Another day, another cyber attack. It seems that as technology grows, so does the frequency and variation among them. From Fortune 500 companies to the everyday internet user, cyber attacks are affecting everyone on a global scale. In fact, cyber attacks are showing continued growth and has officially surpassed the global drug trade in terms of profitability (Khimji). While the motives for the types of attacks are all different, the attack methods are very similar. Therefore, is up to cyber and information security professionals to create new safeguards to reduce the threats of these cyber attacks and protect technology users.

In today's society, different cyber attacks are prompted by diverse types of motives. Over the years, cyber crimes have become lucrative for criminals with personally identifiable information (PII) and zero day vulnerabilities requesting a high price on the dark web. However, not all attacks are for the purpose of financial gain, with the objective of some cyber attacks being hacktivism, notoriety in online hacking circles, and lulz (amusement). One notable non-financially motivated hacking group is that of Anonymous, who is virtually involved in the fight against ISIS (Rogers). In addition, another motive for cyber attacks is the interests of nation states. These types of cyber attacks are considered cyber warfare, where the purpose is to perform espionage, attack critical infrastructure, and cause civil unrest. With that being said, most governments participate in some form of state sponsored attacks with the most notable in today's society being from Russia, China, and the United States government. Each of these types of cyber attackers take advantage of anonymity that the internet provides, which makes identifying the purpose of a cyber attacks a challenging task.

Despite the differences in motivational factors among cyber attackers, these attackers generally utilize the same type of attack techniques. While the list of attack methods is quite extensive, the three most successful forms of attacks in 2016 are phishing, social engineering and malware (ISACA). Phishing and social engineering are the most similar in that both rely on the human element in their attacks. Phishing is the act of sending an email to have the recipient download some form of malware or release some type of confidential information such as PII or intellectual property. Social engineering is the act of manipulating an individual into performing some type of action that helps complete the attacker's goal. While some attacks are completely relied on social engineering and phishing, such as the Seagate W2 Data Breach (Krebs), these attacks are often utilized to gain intelligence on a target as well as gain entry into a target’s environment. From there, an attacker might place malicious software (malware) on the targets network, deploying its payload and then potentially completing the objectives of the cyber attack. Despite phishing, social engineering, and malware being the most common vectors for attacks, cyber attackers will utilize all the tools they can until their objective is met.

Although cyber criminals have multiple attack methods to complete their objectives, government agencies and business organizations are continually trying to safeguard its assets and protect users. First, organizations have recently adopted a “Hack Yourself First” mentality, which is that organizations need to on a regular basis perform penetration tests on its own systems (Hunt). Such benefits include the ability to find vulnerabilities before cyber criminals, is a method to test the effectiveness of security implementations, and assists in the continuous improvement of an organization’s security. Second, organizations need to continually provide awareness training to its employees. Since social engineering and phishing are some of the most effective vectors for attacks, human capital can be the weakest link in an organization's security environment. Therefore, employee training of basic security is critical. Lastly, the government has been taking initiatives which include the White House appointing the country's first Chief Information Security Officer in 2016 (Scott) as well as New York State recently implementing cyber security requirements on banks and insurers (Reuters). While these safeguards only account for a small number of controls, the government and businesses are continually increasing their efforts to protect themselves and their citizens.

Unfortunately for cyber and information security professionals, each day brings a new challenge. Over the last year or so, we have already seen new threats emerge such as IoT device distributed denial of service attacks as well as an increased frequency of mobile malware attacks (Kaspersky). However, an emerging technology that will likely be ripe for potential exploits is that of autonomous vehicles. This technology is considered to affect both consumer transportation and commercial trucking, as it replaces the human need in directing a vehicle with a computer system. Therefore, two threats that could emerge from this technology is that of ransomware and theft. If a cyber attacker can access control of the car, they can hold it for ransom. Much similar, cyber attacks can exploit autonomous commercial trucks by either redirecting the vehicle to loot the physical goods or lock the autonomous vehicle for ransom. Such safeguards that will likely be considered are improved logical access controls protecting access to the vehicle's computer control system. In addition, for commercial trucks, physical security controls, such as security personnel or hardened trailers, might be able to prevent access to the physical goods inside. While the goal of autonomous vehicles is to prevent the need for humans to direct the vehicle, the industry will likely need to address these cyber related threats in the future.

Unfortunately, cyber attackers have the upper hand as each day brings new technology which can be exploited. This means that it is crucial for cyber professionals to stay up to date with the most current vulnerabilities as well as prepare for future threats. Likewise, as new nations develop and internet usage rises, new attackers will enter the market. However, through information sharing, the strive for continuous improvement, and an offensive mindset, organizations can help reduce the threats of cyber attacks and attempt to stay one step ahead of cyber attackers.

Works Cited

Hunt, Troy. "Hack Yourself First – How to Go on the Offence before Online Attackers Do." Troy Hunt. Troy Hunt, 15 May 2013. Web. 09 Apr. 2017 <https://www.troyhunt.com/hack-yourself-first-how-to-go-on/>

Khimji, Irfahn. "Cybercrime Is Now More Profitable Than The Drug Trade." *The State of Security*. 30 Mar. 2015. Web. 07 Apr. 2017. <https://www.tripwire.com/state-of-security/regulatory-compliance/pci/cybercrime-is-now-more-profitable-than-the-drug-trade/>.

Krebs, Brian. "Krebs on Security." Brian Krebs. 6 Mar. 2016. Web. 09 Apr. 2017. <https://krebsonsecurity.com/2016/03/seagate-phish-exposes-all-employee-w-2s/>

"Rise of Mobile Malware." Kaspersky Lab. Kaspersky Lab, Web. 09 Apr. 2017. <https://usa.kaspersky.com/internet-security-center/threats/mobile-malware#.WOg1SVcp99M>

Reuters. "Here's When New York State's Cybersecurity Rules Take Effect." New York State's Cybersecurity Rules Take Effect on March 1. Fortune, 16 Feb. 2017. Web. 09 Apr. 2017. <http://fortune.com/2017/02/16/new-york-state-cyber-security-regulation/>

Rogers, Katie. "Anonymous Hackers Fight ISIS but Reactions Are Mixed." The New York Times. The New York Times, 25 Nov. 2015. Web. 09 Apr. 2017. <https://www.nytimes.com/2015/11/26/world/europe/anonymous-hackers-fight-isis-but-reactions-are-mixed.html?_r=0>

Scott, Tony, and Michael J. Daniel. "Announcing the First Federal Chief Information Security Officer." *National Archives and Records Administration*. National Archives and Records Administration, 8 Sept. 2016. Web. 09 Apr. 2017. <https://obamawhitehouse.archives.gov/blog/2016/09/08/announcing-first-federal-chief-information-security-officer>

"The 'State(s)' of Cybersecurity." Security in Cyberspace : Targeting Nations, Infrastructures, Individuals 15. ISACA. Web. 9 Apr. 2017. <https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf>