CINEC CAMPUS
Beyond A Graduate

BSc (Hons) in Software Engineering

Course Code: GS3207
Cyber Crimes
Ethics & Professionalism

Cyber Crimes

Objectives

Introduction to Cyber offense.

Types of Attacks.

Identification of Cyber stalkings

Laws and regulation in Cyber crime

Learning Outcomes

Define cyber offense and cyberstalking

Identify different types of attacks.

Learn how to protect from cyber attacks

Study laws and regulation in cyber crimes

Cyber Offenses and Cyber Stalking

Cyber offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Attacks

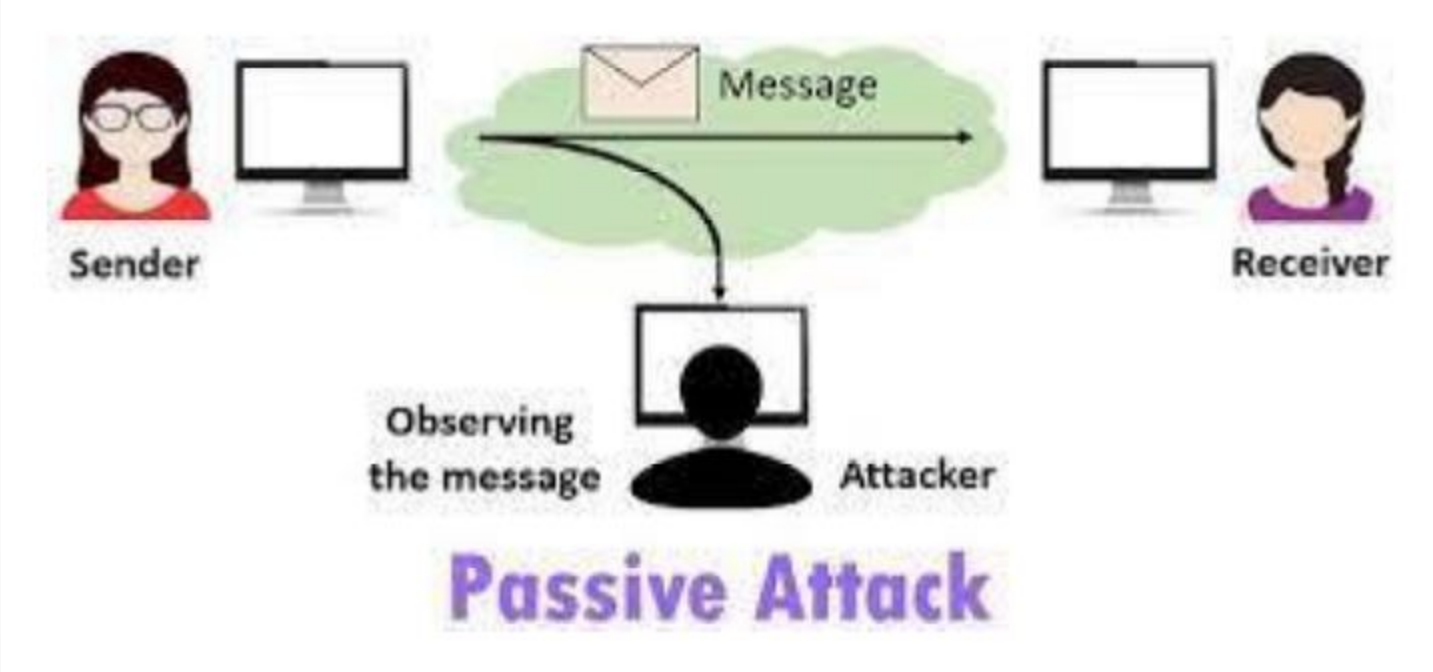
Hacker gaining and maintaining full control of the system access.

It follows scanning and enumeration and consists of the following steps:

1. **Password Bypass**: The attacker may use a brute force attack or other methods to bypass the system's password security.
2. **Exploitation**: Once the password is bypassed, the attacker exploits vulnerabilities in the system.
3. **Execution of Malicious Actions**: Malicious commands or applications are executed to gain control.
4. **File Concealment**: If necessary, the attacker hides files to cover their tracks.
5. **Covering Tracks**: To avoid detection, the attacker erases logs and any evidence of their actions, ensuring there is no trace leading back to them as a malicious third party.

