SYNDICATE RESEARCH SYNOPSIS

OF

PRIVACY : A CRITICAL EVALUTION OF INFORMATION SECURITY IN THE DIGITAL AGE

SYNDICATE GROUP - 'O'

FACULTY OF DEFENCE AND STRATEGIC STUDIES

GENERAL SIR JOHN KOTELAWALA DEFENCE UNIVERSITY

SYNDICATE GROUP 'O'

1. **TOPIC** - THE PRIVACY: A CRITICAL EVALUATION OF INFORMATION SECURITY IN DIGITAL AGE.
2. **MILITARY DS** - Lt. SLMDLS SAMARATHUNGA.
3. **ACADEMIC DS** - MS. IA WIJETHUNGA.
4. **SYNDICATE LEADER** - 5563 C/L/CPL MN JAYASEKARA
5. **SYNDICATE MEMBERS** -

a.	5516	O/Cdt	NAL Pramuditha
b.	5574	O/Cdt	BT Nelaka
c.	5577	L/O/Cdt	AGRPL Gunathilaka
d.	5700	O/Cdt	PDT Perera
e.	5703	O/Cdt	DMAC Pivithuru
f.	5704	O/Cdt	MTD Makonal
g.	5705	O/Cdt	EMNM Ekanayake
h.	5706	O/Cdt	KA Jayasanka
i.	5764	O/Cdt	AWDKB Udangamuwa
j.	5775	O/Cdt	UHW Thamonuda
k.	5776	F/O/Cdt	AAM Ahamed
l.	5788	F/O/Cdt	CS Barro

DS COMMENTS

DECLARATION

1. We declare that this dissertation does not incorporate without acknowledgment any material previously submitted for a degree or a diploma in any university and to the best of our knowledge and belief, this does not contain any material previously published or written by any other person or ourselves except where due reference is made in the text .We also here by give consent for this report, if accepted to be made available for photographing and for interlibrary leans and for the title and summary to be made available to outside organizations.

_ _

Name Signature

5516	O/Cdt	NAL Pramuditha
5574	O/Cdt	BT Nelaka
5577	L/O/Cdt	AGRPL Gunathilaka
5700	O/Cdt	PDT Perera
5703	O/Cdt	DMAC Pivithuru
5704	O/Cdt	MTD Makonal
5705	O/Cdt	EMNM Ekanayake
5706	O/Cdt	KA Jayasanka
5764	O/Cdt	AWDKB Udangamuwa
5775	O/Cdt	UHW Thamonuda
5776	F/O/Cdt	AAM Ahamed
5788	F/O/Cdt	CS Barro

SUPERVISED BY

Military DS:

LT SLMDLS SAMARATHUNGA

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Signature of Supervisor

Date:

Academic DS:

MS. IA WIJETHUNGA

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Signature of Supervisor

Date:

DEDICATION

2. We dedicate our research work to our batch mates. A special feeling of gratefulness to our parents, who encouraged us throughout. We are always thankful to all the Squadron Commanders and Troop Commanders who were behind us giving advice. We dedicate this work and give special thanks to Lt SLMDLS Samarathunga and Ms. IA Wijethunga for being there with us throughout the entire program.

ACKNOWLEDGEMENT

3. No one walks alone in the journey of life. We would like to express our deep gratitude to Colonel HMGE Herath RSP USP psc for his advice and assistance in keeping our progress on schedule. We would also like to thank Lt SLMDLS Samarathunga our research supervisor for his patience, guidance, enthusiastic encouragement, and useful criticisms provided on this research work. Our grateful thanks are also extended to Ms. IA Wijethunga who helped us to improve the English language of the research script and presentation. Finally, we wish to thank our parents and our family members for their support and encouragement throughout this study and syndicate presentation.

AIM

4. The aim of this project is to evaluate information security in the digital age.

OBJECTIVES

5. Understand the concept of digital age and its technologies.
6. Get an idea about privacy.
7. Discuss about information security and present value of it.
8. Identify the most common network security threats.

CONTENT

ABSTRACT

9. This syndicate is mainly directed towards about privacy under the information security in digital age.

10. First, we need to get oriented on this concept of privacy under the information security in digital age also we talk about the historical background of the information security, cyber security and digital age

11. In this presentation we have tried to enlighten what is privacy in digital age, information security, cyber security and difference between information security and cyber security. And also further giving evidence and statistics about what happen invading privacy in digital age.

12. We have brought forward the concept impact of the information security under privacy talking about information security. In this concept we try to give the necessary knowledge about the privacy and its security.

CHAPTER 01

INTRODUCTION

1.1 What is Digital Age?

13. This is otherwise referred to as the Information Age, a historic period in the 21st century characterized by the rapid shift from traditional industry that the Industrial Revolution brought through industrialization, to an economy based on information technology. This new age relies on information and communication technology for social, economic and political activities.

1.2 What does privacy mean?

14.
Well, this depends on who you're asking.Broadly speaking, the right to be let alone or
free from interference or intrusion is privacy.Privacy of information is the right to hav e some control over how to collect and use your personal information.These days, ask most individuals what they think about privacy and you are likely to have a conversati on about massive data breaches, wearable technology, social networking, targeted adv ertising mistakes, not to mention the revelations of Snowden.In addition, different cul tures have widely conflicting opinions about what the rights of an individual are when it comes to privacy and how it should be regulated.

15.With technological advancement, as more data is collected and shared, informatio n privacy is getting more complicated by the minute. As the program gets more com plex (indeed, invasive), so do the uses of information. And that leaves companies facing an extremely complicated risk hierarchy to ensure he security of personal information.As a result, privacy has rapidly emerged in the global information economy as perhaps the most critical issue of consumer security, if not citizens' protection.

1.3 Privacy vs security…isn't it the same thing?

16. Actually not. But they are cousins who kiss. Data privacy focuses on the use and handling of personal data, such as placing in place measures to ensure that personal information from users is collected, shared and used in acceptable ways. Safety focuses more on shielding information from malicious threats and profitably leveraging stolen data. Although security is essential for data protection, it is not enough to fix privacy.

1.4 Where the IAPP fits in?

17. Organizations that do not have the right to privacy are at risk of federal prosecution, class action litigation, financial hardship, lost integrity and loss of consumer loyalty. Privacy is now a must for business to be completed.

The IAPP is where professionals can get education, training and tools, whether from multinationals or start-ups, to ensure that privacy is handled right in their organizations. We're not campaigning, we're not lobbying, we're not describing best practices. What we do is provide a platform for privacy debate and education. And while our name includes "privacy professionals," we're here as a resource for anyone who wants to understand privacy and get the expertise and information they need to get ahead, from HR to IT, from auditing to transparency, from compliance to the cloud.

1.5 Definition - What does Information Privacy mean?

18. Privacy of information is the confidentiality of personal information and typically applies to personal data stored on computer systems. Personal information obtained, such as medical records, financial data, criminal records, political records, business related information or website data, is subject to the need to protect information privacy. The protection of information is often referred to as data privacy. Privacy of information is considered an essential part of exchanging information. Personal information vulnerabilities have increased with the advancement of the digital age.

