Avoiding BYO Policy and Security Pitfalls

Five practical case studies to help you recognize and address potential threats from using personal devices at work. Written in collaboration with TAL Global, an international security consulting and risk management firm.

When employees use their own technology for business purposes they gain mobility and productivity while blurring the lines between work and personal. This white paper highlights the legal risks of personally owned technology used for business purposes and offers policy recommendations and mitigating technology solutions for enterprise organizations to protect business information.
Today’s highly mobile work environment has pushed productivity beyond the constraints of physical offices, traditional work hours and corporate-issued devices. Employees feel they need to be connected all the time and are using their own technological tools to do so. In response, organizations need to ensure that they have combined policies, procedures and technologies to protect their information assets regardless of where this electronic information is used, is accessed or resides.

Organizations must adapt a set of principles and a philosophy for bring-your-own (BYO) initiatives that are implemented through a combination of synergistic IT, HR and legal policies and appropriate technologies.

BYO policies should indicate:
- What information is sensitive
- Which security measures are mandatory
- What access locations to avoid
- Who pays for a lost/stolen BYO device
- Rules for sharing devices with non-employees
- Access conditions especially after employee termination

Setting optimal BYO policies
BYO policies need to be in place and well understood before the use of personal devices is authorized. They need to clearly indicate which people are able to use their own devices for business purposes and how responsibilities are allocated, with careful attention to employees’ specific roles, the sensitivity of data entrusted to their care and whether they are exempt or non-exempt. The policy needs to be clear on who pays for what in the event of loss or damage, as well as provide guidance on geo-location of the device and remote data or device wipe. Detailed recommendations that specify acceptable devices and technologies to enforce baseline security standards should be in place and enforced for employees, contractors, vendors and any others who use their own technologies to access organizational IT resources.

Other policy components should specify:
- which apps are permitted or excluded
- what data can be accessed via personal devices
- what data is not to be accessed with personal devices.

The policy should dictate in what environments (such as public places) sensitive information can be accessed and what software must be used to do so. Employee-owned devices can be used as long as the organization provides specific guidance on which applications and data need to be restricted by potential work location. This should include public WiFi access, airplanes, etc.

Of course, the enforcement of these policies should be automated to the extent possible—with frequent updates as additional automation becomes feasible. End user actions should not be relied on, so that short cuts cannot be taken and insecure means are not used to access sensitive information.

Organizations need to acknowledge that they cannot control what employees do on their own devices; however, they need to set an acceptable use policy that is signed by employees and enforced by technology. Employees must recognize that the ability to use their own device is not a “right” but rather a “privilege,” and the organization will need to collect information from the device and monitor versions of software, etc.
Consequently, the organization should provide guidance on what data is collected from the employee’s device. Where employees use company-owned devices, the organization should provide guidance on permitted employee activity on these devices, including access to social media, file sharing resources and web-based personal mail. This is where enterprise mobility management technologies can be strategically applied to seamlessly separate work and personal usage on the same device and “keep personal devices personal.”

Access to the device after the individual is terminated or leaves the company may be required for legal purposes so the device must be configured to secure potential access in connection with litigation, e-discovery or investigations. It should be noted that admissibility and value of digital evidence are governed by rules of evidence that are designed to ensure its integrity and reliability and must meet rigorous legal process and requirements.

Policies should be part of a potential employee’s interview process and integrated into contracts with vendors and contractors. The individual and organization should be sufficiently trained, specifically acknowledge the policies and keep an acknowledgement of compliance on file. The use of flexible, consistent and agreed-upon policies will help to reduce the possibility of legal and security issues. Sufficiently appropriate and ideally transparent technologies must be in place to enforce these policies and to prevent deviation from them as much as possible.

The following fictitious case studies are intended to illustrate common legal and security issues associated with BYO and provide policy guidance and technology suggestions to minimize these risks. Policy guidance is provided with each case study. Technology solution recommendations apply across the case studies and are detailed in a special section after all are presented.

“Use of personal technology is a privilege being granted by the organization. In order to take advantage of this privilege, the employee (or contractor) must consent to certain terms and conditions. These conditions can include the installation of software or applications on personally owned devices, monitoring by the organization and access to the devices by the organization after the underlying relationship is terminated.”

