MARCH 2013

SECURING BYOD

Guidance on the strategies and tools needed for a secure and productive bring-your-own-device program

800.800.4239 | CDW.COM/BYODGUIDE

CDW REFERENCE GUIDE

A guide to the latest technology for people who get IT

CDW PEOPLE WHO GET IT

WHAT'S INSIDE:

Making it easy to find out what's new >>>

800.800.4239
CDW.com/byodguide

10

BLANKET COVERAGE: SECURING DATA AND TRAFFIC

DATA REQUIRES PROTECTION ON DEVICES, IN TRANSMISSION AND WHEN TAKEN OUTSIDE THE NETWORK.

WHAT IS A CDW REFERENCE GUIDE?

At CDW, we're committed to getting you everything you need to make the right purchasing decisions — from products and services to information about the latest technology.

Our Reference Guides are designed to provide an in-depth look at topics that relate directly to the IT challenges you face. Consider them an extension of your account manager's knowledge and expertise. We hope you find this guide to be a useful resource.

VISIT CDW.com/mobility

For more information on BYOD security.

SCAN THIS!

Lacking a good BYOD offense? Scan this QR code to your mobile device and see what plays IT expert Charles Barkley draws up.

GET M.CDW.COM ON THE GO

m.cdw.com is now available anywhere with our new mobile-friendly website or download the CDW app for your iPhone from the App Store.

SECURING BYOD

SECURITY IS A PRIME CONCERN WITH A BYOD INITIATIVE.

Mobile computing is becoming so ubiquitous that people no longer bat an eye seeing someone working two devices simultaneously. Individuals and organizations are responding to the capabilities and flexibility that mobile devices provide.

Between work-issued and personally owned devices, it's not uncommon for a person to have two notebooks and two smartphones. But ultimately, people find relying on this many devices inconvenient, and organizations find it expensive.

The solution to tackling this problem? Bring your own device. BYOD refers to using a personally owned device, such as a tablet or smartphone, for work purposes. Unfortunately, personal devices are generally harder to secure than organization-issued devices. Using these devices can put the organization's information and systems at higher risk of compromise.

But personal devices can be secured effectively if organizations take an integrated approach to security. Breaking away from traditional notions of mobile security, an integrated approach considers BYOD security in the context of devices, data and networks to design the right solution.

There is no silver bullet that is the be-all, end-all answer to BYOD security. The solution that works best for any particular organization is unique, tailored to that entity's requirements, technologies and environments.

BYOD: The B Is for Benefits

In most organizations, BYOD can't be used if it can't be secured effectively. Benefits that an organization can hope to gain through secure BYOD deployment typically include some of the following:

Increased employee satisfaction | BYOD lets workers choose the device that they use. This generally gives employees greater satisfaction than if they don't have a choice and must use the device selected for them by the organization. BYOD also allows people to have a single device for both personal

>>>

//// ORGANIZATIONS MUST ADJUST THEIR SECURITY STRATEGY TO ACCOMMODATE INCREASED MOBILITY, PARTICULARLY FOR BYOD USERS. ///

use and work, instead of having to carry, secure and maintain separate devices — another satisfaction driver.

More productive employees | Enabling access to the organization's resources through BYOD means that workers can be more productive because they can do their work on their own schedule, from whatever location is convenient for them. Also, allowing staff to choose their devices lets them pick ones that they're more knowledgeable about and more comfortable with — yielding greater productivity from them.

Potential cost savings | An organization may save money by reducing its purchase of mobile devices and (for smartphones and tablets) its monthly data plan contracts. Note that these savings may be offset by the cost of additional security controls, technical support for BYOD users and other costs associated with deploying any technology securely.

Also, many organizations choose to pay for their employees' personal data plan contracts for smartphones and tablets, which would otherwise be the primary area of savings for the organization.

Improved disaster recovery | Implementing BYOD can significantly improve an organization's disaster recovery capabilities. Should a disaster occur, workers can use their devices to remotely access the organization's resources.

Also, across the organization, employees are likely to be signed up with a variety of carriers, unlike a traditional organization-driven mobile strategy, which typically relies on a single carrier. The use of multiple carriers provides stronger redundancy in case one carrier has an operational problem.

Stronger protection of sensitive information | Taking an integrated approach to BYOD security means closely examining and evaluating the risks involved in BYOD usage. This can lead to levels of protection that are equivalent to (or even stronger than) the organization's typical security posture. This helps safeguard sensitive information from unauthorized access and disclosure.

The March Toward Mobility

In addition to all the benefits that a secure BYOD deployment can provide, there are other factors driving the move toward allowing workers to use their own devices while on the job.

The rise of mobility | The increasing use of mobile technologies is driving change in IT structures as organizations change how they do business. Workforces can be much more flexible, performing tasks out in the field that previously had to be done in an office on nonmobile systems. Plus, the mobility options have improved. A person can now use a smartphone or tablet to more conveniently do what previously might have required a notebook computer.

But increased mobility usually entails increased access to sensitive data and a corresponding uptick in risk of that information being compromised. Also, the threats against devices and information are different depending on whether the threats are inward or outward facing (or both). Organizations must adjust their security strategy to accommodate increased mobility, particularly for BYOD users; the old security solutions simply won't cut it anymore.

Increased availability of smartphone and tablet security controls | Until recently, there were few robust security controls available specifically

for managing smartphones and tablets. The rise of technologies such as enterprise mobile device management (MDM) and network access control (NAC) has provided a strong foundation for developing a more comprehensive mobile device security solution.

Even better, these technologies can be used to manage not only smartphones and tablets, but also notebooks, providing a single solution for multiple platforms.

MDM and NAC technologies are good first steps toward securing an organization's BYOD environment, but they are not sufficient by themselves to provide the necessary protection. A range of other security controls is needed. This guide will help organizations understand the capabilities of MDM and NAC technologies, as well as other measures that are needed to complement them.

The consumerization of technology | Many employees, particularly younger staff, are pushing to use their own computing devices instead of organization-issued devices. This is reflective of a larger demographic shift in the consumerization of IT.

Small-form-factor systems with much greater capabilities than previous generations of devices can be purchased today for only a few hundred dollars, putting them within reach of many workers. Also, manufacturers continue to produce devices that are smaller and lighter, making these technology platforms more portable, and therefore more likely to be carried in and out of work by employees.

A consequence of this consumer-driven trend is that employees are using an increasingly wider range of mobile device operating systems and versions. This demands attention from a security perspective because each OS and version has its own unique combination of security characteristics.

The rise of IT consumerization has, in turn, drawn the attention of cybercriminals interested in pursuing attacks against mobile devices. This has motivated a greater security focus on BYOD systems than was true of mobile devices even just a few years ago.

Threats from social networking | Over the past few years, social networks have been increasingly used to perform targeted attacks. Attackers have found social networks to be a convenient source of information for performing social engineering attacks.

For example, a cybercriminal can harvest social networking information to identify a person's friends, family and coworkers, then send the person's mobile device a crafted message that appears as though it was sent by someone that the person knows and trusts. The receiver of the false message — the victim — is a lot more likely to respond if they think it's from someone they know, rather than a stranger.

What's worse, social networking is one of the tasks most commonly done using personally owned mobile devices. BYOD programs within organizations have thus become a high-risk source of social networking attacks. Organizations should be aware that these attacks are often initiated to harvest their users' credentials. For example, users repeatedly use the same passwords across accounts, so their social networking passwords may be the same as their organization passwords. ■

BYOD FOR USERS OUTSIDE THE ORGANIZATION

Organizations may choose to apply the same BYOD security technologies, processes and other principles when providing secure access to individuals outside the organization. This could include onsite associates such as contractors and consultants, business partners, vendors and other guests.

Before granting such BYOD access, carefully consider the associated costs, not to mention the possible problems with violations of acceptable use policies and other policies. It may be necessary to have people sign a usage agreement before granting BYOD access to clarify roles and responsibilities.

CASE STUDY

BYOD BECOMING THE NORM

Read about one company's quick realization that it was BYOD-ready:

CDW.com/byodguide1

DEVICE DEFENSE

SECURING BYOD DEVICES REQUIRES THOROUGH RESEARCH INTO THE SOLUTIONS AVAILABLE.

Securing a mobile device can be a surprisingly difficult endeavor, and this is particularly true for BYOD programs. People who are used to the security controls and tools available for enterprise-controlled desktop and notebook computers may be surprised at the relative lack of corresponding controls and tools for BYOD mobile devices.

It's not that security controls and tools aren't available for these devices, but that they're not integrated into mobile devices in general. This requires the organization to get the device owners to install various security tools on them and change security configurations for the OSs and various applications.

The complexity of this process and its numerous moving parts contributes to the difficulty that users have in securing their own devices. On the surface, it may make sense to have users maintain the security of their own devices. After all, if they want the freedom to use their own devices, then accepting responsibility for security seems appropriate.

But given the difficulty in securing devices across a BYOD program, it's unrealistic to expect users to secure their personal devices effectively and to maintain that security on their own without oversight and assistance from the IT security team. Not only can security be very complex, it's also time-consuming to maintain manually.

For example, consider the effort involved in keeping up with all the patches for the operating system and major applications on a device. BYOD security maintained by users is also error-prone. Manually entering security configuration settings and selecting patches is highly subject to human error.

Another factor complicating personal device security is that there are new mobile devices rolling out constantly. Each new model is likely to have its own unique security features, possible vulnerabilities and significant differences in security characteristics compared with earlier models, even within the same brand. Another

consideration is that cellular carriers may customize their own OSs and add other changes to smartphones and tablets that affect security.

Enterprise Mobility Management

Enterprise mobility management is a general term that refers to everything involved in managing mobile devices and related components (such as wireless networks). EMM is much broader than just information security; it includes mobile application management, inventory management and cost management. Think of all the ways in which a mobile device can be managed; security is just one dimension of that, although a very important one.

There are two basic approaches to enterprise mobility management. One involves using mobile infrastructure services provided by the mobile device vendor (generally for smartphones and tablets only). A classic example of this is Research In Motion and its BlackBerry devices, which are complemented by RIM's BlackBerry Enterprise Server. BlackBerry Enterprise Server is a middleware application that interacts with associated BlackBerry devices to control their OS and security configuration settings.

Such middleware applications allow an organization's security (and other) policies to be enforced on its smartphone and tablet client devices. The key idea here is the organization's devices — not BYOD devices. These middleware applications are great solutions for organization-issued devices, but they generally don't permit personally owned devices to be integrated into the solution.

These middleware applications completely control the devices, so a user would have to turn over all control of their device to a BYOD program in order to use it with a middleware application. This is likely unacceptable for users and is not in keeping with the spirit of most BYOD programs.

Another problem with these middleware applications is that they generally don't support notebooks. An organization would have to manage notebooks and other mobile devices through completely separate mechanisms.

