SIM2K
Adapting Technology to Your Business Needs

9•17
Information you can use

SIMformation

Do You Need CyberInsurance?

Imagine: Your company's security fails. You've been hacked. Credit cards, bank account numbers, addresses, and employee names are now in the hands of strangers, ready to be spread to the rest of the Internet or be sold to spambots. What Do You Do?

Unless you have planned ahead, you're panicking and gearing up for expensive damage control. But if you've properly prepared, your first step is to call your cyberinsurance provider.

Cyberinsurance is a growing segment of the insurance market, and it helps companies avoid huge losses incurred from database security breaches. With so much money and personal information exchanged through and stored on the Internet every day, cybercrime cannot be ignored. Small businesses especially are considered by many organized criminal groups to be easy targets with low risk and high payoffs.

Here are some statistics to ponder: The median cost of managing cybercrime for companies per year has gone from $3.8 million in 2010 to $5.9 million this year, according to a recent study by the Ponemon Institute. Those costs included money spent on security investigations, loss of productivity, software upgrades, and the value of stolen intellectual property.

AON, an insurance brokerage company, offers coverage to many global corporations as well. In 2008, only about 1.5 out of every 10 of AON's clients was interested in or in the process of buying cyberinsurance. This year, that number has jumped to 4.2 out of every 10.

But most of SIM2K clients are not major corporations. Most small businesses don't have the resources to recover from a data security breach alone, and that's where cyberinsurance kicks in. SIMformation sat down with Todd Carbrey of NSB Insurance in Carmel to discuss cyberinsurance for our typical client company.

Todd said that most insurance carriers should write a specific policy to cover your exposure. While some business owner policies have some form of cyber coverage, it is often limited to 3rd party coverage and does not take into account any losses to your own company (1st party coverage.)

Todd recommends that any company should sit down with their agent and their IT provider (like SIM2K) to help set out coverage. Depending on the policy, most cyberinsurance should cover the following key areas:

- Privacy and security liability relates to writing notices and paying clients for any losses that might have been incurred.
- Companies are required to notify their customers of a data security breach in most states, so costs for notification should be included.
- Cyber extortion (including Ransomware) coverage is now moving to the forefront. The policy should cover not only the cost of paying the ransom, but also costs for remediation of the company's IT network to restore it to functionality.
- Data loss and network system damage coverage kicks in when systems have been compromised or damaged. Replacing hardware and recovering files and data can be expensive. Insurance should cover this.
- After a security breach, a database may be out of commission for a few days, and service to consumers will also be affected. Coverage for business interruption, including "Denial of Service" attacks, is useful for when a company loses income because of an incident.
- A security breach can be a PR disaster. But by working closely with the company as well as its customers, an insurance provider can help to mitigate the damage.

If someone threatens a site or systems and demands goods to back off, it becomes the insurance provider's job to cover the settlement, and then hire a security specialist to track down the perpetrator. Cyber extortion has become a popular method by which hackers profit from small businesses.

Having cyberinsurance doesn't mean that you can put yourself at risk with no worries – most insurance companies will ask how your systems are already protected from viruses and hackers, and some might request a form of on-site audits, often from an IT company. Clients are expected to understand the risks of a security breach and to recognize scams such as those that stem from phishing e-mails.

NSB's Carbrey stresses that any policy be specifically tailored to meet that company's risk exposure. Some questions to ask yourself are:

- What data do I have that could be at risk?
- What coverage do I have in place?
- What exposure do I have, both internal and external?
- What resources do I have in place to ride out down time during remediation?

A company with extensive personal data files like medical records or social security numbers will have a higher risk exposure than a small service company. But you can also run the risk of buying more coverage than you need, so avoid "boilerplate" policies and work with your agent and IT company to develop a cyberinsurance policy specific to you. For more information, call SIM2K or NSB Insurance, 317.575.2900.

Are You Prepared?

What is your level of disaster preparedness? While Indiana might not be subject to 50" of rain like Hurricane Harvey dumped on Houston, could this picture be your office some day? We have flood plain areas in Indiana that are subject to flooding from heavy rains. Or, what happens if the sprinklers malfunction and the "rain" is just in your office suite and all your equipment is soaked?

