Introduction

This is the rule of the data revolution: for every action to store, secure, and use data, there is an equal or greater reaction to steal data. It has been proven repeatedly — as recently as the Equifax data breach. Data has changed from forms and documents to bioinformatics and digital transaction histories. Protection has moved from file cabinets and lockboxes to virtual storage spaces on secluded servers with stringent encryption. Malicious parties have likewise transitioned from physical break-ins to ransomware, DDoS attacks, botnets and other nefarious acts.

Companies are acutely aware of cybersecurity's importance, especially those operating via cloud and edge computing models or utilizing IIoT technology. The subject has introduced anxiety for business leadership and consumers alike, with few having full confidence about safe engagement in a digital, data-driven age. This white paper will address those concerns, outlining the stages of security, and introduce exciting technology that could ameliorate tension and stymy hackers.

History of Cybersecurity and Cybercrime

Cybercrimes follow centuries of heists a la Pink Panther and Butch Cassidy. The drama of robberies once surrounded thefts like that of the Boston Museum, where 13 works of art valued over $500 million were stolen. Now, digital objects such as credit card data and film footage have garnered the attention of a new class of thieves. A group of Russian hackers has filched over $800 million from bank accounts electronically in the past two years. One Russian hacker may even be credited with stealing 2016 US election information, invaluable to democracy.

Sanctions against cybercrime were not legislated in the United States until the Computer Fraud and Abuse Act of 1986. Despite recent origin, cyber attackers have a mainstream presence, from the advocacy-based vigilantes of Anonymous to shadowy lone wolves or government suspects featured in the news. They are known for a variety of acts: infecting networks, stealing personal data, attacking foreign government operations and holding sensitive company information hostage.

Computer crimes began at the birth of the internet in 1983. 1988 held the momentous Morris Worm, the first denial-of-service (DoS) attack: a few dozen lines of code that replicated rapidly and crashed 10% of all computers linked to the internet. The mid-90s introduced flash and browser-add on vulnerabilities where hackers took remote control of computers. Taking advantage of flawed software grew as a method of attack, including manipulating Microsoft software, through the early 2000s.

In the past few years, insecure, multi-accessed software has remained a vulnerability. Phishing has increased substantially as people spend more of their time online. Mobilization has created a massive market for spyware and monitoring. Mobile devices have expanded public networks and wireless connections, where hackers lurk. Since 2014, automotive and other machine software has also fallen victim. IoT, a market that continues to grow exponentially, has faced many security concerns as it sits at the center of software, cloud, network and physical access concerns.

It is estimated that 50 billion IoT devices will be connected in 2020. That number becomes especially alarming as 70% of IoT devices provide easy access to hackers.

Types of Cyber-Attacks

Although the forms of illegal computer activity are growing and changing like any type of crime, there are several established categories. Cybersecurity teams should have dedicated methods of management as it relates to each vulnerability.

What are viruses?

Mobile devices have expanded public networks and wireless connections, where hackers lurk.

Viruses are the oldest form of cyber-attacks and the most popularized in early media. They are lines of code embedded in malware or phishing hooks. When opened, they disrupt a computer's normal operating habits. A virus functions like someone else took over, giving the wrong or jibberish commands. An example of this is Stuxnet, which deployed in 2009. Planted in the network of the Iranian uranium enrichment facility, it manipulated its digital surroundings before transferring to computers in industrial equipment. There, it wrought havoc on physical objects by giving them commands that broke them, such as increasing pressure commands on valves in centrifuges.

Is malware different from a virus?

Malware is a catchall term that means "malicious software." Malware can be spyware, ransomware or adware, among many things, and it can carry a virus. Rather than embedding itself into the operating system or hard drive like a virus, it installs itself and runs as a software. Ransomware is malware that closes a computer, network, or other system until a ransom has been paid and the hacker deactivates the ransomware. In 2017, a ransomware called WannaCry infected tens of thousands of computers in 74 countries, exploiting a vulnerability in Windows software. It even shut down the British National Health System.

Is phishing malware?

