 doi:10.20944/preprints202208.0235.v1

Review

Cyber security; Etiology and Importance

Syed Adnan Javed[1*]

1Department of Aeronautics, IGlobal University, 8133 Leesburg Pike, 2nd floor, Vienna, VA 22182, USA
E-mail: adnan.jawaid@hotmail.com

Abstract

Background: Cyber Security is to protect online data and software from cyber threats. These cyberattacks are typically intended to gain access to, change, or delete sensitive information; extort money from users; or disrupt regular corporate activities. It is difficult to keep up a regular follow up with new technologies so it is necessary to keep the important data safe from cyber threats. There are many types of cyber threats; malware, ransom-ware, social engineering, phishing etc. To prevent cyber-attacks one can use password manager tools like LastPass and others. People also use two factor authentication for double security on their accounts.

Methods: Boards such as the National Institute of Standards and Technology (NIST) are developing frameworks to assist firms in understanding their security risks, improving cybersecurity procedures, and preventing cyber assaults. The fight against cybercrimes and attack, rganisations needed a strong base there are 5 types of cyber securities; Critical Infrastructure Security, application security, network security, cloud security and (IoT) Security. In the modern time US is highly based on computers and on different software so it is really important for US to be more conscious about the security as they get many threats almost everyday for hacking their data and accounts.

Results and Conclusion: Nowadays, even small businesses rarely recover their loss from the cyber-attacks and many back-off from continuing their businesses after being target of hackers. The first cybercrime attack was recorded on 1988 by a graduate student. Now that large companies and even small businesses are aware of cyber-attacks so they try their best to take every precaution to prevent the hacking with double security and password manager tools.

Keywords: Malware; cyber security; cyber-attacks; two factor authentication; software; targeting; privacy; causes of cyber attacks

1. INTRODUCTION

1.1 Influence of Cyber Security

Cybersecurity is the protection of internet-connected systems against cyberthreats such as hardware, software, and data. Individuals and businesses utilize the method to prevent illegal access to data centres and other digital systems. A robust cybersecurity strategy can provide a good security posture against hostile attacks aimed at gaining access to, altering, deleting, destroying, or extorting an organizations or user's systems and sensitive data. Cybersecurity is also important in thwarting attacks that try to disable or impair the operation of a system or device. Cybersecurity is the protection of government or business computers, servers, and networks against hostile assaults and threats, as well as the protection of information such as data from unauthorized access (1).

Cybersecurity is critical in the realm of information technology. Securing information has become one of today's most difficult issues. When we think of cyber security, the first thing that comes to mind is 'cyber-crimes,' which are expanding at an alarming rate. Various governments and businesses are taking several steps to combat cybercrime. Aside from such efforts, many people are still concerned about cyber security. This article focuses on the current technologies' cyber security issues. It also covers the most recent developments in cyber security tactics, ethics, and trends that are transforming the face of cyber security.

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. It is necessary in order to protect information and other assets from cyberthreats, which take many forms.

 doi:10.20944/preprints202208.0235.v1

1.1.1 Types of Cyber-threats

- **Malware** is a form of malicious software in which any file or program can be used to harm a computer user. This includes worms, viruses, Trojans and spyware.
- **Ransomware** is another type of malware. It involves an attacker locking the victim's computer system files -- typically through encryption -- and demanding a payment to decrypt and unlock them.
- **Social engineering** is an attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.
- **Phishing** is a form of social engineering where fraudulent email or text messages that resemble those from reputable or known sources are sent. Often random attacks, the intent of these messages is to steal sensitive data, such as credit card or login information.
- **Spear phishing** is a type of phishing attack that has an intended target user, organization or business.
- **Insider threats** are security breaches or losses caused by humans -- for example, employees, contractors or customers. Insider threats can be malicious or negligent in nature.

Both inherent risk and residual risk are increasing, driven by global connectivity and the use of cloud services, such as Amazon Web Services, to store sensitive data and personal information. Widespread misconfiguration of cloud services coupled with increasingly sophisticated cybercriminals means the risk of your organization suffering a successful cyberattack or data breach increases. Business leaders can no longer rely solely on off-the-shelf cybersecurity solutions like antivirus software and firewalls, cybercriminals are getting smarter, and their tactics are becoming more resilient to conventional cyber defenses. It is important to cover all areas of cybersecurity to be well protected. Cyber threats can come from any level of your organization. Workplaces should include cybersecurity awareness training to educate staff on common cyber threats such as social engineering scams, phishing, ransom ware attacks, and other malware designed to steal intellectual property or personal data.

