Managing Risk

ZINN
Clear direction from a trusted source
www.zinn.com

Myerstown Office:
16 East Main Avenue
Myerstown, PA 17067
717-866-5717

Lebanon Office:
761 Poplar Street
Lebanon, PA 17042
717-272-6693

Risk Management **Fall 2013** **Volume 23 • Number 4**

Cloud Computing and Risk Management

Cloud computing, which relies on shared networks (typically the Internet), allows users to access information anywhere, at any time. This decreases infrastructure costs while increasing productivity—and risk.

The National Institute of Standards and Technology (NIST) has defined three cloud computing service models: infrastructure as a service, platform as a service, and software as a service. These service models can be summarized as:

- Infrastructure: the provision of processing, storage, networking and other fundamental computing resources;
- Platform: the deployment of applications created using programming languages, libraries, services and tools supported by a cloud provider; and
- Software: the use of applications running on a cloud infrastructure environment.

Cloud computing vendors provide these IT resources over a wide-area network to anyone willing to pay.

Cloud computing poses privacy and security challenges similar to those in traditional computing, but amplified because the cloud computing buyer loses control of information as well as sys-

continued on next page

Risk Tip

The U.S. Supreme Court's decision in *Vance v. Ball State University* will make it harder for employees to win harassment lawsuits by narrowing the definition of "supervisor."

Maetta Vance, an African-American woman, sued Ball State University (BSU) for harassment. She alleged a fellow employee, Saundra Davis, had created a racially hostile work environment in violation of Title VII of the Civil Rights Act of 1964.

The District Court held that BSU was not vicariously liable for Davis' alleged actions because Davis was not a supervisor and could not take tangible employment actions against Vance. The Seventh Circuit affirmed.

The Supreme Court agreed with the lower courts, ruling in

continued on next page

tem components. For these reasons, it creates the following areas of concern for buyers:

Who? Who will control your data? When outsourcing to a cloud vendor, you lose physical control over your organization's data. You will want to know how your data is stored, protected and used, and who will have access to it. You will also want to know who owns it, particularly if your cloud service provider processes your data in any way. If you terminate your agreement with the cloud service provider, will you be able to obtain your data in an accessible, non-proprietary format?

What? What data privacy and security laws and regulations apply to your organization? These laws and regulations vary by industry and by state. The cloud buyer retains ultimate responsibility for its own data and compliance with privacy and security laws and regulations. Can your vendor comply and respond appropriately to data vulnerabilities and breaches?

When? When do you need your data, and how soon? You'll want to know when your vendor schedules maintenance and updates, and how long your information will be unavailable. Service interruptions could also affect access to your information. If you are considering migrating information that's critical to daily business operations to the cloud, consider how long you can do without it and what a service interruption could cost in lost productivity.

Where? Use of an in-house computing center allows an organization to know in detail where data is stored and what safeguards are used to protect the data. In contrast, many cloud computing services store data redundantly in multiple physical locations, which they usually do not disclose to clients. Some laws and regulations prohibit data from being stored across borders. If such laws or regulations apply to your organization, how will cloud computing affect you?

How? How your employees access data in the cloud could put it at risk. Plug-ins and extensions for Web browsers are notorious for their security problems. Many browser add-ons also do not automatically update, increasing the persistence of any existing vulnerabilities.

Smart phones and portable devices create other security problems. Their small size and portability can result in the loss of physical control. Authorized users often ignore built-in security mechanisms, while knowledgeable users can circumvent them to gain control over the device and data or passwords stored within. How will you ensure your employees can access data when they need it, where they need it, without putting it at risk?

To mitigate cloud computing risks, the NIST offers the following suggestions:

Understand the public cloud computing environment. Understanding the policies, procedures and technical controls a cloud provider uses can help you assess the security and privacy risks involved. You should also understand the technologies used to provide services and their implications for security and privacy.

Ensure that a cloud computing solution satisfies organizational security and privacy requirements. Consumers should require, in writing, a cloud provider to meet any laws and regulations that apply, including any that may prohibit the storage of data outside certain physical boundaries or borders.

