2802 - DTI

Unit 04

Cyber Security & Data Privacy

By Nadinsha Bandara

Content...

4.1 Cybersecurity Threats and Vulnerabilities

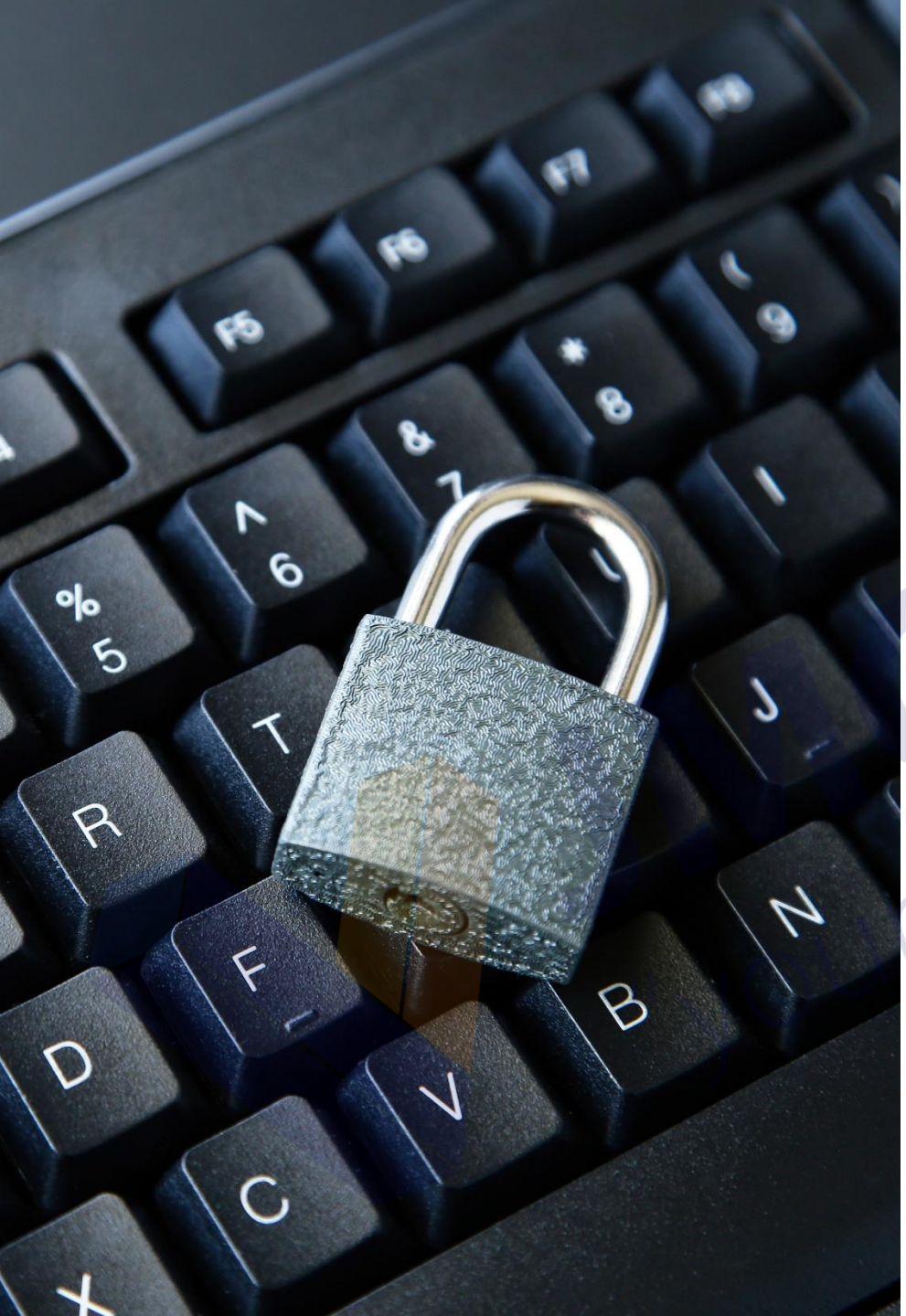
Information Security

- Information security refers to the **mechanisms that protect data.** Often, many consider information security as a mere technical control implemented into IT systems.

