CYBER SECURITY

The Threat Is Real

The most unfortunate thing about cyber crime is that you cannot find out the perpetrator. They are hidden under anonymous network in world wide web.

Every time you do something on the internet, there is a trace which is called the digital footprint. Meaning, it can be traced back to the original user. . Say for example, if you looked at a post on Facebook for quite sometime, did not click it or hit the like button, Facebook has the technology to identify or pin point the user who stopped scrolling onto a story. That is how they target ads.

Social media sites or any website in general can trace a user back to a particular IP address. However, what if that IP address is fake? What if that person is fake? Due to the advent of technology, the complexities of network worldwide, it is easy to create fake credentials and conduct a cyber attack.

Why Cyber Criminals are on a Spree?

Cyber crimes are committed for various reasons. Extortion is not always the motive. There are other reasons too. Hackers will try to hack regular websites, or a regular office server just to learn how to do it. When they start hacking big enterprises generally the intent is to make money. There will be more than one person in this kind of attacks and mostly its done by something called RANSOMWARE. When a group of hackers demand money, they wouldn't ask you to come to a place and drop a back full of cash like seen in movies. They won't even ask you to transfer money to a specific bank account. They will ask the deposit by BITCOIN or any other CRYPTO currency. Transfer of money through Bitcoin, Dodgecoin can often be untraceable.

Cyber attacks and its kind

Malware: Malware short for Malicious Software, is a program that gets installed on your computer when you click an online link, or you accidentally download something from your email to your computer. Malwares can infect your computer by running a program on the background without you noticing it. This software program can start to infiltrate the server you are connected too. Meaning slowly it can grab hold of all the computers on a specific network. Malwares are dangerous because you might have clicked something and nothing happened and you moved on with your daily work. In the background the program just registered itself on your PC or laptop.

Malwares can start giving back data to the hackers who created it. It becomes spyware at that moment. Meaning it starts tracking every move or keystrokes a user is making on the computer. It can trace passwords for regularly used sites for monetary transactions. It is just preparing

for the next step which will lock everything up for you.
Ransomware: Now that the Malware has taken control over all your PC and network, it can lock it down any moment. It can say, "Please send us this much crypto" in order to get the key back. Big corporations will not kneel to such requests. They will hire computer network security personnel to deal with the locked network. But first they will convince the people that "there is a technical issue on our network, until further notice there will be no service from our online and any debit or credit payment will be suspended." They will bring highly paid cyber security specialist to deal with the situation. You might be thinking that they won't be able to crack the lock? Most often the cyber security specialist will be able to identify the program and stop it from working by command prompt (DOS mode, that black screen that only works with commands). Once the program is stopped from working it will unlock the systems and everything will be back to normal.

Then what did the hackers gain from this exercise? They might have already gained a lot that you can see with your naked eyes. They might have taken all your customers information, login details, transaction codes, debit credit card numbers, address information of your clients and start selling these information to something called the DARK WEB. Yes, there is an entire internet world out there hidden from public eyes. In olden times there were trade ships, their normal ports were visible to the public, but there were hidden ports all over the world for pirate ships too. Dark web is a place where these information can be sold to another set of hackers who can then start working or hatching another big attack either on the company's network, or individuals.

A big corporation like INDIGO (the bookstore) were able to retrieve their systems back without paying ransom to the hackers. But let's ask ourselves what if, an individual falls victim to a crime like this? How would they handle the situation? Who do they turn to? How can they retrieve what's taken from them? What are the costs associated with these?

On Feb. 8, 2023, the ransomware attack began and Indigo's website and payment systems were booted offline. The Toronto-based company's temporary website is still limited to selling "select books," as of Wednesday, and current and former employees are bracing for their personal information to be posted on the so-called dark web.
The bookstore chain said its network was hijacked via a ransomware software known as LockBit. The hack plunged the company into turmoil as its e-commerce operations and in-store debit and credit card payment systems were halted.

Read more about this story: https://globalnews.ca/news/9535738/indigo-ransomware-attack-one-month/

Latest cyber attack on Indigo had their employee data stolen. They offered credit monitoring for every employee for the next 2 years so any fraudulent activity to their account, will be notified immediately. However, is this enough? And we don't know to what extent the customer (the number can be thousands) information was stolen. And how it would impact these people?

The Remedy

It is clear that more attacks like this are coming our way. There is no simple solution to this problem. You can be cautious about what you use, how you use your computer and server systems. Doesn't matter how attentive or mindful you are, any other employee of your organization may not be following set standards or principals. We need to realize that its now a part of our daily life. Like we live with any other hazards say wintery weather conditions without noticing it much unless an accident occurs.

"Accident" is defined as unexpected event that can cause you financial losses or loss of live. Insurance is obviously a way to prevent such loss that can be unforeseen and off course non-speculative. There are wide ranges of products for cyber crime insurance these days. Not only they will help you regain control of your data loss but they will help you be back on your feet while there is a financial loss. A question will still remain, what happens in the long run for the data that was stolen from your servers, and how wide an attack can be plotted with that data?

Cyber Insurance

Cyber insurance will protect you from the after effects of a cyber incident. If you take the policy from a good provider, they will bare the cost of your incident response. They will dedicate a team of experts to deal with the situation and work with you as fast as they can to make sure you are up and running again. Any cost relating to inform your customers is also bared by the policy.

There is a difference between cyber liability insurance and cyber crime insurance. Cyber crime coverage can kick in if there is a crime committed by a cyber incident. For example if your employee commits a eTransfer to an fraudulent bank account unknowingly, then that falls under Cyber crime. Cyber crime sometimes is part of cyber liability insurance, or you can purchase it separately.

Business interruption can happen due to a cyber attack. During the Indigo cyber incident there was loss of daily sales both online and in store. This is business interruption. This coverage comes with cyber insurance.

Personally lets all be careful about our online identity. There are insurance companies providing cyber security insurance for individuals. This will become a must have coverage in near future. Its time to stop texting your banking info or your address via unencrypted method of communication like phone message or fb messenger or Instagram messages.