The second approach to enterprise mobility management is the use of add-on management tools, such as enterprise MDM software. This software, which is described in more detail in the next section, enables enterprise management of mobile devices, both organization-issued and BYOD.

Typically, enterprise MDM software allows full management of organization-issued devices and partial management of BYOD systems. This means basically controlling — and securing — a portion of each personal device for organizational use while leaving the rest of the device under the control of its owner.

In terms of security, this means keeping all sensitive information and operations within that secured portion. So instead of providing full-fledged device security (securing the user's entire device), enterprise MDM software provides content security (securing the organization's content on the user's device).

The alternative to enterprise solutions such as MDM software is to manually secure each personally owned device. Such an approach is highly resource-intensive and error-prone, so it's generally not a viable option. Plus, it then becomes nearly impossible to maintain the configuration (and security) of devices that are outside the direct control of the organization.

If an entity has to rely on users to manually maintain the security of their own devices or on system administrators to manually update devices when they are brought into the organization's facilities, it's almost guaranteed that there will be serious security and operational problems with the devices, which in turn will hurt productivity, cost the organization more in technical support costs and endanger sensitive information.

Mobile Device Management Software

Enterprise MDM software has become the primary security control for BYOD programs within many organizations, growing in popularity over the past few years. As enterprise MDM technologies have matured, their capabilities have increased as well. These capabilities can be grouped into three categories:

Remote security configuration | These capabilities let an organization control the security configuration of a device from a distance — that is, whether or not it is currently located onsite. This means the IT team can manage a device whenever it is available through the Internet — over cell phone networks, wireless LANs or other forms of networking. Remote security configuration enforces an organization's security policies within its portion of the device.

There are numerous possible security configuration settings. Some of the major categories for BYOD environments include:

- **Restricting access to hardware,** such as prohibiting the use of removable storage when accessing organizational information, to prevent that data from being saved on removable media that is outside the organization's control
- **Restricting access to software,** such as preventing use of the organization's information on a device with applications not formerly approved
- **Encrypting the organization's data stored on a device,** to stop unauthorized applications and users from accessing it

>>>

- **Requiring authentication,** such as performing successful multifactor authentication before allowing access to the organization's applications and information
- **Restricting applications** (see the proceeding *Mobile Application Management* section).

Another important aspect of remote security configuration is the ability to continuously monitor each device's unique security settings, to detect any violations of the organization's security policies, and to immediately and automatically report all violations as soon as they are discovered.

This will let the security group act quickly, often automatically, to restrict or prevent access to the organization's information from the suspect device until its security issues are resolved. Quick action can make a huge difference in terms of correcting problems rapidly, before they are exploited, and for stopping threats before they can inflict significant damage.

Remote locking and wiping | No matter how careful users are with their mobile devices, accidents happen. Devices will be lost, stolen or otherwise unaccounted for. And these devices may contain sensitive information belonging to the organization, which must be safeguarded from any parties that gain access to the devices.

One helpful feature for safeguarding devices is remote locking. By authorization of an administrator, enterprise MDM software can issue a command to immediately lock a managed mobile device — preventing access until the necessary credentials (such as passwords, biometrics or cryptographic tokens) have been presented. This feature is helpful if a device was unlocked or in an unknown state when lost or stolen because implementing a device lockdown can prevent any further access to applications or data.

Another helpful feature for safeguarding devices is remote wiping. Remote wipes take two forms.

The first, an administrator-issued command through enterprise MDM software, transmits to a lost or stolen device and causes it to destroy its organization-issued data and applications — securely wiping that portion of the device so that no information can be recovered from it. The second involves configuring a device so that after a certain number of consecutive failed authentication attempts, the device will securely wipe itself.

Both forms of remote wiping achieve similar results, but the first form requires a device to be reported to the organization as lost or stolen, while the second automatically works if someone tries repeatedly to log on to a device that isn't their own. Unfortunately, the second form wipes the entire device, not just the organizational content. Plus, if the owner of the device simply fails to authenticate several times in a row, he or she can trigger this type of wipe accidentally.

But if a device is lost or stolen and ends up in the wrong hands, a person may be delighted to have a remote wipe destroy their personal banking information, social networking credentials and other sensitive information on the phone as well. Given this possibility, remote wiping may need to be considered on a case-by-case basis.

Mobile application management | Mobile application management has different meanings in different contexts. But for purposes of this reference guide, it refers to deploying and maintaining mobile applications for organizational use.

One of the primary features of mobile application management is application sandboxing. This refers to *wrapping* an application so that when it executes, it can't access any information or applications outside the sandbox of specific items.

The wrapping also works in the opposite direction: Resources outside the sandbox can't access anything inside the sandbox. Sandboxing an organization's applications on its users' mobile devices is an invaluable step toward protecting the organization's data from misuse — accidental or otherwise.

Another primary feature is app distribution. For example, an organization might facilitate the installation of selected apps onto users' devices. The enterprise MDM software can manage this process and ensure that an app downloads only to those users authorized to run it.

This process relies on the security profiles that the IT department has established in the enterprise MDM software. Likewise, the organization can automatically uninstall any app from these same devices — for instance, if it retires an app or replaces one app with another, or if the user retires or leaves the organization (or even changes positions within the organization).

A complement to application installation services is application update distribution — specifically, distribution of operating system and application patches and upgrades. This is particularly important for an organization's custom apps (including enterprise MDM client software installed on BYOD systems), but it applies to all apps and underlying OSs too.

Vulnerabilities in these can be exploited in an attempt to gain access to the organization's information and resources. Enterprise MDM software has the ability to determine when new patches are available, and then ensure that the patches are downloaded and installed onto all devices, both BYOD and organization-owned.

One note: Patching is often more

problematic on smartphones and tablets than on notebooks. For example, Android devices have their OS versions selected and customized by the device manufacturers, which are then responsible for issuing patches and upgrades. Updates may be available for one maker's device months before they are available for other makers' similar devices.

Also, because of the short lifecycle of mobile devices, manufacturers may not support them for a long period of time, leaving users with older models that have known vulnerabilities that cannot be remediated. This is a serious issue that organizations must consider carefully when deciding which types of smartphones and tablets are acceptable for BYOD use.

Blacklisting, a final security control sometimes used for mobile application management, specifies apps that are not allowed to run on a device. An organization may have policies in place that prohibit certain apps from residing on personally owned devices or running concurrently with the organization's apps because of the security risks those particular apps may pose.

Additional Security Controls

There are many other add-on security controls emerging for securing mobile devices. Major categories include the following:

Host-based firewalls | Most smartphones and tablets traditionally haven't run host-based firewalls because they relied on network-based firewalls (such as those on cellular networks) to prevent unauthorized access. Now, however, mobile devices are increasingly connected to wireless LANs and other networks that don't provide protection through network-based firewalls.

Because of this change, it makes sense for an organization establishing a BYOD program to deploy host-based firewall solutions for mobile devices. It's important to know, however, that host-based firewalls for smartphones and tablets are newer solutions, therefore, offerings and options may be limited.

Antivirus software | Antivirus software on a mobile device can be helpful at stopping malware threats from compromising the device. As with host-based firewalls, antivirus software for smartphones and tablets is also a more recent development. There are some solutions available, but be sure to research them and how they interact with the specific devices used within the organization because some of them can significantly impact performance.

Mobile web security | Many browsers include security controls that may also be helpful for maintaining device security. One example is antiphishing protection, which can prevent a user from being tricked into visiting a fraudulent website. ■

ENTERPRISE STOREFRONTS

No matter the smartphones or tablets that an organization decides to allow for a BYOD program, all users face a common problem: the potential to be overwhelmed by the number of applications available, many for free. Unfortunately, some apps contain malware or are otherwise intended to be hostile, created to steal sensitive data from a user or the user's device.

Organizations cannot fully control apps installed on BYOD systems, in part because users demand the freedom to choose their own apps and also because of the technical challenges in keeping up with available applications. But users can be encouraged to download apps that are known to be safe by setting up organization-controlled enterprise storefronts, better known as app stores.

An organization can perform security assessments on selected apps and post links to those that pass the assessments. Then users can be directed to this trusted app store when they need to download apps, particularly apps for work purposes.

This can be a time-saving convenience for users, who would otherwise have to sift through reviews and other information to try to select productivity apps for themselves.

BLANKET COVERAGE: SECURING DATA AND TRAFFIC

DATA REQUIRES PROTECTION ON DEVICES, IN TRANSMISSION AND WHEN TAKEN OUTSIDE THE NETWORK.

Device security, emphasizing protective measures for operating systems and applications, is only part of the risk that needs to be addressed when establishing a BYOD program. To achieve an integrated approach to BYOD security, organizations must also consider the security of their data. That security must extend to data when stored on a device, when transmitted across networks and when in use both within and beyond the organization's control.

Without securing stored and transmitted data, a BYOD security solution is of minimal effectiveness because data can be accessed fairly easily from network communications or the mobile devices themselves.

Security efforts have typically focused on device security – secure the device and it's assumed that the data on the device is secure as well. But increasingly, IT teams are finding that this simply isn't the case. A device can be secured effectively, but the data on it can still be at considerable risk.

Data is transient; it can be transmitted to the device, processed in device memory and stored on the device within the blink of an eye. Making sure that data is safe in each of these states is not a trivial task. It requires controls beyond those used to secure the device itself.

Traffic & Storage Encryption

Encryption technologies protect the confidentiality of data by altering it using a cryptographic algorithm and a secret encryption key. The algorithm itself doesn't need to be secret. Even someone who knows all the details of the algorithm can't break the encryption with reasonable effort without having access to the secret key.

In many encryption technologies,

the same secret key is used to encrypt and decrypt data; other encryption technologies use a pair of keys, one public and one secret (or private). In this second approach, the public key is used to encrypt data and the private key is used to decrypt it.

By default, most devices that users bring into a BYOD program don't provide strong cryptographic protection for stored and transmitted data. Even so, most of these devices do have built-in (if unused) cryptographic capabilities. They just need to be configured properly to achieve sufficient security effectiveness.

But it's critical to be savvy about encryption tools. Why? Because weak encryption is not much better than no encryption at all. Attackers are familiar with known weaknesses and can circumvent these tools to gain unauthorized access to sensitive information. There are all sorts of free tools available that can collect weakly encrypted traffic and break the encryption.

Cryptographic Keys

Effective protection for data stored on, accessed from or transmitted to devices allowed for a BYOD program includes the use of strong encryption technology. And paramount to the success of any encryption approach is the secrecy of the cryptographic keys. If secret keys aren't kept secret, an attacker can and will use them to decrypt encrypted information.

There are other reasons that cause keys to become weak. For example, over time, attackers find weaknesses in cryptographic algorithms. This may necessitate retiring an old key and generating a new key to use in its place.

Also, brute-force attacks against cryptographic keys become more feasible as hardware capabilities continue to improve. A key that couldn't be manually attacked 10 years ago with much success might be child's play for a cyberthief to recover today. For these reasons, organizations need to replace their keys periodically to reflect advances in attack techniques and speeds.

