**INTRODUCTION:**

Information security is much more involved than simply the theft of passwords and credit card information. Many recent cyber-attacks have taken place involving the theft of personal data, which has financial implications, but the insecurity of systems has the potential to lead to worse affects. Insecure systems can impact the military, national infrastructure, commercial industry, and each individual. If not dealt with properly in a timely manner the effects could be devastating.

**CYBER WARFARE:**

Since the beginnings of the Internet, cyber warfare has continued to spread. Cyber warfare is computer or network-based conflict involving politically motivated attacks by a nation-state on another nation-state (Rouse & Rosencrance, 2016). Within these types of attacks the intent is to disrupt the activities of organizations or nation-states. Thus, making cyber warfares’ purpose for strategic or military purposes as well as cyber espionage.

Although cyberwarfare generally refers to cyberattacks between or on nation-states, it also can describe attacks performed by terrorist groups or hacker groups with the aim of furthering their goal or cause. There are a number of examples of suspect attacks in recent history, however, there has been no formal agreed upon definition for a cyber “act of war” (Rouse & Rosencrance, 2016). However, any act that leads directly to loss of life, experts agree is an act of war (Rouse & Rosencrance, 2016).

Cyber warfare can take on many differing forms. Viruses, computer worms, and malware are capable of taking down infrastructure, military systems, businesses, and even individual people. Some the most common forms of attacks that are performed include, malware, phishing attacks, SQL injection, denial-of-service, and man-in-the-middle attacks.

Malware refers to various forms of harmful software, such as viruses and ransomware. Once it is in a computer, it can create all kinds of havoc, from taking control of the computer, to monitoring the actions and keystrokes, to silently sending all sorts of confidential data from the computer or network to the attacker’s home base(*Rapid7*, 2017). Attackers are crafty in the methods of getting malware into a computer. It often however, requires the user to take an action in order to install the malware. It can include clicking a link to download a file, or even opening an attachment that looks harmless, like a Word document or PDF attachment, but actually has a malware installer hidden within (*Rapid7*, 2017). Attackers often turn to phishing tactics or pretending to be someone or something else in order to have the user take action. In a phishing attack, an attacker may send an email to the user that appears to be from someone who is trustworthy, like a boss or company they work with (*Rapid7*, 2017). The email will seem legitimate, and will have some urgency to it, like fraudulent activity on an account. There will be an attachment to open or a link in the email and upon opening the malicious attachment, the malware thereby installs on the computer (*Rapid7*, 2017). The link may send the user to a legitimate looking website that asks for credentials for the user to log in to access something. The website is actually a trap that captures the user's credentials when they attempt to log in (*Rapid7*, 2017). Ransomware is a more modern malicious attack that holds computer systems hostage until the victim pays the ransom, even then there is no guarantee that the system will be given back.

SQL injection is the next type of attack, that specifically targets servers that hold critical data for websites and services. Malicious code is used to get the server to divulge information it normally would not. The attacks works by exploiting any one of the known SQL vulnerabilities that allow the SQL server to run the malicious code (*Rapid7*, 2017). Therefore, if not protected correctly private customer information for the websites. Like credit card numbers, usernames, passwords, or other personally identifiable information. Another example is a denial-of-service attack, where an attacker takes action that prevents legitimate users from accessing targeted systems devices, or other network resources (Rouse & Rosencrance, 2016). These are especially impactful toward military, infrastructure, and commercial businesses. Man-in-the-middle attacks also is a way for information or critical data to be stolen. When using the internet, a computer has many small back-and-forth transactions with servers around the world letting them know who the user is and requests specific websites or services. The web servers then respond to the request through giving the information. This is called a session and happens whether the user is simply browsing or when they are logging into a website with username and password (*Rapid7*, 2017). A unique session ID is assigned and should remain private between the two. However, an attacker can hijack the session by capturing the session ID and posing as the computer making a request. This allows them to then log in as an unsuspecting user and gain access to unauthorized information on the web server (*Rapid7*, 2017). Several methods used to achieve this are cross-site scripting and man-in-the-middle where the hijacker inserts themselves between the requesting computer and the remote server and pretend to be the other part in the session, allowing them to intercept information in both directions (*Rapid7*, 2017). All of these attacks impact the cyber realm and the physical world through the military, infrastructure, commercial industry, and even individual people.