Phishing is the process that can introduce malware or open someone to cyber theft. Phishers trick unsuspecting users by posing as a legitimate entity, the hook. The hook may be a spam e-mail, malicious ad, a fake phone call, or even a printed document with false website data. Once someone responds to these hooks, consequences may occur: malware downloaded or personal information stolen. Phishing can also occur on social media. A common phishing scheme is

Types of Cyber-Attacks

called "The Nigerian Scam" or 419: a family member of a Nigerian man e-mails asking for money to help free the man, transfer money out of Nigeria or return him to his rightful place as a royal heir. Clicking on the included link will initiate a phishing scam that steals money and personal information.

What are DoS and DDoS attacks?

A Denial of Service (DoS) attack is when a malicious source makes it impossible for a computer, server or website to access the internet. A Distributed Denial of Services (DDoS) attack does the same thing, but with a distributed architecture. Viruses or malware infect thousands of computers and give them similar directions, making a botnet. The botnet directs all participating computers to go to the organization targeted. Overwhelmed by sudden increase in site visits, the site may shut down or freeze. Other methods of DDoS attacks include sending less computers to visit the site, but they are tasked with asking cumbersome requests, likewise slowing down the site. It prevents legitimate users from being able to access the documents or resources on it. One of the first, and most notorious, DDoS attacks happened to the Church of Scientology. Anonymous, a vigilante hacker group, shut down the religious organization's website, momentarily preventing anyone from learning more about the group.

What are Advanced Persistent Threats?

Advanced Persistent Threats, or APTs, are long, directed cyber-attacks that are most often state sponsored. These types of attacks usually begin with a network probe. An organization or individual illegally, and surreptitiously, accesses an organization's local area network or internal internet. This individual may have gotten in through an employee access gateway or found a vulnerability through other means. The hacker will lurk on the network, hiding from detection, while it maps the information stored there and implements malicious measures. Often, results of APTs include theft, such as the Equifax Security Breach or the HBO breach that released Game of Thrones episodes. These are the most dangerous cyber-attacks.

This is the rule of the data revolution: for every action to store, secure, and use data, there is an equal or greater reaction to steal data.

Cybersecurity Measures

Can you predict a cyber-attack?

An organization is only as safe as its least careful employee with access.

Prediction is the easiest way to start securing data. Appraising data, identifying potential parties that would have interest in it, and anticipating events that may trigger attacks are all predictive measures. However, there are also more technical forms of prediction. These methods will be supported by the application of AI and other technologies to analyze surrounding activity instead of personal security. This may include analyzing dark data produced in a workplace to accurately gauge or identify malicious actors.

How do you prevent a cyber-attack?

Prevention is the most common form of cyber security, but is often inefficient or insufficient. This line of defense includes unique passwords with frequent changes, encryption of all data transmissions across any network, firewalls, securely developed applications, restricted access to data, limited authorizations, regular security testing and tightly secured stored data. Prevention also means establishing an information security policy and network security protocols that are strictly adhered to. An organization is only as safe as its least careful employee with access.

How do you detect a cyber-attack?

Detection is the most important aspect of protection. It is the 24/7 surveillance of vulnerable targets and gateways. Organizations should run "fire drills" of hacking frequently, weekly if not daily, to test their response systems. No software or network is fully patched or protected, so finding the gaps in protection is essential. Detection includes having a dedicated development security operation (DevSecOps) team, where security begins from day one of development. Gone are the days of creating a product or service and securing it from the outside, relying on a lengthy chain of communication. Having a one-stop unit that secures its products and detects future vulnerabilities means faster secure response time.

How do you respond to a cyber attack?

Response is the last line of cyber security and the second most important. Even if a vulnerability is exploited, being able to respond quickly and effectively will save billions of dollars in the worst cases. However, this is some of the least funded areas of cyber security in many organizations. The response team should be comprised of IT professionals, members of a DevSecOps team with intricate knowledge of the entry point, and cyber security experts who can evict the intruder and shore up the protections. Response also

Cybersecurity Trends

includes client service teams that can reassure those affected and help handle the potential damages from consequences. Responding by ignoring the issue is the worst reaction.