Typically, a cloud service agreement is non-negotiable, with the cloud provider dictating all the terms of service. If you have particular privacy or security concerns, however, you can request a service agreement negotiated with the assistance of your CIO and risk manager. Negotiated agreements can address an organization's concerns about security and privacy details, such as the vetting of employees, data ownership and exit rights, breach notification, isolation of tenant applications, data encryption and segregation, tracking and reporting

continued on next page

June that an employer is strictly liable for an employee's actions if the employee is a supervisor who can make "tangible employment action." This includes making a significant change in employment status, such as hiring, firing, failing to promote, reassignment with significantly different responsibilities, or making a significant change in benefits. If the fellow employee is not a supervisor, the employer is liable for harassment only if it was negligent in controlling working conditions.

For information on protecting your firm from harassment and other employment lawsuits, please contact us.

service effectiveness, compliance with laws and regulations, and the use of validated products meeting federal or national standards.

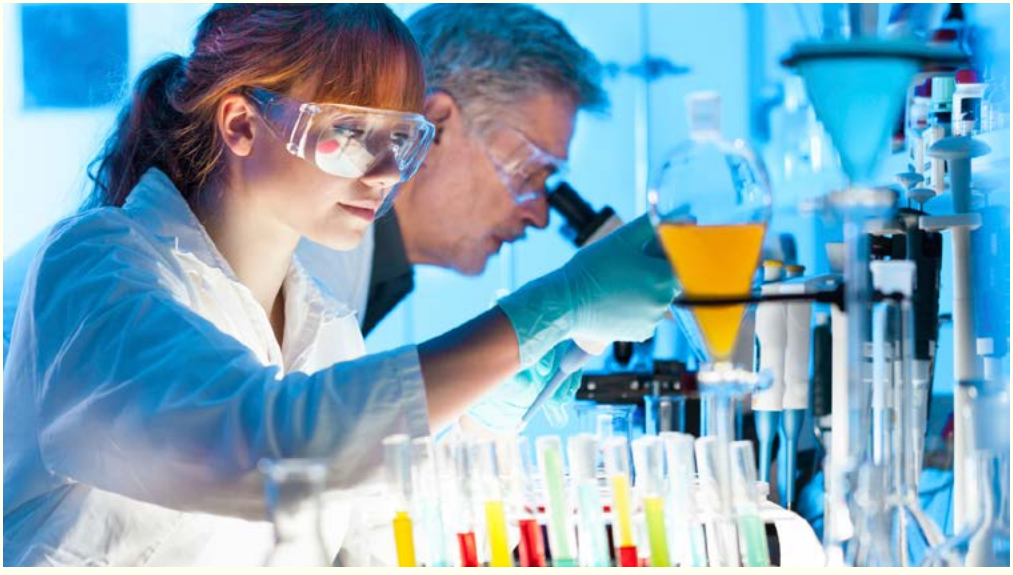
Regardless of whether you negotiate a contract, you will want to review agreements for the following:

- Data ownership and disposition. Agreements should clearly state that your organization retains ownership of data and how long the vendor will retain your data after your agreement terminates. Consumers should require that a cloud provider offer a mechanism for reliably deleting consumer data on request as well as providing evidence that the data was deleted.
- Legal. The judicial process sometimes requires defendants to provide access to information during the discovery process. If that information is in the cloud, it might need to be "frozen" to reflect its state as of a specific date. Can your vendor support such requests?
- Limits of liability. What level of liability does the service provider retain for loss or breach of your data? Does it have appropriate insurance coverage?

Because an organization retains ultimate responsibility for the privacy and security of its own data, regardless of where it is stored, we recommend cyber insurance coverage for organizations that use, store or have access to the personal identifying information of others. For more information, please see the article on P. 6 or contact us.

Genetic Discrimination: The New Liability Frontier

In May, the first genetic discrimination case filed by the U.S. Equal Employment Opportunity Commission (EEOC), settled when an employer agreed to pay $50,000 and furnish other relief. Is your organization next?