Lawrence D. Dietz
General Counsel, TAL Global Corporation
Avoiding BYO Policy and Security Pitfalls

Smith Medical Group LLC
Case study 1

Stanley Smith, MD, FACC, FSCAI, has high-rise offices in Beverly Hills, New York City, Dubai and London. He promotes his practice as one that provides a caring and supportive atmosphere with current surgical knowledge and state-of-the-art technology. Dr. Smith concentrates on a full range of cardiovascular health, treatment and surgery. Business is good and Dr. Smith has recently brought in another surgeon, Max Casey, MD, FACC, FSCAI.

Dr. Smith’s practice is incorporated as a limited liability corporation (LLC) and he is affiliated with a number of local hospitals near his various offices. Dr. Smith has a well-earned reputation for excellence as a surgeon. Like many other surgeons, he is fastidious about the tools he uses inside and outside the operating room. California General Hospital (CGH) is a center city hospital that has been unable to hire its own surgical staff. The hospital relies on Dr. Smith and his colleagues to be on call for emergencies. CGH uses its email system to send patient records to and from physicians. This email is not encrypted. Each of the physicians in Dr. Smith’s practice provides his own smartphone and tablet to retrieve and comment on patient records.

Recently Dr. Casey was in an upscale coffee shop, “Coffeebucks,” preparing for his next operation by reviewing the PDF of a patient record that he just downloaded from Coffeebucks’ free WiFi hotspot. He was studying this prior, similar case to learn more about Dr. Smith’s emphasis on evidence-based medicine.

Dr. Smith, meanwhile, is at Mercy Central Hospital where he is taking a break in the physician’s lounge. He leaves to check on something and when he returns, both his tablet and laptop are gone.

Both of these events have exposed patient protected health information (PHI) to potential compromise. PHI is considered among the most sensitive of all types of information. Dr. Smith needed a policy that ensured patients consented to have their cases used for continuing medical education. The practice also needed a policy that restricted the use of PHI to protected environments where there would be minimal chance of exposure.

“Information is sensitive no matter where it is located. This means that employees should only be able to access sensitive information by using secure means. Use of personally owned devices should only be permitted if sensitive data is compartmentalized and only available to the authorized individual.”

Lawrence D. Dietz
General Counsel, TAL Global Corporation
Franklin Financial Planning LLC
Case study 2

Franklin Financial Planning (FFP) is an independent certified financial planner (CFP). It serves both business clients and individuals. The staff require access to several different investment sources and have their own, proprietary investment tools, some of which are built on legacy Windows software. To encourage creativity and unburden the best sales performers, FFP allows CFPs to use their personal tablets and to back up files on their home computers as well as to consumer cloud services. The company makes aggressive use of graphics that illustrate to customers alternative investment strategies and their respective returns. Franklin does not inspect employees’ devices but does recommend (not provide) security software.

Peter is one of FFP’s star planners. He takes advantage of both his personal tablet and his home computer where, for convenience, he stores copies of all of his customers’ files, including their personal information, credit information, credit card balances, checking account activity, etc. Peter also uses the software as a service (SaaS) tool “AlwaysNote” to keep track of all of his projects and active prospects. To make his life easier, Peter keeps files on each of his current prospects, including their financial data, on AlwaysNote so he can always be ready with answers.

FFP is just asking for trouble. As a fiduciary, it is responsible for safeguarding clients’ sensitive information and is under a high “duty of care” obligation to do so. Client financial information is personally identifiable information (PII) and must be protected. FFP needs to reinforce its policy by ensuring that any device—whether a computer, tablet or smartphone—meets minimal security standards. Also, the company needs to be aware of U.S. Securities and Exchange Commission (SEC) litigation against firms that are negligent in providing duty of care, as it could be the next target. Some financial firms have been targets of class action suits that led to millions of dollars in damages.

“Organizations in selected industries such as healthcare, financial services, government, etc., where there is a higher duty of care for sensitive data than others, must be especially mindful of these expanded responsibilities and should have clear policies and access acknowledgements.”