Biggest threats

Although all internet, network and computer users should be concerned about cyber security, experts express the most concern about IoT security. It is estimated that 50 billion IoT devices were connected in 2020. That number becomes especially alarming as 70% of IoT devices provide easy access to hackers. These devices are used industrially for sensitive data, in government operations and to record personal healthcare data. More data means more value and more likely to be targeted. Such a large vulnerability risk needs to be addressed.

Another big threat is workforce skills. There is a limited number of workers with the needed IT skills who can take on the jobs necessary to keep data, digital records and networks safe. Jobs in cybersecurity remain abundantly available, but few people are pursuing those careers. Unfortunately, the same has not held true for hackers. People need less experience than ever before to gain access and create scams. The tools one needs to become a cybercriminal can be found easily, even off-the-shelf.

New Technology

Blockchain

One of the primary ways that industry leaders hope to secure data and information passing through their networks is by using blockchain. It's a young technology and primarily used for eCurrency like Bitcoin. Blockchain prevents fraud and unauthorized access by employing both encryption and a consensus system. Essentially, it makes a network of anonymous actors trustworthy by a system that can't be defrauded. It works both in cloud networks and in edge networks. Transactions can be carried out and stored without manipulation; data can be transmitted without fear of being infiltrated. Blockchain in cybersecurity offers the potential to strengthen prevention without spending too much money doing it.

Cybersecurity Trends

Artificial Intelligence

Artificial Intelligence (AI) offers the opportunity to begin detection earlier and to think through security in terms of prediction. AI is the umbrella term for a wide range of tools that can be used to conduct smart computing. A key method to applying AI to cybersecurity will be machine learning and deep learning. A massive amount of data regarding attempted attacks, failures and successful hacking is waiting to be used. By training a cybersecurity bot with deep learning and these data sets, an AI could be made that scans for and predicts or detects threats nearly perfectly.

Edge Computing

Edge Computing is not specifically a cybersecurity technology. However, it offers a new way to conduct cloud computing and IoT networks. Rather than constantly transmitting IoT device data to a central cloud system, carrying out local processing would limit network access and exposed information. Edge computing provides that ability to locally process. By implementing IoT devices that can store a limited amount of information, carry out decisions and function without constant communication with the cloud, operators minimize risk. Moreover, having them communicate via a LPWAN and rely on gateway devices would further reduce opportunities for malicious actors to infiltrate an internet or turn devices into a botnet.

More data means more value and more likely to be targeted.

What does this mean for cybersecurity?

Like all endeavors, ensuring cybersecurity will not be 100% efficient. Even the best laid plans and the most well defended cities have experienced fault and defeat. However, understanding the risks that are out there are the first step to understanding what a company or individual faces in our highly interconnected world. Admitting that data is vulnerable and taking the appropriate protections is the second step to keeping your assets safe. Unfortunately, the cyber world is complex and poorly understood. Readiness, and an eye on constant improvement through new technology, is the only way to handle a cybersecurity issue when it occurs.

Cybersecurity Timeline

1983 ARPANET becomes Internet and accessible to users outside of the military/government

1986 Computer Fraud and Abuse Act of 1986 legislates the criminality of cybercrime

1988 Morris Worm virus deploys and creator is convicted of cybercrime

1996 Web tools enable hackers to manipulate Internet and remotely access machines

2000 Malware, like the ILOVEYOU bug, grows exponentially

Mid 2000s Phishing becomes increasingly prevalent

2007 Mobilization, like the iPhone, creates new vulnerabilities

2008 Anonymous DDoS attack on the Church of Scientology website

2009 Stuxnet virus affects digital and physical well-being of nuclear plant

2014 Automotive software and other machine software becomes targeted for crime

2015 IoT technology start new phase of cybercrime, leading to botnets on an unseen scale

2016 US election hacking rumors

2017 Data breaches are enormous and lucrative, especially with new Ransomware like WannaCry; HBO and Equifax experience breaches;

Infographic