Bring your own device
BYOD: Everyone is doing it

THREATS GROW WITH EXPLOSION OF PERSONAL DEVICES AT WORK
At one time, people scoffed at the idea of a personal computer in every home. Today, we not only have high-speed Internet available in our homes, but we also connect to the Internet at will with a variety of mobile devices from wherever we happen to be. Tomorrow, we will be wearing Google glasses that allow us to instantly access all the information we need about anything that can be imagined.

The ubiquity of personal devices is changing the way the corporate world operates. Businesses once built strong firewalls to block external access, banned employees from backing up their work on portable hard drives and allowed connectivity only through company-issued devices. Today, eager to hold down costs and happy to take advantage of well-connected employees, some of these same businesses are adapting their policies to embrace Bring Your Own Device (BYOD). But many more are simply standing by as employees incorporate BYOD into their work lives, without waiting for permission or policies.

Unfortunately, the online-all-the-time reality that employees are creating opens the door to risks and costs that companies should be managing. This is true for businesses across all industries, but even more so for technology companies that may get caught in the crossfire when mobile devices go rogue or provide a gateway for cybercrime. No company can afford to have its own employees be careless with corporate data, but technology companies may also be at risk of liability if products they sold or services they provide are seen as failing to protect customers or contributing to a security breakdown.

In this issue of our Risk Advisor series, we look at both the upside and downside of allowing employees to use their own devices. Topics covered include:

- For many companies, BYOD is worth the risk
- BYOD is here to stay
- How companies benefit from BYOD
- The potential dangers of BYOD
- Strategies for managing risk
- Protect your business financials

With BYOD becoming widespread, it is important for businesses to be proactive about personal device risk management. Our hope is that this Risk Advisor paper will help companies chart a path for creating the most effective corporate policies and protections.

- Mike Thoma
  Chief Underwriting Officer of Global Technology at Travelers

For many companies, BYOD is worth the risk
From the employee side, the solution seems obvious – use their own mobile devices to perform work functions. And indeed, that is what 81 percent of employees questioned in a 2012 Harris Interactive survey say they do.

The reasons go beyond the inconvenience of carrying multiple devices and switching from one device to another. Employees often replace their personal devices more quickly than corporations upgrade their equipment, spurred into getting the most current model by subsidies from service providers. There is also competitive consumerism – many don’t want to be the last to own the newest smartphone. This means their personal devices are often faster, more functional and just plain more fun than whatever their employer is passing out.

In addition, employees today see 24-hour availability as more normal than in the past, when the standard was to have an eight-hour workday and a distinctly separate time for a private life. The overlap of work and personal time has resulted in a desire by employees to connect to work at any time from any place, at their own convenience.

The functionality that employees gain by using their own devices also makes BYOD attractive to them. Corporate IT departments often limit the size of attachments that can be emailed or content that can be stored as a way of improving the efficiency of servers or holding down the cost of adding storage capacity. When employees combine the use of their own devices with cloud-based applications like Google Drive and Drop Box, they avoid limits and increase their ability to work seamlessly with their colleagues. So BYOD makes sense to employees, particularly if the company is willing to subsidize some of the personal cost. For businesses, the BYOD issue is less clear.

Nearly two-thirds of employees told Harris Interactive that their companies have no policies regarding the use of personal mobile devices. In contrast, a separate report by Trustwave found that 26 percent of companies forbid access to corporate data with personal devices, 33 percent have no official policy but tolerate the use, and 41 percent have a formal BYOD policy that dictates how, when and where personal devices can be used.

While it is mathematically possible that the 66 percent of surveyed employees who say their companies have no policy all work at the 33 percent of companies that have no policies but tolerate use, it is much more likely that many employees use their personal devices in either ignorance or defiance of corporate policies.

Regardless of the corporate perspective of the potential impact of BYOD, the reality is that employees are already using their personal devices. In fact, a white paper by Osterman Research released in April 2013 found that the majority of both iPhones and Android phones used for corporate business are owned personally rather than by the corporation.

There is little reason to believe the popularity of BYOD will wane anytime soon – especially in light of the upside for both employees and corporations.
Business thrives on increased productivity – getting more out of assets without increasing incremental costs. For most companies, their most valuable asset is their workforce, and finding a way to keep employees engaged after hours is an opportunity to increase productivity. BYOD facilitates anytime/anywhere connection with employees, encouraging them to keep in touch with communications from work and allowing them to access corporate data at any time.

