Cybersecurity and Data Breach: Impact on Business in Illinois

By Laurie Silvey

There are two types of companies in the world right now: those that are going to be breached and those that have already been breached.

In recent times, over the past year or so, it is apparent that no industry is safe when it comes to cybersecurity. In retail, Target and Home Depot had exposure of over 70 million and 56 million records respectively. Software manufacturer Adobe Software and online marketplace eBay were hit for over 145 million records each. In banking and financial services, JP Morgan Chase was targeted for a loss of over 76 million records. And in healthcare, there were numerous breaches of patients' personal information and medical information.

It seems like every day, one hears about the next hack into another company's systems. Cyberattacks continue to become more and more prevalent, and more and more often, it is not just huge corporations that are being hit. Smaller companies are also being targeted, though you may not hear about them in the news. The costs associated with these incidents are also rising tremendously, not just financially, but also in legal exposure and reputation.

Cybersecurity is about protecting your computer-based equipment and information from access that is unauthorized and unintended, as well as possible change and even destruction.

Nearly everybody uses the internet to do business, some to advertise and sell, some looking for new markets; Others use it for communication with customers and suppliers, and a huge number of us use it for financial transactions.

What is directly at risk from a cyber attack? Rob Aleksick, chief executive officer of InTrust, a web-based security platform, said, "A CEO's job, the CIO's job, and more importantly, customer's data and the company's money."

Maureen Frangopoulos, associate at SmithAmundsen, and member of the Data Security and Breach Team, said, "It can run the gambit from personal information to credit card numbers, addresses, birthdays, names, medical information and on and on. Any company with an HR department is going to have substantial medical information on their employees. So basically every single company is at risk from a data attack – any company that is retaining information on anyone – all of that is at risk from a cyberattack."

Attacks are costly, ranging from financial losses from theft of information, financial and bank details or even money, as well as disruption from doing business - especially if the business is online only or dependent on online sales. Costs also include expenses for cleaning up the affected systems and getting them back up and running plus fines can be imposed if personal data is lost or compromised. Even more expensive can be the loss of business through damage to a company's reputation and customer bas, and it can spread further, causing damage to

"Every company should perform a risk assessment whether they have an attorney involved or not; looking at data that they retain, classify, categorize, determine who has access to it, making sure that people who don't need to have access to certain data to complete their jobs shouldn't have access to it."

- Colin Gainer, Partner, SmithAmundsen LLC

additional companies that are connected and/or do business with the affected company.

The bigger industries, those which store the voluminous amounts of data and information, are going to be the ones that make the newspaper. In those cases, there are thousands or millions of people's information that is involved. But, the smaller companies who don't have the right firewalls in place and are not encrypted, if they are dealing with information that holds credit cards or health information – those are attractive to a hacker.

Aleksick pointed out that the hack at Target started from an air conditioning vendor - a Russian criminal gang hacked into the poorly secured system of one of Target's HVAC vendors where they stole log-in credentials to access Target's corporate network and downloaded millions of credit cards. He commented, "In 2015, every company that does business is electronically connected. The air conditioning vendor had links to Target's electronic infrastructure to monitor the temperatures on their freezers in their food section. The hackers got inside the vendor's electronic infrastructure and then tunneled in through VPN to connect with Target."

So, what does a business need to know about keeping their systems safe and secure? The first steps should be a risk assessment of the business. Colin Gainer, partner at SmithAmundsen and another member of their Data Security and Breach Team, notes "Companies need to be pre-emptive. You can't 100 percent avoid a breach – that's the wrong path. The better approach to minimize risk is with preparation, training of your business employees and a risk assessment of your information and data that you receive, store and transmit."

Every company needs a chief privacy officer in today's world and every business should have a breach team in place before a breach occurs. The team should include IT people, PR people who are going to get the word out about the breach, your outside counsel, and your internal team. The company's chief privacy officer should be a part of the team; the C-suite should all be involved in trying to manage the risk in terms of data breaches. Small companies need to do the same risk assessment. A smaller company could be so overburdened by the cost of a breach that they could be forced out of business by the expense. The team may look different for a smaller company, but could include the business owner, HR director, and IT personnel, along with outside counsel. The team should get together regularly (preferably quarterly) to review risks a company is facing, talk about what IT is doing to prevent a breach, and how the company would be able to detect a breach. It is proven that having these things in place before a data breach can lower the overall cost for the beach. Having a chief privacy officer in place equates out to $6 per record less cost in a breach. This can be a significant amount of savings when there are millions of records involved.

