LOS ANGELES
Daily Journal
www.dailyjournal.com
WEDNESDAY, JULY 17, 2013

LABOR & EMPLOYMENT

'Bring your own device' brings challenges

By Christy Joseph and Kevin Jackson

A day in the life of a busy employee might include contacting valuable clients and recording on her iPad or Android phone confidential information to be utilized later in developing a bid for the client's work. Perhaps on the way home, the employee stops by the doctor and photographs a copy of her latest blood results which cause her some concern and may indicate a health issue she does not want known to others. Exhausted and arriving home, she excitedly sees her son take his first steps and grabs her phone to record the momentous occasion.

The integration of our public, private, confidential and work-related information on one device is a reality — a reality that poses challenges for employers when it comes to the security of company information. These challenges primarily fall into two categories: those related to people and those related to technology. Traditionally, the company's human resources department is responsible for people, while the information technology department is responsible for technology. The successes and failures in the last few years of "bring your own device" (BYOD) implementation have shown that cross-departmental organization is critical. A collaborative approach to BYOD will optimize the company's ability to secure confidential, proprietary and other important information.

One of the fundamental difficulties of protecting employer and third-party information in a BYOD environment is the decentralization and distribution of responsibility for security controls from the employer to the employees. BYOD policies inherently cause a wider distribution of data onto devices not completely controlled by the employer, allowing the element of human error to rear its ugly head. It is not particularly surprising that employee negligence is estimated to be the cause of nearly four out of 10 data breaches. However, employers may be surprised to know many employees still keep work passwords on their device and in a workforce of 1,000 employees, approximately 30 of them will lose or misplace their device at some point. Some of these devices will likely contain confidential, proprietary or otherwise sensitive information and their breach can have devastating consequences for the company.


Shutterstock

The integration of our public, private, confidential and work-related information on one device is a reality — a reality that poses challenges for employers when it comes to the security of company information.

Equally important to containing the human element is creating the technological infrastructure required to secure the BYOD environment. In a recent study, only about a quarter of the IT departments surveyed expect to improve security or risk management in the following year, while nearly half anticipate improving workforce productivity. Issues stemming from the relatively low priority of information security are exacerbated by multiple technologies present in a single workforce. A variation of mobile platforms is inherent to environments that allow individual employees to choose their own preferred device. Before BYOD, a company might issue each employee a Blackberry and its technology infrastructure would be geared toward that specific singular device. Now, in the BYOD environment, a wide array of devices — from iPhones to Androids to tablets and notebooks — must be accommodated and protected. While technology companies have created software to protect devices and networks in this BYOD environment, it is *how people use this technology* that ultimately determines the security of company information. This is where crafting, implementing, training and enforcing departmentally integrated company policies come into play.

A common mistake made by employers when creating BYOD policies is assigning responsibility to just one department. When only one department is responsible for creating BYOD policies, whether that department is legal, HR or IT, the perspective shaping the policies is limited and problems arise. To be effective, policies frequently require input from multiple departments. An example of why this synergy is necessary can be seen in the practice of segregating and limiting access to sensitive information, which is a cornerstone to any effective BYOD policy. Legal requirements might dictate that only certain employees be allowed access to some particular information and input from legal counsel will be necessary to determine which general groups of people should be prohibited or permitted access. HR is in the best position to ascertain the specific individuals who should be placed into one group or the other, while IT is best-suited to choose the technology that can most effectively (and efficiently) achieve the desired result.

Once the foundation of a secure BYOD policy is established, implementing and monitoring the company's BYOD practices are critical. Clearly written policies must be distributed to all BYOD users. Training to ensure understanding and compliance with these policies is strongly advisable. Even the most cutting-edge technology addressing BYOD security can be worthless if employees do not understand their roles and responsibilities. For instance, remote wiping software might seem to be the BYOD safety net in employers' eyes, but the effectiveness of that software is nullified if an employee fails to immediately inform the appropriate people that a device has been lost or stolen. Employees may hesitate before reporting their device missing if the wiping software also destroys needed or cherished personal information saved on it — consider the video of the child's first steps or the confidential medical information that may be housed on the device. Additionally, if the technology used to support a BYOD environment is permitted to become obsolete, the infrastructure will become increasingly vulnerable to breach. Where information security is a concern, the importance of vigilantly enforcing and monitoring BYOD policies simply cannot be understated.

These issues are neither easy nor inexpensive for companies to address, but the consequences of failing to do so can quickly become far more expensive. Loss of valuable competitive information and employee lawsuits bring down business revenues, company value and employee morale.

Christy Joseph *is a partner at Snell & Wilmer LLP. She can be reached at cjoseph@swlaw.com.*

Kevin Jackson *is an associate at Snell & Wilmer LLP. He can be reached at kjackson@swlaw.com.*


CHRISTY JOSEPH
Snell & Wilmer LLP


KEVIN JACKSON
Snell & Wilmer LLP