19. Privacy of information can be implemented in various forms, including encryption, authentication and masking of data-each effort to ensure that only those with approved access have access to information. These protections are aimed at preventing the mining of data and the unauthorized use of personal information that

is illegal in many parts of the world. Information privacy relates to different data types, including:

20. Privacy of the Internet (online privacy): All personal data exchanged over the Internet is subject to privacy problems. Many websites publish a privacy policy that describes the planned usage of collected data collected online and/or offline by the website.

21. Financial privacy: As it can easily be used to commit online and/or offline fraud, financial information is particularly sensitive.

22. Medical privacy: All medical records are subject to specific laws addressing the rights of consumer access. By law, for people who process and store medical records, protection and authentication systems are also required.

1.6 Information security definition

23. Information protection, also abbreviated to infosec, is a collection of procedures designed to protect information from unauthorized access or changes, both when it is stored and when it is transmitted from one device or physical location to another. You may see it referred to as data protection occasionally. As intelligence has become one of the most significant assets of the 21st century, attempts to keep information secure have become increasingly critical as a result.

1.7 Information security vs. cybersecurity

24. Since information technology has become the accepted corporate buzzphrase that essentially means "computers and related stuff," you can also see the interchangeable use of information protection and cybersecurity. Cybersecurity is, generally speaking, the wider practice of protecting IT assets from attack, and under the cybersecurity umbrella, information security is a particular discipline. Infosec's sister activities are network protection and application security, focusing on networks and application code, respectively.

25. There's some overlap here, clearly. Data transmitted over an unreliable network or exploited by a leaky application may not be protected. There is also plenty of information that needs to be secured and that is not stored electronically. Thus, the remit of infosec pro is inherently broad.

1.8 Information security principles

26. The so-called CIA triad most frequently sums up the basic components of information security: confidentiality, honesty and availability.

1.9 What is Confidentiality?

27. The confidentiality provisions are intended to protect against unwanted knowledge disclosure. The aim of the concept of confidentiality is to ensure that private information stays private and that only people who need that information can display or access it in order to complete their job duties can do so..

1.10 What is Integrity?

28. Integrity requires protection against unauthorized data changes (e.g. adding, removing, or changing). The honesty concept is structured to ensure that information can be trusted to be reliable and that it has not been improperly changed.

1.11 What is Availability?

29. Availability preserves the reliability of support systems and guarantees that data is completely usable at the time (or time requirements) that its users need. The aim of availability is to ensure that data is available to be used when decisions need to be made.

30. In an ideal world, your data should always be kept confidential, in its correct state, and available; in practice, of course, you often need to make choices about which information security principles to emphasize, and that requires assessing your data. If you're storing sensitive medical information, for instance, you'll focus on confidentiality, whereas a financial institution might emphasize data integrity to ensure that nobody's bank account is credited or debited incorrectly.

1.12 Information security policy

31. A security policy takes the form of the means by which these concepts are applied to an entity. This is not a piece of hardware or software for security; rather, it is a manual that an organization draws up to decide what data needs to be secured and in what ways, based on its own unique needs and quirks. These policies direct the decisions of the company concerning the acquisition of cybersecurity resources, and also mandate the conduct and obligations of employees.

1.13 History of Information security

32. 1960s: Companies start securing their computers

at this interval, the greatest security issues were at the access points.

Anyone with adequate knowledge of how to operate a computer could break into a facility and start accessing sensitive data. In order to secure terminals, passwords and several layers of security protection have been applied to the computers.

33. 1970s: The first hacker attacks to begin

At this stage in the history of information security, network computing was in i ts infancy (the internet as we know it may not have existed until the end of th e 1980s). However, while there was no huge global network connecting every d evice that

wanted to be connected, large organizations, particularly governments, were st arting to link computers via telephone lines. Recognizing this, people began se arching for ways to penetrate the phone lines linked to the device.

so that they could steal data. These people became the first groups of hackers.

1980s: Governments are being aggressive in the fight against cybercrime

Hacking had already blossomed into an international crime problem by the 198 0s.Limited information security mechanisms have not been able to cope with th e continuous dam of clever methods used by hackers to break into computer sy stems. This became particularly relevant when a small group of teens from Mil waukee, known as the "414s," hacked into more than 60 military and corporate computer networks and stole more than $70 million from U.S. bank in response to this information security crisis, governments started to actively pursue hackers, including the 414s. At this point in time, the sentences were exceedingly light, ranging from stern warnings to probation.

1990s: Organized crime gets involved in hacking

After the global web was made available in 1989, people began placing their pe rsonal information online; organized crime groups saw it as a possible source o f income, and started stealing data from people and governments across the we b.Firewalls and antivirus programs helped guard against this, but the web was a largely unsecured and increasingly burgeoning network.

.

2000s: Cybercrime becomes treated like a crime

Although governments have been targeting cyber criminals for decades, most s entences have been light, often restricted to the confiscation of computer equip ment and the ban on computer usage for a certain period of time.

This changed in the 2000s, when policymakers began to understand the risks of hacking. Hackers have been jailed for years as punishment for cyber-crime activity. For eg, Jeanson James Ancheta, who used hacking to steal less t han a millionth of a percent of the "414s" stole, was sentenced to five years of jail time. By 2010, high-profile hackers were getting decades in prison for cybercrimes.

2010s: Information security becomes serious

While criminal investigations, firewalls and antivirus software had acted as a d eterrent to cyber criminals,they did not stop hackers who were professional and brazen enough to break into computer networks. At this point in the history of information technology, security experts have begun to understand that the onl y way to secure data is to make it completely unavailable to hackers. To this en d, data encryption, which scrambles data to make it unreadable to unauthorized users, has become more common. In many cases, encryption occurs at multiple levels, including on digital files, networks and during data transmissions. Organizations now also implement comprehensive information security policies that prevent their employees from making any mistakes that make data accessible to intruders.

1.14 The most common network security threats

1. Computer virus

They've been heard by many, and we all have our questions. For everyday Internet users, computer viruses are one of the most popular cybersecurity threats. Statistics say that about 33 percent of household computers are infected by some form of malware, more than half of which are viruses.

Software viruses are pieces of software designed to be transmitted from one system to another. They are often sent as email attachments or downloaded from specific websites with the intention of using systems on your network to infect your machine and other computers on your contact list. It is known that viruses send spam, disable your security settings, corrupt and steal your computer's data, including personal details such as passwords, and even delete anything from your hard drive.

2. Rogue security software

Scammers have discovered a new way of committing Internet fraud, taking advantage of the fear of computer viruses.

Rogue Protection Software is a malicious software that misleads users to assume that their device has a virus installed or that their security measures are not up-to - date. They then offer to install or update user protection settings. They will either ask you to download their software or pay for a tool to remove suspected viruses.

Both situations result in the actual malware being installed on your computer.

3. Trojan horse

Metaphorically, "Trojan horse" refers to tricking others into welcoming an intruder to a safely secured area. In programming, it has a somewhat similar meaning — a Trojan horse, or "Trojan," is a malicious bit of attacking code or software that tricks users into running it willingly, hidden behind a legitimate program.

They also spread by email; it may appear as an email from someone you know, and when you click on the email and its attachment included, you automatically downloaded the malware to your computer. Trojans also scatter when you click on a fake advertising.

While inside your computer, a Trojan horse will record your passwords by recording keystrokes, hijacking your camera, and stealing any confidential data that you might have on your computer.