"It can run the gambit from personal information to credit card numbers, addresses, birthdays, names, medical information and on and on. So basically every single company is at risk from a data attack – any company that is retaining information on anyone – all of that is at risk from a cyberattack."

- Maureen Frangopoulos, Associate, SmithAmundsen LLC

"I met our security expert on an airplane three years ago. He had been looking for an opportunity in the security space. We purchased assets of SecureAdvice - who had a similar concept but hadn't been successful with it. Databreach hadn't reached a level of awareness at that point.

- Rob Aleksick, Chief Executive Officer, InTrust

Every company should perform a risk assessment whether they have an attorney involved or not: looking at data that they retain, classify, categorize, determine who has access to it, making sure that people who don't need to have access to certain data to complete their jobs shouldn't have access to it. Data collection should be minimized. Information should only be collected if there is a reasonable business purpose for it. The breach response plan should include a set of policies and procedures to go through in case of a breach. The plan should include passwords for all computers and remote devices, plus virus protection and encryption when transmitting information in and out of the organization.

Passwords should also incorporate failed attempt log-ins, so that if a password is attempted and somebody tries it three or five or 10 times, it is logged out as suspicious activity. This is one of the most often skipped over steps, yet if not in place, a potential hacker can try over and over again until he/she has the correct code.

Cybersecurity
Continued

Another often-overlooked item is wifi. If a company allows visitors to log into the wifi network and doesn't have it password protected, that's a way in for a hacker. Or, if a temporary password continues to be used over and over again, that number could get out and that's an entry into the system as well.

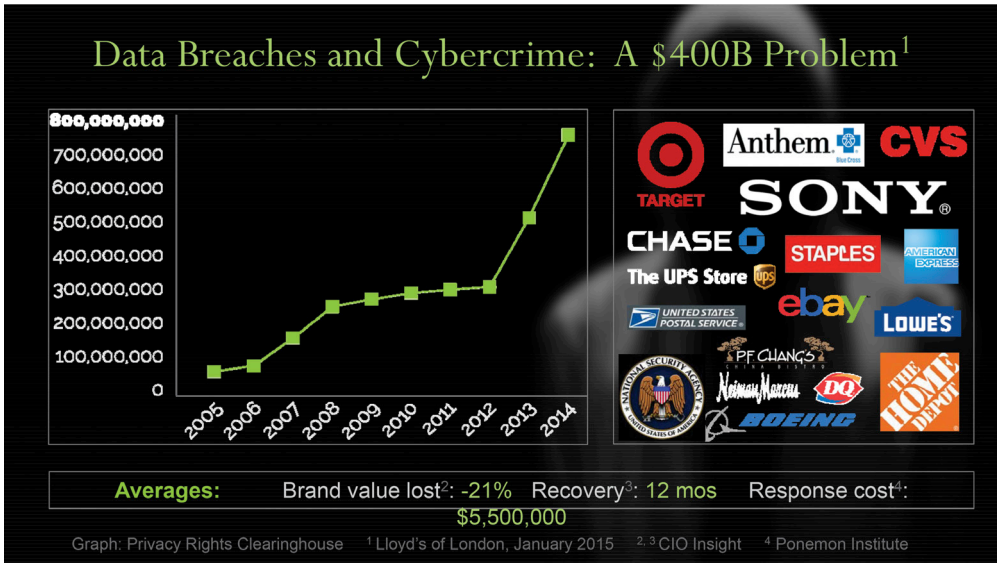
Colin also noted, "I think the one biggest pieces of advice in prevention I can give is if a company doesn't have the resources to test their own systems, hire a third party to test the systems and see the strengths and weaknesses. If that's too expensive for the company, then keep up with the newspapers and online sources to watch how hackers are getting into systems and see if that possibility is a weakness for your company."

Aleksick described their InTrust platform as a kind of a LinkedIn for security. "This is a way for buyers and sellers to come together and prove their bonafides to one another. Enterprises then know that their vendors are strong enough to survive an attempted hack."

A vendor will establish a profile, which shows that the company is compliant with regulations, noting that they do certain steps to make sure the company's systems are safe. Before a buyer works with that vendor, he can then look at the profile and compare to be certain they're doing business with the best security practices. Aleksick continued, "Most large organizations deal with thousands or tens of thousands of third parties continuously. Being certain that the vendors you deal with are as secure as possible improves overall security, reduces risk and prevents more breaches."