- It includes protecting data from **all types of threats, whether individual malicious outsiders or individual perpetrate those threats** with legitimate accesses to IT systems and data within the organization.

CIA Triads

- Confidentiality
- Integrity
- Availability



Confidentiality

- **Means protecting data, in all its forms, from unauthorized access throughout its entire lifecycle (from data creation to data destruction).**

- Unauthorized access includes access by individuals not affiliated with the underlying organization storing the data (e.g., criminals and hackers).

- Confidentiality is the information security concept most often implicated when an organization experiences a data breach.

Integrity

- **Means ensuring that data within IT systems (or recorded or reproduced on physical media) are accurate.**

- This means that IT system creators and managers implement controls within the system to ensure that users enter and process data correctly and that conflicting data elements are identified and resolved.

- When data have integrity, they are considered accurate and can be relied upon for decision-making.

Availability

- **Means ensuring that data are available when needed and that IT systems are operating reliably.**

- Stakeholders can ensure data availability in a number of ways, such as designing IT systems that are "redundant".

Cybersecurity vs Information Security

Cybersecurity	Information Security
• Protects digital systems, networks, computers, and mobile devices from threats like hacking, malware, phishing, and ransomware.	• Protects all forms of information, including both digital and physical data.
• Focuses mainly on securing online and digital environments.	• Has a broader scope than cybersecurity.
• Aims to prevent disruption, unauthorized access, and damage to digital systems and data.	• Aims to prevent unauthorized access, loss, theft, or damage of information in any form.
	• Covers data stored electronically as well as paper-based or physical records.

Cybersecurity Threats

1. **Malware** - Malicious software like viruses, worms, and ransomware that harm systems.
2. **Phishing** - Deceptive emails or messages trick users into revealing sensitive information.
3. **Ransomware** - Attackers encrypt data and demand payment to restore access.
4. **Denial of Service (DoS) Attacks** - Overloading a system or network to disrupt services.
5. **Man-in-the-Middle (MitM) Attacks** - Hackers intercept communication between two parties to steal or alter data.

Cybersecurity Threats

6. **SQL Injection** - Attackers manipulate databases by injecting malicious SQL queries.
7. **Zero-Day Exploits** - Hackers exploit unknown software vulnerabilities before they are patched.
8. **Insider Threats** - Employees or trusted individuals misuse their access to steal or damage data.
9. **Advanced Persistent Threats (APT)** Long-term, stealthy attacks by sophisticated cybercriminals, often for spying.
10. **Social Engineering** - Psychological manipulation to trick people into giving up confidential data

Impact of Cybersecurity Threats on Information Systems

Data Breaches - Hackers steal sensitive data, leading to financial and reputational damage e.g., a bank losing customer credit card details to hackers.

System Downtime - Ransomware or DoS attacks can shut down critical systems, affecting business operations.

e.g., a hospital unable to access patient records.

Unauthorized Access - Attackers take advantage of weak credentials can manipulate or delete critical data.

e.g., a hacker gaining admin access to modify payroll details.

Impact of Cybersecurity Threats on Information Systems

Loss of Data Integrity - Malicious software can alter or corrupt essential files.

Network Compromise - A single infected device can spread malware across the organizational network.

Cybersecurity Vulnerabilities

1. **Weak Passwords** - Easy to guess or reused passwords might allow unauthorized access.
2. **Unpatched Software** - Outdated applications and systems are more susceptible to attacks.
3. **Misconfigured Security Settings** - Poorly set security controls leave systems exposed.
4. **Lack of Encryption** - Unencrypted data can be intercepted and stolen.
5. **Phishing Exposure** - Users who react to fraudulent emails and links become entry points for attacks.

