iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IX **Month of publication:** September 2021

DOI: https://doi.org/10.22214/ijraset.2021.38022

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IX Sep 2021- Available at www.ijraset.com

Overview of Cyber Security

Praveen Pandey
Department of Elec. & Comm. Engg

Abstract: Cyber security are techniques generally set forth in published materials that attempt to safeguard the cyber environment of a user or organization. It manages the set of techniques used to save the integrity of networks, programs and data from unauthorized access. It refers to the body of technologies, processes, and it may also be referred to as information technology security. The field is of growing importance due to increasing reliance on computer systems, including smart phones, televisions and the various tiny devices that constitute the Internet of Things.
Keywords: IT security, Internet of things (IOT)

I. INTRODUCTION

The internet has made the world smaller in many ways but it has also opened us up to influences that have never before been so varied and so challenging. As fast as security grew, the hacking world grew faster. There are two ways of looking at the issue of cyber security. One is that the companies that provide cloud computing do that and only that so these companies will be extremely well secured with the latest in cutting edge encryption technology.

II. WHAT IS CYBER SECURITY?

Its being protected by internet-connected systems, including hardware, software and data, from cyber attacks. In a computing context, security comprises cyber security and physical security both are used by enterprises to safe against unauthorized access to data centre and other computerized systems. The security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security.

III. WHY DO WE NEED CYBER SECURITY?

The range of operations of cyber security involves protecting information and systems from major cyber threats. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people. Some of the common threats are:

1) *Cyber Terrorism:* It is the innovative use of information technology by terrorist groups to further their political agenda. It took the form of attacks on networks, computer systems and telecommunication infrastructures.
2) *Cyber Warfare:* It involves nation-states using information technology to go through something another nation's networks to cause damage. In the U.S. and many other people live in a society, cyber warfare has been acknowledged as the fifth domain of warfare. Cyber warfare attacks are primarily executed by hackers who are well-trained in use of benefit the quality of details computer networks, and operate under the favorable and support of nation-states. Rather than closing a target's key networks, a cyber-warfare attack may forced to put into a situation into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce.
3) *Cyber Spionage:* It is the practice of using information technology to obtain secret information without permission from its owners or holders. It is the most often used to gain strategic, economic, military advantage, and is conducted using cracking techniques and malware.

A. Who are Cyber Criminals?

It involves such activities as child printed sexual organs or activity; credit card fraud; cyber stalking; defaming another online; gaining unauthorized access to computer systems; ignoring copyright, software licensing and trademark safe to protect; overriding encryption to make illegal copies; software piracy and stealing another's identity to perform criminal acts. Cybercriminals are those who conduct such acts. They can be categorized into three groups that reflect their motivation.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IX Sep 2021- Available at www.ijraset.com



1) Type 1: Cybercriminals – hungry for recognition
a) Hobby hackers;
b) IT professionals (social engineering is one of the biggest threat);
c) Politically motivated hackers;
d) Terrorist organizations.

2) Type 2: Cybercriminals – not interested in recognition:
a) Psychological prevents;
b) Financially motivated hackers (corporate espionage);
c) State – sponsored hacking (national espionage, sabotage);
d) Organized criminals.

3) Type 3: Cybercriminals – the insiders:
a) former employees seeking revenge;
b) Competing companies using employees to gain economic advantage through damage and/or theft.

B. How to Maintain Effective Cyber Security

Historically, organizations and governments have taken a reactive, "point product" approach to combating cyber threats, produce something together individual security technologies – one on top of another to safe their networks and the valuable data within them. Not only is this method expensive and complex, but news of damaging cyber breaches continues to dominate headlines, rendering this method ineffective. In fact, given the area of group of people of data breaches, the topic of cyber security has launched to the top of the priority list for boards of directors, which they seeked as far as less risky way. Instead, organizations can consider a natively integrated, automated Next-Generation Security Platform that is specifically designed to provide consistent, prevention-based protection – on the endpoint, in the data center, on the network, in public and private clouds, and across Saabs environments. By focusing on prevention, organizations can prevent cyber threats from impacting the network in the first place, and less overall cyber security risk to a manageable degree.

©IJRASET: All Rights are Reserved

C. What Cyber Security Can Prevent

The use of cyber security can help prevent cyber-attacks, data breaches and identity theft and can aid in risk management. When an organization has a strong sense of network security and an effective incident response plan, it is better able to prevent and serious of these attacks. For example, end user protection defends information and guards against loss or theft while also scanning computers for malicious code.

1) *Types of Cyber Security Threats:* The use of keeping up with new technologies, security trends and threat intelligence is a challenging their task. However, it should be in order to protect information and other assets from cyber threats, which take many forms.

a) Ransom ware is a type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them.

b) Malware is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.



c) Social engineering is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.

d) Phishing is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information.

D. What Does a Security Analyst do?

An information security analysts protects to safe the company"s systems and networks by planning and carrying out measures of security. They create disruptive solutions to prevent critical information from being stolen, damaged, or compromised. Their primary responsibility is to keep a business or organizations data, clients, employees, and any virtual stored information safe from cyber attacks or hacking of any sort.

E. What are the Consequences of cyber attack ?

Cyber-attacks will cause more damage financially and reputational even to the most withstand organisation. The organisation which suffers cyber-attack, have to face the losing assets, business reputation and potentially the organisation have to face regulatory fines and taking legal action and the costs of remediation. A survey taken by UK government about cyber security in 2017, found that the average cost for a large business is £19,600 and for a small to medium-sized business is £1,570.

IV. HACKING TOOLS

There are various tools are the modes of attack. And the malware are used for the totality of these tools. Examples are viruses and worms. Computer programs that reproduce the functional copies of themselves with varying effects ranging from emphasize and inconvenience to compromise of the confidentiality or integrity of information, and Trojan horses, destructive programs that pretence as benign applications but set up a back door so that the hacker can return later and enter the system. Often system intrusion is the main goal of system intrusion is more advanced attacks. If the intruder gains full system control, or „root" access, he has unrestricted access to the inner workings of the system .Due to the characteristics of digitally stored information the person with criminal intent will delay, disrupt, corrupt, exploit, destroy, steal, and modify information. The value of the information or the importance of the application will be depended, which the information are required and that such actions will have different effect with varying degrees of gravity.

©IJRASET: All Rights are Reserved

V. THE LEVEL OF CYBER RISK

There are some additional reasons for that threat is overrated. First, as combating cyber-threats has become a highly politicized issue, official statements about the level of threat must also be seen in the context of different bureaucratic entities that compete against each other for resources and influence. This is usually done by stating an urgent need for action (which they should take) and describing the overall threat as big and rising. Second, psychological research has shown that risk perception is highly dependent on intuition and emotions, as well as the perceptions of experts (Gregory and Mendelsohn 1993). Cyber-risks, especially in their more extreme form, fit the risk profile of so-called „dread risks", which appear uncontrollable, catastrophic, fatal, and unknown. There is an inclination to be afraid of low probability risks, which translates into pressure for serving an action with all sorts of willingness to bear high costs of uncertain benefit. Only the system attacks sufficiently destructive or disruptive need the attention of the traditional national security apparatus. Attacks that interrupt the services or that cost mainly a nuisance to the computer.

VI. REDUCING CYBER – IN - SECURITY

The three different debates have been taken over the many concepts and counter measures have been produced with their focus. The computer network which owns a entities have a common practice to take a responsible for protecting it. However, there are some assets considered so crucial in the private sector to the functioning of society and governments have to take additional measures to ensure the level of protection. These efforts are usually included under the label of critical (information). Information assurance is guide for the infrastructure protection and to the management of risk, which is essentially about accepting that one is (or remains) insecure: the level of risk can never be reduced to zero. This means that minor and probably also major cyber-incidents are bound to happen because they simply cannot be avoided even with perfect risk management.

