The Economics of BYOD Policies and Compliance

Barnes & Thornburg Labor & Employment Department
BYOD – or the concept in which companies allow employees to “bring your own device” to the office to use for work-related purposes – is a growing trend among U.S. and international companies. A recent CISCO study, “The Financial Impact of BYOD,” predicted there will be 108 million BYOD users by 2016 and with that rate of growth comes substantial risk. Experts believe in the next few years, BYOD companies will face increasing compliance and security issues.

While much of the ongoing discussion around BYOD centers on securing devices, encryption, “safe” app stores, and ensuring that networks and infrastructure are up-to-date and capable of handling additional traffic, very few are talking about the overarching issue of training and compliance. In fact, some companies aren’t even paying attention to BYOD risks, according to a recent Dell global security survey.

For good reason, BYOD keeps even the best CIOs up at night worrying about the security of the company’s corporate data. According to a 2013 Symantec study, the average per capita cost of data breaches in the U.S. was $188 (although it varies by industry) with the average organizational cost of these breaches – while decreasing slightly in 2013 – registering at $5.4 million. Additionally, the number of breached records per incident ranged from about 5,000 to more than 99,000.

Creating a BYOD policy and training program can help answer these questions and avoid risks. With the proper guidance from legal advisors and other industry professionals, BYOD companies can sidestep the economic pitfalls associated with an unorganized approach to BYOD.

Key Areas of BYOD

Compliance

One of the best ways to avoid breaches and other major business interruptions as a result of BYOD is to have a clear, realistic and comprehensible policy in place to which employees must adhere.

Of the companies with BYOD policies, almost three-quarters of them imposed highly restrictive rules on their workers by either requiring that the company approve personal devices before the employee is allowed to access the internal networks (43%) or banning personal devices from company nets (31%), which – considering the growing BYOD trend – is neither responsive nor pragmatic.

Restricting employees from using their own phones or placing extreme limits on access to content may result in employees merely ignoring the rules in order to do their job. A 2013 survey reported it is already happening: more than one-third of employees use their smartphones at work without IT knowing or in spite of a workplace ban on personal devices.
Policies

To avoid this type of “rogue” behavior, consider adaptability – rather than domination – when creating a BYOD policy. Companies must approach the policy creation process realistically, be prepared, and clearly understand its employees and what they need, all while effectively assessing and addressing all risks to the company.

When crafting a policy, it is also important to consider who should be involved in creating the BYOD policy. Should the onus fall on IT or compliance? Legal or human resources? Whenever possible, it should be a collaboration among all of these departments.

Employers should first decide the scope of the policy and determine what smartphones and tablets employees are using. Then the company can decide which types of devices to include under the policy and clearly communicate which devices it will and will not support, as well as the information that will be permitted to be accessed through those devices.

The BYOD policy should:

- Require a strong password. Because smartphones or tablets can easily be lost or stolen, most experts recommend that the passwords be alphanumeric.
- Outline who owns what; employers should communicate in the BYOD policy that the company owns the information stored on its servers that the employees access through their devices and explain that the company can wipe (delete) the information stored on the device in the event it is lost or stolen, because that information contains confidential business information owned by the organization.
- Include an acceptable use policy. For example, if a company prohibits access to Facebook or certain objectionable websites via its computers, its BYOD policy would have similar language.
- Additionally, employers should consider adding language in the BYOD policy that requires employees to follow the company’s anti-harassment and non-discrimination policies.
- Explain what happens when an employee leaves the company. When an employee with a personal device separates from an organization, the company could be vulnerable to losing its confidential business information. A thorough BYOD policy will address this by making it mandatory that the employer wipe any company information from the personal device at the time of the employee’s departure, while protecting the employee’s personal information.

Did You Know?

A 2013 survey conducted by Check Point found that 79% of companies have reported security incidents with mobile devices in the past two years, ranging from lost and stolen devices to malware to general device misuse. A majority of those businesses (63%) also said they do not manage corporate information on devices.

In addition to policies, BYOD guidance is making its way into employee agreements, non-disclosures and confidentiality agreements to provide clear definitions of and expectations for what will happen to an employee’s personal device, used in the BYOD context, during and after employment.

Did You Know?

While the Check Point survey unveiled a high percentage of security incidents reported by companies, a separate Gartner study found that only one-quarter of employees admitted to having a security issue on their private device, and even fewer felt obliged to report this to their employer. That points to a potential disconnect between documented and actual security incidents.
Training

A policy means nothing if employees don’t understand or respect it. Therefore, training is as important as creating the policy itself. It is critical to the safety of the company, as well as the protection of company and employee information, that employees understand and embrace BYOD behavior as indicated through the policy.

When conducting formal training, industry experts offer some best practices:

- The first element in the training session should be why the BYOD initiative started, how it is being rolled out and why it is important. Then the company should clearly communicate its acknowledgement of the initiative and its way of managing it. This lays a foundation, which will help employees understand the company’s decisions better and help clear up misconceptions.
- Next, discuss the BYOD initiative in terms of supported devices, mobile operating systems, Wi-Fi, and supported remote access to the company’s network and applications. It is important the employees understand why and how the supported platforms are determined.
- Emphasis should be placed on corporate access, security, data ownership and employee responsibility.
  - The corporate access and security portion of the training should cover how the employees access the corporate network from the corporate Wi-Fi and from the public/hotel Wi-Fi, device password, and loss/theft of the device. VPNs, CRMs, and automation tools, such as SalesForce, should also be covered.
  - Data ownership should cover the corporate/personal e-mail, social networks, corporate/personal contacts and the company data on the employee-owned device.
  - Employee responsibility should be clearly defined whether it’s related to technical details or general compliance with the policies.
- Employees should be trained on the company’s mobile solutions, such as Enterprise Mobility Management and Mobile Device Management. Discuss which applications the company uses, why, what they do, how they manage the devices, and how the BYOD user will benefit from the application.
- Reimbursements also should be covered in the training sessions. Almost all employees will be wondering how the company will handle work-related expenses.
- Finally, the training session should include how the corporate support will be provided to the BYOD users. Emphasize the level of support for everyday use for each device, the escalation paths and the support cases with lost or stolen devices. If a self-service portal is already available on the corporate Intranet, it is better to inform and point the users to the portal during the training.