Lawrence D. Dietz
General Counsel, TAL Global Corporation
**Automotive Accelerators**

Case study 3

Automotive Accelerators (AA) makes components used in premium electric cars. The nature of the business is highly competitive and secretive. While attending one of two major annual trade shows for component manufacturers, an AA executive picked up a brochure from a competitor. The brochure seemed to be featuring a variation of one of AA's soon-to-be-released products. The executive was concerned that there had been a security breach.

AA is a global company. Its headquarters is in the United Kingdom and employees work with designers and suppliers around the world. AA has manufacturing plants in the United States and Mexico. It is not well known, but the company is also exploring sites in Ireland and Hungary.

Ernie Engles, one of the engineers, routinely travels internationally. Wherever he goes he needs access to the design systems that are stored on a computer at each plant. On a recent trip to Italy he needed to work on a new confidential design. However, in an effort to save money, the company travel agent had booked him into a hotel that was in the middle of a renovation. Internet service was not available in the guest rooms. He grudgingly went to the business center where he downloaded a needed file to the hotel's common-use PC. Unfortunately, he could not seem to get it onto a USB device or transfer it to his laptop. Undaunted, he pulled the Ethernet cable out of the hotel's PC and plugged it into his company computer, from which he logged into “Meteorite,” a cloud-based backup service he uses for his home PC. Since Ernie works from home a lot, he had previously downloaded the confidential file from the company server at the plant to his home PC. Meteorite does backup and gives him access to all the files on his own computer through an unencrypted pipe. He downloaded the needed file onto his laptop.

In this situation there are several issues. The company clearly needed a policy prohibiting the use of hotel business centers for accessing confidential information. In this case, Ernie left a sensitive file on the hotel PC. A second issue is downloading of the sensitive file onto the home computer and insecure and uncontrolled access to that sensitive information. The ability to access large files securely from a remote location, perhaps coupled with secure productivity applications, would have helped mitigate the risk in this case. The company should have a policy that prohibits the use of unapproved cloud-based services for the storage of sensitive information.

“Employee use of insecure cloud-based systems for file storage, etc., should be specifically banned with employees specifically acknowledging that they are aware of this restriction and agreeing not to use insecure backup or file repositories.”

Lawrence D. Dietz
General Counsel, TAL Global Corporation
**Extraordinary Customer Resource Management Software Services (ECRMSS)**

*Case study 4*

ECRMSS is a fast-growing SaaS provider of CRM solutions. The firm is targeting the middle market: U.S. enterprises with 500 to 2,500 employees and European enterprises with 200 to 1,000 employees. ECRMSS takes pride in being able to support the latest and greatest technology and has no formal policies with respect to BYO.

Recruiting and retaining salespeople are constant challenges. Over the past several months the company has lost a number of top producers to competitors. The marketing department has noticed that several key customers also left the company for competitors shortly after salespeople joined these organizations.

Sally Superior is one of the top salespeople. She uses her own laptop and tablet. She has regularly downloaded customer files and information to her home computer. She also subscribes to the “Staligmight” suite of services, which includes backup and remote file access as well as the ability to remotely wipe devices.

Sally has just walked into her boss’ office and given two weeks’ notice. A few of her colleagues say that one of ECRMSS’ competitors made her an offer she simply could not refuse. Sally is observed downloading customer information from SalesForce onto her smartphone.

ECRMSS needs to immediately formalize its BYO policies. The organization needs to clearly identify customer lists and information as trade secrets and make them subject to the agreements employees sign before being hired. The company should also have a policy that terminates employee access to sensitive information immediately upon receipt of resignation. ECRMSS needs to restrict the applications and software that employees may use. Employees should not have the ability to massively delete company information or to totally remotely wipe their phones without the consent of the employer. The phone might be an important element in future litigation, for example, and so it is imperative that the employee does not have the ability to destroy any potential evidence.

Today’s mobile business environment, which is blended with personal social connectivity, often means that sensitive company work is done at all hours and on all devices. Organizations that deal with PII, PHI or information falling under the Payment Card Industry (PCI) standard need to be especially mindful.

Certain employees need more guidance and technology to ensure that sensitive company information is safeguarded. This is particularly true of employees engaged in mergers and acquisitions, investor relations and management, as well as those with access to trade secrets and sensitive customer information.

It is imperative to begin building a culture of security with potential employees as early in the qualification cycle as possible.

