Leaderschoice
INSURANCE SERVICES

Leaders News Alert

October 2013, Volume 3, Issue 10

Bring Your Own Device

Is Your Data Secure Enough for Employee

WITH ABOUT 75% of employees using their own devices for their work communications and productivity, businesses must implement safeguards to avoid company data from being compromised should a device be stolen, hacked or contract a virus.

The BYOD (bring your own device) trend has grown as many employees have eschewed company-issued mobile devices, preferring to use their own. But, while a company can install certain software and make security settings on its own phones, the task is harder when your workers want to use their own devices for their jobs, according to a new study by mobile solutions provider CDW.

Fortunately, the market has responded with systems and software to help businesses secure the personal smart phones and tablets that their employees use to conduct their jobs.

There are a number of benefits to allowing your staff to BYOD, according to the CDW report, including:

- **More employee satisfaction** – It allows them to choose the phone they prefer, and requires them to keep one device.
- **Increased productivity** – When your employees have access to your company's resources, they can do their work from anywhere that is convenient.
- **Cost savings** – You won't be shelling out for phones and cell phone plans, although you may need to pay for various security platforms.
- **Disaster recovery** – If disaster occurs, your staff can work remotely with their smart phone.

Also, because the employees are likely to have their phone plans through a variety of carriers, if one carrier goes down in a disaster others may still be operational.

But, increased mobility comes with more risk to your company's data or the information you store on your customers.

Some employees co-mingling personal and business uses on the phone poses dangers, particularly if the device is compromised and passwords discovered.

The biggest concern is hackers gaining access to an employee's personal files and using them as a gateway to your company's data.

This is made particularly easy if an employee uses the same password for both work and personal accounts.

Locked and loaded

The best weapon currently available for BYOD devices is what is known as Enterprise Mobile Device Management software.

Once the software is installed on your employee's phone, it gives you the ability to set the security configurations for the device remotely.

There are a number of great features with this technology, according to the CDW report, including:

- The ability to prevent data from being saved to removable media that are outside the organization's control.
- The ability to restrict access to software, such as preventing use of the organization's data on a device with applications which the company has not approved for use.
- Encrypting the organization's data stored on a device, to stop unauthorized applications and users from accessing it.
- The ability to monitor each device's security settings in order to detect violations of the firm's security policies.

See 'Security' on page 2

CONTACT US

Leaderschoice
INSURANCE SERVICES

2520 Venture Oaks Way, Suite 310
Sacramento, CA 95833

Phone: 866.211.2123
Fax: 866.913.7036
www.leaderschoiceins.com

License No. 0G80276

If you would like to receive this newsletter electronically, e-mail us at: info@leaderschoiceins.com.

EXCHANGE NOTICES MUST BE SENT TO EMPLOYEES BY OCTOBER 1

THE AFFORDABLE Care Act requires that employers notify all their employees of the availability of health insurance exchanges and that government subsidies are available to qualified individuals.

Under the law, employers must provide these notices to their workers no later than Oct. 1. In addition, after that date they will be required to send the notices to new employees within 14 days of their start date.

The Department of Labor has issued guidance saying it would not levy financial penalties on employers that fail to send out the notices. But it is best to play it safe and comply with the regulations.

The Department of Labor has issued model notices for the so-called health insurance marketplaces.

The model notice for employers that currently offer coverage to their employees is available here:

http://www.dol.gov/ebsa/pdf/FLSAwithplans.pdf

The model notice for employers that do not offer their employees coverage can be found here:

http://www.dol.gov/ebsa/pdf/FLSAwithoutplans.pdf

You should send notices to your employees, regardless of if they are eligible to participate in your employee benefits plan.

Also, if you do not offer health insurance coverage in 2014, but plan to do so for 2015, you will likely be required to send an updated notice of exchanges to employees in 2014 to reflect their status change.

Under the regulations, you have a few options for distributing the notices: hand delivery at work, first-class mail, or electronically.

The law does not require you to obtain a proof of receipt, but it's not a bad idea to have your employee acknowledge receipt in writing so that you protect yourself should you be accused of not providing notices.

Also, these model notices expire on Nov. 30 of this year, so after that you will need to use updated ones. We'll notify you in a later newsletter about the updated notices.

Exempt employers

Small employers that are not subject to the Fair Labor Standards Act, meaning those that have less than $500,000 in annual revenues, are exempt.

Also, common ownership rules set out by the IRS apply, so an employer with several small businesses may be considered as one concern under the law. ❖

Continued from page 1

Security Software in Employees' Phones Protects Data

- The administrator can remotely lock a device if it has been stolen or lost. This will keep anybody without knowledge of the unlock password from using the device.
- The administrator can remotely issue a command and all of the organization's data and applications will be wiped from the phone.