All the processes involved in maintaining cryptographic keys are collectively known as key management. Key management is surprisingly challenging, in large part because an organization must administer something that needs to be kept absolutely secret – not an easy task. Plus, although it may sound simple on the surface, keeping backup copies of encryption keys is fraught with logistical complications.

Storage Encryption

Even though they share a common cryptographic basis, the technologies for securing storage and traffic are fundamentally different. Storage encryption focuses on protecting data at rest (stored on the user's device).

There are three main types of storage encryption: disk encryption, file encryption and virtual disk encryption.

Disk encryption | This technique involves encrypting all the data on a physical piece of media, such as an internal flash drive or a removable media card (microSD, for example). Disk encryption capabilities are built into most mobile device OSs.

When using disk encryption, a user who wants to access encrypted data first provides credentials (such as a password or biometric information), which allows access to the secret encryption key, which in turn decrypts the media as needed. Generally, the device won't decrypt the media entirely; rather, individual pieces of data will be decrypted on an as-needed basis and re-encrypted after use.

If a piece of media is encrypted using disk encryption and credentials need to be provided (for instance, the device is locked and it needs

>>>

DECODING STORAGE ENCRYPTION

There are three approaches to protecting data at rest, each one useful in specific circumstances.

Encryption type	How it works	Use scenarios
Disk encryption	This technology encrypts all data on a piece of media. Individual pieces of data are decrypted on an as-needed basis.	This approach is a good fit for devices especially susceptible to loss or theft.
File encryption	This technology encrypts individual files on a device. Decrypting one file will leave all other encrypted files locked.	This approach works well on devices carrying information with varying levels of sensitivity.
Virtual disk encryption	This technology is a hybrid of disk and file encryption. It creates an encrypted virtual container that holds all sensitive files.	This approach is useful for enterprisewide rollouts utilizing MDM technologies.

/// THE BIGGEST CONCERN ABOUT USING VPN TECHNOLOGIES FOR BYOD PROGRAMS IS RESTRICTING WHICH TRAFFIC IS CARRIED THROUGH THE ENCRYPTED TUNNEL. ///

to be unlocked), then the media's data is essentially inaccessible until credentials are provided. This means that if a locked device is lost or stolen, a malicious person who recovers it will be unable to use forensic tools and other techniques to gain access to the data protected through disk encryption.

But if the user forgets the password, the encrypted data may essentially be lost unless the organization has taken specific measures to safeguard against lost passwords.

If a device is not in a locked state, or the credentials that need to be provided are trivial (say, a personal identification number such as "1234"), then disk encryption provides minimal deterrence to attackers. It's vitally important to remember that disk encryption — and other forms of storage encryption — are only as strong as the authentication protecting the technique.

File encryption | This second main type of storage encryption is very similar to disk encryption, except that it protects an individual file on the device instead of the entire piece of media. The file is kept encrypted at all times. If a user wants to access the file, he or she must provide the necessary credentials to trigger decryption. If a user wants to protect 10 files, each individual file must be encrypted. But decrypting one file will leave the others encrypted.

If a user's device is lost or stolen while in an unlocked state, data safeguarded using file encryption is still protected from unauthorized access. However, files that just happened to be decrypted at the time the device was lost or stolen are unprotected.

There is one critical difference between disk and file encryption: Although disk encryption capabilities are typically built into mobile device OSs, the capability to encrypt individual files generally is not.

Virtual disk encryption | This third storage encryption technique is a hybrid of disk and file encryption technologies. The "file" that's encrypted is a virtual container that itself can hold many files.

Virtual disk encryption is the model typically used by enterprise MDM technologies for devices allowed in BYOD programs. The enterprise MDM software establishes a virtual container on the device that holds the organization's applications and data. This MDM application allows decryption of the container only after the user provides valid organizational credentials.

Applying Multiple Storage Encryption Technologies

It is possible to use multiple storage encryption technologies simultaneously. For example, workers using their own devices for work might use disk encryption to provide basic protection for all the information that the devices contain, and also use virtual disk encryption (through enterprise MDM software) to provide protection specifically for the organization's data. A person could also use file encryption for an additional layer of protection for the handful of files on the device that contain particularly sensitive information.

In addition to all the possible storage encryption technologies, there are also traffic encryption technologies to consider. The most widely used traffic encryption technologies fall into two categories: network level and application level.

Network-level Traffic Encryption

Network-level traffic encryption is usually implemented as a virtual private network. For personal devices allowed to connect to an enterprise network, such VPNs take the form of host-to-gateway architectures.

Each VPN endpoint (mobile device) establishes its own connection to a centralized VPN gateway and authenticates to that gateway on behalf of the user. Therefore, the gateway is the encryption-decryption point for all of the VPN connections, which provide strongly encrypted tunnels that other network traffic passes through.

The VPN is essentially a secure wrapper around the network traffic. This provides obvious value for protecting communications with devices allowed in BYOD programs.

A VPN client on each device, which is often built into the OS, can communicate with a VPN gateway at the organization's facilities. All communications will be protected from eavesdropping and tampering en route. This allows BYOD program devices to access designated internal resources, such as the organization's intranet, over the Internet from unsecured, external wired and wireless networks.

The biggest concern about using VPN technologies for BYOD programs is restricting which traffic is carried through the encrypted tunnel.

Conventional wisdom is that split tunneling — routing some traffic through the tunnel and not routing other traffic through it, such as personal activity — is a security risk because it allows a device to act as a link between the organization's network and external networks. But, with mobile devices in general, and devices used in BYOD programs in particular, multiple networks are often linked together; it's just the nature of the technology.

On the other hand, the alternative to allowing split tunneling is to route all network traffic for the BYOD program's devices through the tunnel. There are significant problems with this approach, including the amount of bandwidth it may consume, the degree to which it slows down users' network activities and the privacy issues inherent in routing personal traffic through the organization's networks and corresponding monitoring technologies. As a result, split tunneling is becoming more acceptable today for personal devices on the organization's network.

Application-level Encryption

Application-level traffic encryption can be used instead of a VPN when the traffic to be protected involves particular applications. The most common example is a web application that uses the Hypertext Transfer Protocol for its communications. HTTP can be wrapped in the Secure Sockets Layer (SSL) protocol or its replacement, the Transport Layer Security (TLS) protocol, generating what is known as HTTP Secure (HTTPS).

SSL — or, preferably, the stronger TLS protocol — provides a strongly encrypted wrapper that surrounds the traffic for a particular application. HTTPS is an ideal solution when all the traffic that needs to be protected is web-based and it's desirable to avoid the overhead of a full-blown VPN. HTTPS also obviates the need for a VPN client to be configured and maintained on each user's device. HTTPS support is built into virtually every computing device that has a web browser.

>>>

CLOUD STORAGE

A recent trend affecting BYOD programs is the increased availability and popularity of cloud storage.

Some mobile devices offer built-in backup services that duplicate a user's data from the mobile device to a cloud service. If the device is lost, stolen or damaged, the user's data can be recovered.

Other independent providers offer similar services that are typically web-based or may involve installing client software. There are also countless cloud-based file sharing services that allow a person to store their files in the cloud and access those files from anywhere.

These storage and backup services are quite convenient, and they provide a valuable service that might otherwise not be performed. Even if users don't take the time to perform local backups, the cloud service does. But cloud storage and backup services used for these devices can pose significant risks.

Sensitive organizational data securely stored on a device might be transferred to the cloud service. If not planned properly, an organization might have no idea how secure the cloud service is or even be aware that its data has been transferred to cloud storage.

Enterprise MDM software can be helpful at restricting the usage of cloud storage and backup services. For example, enterprise MDM software could block usage of these services from the organization's secure sandbox on each device. Some enterprise MDM software includes features that establish a secure sandbox in the cloud, allowing backups and storage for devices while ensuring only the user can access the data.

Multifactor Authentication

It was noted earlier that encryption is only as good as the authentication that restricts access to it. Single-factor authentication refers to a single instance of authentication, such as something you know (a password), something you have (a cryptographic token) or something you are (biometric information, such as a thumbprint).

Single-factor authentication tends to be weak. An attacker who guesses a password or steals a cryptographic token can use it to gain access without any other credentials. This is more likely to occur with mobile devices than with other devices because of the typical public use of these mobile tools. For instance, imagine someone using a smartphone while waiting in line at a coffee shop, who enters a PIN into an application with bystanders all around.

The alternative? Multifactor authentication, which involves two or more types of authentication factors (something you know, have and are). One of the most common multifactor authentication arrangements is a cryptographic token (hardware- or software-based) with a PIN. An attacker would have to steal the token and get the PIN to be authenticated and granted access.

It's becoming more commonplace for the "something you have" authentication factor to be virtual — that is, software-based. For example, having software-based cryptographic tokens for devices allowed in BYOD programs and having digital certificates or other forms of digital ID stored on the devices.

This is significantly more convenient for users because it reduces the number of objects that need to be carried around. However, it puts the organization at more risk, because if a device is stolen, so is an authentication factor.

The result is that the malicious agent is only a single-factor authentication away from gaining access to whatever the software token or digital certificate was protecting — unless the mobile device is also strongly protected through storage encryption or other means.

Ideally, in a BYOD scenario, the user has to provide at least single-factor authentication to gain local access to the mobile device, then provide multifactor authentication to use the organization's resources from the device. This may seem like authentication overkill, but it's absolutely necessary. The single-factor authentication proves to the device that the user is legitimate; the multifactor authentication in turn proves to the organization that the user is legitimate.

Data Loss Prevention Software

Data loss prevention software is an emerging technology strategy for protecting an organization's sensitive information from data exfiltration. DLP software examines data for characteristics that identify it as sensitive, such as a file containing Social Security or credit card numbers. DLP software can monitor three types of sensitive information: stored information, transmitted information and information manipulated by actions on the device itself (such as "copy" and "paste").

An organization may have DLP software installed on its networks and servers, but the DLP solution is incomplete unless it is also installed and running on BYOD user devices as well. The DLP software can identify sensitive data belonging to the organization that's stored on the devices, and it can monitor each device's actions to determine if this sensitive data is being used or transmitted inappropriately.

Examples of possible inappropriate use include copying sensitive data to unsecured removable media, taking a screen capture of sensitive data, e-mailing sensitive data to an external e-mail account and copying sensitive data from one document and pasting it into an unprotected document. DLP software can detect and, more important, stop these activities from taking place. Assurance of the protection of sensitive data has been one of the major hurdles slowing adoption of BYOD programs.

INFOGRAPHIC

INSECURE FILE SHARING

Learn about a growing problem, the unauthorized use of insecure file-sharing tools by workers:

CDW.com/byodguide2

Source: WatchDox

DLP DEVELOPMENTS

Data loss prevention solutions have been around for years and they are quickly evolving to become more effective in today's enterprise landscape that now includes a flood of mobile devices. Many manufacturers are expanding their DLP offerings to address BYOD's unique security concerns. This typically involves expanding their solution architectures to include specific mobile device brands or rolling out a new solution to provide DLP oversight to mobile devices.