Cybersecurity Vulnerabilities

6. **Poor Access Controls** - Excessive permissions increase the risk of unauthorized activities.
7. **IoT Vulnerabilities** - Insecure smart devices provide entry points for hackers.
8. **Bring Your Own Device Risks** - Personal devices accessing corporate networks can introduce threats.
9. **Lack of Employee Training** - Human error is one of the biggest security risks.
10. **Open Ports & Weak Firewalls** - Improperly configured networks allow unauthorized access.

Impact of Cybersecurity Vulnerabilities on Organizational Operations

1. **Financial Loss -** Security breaches result in costly fixes, legal fines, and compensation.

   e.g., a retail store paying millions after a customer data breach.

2. **Reputational Damage Customers lose their trust after security failures.**

   e.g., a social media platform losing users after a privacy leak.

3. **Regulatory Non-compliance -** Organizations may face legal penalties for failing to secure data.

   e.g., a healthcare provider fined for not protecting patient records.

Impact of Cybersecurity Vulnerabilities on Organizational Operations

4. **Decreased Productivity -** Reduce workplace productivity by disrupting daily operations, causing downtime, and requiring employees to focus on security issues instead of their regular tasks.

   e.g., staff locked out of email due to a phishing attack.

5. **Supply Chain Disruptions -** Cyberattacks on one company can impact others in the supply chain. e.g., a hacked logistics company delaying deliveries for multiple retailers.

Popular Cyber Scams in Sri Lanka Targeting Individuals

Online loan scams	Fraudsters **create fake online lending platforms**, tempting individuals with promises of quick and easy loans. During the application process, **they collect sensitive personal information**, which is then used for unauthorized activities.
Social media investment frauds	Scammers **utilize social media platforms to promote fraudulent investment schemes,** often promising **high returns with minimal risk.**
Unlawful pyramid schemes	Certain online platforms **mislead investors into participating in pyramid schemes** under the appearance of legitimate investment opportunities. These schemes often claim to be compliant with local regulations and promise high returns, but they are unsustainable and illegal.
Pig butchering scams	**Fraudsters build fake relationships with victims to fraud** them into fraudulent cryptocurrency or forex investments. This scam, originating from Southeast Asia, has expanded globally.

4.2
Importance of Data Privacy and Implications on Organizations and Individuals

What is Privacy?

For individuals, privacy means the right of an individual to control his or her own data and to specify how those data are collected, used, and shared.

Data privacy refers to the protection of personal and sensitive information from unauthorized access, misuse, or exposure.

It ensures that individuals and organizations control how their data is collected, stored, shared, and used.

Why Data Privacy is needed?

1. Protects Personal and Sensitive Information
2. Prevents Financial Loss and Fraud
3. Ensures Compliance with Laws and Regulations
4. Builds Trust and Reputation
5. Protects Freedom and Prevents Surveillance Abuse
6. Prevents Cybersecurity Threats and Attacks

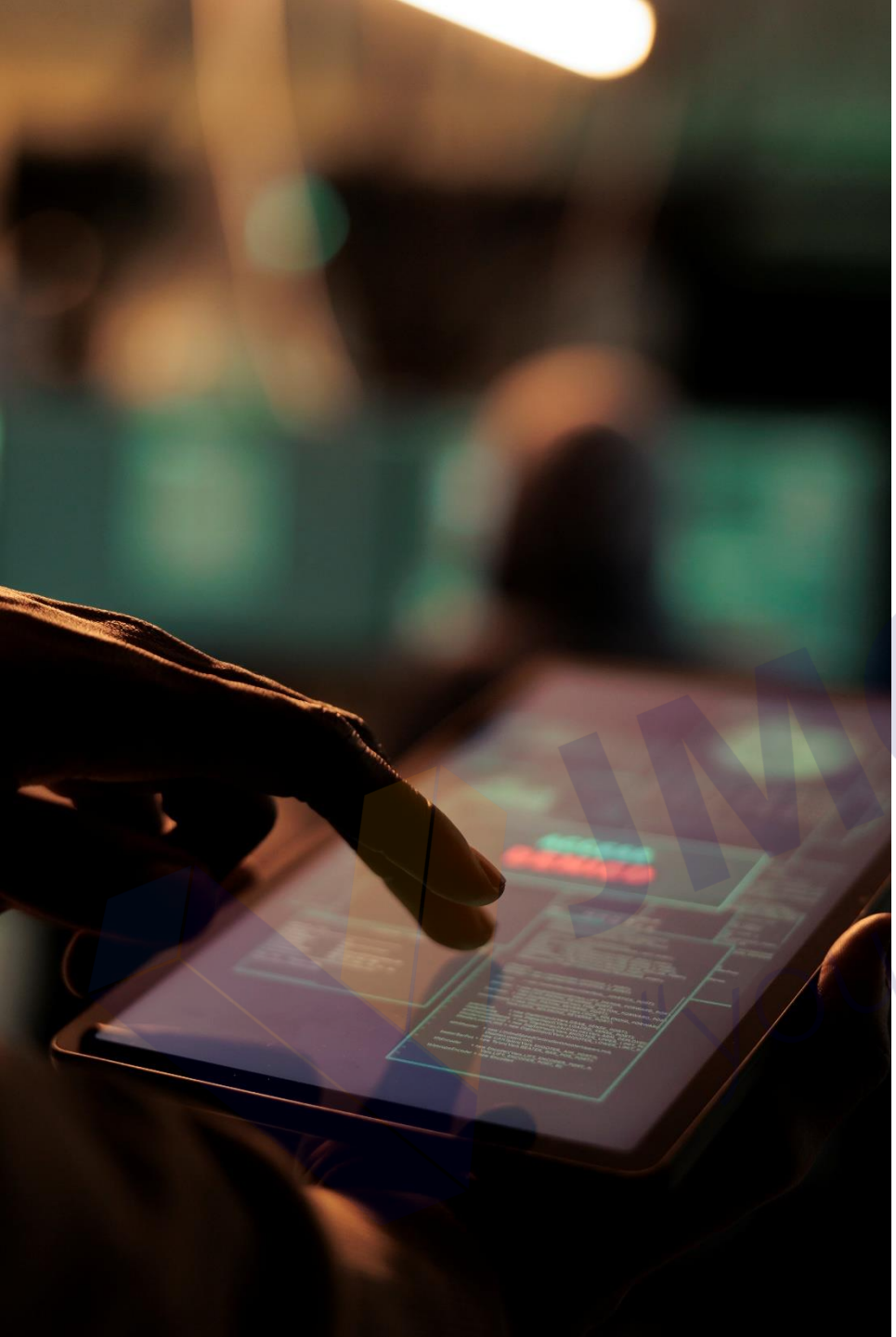
Implications of Data Privacy on Organizations

a) Legal and Regulatory Compliance

Many countries enforce strict data privacy laws, such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the U.S., and Sri Lanka's Personal Data Protection Act (PDPA).

b) Financial Loss and Business Disruptions

Data breaches and cyberattacks can result in significant financial losses. Costs include legal fees, compensation to affected individuals, and cybersecurity improvements. In some cases, businesses may lose revenue due to loss of customer trust.



Implications of Data Privacy on Organizations

c) Reputation Damage and Loss of Customer Trust

Customers expect organizations to protect their personal data. If a company fails to do so, it loses credibility and customer confidence, potentially leading to lower sales and long-term damage to its brand.

d) Increased Cybersecurity Threats

Weak data privacy policies make organizations vulnerable to cyberattacks like phishing, ransomware, and data breaches. Companies need strong security measures such as encryption, access control, and regular security audits to prevent unauthorized data access.

Implications of Data Privacy on Organizations

e) Competitive Disadvantage

Companies that fail to ensure data privacy may struggle to compete in the market. Customers prefer businesses that offer transparency and security, making data privacy a competitive advantage.

Implications of Data Privacy on Individuals

a) Identity Theft and Financial Fraud

Cybercriminals use leaked personal data, such as bank details, social security numbers, or credit card information, to commit fraud. Victims may suffer unauthorized transactions or lose access to their financial accounts.

b) Emotional and Psychological Stress

Privacy breaches can lead to harassment, blackmail, or cyberbullying, affecting an individual's mental health. A leaked private video of an individual spreads online, leading to public humiliation and emotional distress. Victims may experience anxiety, depression, or fear of using online services

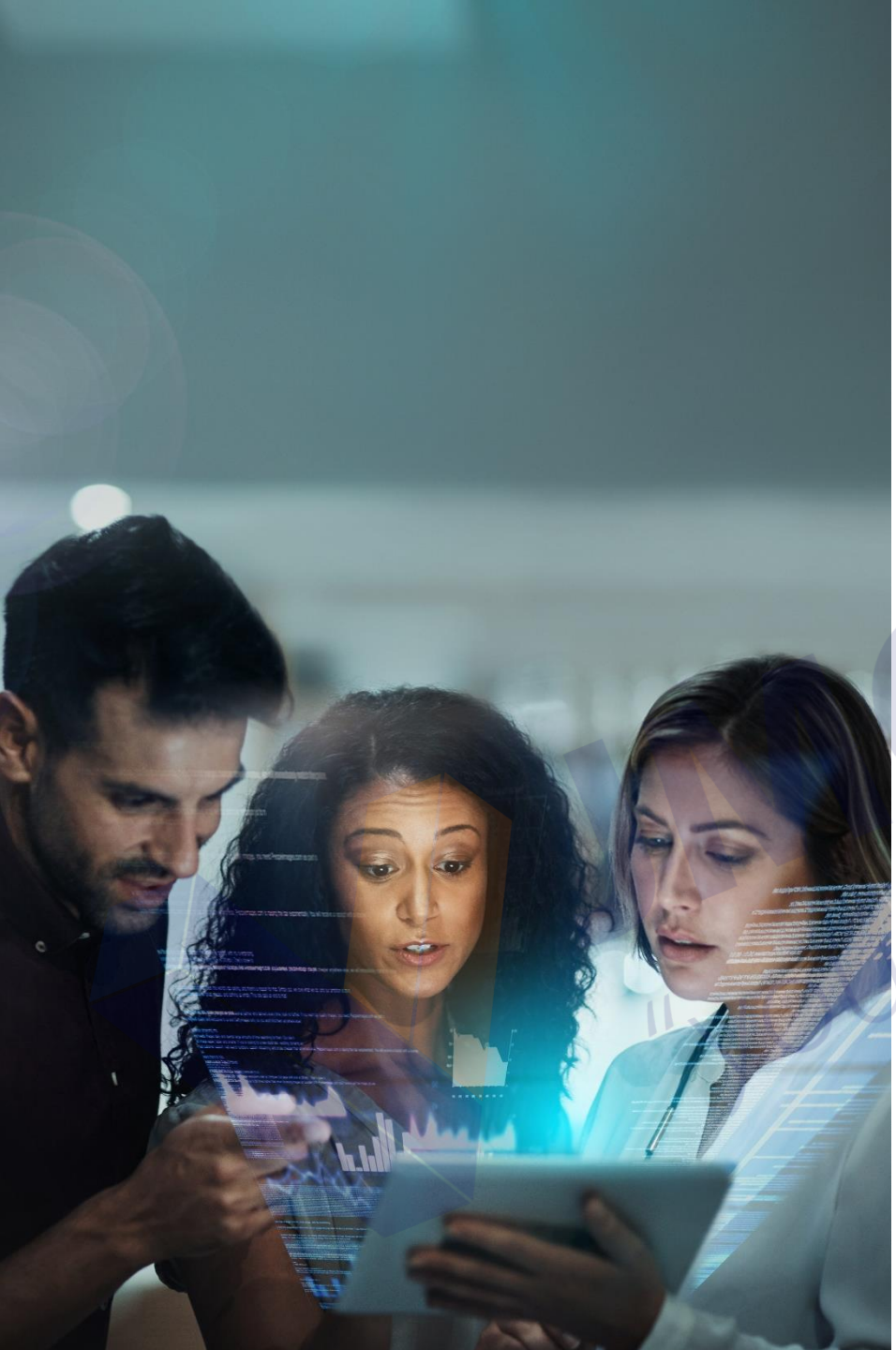
Implications of Data Privacy on Individuals

c) Loss of Personal Security and Safety Risks

Sensitive personal data, such as home addresses and phone numbers, can put individuals at risk of stalking or physical harm. Cybercriminals may misuse this information for illegal activities.

d) Misuse of Personal Information for Advertising and Tracking

Many online platforms collect user data without clear consent, using it for targeted advertising or selling it to third parties. Individuals lose control over their personal information, leading to unwanted surveillance.



Implications of Data Privacy on Individuals

e) Limited Digital Freedom and Privacy Violations

Government agencies or organizations may misuse data for mass surveillance, restricting individual freedoms and privacy rights. Without strong data privacy laws, individuals may lose their right to private communication and online activities.

4.3 Strategies to Mitigate Cybersecurity Risks

Cyberattacks such as data breaches, phishing, ransomware, and malware can result in financial losses, operational disruptions, and reputational damage.

To safeguard sensitive information and ensure business continuity, it is essential to implement proactive cybersecurity strategies.

What is Data Protection?

Data protection refers to laws that safeguard personal information from misuse, unauthorized **access, and exploitation, while giving individuals control over their data.**

In the digital era, large amounts of data are generated through online platforms, apps, and emerging technologies

Weak data protection can lead to risks such as data breaches, identity theft, and misuse of personal information.

Strong frameworks set rules for how data is collected, stored, and used, and give individuals rights like access, correction, and deletion of their data.

How Does Data Protection Work?

There **should be limits on the collection of personal data, and it should be obtained by lawful and fair means**, as well as being done in a transparent manner.

The **purposes for which the data and information is to be used should be specified** (at the latest) at the time of collection, and should only be used for those agreed purposes.

Personal data, as generated and processed, **should be adequate, relevant, and limited to necessity of the purposes for which it is to be used.**

How Does Data Protection Work?

The data should be **accurate and complete, and measures should be taken** to ensure it is up to date.

Reasonable security **safeguards should be used to protect personal data from loss, unauthorized access, destruction, use, modification or disclosure.**

There **should be no secret processors of data, sources, or processing. Individuals must be made aware of the collection and processing of their data**, as well as the purpose of its use, who is controlling it, and who is processing it.

Improving Cyber Security

Technical Controls	**Data Encryption**	Converts normal data (text, files, messages) into a coded format that is unreadable without a special key. It works like locking data in a secure box so only authorized users can unlock it.
	Strong Authentication (2FA/MFA)	Uses extra security steps to verify identity before access is granted. In 2FA, after entering a password, a code is sent to a phone for confirmation. MFA uses two or more methods such as a password plus fingerprint or a phone code, making it more secure even if passwords are stolen.

Improving Cyber Security

Technical Controls	**Strong Passwords**	Passwords should be difficult to guess and not based on personal details like names, pets, or sports teams. Using a mix of random words, numbers, and symbols improves security.
	Regular Software Updates and Patch Management	Keeps systems updated to fix security weaknesses that hackers could exploit. Outdated software or unsupported systems become vulnerable because they no longer receive security patches, making attacks easier. Installing updates quickly helps protect devices.

Improving Cyber Security

Technical Controls	**Network Separation and Firewalls**	Divides networks into smaller sections to limit damage if one part is attacked. Firewalls help by filtering incoming and outgoing traffic and blocking malicious data.
	Security Tools and Software	Uses antivirus, anti-malware, and intrusion detection systems (IDS) to detect, prevent, and remove threats like viruses, spyware, and ransomware. Keeping these tools updated improves protection.
	Continuous Monitoring and Threat Intelligence	Monitors network activity in real time to detect unusual behaviour and emerging threats, allowing quick response to cyberattacks.

