CYBERRISKS&LIABILITIES

Mitigating BYOD and E-discovery Risks

The prevalence of employee-owned smartphones and other devices in workplaces across the country has grown considerably in the last few years and shows no sign of stopping.

A recent study by Bitglass found that 85% of organizations surveyed allowed their employees to use their personal devices for work functions. If it wasn't obvious already, the "bring your own device" (BYOD) era is here to stay.

While there are numerous benefits of implementing a BYOD policy at your workplace, it can be problematic from an e-discovery standpoint, should your company enter litigation.

E-discovery Basics

Electronically stored information, or ESI, can be subject to discovery, which means it can be requested as evidence in court cases.

ESI is a category of discoverable information separate from print documents, and includes both structured and unstructured data such as emails, instant message logs, Word® documents, PowerPoint® presentations and scanned documents.

In litigation, e-discovery is the process of identifying, collecting, preserving, reviewing and producing relevant electronic data or documents as evidence. Determining which ESI is relevant is not simple due to the lack of precedence and established standards; however, it is important to be able to quickly access the right ESI.

While failing to produce all required ESI can be considered negligence, handing over too much data could mean disclosing privileged competitive information and jeopardizing corporate strategy or product plans.

BYOD's Skyrocketing Popularity

Allowing employees to use their personal phones, laptops, tablets or other devices for work purposes has quickly become the new norm. Employees enjoy being able to use their own devices for several reasons:

- They can get more work done on their own devices with a more flexible schedule.
- They may prefer the operating systems of their own devices.
- Company-provided devices may lack the functionality that employees desire.
- Bringing personal activities into their work lives can lead to happier employees and more productivity.

Employees aren't the only satisfied party. Employers can save money by not having to buy company-owned devices for employees to use, including technical support costs associated with diagnosing problems employees may have.

In addition, many employers can save on telecommunication costs, as employees are often willing to self-fund their own mobile plans.

BYOD Litigation Risks

Allowing employees to bring their own devices can seem like a pretty good deal for both sides. However, there are inherent risks with the practice, especially from a legal standpoint.

Employers must consider the following risks that may hinder the e-discovery process:

- Since you do not own employees' devices, you do not have total control over the devices and how they're used.

BITNER HENRY
INSURANCE GROUP

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice.
Readers should contact legal counsel or an insurance professional for appropriate advice. © 2014 Zywave, Inc. Reviewed 7/2/2020 by Zywave, Inc. All rights reserved.

- There are many different types of data on devices, depending on the operating system, applications used, etc., and separating personal data from business data may be difficult.
- Data on devices can be stored in several locations.
- It is difficult to protect data on employees' devices from harm, including theft and hacking.
- Employers cannot just seize an employee's device for discovery—they need consent from the employee.

Best Practices for BYOD Policies and the E-discovery Process

If you have a BYOD policy at your workplace, or are planning to implement one, consider the following to ensure it is comprehensive and e-discovery-friendly:

- Have employees sign an agreement that lets them know how e-discovery requests will be handled, should the need arise.
- Consider using Mobile Application Management (MAM), which allows employers to control how applications perform on employee devices. It can control application encryption and even wipe sensitive data off the phone of a former employee.
- Consider purchasing and implementing one of the many applications capable of separating business data and personal data, making it easy for employers to locate discoverable data.
- Mandate that employee devices be configured to save certain information directly to the company servers.
- Create an acceptable use policy that lets employees know how you want them to handle company data on their personal devices.
- Prohibit employees from uploading sensitive company data to any third-party cloud storage system, such as Dropbox, Google Drive or Box.
- Sync data between employee devices and company servers regularly.
- Educate employees on best practices for keeping all data on their devices safe—the devices may contain sensitive company information.
- Mandate that employee devices be password-protected.
- Ensure that your BYOD policy is forthright and outlines the exact process for e-discovery, including a clear chain of custody.
- Ensure your IT and legal teams are on the same page. Your IT team should be able to advise the legal team on exactly what kinds of data are stored on employee devices and the best way to retrieve the data. The legal team, whether employed or contracted, should be familiar with the e-discovery process to advance the procedure as quickly as possible.
- Require compliance with your BYOD policy. In addition, keep the policy flexible to keep up with the ever-changing data landscape.
- Determine how you will handle the data on phones of former employees. Some companies remotely wipe former employees' devices, but that can bring up questions about the ethics of deleting personal data from a device.
- Carefully decide which employees can use their own devices. BYOD may not be relevant or useful for all employees.
- Consider listing what devices are and are not acceptable. BYOD does not mean employees are free to use whatever device they wish. Employers may not want to offer support for certain devices due to the particular operating system or inherent security issues.
- Always put data security ahead of employee device security. Your company's data should always be your number one concern.

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice.
Readers should contact legal counsel or an insurance professional for appropriate advice. © 2014 Zywave, Inc. Reviewed 7/2/2020 by Zywave, Inc.All rights reserved.