4. Adware and spyware

By "adware" we consider any program designed to monitor your surfing habits and, based on that, show you advertisements and pop-ups. Adware gathers data with your consent — and is even a legitimate source of revenue for businesses that encourage consumers to try their software for free, but with ads shown when using the software. The adware clause is frequently concealed in similar User Agreement papers, but can be verified by carefully reading everything you approve when downloading the app. The existence of adware on your machine is visible only in such pop-ups, and occasionally it can slow down the speed of your computer's processor and internet connection.

If adware is downloaded without permission, it is considered to be malicious.

Spyware functions in the same way as adware, but is installed on your computer without your knowledge. It can contain keyloggers that record personal information, including e-mail addresses, passwords, and even credit card numbers, making it dangerous due to the high risk of identity theft.

5. Computer worm

Computer worms are pieces of malware that reproduce easily and spread from one computer to another. The worm spreads from the infected computer, sending it to all the computer contacts, and then immediately to the contacts of the other computers.

The worm spreads from the infected computer, sending it to all the computer contacts, and then immediately to the contacts of the other computers.

Interestingly, they're not always intended to inflict harm; there are worms that are only created to spread. Transmission of worms is most frequently achieved by leveraging the vulnerabilities of apps.

CHAPTER TWO

BACKGROUND

2.1 Why information security is important?

When anyone thinks of securing information, the first tip that they would come across is to create a password that is tough to crack (often so tough that the user forgets it!), but protecting information is beyond just protecting data under a password. More and more businesses are becoming victims of cybercrime.

According to McAfee, the damages associated with cybercrime now stand at over $400 billion, up from $250 billion 2 years ago, showing that there is a significant spike in more sophisticated hacking.

To combat the situation, organizations are investing in security protocols and digital frontiers. However, many still believe that information security is a burden.

2.2 Five main reasons why people invest in information security

As we all know information security also known as info sec is a process of formulating strategies, tools, and policies to detect, document, prevent, and combat threats targeted on digital and non-digital information devices. Information security in direct context is establishing well-defined security processes to protect information irrespective of its state of presence—transit, processed, or at rest. The five main reasons as follows

- Rising cost of breaches
- Increasingly sophisticated attackers
- Proliferation of IoT devices
- Funded hackers and wide availability of hacking tools
- Regulatory compliances

Rising cost of breaches

Cost of a breach = actual financial loss + cost of incident handling

Global average cost is $3.86 million, the United States is leading with $7.91 million

Increasingly sophisticated attackers

Sophisticated attacks, like DDoS, File less malware, etc., are on rise. DDoS attacks have increased by 110% in third quarter of 2018. File less attacks are 10 times likely to succeed than file-based attacks

Proliferation of IoT devices

IoT is an easy way for cybercriminals into the business. IoT devices are expected to grow to 20.4 billion by 2020 with $134 billion annual investment till 2022 on their security.

Funded hackers and wide availability of hacking tools

Intellectual property threats account for 25% of more than $600 billion cost of cybercrime to the world economy. The commercialization of cybercrime provides easy access to the resources that needed to launch severe attacks

Regulatory compliances

Not just breaches but the regulatory laws, like GDPR, also enforce information security measures. The violation of these compliances may cost heavily to the businesses

2.3 Introduction

Along with the tremendous progress in Internet technology in the last few decades, the sophistication of the exploits and thereby the threats to computer systems have also equally increased.

The exploitation is done by malicious hackers who find vulnerabilities or weaknesses, which are the pre-existing errors in the security settings in the computer systems.

The common types of vulnerabilities are errors in the design or configuration of network infrastructure, protocols, communication media, operating systems, web-based applications and services, databases, etc.

Threat is a potential risk that exploits a vulnerability to infringe security and cause probable damage/disruption to the information/service stored/offered in/by computer systems or through communication links.

A threat to a computer systems occurs when the confidentiality (preventing exposure to unauthorized parties), integrity (not modified without authorization), and availability (readily available on demand by authorized parties) of information on systems are affected.

Thus, a computer system threat in general can include anything deliberate, unintended, or caused by natural calamity that effects in data loss/manipulation or physical destruction of hardware.

Accordingly, the threats on computer system are classified as physical threats and nonphysical threats. Physical threats cause impairment to hardware or theft to system or hard disk that holds critical data.

Nonphysical threats target the data and the software on the computer systems by corrupting the data or by exploiting the errors in the software.

2.4 Motivation And Objectives Of Hackers

The purpose of a hacker is to break the security of computers and networks affecting the confidentiality, integrity, and availability of information/service on systems. Such activities of hackers are considered illegal as they invest their time and know how, to make personal gains and breach the security across networks.

Fun: Fun is the only motivation for the script kiddies and lot of nonserious hackers. For them, the breaking into a secure system is a challenging and adventurous enjoyable game to test their wits and skills.

Vulnerability testing: Vulnerability testing is done by administrators to locate vulnerabilities and hence develop protections. The same is also done by hackers to identify vulnerabilities in target systems and to find the exploits for those vulnerabilities. This is almost a pre-phase of an attack.

Theft: Theft or stealing of data is when hackers infiltrate on a database of credentials of individuals or organizations.

Espionage: Espionage is another type of theft where the hacker tries to get protected information instead of the direct financial gain. The information stolen can be either sold in black market or used by adversaries to gain strategic advantages.

Spamming: Spamming is not just about unsolicited emails. This spam can be due to certain particular malware that invade the web browser and devastate with unwanted ads.

Control: The hacker uses a Trojan or other means to take remote control over another system. Then the hacker can turn that compromised system into a bot or a zombie computer that they use to power spam or to deploy distributed denial of service attacks.

Disruption: Disruption of services or access to information, by taking over websites or social media accounts, is usually an act of competition, protest, or rivalry. This effect will slow down or shut down of the target's Internet activity.

2.5. Computer Threats

Spoofing: Spoofing is when someone hides their identity to evade detection for their wrong acts and pretends to be someone else in an attempt to gain trust and get sensitive system information.

The common spoofing done by changing the hardware or MAC address is called MAC cloning, changing the IP address or the unique identity on the network is called IP spoofing, and impersonating as someone else in their digital communication is called email spoofing.

Information-gathering attacks: Information gathering is the practice of attacker gaining priceless details about probable targets. This is not an attack but only a pre-phase of an attack and is totally passive as there is no explicit attack.

Systems including computers, servers, and network infrastructure, including communication links and inter networking devices, are sniffed, scanned, and probed for information like whether the target system is up and running, what all ports are open, details regarding the operating system and its version, etc. Some of the information-gathering attacks are sniffing, mapping, vulnerability scanning, phishing, etc.

Password attacks: The simplest way to achieve control of a system, or any user account, is through a password attack. If the personal and behavioral details of the victim are known, the attacker starts with guessing password. Frequently, the attacker uses some form of social engineering to trace and find the password. Dictionary attack is the next step in password attacks and is automated.

Malware: After gaining access to a system, the attacker takes the support of malware or malicious software that clandestinely acts against the interests of the computer user.

Virus: Computer viruses are the most communal threat to the computer users. Computer viruses are malicious software designed to blow out from one computer to another through file transfer, piggybacks on genuine programs and OS, or e-mails.

The email attachments or downloads from particular websites contaminate the computer and also other computers on its list of contacts by using the communication network. Viruses influence the system security by changing the settings, accessing confidential data,

Worms: Computer worms are fragments of malicious software that reproduce swiftly and blow out from one computer to another through its contacts, again

spreading to the contacts of these other computers and so on and reaching out to a large number of systems in no time.

