CS 573 FINAL

STATE OF GLOBAL CYBER SECURITY – 2036

RAHUL GODUGUPALLY (CWID-10470581)

INTRODUCTION

In the last 15 years, the world has seen tremendous improvements in the areas of automation, artificial intelligence, and machine learning. Convenience is a huge part as every device has integrated into IOT and communicates information through the network. It made life much easier as almost all devices talk to each other, making human tasks easier. Shopping apps like amazon can predict when you will need groceries, and have it delivered to you before you realize that you need it. During the beginning, there were concerns raised about the security aspects of automation, but convenience topped all. As people grew accustomed to automation technology, devices talking and being in sync with one another, it was harder to replace them.

With the implemetation of Machine learning and artificial intelligence, the low-skilled work started to be replaced by machines as they could do the job more efficiently and at a much lower cost. Cybersecurity has been implemented with the help of Artificial Intelligence. Most of the companies have been deployed on the cloud as they are more secure than maintaining their own servers, and the few which have not completely moved operate in a hybrid model. Internet Of things would be prevalent, and the boundaries of the network would not exist anymore.

6G has been implemented around the world and since it has been released, devices have been able to connect to the internet at blazing fast rates. Also, since computer hardware became more expensive to buy and maintain most of the organizations looked for a solution on the cloud to provide services. Most computationally demanding programs run on the cloud, for example, games are played over the cloud, video editing is done on the cloud and the final file is just downloaded onto the end user system. This alleviates the need for common users to have high-end computers.

Major Cyber Security Threats

The major cyber security threats facing our globe are grouped into the following 4 categories

1. Cyber threats impacting Technology and Finances
2. Cyber Theft
3. Cyber threats impacting Quality of life
4. Cyberwarfare threats

1) Cyber threat impacting Technology and Finance:

These cyber-threats include attacks that impact the finances of a company or state. They range from Denial-of-service attacks, Ransomware to Phishing attacks as they negatively influence the money-making ability of the entity and target the vulnerabilities of technology provided by them to carry out the attacks. For instance, a Denial-of-service attack on an E-commerce website inhibits them from earning money and providing resources to end users.

These types of attacks are performed by hacktivists, Black hat hackers, Disgruntled employees, or Rival organizations. The main aim of these attacks is to impact the finances or reputation of the company. Data breaches, on the other hand, are commonplace as more data is kept online any misconfiguration or mishap is exploited and data is breached.

2) Cyber Theft:

Cyber theft involves stealing confidential information or having access to information to which they are not supposed to. This can also include stealing resources and assets online. For example, Hacking credentials of a user to steal money from their bank account. In 2036, most money is digital, either in the form of decentralized cryptocurrency or digital money in the bank stored on a remote server. And, the use of credit or debit cards is replaced by authenticating transactions with a phone, through NFC or some other technology using personal mobile devices. As these technologies are wireless, attackers can sniff the information and can either decrypt or inject packets to modify the sender and receiver of the transaction. These attacks are performed by Criminals, Rouge organizations, Black hat hackers etc.

3) Cyber threats impacting Quality of life:

These cyber-attacks are the ones that have an impact on people and their quality of life. These could be anywhere from hacking of an Energy plant to shut off electricity to an area, impacting a water plant to prevent Industries or cities with water supply, shutting off the natural gas supply to prevent natural gas to people etc. These attacks have a significant impact on the functioning of a state. This could also include Hacking of medical devices to cause harm to people, taking control of the self-driving car to induce harm etc. The main threat actors of these attacks could be Black Hat hackers, Criminals, foreign government agencies etc.

As Artificial intelligence, Internet of things and Automation grew the instances of these attacks also grew in number. Considering the situation in 2036, the harm these attacks can cause can be substantial to the development of a nation.

4) Cyberwarfare Threats:

In 2036 the state of cyberwarfare has still not reached its peak. Nations are in the process of understanding the impact of these cyber-attacks and how these attacks could be deployed at a higher level. These attacks are nations going against each other exploiting each other's cybersecurity infrastructure. These include exploiting dangerous technologies owned by nations' military or government. It can include the ability of the enemy to take control of the nation's missile system and launch them, their ability to control drones and other military technology remotely. It could also include the ability to exploit nuclear power plants and critical infrastructure of a nation. Advanced persistent threats are mainly used to exploit these, As APT’s can be in the network for a long time without being detected. Critical information such as state secrets and high-level clearance information can be obtained as enemy states invest a lot of time and resources into this.