Did You Know?

Companies that are training employees for BYOD are using internal methodologies to decide how best to train their employees on policies, ethics and codes of conduct. Corporate policy and culture come into play here; there is no one BYOD training “silver bullet.”

- Next, discuss the BYOD initiative in terms of supported devices, mobile operating systems, Wi-Fi, and supported remote access to the company’s network and applications. It is important the employees understand why and how the supported platforms are determined.
- Emphasis should be placed on corporate access, security, data ownership and employee responsibility.
  - The corporate access and security portion of the training should cover how the employees access the corporate network from the corporate

Additionally, BYOD training should take into consideration employees’ previous background and familiarity with BYOD, the devices themselves, and the operating systems, as well as the industries in which the employees work. For example, in the legal industry, discovery procedures should be discussed.

While it may be difficult to get some employees on board – namely, senior management who think the rules don’t apply to them, and younger workers who think the rules are there just to be bypassed – it is critical to communicate clearly that the policy applies to everyone and consequences for noncompliance will be consistent.
The Economics and Impact on Bottom Line

One of the primary benefits of BYOD is the ability to reduce spending by allowing employees to pay part or all of the cost of various devices used for work. BYOD also frees IT from procuring and supporting an expanding array of hardware throughout the enterprise.

The recent Cisco study revealed that 71 million BYOD devices are in use today in the U.S., and that number is expected to grow to 108 million by 2016. These numbers are not surprising, given the reduced costs a BYOD program can offer employers. Cisco has estimated that, if done correctly and comprehensively, U.S. companies can save as much as $3,150 per employee per year with a BYOD program.

However, it is difficult to quantify or monetize such preventive actions as creating BYOD policies and compliance training. What might be more costly is not having control of your data and information during litigation and losing confidential records to departing employees.

Looking Ahead

Though BYOD as a phenomenon appears to be here to stay, Gartner predicts that 20% of specific BYOD programs will fail by 2016. This is one risk that organizations may have to face, as other evolutions will bring additional risks over the next several years as well.

As the “consumerization of IT” continues to take hold, there are potential related trends that will arise; the following points were developed using Network World’s 12 Big BYOD Predictions for 2014. This movement will continue to impact training and compliance requirements for organizations going forward, especially as BYOD policy implementation begins to gain greater market acceptance:

- COPE (Company-Owned, Personally Enabled), or the closely related CYOD (Choose Your Own Device), may serve as mechanisms to ensure that a balance of company interests – security and productivity among them – and employee requirements are met. This would represent a deviation from the currently accepted understanding of BYOD.
- However, another survey says that companies may force their workers to acquire smartphones on their own dime, without stipends. A study by Gartner predicts that 38% of organizations will stop providing mobile devices to employees by 2016 and 50% will mandate a BYOD policy by 2017.
- Tablets and PCs that fall under BYOD policy are growing in number – this could and should mean further training and understanding of risky behaviors, especially as Network World is calling for a hacker-induced BYOD security bombshell in 2014.
- Companies who have gone with smaller Master Data Management (MDM) companies may have continuity issues as vendors are acquired, and Apple and Samsung’s own moves in virtual workspaces and containerization may require corporate agility as solutions change.
- Companies will have to meet their employee needs with respect to file sharing, as unauthorized activity is thriving.
- Users will continue to bring their own devices to work, regardless of whether the organization has a BYOD policy. The current average number of devices connecting to the corporate network is 5.18 per knowledge worker – 4.43 devices across all workers – and predicted to rise to nearly six devices by 2020. In part, this reflects a shift in the nature of the endpoint environment, as traditional desktop PCs give way to a wider range of options for the right mix of device mobility, performance, size and weight, whether it be a laptop, tablet or smartphone.

Did You Know?

BYOD compliance and understanding is generally achieved in organizations through formalized training, or through information disseminated via newsletters and internal networks.
The Internet of Things — the concept that outlines a future where everyday objects will be connected to the Internet and be able to identify themselves to other devices — could radically inject itself in workers’ lives in a variety of ways. On a corporate level, enabled point-of-sale systems could send an alert to a sales representative’s phone or iPad that more product is required. Companies like GE, IBM, AT&T, and Intel are already investing in this sector.

If wearable technology continues to emerge as some are predicting, this would add yet another layer of infrastructure to be managed by IT under the BYOD framework.

As smartphones begin to develop visual spatial awareness and other advanced capabilities, this could have significant ramifications on policies, training, and deployment.

Legacy apps are likely to end, with players like Microsoft moving to a cloud-based offering with Office365. Other players are likely to follow with their own SaaS models.

VDI and DaaS will continue to evolve, and will play a significant role in information access, which will have further policy implications.

Did You Know?

We are seeing several trends: As applications are pushed to SaaS (Software as a Service) models, access to information is evolving through DaaS (Data as a Service) and VDI (Virtual Desktop Infrastructure) and MDM (Master Data Management). CIOs and CSOs will have to continue to work with human resources, legal, and other stakeholders to ensure secure communication and collaboration, and be armed with corporate-approved tools to enable employees to perform their duties efficiently.