**MILITARY IMPACT:**

Insecure computing environments also have and can impact any military in multiple facets. Cyberspace is viewed like a battlefield and nations employ professional hackers as their soldiers. The United States military is no different and is currently, and has in the past, used cyberspace as their battleground with offense and defense maneuvers. The whole process of development began due to insecure computing environments and the threats posed against the United States.

The military action in cyber warfare began with President Reagan in 1983. After viewing the movie *WarGames*, President Reagan was concerned for the cybersecurity within the United States and began to ask questions. After being advised that there were major security concerns a confidential national security decision directive known as NSDD-145 was created to address the numerous threats with current and upcoming technology (Laptops had not really gained popularity yet) (Kaplan, 2017). It was then placed under the care of the National Security Agency (NSA); however, congress would not necessarily pass any legislation that would put the privacy of American citizens to potentially become violated. So, the issue of cyber security faded and then resurfaced during Bill Clinton's presidency. Officials were amazed at the lack of security in the cyber realm, but nothing came about to solve these issues. The issue then resurfaced again with George W. Bush’s presidency but was quickly buried after the September 11, terrorist attacks (Kaplan, 2017). People were concerned with the physical battle rather than one over cyberspace. However, during that time was when the cyber warfare realm changed and emerged as a mutual threat and opportunity for the United States military. Then during president Barack’s presidency cyber warfare took off and was a part of the defense budget that soared.

The cyber field had expanded worldwide, with new reports of cyber-attacks performed by China, Russia, Iran, Syria, North Korea, and others (Kaplan, 2017). However, it was not simply the attacking of opposing nations governments, critical infrastructure was also a target in opposing nations. As far back as Roman times, armies intercepted enemy communications, and this has continued to be a trend in the history of war (Kaplan, 2017). The military use of cyber warfare mimicked that of previous war tactics, just with new methods and technologies applied. The offensive side is to disrupt or feed false information or communication to the opposing force’s leaders. Thus, causing mistakes, disunity, and the misplacement of trust in their communications methods. However, once something can be done to one side it can always be done the other way. Therefore, having secure computing environments is important in many regards to military actions, so that our communications can be trusted.

Having insecure computing environments within the military would have devastating impacts. Seeing as the offensive objective in cyber warfare is to disrupt communication or remove trust in communication of the opposing forces physically or electronically, critical infrastructure then becomes major targets and opportunities (Kaplan, 2017). This puts not only the military in danger, but also citizens. For example, in 2017, *The New York Times* released news of a joint report from the FBI and Homeland Security regarding cyber-attacks on a number of nuclear power plants across America (Ball, 2018). The attacker had used spear phishing methods to target individuals who had access to the critical controls of the plant. Luckily, the attacks were stopped and handled before it was too late, but it proves that critical infrastructure can be used and weaponized as a military objective.

It is also important to keep in mind that whatever one nation can do to another, anyone can potentially do the same to you. Militaries use zero-day exploits, a flaw in software, hardware, or firmware that is unknown to the party or parties responsible for patching or fixing the flaw (Posey & Shea, 2017). Militaries would like to save and store up these zero-day exploits to use as attacks; however, without the patch or fix being developed, another party could perform the same attack on that nation. Therefore, this makes for less secure computing environments within the military. Instead of seeking to use zero-day exploits, the military and government should be using resources to seek them out to preserve and protect computing environments. This would protect not only the military, but also the nation and its citizens from being exploited.