Captivatingly, worms are prepared for spreading by exploiting software vulnerabilities. Worms display unwanted advertisements. It uses up tremendous CPU time and network bandwidth in this process thereby denying access to the systems or network of the victim, creating chaos and trust issues on a communication network.

Trojans: Trojans are programs that appear as perfectly genuine but, in reality, have a malicious part embedded in it. Trojans are spread usually through email attachment from the trustworthy contacts and also on clicking on fake advertisements.

The payload of Trojans is an executable file that will install a server program on the victim's system by opening a port and always listening to that port whereas the server is run on the attacker's system. Hence, whenever the attacker wants to login to the victim machine, they can do so by means of the backdoor entry making it hidden from the user.

Spyware and adware: Spyware and adware are software with a common property of collecting personal information of users without their knowledge. Adware is intended to track data of the user's surfing behaviors, and, based on that, pop-ups and advertisements are displayed.

The adware clause in the agreement during the installation process is often skipped with least seriousness. Spyware on the other hand gets installed on a computer and gathers information about the user's online activities without their knowledge. Spyware contains keyloggers that record everything typed on the keyboard, making it unsafe due to the high threat of identity mugging.

Scareware: Scareware is yet another malware that tricks victims by displaying fake alerts and forcing the victim to buy protective software that is fraudulent. The alerts or the pop-up messages sound like warning messages along with proper protective measures, which if followed creates security issues.

Rootkit: Rootkit is a pool of software tools that gets mounted in stealth along with some genuine software. Rootkit allows remote access and administrative control on a system. With these privileges, the rootkit performs malicious activities like disabling of antivirus, password sniffing, keylogging, etc.

Keylogger: Keylogger software has the ability to record keystrokes and also capture screenshots and save it to a log file in encrypted form. Keylogger software can record all the information that is typed on the keyboard including passwords, e-mail,

and instant messages. The log file created by the keylogger is saved and mailed to the attacker on a remote machine with the motive to extract password and banking details for financial fraud.

Ransomware: Ransomware is a malicious software that hampers admission to computer or files on the computer. The computers may be locked or files encrypted. Accordingly, the two common types of ransomware are lock screen ransomware and encryption ransomware.

The victim will be demanded ransom for the restriction to be removed, and this gets displayed on victim's system. There can also be notification stating that establishments have detected illicit activity on this computer and demands ransom as fine to avoid prosecution.

Rogue security software: Rogue security software is another malicious program that deceives users to believe that there is malware installed on their system or the security measures are outdated and hence of concern. They offer installing or updating users' security settings. Then it is an actual malware that gets installed on the computer.

Botnets: A collection of compromised systems or bots acts as a team of infected computers under the control of a bot master to remotely control and send synchronized attacks on a victim host. This army of bots, agents, and bot master constitute a botnet. Botnets are used for sending spams and also for distributed denial of service attacks.

Denial-of-service attacks: Denial-of-service (DoS) attacks as the name suggests deny users from accessing or using the service or system. This is mainly done by overwhelming the bandwidth, CPU, or memory wherein the access to the network of the victim machine or server offering the service gets denied.

DoS attacks thus interrupt the service of a computer or network systems, making it inaccessible or too inferior in performance.

Distributed DoS: In distributed DoS (DDoS) attacks, the victim is targeted from a large number of individual compromised systems simultaneously. The DDoS attacks are normally done with the help of botnets.

The barmaster is the attacker who indirectly attacks the victim machine using the army of bots or zombies. The DDoS attacks occur when a large number of compromised systems act synchronously and are being coordinated under the control of an attacker in order to totally exhaust its resources and force it to deny service to its genuine users.

IoT-based attacks: The last decade has seen exponential increase in the use of Internet of Things (IoT) that are smart devices used at home, organizations, and businesses.

The issue with these IoT is its weak security as these devices are often overlooked when it comes to applying security patches that create lead-ins for attackers to seize these devices to infiltrate the networks. An IoT-based attack is any cyberattack that leverages a victim's use of IoT to sneak malware onto a network.

Session hijacking: In session hijacking, the hacker takes control of a session going on between two hosts. Session hijacking usually takes place in applications that use TCP with a sequence number prediction. With that sequence number, the attacker sends a TCP packet.

Blended attacks: A blended attack is a software exploit that encompasses a mixture of exploit techniques to attack and propagate threats, for example, viruses, worms, and Trojan horses.

Website attacks: Website attacks are targeting browser components that are at risk of being unpatched even when the browser is patched. SQL injection attacks are intended to target any website or web application that uses an SQL database such as MySQL, Oracle, etc.

By taking advantage of the security flaws in the application's software. This attack is used to obtain and corrupt user's sensitive data.

Mobile phone and VOIP threats: Malware target mobile phones, VoIP systems, and the IP PBXs as these devices have plentiful published vulnerabilities. There are attack tools freely available on the Internet, and misusing these vulnerabilities makes these attacks too common and simple even for a script kiddie.

Wi-Fi Eavesdropping: Wi-Fi eavesdropping is an attack used by network attackers to grab sensitive information of a target system. It is the act of silently listening on an unencrypted Wi-Fi network.

WPA2 handshake vulnerabilities: The key reinstallation attack (KRACK) lets an attacker to decipher the network traffic on Wi-Fi routers. Every device connected to Wi-Fi, such as computers, smartphones, smart devices, and wearables, can be identified by the hacker.

Insider attacks: One of the prevalent all-time computer security threats faced by any organization is from its own employees. Insider attacks are initiated by disgruntled employees of an organization.

Insider usually has certain privileges to the data as well as rights on the systems and networks that they attack, giving them an advantage over external attackers. These attacks can be hard to prevent with firewalls, which are the first level of defense.

Supply chain attacks: A supply chain attack seeks to cause harm by targeting the least secured elements in the supply network.

Buffer overflows: Buffer overflows are used to exploit programming glitches that do not take care of the buffer size. If a buffer is jam-packed beyond its size, the data overflows into the contiguous memory. This flaw gets smartly used by hackers to change the execution of the program.

User to root attack: User to root attack is a case of privilege escalation where a user gains a higher privilege than that authorized. This is not a class of attack as such, and it is the process of any attack. Every attack will do activities the attacker is not privileged to do.

Man-in-the-middle attacks: Man-in-the-middle attacks allow the hacker to snoop on the communication between two systems, affecting the privacy. A common method of doing this is to place the attacker at a point and redirect all the communication through the route that includes that hacker so that eavesdropping is possible by the hacker.

Pharming: Pharming is a widespread online fraud that will automatically point to a nasty and illicit website by relaying the authentic URL. Even when the URL is correctly entered, the redirection happens to some forged website looking similar to the actual one.

This fake site prompts one to enter personal information that gets to someone with a wicked intent.

Spam: Spams are unsolicited bulk e-mail messages that annoy the user with unwanted and junk mails. It gives burden for communications service providers, organizations and individuals alike.

These emails can be commercial ones like an advertisement or noncommercial one like chain letters or anecdotes. Spam is considered an active vehicle for virus propagation, scams, fraud and is a threat to computer privacy.

2.6 Present Day Computer Security Threats and Trends

Predicting the computer security threats and trends is usually done to lend a hand to the security experts who take proactive measures to protect security.

