COMMERCIAL SERIES

Nationwide®, a member of the Insurance Institute for Business & Home Safety, is proud to present you with valuable IBHS loss control resources.

Is BYOD Right For Your Business Continuity Plan?

Bring Your Own Device (BYOD) policies, which permit employees to bring their own smartphone, tablet and/or laptop to the workplace for use and connectivity, are slowly making their way into business continuity plans as workaround strategies. While motivated initially by perceived cost savings and productivity gains, business continuity planners are beginning to take note of the BYOD policy benefits for resiliency. Employees equipped to work remotely by using their own devices can keep working even when their offices have to close for weather and other disruptive events.

In this regard, BYOD policies can enhance flexibility after a temporary emergency or longer facility outage by providing employees with the capability of connecting to the workplace and each other anytime and anywhere. This makes BYOD particularly attractive for business continuity plans. However, implementation of a BYOD policy raises potential functional and security issues, and therefore should not be done hastily. For example, it's not a good idea to quickly adopt such a policy just because severe weather is posing an immediate threat. Instead, the benefits and drawbacks of BYOD for the specific workplace should be carefully considered, taking into account and addressing the following issues:

- **Acceptable devices and configurations:** Clarify which devices (e.g., smartphones, tablets, laptops, etc.) and operating systems the business will support. Once this is determined, interested employees will have to work with I/T personnel to make sure their devices are configured to be compatible with standardly used apps, internet browsers, office productivity software and security tools utilized by the company.

- **Password policy:** Employee-owned devices used for work must be password-protected. Enforce a strong password policy requirement (such as an 8-digit alphanumeric password with at least one special character). Decide if passwords should rotate after a certain period of time and if they should lock after a certain number of unauthorized attempts.

- **Access limits:** Determine which functions employees can access from their mobile devices (e.g., the entire office suite, corporate email, servers, drives, documents, etc.).

- **Data protection and security:** Decide which type of anti-virus, anti-spam, and anti-malware should be installed on employees' mobile devices. Put in place a policy which requires employees to report lost or stolen devices within a specified number of hours. Businesses should also decide if and how often to conduct I/T audits to confirm employees' mobile devices are in compliance with the security policy.

- **Reimbursement:** Detail if and how employees will be reimbursed for mobile costs (e.g., the actual device, apps used for work purposes, usage charges, extra charges such as roaming charges or plan overages, etc.).

Using Personal Devices for Work Has Become the Norm

Use of personal mobile phones for work purposes is widespread in the U.S. at 61%.

49%	Use of personal phone only for work
12%	Use of both personal & company phone for work

Does your employer have a Bring Your Own Device (BYOD) policy currently in place?

34%	Yes
50%	No
16%	Don't use technology devices

Source: Survey by Tyntec, BYOD User Survey Employees' Choice for Mobility - International Study of BYOD User Preferences, July 2015

- **Employee termination:** It is important to remember to include the steps necessary to disable access to the business' network and servers as part of the exit interview process. If an employee leaves abruptly, businesses should have the ability to remote-wipe the device to remove its data.

- **Mobile phone numbers:** Decide who owns the actual phone number—the business or the employee. Another option is to program the phone with more than one telephone number; there are apps available for download that allow smartphone users to add multiple phone numbers.

- **Signed agreement:** Lastly, a business should create an agreement which lays out all of the above details. The agreement should be signed by BYOD employees acknowledging that they have read and understand the policy.

Like other aspects of a business continuity plan, for a post-disaster BYOD strategy to be successful, it is important to include the use of BYOD in periodic testing of how the business will prepare for and respond to an emergency. Periodic testing will disclose issues that will need to be addressed, such as difficulty in accessing central files. Without testing, those issues will stay hidden until it's too late. Once problems are identified, make sure the plan and the BYOD policy gets updated to account for those issues and weaknesses. Then, practice again as soon as practical to make sure the solutions really work. Testing is the only way to translate BYOD and business continuity strategies into effective action. Otherwise, untested mobile devices and weak BYOD policies will leave a business vulnerable just when it is depending on the system to work.

BYOD is most effective when incorporated into a business continuity plan that focuses on all critical people, operations, information, and financial needs. The Insurance Institute for Business & Home Safety (IBHS) created OFB-EZ®, a free business continuity planning toolkit that helps businesses translate professional continuity concepts into an easy-to-use plan. Small businesses can use OFB-EZ to take advantage of many disaster planning and recovery best practices without the need for a large company budget. Download OFB-EZ today at www.DisasterSafety.org/open-for-business, and consider incorporating the benefits of BYOD into your business continuity plan.

IBHS is a non-profit applied research and communications organization dedicated to reducing property losses due to natural and man-made disasters by building stronger, more resilient communities.

Insurance Institute for Business & Home Safety
4775 East Fowler Ave.
Tampa, FL 33617
(813) 286-3400
DisasterSafety.org