Passive Attacks

- In Passive attack, an attacker observes the messages, copies them and may use them for malicious purposes.



Types of Passive Attacks

1) Release of Message (Eavesdropping)

2) Traffic Analysis

3) Scrutiny and Scanning for Gathered Information

1) Release of Message (Eavesdropping)

- It is a theft of information as it is transmitted over a network by a computer, smart phone, or another connected device.
- The attack takes advantage of unsecured network communications to access data as it is being sent or received by its user.
- Ex: hearing a telephone conversation

  the attacker can monitor the content of the transmitted data such as email messages

2. Traffic analysis

- Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.
- The attacker could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of the communication that was taking place.

Example

Suppose an attacker monitors the flow of data packets between a user's device and a banking website. Even though the content is encrypted, the attacker can analyze the packet sizes and timing, potentially inferring the user's behavior, login times, or transaction frequencies. This information might be used for fraudulent activities or identity theft.

3. Scrutinizing and Scanning the Gathered Information

Gathering Information: The initial phase of an attack involves collecting data on the target, such as IP addresses, network structure, and potential vulnerabilities.

Scrutinizing Information: The next step is to scrutinize the collected data to identify weak points, system configurations, and potential entry paths.

Scanning for Vulnerabilities: Hackers use various scanning techniques like port scanning to detect open ports or services that might be exploited.

Example

An attacker collects data on a company's network structure and then scans it to find open ports or unpatched software that could be exploited for unauthorized access. This stage helps pinpoint potential entry points into the target system.

Social Engineering

Social Engineering

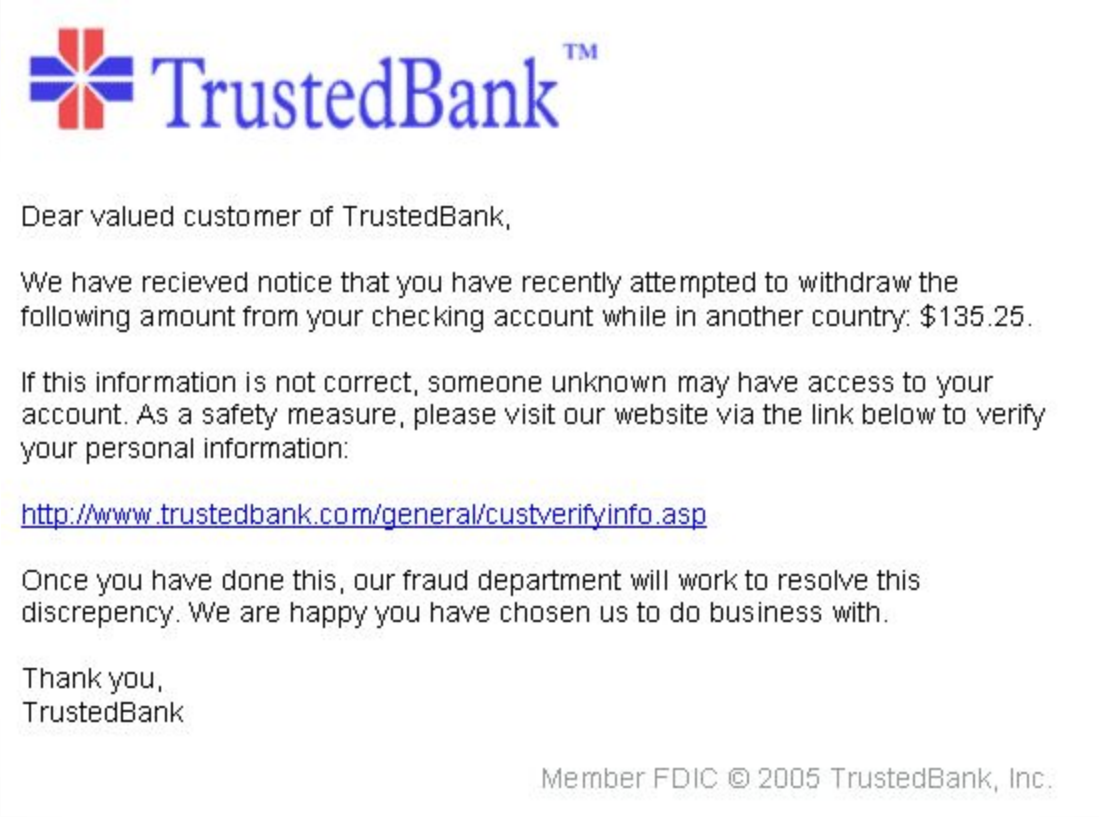
- Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.
- Social engineers are clever and use manipulative tactics to trick their victims into disclosing private or sensitive information.
- Social engineering is a term that encompasses a broad spectrum of malicious activity.