Despite the best efforts, after a hack occurs, a company most likely will not find out about it internally; Maureen commented, "A majority of breached companies are notified about it from an outside source that a breach has occurred. Anthem actually detected its breach internally, but that is extremely rare. It is huge to be able to have the right IT structures in place to be able to detect a breach."

The more information a company is retaining, the more likely it is that somebody is going to want to hack into its systems. Colin and Maureen noted, "law firms for example, have sensitive confidential client information. As for health companies, 2015 is being called the year of the health breach. Hackers know all of the private information that insurers and health companies have to hold on to. That information sells for more than a credit



ABOVE - This graphic shows the cost of data breaches and cyber crime. Over the past 10 years, the frequency has steadily climbed along with the cost. Average time for recovery is a full year, and average response cost is $5.5 million.

card number on the black market. We know that a medical record sells for $50 on the black market and a credit card number will sell for a dollar. A credit card can be cancelled in a very short time, so there is a very short window for that card to be able to sell it and make a profit off of it. The more sensitive information that a company retains, the more at risk they are."

Aleksick and his partners focused on three verticals - healthcare, banking/finance and critical infrastructure with their pilot program for InTrust. "We selected those verticals because they have the largest need for this service. They have more to lose - and it's more important that those buyers be secure."

Once a company has been breached, the work begins to repair the problem. Colin and Maureen both recommended that the first step be to get outside counsel involved as quickly as possible. "As outside counsel, we can establish attorney client privilege, then your statements regarding the incident can be reviewed by counsel and be protected as much as possible in the law."

At the same time, the breach team should meet to start to work on mitigating the damage. A forensic specialist should be called in to work with the IT department to determine what type of breach the company is dealing with and the extent of it and the neutralization of that breach. From there, the team will look at the type of information involved, and, more importantly, the type of laws involved. Whether it's health, credit card information, financial information, etc. – that will determine the types of responses under the government.

Preservation of the incidences is very important because in the breach world, often it's too late by the time the breach is discovered. The information that can preserved in the early stages can help to track down what's going on and get it stopped as soon as possible. Cybercrime is comparable to any other traditional crime. Law enforcement agencies will expect and appreciate the collection and preservation of evidence if they conduct an investigation.

Most importantly for prevention, policies and procedures need to be checked and run against day to day operations to make sure that what is written is being followed at work.

Training is important – in fact, the most important aspect of data breach prevention. A company is only as strong as the weakest link – one employee who isn't up to date with the types of preventions and measures that you have implemented at your workforce to prevent breaches can open the floodgates.

"InTrust Chief Technology Officer Anders Noremo was looking for a way to make it easier for companies to deal with compliance issues and handle the statutory requirements. "SecureAdvice had a similar concept, but hadn't been successful with it. " - **Anders Noremo, Chief Technology Officer, InTrust**

LEFT - Checking and rechecking your systems never ends. Whether you have an in-house IT support staff or a third party IT administrator, paying attention to the most up-to-date hardware and software is key.

Identity Theft and Cyber Crime Prevention

By Laurie Silvey

Identity theft is one of the fastest growing crimes in America. For financial institutions, medical facilities, retail stores and other businesses, it affects their companies on a regular basis as data breaches occur more and more often. Identity theft occurs when a thief obtains your personal information, such as your credit card information or social security number, and utilizes it to commit fraud or other crimes. It is estimated by the Federal Trade Commission that nine million Americans are hit by identity theft annually. Two-thirds of identity fraud victims in 2014 had previously received notification of a data breach earlier in the year.

When a company has been hacked, it can affect its customers very quickly as their personal information can be used to obtain a duplicate credit or debit card, or an account can be opened utilizing the stolen information. One of the biggest problems is the time needed to fix a person's credit after it has been compromised.

According to Habeeb Habeeb, CEO and president of Benefit Planning Consultants, identity theft is one of the major stressors in somebody's life. "When they have experienced an identity theft breach, they will do one of two things – because they have to react immediately. That means they're either reacting on company time or they're missing work to react. It takes an average of 21 hours best case scenario to fix the problem (Javelin Strategy & Research 2015 Identity Fraud Study), The productivity of the employee is reduced at work and their worry is increased."

That stress and time level needs led BPC to look for a professional solution to offer to clients. "One of our clients wanted to use it as a part of its financial wellness program. At first, they started wellness with health, but then they wanted to help their employees with financial stability, with stress, with spending too much during the holidays, etc. It's a known fact that identity theft is a big stressor."

