Insurance Service Providers and the Communications Circle

March 10th, 2015

Presented by:

Sean Cassidy- Benchmark IME

Security Breaches Affect Us All

New York

According to New York's Attorney General, 22.8 million private records of New Yorkers were exposed due to data breaches over the last eight years. The data breaches were reported by over 3,000 businesses, nonprofit organizations and government agencies. Intentional hacking exposed most of the accounts, accounting for 40% of the 5,000 incidents. Lost or stolen equipment, insider wrongdoing and inadvertent errors were also major factors.

Security Breaches Affect Us All

UPS

In August, United Parcel Service reported a data breach occurred in 51 of their Stores, possibly leading to the theft of customer debit and credit card information. Malicious software that was not identified by current anti-virus software led to the breach. Names, postal addresses, email addresses and payment card information may have been exposed.

BENCHMARK

EXPEFLOW
Expedite your workflow.

Security Breaches Affect Us All

Community Health Systems

In August, Community Health Systems said information on 4.5 million patients was stolen in a cyber attack that may have originated in China. The data breach may have impacted anyone who was a patient in a CHS hospital during the last five years. Hackers may have obtained the patient names, birth dates, addresses, telephone and social security numbers.

BENCHMARK

EXPEFLOW
Expedite your workflow.

Security Breaches Affect Us All

JP Morgan Chase

JP Morgan Chase, United States' largest bank, acknowledged a massive data breach that affected 76 million households and 7 million small businesses. Hackers obtained personal information such as customer names, addresses, phone numbers and email addresses.

BENCHMARK

EXPEFLOW
Expedite your workflow.

Security Breaches Affect Us All

Sony

In early December, hackers leaked five unreleased movies online and some employees' Social Security numbers. The hack exposed over 47,000 Social Security numbers, including over 15,000 current or former employees other personal information, such as full names, dates of birth and home addresses, increasing the chances of identity fraud. Data continues to come out about this Sony breach which now includes private emails and other sensitive information.

Traditional Risks- Fax & Paper

Where are your fax machines located? In an easily accessible location? A hallway for convenience, a room without a door, at the front desk, or in an open office group? A fax machine sitting in the open not only makes it easy for employees to access but also for wandering eyes to notice as they pass by. Having confidential information easily seen in an area accessible to a public eye is a huge security exposure.

Traditional Risks- Fax & Paper

With Intent: HR regulations require employee and customer information and history be kept securely private. A guest walking back to an office for a meeting can easily glance at a just received fax or a delivery person comes in to deliver food for the office and conveniently picks up sensitive information.

Traditional Risks- Fax & Paper

Without Intent: Fax piggy backing. A one page fax can get mixed in with other longer faxed documents that have come in and picked up by another employee expecting a fax. Unintended theft. A person places a lengthy document to be faxed and leaves the room and another document is received and placed into the same pile. A long insurance claim is received and waiting to be picked up by an adjuster and a co-worker picking up one of their faxes accidentally knocks one of the pages with critical information onto the ground or puts the page in with their file.

Traditional Risks- Fax & Paper

One of the main issues with using a fax machine is that a fax can be sent at any time of day, without your receiving any notification of its arrival. That means anyone could pick up a fax and see potentially private information, whether it's janitorial staff or nosy coworkers. The only way to avoid this is to either use a private fax machine behind locked doors or use SSL-encrypted internet faxing.

Traditional Risks- Fax & Paper

The biggest risks are actually in the fax machine itself. One day, your company's fax machine will be tossed to the trash, recycled or even resold. Some devices, known as thermal transfer fax machines, typically used by small businesses, contain rolls of film or ink ribbon that record everything you've ever faxed. Other fax machines often retain document memories as well. In a report about this topic, CBS News noted, "Nearly every digital copier since 2002 contains a hard drive storing an image of every document copied, scanned or emailed by the machine.“

BENCHMARK

EXPEFLOW
Expedite your workflow.

Traditional Risks- Fax & Paper

There are warehouses across America that house countless used fax machines and typically, they are sent overseas. The threat of anyone having access to your personal information should be enough motivation to erase a hard drive or destroy used film. The security provided by online faxing services is designed to cater to those who want to be notified every time a fax is sent and received and boasts password protection and SSL encryption.

Traditional Risks- Email

Legal liability: In most cases the employer is held responsible for all the information transmitted on or from their systems. Consequently inappropriate emails sent on the company network can result in large penalties. In the last few years there have been several high profile lawsuits such as the case against a global oil company filed by four female employees. The employees alleged that sexually harassing emails sent through the company email system caused a threatening work environment.

Traditional Risks- Email

Regulatory compliancy: This now affects many companies across several industries. New and existing regulations such as PIPEDA and PHIPA are forcing companies to prove they are protecting their clients privacy and in some cases even store the email as a permanent record as proof of compliance.

Traditional Risks- Email

Lost productivity: Employees sending personal emails and sifting through spam mail can cause a major loss of productivity. In addition to spam and personal emails, other potential risks such as viruses can also lead to network downtime and lost productivity.

Traditional Risks- Email

Confidentiality breaches: Most confidentiality breaches occur from within the company. These breaches can be accidental, but quite frequently they are intentional. Several years ago, a well-known software company filed a lawsuit against one of their former employees who had used the company's email system to send out confidential information to a competitor.