Other measures you can implement include:

- **Host-based firewalls** – These are on top of any firewalls you may have in your network, and are installed on the phone. But these are new solutions and there are not many on the market currently, so choose carefully.
- **Antivirus software** – This too is a relatively new development for mobile devices, but as needs grow the market will, as well. For now, research any software you are considering.
- **Mobile web security** – Many mobile phone browsers include security controls that can help thwart unwanted programs and viruses from getting a foothold as a result of an errant click on a bad link. ❖

Risk Management

Tech Failures the Biggest Threat to Supply Chains

WHILE MOST cyber security is focused on hacking and the theft of important data, a bigger threat is the costly and disruptive effects of a technology failure on a company's supply chain.

Technology outages are the single most common reason for supply chain disruptions, costing companies billions in extra expenses and lost income, according to a new study. The reasons for the outages are varied, from hacking and viruses to technological glitches, and more.

A majority of the companies surveyed (52%) said that they had experienced supply chain disruptions from technology and telecommunications outages, more than from other events such as adverse weather, earthquakes, product contamination and transportation disruptions, the Business Continuity Institute said in its "Supply Chain Resilience 2012" report.

In fact, tech failures resulting from cyber attacks or data breaches can cause as much damage as fire and civil unrest, the institute says.

The report cites numerous examples of how tech failures have created significant operational and supply chain problems, including:

- Various stock exchanges have suffered outages as a result of problems in the software they use to run their trading systems, which cost stock brokerages and investors hundreds of millions of dollars.
- A subsidiary of U.K.-based Imperial Chemical Industries saw a 38% fall in profits after its new supply chain management software went on the fritz resulting in "an inability to locate raw materials."
- The Sainsbury retail chain in England wrote off 260 million British pounds after an IT failure resulted in inventory shortfalls.
- Every year, business operations are disrupted or brought to a standstill as a result of e-mail and phone system outages. And with many businesses now relying on Voice Over Internet Protocol phone systems, an Internet outage also means a phone system outage.

While IT and telecom outages were the most reported problem, and the one that had the most severe impacts, further down the line were more specific cyber threats like data breaches and cyber attacks, which were not rated as damaging in the report.

The most common issues created by these events were loss of productivity, impaired services, loss of revenue, customer complaints and delays in product releases.

IT disruptions result in not only lost revenue, but also cost increases. According to another study – by CA Technologies in 2011 – the average business loses 545 man-hours a year in employee productivity as a result of IT downtime. Businesses can also suffer loss of revenue and reputational damage, particularly from extended or repeated outages.

What you can do

There are number of steps that companies can take to prepare for and reduce the effects of IT/ telecommunications failures or cyber attacks that lead to disruptions.

- One of the keys to surviving and coping with an IT or telecommunications failure is to have a solid business continuity plan in place – one that you test. The plan should include IT outages, and communications with employees, customers and vendors.
- If you rely heavily on suppliers, you should liaise with them to see if they have their own continuity plans in place. You should also verify the plans and capabilities of any IT vendors you are using.
- Consider migrating your data and other systems to the cloud, and then also having a mirror of all that backed up to your server. That way, if either the cloud or your network suffers an outage, you have a back-up plan to keep your operations going.
- Determine which of your IT systems are the most critical in keeping your operations running, and what alternatives you can use should they go down. You may also consider how you can better protect these systems from failure in the first place.
- Also, consider where you are keeping your IT equipment and if it is in an area that is susceptible to natural catastrophe.

An additional layer of protection

Cyber insurance will also cover your costs from an outage. Although these policies when they first hit the market covered mainly costs associated with data breaches and cyber theft, they've evolved and many also will cover various types of technology failure.

Policies may reimburse you for lost revenue, forensic costs, and extra expenses incurred to continue operations as a result of technology failure, network outage, cyber attack or data breach.

Many insurers will offer an additional endorsement that covers business interruption due to the failure of a vendor, like a cloud-computing provider. ❖

Workers' Comp

Costs Rise Quickly the Longer Claims Stay Open

NEW DATA and studies show just how quickly costs can spiral out of control the longer a workers' comp claim stays open.

Recent data indicates that claims that close within 30 days of an injury incur an average cost of $287 (with 90% of those cases being medical only – meaning they required no lost time from work).

However, between 31 and 90 days, the average claims cost jumps 150% to $722 (and the number of medical-only cases drops to 81%), according to information released by Sedgwick Claims Management Services Inc. on its book of workers' comp claims that closed during 2011.

For claims that close between 91 and 180 days after an injury, the average cost jumps to $2,150 and, if it goes beyond that, the average cost leaps to $6,875 when such cases stay open 181 days to one year – that's about 3.5 times more than the $2,150 cost when they remain unresolved for 91 to 180 days, according to Sedgwick's book of claims.

The percentage of medical-only claims drops to a minority of all claims when they are unresolved from 181 days to one year, with only 37% in that category.

When comp claims close between one and two years, Sedgwick's data shows their average cost jumps to $19,888, when only 21% are medical-only claims.

Claims that close between two and three years incur average expenses of $36,792, when the medical-only proportion drops to 13%.