Other areas of improvement have been implementation and data-profiling complexities, which have challenged DLP rollouts in the past. Classifying and tagging data, a necessity for successful DLP implementation, can be a difficult task. Today, third-party services are available that provide automated discovery of unprotected sensitive information and provide snapshots of potential exposure points.

DLP software can identify sensitive data in many ways, but the techniques have three main classes:

- **Pattern matching** | The DLP software looks for keywords, such as "SSN," or character patterns, such as "XXX-XX-XXXX," where "X" is a digit.
- **Fingerprinting** | This technique involves using cryptography to generate hashes for sensitive pieces of information — an identical hash found elsewhere indicates a copy of the sensitive data.
- **Statistical analysis** | This approach uses advanced statistical techniques to analyze the characteristics of documents containing sensitive data — new documents are checked in the same way and similarities investigated as possible duplication of data.

Most DLP software uses a combination of these techniques to identify sensitive data, with each technique being used in the situations where it is likely to be the most effective.

Secure Application Delivery

Because delivering sensitive data to personal devices allowed on enterprise networks necessitates so many security controls, many organizations move in the opposite direction and try to reduce the amount of sensitive data being delivered to these devices. Some organizations take this to the extreme and prohibit access to any sensitive data from users' personal devices, requiring organization-issued devices instead. Other organizations attempt to balance the benefits of BYOD with the increased risk that such programs place on sensitive data.

A helpful step in reducing risk is using secure application delivery techniques. Rather than installing application client software on each mobile device and storing sensitive information on the devices as well, it is often possible to house the apps and the data in the data center. In this situation, only the image of the app and data — screen updates and keystrokes, essentially — are transmitted back and forth between the mobile device and the enterprise. This minimizes the exposure of sensitive data to the devices.

Secure application delivery techniques also use other technologies described in this reference guide. They typically offer some sort of centralized authentication control, which can be part of a multifactor authentication solution to restrict access to the enterprise. Also, they encrypt their network communications, typically using HTTPS, to prevent any eavesdropping of sensitive information carried over networks.

Secure application delivery may sound fairly mundane, but it's an effective way of reducing risk. Its biggest limitation is that it often requires a change in application architectures, which may not be possible with commercial off-the-shelf software. But as mobile initiatives continue to expand, software makers are producing more products that offer web-based client interfaces. ■

WE GET DATA LOSS PREVENTION

KEEPING UP WITH AN EVOLVING THREAT ENVIRONMENT.

76%

THE PERCENTAGE OF ORGANIZATIONS THAT ALLOW WORKERS TO USE PERSONAL MOBILE DEVICES FOR WORK-RELATED TASKS, ADDING ADDITIONAL RISKS TO THE NETWORK.

Source: CDW IT Monitor, IT Growth Outlook Hits Record High Led by Surge in Expected Investments, newsroom.CDW.com, January 30, 2012

The security landscape is changing. From mobile access to cloud computing, new approaches to data access create inherent weaknesses. Outside threats — including spam, viruses and malware — continue to be a problem, but threats from inside your organization also have to be mitigated. An incorrect, auto-populated email address can put data at risk as much as the intentional sharing of confidential information.

But accessibility, when combined with proper security measures, enables productivity and efficiency. A secure infrastructure can offer additional support by creating new value streams — from enabling information-sharing applications to empowering knowledge workers. Your organization needs a data loss prevention (DLP) solution. And it depends on you to build one.

A complete solution includes multichannel protection that utilizes a mix of these elements:

Channel-specific Protection

Working with other security tools such as antispam gateways, channel-specific tools focus on a single channel such as email rather than the entire network.

Endpoint and Data-at-Rest Products

These tools help to enforce a policy such as a prohibition against flash memory devices and can scan network and local hard drives for improperly stored sensitive data.

Network-based Tools

By examining network traffic, these tools can report or block transactions that violate policy such as preventing personal ID numbers from being sent off network.

Encryption

Data that is lost or stolen may still be protected if it is properly encrypted. This method of protection works on a variety of devices including notebooks, networked systems and removable media.

/// KEEP YOUR DATA IN THE RIGHT HANDS. VISIT CDW.COM/DLP TO LEARN MORE. ///

Symantec. CDW.com/symantec

Symantec's cutting-edge data loss prevention (DLP) solutions reduce risks and protect critical information with a single-source, multilayer technology that results in measureable reduction of risk. CDW and Symantec together have the technology and design and implementation expertise that addresses the ever-changing data protection needs your agency faces. CDW works closely with Symantec and has a Symantec DLP risk assessment team onsite.

McAfee An Intel Company CDW.com/mcafee

McAfee Total Protection for Data Loss Prevention (DLP) safeguards intellectual property and ensures compliance by protecting sensitive data wherever it lives — on the network, in storage systems or at the endpoint. It delivers high levels of protection for sensitive data, while saving time and money with centralized deployment, management and reporting.

websense CDW.com/websense

Websense TRITON Mobile Security provides effective web security, mobile malware protection, app controls and reporting for mobile devices. Safely enable mobile devices in your workplace while protecting them from mobile malware, web threats, phishing attacks, spoofing and more. Top features include: real-time security protection from threats targeted at mobile devices, MDM features such as encryption, password enforcement, jailbreak detection, remote lock and wipe and selective wipe make it easy to secure and manage mobile devices, mobile app controls provide the ability to push and pull corporate apps to and from devices, plus controls for iCloud, Siri, App Store and iTunes, flexible management that supports separate policies for corporate devices and personal devices, and In-the-cloud solution eliminates the need to invest in additional hardware or infrastructure.

RSA The Security Division of EMC CDW.com/rsasecurity

Defending against advanced threats requires an adaptive approach, oversight of processes and reporting key metrics. Unlike traditional signature based/endpoint security solutions, RSA provides an integrated set of tools and services that can easily fit into your existing environment, enabling you to identify, protect, and respond to security incidents rapidly.

RSA provides a complete product set designed to find and address the unique characteristics of advanced threats that help your organization be better prepared to manage and respond to advanced threats; positioned to identify, prioritize and respond to attacks; and more coordinated with visibility and reporting across the extended enterprise.

232 MILLION +

MORE THAN 232 MILLION **IDENTITIES WERE STOLEN IN 2011.**

Source: Internet Security Threat Report, Symantec, 2011

PREVENTING DATA LOSS

If you know where your weaknesses are, you can better focus your security plan. Our Data Loss Prevention Risk Assessment helps identify where sensitive data is created, stored and used to help determine the specific points at which you're most vulnerable to data loss. You'll receive a report that details these findings, as well as remediation recommendations prioritized by risk, cost and organizational impact. And if you have any questions or want to move forward with any of the recommendations, we're here to help.

GET STARTED AT CDW.COM/DLP

WE GET MOBILE ENDPOINT SECURITY

EASIER MOBILE DEVICE MANAGEMENT

33%

THE PERCENTAGE OF ORGANIZATIONS THAT HAVE IMPLEMENTED AN MDM SOLUTION.

Source: Survey Employees to Target Mobility Improvements, Forrester, April 2012

From iPhones and Android devices to tablets and notebooks, employees are increasingly bringing devices from home to the office for both work and personal reasons. Once they arrive, they expect to be able to join those devices to the network, either to access shared resources or simply to connect to the Internet.

While introducing a BYOD solution can help an organization increase productivity and efficiency, it can also cause issues with IT and security if not implemented properly.

Putting a mobile device management solution in place can help you keep track of devices in use while making sure your network can support them. Everyone on your team has the mobile devices to help keep them productive even when they're not in the office. And they have the correct applications and support to get their job done efficiently. So you get more time to focus on other strategic initiatives. With the right mobile device management solution in place, your organization can experience increased productivity and efficiency.

- **PRODUCTIVITY.** A mobile policy that accommodates a variety of devices gives each user the correct applications and permissions to do their job effectively — from wherever they may be.
- **SECURITY.** Mobile device management can help you make sure all devices are fully compliant with your security policy. You can also be confident that the possibility of a security breach has been minimized.
- **I.T. EFFICIENCY.** Mobility can be an asset to your organization, but can also drain your IT team. Mobile device management can help address the needs of your workforce while allowing you to focus on other projects.

The challenge for organizations is to find the management system that best fits their needs. And that's where we can help. We can help you sort through your options to find the solution that's tailored to the needs of your organization.

/// TO LEARN MORE, CONTACT YOUR CDW ACCOUNT MANAGER AT 800.800.4239 OR VISIT CDW.COM/MOBILITY TODAY. ///

SOPHOS

Sophos Complete Security Suite gives you the antivirus, endpoint and mobile protection you need with device control, encryption, web and email gateway security you demand. And, because it's all from Sophos, it works better together. It's backed by a vendor you trust. Even better, it's so simple to use you'll actually turn it on — delivering exceptional protection that saves you time and money.

varonis
all about the data

Varonis provides organizations the ability to keep pace with their data, manage access entitlements efficiently and effectively, audit access to every file event, identify and involve data owners and find and classify sensitive and business-critical data. Varonis offers a comprehensive and effective solution for data governance using a scalable and extensible metadata framework.

airwatch

AirWatch's Mobile Device Management (MDM) solution enables you to manage deployments of mobile devices. The solution provides the ability to quickly enroll devices in your environment, configure and update device settings over-the-air, enforce security policies and compliance, secure mobile access to corporate resources, and remotely lock and wipe managed devices.

MobileIron

The MobileIron Mobile IT platform secures and manages apps, docs and devices for global organizations. It supports both corporate-liable and individual-liable devices, offering true multi-OS management across the leading mobile OS platforms. MobileIron is available as both an on-premises system through the MobileIron VSP and a cloud service through the MobileIron Connected Cloud.

48%

THE PERCENTAGE OF DEVICES THAT WERE **SELECTED BY USERS WITHOUT REGARD TO I.T. SUPPORT.**

Source: *Survey Employees to Target Mobility Improvements*, Forrester, April 2012

WE GET MOBILE SECURITY

When you decide that your computing environment and IT security program would benefit from a mobile device management system, we have the experts and resources to get it up and running.

We take the guesswork out of buying MDM systems by pretesting best-of-breed solutions to match any budget. Our solutions include the most commonly deployed products on the market and accommodate a wide range of technical requirements and budget constraints.

READ UP ON MDM SUCCESS STORIES IN THE CASE STUDIES SECTION AT CDW.COM/MOBILITY

MOBILITY PEACE OF MIND

75%
THE PERCENTAGE OF EMPLOYEES WHO ALREADY USE THEIR OWN DEVICES TO ACCESS WORK-RELATED DATA.