https://en.wikipedia.org/wiki/Social_engineering_(security)

Phishing

- Phishing is a form of social engineering and scam where attackers deceive people into revealing sensitive information or installing malware such as ransomware.
- Phishing target or targets are contacted by email, telephone or text message by someone posing as a genuine (legal) organization to ensnare(a trap) individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
- The information is then used to access important accounts and can result in identity theft and financial loss.
- Phishers frequently use emotions like fear, curiosity, urgency, and greed to force recipients to open attachments or click on links.
- Phishing attacks are designed to appear to come from legitimate (legal) companies and individuals.

Example of Phishing



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

The sender is attempting to trick the recipient

Types of Phishing

- Email phishing
- Spear phishing
- Whaling
- Social media phishing
- Clone phishing
- Voice phishing
- SMS phishing

https://en.wikipedia.org/wiki/Phishing

DoS and DDoS Attack

A denial-of-service (DoS) attack floods a server with traffic, making a website or resource unavailable.

A distributed denial-of-service (DDoS) attack is a DoS attack that uses multiple computers or machines to flood a targeted resource

DoS and DDoS Attack

What types of resources are targeted by such DoS attacks?

DoS and DDoS Attack

What types of resources are targeted by such DoS attacks?

- Websites
- Online Services
- Networks
- DNS Servers
- Email Services
- E-commerce Platforms
- Financial Services
- Gaming Servers
- Government Websites
- Cloud Services

DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.
In Dos attack single system targets the victims system.	In DDos multiple system attacks the victims system..
Victim PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple location.
Dos attack is slower as compared to ddos.	DDos attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and

DOS	DDOS
	attacking from multiple locations.
In DOS Attack only single device is used with DOS Attack tools.	In DDos attack Bots are used to attack at the same time.
DOS Attcaks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks

Cyber Stalking

Cyberstalking is when someone uses electronic communication, social media, and other technology to commit crimes.

Definition from wikipedia:

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization.[

It may include false accusations, defamation, slander and libel.

It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, doxing, or blackmail.

Real Example from cyber stalking

o Placing orders for delivery in someone else's name.

o Gathering personal information on the victim.

o Spreading false rumors.

o Encouraging others to join in the harassment.

o Threatening harm through email.

o Creating fear and paranoia(terror / distrust) for someone else.

o Post rude, offensive, or suggestive comments online.

o Follow the target online by joining the same groups and forums.

o Send threatening, controlling, or lewd messages or emails to the target.

o Use technology to threaten or blackmail the target.

Cyber Stalking

To guard against cyberstalking include the following:

o update all software to prevent information leaks;

o mask your Internet Protocol address with a virtual private network;

o strengthen privacy settings on social media;

o strengthen all devices with strong passwords or, better, use multifactor authentication;

o avoid using public Wi-Fi networks;

o send private information via private messages, not by posting on public forums;

o safeguard mobile devices by using password protection and never leave devices unattended;

o disable geo location settings on devices;

o install antivirus software on devices to detect malicious software

o always log out of all accounts at the end of a session; and

o beware of installing apps that ask to access your personal information.

What to do in case you are being cyberstalked

1. Block the person
2. Report to the platform involved
3. Call the Police

Top Mobile Device Information Security Risks

1. Unsafe apps.
2. Unsafe operating systems.
3. Unsafe devices.
4. Unsafe connections.
5. Lost devices
6. Uncontrollable users
7. Lack of monitoring

Cybercrime and legal landscape around the world

- Cybercrime is a crime done with the misuse of information technology for unauthorized or illegal access, electronic fraud; like deletion, alteration, interception, concealment of data, forgery etc.
- Cybercrime is an international crime as it has been affected by the worldwide revolution in information and communication
- Among 154 countries (79 per cent) have enacted cybercrime legislation, the pattern varies by region: Europe has the highest adoption rate (93 per cent) and Asia and the Pacific the lowest (55 per cent).
-