These attacks are performed by threat actors such as Nation-states, Terrorists, Government agencies

Major Cyber Security Protections

The major cyber security protections protecting our globe today can be grouped into the following:

Automation: Automation has become a key aspect of cybersecurity; major companies have developed AI algorithms that detect and prevent attacks from taking place. These AI algorithms have been very impactful in dealing with various attacks such as flooding, denial of service, jamming attacks etc. The implementation of (good) bots to detect and deal with these problems is taking place in all major organization networks. On the other hand, many bots developed using AI are used for nefarious purposes. The bot vs bot attacks are expected in these times, the bots which defend the network give more time for security professionals to identify and deal with the incident taking place.

Antivirus implemented with AI analyses the user behavior and maintains a pattern of the user. In case of any abnormalities in the pattern, the antivirus can flag that and compare it to the usual behavior and report if anything suspicious. It reports on threats such as malware, phishing etc.

Multi-Factor Authentication: Multifactor authentication mechanisms play a huge role in authentication of end users now-a-days. As people realized the weak points of using only passwords and their ineffectiveness to properly authenticate users. Various multifactor authentication mechanisms have been implemented in most of the systems to prevent spoofing and fraudulent practices. These mechanisms include Biometrics (Something you are) in addition to Pin, Passwords (Something you know) or devices to identify your authenticity (Something you have). Implementation of these mechanisms has seen a significant boost in the prevention of malicious activities, especially with hackers being able to spoof the identity of the user with development of AI and ML tools.

Stronger Encryption Algorithms: As the world has seen leaps of improvements in quantum computing and as more computational power becomes available the need for stronger encryption algorithms was a necessity. These new Encryption Algorithms with larger key sizes and stronger encryption have made cracking them much more difficult. These algorithms are paired with salting techniques that have made cracking them difficult even with a brute force attack with unlimited resources.

Decentralization: Many of the software's have been decentralized to have better security, the use of cryptocurrencies with blockchain and peer-to-peer networks has gained popularity as privacy has become a huge concern among certain population.This led to many of them using VPN’s and tor browsers to mask their identities.

Recommendations

As most of the world leaders in 2036 have at least a basic knowledge of cyber security it is easier to convince them compared to 2021. The governments have dedicated a significant amount of funds to cyber security research to improve cyber security practices. However, still the smaller countries lack the resources needed to compete with the top nations, this would make them vulnerable to attacks and incapable of defending themselves in case of a full-out cyber warfare.

My first recommendation to the world leaders in 2036 would be to implement a **universal framework** for identifying cyber security threats, risk, and their responses to these threats. As cyber threats continue to take new forms it is essential to understand how to deal with these threats by coming together and proactively dealing with them. This would significantly help the nations who do not have the capacity to invest and research these defenses.

My other recommendations for world leaders today in 2036 include the implementation of multilayer security approaches such as Defense in Depth in all critical networks. As defense in depth incorporates multiple layers of defensive mechanisms with redundancies to improve the security of systems and increases the complexity to exploit the system.

I would also advise them to place critical information servers which host valuable information such as State secrets, launch codes, isolated from the network. This way they are secure from various attacks such as APT’s and Phishing.

Also, the implementation of **access controls** with the help of multifactor authentication should be implemented on all the networks. Users should be able to have access, read and edit the data they have access to and should not be able to access the data which is not assigned to them. As stricter access control methods can help prevent a rogue employee from gaining access to confidential information.

Various attacks such as ransomware, phishing and different malware still cause a huge concern to the users. Constant updates and frequent security assessments are required to be mandated for these problems to be mitigated. Hence, I would recommend frequent security assessments for these systems.

The use of legacy devices should be avoided as they are vulnerable to attacks and could be easily exploited. Similarly, weaker encryption algorithms should be avoided in order to have secure infrastructure.

The use of end-to-end encryption should be implemented on all modes of communication such as emails, texts etc. even within the infrastructure networks as these can be easily accessed with sniffing or man in the middle attacks. With stronger encryption these can be even more difficult to decrypt and can help prevent leakages.

CONCLUSION

The cybersecurity landscape in 2036 is evolving into a main category of warfare and is a constant threat as most things take place over the internet. With the implementation of various technologies in Cyber security such as Artificial Intelligence, Machine learning and automation, security remains a key aspect of everyday life. Many implementations will have been made to secure oneself to an extent, but it is still important to educate users about cyber security and how to mitigate the risks caused by the attacks.