2020 Quarterly Gemini IBD® Newsletter: What Will Happen In The Second Half Of 2020 For The Cybersecurity Landscape

Introduction

It is so hard to believe that 2019 is over, and that not only 2020 has started, but an entirely brand-new decade for that matter. When it comes to Cybersecurity, a lot did happen in 2019, but what 2020 holds could be even more interesting.

A lot of this has to do with the upcoming Presidential Elections. We say how the Russians possibly interfered back in 2016, and now it is predicted that other nation state threat actors will come into the foray, especially that of North Korea and Iran.

A big concern here is the use of Deepfake Technology. This is when the tools of Artificial Intelligence (AI) are used to mimic people and their voices and make them look like the real thing when they are not. But, other Cyberthreats loom on the horizon for 2020. It is expected that Phishing, probably the granddaddy of all Cyberthreats will continue to evolve and grow into much more advanced that we have never seen before.

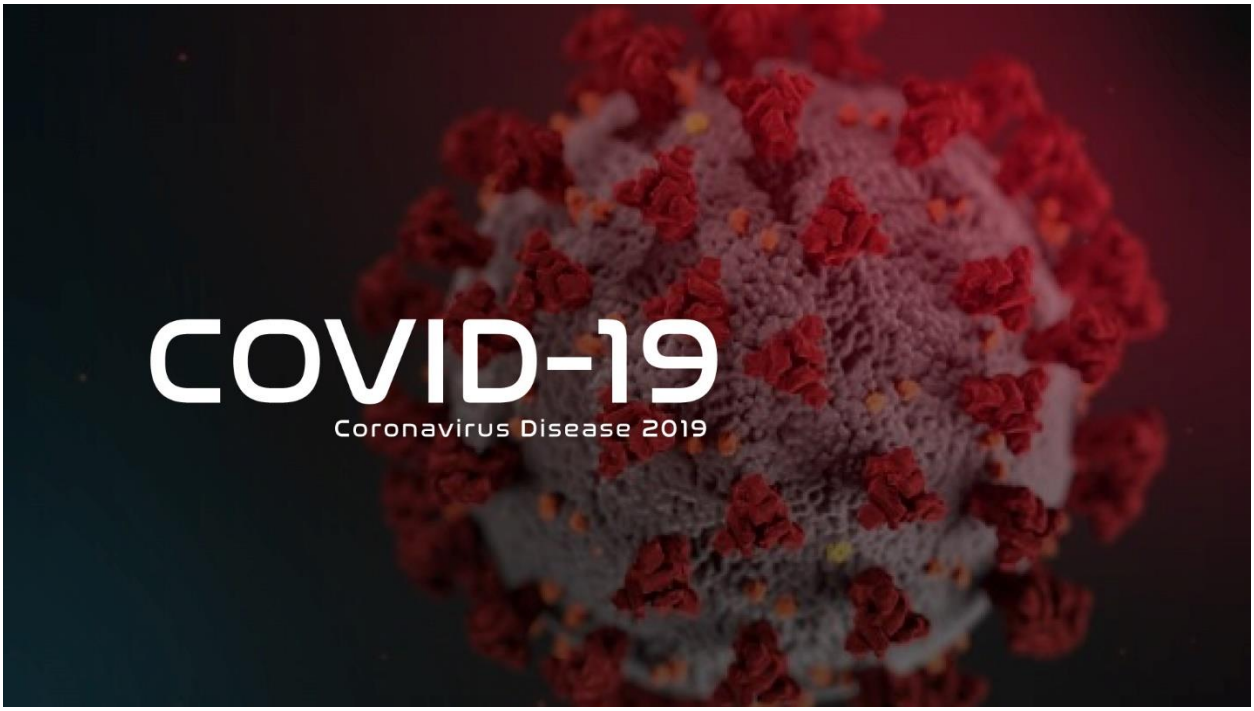
Again, AI will make a huge splash, both for the good and the bad. Ransomware will continue, but to what extent it will be used nobody knows for sure. But 2020 will bring usher in some new trends, such as:

- Major attacks on Critical Infrastructure, which includes our food supply, water supply lines, gas and oil lines, the national electrical grid, nuclear facilities, etc.;
- An explosion into the procurement and acquisition of Cybersecurity Insurance Policies by all types and kinds of businesses in Corporate America;
- The use of more traditional attack vectors such as Social Engineering the proliferation of Voice Phishing (aka “VPhishing”) scams;