Normally the predictions for any year depends on how it went in the previous years, and the changes expected are mainly in terms of the tactics and scale of the biggest and significant threats that were successful in implementation and also in evading detection.

The investment on security is justified in many organizations only after analyzing these predictions.

Artificial intelligence also gets applied on both sides of the barricade for protecting and attacking the computers. Artificial intelligence is being used for person identification, threat detection.

To aid security; however it is also being weaponized by hackers to develop increasingly complex malware and attack methods.

2.7 PRIVACY

2.7.1 What is data/information privacy?

Simply, Privacy of information is the confidentiality of personal information and typically applies to personal data stored on computer systems. Information privacy is considered an important aspect of information sharing.

With the advancement of the digital age, personal information vulnerabilities have increased.

Privacy of information can be implemented in various forms, including encryption, authentication and masking of data - each effort to ensure that only those with approved access have access to information. These protections are aimed at preventing the mining of data and the unauthorized use of personal information that is illegal in many parts of the world.

In other way round Privacy is an individual's right to be protected from uninvited monitoring. It is important to live in a democratic society to comfortably remain in one's room and openly share one's views behind closed doors.

2.7.2 Data Privacy vs. Data Security

- Data privacy – governing how data is collected, shared and used.
- Data security – protecting data from internal and external attackers.

Organizations typically assume that keeping confidential data protected from hackers implies that they comply with data privacy legislation automatically. It's not the case here.

Data protection and privacy of data are frequently interchangeably used, but there are distinct differences:

- Data Security protects data from compromise by external attackers and malicious insiders.
- Data Privacy governs how data is collected, shared and used.

2.7.3 Why Data Protection is Necessary for Sri Lanka?

Within Sri Lanka, there is also an increasing reliance on digital and cloud services, which collect data. There is increased usage of social media platforms and cloud communication platforms.

Virtual Private Networks (VPNs) can capture all data that are being transmitted or received by a device. The information captured can be very detailed and can easily be personally identifiable.

Sri Lanka is set to enable 5G transmission in 2020. A large amount of data sent over current mobile networks.

2.7.4 Data Privacy Laws and Acts

Sri Lanka does not have any consolidated and/or specific laws on privacy and data protection. While no clear legislation on the security of the right to privacy exists in Sri Lanka, such statutory requirements can be considered as applicable to the right to privacy in cyberspace.

2.7.5 Privacy Tips

Here some tips can you take to protect your privacy.

- Do business with credible companies.
- Do not use your primary email address in online submissions.
- Avoid submitting credit card information online.
- Devote one credit card to online purchases.
- Avoid using debit cards for online purchases.
- Take advantage of options to limit exposure of private information.

2.7.6 FAQs About Data Privacy?

Q: Is There a Global Data Privacy Law?

A: No. In either case, data privacy regulations are relatively recent, and no worldwide standard exists. That said many businesses look to the GDPR as a guide to how to properly store and handle data privacy, even if they are not doing business in the EU. Depending on your sector and venue, different laws can apply to your company, so make sure you check your responsibilities.

Q: Can We Protect Our Data in Other Countries?

A: Again, it can be exceedingly difficult to guarantee the security of your data if you send it overseas, because of the fragmentary existence of data privacy laws. As a concerned customer, the trick is just to share details with organizations who are transparent and truthful about their data privacy policies and who are not going to sell your data to the highest bidder.

Q: How Can Companies Ensure That They Have Data Privacy When Using Public Clouds?

Choose the correct cloud provider. In truth, most companies will not have the time or resources to employ a dedicated cloud security specialist. The best solution for most will, therefore, be to choose a cloud provider who also provides you with security features, and who can advise you about your legal responsibilities.

CHAPTER 03:

PRESENT VALUE OF INFORMATION SECURITY

Considering the importance of internal information and its participation in any organization's own equity, if it is harmed, this can leave huge drawbacks which trigger

several unpleasant consequences. These range from damage of organization's image, exposure of secrets to affecting plans.

A reasonably complete survey of the technology needed to protect information and other resources controlled by computer systems, this chapter discusses how such technology can be used to make systems secure. It explains the essential technical ideas, gives the major properties of relevant techniques currently known, and tells why they are important.

As **James Scott** just said: "We need cybersecurity renaissance in this country that promotes cyber hygiene and security centric corporate culture applied and continuously reinforced by peer pressure."

This discussion of the technology of computer security addresses two major concerns:

What do we mean by security?

How do we get security, and how do we know when we have it?

The first involves specification of security and the services that computer systems provide to support security. The second involves implementation of security, and in particular the means of establishing confidence that a system will actually provide the security the specifications promise. Each topic is discussed according to its importance for the overall goal of providing computer security, and not according to how much work has already been done on that topic.

1. Specification versus Implementation

The distinction between what a system does and how it does it, between specification and implementation, is basic to the design and analysis of computer systems. A specification for a system is the meeting point between the customer and the builder. It says what the system is supposed to do. This is important to the builder, who must ensure that what the system actually does matches what it is supposed to do. It is equally important to the customer, who must be confident that what the system is supposed to do matches what he wants. It is especially critical to know exactly and completely how a system is supposed to support requirements for security, because any mistake can be exploited by a malicious adversary.

Specifications can be written at many levels of detail and with many degrees of formality. Broad and informal specifications of security are called security policies, examples of which include the following: Confidentiality: Information shall be disclosed only to people authorized to receive it. Integrity: Data shall be modified only according to established procedures and at the direction of properly authorized people.

2. Specification: policies, models, and services

There are only a few highly developed security policies, and research is needed to develop additional policies, especially in the areas of integrity and availability. Each of the highly developed policies has a corresponding (formal) security model, which is a precise specification of how a computer system should behave as part of a larger system that implements a policy.

2.1. Policies

A security policy is an informal specification of the rules by which people are given access to a system to read and change information and to use resources. Policies naturally fall into a few major categories:

- ✓ Confidentiality: controlling who gets to read information;
- ✓ Integrity: assuring that information and programs are changed only in a specified and authorized manner; and
- ✓ Availability: assuring that authorized users have continued access to information and resources.

Two orthogonal categories can be added:

- ✓ Resource control: controlling who has access to computing, storage, or communication resources (exclusive of data); and
- ✓ Accountability: knowing who has had access to information or resources.

Security policies for computer systems generally reflect long-standing policies for the security of systems that do not involve computers. In the case of national security these are embodied in the information classification and personnel clearance system; for commercial computing they come from established accounting and management control practices.

2.2. Models

To engineer a computer system that can be used as part of a larger system that implements a security policy, and to decide unambiguously whether such a computer system meets its specification, an informal, broadly stated policy must be translated into a precise model. A model differs from a policy in two ways:

- ✓ It describes the desired behavior of a computer system's mechanisms, not that of the larger system that includes people.
- ✓ It is precisely stated in formal language that resolves the ambiguities of English and makes it possible, at least in principle, to give a mathematical proof that a system satisfies the model.

a) Flow Model

In this model (Denning, 1976) each piece of data in the system visible to a user or an application program is held in a container called an object. Each object has an associated security level.

b) Access Control Model

The access control model is based on the idea of stationing a guard in front of a valuable resource to control who has access to it. This model organizes the system into

Objects: entities that respond to operations by changing their state, providing information about their state, or both;

- ✓ Subjects: active objects that can perform operations on objects; and
- ✓ Operations: the way that subjects interact with objects.