Cybercrime and legal landscape around the world

- List of Top 3 Countries with the highest rate of Cybercrime

Cybercrime and legal landscape around the world

List of Top 3 Countries with the highest rate of Cybercrime

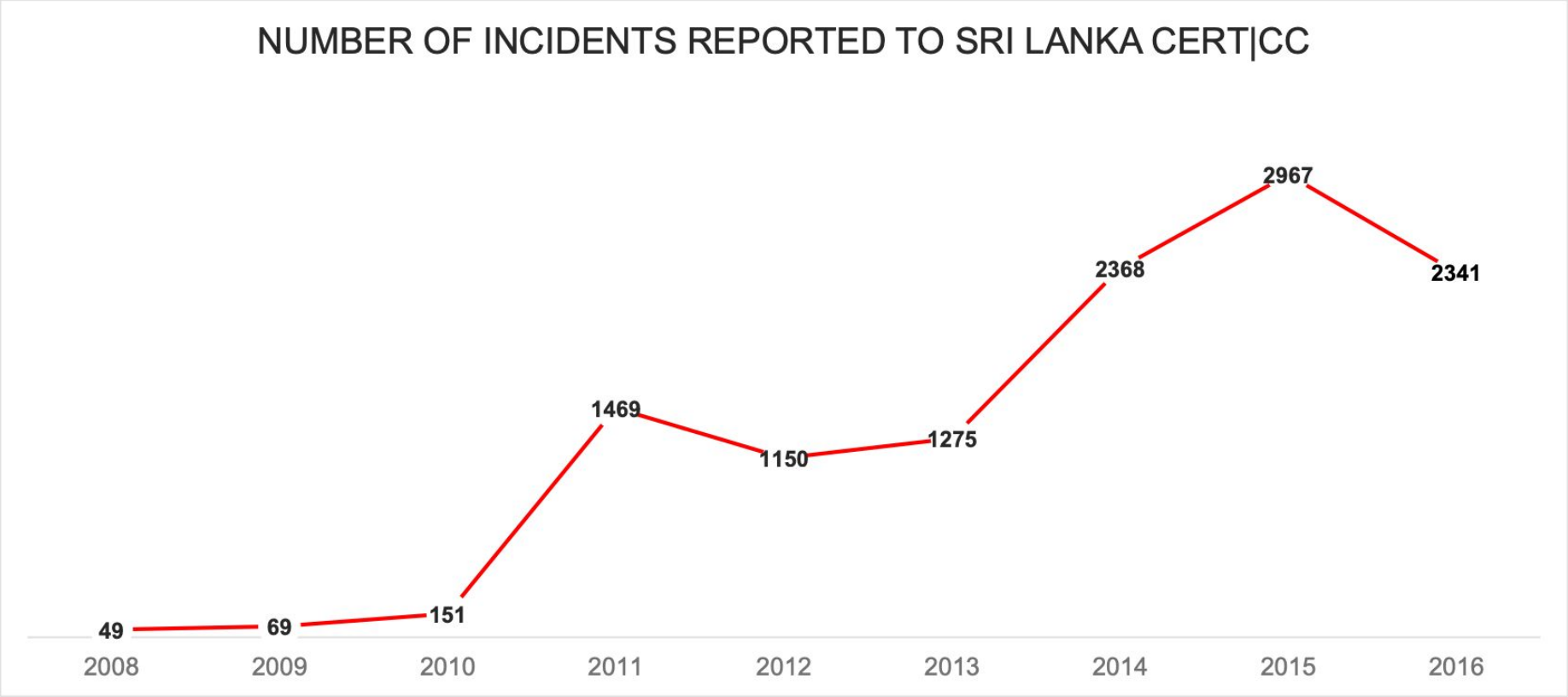
- Russia: Russia has been cited in various reports as a source of significant cybercriminal activity, including hacking, malware development, and cyberattacks on other nations.
- China: China has also been linked to various cybercrimes, including state-sponsored cyber espionage and hacking activities, as well as a significant number of cyberattacks.
- United States: While the United States has a highly developed cybersecurity sector, it is also a hub for some cybercriminal activity, including various types of online fraud, identity theft, and hacking.