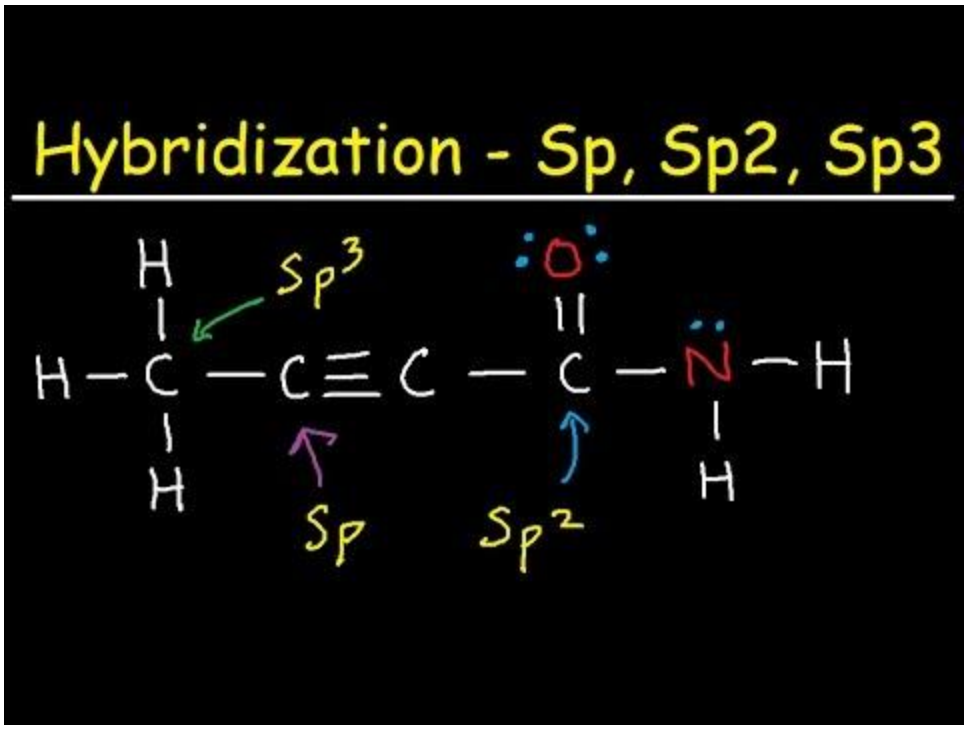
- The Cyberattacker now taking their own sweet time to launch their attacks and stay inside their victims for an extended period of time.

In this issue of the Gemini IBD®, we look into much more detail for what 2020 will hold in terms of the Cybersecurity Threat Landscape, and yes, the Coronavirus which has turned the world upside down.

What Wil Happen In 2020



So, what are some of the big trends in Cybersecurity that actually occurred in 2019? Keep in mind that many of these are still "left over" from even previous years but keep getting rolled into the new year. So, it is quite possible what we project for 2020 (which is covered in the next section) will have a greater than 90% chance of being rolled over into 2021, and even quite possibly for the rest of the decade.



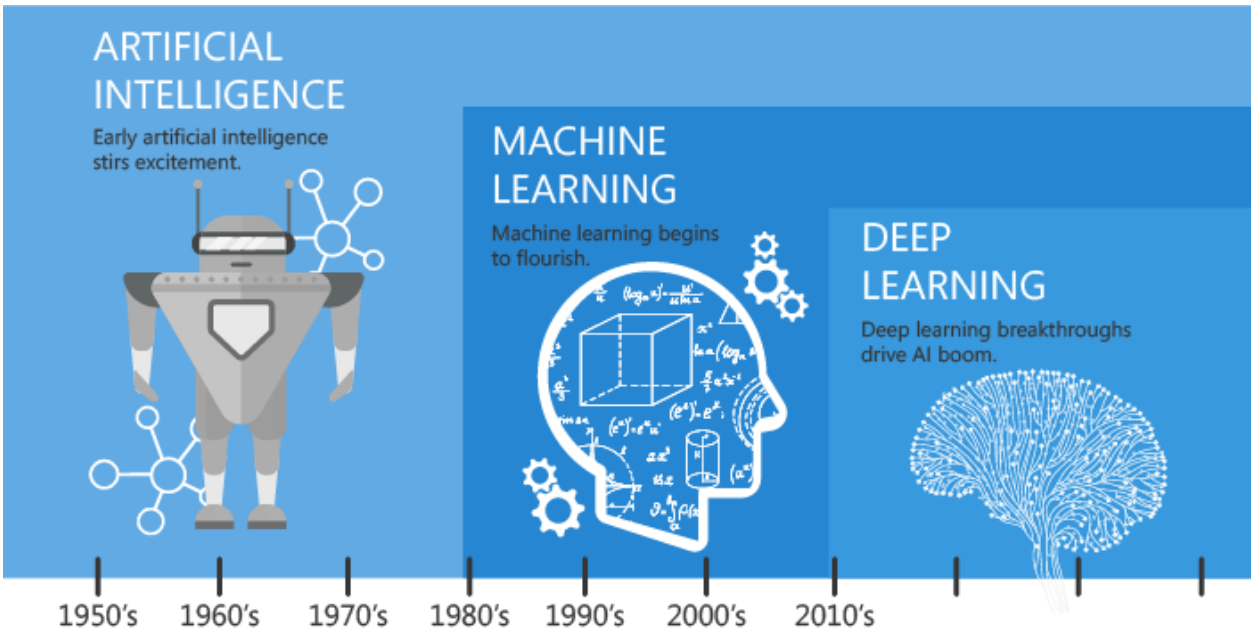
- <u>Businesses and corporations are now adopting a much Hybrid IT Infrastructure</u>:

  This simply means that rather than doing everything in house, or what is known as “On Premises”, or even “On Prem”, many businesses in Corporate America are now leveraging further use of the various Cloud based platforms, third party vendors, and even other types of microservices. Microservices can be specifically defined as follows:

  “Microservices is a method for developing software applications for enterprises that are more flexible and independently deployable with smaller modular services. Microservices architecture follows the DevOps implementation approach for service-oriented architectures (SOA) and communicates with each other over a network for building a continuously deployed system.”

  (SOURCE: 1).

  But given the fact that is not a unified, harmonious methodology with the Hybridization approach, many Security related threats have occurred, and this has required much more attention, and will even be a bigger trend in 2020. The biggest issue here leading to these Cyberthreats is that is that there is no centralized level of control or visibility for the IT Security to make use of.



- <u>The Use of Artificial Intelligence and Machine Learning</u>:

  These are also affectionately known as "AI" and "ML", respectively. Although many of is heard have heard of these terms, just what exactly are they? Here are some technical definitions for you to consume:

  AI can be defined as:

  "Artificial intelligence (AI) makes it possible for machines to learn from experience, adjust to new inputs and perform human-like tasks. Most AI examples that you hear about today – from chess-playing computers to self-driving cars – rely heavily on deep learning and natural language processing. Using these technologies, computers can be trained to accomplish specific tasks by processing large amounts of data and recognizing patterns in the data."

  (SOURCE: 2).

  In other words, with AI, the goal is to as much as possible match up the neuronic activity that is taking place inside the actual human brain in order to for computers to learn over time based upon the past information and data that they are being fed into it.

  ML can be defined as:

  "Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data and use it learn for themselves.

  The process of learning begins with observations or data, such as examples, direct experience, or instruction, in order to look for patterns in data and make better decisions in the future based

on the examples that we provide. The primary aim is to allow the computers learn automatically without human intervention or assistance and adjust actions accordingly."

(SOURCE: 3).

As you can see from the above two technical definitions, ML actually comes from AI. But the primary difference between the two is that with AL, it requires human intervention as information/data needs to be fed into it initially, and certain permutations have to programmed into the system in order for it to learn. But with ML, the amount of human intervention that is required is minimal, and the system can virtually learn on its own.

As it relates to Cybersecurity, it is expected that AI and ML will help fill the gap in the severe worker shortage. For example, many IT Security teams are simply too overwhelmed with going through the hundreds if not thousands of alerts and messages that they get every day, and because of that, many legitimate ones often get overlooked. In this regard, it is highly anticipated that AI will help filter through all of this noise, and present to the IT Security staff only those alerts and warnings which seem to have a high degree of credibility to them.

It is also highly expected that ML will be used to help project what the future Cybersecurity Threat Landscape will look like, and be able to use the concepts of Big Data and Data Warehousing in just a matter of a few minutes, versus the hours and days it can take a human being to accomplish.