The objects are the resources being protected; an object might be a document, a terminal, or a rocket. A set of rules specifies, for each object and each subject, what operations that subject is allowed to perform on that object. A reference monitor acts as the guard to ensure that the rules are followed.

2.3. Services

Basic security services are used to build systems satisfying the policies discussed above. Directly supporting the access control model, which in turn can be used to support nearly all the policies discussed, these services are as follows:

- ✓ Authentication: determining who is responsible for a given request or statement.
- ✓ Authorization: determining who is trusted for a given purpose, whether it is establishing a loan rate, reading a file, etc.
- ✓ Auditing: recording each operation that is invoked along with the identity of the subject and object, and later examining these records.

Given these services, it is easy to implement the access control model.

CHAPTER 4

Impacts of information security

Viruses, worms, and Trojan horses can corrupt data on a user's computer, infect other computers, weaken computer security, or provide back doors into protected networked computers. Although seemingly less dangerous than viruses that can corrupt digital content on a user's computer, spyware, adware, and other forms of security risk also represent a significant problem to small businesses, their users, and the company networks. All types of threat and security risk can seriously impair business operations, network use, and computer performance while performing many tasks unknown to the user of an infected computer. Some of the areas of impact are discussed here.

4.1 Information security impacts to economy

The economics of information security has recently become a thriving and fast-moving discipline. In a context of globalization and further economic integration in recent decades, the relationship between the economy and a security of information has become increasingly interlinked. Compared to world history, the economics of information security has recently become a thriving and fast-moving discipline. This high interlinked connection between economy and information security represent both opportunities and potential threats for a national security of a country. There are many active areas of security-economics research. But we highlight just four live problems as core problems in economy of information security. Each lies not just at the boundary between security and economics, but also at the boundary between economics and some other discipline respectively algorithmic mechanism design, network science, organizational theory and psychology.

Over the final little a long time, individuals have figured it out that security disappointment is caused at slightest as often by terrible motivations as by awful plan. Frameworks are especially inclined to disappointment when the individual guarding them isn't the individual who endures when they fall flat. Diversion theory and microeconomic hypothesis are getting to be fair as critical to the security build as the mathematics of cryptography. The developing utilize of security instruments for computerized rights management, extra control and other trade models that apply power over system owners, instead of to ensure them from exterior foes, presents numerous vital and policy issues. The framework proprietor gets to be the foe; her interface strife specifically with the security components on her machine. Here as well, financial investigation can sparkle light in some or maybe dim darkness.

Over the last few years, people have realized that security failure is caused by bad incentives at least as often as by bad design. Systems are particularly prone to failure when the person guarding them does not suffer the full cost of failure. Game theory and microeconomic theory are becoming important to the security engineer, just as the mathematics of cryptography did a quarter century ago. The growing use of security mechanisms for purposes such as digital rights management and accessory control which exert power over system owners rather than protecting them from outside enemies introduces many strategic issues.

Economic thinkers used to be keenly aware of the interaction between economics and security; wealthy nations could afford large armies and navies. But nowadays a web search on ‘economics’ and ‘security’ is a two different dimension that are highly inter-related. The main reason is that, after 1945, economists drifted apart from people working on strategic studies; nuclear weapons were thought to decouple national survival from economic power [1], and a secondary factor may have been that the USA confronted the USSR over security, but Japan and the EU over trade. It has been left to the information security world to re-establish the connection.

Because of the open and mixed economic systems that most of countries using as their economic system whole over the world, the trade economy of many counties is becoming an international trade economy. Base on this situation, any person can easily access the institutions that affect the economy of a country and due to leaks various important information from institutions, those institutions incur huge loss.

Massive Enterprise Data Leak Incidents in Recent Years (Data Source Is from the Dataset of World's Biggest Data Breaches[15])

Organization	Records	Breach Date	Type	Source	Industry	Estimated Cost
Anthem insurance	78 million	January 2015	Identify theft	Malicious outsider	Healthcare	$100 million
Yahoo	500 million	December 2014	Account access	State sponsored[†]	Business	$350 million
Home depot	109 million	September 2014	Financial access	Malicious outsider	Business	$28 million
JPMorgan chase	83 million	August 2014	Identify theft	Malicious outsider	Financial	$13 billion
Benesse	49 million	July 2014	Identify theft	Malicious insider	Education	$138 million
Korea credit bureau	104 million	January 2014	Identify theft	Malicious insider	Financial	$100 million
Target	110 million	November 2013	Financial access	Malicious outsider	Business	$252 million
Adobe System	152 Million	September 2013	Financial access	Malicious outsider	Business	$714 Million

[†] Announced by U.S. Department of Justice.[16]

These kinds of huge losses can completely destroy a country's economic expression. The economy of a country depends primarily on taxes levied on international institutions situated in that country. So when an international institute incurs huge loss, government will reduce the amount of tax. The government is directing more taxes to the public to prevent instability caused by non-payment of taxes by international trade bodies and to keep the country’s economy stable. This can be a cause to increase the living cost of people in the country. Therefore, it can in some way contribute to the breakdown of the country’s economy and the country’s economic instability. As a result of this process there is a tendency to take countries back to the colonialism period through wars once again.

Furthermore because of internal data leak incidents can lead a government to an economic instability situation. As an example for internal data leak incidents in October 2016, a staff from Australian Red Cross Blood Service accidentally placed the documents that contain more than550, 000 blood donors’ personal information on an unsecured, public-facing directory of their website. The sensitive information relates to donors from 2010 to 2016, and includes names, addresses, and dates of birth as well as sexual activity, drug use, and medical histories. Because of these incidents people will not attempt in donations. Data leaks such as the one in the example above could lead to an increase in the number of deaths due to declining medical donations, which

in turn could lead to a decrease in the number of people who provide government revenue, which in turn can lead to the collapse of the county's economy. And also with the leak of these internal data, the government will have to re-allocate money for medical activities or various other activities and their economy may collapse due to having to spend large sums of money among them.

According to reported data about the information security we can recognize some key factors which have effects on employees' behaviors in violating rules which are related to information leaks. First of all, myopic cognition and hyperopic cognition measured by the CFC scale have effects on the behaviors of violating organizational rules in almost all cases. Next, in many cases, individuals whose information security awareness is higher tend not to violate the rules. Third, the behavior of violating the rules is independent of the size of the organization, and is not related to the degree of workplace satisfaction and the evaluation toward the managers in some cases. Fourth, in an organization in which permanent employment is implemented, individuals tend to violate the rules. It is not easy to control psychological factors such as an individual's attitude toward risk. Conversely, the factors regarded as organizational attributes, such as the degree of workplace satisfaction or the employment system utilized may be controlled by designing the appropriate organizational environment. Consequently, we consider that it may be effective to improve information security awareness by information security education and training.

The data security world has been directed from the starting, in spite of the fact that initially government concerns had nothing to do with competition arrangement. The primary driver – in long time when data security generally implied cryptography, and the US and allies had a mechanical advantage over the rest of the world – was a straightforward non-proliferation concern. Governments utilized send out licenses and controlled inquire about financing to deny wider get to to cryptography for as long as conceivable. This exertion was to a great extent surrendered in 2000. The moment driver was the trouble that indeed the US government had over many years in securing frameworks for its claim utilize, once data security came to encompass software security as well. Hence, amid the 80s and 90s, it was arrangement to advance research in security whereas preventing inquire about in cryptography, for case by redirecting researchers into hypothesis and absent from connected points.