Source: Fortinet Internet Security Census, 2012

Communication and collaboration are the keys to running a successful organization. But without a solid mobility plan in place, those necessities are hard to come by. To help boost productivity, IT departments have been forced to adopt the bring-your-own-device (BYOD) trend. But with more devices come more problems. Although BYOD gives users the freedom to use a device of their liking, it takes the control out of the hands of the IT department.

Which can mean added security, manageability and bandwidth issues. A solid mobile solution can help alleviate the problems of mobile mayhem. The right technology will evolve with your organization's growing needs. It will increase efficiency and improve manageability while tightening up security. This will also allow your users to access emails, files and applications from just about anywhere.

Initialize the Right Plan

Choosing the right solution can help deliver applications version control while providing purchasing storefronts and security.

Mobile Device Management (MDM)

MDM provides over-the-air configuration tools to help administer and control device settings. It also provides a real-time inventory of installed applications and security configuration. Troubleshooting and intelligence enable staff to manage mobile environments and remote control to take over devices and see what users see.

Network Access Control (NAC)

NAC allows organizations to assess the security of devices connected to enterprise networks. In addition to providing authentication capabilities, NAC can also dynamically assess the security posture of wireless devices. It can block devices from connecting to the enterprise network if they lack appropriate security controls, such as antivirus software with updated signatures, a current and patched version of a supported operating system or a functioning host firewall.

Mobile Application Management (MAM)

MAM is a necessary component of an MDM solution. You should prepare for future mobile requirements by adopting technologies with strong application management and security features. A MAM solution can also allow you to create a secure container for organizational data and applications while sectioning off sensitive information from the rest of the device's operating system.

/// IT TAKES A LOT TO MANAGE YOUR ORGANIZATION'S MOBILITY NEEDS. WE GET IT AND WE'RE HERE TO HELP. VISIT CDW.COM/MOBILITY TO LEARN MORE. ///

CDW.com/cisco

The Cisco BYOD Smart Solution provides a comprehensive approach to effectively design, manage, and control the access of a bring-your-own-device (BYOD) network. Cisco BYOD enhances user experience and productivity.

BlueCoat CDW.com/bluecoat

Most environments today have hundreds of applications running on the network at any given time. They all have different management issues, depending on the application type, and there is no one-size-fits-all technique to optimize performance across the board.

To help you manage and optimize all your internal, external and real-time applications, Blue Coat offers a variety of bandwidth management technologies to help manage and optimize all your internal, external and real-time application, including: Layer 7 traffic classification and discovery to precisely identify traffic; traffic shaping to control bandwidth utilization by application; compression and caching technologies to reduce bandwidth utilization; and video stream-splitting to reduce bandwidth utilization.

BARRACUDA NETWORKS CDW.com/barracuda

With hundreds of lines code to check — and vulnerabilities often subtle and hard to find — a serious data breach is often the first sign that a web application has problems.

Barracuda Networks Web Application Firewall quickly protects web servers from data breaches and websites from defacement without administrators waiting for clean code or even knowing how an application works.

WatchGuard CDW.com/watchguard

WatchGuard's Application Control enables policy-based monitoring, tracking, and blocking of over 1,800 unique Web 2.0 and business applications. Gain visibility and control over your network by deploying WatchGuard's award-winning XTM solution today. Gain control. Gain visibility.

350%

WI-FI HOTSPOTS ARE SET TO **INCREASE 350% BY 2015**, PROVIDING MORE OPPORTUNITIES FOR **"MAN IN THE MIDDLE" ATTACKS.**

Source: Juniper Networks Malicious Mobile Threats Report 2010/2011, May 2011

NETWORK ASSESSMENT

Our engineers can provide a tailored, onsite assessment of your current network to determine how it is helping or hindering the achievement of your organization's goals. After the assessment, they will deliver a written report that details our recommendations to improve your network's speed, scalability and security.

GET STARTED AT CDW.COM/NETWORK

WE GET BYOD

MINIMIZE THE RISKS OF BYOD

33%

THE PERCENTAGE OF ORGANIZATIONS SUPPORTING BYOD POLICIES THAT ARE NOT CONFIDENT THEY ARE EFFECTIVELY MANAGING RISK.

Source: *Survey Employees to Target Mobility Improvements,* Forrester, April 2012

Managing mobility can be a tough task. Especially with the BYOD trend in full effect. It's an ever-evolving world of operating systems. Endless endpoints. Many media-rich applications. Bottlenecks and limited bandwidth. And if your IT department doesn't have the capacity to respond to it all, efficiency will plummet.

To get on the path to a solid mobility plan, a multipronged approach is a must. Starting with a mobile device policy. This will ensure you set limits with your workers and help eliminate self-service IT issues such as file lockers. Utilizing mobile device management tools such as application management, remote configuration and security will keep you in control and in touch.

Map out your route

Determine deployment

While an on-premises solution offers direct control, a SaaS solution offers scalability and availability. Narrow the field to decide which is best for your organization.

Consider coverage

Choose your mobile device management solution based upon what types of mobile devices your organization needs to cover.

Take on tools

Based on your IT environment, decide what tools work best for you. While some products run wirelessly, others require manual installation.

Administrative assistance

Device inventory and help desk support among other administrative tasks can be taken care of with the right tools.

Strengthened security

As mobile devices are often lost or stolen, protecting the data they contain is key; but different devices require different tools. Determine the appropriate third-party tools to enforce encryption across all devices.

With the right mobility plan in place, your organization will reap the rewards of a more efficient and more agile workforce.

/// TO LEARN MORE, CONTACT YOUR CDW ACCOUT MANAGER AT 800.800.4239 OR VISIT CDW.COM/MOBILITY TODAY. ///

CDW.com/cisco

To manage the proliferation of personal devices, Bring Your Own Device (BYOD) policies have moved to the forefront for IT professionals.

As the lines between personal and professional lives continue to blur, security is no longer a question just of how to keep people out; it is also a question of how to let them in. Moreover, new business requirements, such as the need to use collaborative applications, are driving the demand for greater flexibility and more choice, even as users demand the same levels of network performance and security. IT professionals must balance security and enablement so that users can collaborate with confidence.

CDW.com/barracuda

The Barracuda Networks NG Firewall is an ideal solution for IT administrators seeking to re-establish control of networks made chaotic and vulnerable by the explosion of mobile and BYOD devices, evasive Web 2.0 applications, and remote network users.

While other "next-generation" firewalls use application visibility only to enhance security — by inspecting application traffic and blocking malware and other attacks or intrusions — the Barracuda NG Firewall goes far beyond this. It further leverages the power of application visibility and user awareness to manage traffic and bandwidth intelligently, and adds capabilities to optimize WAN performance and reliability.

CDW.com/netgear

NETGEAR offers value-based networking products, including those for security. NETGEAR's ProSecure UTM Series is designed to provide a comprehensive, all-in-one gateway security solution. It combines tools for application proxy firewall, virtual private network (VPN), zero-day protection, antivirus, antispyware, antispam, intrusion prevention and URL filtering for multilayer protection.

CDW.com/trendmicro

Trend Micro Deep Security provides a comprehensive server security platform designed to simplify security operations while accelerating the ROI of virtualization and cloud projects. Tightly integrated modules easily expand the platform to ensure server, application and data security across physical, virtual and cloud servers, as well as virtual desktops.

43%

THE PERCENTAGE OF COMPANIES THAT HAVE ROLLED OUT A **BYOD SECURITY STRATEGY.**

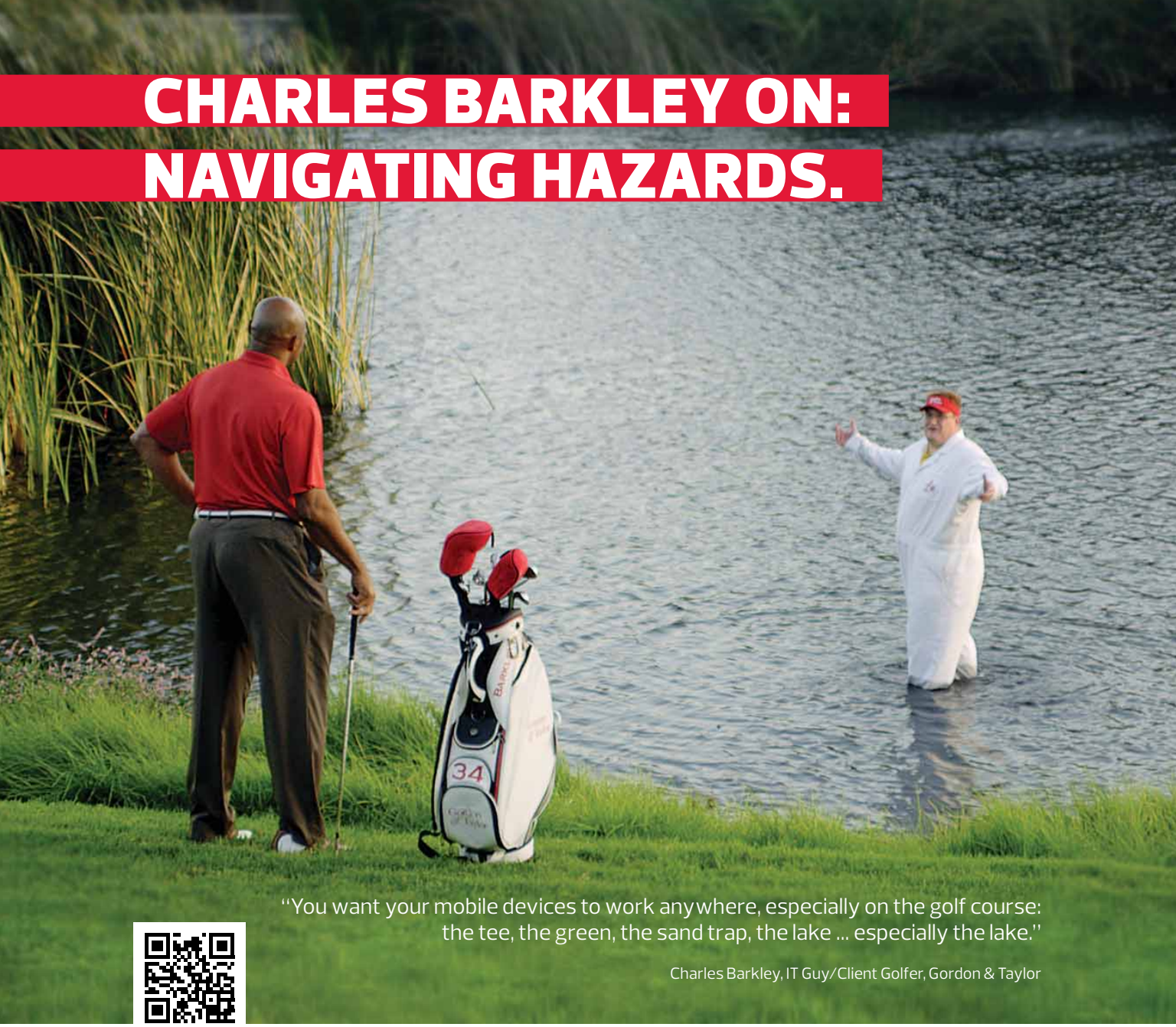
Source: 2012 PwC Global State of Information Security Survey

WE GET MOBILITY

Upgrading and maintaining your mobile technology can be overwhelming. We're here to help. Our experts can simplify the process and will be with you every step of the way from implementation to support throughout the lifecycle of your technology. Our complete mobility configuration services include user administration and configuration across multiple platforms.