The case serves as a warning that the EEOC is taking enforcement of the Genetic Information Nondiscrimination Act (GINA) seriously. The EEOC filed suit against Fabricut, Inc., one of the world's largest distributors of decorative fabrics, for violating the Americans with Disabilities Act (ADA) when it refused to hire a woman as a memo clerk because it regarded her as having carpal tunnel syndrome, and for violating GINA when it asked for her family medical history in its post-offer medical examination.

"Employers need to be aware that GINA prohibits requesting family medical history," said David Lopez, general counsel of the EEOC. "When illegal questions are required as part of the hiring process, the EEOC will be vigilant to ensure that no one be denied a job on a prohibited basis."

continued on next page

Title II of GINA became effective on November 21, 2009 and applies to all private employers and state and local government employers with 15 or more employees, employment agencies, labor unions, and joint labor-management training programs. It also covers Congress, federal executive branch agencies, and the Executive Office of the President. GINA makes it an "unlawful employment practice" to take discriminatory employment actions against an individual because of genetic information. The Act specifically prohibits failing to hire or discharging an employee on the basis of genetic information.

Specific Exceptions

GINA also prohibits any employer or related entity from requesting, requiring or purchasing an employee's genetic information, unless they are using it (1) to comply with certification requirements of family and medical leave laws; (2) for monitoring the biological effects of toxic substances in the workplace; or (3) for DNA analysis for law enforcement purposes or for purposes of human remains identification, when the employer is a forensic lab.

The law also allows employers to request genetic information for health services, such as under a wellness program, when the employee provides prior written authorization. In all instances, the employer must treat genetic information as confidential and maintain it in separate medical files.

Employees who believe an employer has used genetic information to discriminate against them may file a claim with the Equal Employment Opportunity Commission (EEOC). If the EEOC finds evidence of discrimination, it can file a lawsuit on behalf of the plaintiff in federal court or give the plaintiff a "right to sue" notice. If the employee prevails, possible damages include compensatory damages, back and front pay, and equitable relief.

Your commercial general liability (CGL) or business owners policy (BOP) typically excludes employment-related claims. Employment practices liability insurance (EPLI) protects an organization, its directors and officers from lawsuits by current, prospective and former employees, including claims for genetic discrimination and other forms of discrimination. We can provide more information on this non-standard coverage— please contact us for details. ■

Preventing Opioid Abuse

Opioid drugs used in workers' compensation cost employers an estimated $1.4 billion in 2012. However, much of this use is unneeded and possibly dangerous.

The Problem

Opioid pain relievers (also called narcotics) derive from opium and include morphine, heroin, oxycodone, and the synthetic opioid narcotics. Medical experts recommend their use only for short-term pain relief due to acute conditions such as cancer, when a patient does not respond to other therapies. According to the National Institutes of Health, "Almost always, you should limit their use to no more than 3 to 4 months." However, between 55 and 86 percent of all workers' compensation claimants receive opioids for chronic pain relief, said Keith E. Rosenblum, a senior risk consultant with Lockton Companies.

Opioid drugs used in workers' compensation cost employers $1.4

continued on next page

billion in 2012, estimated Joseph Paduda, president of CompPharma, LLC, a consortium of workers' compensation pharmacy benefit management (PBM) firms. In a white paper called "Wasted Dollars, Wasted Lives—How Opioid Overprescribing and Physician Dispensing Are Harming Claimants and Employers," Paduda also noted, "There is ample evidence that long-term opioid use leads to longer claim duration, long-term disability, higher costs, and higher medical expenses."

Many studies show that after 90 days of continuous use, opioid treatment is more likely to become lifelong. When used long-term, opioids can create changes in a person's opioid receptors. This can diminish a person's natural abilities to modulate pain and creates a tolerance for the drug. Over time, a person will require higher doses for effective pain relief, which can lead to abuse, addiction and increased risk of overdose.