Need for cyber law in Sri Lanka

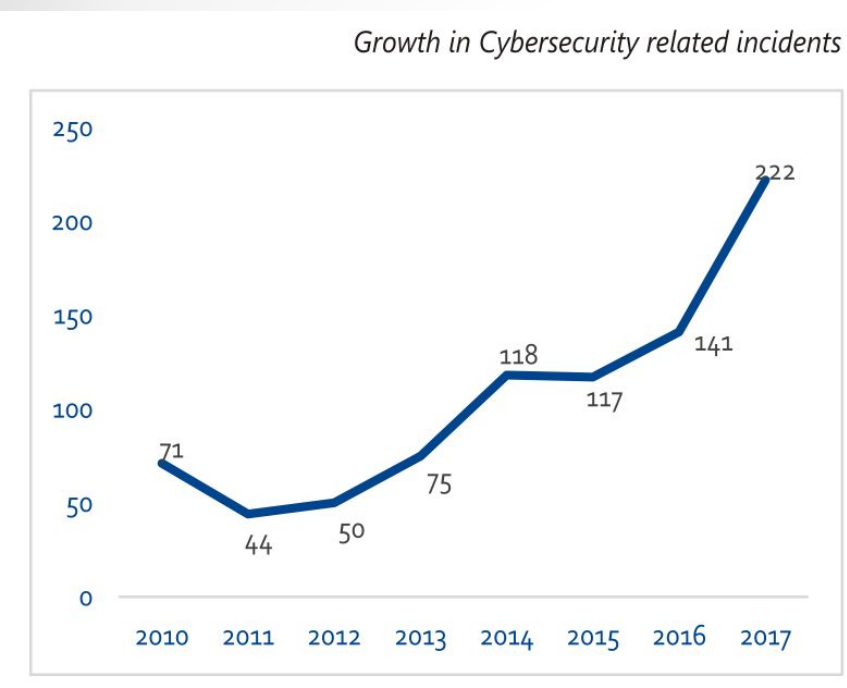
- The law is enacted to save people and organizations from cybercrime and other internet-related crime.

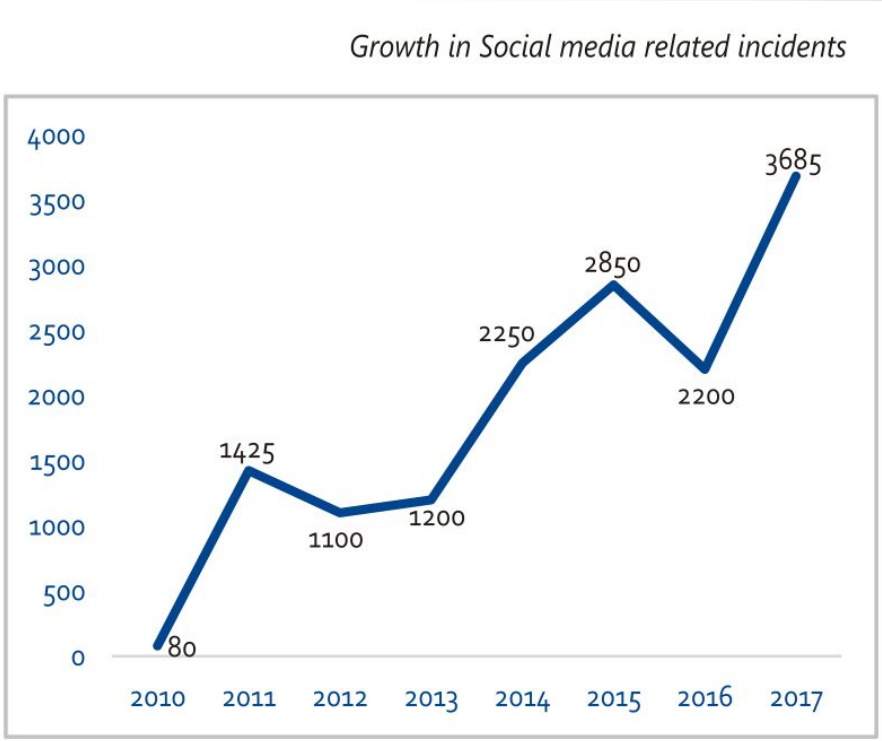
Cyber Security in Sri Lanka

Cyber Security in Sri Lanka



Information and Cyber security strategy in Sri Lanka





Cyber Crimes Division at CID

- To prosecute cyber security incidents
- Digital forensics lab facility
- Training has been provided by CERT

Computer Crimes Act

- Computer Crimes Act No.24 of 2007
  - ➢ Brought into operation on 15th July 2008
  - ➢ Scope of applicability is very broad
  - ➢ Covers broad range of offences

High Level IS Policy

- Based on ISO 27001
- 17 domains covering most of the areas in IS
- Used by Government Organizations

Cyber Security in Sri Lanka

Cabinet Approved National Policies & Strategies on Cyber Security:

National Information and Cyber Security Strategy of Sri Lanka (2019-2023)

Information and Cybersecurity policy for government organization

Contact details of CERT

Contact

Hotline : 101

+94 11 269 1692

Room 4-112, BMICH, Bauddhaloka Mawatha, Colombo 07, Sri Lanka.