There are three components in helping to manage cyber security risks with the military of the United States. They include minimizing vulnerabilities to systems, understanding the threats to those systems, and minimizing the impact to operational missions (Snyder, 2015). Many layers of software and hardware contribute to these defensive measures to deny access to a system. They should have a robust and resilient backup design while being able to recover rapidly to perform on an acceptable functional level (Snyder, 2015). Security engineering needs to assess how mission assurance is affected. Adaptive solutions can be created to combat the ever-changing cybersecurity environment. However, due to the complex nature of the cybersecurity environment, policies may first need to be adaptive to this feature rather than being conducive and only accounting for simple, stable, and predictable computing environments (Snyder, 2015). The implementation of cybersecurity should be carried and put into effect throughout the life cycle of a military system, instead of taking action only after something has occurred (Snyder, 2015). Accountability should be emphasized within integration and should maintain priority and focus. This will then allow for accountability to be established and for ambiguities in decisions to be erased. Lastly, there should be monitoring and feedback for cybersecurity (Snyder, 2015). It should provide complete, coordinated, and sufficient content for effective decision making for accountability in the future.

**INFRASTRUCTURE:**

Cybercriminals are increasingly attacking governments through their critical infrastructure. Critical Infrastructure includes transportation systems, banking systems, power grids, water supplies, dams, hospitals, and even manufacturing. The connection to the Internet is why the threat of attack has increased. Even if and when these systems can be properly secured, they can still be exploited and hacked.

Industrial Control Systems (ICS) is a term used to refer to a group of process automation technologies, such as Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS) (Maglaras, 2018). These systems have been subject to a growing number of attacks in recent times. These systems deliver vital services to critical infrastructure and hostile intruders performing attacks represents a serious threat to every nation-state.

Industrial Control Systems have special performance and reliability requirements and typically use operating systems, applications, and procedures that may be considered unconventional by modern information technology professionals. The requirements usually follow the priority of availability and integrity, which is followed by confidentiality and include the management of processes that, if not executed correctly, pose a significant risk to the health and safety of human lives, damage to the environment, and serious financial issues such as production losses (Maglaras, 2018). The unavailability of critical infrastructure then negatively impacts the local, regional, national, and even global economy.

Advanced Persistent threat (APT), which is a prolonged and targeted cyber-attack where an intruder gains access to a network and remains undetected for an extended period of time (Rouse & Rosencrance, 2016). The intent of APT attacks is to monitor network activity and steal data rather than to cause damage to the network or organization. However, when it comes to causing damage these attacks they can devastate a country. For example, attacks on a nation’s utility systems can cause havoc by causing widespread power outages, and if an attacker has access to hydropower grids they could also cause flooding through open dams and much more.

In 2010, the Stuxnet worm was used to attack Iran's nuclear program. The worm targeted SCADA (supervisory control and data acquisition) system and was distributed through infected USB devices (Kaplan, 2017). The device was created and used by the United States and Israel to affect and stop/slow down Iran's nuclear program (Kaplan, 2017). It was a computer virus specifically designed for attacking Windows based industrial computers and taking control of the Programmable Logic Controller, influencing the behavior of remote actuators and leading to instability phenomena or worse (Maglaras, 2018). The paradox is that critical infrastructures massively rely on newer interconnected and vulnerable Information and Communication Technology (ICT) technologies, while the control equipment is old legacy software/hardware (Maglaras, 2018). This combination of factors may lead to dangerous situations, exposing the systems to a wide variety of attacks. The worm was affective and did slow down the program, without causing mass destruction. However, this is also concerning to infrastructure due to the fact that it could be implemented and used against other forms of infrastructure with the intent of causing mass destruction.

Even political infrastructure can be affected through Cyber warfare. In March of 2014, the Russian government allegedly perpetrated a distributed denial-of-service attack that interrupted the Internet in Ukraine (Rouse & Rosencrance, 2016). The pro-Russian rebels were then enabled to take control of Crimea. Then in May of that same year, a hacking group based in Russia was able to take down Ukraine’s election commission’s systems three days before their presidential election (Rouse & Rosencrance, 2016). The Ukrainian computer experts were able to get the system back up and running before the election. The attack was to produce havoc and damage the nationalist candidate while assisting the pro-Russian candidate. The attack did not allow the pro-Russian candidate to win the election but did cause havoc and panic.

Then in December of 2016 more than 230,000 people in the Ukraine experienced a blackout, which was the result of remote intrusions at three regional electric power distribution companies (Rouse & Rosencrance, 2016). The attack was suspected to come from Russia. The attacker had flooded phone lines with a denial-of-service attack as well as malware to attack and destroy data on the targeted companies’ hard drives (Rouse & Rosencrance, 2016). Power was able to be restored within a few hours, but the companies that were targeted took months to restore full functionality due to the damages that ensued.