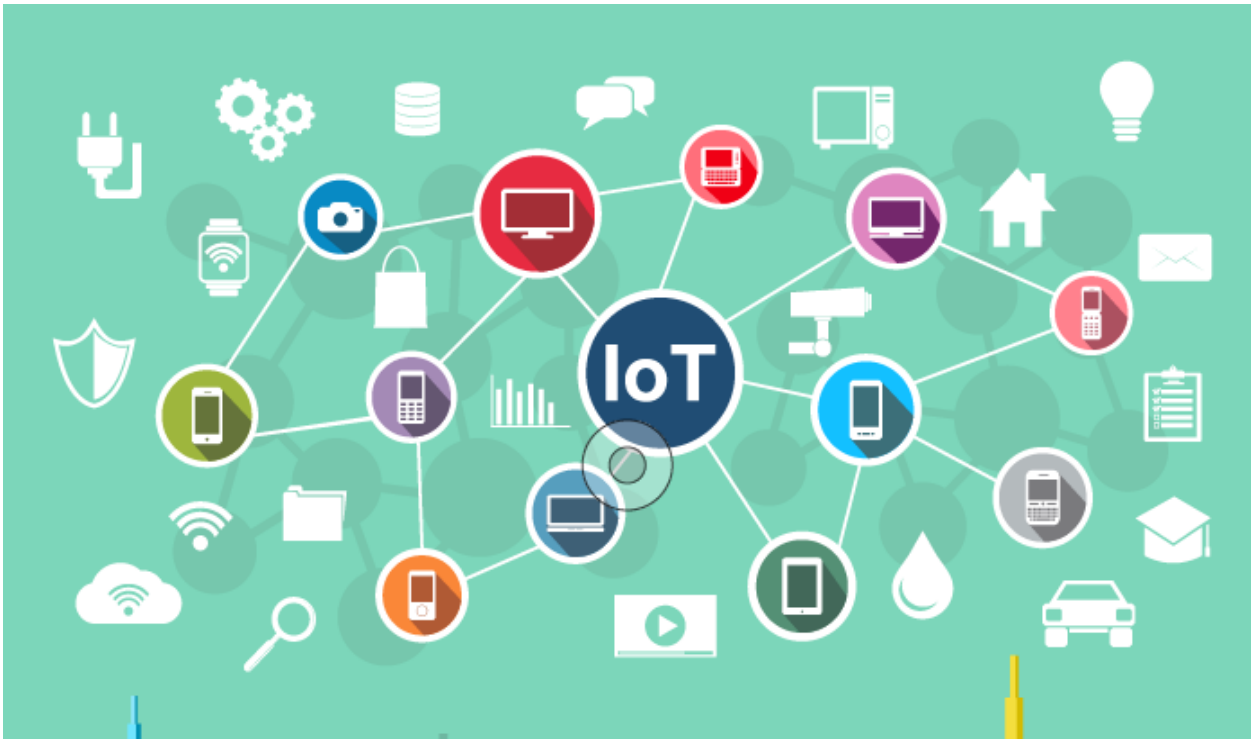
It is also expected that both ML and AI will be heavily used in terms of automating routine tasks, especially when it comes to Penetration Testing and Threat Hunting. But despite all of these advantages, there is a flip side as well: It is highly expected also that the Cyberattacker will use these tools for nefarious purposes as well.

It should be noted that a close cousin to both ML and AI is what is known as "Robotic Process Automation", aka "RPA" for short. It is technically defined as follows:

Robotic process automation (RPA) is the term used for software tools that partially or fully automate human activities that are manual, rule-based, and repetitive. They work by replicating the actions of an actual human interacting with one or more software applications to perform tasks such as data entry, process standard transactions, or respond to simple customer service queries."

(SOURCE: 4).

The use of RPAs is found extensively with the use of Chatbots. This is the Instant Messaging Agent that you see on many websites, and these make use of AI in order to provide you with answers that are tailored to your unique questions and concerns. It is highly expected that the usage of these will proliferate in 2020, as well as the Cyberthreats that are posed to them.



- <u>The explosion of the Internet of Things</u>:

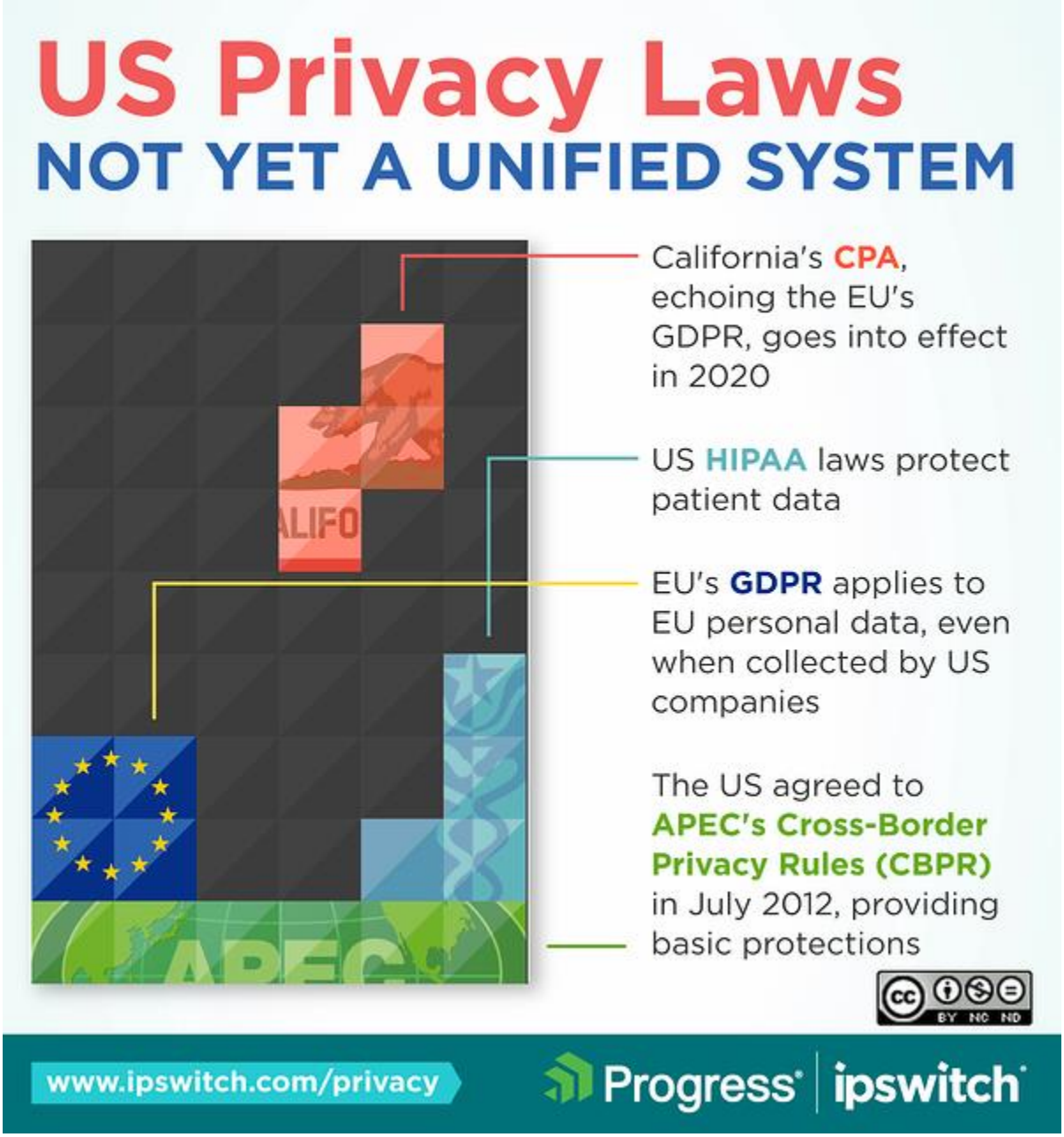
  For the most part, we all have heard this. This is where anything and everything that we interact with in our daily lives in both the virtual and physical worlds are connected to each other. But what is the Internet of Things, or IoT exactly?

  "The Internet of Things is the concept of connecting any device (so long as it has an on/off switch) to the Internet and to other connected devices. The IoT is a giant network of connected things and people – all of which collect and share data about the way they are used and about the environment around them. That includes an extraordinary number of objects of all shapes and sizes – from smart microwaves, which automatically cook your food for the right length of time, to self-driving cars, whose complex sensors detect objects in their path, to wearable fitness devices that measure your heart rate and the number of steps you've taken that day, then use that information to suggest exercise plans tailored to you."