So as a conclusion we can say that secure of information is much more important to protect an economic stability of an country in this digitalized era than other past eras because all the whole economy is depend on the information security due to its high improved interlink. Over the last few years, a research program on the economics of security has built many cross-disciplinary links and has produced many useful (and indeed delightful) insights from unexpected places. Many perverse things, long known to security practitioners but just dismissed as 'bad weather', turn out to be quite explicable in terms of the incentives facing individuals and organizations, and in terms

of different kinds of market failure. As for the future, the work of the hundred or so researchers active in this field has started to spill over into at least four new domains.

The first is the technical question of how we can design better systems by making protocols strategy-proof so that the incentives for strategic or malicious behavior are removed a priori. The second is the economics of security generally, where there is convergence with economists studying topics such as crime and warfare. The causes of insurgency, and tools for understanding and dealing with insurgent networks, are an obvious attractor. The third is the economics of dependability. Large system failures cost industry billions, and the problems seem even more intractable in the public-sector.

We need a better understanding of what sort of institutions can be evolve and manage large complex interconnected systems. Finally, the border between economics and psychology seems particularly fruitful, both as a source of practical ideas for designing more usable secure systems, and as a source of deeper insights into foundational issues.

Over the past few a long time, a investigate program on the financial matters of security has built numerous cross disciplinary joins and has delivered numerous useful (and in fact delightful) bits of knowledge from unexpected places. Numerous unreasonable angles of information security that had long been known to professionals but were expelled as “bad weather” have turned out to be very intelligible in terms of the incentives confronting people and organizations, and in terms of diverse sorts of advertise failure. As for end of, the the work of the hundred or so researchers dynamic in this field has begun to spill over into two modern spaces. The primary is the economics of security for the most part, where there is convergence with financial analysts examining topics such as wrongdoing and fighting. The causes of guerilla, and apparatuses for understanding and dealing with guerillas systems, are an obvious attractor.

4.2 Information security impacts to physical security

While some might consider information security and physical security to be distinct disciplines, they are, in fact, highly connected. Obviously, one cannot ensure the availability of data systems, for example, if criminals can easily steal the equipment on which they reside. Likewise, information security failures can lead to serious consequences in the physical world.

Here are five areas of emerging technology in which information security can significantly impact physical risks, and which people concerned with risk management should learn about:

4.21 The Internet of Things(IoT)

The Internet of Things (or IoT) that is, the collection of devices that are connected to the Internet, but which are not computers in the classic sense of the word is rapidly expanding. While the typical consumer may experience the emergence of such technology in the form of smart household appliances. For example, a refrigerator that allows its owner to check its contents while shopping via an Internet-connected camera inside the device, or a television that contains all sorts of apps that allow viewers to check the weather, play games, or watch movies from subscription sources without the need for a cable box .The reality is that commercial and industrial uses dominate IoT, and will account for the vast majority of IoT devices for the foreseeable future.

Various smart devices on factory floors, self-repairing equipment, equipment that reports on production status, and numerous other newer technologies will make many non-smart devices obsolete in just a few years. Firms that don't embrace newer technologies will quickly grow uncompetitive and be relegated to history books.

Of course, all of IoT creates risk. Household devices can potentially be turned off or "played around with" by hackers. But, industrial IoT poses even greater risks. Terrorists, criminals, or even competitors could potentially hack into such systems in order to cause failures . Many of which may endanger human lives; it is not hard to picture how industrial equipment set to intentionally malfunction could directly kill or injure people or create dangerous situations such as fires or chemical spills that may result in human deaths.

4.22 Social media

Social media has quickly become one of the most powerful mechanisms for human communication. Yet, this new medium also creates serious security concerns. It is not a secret that cyberbullying on social media has led to teenagers committing suicide, nor that information overshared on social media has led to all sorts of physical crimes. People who have shared their vacation plans or posted photos of themselves away with their entire families, for example, have come home from vacation to find their homes robbed. Parents who post information about their children so as to let strangers calculate the children's schedules and whereabouts may expose their children to unnecessary risks. Likewise, employees oversharing has allowed criminals to craft highly effective spear phishing emails used to trick employees into taking actions that undermine security systems; this may lead to both digital penetration (data breaches and hacking) and physical penetration (robberies).

In fact, social engineering type attacks that often begin with criminals doing reconnaissance by scanning social media for overshared information is believed by many experts to be the number one way of commencing an attack in today's world of numerous security systems.

4.23 Security and Safety Systems

Today, many offices and factories are secured with physical access control systems that utilize smart cards for identification. By holding a card near a reader authorized individuals can enter a building or specific sections within a building. Many of these systems, however, are connected to the Internet raising possibilities that hackers could potentially allow unauthorized parties to gain access into a building, or into a sensitive region within a facility. Obviously, such a risk means that corporate espionage is a concern but so is robbery and sabotage.

Furthermore, many safety systems are also now "smart" and "connected;" it is obviously of tremendous benefit if a fire suppression system can, for example, notify administrators if it detects some sort of pressure problem in a particular section of its plumbing. At the same time, however, connecting safety systems to the Internet creates risks. Consider, for example, if a hacker were to breach a connected fire alarm system or fire suppression system and disable it, or cause it to go off unnecessarily at periods of peak production? Or what would happen if someone triggered it repeatedly to the point that people began to ignore it? What if a criminal sent false signals to a centralized monitoring and control system or to someone monitoring the system that impersonated a safety system and reported that everything is fine when it is not? The impact in any of the afore mentioned scenarios could be devastating.

4.24 Hackable Medical Systems

As smart devices increasingly permeate the healthcare field, information technologies have created numerous risks to human life. According to a report issued last month, studies performed by researchers found that hackers were able to successfully breach patient monitoring systems, check-in kiosks, and drug dispensers, using a variety of hacking techniques. Had such attacks been conducted by nefarious parties intent on inflicting harm rather than by researchers, there is little doubt that the lives of patients could have been put at risk.

Sadly, the findings of the recent report were not unexpected. Earlier this year, a researcher managed to hack into hospital systems in Russia via an improperly configured Wi Fi network. Last year, researchers found that many hospitals have poor passwords protecting their X-Ray and CT scanners and associated data. It's not hard to imagine the risks to human life: What if someone swapped the results of two patients' tests, or modified electronic health care records?

Besides the obvious liabilities involved in putting human lives and health at risk, there is also the possibility of direct financial damage to hospitals and healthcare facilities: What if a hacker remotely controlling expensive and highly needed medical equipment abused it and caused it to break?

The physical risk from medical equipment is not limited to situations involving a technology breach; the impersonation of medical devices could lead to catastrophic consequences as well. Imagine, for a moment, that someone impersonated the transmissions from a smart pacemaker that regularly transmits patient and device status information to doctors and sends distress signals when the patient is actually fine. Could that result in unnecessary procedures and associated risks? Could it lead to doctors ignoring distress signals when they are actually real? Similar risks apply for any other medical equipment that transmits patient information across the Internet; if it is not properly secured there could be serious consequences even without anyone actually breaching a medical system.