Therefore, the question is raised, Due to all of these attacks is there a way to have secured SCADA systems? Security in SCADA systems is more inclined than with most other computer systems owing to the serious issues and outcomes if there were to be degrading of service, as well as the disruption to day to day life. Today security is of the utmost importance due to greater connectivity, than compared to older systems (Maglaras, 2018). Their communications are also operating through shared Internet Protocol (IP) infrastructure. Thus, more concerns have arisen, like reliability taking precedence over security, absence of encryption with early protocols are still in use, updates patching, or modification are hard to make due to ongoing operation, and expanded lifespan meaning that hardware and software are operating beyond supported lifespans (Maglaras, 2018). With all of these concerns in mind with the characteristics and constraints with SCADA systems, means that domain specific approaches are necessary (Maglaras, 2018). In-line security mechanisms or security tools on a host level are not recommended due to the possible delayed impact or the occurrence of single points of failure along vital communication paths (Maglaras, 2018). Also, seeing as attacks are increasing in sophistication, current cyber security cannot depend on pattern-based detection to guarantee continuous security monitoring. Rogue threats need to be able to be caught and handled, which would provide a suitable balance between maintenance and detection power (Maglaras, 2018).

Furthermore, a large percent of attacks are induced by inside attackers. Therefore, perimeter defense alone cannot defend the systems. There must be a way to determine if there is an ongoing attack through the dynamics of the system itself (Maglaras, 2018). However, human error gets in the way and prevents methods like this to currently be in use (Maglaras, 2018). Therefore, more research should be done in studying the errors people have made to establish ways in which cyber security can develop and overcome this challenge.

Security measures also do not take into account that attackers are persistent and will do everything in their power to gain access, no matter what the perimeter protection is. The main objective of modern security solutions is to develop novel methods that could detect and disturb the activities of the attackers once they have gained access (Maglaras, 2018). Special care should be given to the implementation of these new strategies, seeing as they can detect, prevent, and mitigate data exfiltration attacks, since intrusion detection/prevention strategies are not suitable for data protection (Maglaras, 2018).

To strengthen the security of SCADA systems, a solution is to deliver defense in depth through the layering of security controls to reduce the risk to the assets being protected. Through the application of multiple controls on top of the information asset (ICS configuration and management data) the architect would introduce further barriers that attackers would then have to overcome (Maglaras, 2018). This will slow down attackers and within the time it would take to get through some of the controls the monitoring service should have alerted someone to the attack. This allows for further action to be taken. The depth of the defense ensures that there would be no single point of failure from threats, through the different barriers (layers) (Maglaras, 2018).

**COMMERCIAL IMPACT:**

The commercial industry is another area in which insecure computing environments have a great impact. Commercial industry focuses on widespread production and has the goal of selling the maximum amount of products or services to customers. E-commerce has improved and increased in popularity thanks to the commercial industry as well. However, insecure computing environments bring about attacks dealing with theft of customer information and corporate espionage.

The types of attacks that are used within computing environments are plentiful. Some of the most commonly used are malware, phishing attacks, SQL Injection, and Man-in-the-Middle attacks. With the boom in e-commerce in society, more data about customers is stored by companies. Unfortunately, this data that is stored in databases by these companies is sometimes not well protected and/or employees are untrained or uninformed on how this information can be stored properly with the amount of protection it needs. For, example in April of 2018 Hudson’s Bay Company, the parent company for Saks and Lord & Taylor retail stores, announced that they were victims of a security breach (DiGiacomo,2018). The breach had compromised data on payment cards used at Saks and Lord & Taylor stores in North America (DiGiacomo,2018). Their entire system for Lord & Taylor was compromised, while only 83 Saks stores were compromised in the New York and New Jersey regions (DiGiacomo,2018). The details on five million credit cards and users had appeared on the dark web for sale, however, they cannot be sure if more information was stolen (DiGiacomo,2018). Another attack was that of the WannaCry Ransomware in May of 2017. While this is not necessarily a data breach it also is evident to the impact of insecure computing environments. This ransomware attack infected computers and servers in 74 countries and millions of users around the world (DiGiacomo,2018). It affected hospitals, businesses like FedEx, rail stations, and universities (etc.) (DiGiacomo,2018). These attacks cause for lack of trust from customers and will cause them to move their trust and business to another company or organization, which can be devastating to that organization.

