A LEGAL PERSPECTIVE OF BYOD

Building Awareness to Enable BYOD and Mitigate Its Risks

By Michael Finneran and Jim Brashear
January 2014

zix

THE POWER OF
EVERYONE

In managing the Bring-Your-Own-Device (BYOD) strategy for your company, it's easy to focus on the multitude of devices and mobile applications that make the BYOD trend so overwhelmingly complicated. Companies tend to want to manage employees' devices, apps and connectivity to reduce business risk. One chief source of legal risk, however, is the data – both corporate and personal – that resides on personal mobile devices. Another source of risk, surprisingly, involves potential employer intrusion into employees' personal data. You will get closer to a successful BYOD strategy by appropriately balancing the company's need to protect corporate data against employee concerns about employer controls over personal devices.

What to Consider

- Obligations to protect corporate data
- The complexity of access to employee personal data
- Approach modifications based on your company, employees and culture
- The use of policies and contracts
- The impact of BYOD security solutions
- Maximizing the success of your BYOD strategy

OBLIGATIONS TO PROTECT DATA

There is no denying the efficiency created by mobile devices. No longer confined to an office or laptop, and with their choice of devices and business apps, your employees can fill customer orders on the road, review business documents at the airport and respond to critical emails over dinner. As a result, your corporate data now resides on your employees' smartphones and tablets where its loss or theft can put your company at risk. Your trade secrets, customer and prospect lists and financial data represent only a small portion of business information that can be stored on employees' mobile devices. Similarly, your company may have obligations, under non-disclosure agreements or otherwise, to take reasonable steps to protect data belonging to other companies which may also reside on your employees' personal devices.

While the threat to business data should cause alarm, a breach of sensitive personal information can create a storm of legal headaches. Your employees, customers and patients expect your company to protect Social Security Numbers, birth dates, medical conditions, bank and credit information and other personal data. National and state laws, such as the U.S. Health Insurance Portability and Accountability Act, require your company to protect it. The loss of an employee's unsecured personal smartphone or tablet can set off a whirlwind of expensive responses, such as data breach notifications, identity theft protection, regulatory enforcement and civil lawsuits.

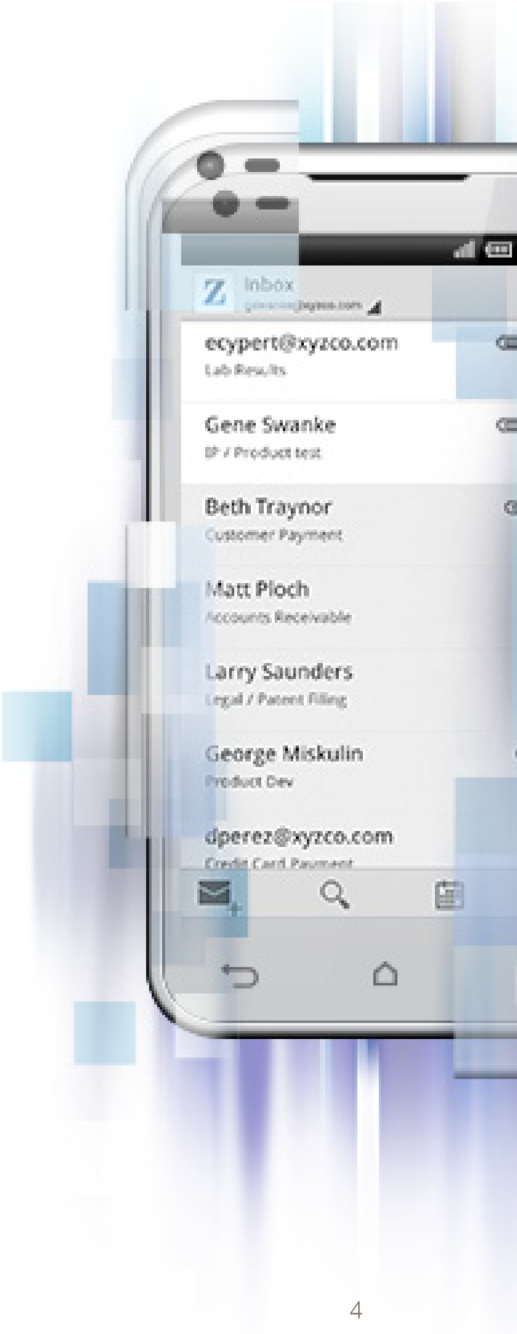
An even bigger risk from the loss of business or personal information may be the damage to your company's trusted reputation. So, safeguarding data on mobile devices should be the focus of your BYOD strategy.