  (SOURCE: 5)

  A very basic example of the IoT is that of Siri and Cortana. These are the Virtual Personal Assistants (VPAs) that have been designed for the iOS and Android platforms, respectively. You can ask them just about any kind or type of questions, and more than likely they will find an answer for you. This could be anything from finding the quickest route from Point A to Point B or which is a good restaurant to eat at. Now amplify this on a scale of 100X, and now you have what is known as a "Smart Home" or even a "Smart City". This is where with the clap of your

hands, your dinner will start cooking, and cars can pretty much drive themselves. While all of this may sound great, it does come with a grave risk. As of today, most of the IoT products that have been mass produced do not have any sort of security features installed into them. But worst yet, with all of this interconnectivity going on with all of these objects, the attack surface for the Cyberattacker has just greatly increased by 100X, because the network connections that are used are not themselves encrypted. So, if the Cyberattacker can penetrate into one connection, more than likely, he or she will be able to gain covert access to all of the others as well, deploying all sorts of nefarious malware. But despite this, the popularity and demand of the IoT is expected to grow strong into 2020 and well into this decade.



- Data Privacy Laws going amuck:

  Remember that hitting upon the digital assets of a business is just one goal of a Cyberattacker. There ultimate goal is to go after your Personal Identifiable Information, or PII for short. This includes anything and everything that is confidential and private to you, ranging from your credit card information to your checking/savings account number to even your Social Security number. Because of this, there has been an explosion of data privacy laws, designed to give you more control over the kinds of information and data that other people and businesses have about you. But what exactly is a Data Privacy Law? It is:

  "Information privacy law or data protection laws prohibit the disclosure or misuse of information about private individuals."

  (SOURCE: 6).

  There are different types of laws, some of the more famous ones are that of the GDPR (General Data Protection Regulation), HIPAA (Health Information Privacy and Portability Act), the GLBA (Gramm-leach-Bliley Act), and the CCPA (California Consumer Privacy Act). HIPAA and the GLBA have been around for quite some time, but it is the GDPR and the CCPA that are the most recent pieces of legislation to have been passed. And also, they carry amongst the harshest of the financial penalties if a business is found to be non-compliant with these regulations. Expect to see more laws like these to be passed in the United States. There are several pieces of new bills that are still pending in the United States House of Representatives, but there is no guarantee that they will be passed in 2020, rather there are higher probabilities that they will be passed earlier this decade. As of now, the CCPA is deemed to be the strictest Cybersecurity Law in the United States, and it is also widely expected that there will be more pieces of legislations introduced when it comes to data privacy and data security regarding the IoT. What is the difference between the two?

  "Data Security protects data from compromise by external attackers and malicious insiders.

  Data Privacy governs how data is collected, shared and used."

  (SOURCE: 7).

  For more insight into the GDPR, listen to this podcast:

  https://www.blogtalkradio.com/apollobiometrics/2020/01/03/learn-more-about-the-impacts-of-the-gdpr

- More spending in Cybersecurity:

Watch for more spending to happen in 2020. In fact, watch for this to happen just about every year in this new decade. The primary catalyst for these increases is that the Cybersecurity Threat Landscape is very dynamic, it keeps changing on a daily basis, and in fact, even by the minute. Hardly it seems like that one threat vector is launched, another new variant is launched. With each new security breach occurring more, damage is done, and therefore more crucial $$$ have to be spent in repairing these damages. But there will be a new trend that will be occurring in 2020 that what has happened in previous years. Rather than spending critical money on every new fancy security technology that is available, CIOs and CISOs alike are going to be held much more accountable than ever before by their respective Board of Directors. So, while the CIO/CISO will be given a budget, they will be expected to spend those $$$ extremely wisely. In other words, the CIO/CISO will be first expected to conduct a Risk Assessment and Security Audit of the IT/Network Infrastructures to see how the security technologies can be strategically placed so that they can be used to their maximum workload. So, rather than simply deploying ten firewalls, the CIO/CISO will probably just implement three of them in the most strategic areas of the business for in order to beef up the lines of defenses to the maximum possible. This is a radical shift in thinking that just started in late 2019 and will continue to grow into 2020. Want more information on how to properly plan your 2020 budget? Check out some of these blogs:

http://biometricnews.blog/how-to-compute-your-cybersecurity-budget-2-top-methodologies/

https://www.kamind.com/2020/01/14/how-to-plan-your-it-budget-for-2020/

- Attacks onto Critical Infrastructure:

  We all remember the horrific incidents of what happened on 9/11. We saw airplanes pummel into the World Trade Center, and the Pentagon, and yet another crash where in Pennsylvania where innocent live were taken while trying to protect others. Will this happen again? Fortunately, it has not, but there are good chances that it could happen in 2020, or earlier in the decade, whatever comes first. But rather than using bombs and airplanes, it will be a Cyberattacker that will bring down the Critical Infrastructure of the United States, in a style much worse than of 9/11. But first, what exactly is Critical Infrastructure. It can be specifically defined as:

  "Critical Infrastructure Protection (CIP) is the need to protect a region's vital infrastructures such as food and agriculture or transportation. Every government in every nation has a responsibility to protect these essential critical infrastructures against natural disasters, terrorist activities and now cyber threats. From energy organizations to transportation companies, it is paramount that security in all critical infrastructure sectors is of the highest standard and that disaster preparedness, response and recovery are top priorities. Common components of critical infrastructure needing security considerations include Industrial Control Systems (ICS), Operation Technology (OT), and SCADA Systems."