Improving Cyber Security

Administrative Controls	**Conduct Regular Risk Assessments**	Systematic evaluations used to identify, analyse, and address potential threats and vulnerabilities in systems, data, and operations. Security teams review assets, assess risks like data breaches or system failures, and evaluate their likelihood and impact. The results help prioritize security measures, update policies, and proactively reduce vulnerabilities to prevent costly incidents.
	Employee Training and Awareness	Educates staff on identifying threats such as phishing and handling data securely. Regular updates in training (often included in annual plans) are important due to constantly changing cyber threats. Spam or junk emails can sometimes be malicious and cause serious damage to systems.

Improving Cyber Security

Administrative Controls	**Develop an Incident Response Plan**	Provides clear procedures for detecting, responding to, and recovering from cybersecurity incidents. It includes steps such as identifying threats, containing damage, removing the cause, restoring systems, and reviewing incidents to prevent future attacks. It also defines roles and responsibilities for the security team.
	Implement Access Control Policies	Uses role-based access control to limit what users can access based on their job roles. This ensures only authorized individuals can view or use sensitive information, reducing the risk of data breaches or misuse. For example, different employees may have access to different types of company data depending on their responsibilities.

Improving Cyber Security

Administrative Controls	**Collaborate with Third-Party Security Experts**	Involves working with external experts who evaluate systems, identify vulnerabilities, and recommend security improvements. These specialists use advanced tools and knowledge to strengthen defenses and ensure organizations follow best practices and industry standards.
	Manage Security Relationships with Suppliers and Partners	Ensures that third-party vendors and partners follow strong security standards, since they can also introduce risks into the supply chain. Organizations must review contracts and service level agreements (SLAs) to confirm that external providers protect data properly and maintain required security controls.

Improving Cyber Security

Administrative Controls	**Collaborate with Third-Party Security Experts**	Involves working with external experts who evaluate systems, identify vulnerabilities, and recommend security improvements. These specialists use advanced tools and knowledge to strengthen defenses and ensure organizations follow best practices and industry standards.
	Manage Security Relationships with Suppliers and Partners	Ensures that third-party vendors and partners follow strong security standards, since they can also introduce risks into the supply chain. Organizations must review contracts and service level agreements (SLAs) to confirm that external providers protect data properly and maintain required security controls.

Improving Cyber Security

Physical Controls	**Backup and Disaster Recovery Planning**	Involves physically storing backup copies of critical data and systems in secure locations to prevent loss from physical damage or cyberattacks.
	Surveillance and Monitoring	Installing cameras and surveillance systems around sensitive areas helps monitor and record activities, deterring unauthorized individuals and ensuring a record of events for security purposes.
	Restricted Access to Facilities	Limiting physical access to servers, data centers, and critical infrastructure to authorized personnel only helps protect against unauthorized access or tampering with sensitive equipment.

4.4 Importance of Compliance with Regulations

Cybersecurity compliance is the practice of ensuring that an organization adheres to established security standards, laws, and regulations to safeguard its digital assets and sensitive information.

Why Compliance and Regulations are Important?

Adhering to local regulations	Ensures personal data is handled lawfully, protects individual rights, and requires organizations to prevent data breaches and cybercrime.
Key Sri Lankan laws	Includes the PDPA for data protection, the Computer Crimes Act for cyber offences, and the Electronic Transactions Act for secure digital transactions.
International compliance	Standards like GDPR and ISO/IEC 27001 guide organizations in following global data protection and security practices.
Stronger cybersecurity	Requires risk assessments, audits, and security controls to reduce threats like phishing, ransomware, and data breaches.
Trust and reputation	Compliance builds customer confidence and strengthens business relationships.

Why Compliance and Regulations are Important?

Competitive advantage	Helps organizations gain credibility and access international markets more easily.
Protect Sensitive Data	Safeguarding customer, employee, and business information from cyber threats.
Mitigate Financial Losses	Reducing the risk of costly data breaches, fines, and legal consequences.
Maintain Business Continuity	Ensuring operational resilience in the face of cyber incidents.
Competitive advantage	Helps organizations gain credibility and access international markets more easily.

Consequences of Non-compliance

1. Legal Penalties and Fines Under Sri Lanka's PDPA (Personal Data Protection Act)

Non-compliance can lead to administrative fines imposed by the Data Protection Authority.

2. Financial Losses

Non-compliance often results in weak security, leading to data breaches, ransomware attacks, and online scams that cause direct financial losses. Non-compliance can raise cyber insurance costs or even result in denial of coverage.

3. Reputational Damage and Loss of Trust

Data breaches damage public trust, leading to customer attrition. Cyber incidents often attract bad publicity, harming brand reputation.

Consequences of Non-compliance

4. Operational Disruptions

Cyberattacks like ransomware can lock critical systems, halting operations, lead to permanent data loss. In 2022, a Sri Lankan government agency faced a ransomware attack that disrupted its services for several days, exposing the lack of disaster recovery protocols.

5. Lawsuits and Legal Actions

Customers may sue organizations for negligence in protecting their data. Non-compliance can trigger investigations and audits from regulatory bodies such as the Data Protection Authority or CERT CC.

6. Increased Cybersecurity Vulnerability

Weak cybersecurity controls make organizations an easy target. Hackers may alter sensitive information, causing financial fraud or system failures.

Global Cybersecurity Standards and Frameworks

1. ISO/IEC 27001 (International Standard for Information Security):

A globally recognized standard for information security management systems. It provides best practices for managing data security risks. ISO is widely adopted across industries for certification and compliance.

2. NIST Cybersecurity Framework (National Institute of Standards and Technology, USA):

A voluntary framework for managing cybersecurity risks. NIST consists of five core functions. Identify, Protect, Detect, Respond, and Recover. Commonly used by critical infrastructure sectors and enterprises.

3. COBIT (Control Objectives for Information and Related Technologies):

A framework for developing, implementing, monitoring, and improving IT governance and management practices. Widely used in conjunction with ISO 27001 and NIST standards.

4. General Data Protection Regulation (GDPR):

A comprehensive data protection law regulating how organizations collect, store, and process personal data. GDPR requires breach notifications within 72 hours.

Non-compliance can lead to fines of up to £20 million or 4% of annual global turnover. GDPR is implemented in Europe Union and associated countries with the EU for businesses.

5. PCI DSS (Payment Card Industry Data Security Standard):

Applies to organizations handling credit card transactions. It ensures secure storage, processing, and transmission of cardholder data.

International Compliance and Agreements Adopted by Sri Lanka

Budapest Convention on Cybercrime:

- International treaty focused on fighting cybercrime through global cooperation.
- Sri Lanka’s observer status helps it stay connected with international cyber laws and practices.
- Supports sharing digital evidence, improving legal frameworks, and strengthening cross-border investigations.
- Helps align national laws with global standards to respond more effectively to cyber threats.

APCERT (Asia Pacific Computer Emergency Response Team):

- Regional network of cybersecurity teams across Asia-Pacific countries.
- Enables fast sharing of cyber threat information and alerts.
- Supports coordinated response to cyber incidents like hacking, malware, and ransomware attacks.
- Helps improve incident reporting and reduces the impact of cross-border cyber threats.

- **Commonwealth Cyber Declaration:**
  - A collective agreement among Commonwealth countries to improve cybersecurity.
  - Promotes cooperation in sharing knowledge, tools, and best practices.
  - Focuses on building cybersecurity skills and national cyber defense capacity.
  - Helps countries like Sri Lanka strengthen their ability to prevent, detect, and respond to cyberattacks.