General inquiry: cert@cert.gov.lk

Security incidents: incidents@cert.gov.lk

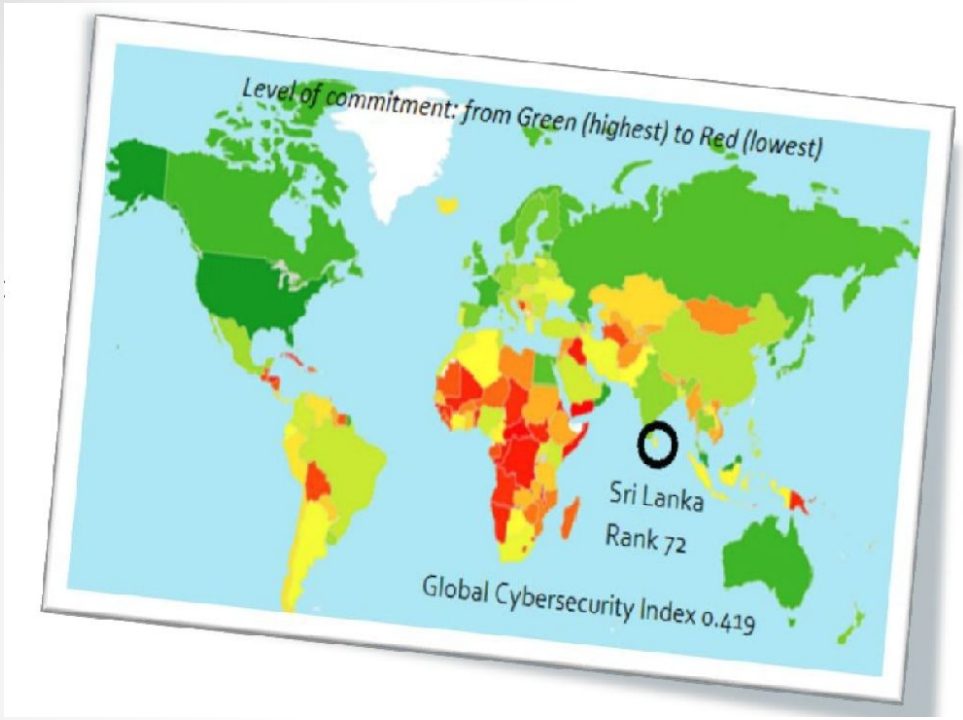
Social media incidents: report@cert.gov.lk

National Information and Cyber Security Strategy of Sri Lanka (2019-2023)

Our strategy is underpinned by six pillars:

1. Establishment of a governance framework to implement the National Information and Cyber Security Strategy
2. Enactment and formulation of legislation, policies, and standards to create a regulatory environment to protect individuals and organizations in the cyber space
3. Development of a skilled and competent workforce to detect, defend and respond to cyber attacks
4. Collaboration with public sector authorities to ensure that the digital government systems implemented and operated by them have the appropriate level of cyber security and resilience
5. Raising awareness and empowering citizens to defend themselves against cybercrimes
6. Development of public-private, local-international partnerships to create a robust cyber-security ecosystem

Information and Cyber security strategy in Sri Lanka



Our Performance in the GCI in detail[6]		
Assessment Criteria	**Assessment Sub Criteria**	**Our Status**
a. Legal	Cyber Crime Legislation	Initiating
	Cyber Security Legislation	Initiating
	Cyber Security Trainings	Leading
b. Technical	National CERT/CIRT/CSIRT	Leading
	Government CERT/CSIRT	Leading
	Sectoral CERT/CIRT/CSIRT	Leading
	Standards for Organizations	Initiating
	Standards for Professionals	Initiating
	Child Online Protection	Initiating
c. Capacity Building	Standardization bodies	Initiating
	Cybersecurity good practices	Leading
	R & D Programs	Maturing
	Public awareness campaigns	Leading
	Professional training courses	Leading
	Educational programs	Maturing
	Incentive mechanisms	Initiating
	Home-grown industry	Initiating
d. Organizational	Strategy	Initiating
	Responsible Agency	Maturing
	Cyber Security Metrics	Initiating
e. Cooperation	Bilateral agreements	Initiating
	Multilateral agreements	Leading
	International participation	Leading
	Public-private partnerships	Maturing
	Interagency partnerships	Initiating