Photo: Houston Chronicle

According to the Federal Emergency Management Agency (FEMA), more than 40% of businesses never reopen after a disaster, and for those that do, only 29% were still operating after two years. And guess what likely becomes of those that lost their information technology for nine days or more after a disaster? Bankruptcy within a year.

As it happens, September is National Preparedness Month, so the timing is perfect for company leaders to examine their awareness and plans to handle the full range of disasters, whether natural or man-made. Disaster preparedness equates to disaster recovery and business continuity. Companies should have plans ready in case of any sort of emergency situation, be it a flood, fire, tornado or any disruption of normal business activity.

SIM2K has several support programs to help provide the basics for a business continuity program. These include SIM2K® Backup Backstop(BUBS) and SIM2K® Remote Backup Service (RBS). BUBS helps ensure your essential data is 1) being backed up correctly; 2) can be restored from these backup files, and 3) copied to a second drive that is taken off-site for storage. RBS takes data nightly and remotely copies it to SIM2K where it can be restored if needed.

However, protecting data is just "job one" for disaster recovery. The configuration of your network, the settings for your servers and workstations and just the physical hardware in place must be taken into account. This is why SIM2K offers counseling to help your develop a true business continuity program specific to your business needs. This National Preparedness Month, let us help you be ready to face any potential pitfall that could seriously disrupt your business, let alone cause you to never re-open your doors.

Severe Equifax Data Breach

A huge security breach at credit reporting company Equifax has exposed sensitive information, such as Social Security numbers and addresses, of up to 143 million Americans. Unlike other data breaches, those affected by the breach may not even know they're customers of the company. Equifax is one of three nationwide credit-reporting agencies that track and rate the financial history of consumer, getting data from credit card companies, banks, retailers and lenders. You do not have to be a "customer" of Equifax for all your personal information to be on file with the company.

The hackers accessed personal information such as names, Social Security numbers, birth dates, addresses, credit card numbers and the numbers of some driver's licenses. The data breach is among the worst ever because of the amount of people affected and the sensitive type of information exposed. This information is exactly what hackers sell on the Dark Web that leads to identity theft, plus it provides a hacker with the types of information they need to break into other sites such as financial and banking.

The company says as many as 143 million people in the United States were hit. Credit card numbers for about 209,000 U.S. customers were compromised, in addition to "personal identifying information" on about 182,000 U.S. customers. Equifax said it will send notices in the mail to people whose credit card numbers or dispute records were breached.

Equifax said the breach happened between mid-May and July. It discovered the hack on July 29. It informed the public on September 7. Equifax said criminals "exploited a U.S. website application vulnerability to gain access to certain files."

Equifax is proposing that customers sign up for credit file monitoring and identity theft protection. It is giving free service for one year through its Trusted ID Premier program, whether or not you've been impacted by the hack. You can go to www.equifaxsecurity2017.com and click on the Check Potential Impact tab. You enter your last name and last six digits of your social security number and the site will tell you if you are one of the affected customers. If so, there is a "click here" button to enroll in the Trusted ID program.

Several law firms have launched investigations into potential securities law violations by Equifax, and a class action lawsuit has already been filed accusing the company of negligence in protecting personal data. "It is ideal, if ironic, for cybercriminals to compromise the very companies that internet users rely on to safeguard their identities and finances," said a security expert at Comodo. "Even if you are not a customer, Equifax likely has a lot of data about you, and you should take proactive steps in response to this hack." SIM2K urges everyone to be aware of their credit records and watch for suspicious activity that might indicate identity theft. Call us for more details.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Ransomware Won’t Go Away

In June, South Korean hosting company Internet Nayana, Inc., was hit by a ransomware attack that took down all 153 webservers hosting more than 5,000 customer websites. The company ended up paying the ransom because, as the company CEO said, “I would not negotiate with the hacker if was the case that it ended in the damage of my company alone. However, the scale of the damage was too great and too many people would suffer.” The company wound up paying nearly 400 Bitcoin to get its data back, which at the time was more than $1 million. That was just part of the total costs the company incurred. In addition to the time and money spent on the recovery, the company had to give discounts and refunds to affected customers. Not all data could be restored, and the company promised affected customers free hosting for life. And, shipping giant Maersk says that a ransomware attack hit them affecting users and applications in 500 locations. While no data was lost, the recovery and loss of revenue is estimated to cost Maersk between $200 and $300 million.