  (SOURCE: 8).

So, as you can see, it includes everything that makes our lives as American citizens run as smoothly as possible when it comes to essential services. This includes everything from the water supply lines to the oil supply lines, nuclear facilities, the food production/distribution systems, the national power grid, etc. From the definition it is the ICS, OT, and the SCADA systems that make all of these pieces of Critical Infrastructure work in a harmonious fashion. But it is important to keep in mind that these are legacy based systems, built and deployed in the late 1960s and early 1970s. At that time, physical access was the primary security concern; the thought of Cyberthreats was not even conceived of back then. As a result, it is difficult to secure these Critical Infrastructure items with from a Cyberattack, without ripping apart, gutting out, and rebuilding all of these systems from scratch again. The only solution to this is to is to simply add on layers of Cybersecurity mechanisms, but it is crucial that it is interoperable with the legacy-based security systems. Because of these huge gaps and weaknesses, the Cyberattacker can very quickly and easily shut down mission critical operations of multiple cities all at once. But we will not be able to restore operations back to normal again within days, it could take weeks and even months. Can you imagine having to go without food and water like that? Well, this is the stark reality that we face here in the United States in 2020 and in this new decade.

- <u>The explosion of Cybersecurity Insurance Policies</u>:

Let's face it, here in the United States, we need insurance for just about anything we engage in today. Whether it is business insurance, medical insurance, car insurance, etc., you name it, it is all there. But now, given the dynamics of the Cybersecurity Threat Landscape, there is a new type of insurance that is coming out: Cybersecurity Insurance. But what exactly is it? It can be defined as follows:

"Cybersecurity insurance is a product that is offered to individuals and businesses in order to protect them from the effects and consequences of online attacks. This product is a recognition

of the inherent dangers of storing customer information online and the risks businesses face in this online age.

Cybersecurity insurance can be obtained as a first-party product that focuses on compensating or mitigating the costs that are borne by the holder of the policy. It can also be sold as a third-party insurance product that covers the businesses and people that are found to be "responsible" for a breach. Sometimes you will be encouraged to add "Errors and Omissions" coverage to your policy as well for added protection."

(SOURCE: 9).

Let's illustrate with an example. Suppose your business has been hit by a Cyberattack, and you have of course, have suffered a good deal of financial damage. If you have an insurance policy, you can file a claim, and expect to get a quick payout right, like with car insurance? Think twice. Cybersecurity Insurance is still a very murky area, and in fact, it is even more messed up that the healthcare industry. You may get a payout for any direct costs that you may have suffered. For example, this can include such financial losses as downtime, restoring mission critical operations back up to normal, etc. But what about the indirect costs, such as reputational and brand damage, lawsuits filed by customers, credit reporting costs, damage caused to third party suppliers, damages inflicted to shareholders (this will be more likely if the Earnings Per Share [EPS] value drops if you company is a publicly traded one), etc.? Will all of these covered by the Cybersecurity Insurance Policy? What about physical damage done to your business as a result of a Cyberattack? Will this be covered? To this date, these are difficult questions to answer. Nobody has the answers yet to these, and no one can say for sure if you will get a payout to cover these indirect costs. This is going to be a hotly debated topic in 2020, with maybe some of these questions being answered. In Cybersecurity Insurance is such a new concept, that there are no set of uniform standards or best practices yet that have been adopted by the major insurance carriers here in the United States. But there is one thing that is for certain: In order to get the best Cyberinsurance Policy available, and to increase the probability of getting a 100% payout under any type or kind of circumstance, you will have to prove that you maintain a proactive Cybersecurity stance by making sure that you have all of the right levels of controls and Security Policies in place, and are being practiced on a daily basis. It is important to note that under "Security Policy", many insurance carriers lump Incident Response, Disaster Recovery, and Business Continuity Plans into this category as well. You will also be on the hook to make sure that you are assessing your levels of Cyberrisk as well on a regular basis.