After three years, when fewer than 10% of cases are medical-only claims, the average cost soars to $63,087.

Among factors blamed for average claims remaining open longer than expected while their costs balloon, are the growing incidence of worker obesity and related co-morbidities, Medicare set-aside mandates that complicate settlements, as well as litigation, observers say.

Art of closing claims early

So how can you ensure that your workers' comp claim does not languish and end up costing more than it should?

Risk managers say that to get claims closed early, the injured worker needs aggressive up-front treatment and attention.

Delays in treatment can result in further complications down the road, and what was once a medical-only claim can then turn into one that also includes lost time from work – which means indemnity payments.

Interestingly, these long-term claims often start out as injuries expected to require only limited medical attention without the employer having to pay indemnity benefits since the injured worker remains on the job while recuperating.

In fact, more than half of all workers' compensation claims are medical-only claims, meaning they require no time off from work. You as an employer also have a role to play, and that's being there for your injured worker.

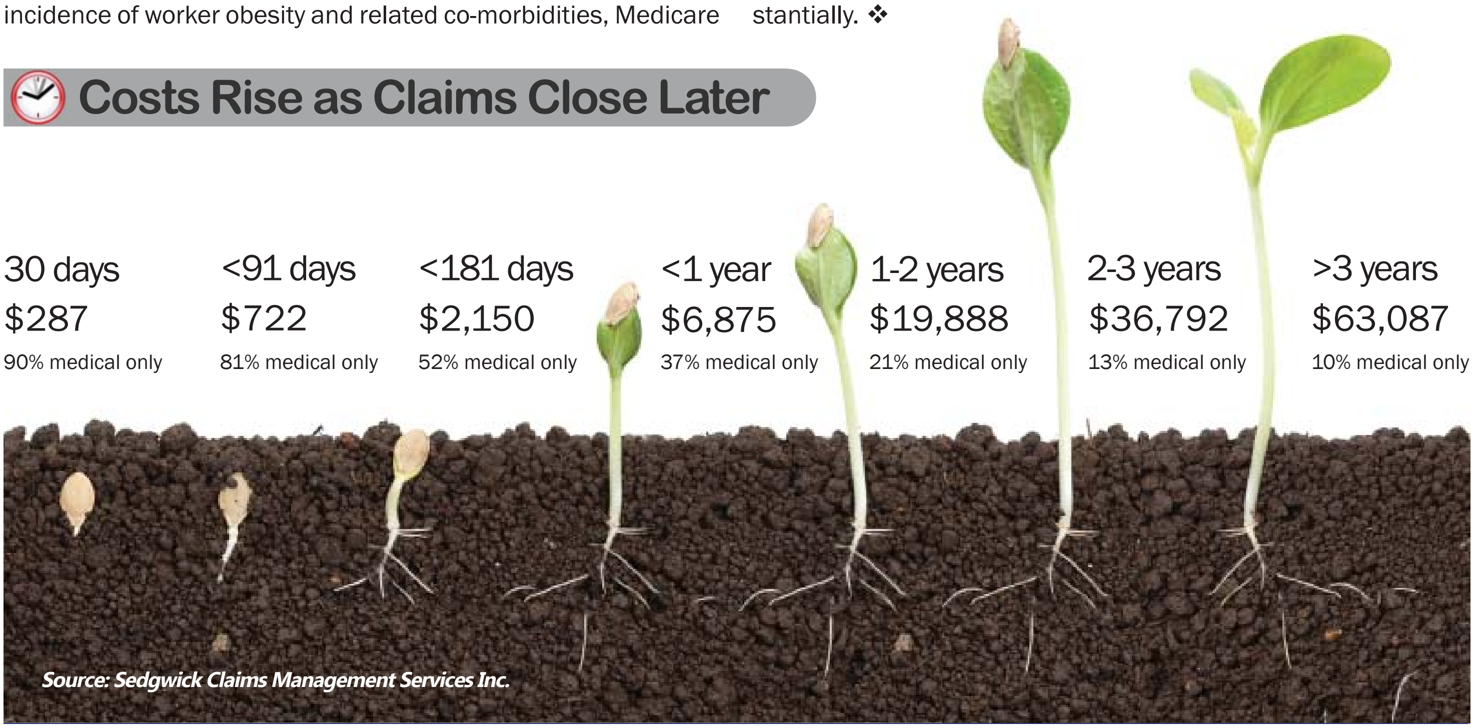
Claims specialists say that claims for workers who are left in the dark can easily take a turn for the worst. After they file a claim, you should contact the employee immediately and let them know that their treatment will be paid for.

Most workers have never filed a workers' compensation claim, and they don't know what to do or what to expect.

And, if they are unsure of what's going to happen, they'll often start by consulting friends, and then searching online. Before you know it they've hired an attorney who may try to move them to a new doctor of the lawyer's choosing.

At that point the chances of closing the claim diminish substantially. ❖

Costs Rise as Claims Close Later



Source: Sedgwick Claims Management Services Inc.