ACCESS TO EMPLOYEE PERSONAL DATA

As employers attempt to protect corporate data and the corporate network by managing personal mobile devices, they potentially gain access to their employees' personal data, including emails, photos and videos, documents, social networking activity, web site history, app usage and location tracking. An employee may claim that an employer's decisions about compensation, promotions or discipline were influenced by the employer's BYOD monitoring activities. The result may be an expensive employment discrimination case. New laws prohibit employers from accessing private content of employee social media accounts, including personal email. That likely covers access that results from monitoring mobile devices.

Another concern about having access to employees' personal data arises when companies trigger a remote wipe to delete data from an employee's device. The destruction of an employee's valuable personal property could lead to a civil lawsuit. Unauthorized destruction of employee data may violate criminal laws such as the U.S. Computer Fraud and Abuse Act.

Some companies try to address these concerns by creating separate work containers and personal containers on the employees' personal mobile devices. That approach assumes employees actually keep their work lives and personal lives neatly segregated in appropriate containers. Moreover, relying on the ability to remotely wipe a device assumes the device will be accessible by you at that time.



ONE APPROACH DOES NOT FIT ALL

In evaluating current or future BYOD policies and deployments, it’s important to recognize that your industry regulations, employee needs and company culture should play a significant role in determining how your company enables BYOD. One approach does not suit all companies. Even within a company, you may want different BYOD policies and solutions for various workgroups. To identify the approaches that best meet your needs, you should start by asking:

To what data and systems does the employee require access? The most secure and cost-effective approach is to give each employee only the access he or she needs. Some work groups need mobile access only to company email but not connections to other company servers.

Where are your employees located? Regulations vary by jurisdiction, so your BYOD approach for U.S.-based employees may differ from your BYOD approach elsewhere. For example, Europe generally has stricter employee privacy laws. Similarly, your BYOD approach in states such as California, Massachusetts and Nevada needs to reflect those states’ personal data breach laws.

What is your industry? Companies in healthcare, for example, face industry-specific privacy regulations that cover personal information on mobile devices. Financial services companies have data retention requirements that affect BYOD policy. Companies that are targets of data theft may need more protective BYOD measures.

What is the makeup of your workforce? The use of BYOD may offer an edge in recruiting younger or tech-savvy professionals. If you have a unionized workforce, or workers councils, implementing strict rules affecting BYOD may present negotiating challenges.

Are there any external factors to consider? The job market for your location or industry could impact how BYOD expands in your company. If the market is hot and your competitors are offering the convenience and work-life balance of BYOD, your company may need to expand your BYOD program faster to entice new employees to join and current employees to maintain their loyalty. However, if the job market is sluggish and competitors are slow to adopt BYOD, then the expansion of BYOD to your workforce may be more flexible.

BYOD POLICIES AND CONTRACTS

The BYOD movement resulted from employee demands that employers provide more flexible IT policies. With company-issued devices, employers were generally comfortable that they could monitor the devices and delete data. Under a BYOD approach, your employees have different expectations about the extent to which their employer should monitor and control a device owned by the employee. Despite containerization and employer assurances, employees fear that their information and activities will be monitored and their data destroyed. Overly liberal and overly restrictive BYOD policies each can create their own problems for the employer. With an understanding of your company's legal obligations and needs, you can collaborate with your legal and HR colleagues to determine the right approach to policies and written agreements.