Traditional Risks- Email

Damage to your company's reputation: A badly written email, or an email containing unprofessional remarks will cause the recipient to gain a bad impression of the company that the sender is representing. A UK law firm had to find this out the hard way when two of their employees originated the 'Claire Swire' email, a sexually explicit email that ended up being read by over 10 million people around the world.

Traditional Risks- Email

Most organizations see this threat as existing in the data centre and spend many millions of dollars on securing it. In fact, the threat is most likely to come from lost or stolen hardware, such as laptops containing offline email files. When you consider that the number of employees working remotely is growing; including those who only work away from the office periodically such as flex-time workers.

BENCHMARK

EXPEFLOW
Expedite your workflow.

Traditional Risks- Email

Pure Email security threats: Spam, Adware, Phishing, viruses, and routing. Because email connects through so many routers and mail servers on its way to the recipient, it is inherently vulnerable to both physical and virtual eavesdropping. Current industry standards do not place emphasis on security; information is transferred in plain text, and mail servers regularly conduct unprotected backups of email that passes through. In effect, every email leaves a digital paper trail in its wake that can be easily inspected months or years later.

BENCHMARK

EXPEFLOW
Expedite your workflow.

Lesser Known Risks- Right on Your Computer

- **File Shadow Copies**-The service copies ALL data on the volume, including not only your documents, or program files, but system restore files too. The default setting for the service activates it every time the computer is started and every day at midnight, if the PC is idle.
- **Temporary Files-** are files created to temporarily contain information while a new file is being made.
- **Data Remanence-** is the residual representation of digital data that remains even after attempts have been made to remove or erase the data

Impact on Insurance Claims

To settle a claim the insurer has to communicate with numerous different parties ranging from the various vendors and their sub-contractors to brokers and policy holders. Based on the security issues we just discussed, it is clear there are real challenges that arise when attempting to accommodate the multiple ways participants are invited into the communications circle.

BENCHMARK

EXPEFLOW
Expedite your workflow.

Security

Cybersecurity has been sold since the dawn of the PC era with images of brick walls, iron gates, and steel padlocks. However, things have evolved significantly even in the past 5 years.

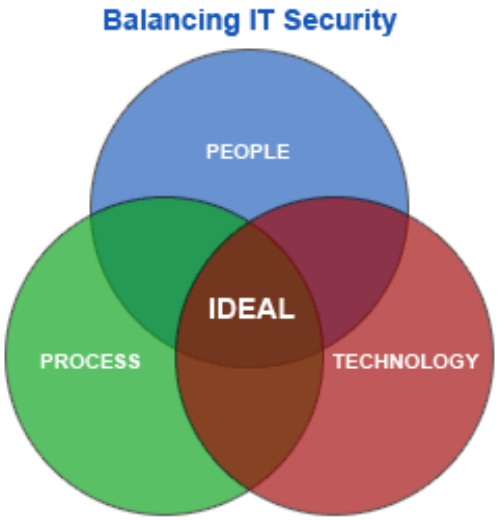
The cyberintelligence spyware first reported by the Russian security firm Kaspersky - with subsequent media stories tying in the NSA - hides deep inside target hardware, missed by antivirus programs and unperturbed by eradication efforts.

BENCHMARK

EXPEFLOW
Expedite your workflow.

Security

It's time to acknowledge the futility of focusing solely on defending impregnable data fortresses and equipping remote computers with antivirus and group policy rules. While this is still important, alone it is no longer enough. It's time for a new, practical security strategy emphasizing high environmental awareness, constant learning, and a new more standardized way of conducting business.



BENCHMARK

EXPEFLOW
Expedite your workflow.

New Shift in Security Focus

First, we need network security solutions that give complete visibility - so managers know every minute who's on the system, where they're located, and what they're accessing. Such software already exists and works well, but requires additional investment. There is little choice in a "bring your own device" world where work traffic is no longer confined to uniform, corporate-issued laptops. One of the best solutions is to utilize cloud based workflow solutions so that all users, regardless of their devices and motives, are operating on the same playing field.

New Shift in Security Focus

Second, most current processes in claims handling today don't talk enough and operate in the communication silos previously mentioned. Having a single system greatly reduces the silo-style constraints that limit knowledge of trends and patterns . As a result, we pay a high collective price because it ultimately will lead to some form of a breach as per the examples we started off with. Rather than trying to become more secure, add more rules, and more layers of security, we need a new model.

BENCHMARK

EXPEFLOW
Expedite your workflow.

New Shift in Security Focus

Third, we need a widespread culture shift. All users must take a measure of personal responsibility for data security. Our society has solved big issues from vehicle safety to containment of infectious diseases this way, and it's time for the insurance industry to promote a similar mindset in cyberspace. (You can equip a car with air bags and safety gadgets galore, but it's ultimately up to the driver to buckle up and drive safe.)

BENCHMARK

EXPEFLOW
Expedite your workflow.

Conclusion

Real-time awareness, lightning remediation, collaboration, and responsible habits: the pillars of new-school security. Security calls for intelligence, speed, and collaboration and this can be best achieved by shifting all workflows into a single best practices system that is centrally managed, supports any device, and, most importantly, guides users down the correct path and shares information in real-time when this is deviated from.