Altogether, more than a million computers have been infected by WannaCry, Petya and other variants, with costs exceeding $5 billion in 2017, up from $325 million in 2015. This is a problem that is not going away. The security industry has been working hard to improve defenses, but it’s hard as the Ransomware attackers are now launching attacks that require no software downloads at all. Instead, the attackers take advantage of the tools and software that already exist on the victim’s machine.

For example, users have been trained on not clicking on malicious attachments or visiting malicious sites, and anti-malware vendors have been getting better at spotting those sites and attachments. But worms spread themselves without the user needing to do anything at all – it looks and scans the network that has the vulnerability that it is looking to exploit, and copies itself onto the exploited machines. The attackers can steal data, for example, or do other damage. Then the ransomware will go off, and help the attackers cover their tracks.

Traditional signature-based anti-virus programs can’t keep up with new variants, new zero-days and infections that don’t depend on executable files. In addition to the traditional AV vendors, the new crop of security vendors on the market specifically focused on next-generation malware detection that is designed to either replace or supplement traditional signature-based antivirus, such as SIM2K security partner Cylance. Vendors at the Black Hat conference this summer reported zero ransomware infections using the new Artifical Intelligence/machine learning tools like CylancePROTECT®. Where there were infections, it was not that the ransomware was still getting through the protections, it’s that the machines weren’t protected in the first place.

At the end of the day, multiple layers of protection are needed as the bad guys will always be innovating, seeking to get around lax protocols. Law enforcement will also need to step up, putting cybercriminals behind bars. That requires time, however, and a lot of inter-agency cooperation since the attackers tend to be all over the world and key infrastructure is hosted in areas with the poorest enforcement. The flow of money also needs to be addressed such as regulating cryptocurrency. So to be safe, companies need steps beyond traditional anti-virus programs and training. Call SIM2K for more information on CylancePROTECT.

CYLANCE

“Random Tid-Bytes”

New SD Card for Smartphones Adds Features

SanDisk this week introduced the 400GB micro SD card, the world’s highest capacity microSD card which can now also support running applications on smartphones, tablets and laptops. According to SanDisk, the micro SDcard achieves UHS Speed Class 1 – the best performance available for a microSD card and one that enables the speedy loading and running of apps. This is the equivalent of putting a USB drive on your computer and running apps from it. The new Ultra microSD card can hold up to 40 hours of full HD video and features data transfer speeds of up to 100MBps. At 100MBps, SanDisk’s new microSD card can also move up to 1,200 photos per minute. SanDisk’s 400GB Ultra microSDXC UHS-I card features a 10-year limited warranty and will be available at SanDisk.com and other major retailers at an estimated retail price of $250.

3-D Printing Now a Fixture in the Enterprise

Additive manufacturing at Ford has evolved from being a niche technology a few engineers toyed with 20 years ago to its integration in the R&D process 10 years ago to the entrenched development process it is now. Ford is prototyping virtually everything using 3D printing from “road to roof.” A little more than a decade ago, Ford 3D-printed perhaps 4,000 prototype parts for its vehicles. Today, the automaker’s five 3D prototyping centers churns out more than 100,000 parts annually. In the future, additive manufacturing (3D printing) will likely be used to construct a least a portion of production parts on vehicles says Ford. This is not unique to Ford, as a 2016 PwC survey showed 71% of the top 100 US manufacturers were using 3D printing for both prototyping as well as production and custom parts. Over the next three to five years, 52% of manufacturers surveyed expect 3D printing to be used for high-volume production compared to two years ago, when only 38% thought the same. Sixty-seven percent of the companies surveyed believe 3D printing will be used for low-volume, specialized products within five years. Global spending on 3D printers hit $11 billion in 2015 and is expected to exceed $27 billion by 2019.

Hackers not on PC Networks Only!