Basically, our society is more dependent on technology than ever before and there is no sign that this trend is abating. Data breaches that can lead to identity theft are now posted on social media accounts. Sensitive information such as social security numbers, credit card information and banking details are now stored in cloud storage services such as Dropbox or Google Drive. The fact is, whether you are an individual, a small business or a large multinational, you depend on IT systems on a daily basis. Combine that with the rise of cloud services, poor cloud service security, smartphones, and the Internet of Things (IoT) and we have a host of potential security vulnerabilities that didn't exist a few decades ago. We need to understand the difference between cybersecurity and information security, even though the skills are increasingly similar.

To keep track of everything for cybersecurity precautions, use a password manager application such as LastPass, Dashlane, or Sticky Password. These programmes assist in the usage of unique, safe passwords for each site's needs while also keeping track of them all for themselves. An attacker can easily obtain access to your network by using obsolete credentials that have gone by the wayside. Delete any unneeded accounts. Enabling two-factor authentication to offer extra protection to your logins may assist with account security. It is an additional layer of protection that makes it more difficult for an attacker to get access to your accounts (2).

California was the first state to regulate data breach disclosures in 2003, requiring individuals or companies to notify affected individuals "without reasonable delay" and "immediately upon discovery". Victims can sue for up to $750 and companies can be fined up to $7,500 per victim. This has prompted standards bodies like the National Institute of Standards and Technology (NIST) to publish frameworks to help organizations understand their security risks, improve cybersecurity measures, and prevent cyberattacks.

 doi:10.20944/preprints202208.0235.v1

2. METHODS

In today's technical environment, many of the latest technologies are changing the face of humanity. But due to these emerging technologies, we are not able to protect our private information very effectively and hence, at present, cyber crimes are increasing day by day. Today, more than 60% of total business transactions are conducted online, so this area required high-grade security for seamless and better transactions. Therefore, cybersecurity has become a recent topic. The scope of cyber security is not only limited to the protection of information in the IT industry, but also to other areas like cyberspace, etc. Even the latest technologies like cloud computing, mobile computing, e-commerce, online banking, etc. they also need a high level of security.

Since these technologies contain important information about a person, their security has become a must. Improving cybersecurity and protecting critical information infrastructure is essential to the security and economic well-being of every nation. Making the Internet safer (and protecting Internet users) has become an integral part of the development of new services as well as government policy. The fight against cybercrime requires a more secure and holistic approach. Since technical measures alone cannot prevent any crime, it is essential that law enforcement is able to effectively investigate and prosecute cybercrime. Today, many countries and governments enforce strict cybersecurity laws to prevent the loss of important information. Every individual should also be trained in this cyber security and protect themselves from these growing cyber crimes.

2.1 Types of Cyber Security

There are five main types of cyber security which includes;

1. Critical Infrastructure Security

This sort of cybersecurity guarantees that our important public services' digital infrastructure is kept and safeguarded from malicious usage. Simply said, critical infrastructure security includes keeping hackers away from our hospitals, traffic, and power system, among other things.

2. Application Security

Nowadays, with apps for almost everything, it's critical to maintain the area safe. Application security does this by including all security measures, such as encryption, firewalls, and anti-virus systems, from the beginning of the development process.

3. Network security

Network security, as the name indicates, is a field of expertise largely concerned with maintaining network integrity. In practise, this entails exercising due diligence to ensure that networked data and systems are protected by the highest security standards and protocols.

4. Cloud Security

Despite the fact that cloud computing is widely regarded as the least secure method of storing data, experts believe that clouds are safer than traditional IT infrastructures. On-premise environments have approximately half the number of assaults as those supported by a provider. In general, these companies are the largest producers of cloud security products that maintain the space safe.

5. Internet of Things (IoT) Security

The Internet of Things security is concerned with safeguarding all internet-connected devices, and we are reaching a point where they will simply be referred to as our "things." Everything is networked, from security cameras to the tiniest home appliances. As a result, practically everything can and should be free of vulnerabilities and secure against future cyber attacks.