BPC decided to partner with Lifelock. "We chose it because it is proactive and monitors everything about your personal items, your credit cards, your banks, your medical records if you tell them. It proactively tells you if anything happens. After you sign up for it, you go onto itswebsite and explain everything you want the company to know about you. They are watching for anything that happens under those numbers that you give them and they send you alerts whenever something happens."

"Identity theft is one of the major stressors in somebody's life. When they have an identity theft breach, they do one of two things because they have to react immediately. That means they're reacting on company time or they're missing work to react. It takes an average of 21 hours best case scenario." - **Habeeb Habeeb**

"Our risk as a bank is that if a cyberattack happens, data can be compromised. They could get into customers' information and it would be PNC's responsibility, not the customers. We have our firewall and our security systems are up to date. " **- Marzena Szlaga**

But, if something does happen, Patti Lyons, senior vice president, said, "the program is also reactive. The employee can contact staff if something is compromised and they make the calls for you, cancel the credit cards, and clean up the mess in the wave of the breach. When Sony had its major security breach in November, itnot only lost customer information, it also lost its employees' information. So, the company had to deal with the internal security breach, but also all of its own employees had to spend hours and hours resolving and protecting their own individual identity. So, Sony had not only the liability loss of pr resolution and fixing its IT network, but it essentially lost itsemployee network for a period of time while this was being resolved."

PNC Bank also recognizes the level of identity theft crimes in America. They offer seminars to their customers to show them how they can protect themselves against the problem. Marzena Szlaga, vice president and senior business development officer at PNC, says "It is definitely an important issue for PNC Bank – because of what we see on a daily basis and how it affects our customers. We want to be sure that we are doing everything we can to protect our customers from becoming a victim of identity theft."

When a cyberattack occurs and personal information is taken, it can affect customers in different ways. "Fraudulent emails can go out to clients to damage them in terms of retrieving a lot of information. Wire transfers can be sent out on their behalf. Requests can be sent to family and friends saying that they need money and asking for it to be sent to them."

When a customer shops online and his or her information gets hacked into, a debit or credit card can be compromised. Duplicate cards can be made on his or her behalf, which could put a customer at risk of running negative on checking accounts or fraudulent charges on a credit card. That takes time to investigate as well.

The PNC seminars focus on techniques to avoid becoming a victim in public. They mention knowing what's in your purse or wallet. Never carry multiple credit cards on your person, only carry one or two at a time. When using your debit card, protect your pin number and yourself. ATM skimming devices have been on the rise recently, and when you put in your card, it reads the card and a camera reads the pin number as you enter it in. Another suggestion is when you're finished with documents containing personal information, be sure to

shred them rather than just tossing themin the trash.

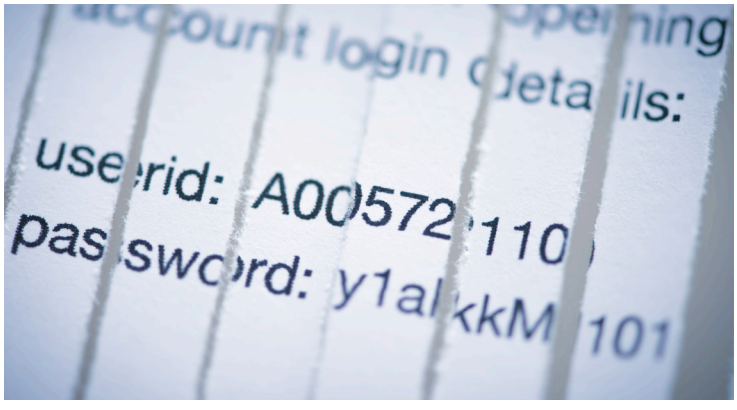
Though the corporate breaches are best known, there are also tax filing breaches. In that case, a hacker goes to file a tax return before the owner of the return can do so and gets your refund. Habeeb said, "It is an incredible worry for everybody. The government has been hacked, everybody will be hacked. The program is an inexpensive simple way to help when you get hacked or to know you've been hacked in the future."

Marzena added, "Some of our customers have had tax returns filed on their behalf and the refund directed to another address or account number. Some have had W2s stolen out of their mailbox, or duplicated somehow. This can take a long time to get fixed, and can delay a refund or cause other problems for the taxpayer."

The Illinois Attorney General's office is very much involved with protection of the consumer from identity theft issues. Habeeb pointed out that the attorney general's office recently released a report that identity theft is among Illinois' biggest concerns. "There were 2614 cases in 2014 and the office helped to remove more than 27 million dollars in charges to 37,000 Illinois consumer accounts." While identity theft has been one of the leading complaints to the Attorney General's office, Madigan credited last year's ranking to the plentiful major data breaches that were recounted in 2014, which many have named "The year of the Data Breach."