Although payment and personal information are mostly sought after through data breaches, it is not the only data that is sought after. In the manufacturing industry 53 percent of breaches were state-affiliated attacks according to the 2018 Verizon Data Breach Investigations Report (Calyptix ,2018). The strength of a country's economy is truly what the strength of a country rest on and many nation-states want to give their companies a leg up to the competition. Therefore, more than half of the data breaches in manufacturing were state-sponsored attacks in order to gain other competitors trade secrets, personal information, and credentials (Calyptix ,2018). Cyber-espionage followed with making up 31 percent of breaches. Espionage was the leading attack pattern for breaches in manufacturing (Calyptix ,2018). Espionage is said to be 47 percent of the motivation behind data breaches (Calyptix ,2018). In manufacturing 50 percent of breaches discovers were found to be the result of hacking, including brute force and SQL injection (Calyptix ,2018). 58 percent of breaches involve the compromising servers (Calyptix ,2018). Corporate espionage can be devastating and cause an organization to become unstable. They can lose customers to competition, lose financial backing, and even go out of business. Therefore, the impact is increasingly heavy with consequences not for the organization alone, but for a country’s economy.

There are many motives for attacking companies, businesses, and commercial industries. However, whatever the motive is, the impact of these attacks are financially and economically devastating. Therefore, companies and businesses should be putting increasing effort into prevent these attacks from being successful and making their computing environment more secure. Some ways that organizations can improve their computing situation is to perform risk analysis regularly to first identify the economic and financial consequences of a breach so that they can then be quantified. They then can develop solutions to combat the attacks based upon those findings. Another way is to have informational and educational sessions to teach employees about some of these attacks and what they look like so that they can avoid making the mistake and allowing malicious code to have access to the network. Lastly, the technology department should always be on alert and seeking out new adaptive solutions to keep intruders and attackers out. They should make sure all equipment and software is patched and there should be monitoring of every system. All safety measures and precautions should be taken or be sought out to bring more secure computing environments.

**PERSONAL IMPACT:**

Insecure computing environment also being about concerns for individuals. Individuals are also impacted through all of the other areas as well. They can be impacted through nation infrastructure, military attacks or defense, as well as commercial industry with security breaches. As seen already, insecure computing environments can lead to the loss of personally identifiable information and manipulations, which can bring financial losses and hardship. However, there are was for everyone to protect their information and identity.

One way to provide better protection from cyber-attacks is to use different passwords for each account a person has. Once an attacker has one password, if the individual uses that password for all or multiple accounts they have access. The impact can be quite heavy if the password is used for social networking and online payment accounts. Another way individuals can protect themselves is to update browser and payment wallet aps software regularly. Browsers may contain some vulnerabilities which attackers can exploit to steal information (Kulkarni, 2017). Updates and patches are made by the developers regularly to fix these flaws so that they can no longer be used. Individuals should also avoid opening links of prizes, gifts, and discounts, like those that come with email. As stated with commercial industry, phishing attacks are commonly used to deceive users into allowing malicious files to be downloaded onto their computer. The attackers can then gain access and manipulate the persons data and information.

Users should also make sure that any software they download is from authentic sources. Otherwise it may have been modified by an attacker to steal user information (Kulkarni, 2017). When using third-party computers or mobiles for browsing use the private/incognito mode. This prevents the browsing history and user credentials from being stored so that they cannot be stolen (Kulkarni, 2017). Also, while using third party computer use and on-screen keyboard while entering important details. This prevents a software known as a keylogger from capturing all the data entered by a user. Users should also always check the URL to make sure they are going to the site they want to as well as ensuring that the site contains HTTPS instead of HTTP (Kulkarni, 2017). the HTTPS is a protocol for browsing the internet that uses encryption techniques and is more secure than HTTP (Kulkarni, 2017).