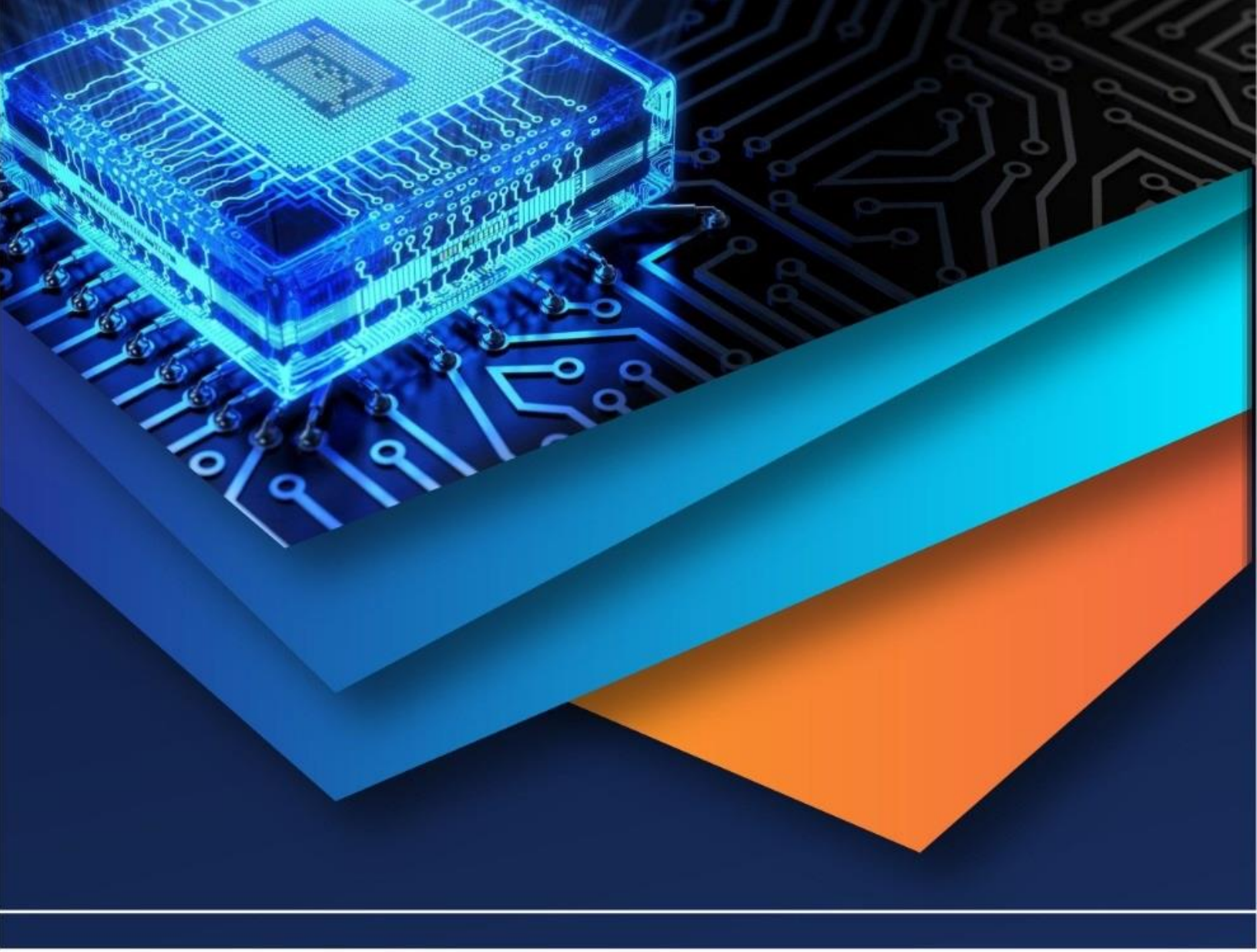
VII. CONCLUSION

Depending on their (potential) severity, however, disruptive incidents in the future will continue to fuel the military discourse, and with it fears of strategic cyber-war. Certainly, thinking about (and planning for) worst-case scenarios is a legitimate task of the national security apparatus. However, for the favour of more plausible and more likely problems they should not to get more attention Therefore, there is no way to study the „actual" level of cyber-risk in any sound way because it only exists in and through the representations of various actors in the political domain.

REFERENCES

[1] Daniel, Schatz,; Julie, Wall, (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215. Archived from the original on 28 December 2017.
[2] Rouse, Margaret. "Social engineering definition". Tech Target. Archived from the original on 5 January 2018. Retrieved 6 September 2015.
[3] Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.
[4] "Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian
[5] Stevens, Tim. "Global Cyber security: New Directions in Theory and Methods". Politics and Governance. 6 (2). doi:10.17645 /pag.v6i2.1569.
[6] "Computer Security and Mobile Security Challenges". researchgate.net. Archived from the original on 12 October 2016. Retrieved 4 August 2016.
[7] "Distributed Denial of Service Attack". csa.gov.sg. Archived from the original on 6 August 2016. Retrieved 12 November 2014.
[8] Wireless mouse leave billions at risk of computer hack: cyber security firm Archived 3 April 2016 at the Way back Machine.
[9] "Multi-Vector Attacks Demand Multi-Vector Protection". MSSP Alert. July 24, 2018.
[10] Millman, Renee (December 15, 2017). "New polymorphic malware evades three quarters of AV scanners". SC Magazine UK.
[11] Turner, Rik (May 22, 2018). "Thinking about cyber attacks in generations can help focus enterprise security plans". Informa PLC. Ovum.
[12] "Identifying Phishing Attempts". Case. Archived from the original on 13 September 2015.
[13] Arcos Sergio. "Social Engineering" (PDF). Archived (PDF) from the original on 3 December 2013.
[14] Scannell, Kara (24 February 2016). "CEO email scam costs companies $2bn". Financial Times (25 Feb 2016). Archived from the original on 23 June 2016. Retrieved 7 May 2016.
[15] "Bucks leak tax info of players, employees as result of email scam". Associated Press. 20 May 2016. Archived from the original on 20 May 2016. Retrieved 20 May 2016.
[16] "What is Spoofing? – Definition from Techopedia". Archived from the original on 30 June 2016. [17]. "spoofing". Oxford Reference. Retrieved 8 October 2017.
[17] Marcel, Sébastien; Nixon, Mark; Li, Stan, eds. (2014). Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks (PDF). London: Springer. doi:10.1007/978-1-4471-6524-8. ISBN 978-1-4471-6524-8. ISSN 2191-6594. LCCN 2014942635.Retrieved 8 October 2017 – via Penn State University Libraries.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)