Information and Cyber security strategy in Sri Lanka

Incidents Types	2012	2013	2014	2015	2016	2017
Phishing	08	08	12	14	23	42
Privacy Violation	08	08	08	21	32	29
Scams	06	18	12	18	12	32
Malicious Software/ Ransomware	02	02	03	12	21	39
Financial Frauds	-	-	-	10	16	35
Compromise Websites	15	16	56	20	10	25
Compromise Emails	06	08	10	16	16	14
Intellectual Property Violation	03	03	03	03	07	06
Unauthorized Access	01	11	08	-	-	-
DoS/DDoS	01	01	06	03	04	-
Social Media Incidents	1100	1200	2250	2850	2200	3685

Information and Cyber security strategy in Sri Lanka

Establishing a resilient and truster cyber security ecosystem that will enable Sri Lankan citizen.

Cyber Security Policy Framework in Sri Lanka

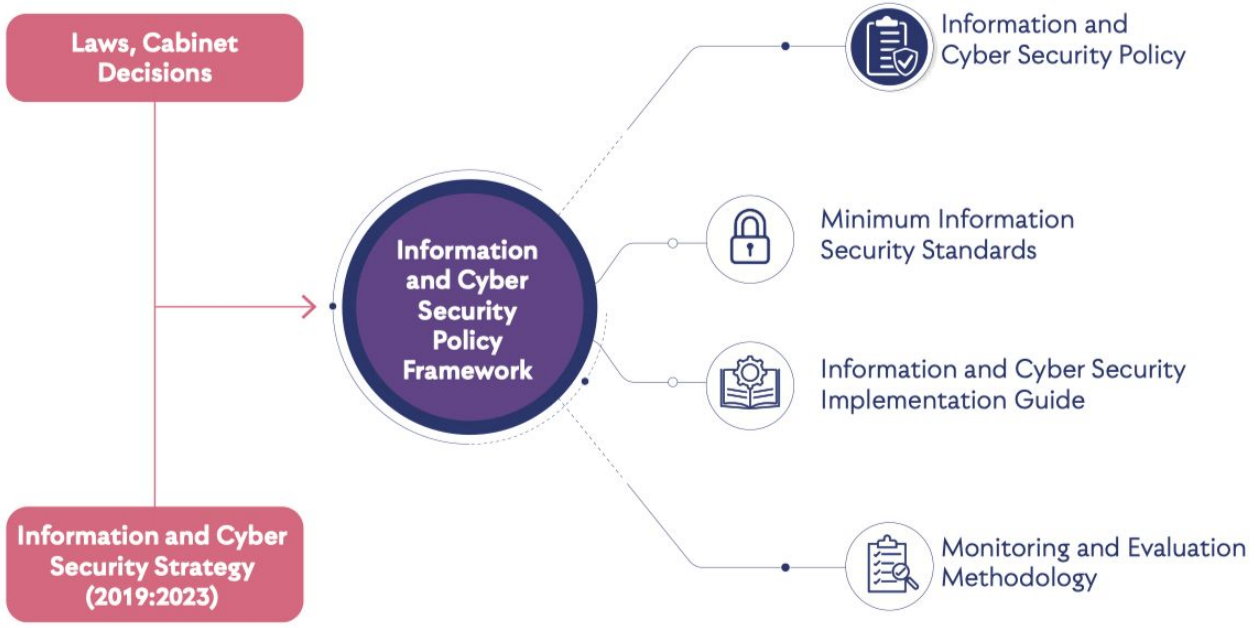


Figure 1: Information and Cyber Security Policy Framework

Brief of the Next Lecture

Intellectual Property

Reference

Joseph Migga Kizza, Ethical and Social issues in the information age,1997

https://oulms.in/wp-content/uploads/2022/04/Chapter-1.pdf

http://dacc.edu.in/wp-content/uploads/2021/12/TYBCA-Cyber-Security-Notes-1.pdf

Q & A

Thank You.