The study begins with a case study of three actors involved in cybercrime and their use of the public forum. We rank you against other forum users using machine learning and perform content analysis on your forum interactions. These analyzes provide a better understanding of the role of public space for these actors, as explained below. This section first introduces the background to the case study, including an introduction to the public forum and how we collect your publicly available data. The data and methods

 doi:10.20944/preprints202208.0235.v1

are then presented, followed by the results of the case study. Additionally, today's online configuration may change the way criminal and informal markets intertwine in specific cases. This is all the more true as the Internet becomes an important channel for economic transactions and as informal online economies flourish. Furthermore, the potential trust issues and uncertainties that informal market actors often face in traditional contexts, leading them to develop strong social structures, have been partially counteracted by the rise of informal institutions. Informal institutions are platforms that provide mechanisms to neutralize trust issues between market participants through various reputation systems, such as feedback. (3)

Cyber-attacks pose a significant threat to businesses of all sizes, government agencies, and individual internet users. Recent cyber-attacks have come from hacktivist groups, lone wolf hackers, and nation-states.

The first cyber-attack on record was The Morris Worm in 1988. Robert Tappan Morris, a graduate student at Cornell University, developed a worm program that would crawl the web to count how many computers were connected to the internet. However, the worm installed itself on one in seven computers and forced them to crash, which saw it inadvertently become the first distributed denial-of-service (DDoS) attack. The Morris Worm damaged around 6,000 computers, which then comprised 10% of the entire internet. In 2002, the first internet attack as we now know it saw a DDoS attack target the 13 Domain Name System (DNS) root servers. The attack could have brought the internet down if allowed to continue and was then the most sophisticated and widescale cyber-attack ever launched. Recent cyber-attacks have advanced and can affect vast numbers of people. Single attacks now regularly steal the data of hundreds of millions of people.

Moreover, the crisis between Russia and Ukraine, which began in February 2022, involved not only physical battles that displaced thousands of people and killed many, but also cyberattacks. FortiGuard Labs determined that the new Viper malware was being used to attack Ukrainian targets and found that it was installed on at least several hundred machines in Ukraine. Several Ukrainian organizations have also been targeted by sophisticated attacks using the KillDisk and HermeticWiper malware chains, which appear to destroy data on devices. Additionally, a tool that controls devices remotely, the Remote Manipulation System (RMS), was discovered to have been distributed in Ukraine via fake “Escape Plan” emails. Ukraine has also suffered a wave of Distributed Denial of Service (DDoS) attacks. This included a targeted attack on the State Savings Bank, which affected banking services and cash withdrawals from ATMs, as well as the disruption of Ministry of Defense and Armed Forces networks. (4)

3. RESULTS

China has fully recognized the significance of cyber security and has elevated its potision to one of national security. Aside from establishing its leading group for cyber security, the National People’s Congress (NPC) has conducted a second review of its Cyber Security Law in June 2016. Organisations in China across a whole range of industries including e-commerce, insurance, banking, IT, education, tourism and automotive are in possession of an increasing amount of personal information and transaction data. These organisations are now the main targets of cyber attacks with sensitive data often being leaked due to organisational system vulnerabilities. Which includes;

- inadequate data transmission, access control, and security management safeguards; sensitive data (in transit, storage, or use) can be purposefully or unintentionally disclosed;
- insufficient capabilities in security services and incident response, making it difficult for organisations to effectively react and respond to possible security risks. (5)

As a large industrialised economy, the United States is heavily reliant on the Internet and hence vulnerable to cyber assaults. At the same time, because to relatively sophisticated technology and a big military budget, the United States possesses significant capabilities in both defence and power projection. Cyber warfare is posing an increasing danger to physical systems and infrastructures linked to the internet. Malicious hacking from local or foreign adversaries continues to be a continual concern to the United States. The United States has developed strong cyber capabilities in response to these expanding concerns.

 doi:10.20944/preprints202208.0235.v1

The US Department of Defense views the use of computers and the Internet to conduct cyberwarfare as a danger to national security as well as a platform for assault. (6)(7)

"Cybersecurity is constantly improving, but the complexity of our digital society may overwhelm our efforts to keep pace," said John Hultquist, head of Mandiant Threat Intelligence.