What is your company culture? If your workforce is open to change and embraces technology in the workplace, then your BYOD implementation may be more widespread. Whether created by your industry, legal obligations or executive direction, some companies are more attuned to employee compliance and policy reinforcement. If your employees are used to taking compliance tests, seeing policy reminders in the hall and making security a priority, then BYOD policies will be easier to accept by your employees and easier to enforce by your company. However, if your culture is more relaxed and does not emphasize compliance, then your BYOD strategy needs to consider how well it will be received and followed by your workforce.

Where does that leave your company? Your company can proceed or modify your current BYOD approach in various ways, including:

- You might leverage policy and consent to the full extent by getting your employees to expressly agree to mobile device management (MDM), including their consent to remote wiping with a clear description of the possible loss of their personal data. Employee backlash or workarounds may be a by-product, but you might decide that business and legal risks created by BYOD should not be overshadowed by employee preferences and concerns.

> "Overly liberal and overly restrictive BYOD policies each can create their own problems for the employer."

- You might provide managers or employees with a set of BYOD security options and allow them to choose the approach that best fits their needs. This approach allows companies to be BYOD friendly and develop employee buy-in for the BYOD approach that best balances the company's data security and compliance needs with employee preferences and concerns. Choices can include:

    - Providing company-owned devices and enabling employees to use them for personal purposes – sometimes called COPE (company-owned, personally-enabled). This traditional approach presents many of the same issues that arise with managing employee-owned devices in a BYOD scenario, although employees may have lower privacy expectations. Employees may implement their own shadow IT with personal devices if they are dissatisfied with the company's approach.

    - Using written contracts and MDM solutions that offer employees device flexibility and optimal network access in exchange for giving up some control over their personal devices. For employees who require it, companies can provide greater mobile access to more company systems, accompanied with more-intrusive BYOD security solutions and an employee contract that expressly gives the company the right to wipe the device or particular containers.

    - Limiting network access and company data storage on the device in order to improve data security and employee privacy. For employees who only need access to certain applications, such as email, calendar and contacts, solutions can be deployed to enable secure access from mobile devices without storing the data on the device, thereby eliminating the need for the employer to control the device and reducing employee privacy concerns.

SELECTING THE RIGHT SOLUTION

Understanding the landscape of BYOD security solutions and how they merge with your company's BYOD strategy is another key step in addressing legal concerns. MDM and containerization, virtual desktop presentation, browser-based services and application streaming require varying levels of legal oversight that needs to be evaluated along with the solution's advantages and disadvantages.

MDM and Containerization: Enables employees to conduct work across numerous office platforms. Whether corporate data is located with personal data or isolated in a container, companies have the controls to monitor and wipe data. However, data is stored on the device and in jeopardy if the device is taken offline so that it cannot be wiped. Employees sacrifice device control and personal data privacy and should be required to sign a contract.

Virtual Desktop Presentation: Enables employees to access work across numerous office platforms. Without data stored on the device, companies do not need to control the device to protect their data and can secure data without a contract or user consent. Employees enjoy full control and privacy but cannot connect when offline. Poor user experience, due to data transmission latency and limited screen visibility, reduces usage and productivity advantages created by BYOD.

Browser-Based Services: Enables employees to access office platforms that have an online version. Browser caching stores data on the device, and therefore companies should incorporate additional measures such as MDM or containerization to secure the data. Poor online user experience, due to full credential requirements and a lack of mobile responsive designs, minimizes use and the productivity advantages created by BYOD. The presence of an MDM or container limits user control and privacy and should require a contract waiving those rights.

Application Streaming: Enables employees to access specific office applications while largely eliminating data transmission latency inherent in full virtualization. Through streaming, data is securely presented in a user-friendly environment and is not stored on the mobile device. Companies control network access without the need for written contracts. Employees enjoy full device control and privacy, but the device must have network connectivity in order to access company data.