The attorney general's office, itself, is extremely concerned about the increasing number of data breaches and the resultant victims of identity theft. Attorney General Lisa Madigan's office has an identity theft unit and hotline. More than $27 million worth of fraudulent charges have been removed with help from the team of experts. They provide one on one assistance to the victims of identity theft and data breaches.

Recently, Madigan drafted legislation to reinforce and update Illinois' Personal Information Protection Act (PIPA). The act was originally passed in 2005, and required entities that suffer a data breach to notify Illinois residents if the stolen information included drivers' license numbers, social security numbers or financial information. The amended legislation will expand the type of information that requires a company to notify customers of a breach. It will include medical information outside of federal privacy laws, biometric data, geolocation information, sensitive consumer marketing data, contact information when combined with identifying information and log-in credentials for online accounts. The bill also requires entities that are holding sensitive information to take "reasonable" steps to protect the information and requires entities to notify the attorney general's Office when breaches occur. The threshold for notification of the AG's office has just been amended to include more than 250 Illinois residents as a result of a single breach of the security system, within 30 days of the breach. This does not affect the notification of the affected consumers, which is required within all reasonable efforts as soon as possible.



PROTECT YOUR BUSINESS FROM CYBER CRIME

By Wintrust Outreach

These days, cyber crime is a very real and dangerous threat, both personally and professionally. As technology increases, so does the opportunity for cyber crime, as more and more sensitive data is passed around. But, there are steps you can take to protect yourself and your business.

There's one main thing to remember about cyber crime: it's all about prevention. It's much easier to avoid something before it happens than to pick up the pieces after. With the proper tools, and a little skepticism and caution, you can keep your sensitive information safe.

Make sure your equipment is up-to-date

Obviously, because cyber crime involves your computer and technological infrastructure, it's important to have the most up-to-date patches, updates and security software. Cyber criminals target those most vulnerable, so while these things aren't guaranteed to prevent an attack, it does make it harder for a criminal. It may be just enough to deter an attacker.

For smaller companies, it's important not to cut corners on security. Make sure you invest in the best business-class antivirus software: it detects, removes and protects against malware (software that damages or disables computers). And, even though many companies protect against malware internally, also be aware that much of what puts your system in jeopardy comes from the Internet. Be cautious of websites and applications that could leave you susceptible.

Educate yourself and your staff

It's important to education yourself, and your staff, before there's an issue. Your employees should be informed about phishing and social engineering so they understand that it's NEVER okay to provide sensitive information via an unsolicited phone call or email. As companies become more proactive about protection, criminals become increasingly clever to compensate. Take the time to educate your employees: they are sometimes your first line of defense.

Stay informed so you're aware of issues right away

The impact of cyber crimes can be greatly reduced if you can catch it right away. You need to know as soon as possible if someone has stolen data, or has attempted to, so you can take proper action. The best way to do this is to stay on top of your accounts and sign up for any possible alerts that inform you of unusual activity right away. Your employees should also be trained to report anything at the first sign of something unusual.

Cyber crime can happen at any time, to anyone. But, with a few tools and proper planning, you and your business can stay safe from cyber threats. Just be sure to take the time, before something occurs, to strengthen your plan for cyber security.

Cybercrime Prevention
Continued

Recently, there has also been a White House push to focus on cybersecurity and protecting our cyberspace. In February 2015, President Obama signed an executive order that pushes for companies to share cybersecurity threats and other information with each other, as well as the government.

The order, which is advisory in nature, was signed during the first White House Summit on Cybersecurity and Consumer Protection. The summit focused on private-public partnerships and consumer protection. The Illinois Chamber's Vice President of Policy Benjamin Brockschmidt spoke at the summit in Chicago, explaining the need for the private and public sectors to work together to share strategies against data breaches and provide some markers on a path forward. He spoke about the need for national legislation to ensure that responses are timely and that businesses are not concerned about 50 different laws and regulations and that any legislation should not open businesses to additional liability.

Obama commented that the potential of cyber attacks currently is one of the country's most immediate national security, economic and safety issues. He spoke of the very real chance of a cyber attack knocking out power to a city or taking out the nation's air traffic control system. He also mentioned the possible effects on children who are online.