FIND OUT HOW WE CAN HELP YOU SOLVE YOUR MOBILITY ISSUES AT CDW.COM/MOBILITY

CHARLES BARKLEY ON: NAVIGATING HAZARDS.



"You want your mobile devices to work anywhere, especially on the golf course: the tee, the green, the sand trap, the lake ... especially the lake."

Charles Barkley, IT Guy/Client Golfer, Gordon & Taylor

There are lots of hazards on the golf course. Bunkers, trees and water, just to name a few. Just like there are lots of hazards in deploying a mobility strategy. There's the issue of how to keep people on the road or in multiple locations connected. There's the BYOD issue. And the issue of how to make countless different platforms work together seamlessly. Just as the right caddy can help you navigate the hazards of the course, partnering with the right people can help you turn your technology into a strategic business asset.

Mobility issues won't keep Charles off the golf course. Find out why at CDW.com/Barkley

CDW PEOPLE WHO GET IT™

©2013 CDW LLC. CDW®, CDW·G® and PEOPLE WHO GET IT™ are trademarks of CDW LLC.

ARMORED ARCHITECTURE: SECURING THE NETWORK

SECURITY ACROSS THE NETWORK HELPS ENSURE BYOD SAFETY.

So far, this reference guide has focused on securing devices allowed for BYOD programs and the data those devices access and use, whether it's stored or being transmitted. There is another dimension to implementing an integrated BYOD security strategy: safeguarding any organizational networks that will be carrying BYOD traffic. If these networks are not secured, attackers have an opportunity to eavesdrop.

There is another defensive component too. The organization needs to monitor its networks so that it can react if an attack or other policy violation takes place. Policy violations may happen accidentally (such as someone inadvertently trying to connect to the wrong network) or intentionally (such as someone refusing to allow patches to be installed on their personal device and then attempting to use it on the organization's networks).

The proactive solution requires a combination of well-secured networks and continuous monitoring of the activity on those networks so that IT decision-makers can keep a close eye on BYOD usage.

Secure Wireless Architectures

A primary BYOD risk results from employees bringing devices into the workplace and connecting them to their organization's internal networks. This exposes those networks — and the computers and information on them — to possible compromise from an infected or unsecured personal device. Therefore, it's generally recommended that organizations create a separate network segment just for BYOD access.

Having a separate network segregates the BYOD traffic from all other traffic within the organization's facilities. And a segregated network can be secured and monitored more completely and easily than a mixed network containing traffic from both personal devices and organization-supplied devices.

>>>

Separating BYOD Traffic

The topology can be structured so that devices on the BYOD network can contact any external host but only a few designated servers within the organization, such as e-mail servers. In addition, network policies can prohibit BYOD users from directly contacting any other internal hosts, including all other devices on their local network.

This prevents infected or otherwise compromised devices from attacking each other and from attacking any other hosts besides those few it is authorized to contact. Additional security controls can be deployed to a BYOD network to compensate for the security controls that users' devices may lack.

Because many personal devices can only use wireless networking protocols by default and not wired networking (because they don't have wired network interfaces built in), a segregated BYOD network is almost always a wireless network. An IT team can create this segregated network simply by standing up a new wireless network for BYOD use only.

This generally involves deploying new wireless access points around the organization's facilities and building a small wired network infrastructure to link the new wireless network to the wired networks.

Organizations should be cautioned to make the BYOD wireless network an external network rather than an internal one. The BYOD wireless network should reside outside of the organization's network perimeter and the enterprise firewalls.

BYOD users should have the same basic access to the organization's resources, whether they are on the organization's BYOD wireless network or are on an external, Internet-connected network. Think of the BYOD wireless network as providing Internet access for users' devices while they are at the organization's facilities.

Organizations that want to allow guest access, such as for contractors' and visitors' devices, should consider having a separate guest wireless network. It is not advisable to mix these devices with employees' personal devices or organization-issued devices.

Often, guests want access to contact external resources, such as personal email services, not resources within the organization. So it makes sense to give these temporary users a separate external network to prevent their traffic from commingling with the organization's traffic.

There are some additional special considerations for establishing BYOD wireless networks: wireless access point security, device authentication and wireless intrusion detection and prevention systems.

Wireless Access Point Security

Wireless networks are at high risk of eavesdropping because they transmit their signals through the air. This is particularly true for organizations that are in close proximity to other entities, such as businesses that share an office building.

With special antennas, attackers can intercept signals from considerable distances. Also, an infected mobile device within the organization's facilities could conceivably be configured to monitor and intercept wireless communications involving other devices.

All wireless networks should be configured to protect their traffic from eavesdropping. For an organization's BYOD wireless network, this means using strong wireless networking encryption protocols, such as Wi-Fi Protected Access 2, and avoiding the use of known weak protocols, such as the original Wi-Fi Protected Access and the old Wireless Equivalent Privacy protocols. WPA and WEP have known vulnerabilities that make it easy for attackers to circumvent their intended protections.

WPA2 has been built into nearly all wireless networking equipment for several years, so it should be a standard option on any access point that the organization acquires. All wireless APs should be configured to permit communications only if a strong protocol is in use.

Additionally, the APs should not be set with a fallback policy that permits the use of weaker protocols if a stronger protocol is not supported by a mobile device or other wireless endpoint. IT administrators should specify which wireless protocols are acceptable for BYOD and be willing to block the use of devices that can't or won't use an acceptable protocol.

One more aspect of wireless APs that organizations should carefully consider is their physical security. If the APs are in physically accessible areas, which is often the case, they may be subject to physical attack.

/// ADDITIONAL SECURITY CONTROLS CAN BE DEPLOYED TO A BYOD NETWORK TO COMPENSATE FOR THE SECURITY CONTROLS THAT USERS' DEVICES MAY LACK. ///

For example, a person could hit a reset button on an AP that causes its security configuration to return to default settings, thus circumventing the intended security. It may be necessary to place APs in less readily accessible areas, particularly those that are in the public space of a building, such as a lobby or auditorium.

Device Authentication

In Chapter 3, the need for user authentication to secure storage and traffic was covered. Sometimes, it is also advisable to have device authentication. In the past, this was most commonly implemented by collecting the unique Media Access Control address of each device authorized to use the network, and then permitting only those devices access.

Unfortunately, it's easy to forge a MAC address. And because wireless network traffic is transmitted through the air, it's also easy to intercept traffic and potentially recover a legitimate MAC address from it. While authenticating devices by their MAC address is better than no device authentication at all, it's an approach that can be defeated by someone who wants to circumvent it.

Today, there are alternatives to MAC address filtering for achieving device authentication. The most popular choice today is using Protected Extensible Authentication Protocol (PEAP), which derives its security strength by making use of Active Directory to authenticate users. Another go-to option for authentication is Extensible Authentication Protocol Transport Layer Security (EAP-TLS), which derives its strength from requiring a client-side certificate to access the network (and which has the added bonus of certifying asset ownership of the device).

Going forward, newer standards, such as Extensible Authentication Protocol Transport Layer Security version 2 (EAP-TLSv2), hold much promise, providing the ability to perform two-factor authentication on 802.1x networks.

Wireless Intrusion Detection and Prevention Systems

Another important security control for protecting wireless networks are wireless intrusion detection and prevention systems. A WIDPS sensor monitors all wireless network communications within its range and analyzes them for signs of wireless attacks, wireless policy violations and other problems.

A WIDPS has another important role: detecting unauthorized wireless networks. A common technique that attackers use is to set up rogue access points in the hope that users will inadvertently connect to them. WIDPS technologies can detect these rogue APs and alert administrators not only to their existence, but also to their approximate physical location.

Network Access Control Solutions

As the name implies, a network access control solution regulates access to an organization's networks for user devices. A NAC solution examines the security characteristics of a device every time it attempts to connect to the BYOD wireless network.

If these security characteristics comply with the organization's security policies, then a device is granted access to the BYOD wireless network and the accompanying approved resources. If the device's security characteristics don't comply with organizational security policies, the device is either completely denied access or given access to a separate "remediation" network for corrective action.

There are many mobile device characteristics that NAC solutions can potentially review, including:

>>>

PERSONAL DEVICES AS HOTSPOTS

Many of the latest notebooks, smartphones and tablets offer a "hotspot" feature that allows other devices to use them as a wireless access point.

For example, if a tablet has a cellular data connection, the user can enable its hotspot capability and allow a notebook (without a cellular data connection) to connect to the tablet and borrow some of its cellular data connection. Wireless LAN connections can also be shared, which effects BYOD usage.

From a BYOD perspective, allowing wireless LAN hotspot usage is problematic because the devices using the hotspot are somewhat hidden behind the hotspot capability. These devices may not be readily detectable by enterprise security controls, such as MDM and DLP solutions.

Organizations may need to use tools such as enterprise MDM on all personal devices used for work to detect and report wireless LAN hotspots so that they can be disabled. Consideration should be given to the risks posed by such hotspot usage compared with the benefits that it provides employees.

- security configuration settings
- operating system and application patches
- antivirus software
- host-based firewall

So a NAC solution can be quite useful in a BYOD environment, making sure devices are reasonably secure before allowing them to use the organization's networks and services. And with NAC features now being integrated into MDM solutions, BYOD programs can have even stronger access protection, as well as granular control over it.

NAC solutions come in two architectures: agent-based and agentless. An agent-based NAC solution works through a client installed on each device. An agentless NAC solution requires no software on the user device. Instead, it performs network scans of each device before granting it access.

Agent-based NAC is more accurate at performing health checks than agentless NAC, but there may be technical and logistical problems with relying on agents installed on users' devices. For example, an organization's NAC solution is unlikely to have agents that run on all possible device types.

To use agentless NAC tools, IT administrators can choose to exempt certain devices or prohibit the use of devices not supported by the NAC solution. It should be noted that these two approaches can be mixed and matched because many NAC products offer both agentless and agent-based modes.

Continuous Monitoring

Finally, it's important to also deploy continuous monitoring to the process of auditing the security posture of a device or network to detect any attacks, policy violations or other problems.

Before continuous monitoring technologies became available, organizations often reviewed the security of devices only occasionally, when they conducted specific audits. This strategy, besides leading to long periods of weak security, fails to detect compromises quickly and so leaves damaging behavior to continue to users without their knowledge.

Interest in continuous monitoring has grown over the past few years because of attackers' focus on stealing sensitive information, an act that once done cannot be undone. For example, once a person's medical records have been compromised and revealed, that action cannot be reversed — the confidentiality has been destroyed; there is no way to regain it.

