BYOD: Getting (and Staying) Ahead of the Risk Curve

Employers must craft policies and procedures to mitigate the risks of employees using their own mobile devices.

In a relatively short time, bring your own device (BYOD) has moved from a fringe concept to a widely accepted business practice.

Having employees using their own mobile devices (smartphones, tablets, smart watches, etc.) to conduct company business has taken hold, and it is not expected to go away any time soon.

According to a global survey of CIOs by Gartner Inc.'s Executive Programs, 38 percent of companies expect to stop providing devices to workers by 2016, and by 2017, 50 percent of American companies will be deploying BYOD.

"Employers clearly are embracing BYOD," said Joe Coray, vice president of The Hartford's Technology & Life Science Practice. "Having employees use their own devices brings changes to a company's risk profile, so there are important considerations for employers before adopting a BYOD program."

DRIVING THE BYOD WAVE

BYOD has been growing quickly for a few key reasons. The primary driver has been expected cost-savings, as employers no longer need to purchase devices and data plans, and, fewer company-owned devices require fewer IT staff resources to manage them. BYOD is also viewed as a potential productivity booster.

"While many companies are taking steps toward BYOD, anticipating the benefits," noted Coray, "most adopters have yet to realize those benefits."

"COMPANIES NEED TO BE VERY ASTUTE IN THE WAY THEY RECEIVE AND CONNECT WITH EMPLOYEE-OWNED DEVICES AND AUTHORIZE ACCESS TO COMPANY SERVERS AND DATA."

— Joe Coray, vice president of The Hartford's Technology & Life Science Practice

According to Coray, among the soft benefits of a BYOD program is the attraction and retention of key talent.

"Our culture is shifting to an on-the-go mind-set, and many newcomers to the workforce -- particularly millennials -- are much more comfortable using their own mobile devices in an integrated model," said Coray, noting that organizations that do not allow employees to integrate their personal devices may risk lower employee satisfaction and engagement.

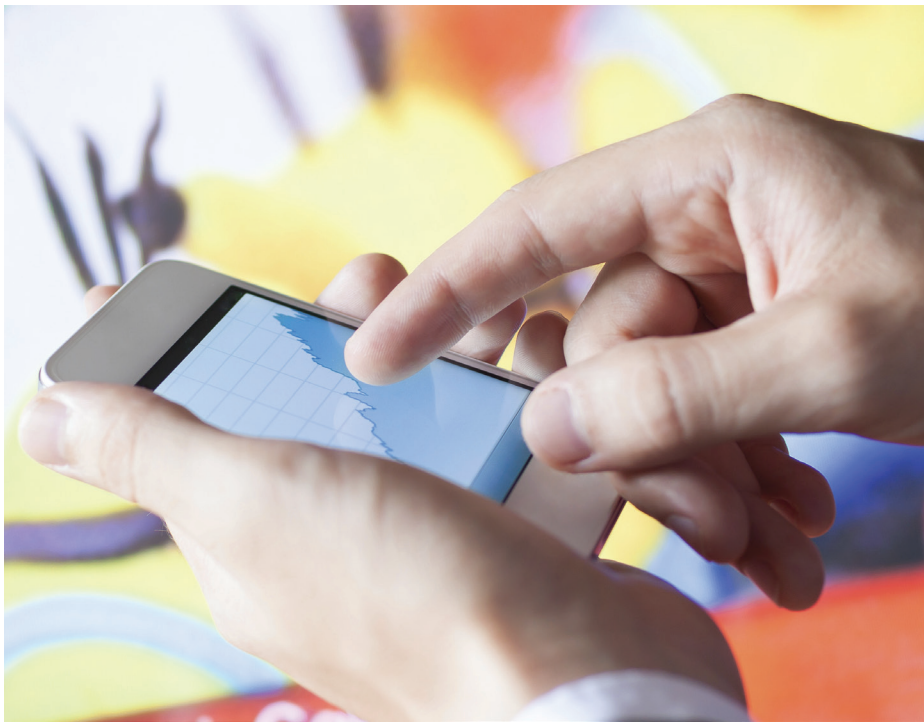
"BYOD is an important consideration for companies wishing to be viewed as a contemporary place to work by current and prospective employees," said Coray.

BYOD RISK CONSIDERATIONS

Naturally, there are specific risks associated with the BYOD trend.

Apart from the obvious exposure to traditional data breaches, companies may have additional exposure to a "more sophisticated" network security event.

For example, a company's email servers could be vulnerable to malware or virus transmissions from an employee's smartphone application originating from use of a social media platform.



THE RISKS and benefits of BYOD programs are complex.

"These vulnerabilities underscore the need for firewalls, strong authentication protocols and other precautions," said Coray.

A company may also want to limit how much of its network an employee-owned device is able to access. For example, an enterprise mobility management application may replicate an employee's email and calendar functions rather than allow the device to access the company's server.

"Companies need to be very astute in the way they receive and connect with employee-owned devices, and authorize access to company servers and data," said Coray.

Companies also need to address user-related risks.

For example, a number of personal device users don't use passwords on their phones or tablets. Also, personal devices often are not exclusive to a single individual. Family members or friends may have access, which can lead to inappropriate use of the device, accessing unprotected networks, and other vulnerabilities.

Also, smartphones are just one type of employee-owned devices being used for businesses purposes. Tablets typically run on Wi-Fi, which is often more vulnerable than cellular networks. This is especially the case if devices are used on public Wi-Fi systems in hotels, restaurants, coffee shops or airports, which are fertile hunting grounds for hackers.

The security of the device is paramount," said Coray, "With the growth of social media, the device itself has become increasingly vulnerable."

EMPLOYER BEST PRACTICES

"CIOs and IT managers need to architect ways to protect their company's data while allowing employee productivity," Coray said. "Vulnerabilities exist, so as companies build out their BYOD policies, they need to include strong use and security management guidelines."

BYOD policies should spell out expectations of both employer and employee related to security, which may include an employer's right to wipe an employee's device of company data if the device is lost or stolen, or if the employee leaves the company.

"With BYOD, employees assume greater responsibility for securing their devices," said Coray.

"If employees expect to use their personal devices for company business, they need to maintain the security of that device."

Ideally, a company's IT department is equipped to support employee-owned devices and ensure that appropriate security is in place to protect company servers and the business-critical data that sits on them.

"These devices are essentially computers that happen to be mobile," Coray said. "We know cyber criminals exist, and if they can get to a company's servers, they can plant malware, steal data or encrypt and hold files for ransom."

Coray emphasized the importance of carriers, agents and brokers working with risk managers to understand the full scope of risk and insurance considerations as they develop effective BYOD policies.

"BYOD is here to stay, and it adds another dimension to the ongoing conversation around cyber risk and ways to prevent, or react to, associated loss," Coray concluded.

Joe Coray can be reached at **joseph.coray@thehartford.com**. *To learn more about The Hartford's Technology & Life Science Practice, visit* **www.thehartford.com/technology**.