The executive order that the president signed pushes for the development of a central arena for the government and businesses to share data and areas where data can be shared across specific geographic regions. Obama wants collaboration between the private and public sectors.

In addition to his executive order, President Obama has proposed legislation that would protect companies from a lawsuit should they share threat data with the government.

Obama has signed other executive orders in the past, including one last year to protect consumers from identity theft and another one that looks for the creation of voluntary standards to reinforce the security of computer networks in critical industries and lays the groundwork for cybersecurity.

If a company does get attacked by a hacker, the first place it may think to go is its insurance company, thinking that coverage may be provided by its business liability insurance. However, this is usually not the case. A general liability policy often specifically excludes losses provoked by the internet. There is insurance avalable that specifically protects a company in case of a cyber attack.

Cyberliability insurance is a fairly new concept, so policies vary widely, both in coverage and cost. Premiums are based on industry and risk assessment. So, the more security steps a company has taken can lower the costs tremendously.

Cyberliability policies can cover things like business interruption, the cost of notifying customers of a breach, and sometimes even the cost of hiring a public relations firm to repair damage done to the company's reputation by the cyber attack.

It may be even more important for a small business to obtain cyberliability insurance. The insurance carrier can help out with analyzing the risks the company could face. Then, they can work with the company to be sure a firewall is in place to protect your network, or help to set policies for social media use that could mitigate the risk.

Another realization is that even if a business stores or hosts its website and data in the cloud it is still legally responsible for any breach.

There are several ways that businesses and individuals can protect themselves against hackers and cyber attacks. Hackers often exploit people's weak passwords to enter secured websites. Many people will utilize the simplest of passwords in order to to make it easier to remember them, but if they're easy to remember, they are also easy to hack. Hackers have been known to crack 8 character passwords in less than 38 seconds. A good frame of reference is that passwords should be no less than eight characters and should include a combination of numbers, letters and symbols and not utilize words related to the company or the person. Many good passwords utilize a phrase, such as "John was hired in 2007 as a welder. The password would

then be Jwhi2007aaw# (adding a symbol of choice at the end).

Even if a person is a trusted friend, they should not be allowed access to a password protected site unless the owner is there to enter the password. If that happens, the owner should change the password after the access.

It goes without saying that it's not a smart idea to use the same password for multiple sites. But, how does one remember those passwords and for which site? There are multiple file encryption tools that can be utilized, but another idea is to keep the list of passwords on another computer that is not connected to the internet or on a flashdrive or dvd not kept with the computer, but in a locked drawer.

Additionally, people should be careful about visiting internet sites that can put their computer at risk. Viewing adult content, going to hacker sites or opening pop-up windows that ask you to enter a user name or password can be risky. A reputable company will never ask for log-in information through an email.

By regularly updating every computer, hackers are not able to take advantage of software vulnerabilities that could be used to break into a system. Software patches and updates should be applied as soon as they become available. Recent versions of popular software can be configured to download and apply updates automatically, so that the computer is always up to date.

Several types of security software are available and essential for basic online security. Security software necessities include firewall and antivirus programs. A firewall analyzes all of the data attempting to stream in and out of a computer while the user is on the internet. It allows communications that it knows are safe and blocks items that could damage a computer.

Another realization is that even if a business stores or hosts its website and data in the cloud, they will still be held legally responsible for any breach.

Antivirus software is the next line of defense. This software watches all online activities and safeguards a computer from viruses, worms, and other types of malicious programs.

Anyone who shops online will inevitably need to enter name, home address, phone number and email address in order to complete a purchase and billing. Since not providing personal information is seldom possible, people should be aware of the following suggestions for sharing personal information safely online.

Fake email messages are often phishing attempts to try to get personal information. Indications that a message is phony include misspelled words, poor grammar, website addresses with unusual extensions, and odd phrasing in the body of the email.

Legitimate companies will not ever use an email to ask for personal information. If in doubt, one should contact the company by phone or type the company web address into the web browser. Clicking on a link in one of these messages may take the user to a fraudulent, malicious website.

Additionally, checking your credit card and bank statements monthly can help to catch an online crime quickly and lessen the impact. Banks and credit card companies also have fraud prevention systems to question unusual purchases. If a customer lives in Illinois, but buys an appliance in India for example, the bank may call the customer to question it.

Prevention will always be the best first line of defense against cyber attacks. Thinking like a cyber criminal creates better security awareness. Every business is responsible for its own security and the security of its computers and private information. Thinking like a cyber criminal can go a long way in preventing yourself from becoming a victim of cyber crime.