In the context of BYOD, continuous monitoring is an important component of an integrated security solution. It is necessary to monitor the activity on the organization's networks being generated by personal devices to determine if any of it is malicious in nature or otherwise inappropriate.

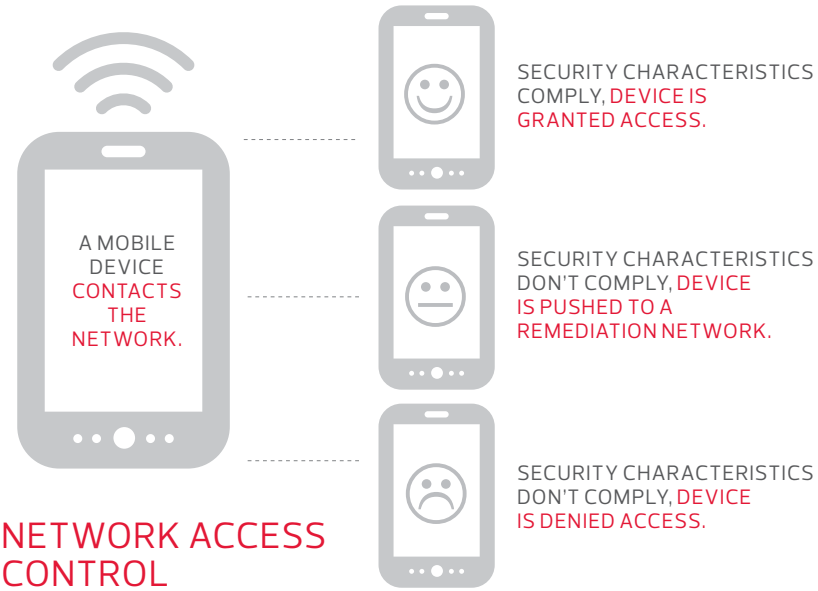
One of the disadvantages of adopting BYOD is that a user's activity can appear to be coming from within the organization. A user may be doing things that might embarrass the organization, such as viewing pornography or downloading pirated digital content from a device over the organization's networks. Detecting and stopping such incidents before the organization is publicly embarrassed is yet another reason for using continuous monitoring technologies. ■

TACTICAL ADVICE

HOLISTIC NETWORK HEALTH

Read about specific steps that can be taken to better integrate wireless and wired network security:

CDW.com/byodguide3



NETWORK ACCESS CONTROL

STRATEGIES FOR BYOD SUCCESS

STARTING WITH A CLEAR, THOUGHT-OUT BYOD POLICY WILL YIELD LONG-TERM BENEFITS.

BYOD security relies heavily on device security, data security (including traffic security) and network security. It also involves IT governance. Technical controls aren't enough to provide a fully integrated BYOD security solution. There are also management and operational controls that need to be put in place. What's more, the various security and disparate technical controls need to be integrated.

Mobile Use Policies

All the security controls in the world won't fully protect wireless networks unless those networks are implemented to enforce a strong, sound security policy. A policy is the foundation of any security implementation. An organization must have a wireless security policy that specifies security requirements for wireless usage. It's also recommended that, in order to take advantage of BYOD technologies, a separate BYOD security policy should be in place as well.

Topics that a BYOD security policy should address include:

- The types of devices permitted;
- The resources or types of resources that may be accessed;
- The provisioning of BYOD access (such as registering devices and issuing credentials);
- How remote access to the organization must be secured.

It's also commonplace to have acceptable-use guidelines for BYOD, possibly in a BYOD security policy or in the organization's general acceptable-use policy. These guidelines explain how personal devices should or should not be used within the context of the organization. This is a way to highlight unsafe practices that could affect BYOD security, such as allowing unauthorized people to use a device and leaving an unlocked device in an unsecured location.

Establishing acceptable-use guidelines (and educating users about them) is particularly helpful for things that can't be enforced through automated tools or other means, such as physical security.

>>>

Device and App Choice Guidelines

Organizations with serious security concerns regarding BYOD tend to restrict the types of devices that may be used. Common reasons for these restrictions include:

Technological limitations | Security tools, such as enterprise MDM software, typically run only on certain mobile operating systems and certain versions of those OSs. This is particularly true for smartphones and tablets. Also, the organization's key mobile apps may run on only one or a few mobile OSs (and possibly only on particular versions). Therefore, using those apps necessitates using a certain mobile OS and version.

Missing security capabilities | An organization may need to rely on security controls built into the devices of BYOD users, at least to some extent. Accordingly, IT administrators should permit the use of only those personal devices that support the necessary security controls (or that have acceptable third-party applications available to provide the same security function). An example of such a guideline is ensuring that all personal devices have strong disk encryption enabled, so as to protect sensitive information stored on them.

Known vulnerabilities | Certain mobile OSs may have known vulnerabilities that cannot be remediated. An example is an old version of an OS that is no longer supported by its software maker, which means patches will no longer be released to fix known flaws. The workaround for this is to upgrade to a newer version of the OS, but this is not possible with many devices given hardware limitations or a lack of manufacturer support.

Limited technical support capabilities | BYOD users may need technical support with security from time to time, and this may be difficult or impossible for an organization to provide across all possible mobile OSs and versions. Accordingly, IT decision-makers may want to limit which OSs they permit and train technical support staff to handle only those approved OSs. This should improve the quality of technical support for security while excluding only a relatively small number of users with devices running less common OSs.

In addition to restricting types of devices for security-related reasons, many organizations also restrict the apps that users may install on personal devices used for work. Among the common apps often prohibited are third-party file-sharing and backup services. Such prohibitions will reduce the chance of users inadvertently transferring organization data to uncontrolled sites.

There are also technical reasons for restricting app use on these devices, particularly when it comes to apps that will access or make use of the organization's data. Exfiltration of data is a legitimate concern, so it may be wise to allow only those apps that prevent data exfiltration or that are compatible with third-party utilities that prevent data exfiltration.

Organizations may also restrict apps based on reasons similar to those cited earlier for OSs — because of technical limitations, missing security capabilities, known vulnerabilities or limited technical support capabilities.

Incident Response Strategy

Organizations can use their existing incident response strategy as the foundation for creating one for their BYOD program. There are, however, a few significant issues specific to BYOD use that need to be carefully considered and then incorporated into incident response policy, plans and processes.

One problem is that these devices often will be used outside the organization's facilities. This complicates the collection of information from the devices. There is a similar problem with incidents involving mobile devices issued by the organization, such as notebooks used for telecommuting and travel, except that in the case of BYOD, the organization doesn't have full technical control over the devices.

For example, organization-issued devices are likely to have remote management utilities installed that allow an incident responder to remotely take control of the device to

examine it. This capability is typically less likely for the personal devices allowed for BYOD programs.

There are no easy answers when it comes to resolving this problem. If handling an incident requires examining an affected mobile device, then the user may have to bring in or ship the device to the IT department. Naturally, users will be reluctant to hand over their own phones, notebooks and other computing equipment for an extended period so that the organization can investigate an incident that may seem insignificant to the user.

Also, the organization doesn't want to be responsible for personal devices. The most common solution to this problem is to have users sign an agreement before being given BYOD access that requires them to hand over their devices under certain circumstances. Users who decline this arrangement would not be eligible for BYOD access.

Another challenge is getting users to report incidents involving their devices. It can be difficult, if not impossible, for a user to determine on their own if a security breach has affected only their personal information and applications or if it has also affected the organization's information and applications. And users won't want to report incidents unless absolutely necessary because of the possible embarrassment and inconvenience, particularly if they know they will be asked to surrender their device for incident analysis.

Therefore, the best approach is user education and awareness. Users must be made aware of what constitutes an incident and under what circumstances a suspected incident should be reported, erring on the side of caution.

Many organizations require their BYOD users to sign an agreement that spells out the mandatory reporting of suspected incidents, so that users feel obligated to report incidents. Also, users should understand that

>>>

IT'S A PEOPLE THING: **TIPS ON ESTABLISHING BYOD POLICIES**

An explicit policy for a bring-your-own-device program is essential.

A detailed and well-promoted policy will encourage BYOD adoption and user satisfaction. Additionally, it will establish enterprise practices as de facto standards for groups within the organization.

HERE ARE **FIVE TIPS** TO KEEP IN MIND:

1. **Make users aware of the policy and any other rules that will apply before beginning any BYOD program.** Even if any existing employee materials note that the organization reserves the right to remove data on any technology device containing its information, a separate policy makes sense to clarify that the rule applies to organization data on users' personal devices.
2. **Include information about expenses that the organization will and will not cover.** This will vary greatly depending on the organization and perhaps even within an organization, so establishing some guidance will assure users that the expense plan was both well-conceived and fair.
3. **Clearly spell out data removal practices and procedures that will take place upon an employee's departure — whether voluntary or involuntary.** The need for a process for loss or theft is generally obvious, but one for employee departure is equally critical and must not be an afterthought.
4. **Invest in extra training to maintain best practices for mobile device management software.** It will help if one or more of the technologists on staff can become the organization's go-to MDM experts. That way, someone on the IT team is devoted just to this aspect of the BYOD program.
5. **Understand and communicate that enterprise security policies for BYOD are a work in progress.** Although it's important to be as comprehensive as possible in the beginning, an organization will need to tweak security settings as new security issues arise or changes occur in the IT infrastructure.

//// DEVICE VENDORS HAVE ALREADY STARTED TO RESPOND TO THE BYOD TREND BY BUILDING ADVANCED SECURITY CAPABILITIES INTO THEIR HARDWARE. ///

they risk negative consequences if they don't report an incident, such as suspension of BYOD privileges.

A final concern for incident response is user privacy. Users will be understandably reluctant to hand over their personal devices for the organization to examine as part of incident response efforts. Such examinations are likely to cause inadvertent exposure of personal information, activities and other details that the user does not want the organization to know.

This should be addressed in the organization's policies and user agreements, and the IT staff should endeavor to preserve privacy to the maximum extent possible, examining devices only when necessary and taking care to limit the information reviewed on a device.

BYOD Security Solution Planning

This reference guide has focused on the current state of BYOD security. But what does the future hold? Here are some developments to consider while planning out a BYOD program.

Maturation of MDM technologies | Enterprise MDM technologies are rather immature today. Over the coming months and years, they will undoubtedly become significantly more mature.

It is reasonable to expect that many more security capabilities in general will be built into MDM software to reduce reliance on third-party software controls and on a device's own built-in security capabilities. It would not be surprising if NAC agent capabilities were built into most MDM products, thus resolving the need for having NAC technologies that work well with personal devices without requiring installation of a separate NAC agent.

Adoption of additional security controls | In Chapter 2, categories of security controls currently emerging for securing BYOD environments were explained, including host-based firewalls, antivirus software and mobile web security. As mobile devices continue to increase in basic functionality and become more like their deskbound counterparts, CEOs and CISOs may seek out the same kinds of protection for both classes of devices running on their networks.