In reviewing your BYOD strategy, keep in mind that many factors may influence the solution that is finally implemented. You should involve coworkers with expertise in data security, industry compliance, HR policy and legal liability. By involving those executives early in the process and explaining the range of solutions available, your company can save time and avoid the problems encountered with a one-size-fits-all approach and top-down decision-making. A cross-functional project team will contribute to your insight into issues such as:

- Can your company execute a BYOD program with all employees? What are the benefits? What are the costs? Who needs to approve it?

- Would a single approach work across all participating departments, or would a combination of solutions better meet the requirements of various user groups?

- What devices and versions should to be supported by your company?

- What training and IT support will your employees need to effectively use the BYOD security solutions in place?

SETTING THE STAGE FOR A SUCCESSFUL BYOD PROGRAM

Careful consideration and work goes into building tailored BYOD policies and strategies that secure corporate data, enables employees and mitigates legal risks. Don't let it go to waste without a thorough plan to deploy and maintain that BYOD strategy. Take these extra steps to assist your success:

- Maintain your relationships with influencers and engage executives and other department managers to gain buy-in. With their support, they can encourage employees to accept and work within your BYOD policies and strategy.
- Implement employee training to not only highlight the importance of protecting corporate data on mobile devices but to explain how employees can protect their privacy and personal data.
- Regularly reach out to your legal advisors for updates on changes in laws due to new technologies, compliance or liability concerns.
- Stay current on new security solutions that may better address your BYOD needs and corresponding legal risks.

With the fast pace of BYOD adoption, it's easy to understand why some decision-makers were driven to choose technology approaches that seemed to address one set of concerns, only to learn that they are not a complete solution. Developing a comprehensive view of your competitive environment, company culture, industry-specific regulations, workforce requirements and legal concerns will enable you to fully leverage BYOD and mitigate its risks.

Employee Training

To reinforce the importance of corporate data protection and mobile security, incorporate information and tips that employees can use in their personal lives, such as:

- Protect personal data by using a PIN and auto-lock
- Don't click on suspicious emails or links
- Double-check the URL in mobile searches to avoid phony sites
- Be wary of bad apps that can spread malicious software to devices
- Don't use public Wi-fi to access bank or credit card information
- Be careful of location tracking on social sites

By investing time to help your employees, they will be more receptive to and invested in meeting company needs.

ABOUT THE AUTHORS

Michael Finneran

Michael Finneran is principal at dBrn Associates, an independent, full-service advisory firm specializing in wireless and mobility. With more than 30 years of experience, Mr. Finneran serves as a consultant with vendors, carriers, investment firms and end users on the full range of mobility issues. Mr. Finneran contributes regularly on mobility topics for *InformationWeek*, *Network Computing*, NoJitter.com, UCStrategies.com and Webtorials. Mr. Finneran has published hundreds of columns and articles as well as white papers, research reports, product comparisons and industry research including the "State of Unified Communications" and the "State of Mobile Security" reports for *InformationWeek* Analytics.

Jim Brashear

Jim Brashear is General Counsel for Zix, a leader in email data protection. He is a member of the Bar of the United States Supreme Court, the California Bar Association and the State Bar of Texas. Mr. Brashear's legal experience includes data security, technology, cloud computing and corporate compliance. He is a Certified Information Privacy Professional (CIPP/US) and frequently appears as a public speaker on corporate governance, data security and information technology legal topics. Mr. Brashear earned a juris doctorate degree, magna cum laude, from the University of San Diego School of Law.

ABOUT ZIX

Zix is a leader in email data protection. ZixCorp offers an innovative email BYOD solution, industry-leading email encryption and a unique email DLP solution to meet your company's data protection and compliance needs. Recognized for its easy to use secure email solutions, ZixCorp is trusted by the nation's most influential institutions in healthcare, finance and government, including all U.S. federal financial regulators, one in every five U.S. banks, more than 30 Blue Cross Blue Shield organizations and one in every five U.S. hospitals.

To learn more about Zix and our No-Data-on-the-Device solution, visit zixcorp.com/byod.

zix

THE POWER OF EVERYONE