Emerging cyber security threats and trends, 2021 and beyond

Hello, I am Earl Johnson, CEO of International Consultants and Investigations from New York. I’m here to talk to you about some emerging threats that we see in 2020 as having a major effect on the world, as well as the opportunity to join those in the career of defending against these threats.

There is no denying that the world of cybercrime has changed the way businesses think about security. Not only do you need to consider physical security but also your digital security. Everything in your business is at risk if the business has an internet connection. Intellectual property, trade secrets, personal data, financial data are just a few of the things that hackers will try to steal from your business.

So let’s talk about cybercrime and the top cybercrime trends we have seen in 2020.

Cybercrime – as-a-service – Cybercrime has gone mainstream and like software, cloud, and infrastructure technologies, it is now being offered as-a-service. With the rise in computing power and the decrease in cost, cyber criminals have seized the chance to make money by offering their cybercrime skills to others who have the money to pay for their services with no technical experience required. Denial of service attacks can be launched for less than US$10 and email accounts on popular sites like Gmail, Yahoo, and Hotmail cost around $130.

State sponsored cyber-attacks – Hacking is no longer performed by the stereotypical teenage hacker in his basement trying to access your systems. State sponsored hacking is now performed by sophisticated organized groups are using every tool available to steal valuable intellectual property & critical data, damage or shut down core infrastructure.

Think of the Sony Pictures or Office of Personnel Management data breaches in the US for examples of how state sponsored hackers have stolen valuable or damaging information from companies. These hackers are targeting companies and information that can provide economic or political advantages.

Recently publicized cases in the US show that state-sponsored hackers from Iran accessed critical infrastructure systems at a dam in upper New York state. In late December, alleged Russian hackers took down the power grid in Western Ukraine. Hackers have turned the fantasies of Die Hard into reality by accessing the core infrastructure of nations with direct penetration attempts. The state sponsored hackers are trying to get control of everything from oil fields, power stations, water stations, and nuclear facilities.

Hackivism – One of the emerging cybercrime threats to the world is what is termed "hactivism" or politically motivated hacking to destroy reputation, steal data, or affect critical infrastructure. Hackers such as Anonymous use their skills to forward their own political agenda. This trend began to gain traction during the US elections where people from around the world enlisted hacking as a form of speech. Businesses must have protections in place that can address the threat of hacktivism. From defacing your website to bringing down your network with a denial of service, hacktivism must be defended.

Ransomware – Ransomware is becoming a household name. For those of you who aren't aware, ransomware is a computer infection that encrypts the data on your computer and asks for money for the decryption keys. While ransomware is becoming much more of a mainstream cybercrime today, believe it or not, ransomware for computers has existed since 1989 when the first version was mailed out to the participants of a World Health Organization conference on a 5 ¼ inch disks and the victims had to mail the ransom to a Post Office Box in Panama.

Ransomware is becoming more and more sophisticated by the day. The use of digital currencies like Bitcoin have replaced the old ways of collecting through mailing a check or using a prepaid credit card. Due to the anonymity of Bitcoin and digital currencies, it has also made tracking down the perpetrators of ransomware more difficult. While Bitcoin does have an indelible ledger of transactions where you can track the flow of the money, there are no names associated with the accounts in the ledger.

The newest versions are stealing your files before locking them. We have seen a large number of attacks that have stolen critical data out of the business, school or hospitals.

Ransomware saw a 165% increase in the amount of ransomware and 2020 is off to a stellar start with the UK reporting that Britons are seeing more than 2000 attacks per day. The makers of Emotet and Trickbot are rumored to have made over $325 million in ransom since the first version.

Denial of Service attacks – With political statements being the main motivator for Distributed Denial of Service (DDoS) attacks, countries like Turkey have seen incidents increase to over 30,000 occurrences each day. While the US has overtaken all other countries as the main target for attackers, cyber criminals have attacked news agencies, companies, and governments around the world in an effort to take their computer systems and websites offline.

The common misconception about DDoS attacks is that it only affects a business with a website but that is simply inaccurate. A DDoS attack aimed at a business can shut down the businesses internet access to the outside world by flooding the connection with too much incoming traffic to the point that nothing goes out. That means that all cloud services will be inaccessible, email will not be delivered,

Email phishing schemes – Phishing schemes used to target individuals trying to obtain access to bank accounts or credit cards but it has become a major source of information and money for cyber criminals and the new term "whaling" has been coined for the large attacks. In the US, we have seen emails appearing to come from the company CEO requesting wire transfers from the accounting departments to pay urgent invoices that has resulted in the money disappearing to fake vendors. Or to the Human Resources Department asking for information about employees that has led to leaks of social security numbers and other sensitive employee data. Mattel lost $3 million in a phishing scheme that appeared to be a legitimate invoice for goods that turned out to be fake. Luckily for Mattel, they were able to recover the funds with the assistance of the Chinese authorities but most companies are not as fortunate.

Known Vulnerabilities - Most firewalls require a reboot following patching so most companies schedule quarterly, bi-annual, or annual updates. This leaves enterprises open to attack.

The Panama Papers leak has been attributed publically to outdated, unpatched software running its customer portal and email servers.

With the list of known vulnerabilities growing each day and information about the vulnerabilities public knowledge, cyber criminals are targeting zero-day vulnerabilities which more than doubled from previous years in 2019. HP's 2019 Cyber Risk Report found that 44% of breaches in 2019 came from vulnerabilities that are two to four years old showing that enterprises are not taking updating the hardware and software on a regular basis seriously.

Internet of Things – The internet of things is exploding. Everything around us is becoming "intelligent" and connected. From the refrigerator that tells us when we need to buy more food, to the connected thermostats and light bulbs in our homes, everything is getting a chip inside. This means that hackers have new ways to get into our homes. There have been many reports of a hacker taking control of a baby monitor and was talking to the child through the internet. Home camera systems allow for hackers to watch our every move. They know when we are home, and when we are not.

One of the major areas of concern for IoT security is with medical devices. There have been numerous recent cases of vulnerabilities with connected medical devices that lacked security to keep hackers from making changes to medication dosages.

With the internet of things, we must begin to have a standard of security before allowing these technologies in our home. We are constantly researching new "IoT" items and looking for the vulnerabilities. We work with manufacturers to plug these security holes.

Mobile vulnerabilities – There are now malware and ransomware specifically designed for mobile devices that can lock your device or steal data from it. Hackers are using smart phone vulnerabilities to track people with GPS. We have found many cases where people were surveilled by criminals after having their phone infected. Hackers are also using ransomware to lock your smartphone and ask for money to unlock it. In some cases, this malware allows the criminals to steal valuable banking data from your device which can give them access to your bank account.

With many businesses having Bring Your Own Device (BYOD) policies, enterprises must be aware of the risks of mobile devices being active on business networks. With the lines between business and personal usage of mobile devices being blurred, there is an increase for the business that allows personal devices to be used for business purposes.

Careers in cyber security - There is a tremendous shortage of qualified candidates with cyber security skills. There is an estimated 1 million unfilled cyber security jobs across the globe. By 2025, it is expected that there will be over 1.5 million vacancies unfilled.

In the US, not a single one of the top 10 computer science universities require a cyber-security course in order to graduate. Higher education needs to begin to start cyber security education programs in order to give the workforce of the future the skills they need to succeed.

As the world becomes more connected and reliant on technology, the need for cyber security will only grow. Now is the time to start getting involved, start educating, and start securing the future.

Thank you.

Dr. Earl R. Johnson

johnson@icicompanies.com

www.icicompanies.com