Users are able to provide and establish protection for themselves against insecure computing environments in multiple ways, even if there are rippling affects that flow down from military, infrastructure, and commercial industry. Therefore, if users take precautions they should be able to lessen the impacts that insecure computing environments present.

**CONCLUSION:**

Insecure systems impact the military, national infrastructure, commercial industry, and each individual person. Within the military and the realm of cyber warfare communication can be disrupted or edited to seek out commotion and havoc. This can damage military efforts to combat an enemy and impacts warfare in a large way. Opposing forces can gain intel due to insecure environments which impacts war efforts. Also, within military impacts, it is a necessity for military leaders to keep in mind that when dealing in cyber warfare, that whatever is capable of being done to one side is capable of being done back. Thus, security within military entities is in need of constant improvement and new adaptive solutions to combat the changing cyber environment. Infrastructure is sometimes an easy target due to insecure computing environments. With the extended and increased connectivity national infrastructure becomes a target (not just to military entities). The attacks can lead to the damage and loss of human lives, damage to the environment, and financial losses with economic consequences. Even politics and be impacted through attacks on national infrastructure. These computing systems should be constantly increasing in security measures. Commercial industries also are in need of boosting their cybersecurity. With e-commerce booming and constantly changing, customers and companies can become subject to attacks. Whether the motivation behind is theft of customer information or for corporate espionage the organization and the economy is impacted. Organizations need to continue to provide protection for customers and themselves as the digital age continues to advance. Lastly, individuals need to protect themselves within their own computing environments but also from all of the levels above each individual. Each individual person could potential be impacted through military, infrastructure, or commercial insecure computing environments. Therefore, educating and learning ways to protect themselves is increasingly important. As the digital age continues to advance, solutions should continue to be developed to combat and face the issues of insecure computing environments.

Work Cited

Ball, Tom. “Top 5 Critical Infrastructure Cyber Attacks.” *Computer Business Review*, Computer Business Review, 18 Jan. 2018, www.cbronline.com/cybersecurity/top-5-infrastructure-hacks/.

Calyptix. “Top Causes of Data Breaches by Industry 2018: Verizon DBIR.” *Calyptix Security*, 13 Apr. 2018, www.calyptix.com/top-threats/top-causes-of-data-breaches-by-industry-2018-verizon-dbir/.

“Common Types of Cybersecurity Attacks and Hacking Techniques.” *Rapid7*, 2017, www.rapid7.com/fundamentals/types-of-attacks/.

DiGiacomo, John. “Data Beach Statistics For 2018 Plus Totals From 2017 | Revision Legal %.” *Revision Legal*, John DiGiacomo Https://Revisionlegal.com/Wp-Content/Uploads/2014/09/Trans-RL-Logo-Grey1.Png, 29 Aug. 2018, revisionlegal.com/data-breach/2018-statistics/.

Kaplan, Fred M. *Dark Territory: the Secret History of Cyber War*. Simon & Schuster Paperbacks, 2017.

Kulkarni, Ashish. “10 Ways to Stay Safe from Cyber Attacks – All Technology Feeds(Powered by Algoworks) – Medium.” *Medium.com*, Medium, 23 May 2017, medium.com/all-technology-feeds/10-ways-to-stay-safe-from-cyber-attacks-6449219ceb54.

Maglaras, Leandros A., et al. “Cyber Security of Critical Infrastructures.” *ICT Express*, vol. 4, no. 1, 2018, pp. 42–45., doi:10.1016/j.icte.2018.02.001.

Posey, Brien, and Sharon Shea. “What Is Zero-Day (Computer)? - Definition from WhatIs.com.” *SearchSecurity*, 2017, searchsecurity.techtarget.com/definition/zero-day-vulnerability.

Rouse, Margaret, and Linda Rosencrance. “What Is Cyberwarfare? - Definition from WhatIs.com.” *SearchSecurity*, 2016, searchsecurity.techtarget.com/definition/cyberwarfare.

Snyder, Don. *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles*. 2015, *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles*, www.rand.org/content/dam/rand/pubs/research\_reports/RR1000/RR1007/RAND\_RR1007.pdf