The number of accidental deaths associated with the use of prescription opioids has increased dramatically since 1999. In fact, the number of accidental deaths resulting from prescription opioid use now exceeds the number of deaths from heroin and cocaine overdoses, reported the Centers for Disease Control. The misuse and abuse of prescription painkillers led to more than 475,000 emergency room visits in 2009, twice the figure for 2004.

Researchers have also linked long-term opioid use to poor workers' compensation claim outcomes. A study published in the Journal of Bone and Joint Surgery in 2009 reported that chronic opioid use after a work-related injury predicted "less successful outcomes." The researchers found that higher dose levels were associated with higher costs for indemnity and medical costs for disability. Opioid users were also less likely to return to work. Among injured workers completing a functional restoration program, those who were using opioids at the time of admission were half as likely as the users to return to work during the year after treatment. They were also more than 2.6 times as likely to not be working at the one-year follow-up point.

The Solutions

Promote the use of alternatives to opioids. The American College of Environmental and Occupational Medicine recommends that physicians treating occupational injuries consider other treatments before prescribing opioids. "Depending on the exact diagnosis, these treatments may include exercise, topical medications, distractants (e.g., heat), NSAIDs, low-dose heterocyclic anti-depressants, anticonvulsant agents, and self-applied palliative modalities such as transcutaneous electrical nerve stimulation (TENS)." It also stresses the importance of active exercise and return to work in conjunction with opioid use.

Test opioid users. Although medical treatment guidelines recommend periodic drug testing and psychological evaluation for long-term users of opioid drugs, studies have found few physicians observe the guidelines. Only 24 percent of long-term opioid users in one study received at least one drug test. Ideally, treating physicians should screen workers' compensation claimants for prior opioid use before prescribing, since prior use increases the risk of tolerance and addiction. Second, treating physicians should require drug testing at regular intervals to monitor patients for compliance. Are they using the drug, and at the level prescribed? Many opioid users will stop using the drug on their own initiative, while those who become dependent will "doctor shop" and obtain prescriptions from more than one physician.

Better management of prescription painkillers can lead to better coordination of care among multiple providers, earlier intervention with patients at risk of addiction or overdose, and better treatment outcomes. All of these can reduce unneeded costs for employers and make valued workers more likely to return to work after an injury. If overuse or misuse of opioids might be a factor in your organization's workers' compensation costs, a third-party administrator or prescription benefit manager can help you evaluate and/or monitor drug use patterns among your injured workers. For more information, please contact us.

Cyber Insurance Covers the Cloud

A recent claims trend study found that cloud service providers and other third parties are responsible for approximately one-third of cybersecurity vulnerabilities and resulting cyber incidents. That fraction is likely to increase, since most companies have begun putting sensitive information into clouds only in the past year or so. Some cloud service providers are now outsourcing this data to other cloud service providers, a trend that could create a "spider web" of liability in event of a breach.

When they can, customers need to negotiate and specify in cloud contracts what losses are covered, by whom, and at what levels. However, unless your organization is large and influential, you may have little negotiating power.

Cloud service providers will not accept liability for losses to your data (property coverage). When they do accept liability to third parties resulting from loss or breach of your data, they usually limit it to the service they've agreed to provide. Traditional commercial general liability policies typically exclude data-related risks; however, specialized cyber insurance can protect your organization from data-related risks, including cloud computing.

Cyber insurance policies may include first-party coverage against losses such as data destruction, extortion, theft, hacking and denial of service attacks. They may offer liability coverage that indemnifies you for losses to others caused by errors and omissions, failure to safeguard data or defamation. They also offer other benefits, including regular security audits, post-incident public relations and investigative expenses, and criminal reward funds.

Insurers require organizations to maintain a level of security as a precondition of coverage. Typically, an underwriting analysis will include a review of: 1. General risk exposure of the industry and business activities, 2. general risk exposure of the size of the company, 3. loss history, 4. years in business, 5. financial condition, 6. extent of use of outsourced network security services, 7. dependency on third-parties' networks, and 8. in-depth analysis of network security. For more information, please contact us. ■

Managing Risk