- Cybersecurity and the Presidential Elections:

  Ok, 2020 is the year of the next Presidential Election. There will be the usual mudslinging, attacks, rumors, blah, blah, blah. But this one will be different from the others, in that Cybersecurity will be of the gravest concern than ever before. We got a taste of this back in the 2016 Presidential Election when the Russians were accused of meddling, and two years were spent by Richard Mueller and his team investigating into this. Concerns will run all over the place, such as voter fraud, online security, etc. But there is yet another horrible, new Cyberthreat that will emerge at the top in 2020, and that is the development and use of Deepfakes. What exactly is it?

  "Deepfake is an AI-based technology used to produce or alter video content so that it presents something that didn't, in fact, occur. Deepfake video is created by using two competing AI systems -- one is called the generator and the other is called the discriminator. Basically, the generator creates a fake video clip and then asks the discriminator to determine whether the clip is real or fake. Each time the discriminator accurately identifies a video clip as being fake, it gives the generator a clue about what not to do when creating the next clip."

  (SOURCE: 10).

  In other words, you see a video of Donald Trump or his Democratic Party contender in a commercial asking for political donations on your iPhone or Android device. But is this for real? Is this the real Trump (no pun intended on his Twitter handle), or a fake one? This is what "Deepfakes" is all about. It takes a branch of Artificial Intelligence (AI), known as "Neural Networks", and uses the algorithms from that in order to create fake videos or pictures that look

almost like the real thing. While this may have some entertainment value to it, the real fear here is that a Cyberattacker can use this technology and bait in unsuspecting users into a massive Phishing scheme. For example, they could be asked to donate large sums of money; but rather than those funds going into the respective Republican or Democratic party coffers, the money is really being sent to some offshore bank account located in China. This is a very scary proposition, and the state governments are fully aware of this. In fact, many of them have started to introduce and pass separate pieces of legislation before the 2020 Presidential Elections in order to mitigate the risks posed by Deepfakes as much as possible.

Conclusions

Ok, so there you have it, some of the predicted Cybersecurity trends for 2020. There are many others of course, but the above ones seem to the common thread with most of the Cybersecurity pundits. But the ones that were prevalent in 2019 will also steamroll into 2020, and they are follows:

- Phishing:

  This is the oldie but the goodie. According to the Verizon's 2019 Data Breach Investigations Report, 32% of data breaches and 78% of Cyber Espionage incidents all came down to some sort of Phishing scheme being deployed. However, its not all about the Emails anymore. SMS Phishing (aka "Smishing") and Voice Phishing (aka "Vishing") will be on a huge rise here in 2020.

- Rogue mobile apps:

  According to the RSA's 2019 Current State of Cybercrime report, the use of malware based mobile apps has increased by over 680% since 2015. This is highly expected to continue into 2020, as just about everything will have a mobile app associated with it. Google Store is notorious for this, but Apple's iTunes is far safer, as they make the software developer follow a rigid set of rules before being allowed to upload any mobile app onto their platform.

- Ransomware:

  According to a recent report from Malwarebytes, there was a 500% Year Over Year (YOY) increase from 2018 to 2019. Will this multiply in 2020? You can bet for sure that it will.

Contact Us

Do you have questions on these trends, or need help/assistance in addressing them for your business? Here is how to get a hold of us:

Email: ravi.das@astcybersecurity.com

Phone: 630-802-8605

Thanks for taking the time to read this!!!

Sources

1) https://www.happiestminds.com/Insights/microservices/
2) https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html
3) https://expertsystem.com/machine-learning-definition/
4) https://www.aiim.org/What-is-Robotic-Process-Automation#
5) https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/
6) https://en.wikipedia.org/wiki/Information_privacy_law
7) https://www.varonis.com/blog/data-privacy/
8) https://www.forcepoint.com/cyber-edu/critical-infrastructure-protection-cip
9) https://cyberinsureone.com/faq/what-is-cyber-security-insurance/
10) https://whatis.techtarget.com/definition/deepfake
11) https://www.securitymagazine.com/articles/90105-cyber-security-trends-to-watch-for-in-2019

12) https://enterprise.verizon.com/resources/reports/dbir/
13) https://www.rsa.com/en-us/offers/2019-current-state-of-cybercrime-white-paper
14) https://www.thesslstore.com/blog/the-top-cyber-security-trends-in-2019-and-what-to-expect-in-2020/