This will inevitably mean the installation on mobile devices of host-based firewalls, antivirus software and other such security controls, ideally in an integrated suite that will reduce the number of applications that need to be installed to achieve security and make management and monitoring more streamlined.

Product integration | As already mentioned, it's likely that manufacturers will consolidate technologies such as enterprise MDM software with other security controls such as NAC — offering more capabilities in fewer components. This product integration will greatly simplify BYOD security deployment, management and monitoring by centralizing controls in just a few pieces of software.

Reducing the complexity of the security solutions will reduce errors and improve efficiency. It will also minimize conflicts among security solutions, such as having multiple tools trying to perform the same task.

Hardware security in devices | Device vendors have already started to respond to the BYOD trend by building advanced security capabilities into their hardware. An example is mobile devices (including smartphones and tablets) that include a built-in Trusted Platform Module. A TPM is basically a specialized chip that can securely hold cryptographic keys.

Such TPM keys could be used for user authentication, device authentication, virtual private networking and other purposes. A TPM would be capable of protecting both personal cryptographic keys and an organization's keys.

Unification of mobile devices | Smartphones and tablets have always lagged behind notebooks in terms of security features and tools. Recently, smartphones and tablets have become more security savvy, and this trend will likely continue. The lines are already blurring between smartphones and tablets and between tablets and notebooks in terms of functionality.

With similar functionality come similar threats and the need for similar security controls. That's not as dire as it might sound. Eventually, as the divisions between types of devices fade, it should be simpler to plan a security strategy because different devices will have similar security capabilities. ■

This glossary serves as a quick reference to some of the essential terms touched on in this guide. Please note that acronyms are commonly used in the IT field and that variations exist.

Glossary

Acceptable-use policy
This policy defines how computing devices may and may not be used by an organization's users.

Agent-based
Agent-based refers to the architecture of a technology that requires client software to be installed on each device using the application.

Agentless
Agentless refers to a technology architecture that is not agent-based and that generally relies on remote services (such as scanning) for its functionality.

Authentication
Authentication is the technique a system or network uses to verify the identity of someone seeking access.

Biometric
Technologies that use human characteristics, such as fingerprints and irises, for authentication are referred to as biometric.

Bring your own device (BYOD)
BYOD means using a personally owned mobile device, such as a tablet, notebook or smartphone, to perform work on the job.

Cloud storage
Cloud storage refers to services that hold a copy of a user's data within the cloud, such as a backup of data stored on a BYOD system.

Continuous monitoring
This is the process of continuously auditing the security posture of a device or network to detect attacks, policy violations or other problems related to security and operations.

Cryptographic token
A cryptographic token is a hardware or software device to authenticate a user's identity electronically.

Data exfiltration
Data exfiltration is the unauthorized transfer of an organization's sensitive information from an authorized source, such as copying information from a database into an email message and sending that email to an unauthorized person.

Data loss prevention (DLP)
DLP refers to the technologies that protect an organization's sensitive information from data exfiltration by examining data for characteristics that identify it as sensitive information.

Device authentication
This is a process to validate that a mobile device is registered as approved for use on a network.

Digital certificate
A digital certificate is a virtual document that links a cryptographic key with the identity of a person or organization.

Disk encryption
This is a form of storage encryption that involves encrypting all the data on a physical piece of media, such as an internal flash drive or a removable media card.

Encryption
Encryption refers to a technique to protect the confidentiality of data by using a cryptographic algorithm and a secret encryption key to restrict access to only those individuals or devices that possess the secret key.

Enterprise mobility management (EMM)
EMM refers to everything involved in managing mobile devices and related components (such as wireless networks).

File encryption
This is a form of storage encryption that is similar to disk encryption, except that it protects an individual file on a device.

Hotspot
A hotspot is a mobile device that allows other devices to use it as a wireless access point and to utilize its network connectivity.

Incident response
This is the process of detecting a computer security incident and handling that incident, such as documenting it and removing malware and other malicious content from computers.

Key management

Key management refers to all the processes involved in maintaining cryptographic keys, such as securely issuing them and updating them on an as-needed basis.

Media Access Control (MAC)

In the Open Systems Interconnection (OSI) stack, this sublayer of the Data Link Control (DLC) layer provides unique identification and access control for systems on an IP network.

Mobile application management

This refers to the process of deploying and maintaining mobile applications for organizational use.

Mobile device

A mobile device can be a notebook, smartphone, tablet or other similar computing device form factor.

Mobile device management (MDM)

MDM is a class of software used to manage the configuration, including the security configuration, of mobile devices such as smartphones and tablets.

Multifactor authentication

Multifactor authentication is a form of authentication that involves two or more instances of authentication factors — typically, a combination of something the user knows, something the user has and something the user is.

Network access control (NAC)

NAC is a solution that controls access to an organization's networks by examining the security characteristics of a device every time it attempts to connect to the network.

Patching

Patching is the process of acquiring and installing updates to mobile device operating systems and applications, so as to fix problems with functionality and security.

Personal identification number (PIN)

A PIN is a code that might be used to authenticate someone before granting access to a network or application.

Remote locking

This is the process of remotely ordering a managed mobile device to immediately lock, to prevent access until the necessary credentials have been presented.

Remote wiping

This is the process of securely scrubbing data stored on a mobile device once it is believed that the device is irretrievable or has fallen into the wrong hands.

Sandboxing

Sandboxing refers to the technique of wrapping an application, stored data and other computing resources so that the information cannot be transferred outside the wrapper and entities outside the wrapper cannot gain access to the contents.

Security control

This refers to a management, operational or technical mechanism for securing a system or a system's information.

Smartphone

A smartphone is a mobile phone device that has advanced computing capabilities.

Social engineering

The process of tricking people into performing actions that they would otherwise not perform, such as revealing their passwords, is referred to as social engineering.

Tablet

A tablet is a mobile computing device, significantly larger than a smartphone, that is operated by using a large touch screen.

Threat

This term refers to a circumstance that could potentially negatively affect the confidentiality, integrity or availability of an organization's systems or information.

Transport Layer Security (TLS)

TLS is a protocol that provides an encrypted wrapper to surround traffic for a specific application.

Trusted Platform Module (TPM)

TPM is a specialized chip that can securely hold cryptographic keys.

Virtual disk encryption

This is a form of storage encryption that is a hybrid of disk encryption and file encryption technologies; the encrypted "file" is a virtual container that can hold many files.

Virtual private network (VPN)

A VPN is a type of network-level traffic encryption that forms essentially a secure wrapper around network traffic — protecting its confidentiality from eavesdroppers.

Wi-Fi Protected Access 2 (WPA2)

WPA2 is an encryption protocol to secure computers connected to wireless networks, replacing the weaker Wi-Fi Protected Access (WPA) and the older Wireless Equivalent Privacy (WEP).

Wireless access point

This is a communications node on a wireless LAN that connects wireless clients (notebooks, smartphones or tablets) with other networks, including wired networks.

Wireless intrusion detection and prevention system (WIDPS)

WIDPS refers to a series of sensors that monitor all wireless network communications within their range and analyze them for signs of attacks, policy violations and other problems.

Disclaimer

The terms and conditions of product sales are limited to those contained on CDW's website at CDW.com. Notice of objection to and rejection of any additional or different terms in any form delivered by customer is hereby given. For all products, services and offers, CDW® reserves the right to make adjustments due to changing market conditions, product/service discontinuation, manufacturer price changes, errors in advertisements and other extenuating circumstances. CDW®, CDW·G® and The Right Technology. Right Away.® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC. All other trademarks and registered trademarks are the sole property of their respective owners. CDW and the Circle of Service logo are registered trademarks of CDW LLC. Intel Trademark Acknowledgement: Celeron, Celeron Inside, Centrino, Centrino Inside, Core Inside, Intel, Intel Logo, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, Intel Inside Logo, Intel Viiv, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, Viiv Inside, vPro Inside, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries. Intel's processor ratings are not a measure of system performance. For more information please see intel.com/go/rating. AMD Trademark Acknowledgement: AMD, the AMD Arrow, AMD Opteron, AMD Phenom, AMD Athlon, AMD Turion, AMD Sempron, AMD Geode, Cool 'n' Quiet and PowerNow! and combinations thereof are trademarks of Advanced Micro Devices, Inc. HP Smart Buy: HP Smart Buy savings reflected in advertised price. HP Smart Buy savings is based on a comparison of the HP Smart Buy price versus the standard list price of an identical product. Savings may vary based on channel and/or direct standard pricing. This document may not be reproduced or distributed for any reason. Federal law provides for severe and criminal penalties for the unauthorized reproduction and distribution of copyrighted materials. Criminal copyright infringement is investigated by the Federal Bureau of Investigation (FBI) and may constitute a felony with a maximum penalty of up to five (5) years in prison and/or a $250,000 fine. Title 17 U.S.C. Sections 501 and 506. This reference guide is designed to provide readers with information regarding BYOD security. CDW makes no warranty as to the accuracy or completeness of the information contained in this reference guide nor specific application by readers in making decisions regarding BYOD security. Furthermore, CDW assumes no liability for compensatory, consequential or other damages arising out of or related to the use of this publication. The content contained in this publication represents the views of the authors and not necessarily those of the publisher.
©2013 CDW LLC. All rights reserved.

Index

ABOUT THE CONTRIBUTORS

JASON BROWN is the Technical Field Mobility Solution Architect for CDW, helping inform customers about the ever-changing mobility landscape. He works closely with a team of internal and field Solution Architects, assessing customer needs in all aspects of the mobility workplace. With over 18 years of technical experience, he brings a wealth of knowledge to the team, researching updates from CDW's partnerships with the top MDM providers and helping provide successful solutions for education, healthcare, government and small, medium and large enterprise environments.

SHILOH JACKSON is a Security Solutions Architect for CDW and covers the Great Plains region. With more than 10 years experience with network and security engineering, he is responsible for technical pre-sales for the Advanced Technology group in Minnesota, a role that allows him to assist customers in finding real-world, comprehensive security solutions to meet their IT challenges.

KAREN SCARFONE is the principal consultant for Scarfone Cybersecurity. She previously worked as a senior computer scientist for the National Institute of Standards and Technology. She specializes in writing and editing publications on system and network security, incident response and telework security.

LOOK INSIDE FOR MORE INFORMATION ON:

- Implementing comprehensive enterprise mobile management plans
- Securing data in all contexts: network-level, traffic-level and device-level
- Drafting an effective BYOD policy
- Protecting against social network-based threats

CDW PEOPLE WHO GET IT™

ISO 9001 SRI CERTIFIED ISO 14001 SRI CERTIFIED

SCAN THIS!
Lacking a good BYOD offense? Scan this QR code to your mobile device and see what plays IT expert Charles Barkley draws up.

800.800.4239 | CDW.COM/BYODGUIDE

130226 121828