Organizations in selected industries such as healthcare, financial services, government, etc., which are subject to a higher duty of care obligation for sensitive data than others, must be especially mindful of these expanded responsibilities and should have clear policies and access acknowledgements.

“Technology should be implemented in a transparent manner so that users can’t invent insecure short cuts.”

Lawrence D. Dietz
General Counsel, TAL Global Corporation
“Security policies and procedures need to be written for any party that accesses sensitive information. This includes employees, contractors and vendors.”

Lawrence D. Dietz
General Counsel, TAL Global Corporation

Black, Pinto and Gray (BPG), Attorneys at Law
Case study 5

BPG is a large regional law firm that caters to high-tech companies and is known for aggressive litigation in matters involving trade secrets and patents. BPG’s largest offices are on the West Coast, but a few offices are located in other major U.S. cities and the firm recently opened an office in Shanghai, China.

The company recognizes the sensitivity of its work and responsibility to protect sensitive client information, and requires employees to use company-supplied smartphones. However, BPG is a strong supporter of family time and has allowed selected lawyers to use their home computers. In addition, a few of the company’s top litigators have started to use tablets in court to track evidence, take notes and occasionally show evidence to the jury.

Larry is a litigator in the firm’s New York City office. He is preparing for electronic discovery in a particularly contentious case between two large high-tech competitors. Unfortunately, he is scheduled to deliver a major presentation at an Asian lawyers’ conference in Beijing just prior to a status meeting on discovery. He must work from his hotel room in China to be ready when he returns to New York for this meeting.

Harry is another attorney, but rather than an employee, he is “of counsel.” This means he is a contract attorney to the firm. He is a recognized healthcare law specialist, in part because he was a physician before becoming an attorney. As a contractor, Harry uses his own technology. A medical device maker has retained the firm to defend it in a lawsuit where the plaintiff, a patient, claims that a defective device design caused long-term impairment from an allergic reaction to the component itself. Harry will need access to the plaintiff’s medical records that are introduced into evidence because they address the issue of his medical condition. Harry also needs access to the proprietary designs of the client company and any correspondence relating to the machines, as well as any material that may be turned over to the plaintiff’s legal team as a part of electronic discovery.

The client firm needs to be assured that its remote communications are secure and that sensitive information of any type is not at risk. This means BPG needs policies concerning where attorneys can work and regarding security for sensitive information on joint-use devices to which family members or others may have access. The law firm also needs travel policies for specific countries that describe what types of devices should be used there and how to secure them. BPG might even consider using “disposable” devices that are only used on one trip and then sanitized or destroyed and do not permit sensitive data to be saved to the device itself.
Risk mitigations for described threats

The table below presents the threats and issues from each case and suggests appropriate technologies, including brief summaries of relevant Citrix® solutions.

<table>
<thead>
<tr>
<th>Case</th>
<th>Threats/Issues</th>
<th>Technology</th>
<th>Citrix solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smith Medical Group LLC</td>
<td>Lost devices</td>
<td>Mobile device management</td>
<td>XenMobile® for secure mobile app and device management</td>
</tr>
<tr>
<td></td>
<td>Exposed PHI in email</td>
<td>Secure email and attachments</td>
<td>Worx Mobile Apps for secure mobile email</td>
</tr>
<tr>
<td></td>
<td>Personal tablets and laptops accessing PHI</td>
<td>Secure access to sensitive information</td>
<td>XenApp® and XenDesktop® to securely deliver Windows apps and desktops while keeping sensitive data in the datacenter</td>
</tr>
<tr>
<td>Franklin Financial Planning LLC</td>
<td>Potential exposure of company trade secrets</td>
<td>Secure file sync</td>
<td>ShareFile® for secure enterprise data sharing, sync and storage</td>
</tr>
<tr>
<td></td>
<td>Exposure of sensitive customer PII and PCI data</td>
<td>Mobile access to sensitive business information including enterprise-controlled access to SaaS apps</td>
<td>XenMobile for secure mobile app and device management, including the provisioning of SaaS apps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure, remote access to sensitive information from laptops</td>
<td>XenApp and XenDesktop to securely deliver Windows apps and desktops while keeping sensitive data in the datacenter</td>
</tr>
<tr>
<td>Automotive Accelerators</td>
<td>Trade secret exposure</td>
<td>Secure file access</td>
<td>ShareFile for secure enterprise data sharing and storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure remote access</td>
<td>XenApp and XenDesktop to securely deliver Windows apps and desktops while keeping sensitive data in the datacenter</td>
</tr>
<tr>
<td>ECRMSS</td>
<td>Need to immediately terminate access to sensitive information for people who no longer need it</td>
<td>Enterprise-controlled file sync and share</td>
<td>ShareFile for secure enterprise data sharing and storage</td>
</tr>
<tr>
<td></td>
<td>Customer list and account information exposure</td>
<td>Mobile device and application management</td>
<td>XenMobile to secure mobile app and device management including the remote wipe of enterprise apps and data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure remote access</td>
<td>XenApp and XenDesktop to securely deliver Windows apps and desktops while keeping sensitive data in the datacenter</td>
</tr>
<tr>
<td>Black Pinto and Gray (BPG), Attorneys at Law</td>
<td>Risk of unsecure email communications</td>
<td>Mobile application management</td>
<td>XenMobile for secure mobile app and device management</td>
</tr>
<tr>
<td></td>
<td>Potential exposure of client confidential information from overseas</td>
<td>Secure email</td>
<td>WorxMail™ for secure mobile email</td>
</tr>
<tr>
<td></td>
<td>Potential exposure of PHI</td>
<td>Secure remote access</td>
<td>XenApp and XenDesktop to securely deliver Windows apps and desktops while keeping sensitive data in the datacenter</td>
</tr>
</tbody>
</table>