Another truism is that companies that encourage teamwork and collaboration are more successful than those that do not. BYOD increases opportunities for teams to work together and communicate more clearly, without barriers of time zones or geography. Employees located around the globe are less constrained about communicating when they can ignore the eight-hour workday and reach out to their colleagues on personal devices.

The reduction in corporate cost is also another big benefit of BYOD. A May 2013 report by Gartner puts the average cost of supplying mobile computing devices at $600 annually per employee, an expensive undertaking for mid-size and large employers. This more than offsets the estimated $100 to $300 added costs for security or employee compensation for BYOD programs. While some corporations compensate some workers, at least partially, for the use of their personal device, many do not. Gartner reports that only about half of BYOD programs provide compensation, usually for the service plan rather than for the cost of the device. Only 2 percent cover all costs.

Finally, employee satisfaction, motivation and innovation are strongly linked to the ability to use their own devices. A 2012 Unisys report found that 44 percent of employees find a job offer more attractive if they know the use of their personal iPads are supported at work.

Between employee pressure and the benefits to corporations, many expect the use of BYOD to grow. Gartner predicts that by 2017, almost half of the world’s companies will no longer provide computing devices to employees, while another 40 percent will offer a choice of corporate or personal equipment. The report says the remaining 15 percent will never move to a BYOD model.
The potential dangers of BYOD

A free flow of information and round-the-clock connectivity benefits corporations in many ways, but BYOD is a mixed blessing. When corporations lack control of their data, the possibility that something will go wrong increases, as does the cost of addressing whatever has gone wrong.

For example, an employee who uses a personal tablet to work on company spreadsheets may lose the device (at just seven airports, 7,000 mobile devices were left behind during one 12-month period, according to Trustwave). The employee may upgrade to a different device without wiping clean the hard drive of the prior one, or share it with a spouse or friend who has no authorization to view the information. Among the problems this could cause:

- Businesses that are tightly regulated in terms of retaining data or keeping it private (particularly in the financial services and health care industries) are subject to fines, liability lawsuits and remediation costs when data security is breached, even if the breach occurs on an employee’s personally owned device.
- The incursion of hackers or spread of malware into the company’s database can come through public wi-fi connections used by an employee or infected applications that the employee downloads. Many employees are also lax about security, failing to update their operating systems or install effective anti-virus software on their personal devices.
- Trustwave reports that 90 percent of Android users have not updated their operating system and 37 percent have not activated their auto-lock feature. More than half of companies with a BYOD policy in place report they have experienced a mobile data breach, according to Trustwave. A Symantec survey found that over a 12-month period, 43 percent of organizations reported malware infections from mobile devices.
- The risk that an employee sitting at a desk using a computer mouse will develop a repetitive stress injury can be managed by ergonomic best practices. But what is the liability for a company if an employee files a workers compensation claim based on an injury from the overuse of a personal device that is used for both work and pleasure? In 2012, InformationWeek reported two such claims had been made.

Other problems can occur when an employee no longer works for a company, either by voluntary or involuntary separation. The employee may forget to transfer data from the personal device to the corporate database before departing or may intentionally misuse information stored on a personal device after separation. The loss of control over their own information should be a major concern for corporations, especially those that are required by law to archive and retain information for a certain number of years.

In addition, a variety of legal complications can arise from BYOD, many of which can dramatically increase the cost of responding to lawsuits or government subpoenas. Discovery demands can be broad enough to include all devices used by employees, including their own, whether or not BYOD is allowed by corporate policy. Each device increases the amount of data to be reviewed, which drives legal bills higher.

Technology companies that provide services or products to their customers also may see increased exposure to risk when companies allow BYOD. If they provide security software that fails to block a virus or malware that infects the customer’s network through an employee’s personal device, they may face a claim for damages.

Finally, employees often are unaware of their own risk from using their personal devices. For instance, in the event of discovery demands connected to a lawsuit against their employer, all of their data – both work-related and personal – can be exposed to examination. They may also feel unduly constricted by corporate policies that forbid the downloading of unapproved applications on their personal devices, especially if they are receiving no or little compensation from the company to subsidize the cost of their device.

