Enemy at the Gate: Data Security Risks in Workers' Comp

Unlike other industries, most notably health care, the workers' compensation industry has not been directly affected — at least publicly — by data security problems. But that peaceful prelude began to wane in September 2013 with the implementation of the HITECH Act, which also regulates comp industry security and privacy controls. As if that wasn't enough, massive breaches at some of the nation's largest health plans, not to mention the mega-giant retailer Target, raised industry concerns about data security. After all, comp utilizes critical data such as Social Security numbers and demographic information, not to mention personal health information (PHI).

Our industry certainly could be, and perhaps already is, at risk. Lack of strong data security could expose an organization to millions of dollars in litigation, damage control and repair costs. The well-publicized Anthem data breach is likely to cost more than $100 million.

Assuring Data Security

The ability to show strong data security controls is critical for employers and carriers. Assurance of data security knowledge, systems and protocols is becoming a routine line item for industry RFPs.

Companies want assurance that their data will be stored and backed up securely and in a physically safe location, that there are controls for who can access data, who can share information and the manner in which data is shared (e.g., secure email server).

But beyond the basics, what do program managers and those not directly in the world of information technology need to know? Where do data security and program performance intersect?

GENEX Services, with some of the most advanced security protocols in the industry, has some insights for workers' comp professionals who may not work in information technology but need to understand the issues and language to ensure their organization is asking the right questions. There are three types of controls:

1. Administrative – including background checks and, use of confidentiality agreements, privacy and security awareness training, and change/incident/patch management policies and procedures.
2. Technical – primarily IT functions such as anti-virus, intrusion detection and prevention services, network segmentation, and web and email filtering.
3. Physical – including access to buildings and strict data center access controls, key fob or card entry building access systems, CCTV, BCP/DR plans for critical services, and N+1 redundancy for critical environmental items, such as power and HVAC.

Identifying the Risks

There are a number key domain risks for the industry. The primary worry is unauthorized access to PHI, which could be used for identity theft or even blackmail. Unfortunately, there are many ways for such data to be accessed. Data is always in motion in comp claims as there are various vendors, case managers, bill review specialists, and independent medical examiners (IME), all transmitting and sharing files and forms every day.

WHAT IS HITECH?

According to the U.S. Department of Health and Human Services,

"The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on Feb. 17, 2009, to promote the adoption and meaningful use of health information technology. More specifically, it addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules." Enforcement of this Act went into effect September of 2013.

Your data security goal should be to ensure your data never leaves your organizations' technology or devices.

Indeed, transfer of data to vendors is one of the most common security risks for any industry. It is important to carefully vet vendors to ensure their security controls are in line with your organization's standards, including regulatory controls and HIPAA.

Password management is also critical. They should be easy to remember, but not overly simplistic and be changed more than twice a year to reduce potential risks. An organization will want to establish password parameters for all applications and networks, including how often passwords are changed and how long and complex they should be.

Remember that exposing claim information to the Internet is also risky. Today's emphasis on a mobile workplace, with smartphones, tablets, laptops, etc., exacerbates risk from the Internet. In addition, just as we have seen recently on the political stage, using personal emails to transmit company documents can be dangerous.

Securing Your Data

So what steps can be taken to better security?

- Create a security triangle aimed at ensuring administrative, technical and physical controls are always highly secured and monitored. Administrative controls ensure all employees have background checks and drug screening when hired. Another step is to require passwords to be complex (but not to the extent they are hard to remember) and changed frequently, typically no longer than 90 days.
- Ensure technical controls are being adhered to properly and that a process for continual review and improvement is implemented.
- Provide clear guidance and instruction to employees regarding restrictions on using personal devices to transmit company data. Be very clear what can and can't be sent over the Internet.
- Ensure antivirus programs are installed on all systems and virus definitions are updated often, ideally every three hours.
- Encrypt data on the C drive, data-in transit, and databases on servers. This helps in the event someone loses a laptop, or if laptops or other mobile devices are stolen. Server based encryption guards against data access from unauthorized internal users, or malicious insiders.
- Implement role-based access protocols (e.g., which department or individual can access data) and then limit the number of people who have full access to everything.

- Train employees in security privacy awareness. It is important to do this systematically — once a month or quarter. Structure training to increase awareness of issues, but also to provide advice, and answer questions.
- Guard against email phishing. We all know about the "I'm an Ethiopian prince" email, but new, more sophisticated scams come out daily. Be aware of anything involving shipping or delivery of product, and warn employees to be especially wary of unsolicited emails purporting to be from government agencies and popular internet ecommerce sites, such as the IRS or PayPal, especially during tax season, and high volume online shopping periods.
- Tell all employees that data security is their responsibility. Remind them that as a company you put processes in place, but they must abide by rules and use common sense.
- Make sure your vendors communicate the importance of security to their employees, because all links in the data security chain must be strong.

Remind employees to remain vigilant when individuals — especially adjusters, providers and claimants — send emails containing PHI such as address, date of birth, Social Security number, etc., through non-secure servers such as a Gmail account. These senders need to be informed and educated of the dangers associated with nonsecure platforms.

Don't be quiet. Yes, yours may not be the organization sending the data, but it is up to each individual to strongly recommend that personal information only be faxed, mailed or sent through secure electronic channels. Little missteps often lead to the greatest threats to security.

IF TROUBLE ARRIVES

What happens if there is a breach, natural disaster or other event that causes a loss of data? While your organization may have a plan, ensure that your vendors also have a well-thought-out strategy to resume business at the field-office level as well as recovery capabilities at the main office. Make sure data can be quickly brought up from a secondary location in the event of a disaster or breach. Look for companies that can offer recovery time options for your basic functions, such as case management data, within three to six hours for RTO and RPO. Identify the point that data is accurate: it should be within 10 minutes of the outage. For tier zero applications such as internal call systems and network links, email exchange, etc., you need to transfer to a recovery site within a few minutes — ideally so quickly that the customer isn't aware there was a problem.

WHAT KEY DATA SECURITY ACRONYMS MEAN

TLS – Transport Layer Security – security protocol utilized to encrypt communications over a computer network.

CIA – Confidentiality, Integrity, Availability - triad model designed to guide policies for information security within an organization.

SDLC – Systems Development Life Cycle – term used to describe the process for planning, creating, testing and deploying an information system or application.

RTO – Recovery time objective is the amount of time it takes to get back online

RPO – Recovery point objective refers to the point in the data where you want/need to be able to recover data

Must-have Security Capabilities

To be sure that your workers' comp data is secure, check for these five key capabilities when looking for managed care partners:

1. Utilize the latest technology and platforms
2. Integrate seamlessly with existing technologies
3. Provide reports and updates on security status
4. Offer education and data security training to adjusters and relevant key internal staff
5. Feature industry leading RTO and RPO

Can Paranoia be Good?

The importance of data security can't be overstated. Targeted attacks are coming from sophisticated organizations around the world. The good news is many in the workers' compensation industry are stepping up their game by investing in new technologies and prioritizing security.

However, the workers' compensation industry must follow the lead of the best of the best in data security, such as banks and airlines. If we don't, we too could see massive security breaches.
A healthy dose of paranoia is a necessity for today. It is clearly in the best interest of our industry, and of workers, to err on the side of caution.

GENEX Services, LLC
440 East Swedesford Road, Suite 1000
Wayne, PA 19087
888.GO.GENEX | genexservices.com