ShareFile extends cloud data sharing to ensure that enterprise data is both available and protected from the mobile device to the cloud. Email attachments are kept out of vulnerable email systems and backups while being available to authorized users inside and outside the organization. ShareFile is one of the top ways organizations protect files when employees share sensitive data among themselves and with third parties.

XenMobile securely mobilizes apps and data in an encrypted container, with granular policies specifying how data and apps are accessed. From device control to app usage specification to full data management, XenMobile keeps enterprise data under enterprise control – even on personal and BYO devices. XenMobile is complemented by WorxMail, a containerized email, calendar and contact app with a rich user experience.
XenApp and XenDesktop keep apps and sensitive data in the datacenter and provide secure, remote access to these resources. Using virtualization, only the pixels that represent the data are displayed on the client machine, greatly reducing the threat of data distribution and loss.

**Summary of best legal, policy and security practices for BYO**

Minimizing the legal and security risks associated with BYO requires a synergistic combination of policies, procedures based on those policies and technology to serve as a powerful catalyst. Partnering with Citrix, companies can ensure that their data is protected from collection, usage, sharing and storage across mobile devices and geographic boundaries.

Here are some important ways that organizations can minimize their potential BYO liability:

1. **Conduct a thorough evaluation of the potential uses and related risks for personally owned devices in the organization.**
2. **Limit the data and applications that can be used on personal devices or provide security technology to insulate the data from exposure or risk.**
3. **Two-factor authentication should be employed to reduce risk to sensitive data or when data connections may be vulnerable to compromise. It should be coupled with situational and adaptive access controls that reconfigure apps automatically to ensure appropriate security.**
4. **Provide easy-to-comply-with security measures that combine policies, procedures and technologies.**
5. **Conduct frequent audits and monitoring of compliance and updating of policies and procedures.**
6. **Provide effective training and awareness and take special care to craft policies that safeguard information after the organization no longer has a relationship with the employee but might need access to the device for legal purposes.**

These common themes play out every day in organizations that support BYO, remote working, international travel, external collaboration and sharing of information.

This paper is not intended to provide legal advice; instead, it is educational. Legal advice can only be obtained from a properly licensed and qualified attorney in your legal jurisdiction. The information contained in this paper is believed to be complete and accurate; however, its completeness and accuracy cannot be guaranteed.

---

**About Tal Global**

TAL Global is an international security consulting and risk management firm that provides a comprehensive array of investigative, disaster mitigation planning and risk management services, including Executive Protection, Counter Terrorism and Critical Infrastructure Protection, Cyber Security Consulting, and School and Hospital Security. Our extensive international network of professionals enables us to provide our clients with the highest level of security and loss prevention services around the globe.

**About Citrix**

Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.