The answers to the Harris Interactive survey demonstrate why BYOD is a problem:

<table>
<thead>
<tr>
<th>31 PERCENT</th>
<th>46 PERCENT</th>
<th>33 PERCENT</th>
<th>25 PERCENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>connect to their company’s network from unsecured free or public wi-fi.</td>
<td>share their personal devices with others, opening the door to unintended access to corporate data.</td>
<td>say the company data they use and store is not encrypted.</td>
<td>have been a victim of hacking or malware on their personal devices.</td>
</tr>
</tbody>
</table>

Statistics like these are frightening for security-conscious corporate IT teams.
Strategies for managing risk

The most complete and effective defense against the risks of BYOD is to ban employee use of personal devices for work-related activities. However, abstinence can be a tough sell to employees, and non-compliance can be difficult to control. The smarter approach is to put a strong policy in place, educate employees about best practices and take actions that will manage the risk as much as possible.

1. **Policy elements** – A company’s BYOD policy may include what type of devices are allowed to be used, how employees may use devices to connect to corporate networks (such as always using a secured wi-fi connection) and what applications are approved for use, including both downloadable apps and cloud-based tools. It can also set expectations, such as the company making clear it has no responsibility for lost or damaged personal devices or employee injury from misuse of a personal device. In addition, it can restrict the type of data that can be transferred to personal devices, as well as set out protocols for data synchronization and backup. Finally, it can require employees to install the latest operating system updates, corporate-designated anti-virus software, encryption software and remote data wiping capability.

2. **Employee training** – Employees should receive training on best practices for data security. The goal is to have them not only understand all of the elements of the corporate BYOD policy but to also realize the exposure to risk and the consequences if they fail to take the prescribed precautions. For example, few employees are aware that 87 percent of mobile applications tested had one or more security flaws, according to Trustwave, including transmitting sensitive data automatically. When training is complete, employees should know how to access corporate data from their personal devices, which applications are risky and which are safe to use, how to separate work and private data on their devices, and what types of work activities are appropriate for BYOD.

3. **Risk management** – Striking a balance between restrictions to protect the corporate network and the flexibility that will allow employees to use personal devices productively is key. Types of personal devices and applications should be vetted for risk so that companies can make sound decisions about approved BYOD usage. Corporate network protection should be updated with personal device use in mind, including requiring a two-step process for authentication to access the corporate system that recognizes not just the device but also the person using it. Software tools should be in place that allow remote wiping of data, scanning for malware and data leakage, and archiving of corporate data.
Protect your business financials

A Symantec survey found that the majority of companies believe the benefits of BYOD outweigh the risks – but the risks are real. More than half of the companies reported at least one mobile security incident over a 12-month period, including lost or stolen devices (60 percent), spam (60 percent), malware infections (43 percent), phishing attacks (40 percent) and exposure of confidential information (19 percent). Clearly, mitigating exposure to risk is critical.

One important tool is cyber security insurance. These specialized policies go beyond general corporate liability policies, offering specific coverage to address cyber exposures. The best policies include:

- **Errors and Omissions**
  Coverage that protects a business that sells products and services to others when claims are made about their failure to block cyber intrusions.

- **Data Breaches**
  Coverage that takes care of the cost of breach notification, public relations crisis management services, credit repair services, etc.

- **Network Impairment**
  Coverage that addresses losses due to hacking, denial of service attacks and other forms of cybercrime.

Working closely with a knowledgeable broker is the best way to identify the right cyber policy to cover the risks that a company faces.

An evolving world

As mobile devices continue to develop and adoption of BYOD becomes even more prevalent in the work world, new security features and capabilities are likely to emerge. In the meantime, businesses should assess the risk-versus-benefit status of BYOD in their corporate environment, adopt strong policies that protect them while encouraging employee productivity, and take steps to mitigate the inevitable risk that BYOD brings.
SOURCES

Gartner research

Harris Interactive survey
http://www.welivesecurity.com/2012/04/04/byod-infographic-for-security-not-a-pretty-picture/

InformationWeek
http://www.informationweek.com/mobile/6-%20risks-your-byod-policy-must-address/d/d-id/1107451?page_number=2

Legal risks
http://www.informationweek.com/smb/mobile/6-risks-your-byod-policy-must-address/240142320

Osterman research
http://www.ostermanresearch.com/whitepapers/download179

Trustwave graphic
https://www.trustwave.com/trustednews/2013/04/infographic-the-high-cost-byod#sthash vpLp3nzr.dpbs

Symantec survey