While the man and woman allegedly responsible for an attempted armed robbery in Australia are no Bonnie and Clyde, they had something the infamous outlaw couple didn’t … a little help from a hacker, who was credited with hijacking the Victoria Police emergency services radio network, impersonating an officer as he broadcast, which ultimately led to the cops calling off the chase. Victoria Police officers were chasing an armed man who had allegedly attempted to rob a store; he and a woman ran to a stolen car and fled. Victoria Police raced after them. During the car chase, an unknown person posing as a cop came over the police radio multiple times. The unauthorized voice reportedly interrupted so often that the real cops abandoned the chase. The police are now hunting for the person behind the hack – but did find the thieving couple in a nearby town and arrested them.

Two Factor Authentication for Safety

About 63% of confirmed data breaches involved weak, default or stolen passwords. One way to overcome issues with passwords is to use Two Factor Authenticatin (2FA) like SIM2K offers with our partnership with Duo. You may not know it, but you probably already use two-factor authentication in the physical world. This explanation of what it is should help convince you why it's a good idea to use it with mission-critical online services, too.

Two-factor authentication adds a second level of authentication to an account log-in. When you have to enter only your username and one password, that's considered a single-factor authentication. 2FA requires the user to have two out of three types of credentials before being able to access an account. The three types are:

- Something you know, such as a personal identification number (PIN), password or a pattern
- Something you have, such as an ATM card, phone, or fob
- Something you are, such as a biometric like a fingerprint or voice print

While it adds an extra step to your log-in process, usually 2FA can be a minor inconvenience. It comes down to your patience and your willingness to spend the extra time to ensure a higher level of security.

As Fred Milch, Senior Network Analyst for SIM2K says, two-factor offers more protection than logging in without it. “When you make an attack harder, you're disabling a certain subset of the hacker community. Those looking for the ‘low hanging fruit’ of easily-hacked sites are quickly stymied by two-factor plans.”

Milch explains how Duo can work for SIM2K clients. “Duo Push is an app that installs on Android or iPhones that allows users to quickly reply to a request from Duo for authentication. You start to log into your account, and after entering your user name and password, you are directed to your smartphone and the Duo app where you can click on the Approve button to finalize your login and have access to the account. Of course, should you not be logging into your account and get one of these notices, you can see who is attempting to access it and click Deny to block them. This is the beauty of 2FA in practice.”

Milch continued, “Right now we are primarily adding Duo to those clients using connections to a Microsoft Terminal Server set-up through Remote Desktop Connection (RDP) protocols. Since RDP permits a user to connect directly into the network from any outside device, this is a way to add that extra layer of security to be sure that this outside login attempt is a valid company user. And with the Duo Push app, it is easy for the company user to validate their login by just pushing Approve on their phone. ”

Duo also offers additional ways to receive your 2FA passcode, so there are more options for SIM2K users. One involves having Duo call your cell phone, desk phone or other landline. If this method is selected, you are given a specific pattern of keystrokes to push to verify your identity and complete the challenge. When your phone rings, you merely complete that series of keystrokes to confirm your identity. This is just like entering your PIN to unlock your smartphone.

The other method is to have Duo send a text or e-mail back to the user with a unique passcode that must be entered into the login challenge screen to complete the authentication.

Many SIM2K clients fall under some sort of “protected” industry status – such as HIPAA for medical/patient information, or SarbOx for financial industry regulations. Often times, these federal regulations require more in-depth protection for personal information. Or, some clients are involved in on-line retail sales and must comply with PCI standards. Even law firms need protection due to the sensitive litigation data files they now keep. Milch points out that Duo is recognized as complying with advanced data protection under all these standards. “If any client is concerned at all about protected or personal information that may exist on their network, adding Duo 2FA makes sense for the safeguards it offers.”

Duo can also be applied to specific uses. It can be installed to protect applications or data stores on a network. Some examples are Outlook Web Access, a company web-based software platform or even into a company VPN. Here, the user can log onto the company network with just their regular user ID and password, but to then get into more protected areas, they will be faced with the Duo challenge. This is one way for a company to keep “wandering eyes” away from sensitive information that lives on the network. And, installing Duo on hardware sets up a “Trusted Device” policy, which can be important for those companies where employees can bring in their own devices to connect to the network. Duo ensures that only approved devices can connect, keeping visitors or vendors out of sensitive areas of your network data.

SIM2K will be glad to meet with you to discuss putting Duo 2FA to work for your company. In this age of hacker attacks and cyber extortion, the benefits from improved security is something everyone should consider. Call us for more information.

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com