Niloofar Razi Howe, cyber and technology investor: “We are more vulnerable due to the rapid pace at which we are embracing technology, engaging in technological transformation and adding devices without prioritizing security.

A particularly rich target has been a large new line of Internet-connected devices, such as refrigerators, thermostats and cameras. These devices, commonly referred to as "Internet of Things" or "IoT", are notorious for relying on weak or default passwords and for being difficult to update with software patches, making them an easy choice for hackers. “A lot of these technologies have reduced your cybersecurity spending, creating ever-increasing responsibilities for everyone,” said Sascha Meinrath, founding director of X-Lab, a Penn State think tank that focuses on the intersection of technology and public policy. (8)

Small businesses are the least concerned about cyberattacks: Only 33% of owners with 0-4 employees fear being hacked within a year, compared to 61% of owners with 0-4 small businesses with 50 or more employees. Few small business owners consider cyber threats their top business risk and less than half consider them a concern, but most express confidence in their ability to respond to a cyber attack. Similar to previous quarters, about six in 10 small business owners are very or somewhat confident that they could quickly resolve a cyberattack on their business if needed.

Small business owners in the finance and insurance industries are among the most confident in their ability to respond quickly to a cyberattack more than seven out of 10 say they can fend off an attack. Among those in the arts, entertainment and recreation industry, that number drops to 50%. This is important because any cyberattack, even if quickly resolved, can have a lasting negative impact on a business. Consumers prefer not to fall victim to a cybersecurity attack and are wary of businesses that have been compromised in the past. In the SurveyMonkey survey, 55% of people in the United States say they are less likely to continue doing business with brands that have suffered a cyberattack. For small businesses to be truly prepared, they need to take more concrete steps. Less than half say they have installed anti-virus or malware software, strengthened their passwords or backed up files to an external hard drive to protect their business from potential cyberattacks. Only a third each have enabled automatic software updates or enabled multi-factor authentication. Only a quarter have installed a virtual private network (VPN).

These are basic actions that most companies in corporate America would consider to be table stakes, but they are admittedly much more costly to implement in a small business environment. Small businesses that fail to take the cyber threat seriously risk losing customers, or much more, if a real threat emerges. (9)

Healthcare ransomware attacks have become a pressing issue in healthcare. There are some ways to prevent these attacks from affecting organization:

1. Employees must be trained to identify phishing attacks and report them to IT. Employees should be taught what a ‘typical’ phishing email looks like, with the goal being to help them recognize the many different ways in which a cybercriminal may try to trick them into clicking on an attachment or link. The most common types of phishing attacks include; Forged email addresses that appear similar but aren’t actually from your organization’s domain name, also messages requesting personal information that employees shouldn’t give out without first verifying its validity through another method (e.g., an authenticated phone call or text message).

2. To prevent ransomware attacks, you need to understand their vulnerabilities. A vulnerability assessment can help you identify and close gaps in your cybersecurity. Regular vulnerability assessments are important for healthcare organizations because they allow you to learn about potential weaknesses in your security from a third party or your own team. If you have an internal team conducting the assessment, ensure that the team has

 doi:10.20944/preprints202208.0235.v1

experience conducting such assessments and understands how best practices should be followed when discussing results with senior management. However, for most healthcare facilities, it is often necessary to hire a specialist service such as Truenorth ITG and others to diagnose and address industry-specific threats. Here are some considerations when performing a vulnerability assessment: Choose an external third party specialized in this type of work so that its conclusions are objective and impartial; Ask them if they will provide recommendations or list possible problems; many vendors charge more than others but offer less value because they don't offer actionable steps on how to fix identified issues. (10)

In 1989, the American Robert Morris created what is considered the first computer virus in history. This self-propagating worm was so aggressive that it managed to shut down most of the Internet. Other attacks have gained notoriety since then, but the Morris worm remains a landmark incident in what was the first large-scale cybercrime. While the internet was still in its infancy at the time, the attack was far less devastating than it could have been. But it set the tone for the kinds of security issues the internet has faced ever since.

According to the FBI, “cybercrime is becoming more common, more dangerous and more sophisticated”. It is an industry with profits of hundreds of millions of US dollars that employs thousands of hackers around the world. Cybersecurity is struggling to keep up. But there are some things you can do to protect yourself as an individual or business.