4.25 Smart Vehicles

It doesn't take much imagination to realize the danger that poor cybersecurity in smart cars could create. And, that risk is not theory anymore. Over the past few years, experts have discovered significant vulnerabilities that almost certainly would have led to deaths had they been discovered first by malicious parties rather than by whitehat hackers. Researchers were able to remotely breach a Jeep Cherokee via its cellular-connected entertainment system, attack the vehicle's computer system, and gain control of the car's brakes, engine, and transmission. Fiat Chrysler had to issue a recall and update the software on over a million vehicles after hackers demonstrated that they could take remote control of various cars from across the Internet. Last week, Nissan was forced to disable an app that allowed owners of its electric Leaf car to control their cars' heating and cooling from their smartphones, after a researcher demonstrated that he could use the app to control the systems in cars not belonging to him.

The risks are obvious. Ironically, much of the equipment used to make vehicles today is itself "smart," so any system used to ensure that vulnerabilities don't enter a car is itself subject to risk bringing us back to the risks mentioned above about industrial IoT systems.

As technology evolves new risks will emerge. And in today's technology-reliant world, that means significant risks to both individuals and businesses. To successfully manage those risks, managers must understand the role that cyber issues play with regard to the physical world.

4.3 Information security impacts to political

The purpose of this paper is to investigate a significant and increasing role of cybersecurity in world politics. Cybersecurity threats are one of the main national security, public safety, and economic challenges every nation faces in XXI century. Cyberspace is a defining feature of modern life. Individuals and communities worldwide connect, socialize, and organize themselves in and through cyberspace. The existence of numerous cyber security issues on various spheres of life naturally increase political interest in resolving them. The need for cybersecurity is growing ranging from particular cases to national and international — becoming the main problem of diplomacy and world politics

As the Internet experienced its rapid expansion in the 1990s, hackers began engaging in cyber "pranks" while low-level criminals began exploring the potential for cybercrime. Once it was shown that "crime pays" in the cyber domain, organized crime began muscling its way onto the scene, in some cases apparently with the blessing — and even support — of the governments on whose territory they were operating

ICT today form the basis of a rapidly developing global information society. Global network the Internet covers about 3.6 billion people The United States, being the leaders in the field of ICT, among the first to encounter the negative consequences of the information revolution. To date, the US experience in the field of information security is an advanced, which leads to the relevance and importance of the study.

Today, cyber security is increasingly discussed at the level of international politics and, both as a stimulus and a consequence, integrated into the dynamics of (great) power competition and cooperation. Three developments in cyber conflict stand out, signifying how digital technologies are used in political contexts and how the link to state actors is made: First, attention is shifting from theoretical "doomsday" cyber-attack scenarios towards the reality of persistent (low-level) cyber operations in different types of conflict settings. Second, attention has partially shifted to targeted cyber-attacks. Third, and as a corollary of growing unease about the destabilizing role of cyber operations, state and non-state actors are more actively searching for ways to control the risk of escalation and conflict through different means. At the same time, they are redoubling their efforts to ascertain their respective roles and responsibilities at the domestic and bureaucratic level.

As a example we can get in 2016 The U.S. Presidential campaign was affected by a cyber attack Hillary Clinton's private email server has already brought cybersecurity into the U.S. Presidential race. In 2016, a cyberattack will strike the campaign, causing a major data breach that will expose donors' personal identities, credit card numbers and previously private political preferences. Imagine being a donor with an assumption of anonymity. Or a candidate whose "ground game" depends on big data analytics about voter demographics and factors affecting turnout – data that turns from an asset to a liability if it isn't protected. The breach will affect the campaign not only as a setback for the unfortunate candidate or party affected, but by bringing the issue of cybersecurity prominently into the campaign as a major issue that is closely related to geopolitical threats such as the spread of terrorism. Campaign data is a gold mine for hackers (donor lists, strategies, demographics, sentiment, opposition research), and an event like this will serve as another wake-up call to the U.S. government that cybersecurity needs to be a continual, central focus and investment at the highest levels. The candidate who demonstrates knowledge and command of cybersecurity threats and government readiness will win the election

METHODOLOGY

27. Following methods and approaches will be followed and included in the presentation. The primary data that are requires to conduct the research was collected but distributing a Google form among young people. The research team was able to collect 50 responses from them.

28. A google form was used to distribute the questionnaire among these targeted internet users. It allows to collect information easily and efficiently. The questionnaire was prepared of ten questions with MCQs, short answer questions.

29. The secondary data was collected by referring different websites and articles relative to cyber security and privacy. We could gather valuable information.

30. We found solutions and suggestions according to the information gathered from the responses received regarding the knowledge of the society about cyber security in concern of privacy.

31. The data are represented in both qualitative and quantitative aspects in the relevant areas for better understanding of mentioned information. After studying the above references, a presentation will be conducted which will include relevant photographs, videos, audio, clip art etc.…

32. A verbal description about each slide will be presented and a script will be provided before the presentation.

CONCLUSION

33. We have examined the impacts of the privacy under the information security in digital age hosting through economic, social, political, environmental and security perspective. We can see all those impacts will make a big issue in the society. There are so many impacts under this topic because person's privacy contains all that person's life and the identity. As we can see invading privacy became an issue in this era. In order to protect this identity and the privacy people take some security measures in this presentation. We have talked about those security measures and how information security will help to protect those privacy. As we have seen information security concept is a mass concept that spread out through many directions. Privacy is an important part of it .This presentation include the all the topics that people need to know about in privacy; the critical evolution of information security in digital age.

34. It is advised that the all internet users, specifically when using their personal devices, needs to take necessary measurements in order to ensure the protection of their valuable data and gain some sort of knowledge about this digital era to defend themselves.

REFERENCES

1. Medium. 2020. *Medium*. [online] Available at: <https://medium.com/@harish_6956/the-importance-of-information-security-for-your-business-9a0fe0bb1e34.> [Accessed 28 November 2020].

2. Read "Computers at Risk: Safe Computing in the Information Age" at NAP.edu. (n.d.). [Online] *www.nap.edu*. Available at: https://www.nap.edu/read/1581/chapter/5#85.

3. Anderson, R. and Moore, T., 2006. The Economics of Information Security. Science, 314(5799), pp.610-613.

4. Cheng, L., Liu, F. and Yao, D., 2017. Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5), p.e1211.

5. World Economic Forum. 2020. Why Information Security Is Not Just A Technical Problem. [online] Available at: <https://www.weforum.org/agenda/2015/03/why-information-security-is-not-just-a-technical-problem/> [Accessed 7 November 2020].

6. D, C. (2019). *The Importance Of Information Security For Your Business*. [online] Medium. Available at: https://medium.com/@harish_6956/the-importance-of-information-security-for-your-business-9a0fe0bb1e34.

7. Read "Computers at Risk: Safe Computing in the Information Age" at NAP.edu. (n.d.).[online] *www.nap.edu*. Available at: https://www.nap.edu/read/1581/chapter/5#85.

TIME PLAN

	November				December	
Week / Activities	1	2	3	4	1	2
Preparation of Synopsis						
Information gathering						
Information analysis						
Conclusion and recommendation						
Discussion & preparation of Final Script						
Elaboration of Presentation						
Rehearsal						
Topic Presentation						

GRAPH 1 - Activities having same color can be done in parallel.