily removed

Ensuring System Security

IT professionals, as well as the



various software manufacturers, are familiar with the securities issues surrounding e-mail access and mobile devices. The increasing use of mobile devices to interact with additional and varied repositories creates a set of new questions, including how the organization can:

- Control access to disparate systems
- Ensure the device applications offer secure connections to only specified information repositories
- Be certain that the access granted for these applications is used only as intended
- Audit and manage this mobile traffic

Security must include all of the systems involved. This is where the slope becomes very slippery. For example, in a highly regulated environment, an organization traditionally would choose a DoD 5015.2-certified solution for managing its information at the enterprise level. This certification ensures that certain base security requirements are met and information within the corporate ecosystem is secure. The same level of certification does not exist in the mobile application environment. External access to many of these systems has not gone through that level of testing or certification. In fact, third-party organizations develop many of the applications providing remote access. This instantly changes the security landscape of the system.

A careful organization will mandate that the software vendor addresses access- and security-related issues, such as ensuring that access protocols are secure and that its systems are allowing requests and traffic only from approved applications, devices, and users.

But, here is where the slope becomes even "slipperier." Quite often, an organization cannot be in control, from an individual and device standpoint, in a BYOD environment.

This is because users will likely mix multiple manufacturers' devices running various versions of operating systems. Some may be using "jail-broken" devices running a modified version of their traditional operating systems, but without many of the standard restrictions or safe-

BYOD Policy Considerations

Below is a list of suggestions and issues organizations should consider when creating or revising their BYOD policies.

If personal devices are allowed in any capacity, restricted or unrestricted, then:

1. Restrict employees to the use of selected mobile communications carriers.
2. Require employees to sign a waiver or release form.
3. Determine how organizational policies will be audited, assessed, and enforced in relation to the devices.
4. Consider how/if employees will be reimbursed for organization-specific use of a personal device.
5. Prohibit or limit software applications employees can download.
6. Determine the types of organization-related resources/systems employees may access on the devices.
7. Instruct employees on the use of appropriate security procedures and enable them to segregate the organization's information from personal information on the device.
8. Require employees to load approved security-related software for access to the organization's systems and servers.
9. Determine the level and types of IT support (for the device and/or its applications) provided by the organization, if applicable.
10. Create a procedure for retrieval of the organization's data when a personally owned device user's employment is terminated or the device is lost or stolen.
11. Create a procedure for the retrieval of the device if it is needed for data collection and preservation in association with a legal hold order.

Source: *Mobile Communications and Records and Information ARMA TR 20-2012,* © ARMA International, *www.arma.org.*

guards – although that may not be apparent to the user or organization.

By embracing BYOD, then, organizations may be opening up their systems to user devices that have the ability through nefarious third-party applications or insecure operating systems to capture login information to secure corporate systems and send it back to someone who will sell it to the highest bidder.

BYOD Policy

Many organizations are adopting an open workplace policy allowing employees to get their work done from wherever they want to do it. When doing this, the organization must identify their security and management needs requirements. The first step in doing this is to gather all concerned parties.

Too often these initiatives take place in a vacuum because time is of the essence, and the ramifications seem slight. However, an amazing amount of data can be held on portable devices. Many come with 64GB of built-in memory or allow for expansion through memory cards, so the risks are great.

Identify Stakeholders

The business units that should be involved in creating a BYOD policy include IT, information security and protection, records management, information governance, internal compliance and auditing, and legal. All have a stake in the game, and it is imperative that they understand the opportunities and risks associated with mobile access to the organization's information, especially in a BYOD environment.

For example, the legal unit must understand and comment on the personal nature of corporate information on a personally owned device. Legal will need to determine such things as whether:

- The organization needs to secure the device for a legal hold
- The device can be imaged remotely as needed
- Personal information on the device can be segregated without risk of spoliation

As another example, IT needs to understand the impact mobile devices have on the organization's infrastructure. Ideally, the organization will limit (either by classification or other metadata) the types of information available for displaying or downloading to a portable device. The IT group will need to determine such things as:

- How access can be secured to defined repositories
- If it is possible to secure the systems and information based on classification and sensitivity criteria

Work with the internal audit team or a third party to ensure that your organization has a plan to address these concerns.

Identify Information to Be Accessible

Care must be taken to identify the information that truly needs to be remotely accessible. This will be unique to each organization; similar organizations may have disparate needs for mobile access depending on their history and organizational philosophy.

Some information (e.g., personally identifiable information) should not be available outside of the organization unless the system has been validated against a defined set of rules or protocols. Quite often, remote access of certain information or datasets violates corporate policy; those giving access may not know to review the policy, or they don't know where to find it.

It is important, then, to work with IT and business units to identify the information that needs to be accessed remotely, and then work with vendors to secure access. Finally, security and audit controls need to be in place to monitor access by those having rights and spotting those who do not.

Review Existing, Create New Policy

It is quite possible that existing policy may need to be updated. Reviewing and discussing the pros and cons of existing policy with the various business units will lead to an educated decision and direct current policies and compliance. (See the sidebar "BYOD Policy Considerations" for suggestions.)

Of particular importance is to have a legal hold policy identifying the corporate policy as it relates to personal devices used for business. This was fairly simple when mobile devices merely accessed e-mail, and a copy of the e-mail was on the corporate server. But today's devices access much more than e-mail and often can generate and create information. A tablet, for example, can be used to modify, edit, and produce documents that may not reside anywhere in the organization's infrastructure. The corporate policy must, therefore, address the capture of this information.

The organization should also create a protocol for duplicating information from the mobile device or for locking it remotely and accessing the information it contains. Requirements that were not a concern previously because the data always made its way to the corporate infra-

structure are now issues that may end up in a court of law or, at the very least, responsive to a subpoena.

Once the BYOD policies are finalized, update them annually – maybe even twice a year – as technologies are rapidly changing.

Train Personnel

Even with all of the proper tools in place, an unlocked phone left on a park bench across from corporate headquarters could be disastrous. Employees must be trained on, understand, and comply with BYOD program policies and their obligations related to them when accessing corporate systems or assets, including:

- Password-protecting devices
- Using only supported operating systems (not jail-broken)
- Following protocols for reporting a lost or stolen phone
- Understanding the possibility of remote wiping of lost personally owned devices

The Go-Forward Plan

There are new tools in the marketplace that may soon make this process easier. Vendors are developing applications and operating system adaptations that fundamentally allow for a "virtual operating system" on a personally owned device, essentially allowing for a corporately controlled environment.

Creating, implementing, and enforcing BYOD policies may seem like a daunting task initially, but your organization will be safer because of it. This space will change rapidly; it is important to keep the organization aware of the capabilities and risks associated with BYOD changes. Everyone should keep their eyes open and their smartphones on. **END**

Brent Gatewood, CRM, can be contacted at bgatewood@consultig.com. *See his bio on page 47.*