While it's understandable that you want your passwords to be easy to remember, you're putting your computer and online data at risk. A hacker reported that the most common way to break into secure websites was by exploiting weak passwords. To strengthen your password set, make sure your password is at least eight characters long and includes a mix of numbers, letters, and symbols. And try not to use words that relate to you. Instead, try using a memory device. For example, if Samantha was born in New York in 1994, her password might be SwbiNY1994$ (the symbol at the end to represent her American roots)

Alternatively, there are quite a few exceptional password generators and password storage programs available. LastPass is a great example of this. It’s also advisable that you have multiple passwords across your online presence, rather than a single password that offers access to everything. (11)

CONCLUSION

The protection of daily internet users is equally integrated with the other resources involved for the expansion of new services both at civilian or government levels. The different training sessions must also be executed at the government level for the awareness of cybercrimes among the individuals. Ransomware attacks are becoming more common, and healthcare organizations should be prepared to respond. It’s important to consider that we’re still early in the digital age. As more citizens are affected or learn of cyber-enabled crimes, public opinion will inevitably shift. Both government and technology companies will have to rethink their positions.

Fundamentally, liberal-democratic societies cede reasonable amounts of individual civil liberties in exchange for societal security. There isn’t a static balance. It’s highly dependent on the current state of affairs. Without meaningful and regular dialogue between all vested interests, the current chasm will only grow. These parties will have to work with lawmakers around the world to reshape relevant legislation, in a principle-based fashion.

Large technological corporations must also play a leading role. They, too, must take precautions to guarantee that their platforms do not facilitate crime and despair. Balancing their desired technical output with the rule of law and the protection of vulnerable communities must be central to their development strategy. Collectively, this may be accomplished if all stakeholders agree on the principle that, at its finest, technological progress enhances people's lives while protecting society's essential values (12)

FUNDING

None

CONFLICT OF INTEREST

The authors declare no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENTS

Declared None

References List

1. Sharon, S.; Alex S., Gillis.; Casey, C. Security operation and management, **2021.**
Available at: https://www.techtarget.com/searchsecurity/definition/cybersecurity
2. Available at: https://www.toppr.com/guides/essays/cyber-security-essay/
3. Mas, P.; Cloustan..; Serge, O., Paquette.; Seb, Gracia.; Maria, J., Erquiaga. cybercrime connections of a public forum population. Journal of Cybersecurity: **2022**, 8(1).
Available at: https://academic.oup.com/cybersecurity/article/8/1/tyac010/6644916?searchresult=1
4. Available at: https://www.fortinet.com/resources/cyberglossary/recent-cyber-attacks
5. KPMG: Cyber Security in China. **2016**.
Available at: https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2016/08/cyber-security-in-china.pdf
6. Grenoble, Ryan (16 August 2018). "Trump Reverses Obama-Era Rules on Cyberattacks". *HuffPost*. Retrieved 1 October 2018.
7. "How the US military is beating hackers at their own game". *Business Insider*. Retrieved 1 October 2018.
8. Joe, Marks.; Aar, Schaffer. The Washington Post, Democracy dies in Darkness: The Cyber security 202. **June 06, 2022.**
Available at: https://www.washingtonpost.com/politics/2022/06/06/us-isnt-getting-ahead-cyber-threat-experts-say/
9. L., Wronski; J., Cohen. CNBC: Small Business Playbook, America's small businesses aren't ready for a cyberattack. **2022.**
Available at: https://www.cnbc.com/2022/05/21/americas-small-businesses-arent-ready-for-a-cyberattack.html#:~:text=Some%20of%20the%20highest%20profile,into%20the%20Democratic%20National%20Committee.
10. E., Chachak. The Cyber Research Data Bank.
Available at: https://www.cyberdb.co/6-tips-to-prevent-healthcare-ransomware-attacks/
11. Available at: https://www.clickatell.com/articles/information-security/5-easy-ways-fight-cybercrime/
12. N., Desai. Centre of International Governance Innovation: Security, Surveillance and Privacy. **2019.**
Available at: https://www.cigionline.org/articles/tackling-cyber-enabled-crime-will-require-public-private-leadership/?utm_source=google_ads&utm_medium=grant&gclid=EAIaIQobChMI7ObRvNuq-QIVw5JmAh2-Ng9kEAAYBCAAEgIESfD_BwE