Threat Landscape

A threat landscape refers to the overall environment of potential security threats facing an organization or individual. It includes an assessment of the likelihood and impact of various types of threats, such as cyber-attacks, data breaches, and malware. It also includes an analysis of the effectiveness of existing security controls and countermeasures. The threat landscape is constantly changing, as new technologies and attack methods are developed, and existing ones evolve.

The threat landscape can be divided into several categories, such as:

Cybercrime: This includes attacks such as phishing, ransomware, and financial fraud.

Advanced Persistent Threats (APTs): This refers to targeted attacks, often by nation-state actors, that seek to gain access to an organization's sensitive information over an extended period of time.

Insider threats: These refer to threats that originate from within an organization, such as employees or contractors who misuse their access to sensitive information.

IoT threats: This includes threats related to Internet of Things (IoT) devices, such as connected cameras, smart home devices, and industrial control systems.

Cloud and mobile threats: This includes threats related to the use of cloud services and mobile devices, such as unauthorized access to cloud data and mobile malware.

Social Engineering: This includes threats that rely on psychological manipulation to trick users into divulging sensitive information or performing actions that compromise security.

Computer incident and types of exploits

A computer incident refers to a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Computer incidents can take many forms, including:

Malware: This includes viruses, worms, Trojan horses, and other malicious software that can damage or steal information from computer systems.

Phishing: This is an attempt to trick users into providing sensitive information, such as login credentials, through email or other electronic communication.

Denial of Service (DoS) attacks: This is an attempt to disrupt the normal functioning of a computer system by overwhelming it with traffic or requests.

Distributed Denial of Service (DDoS) attacks: This is a type of DoS attack that uses a network of compromised computers, known as a "botnet," to launch the attack.

Hacking: This is an unauthorized attempt to access a computer system or network.

Insider threats: This refers to threats that originate from within an organization, such as employees or contractors who misuse their access to sensitive information.

Social engineering: This includes threats that rely on psychological manipulation to trick users into divulging sensitive information or performing actions that compromise security.

Data breaches: This refers to the unauthorized access, use, disclosure, disruption, modification, or destruction of sensitive information.

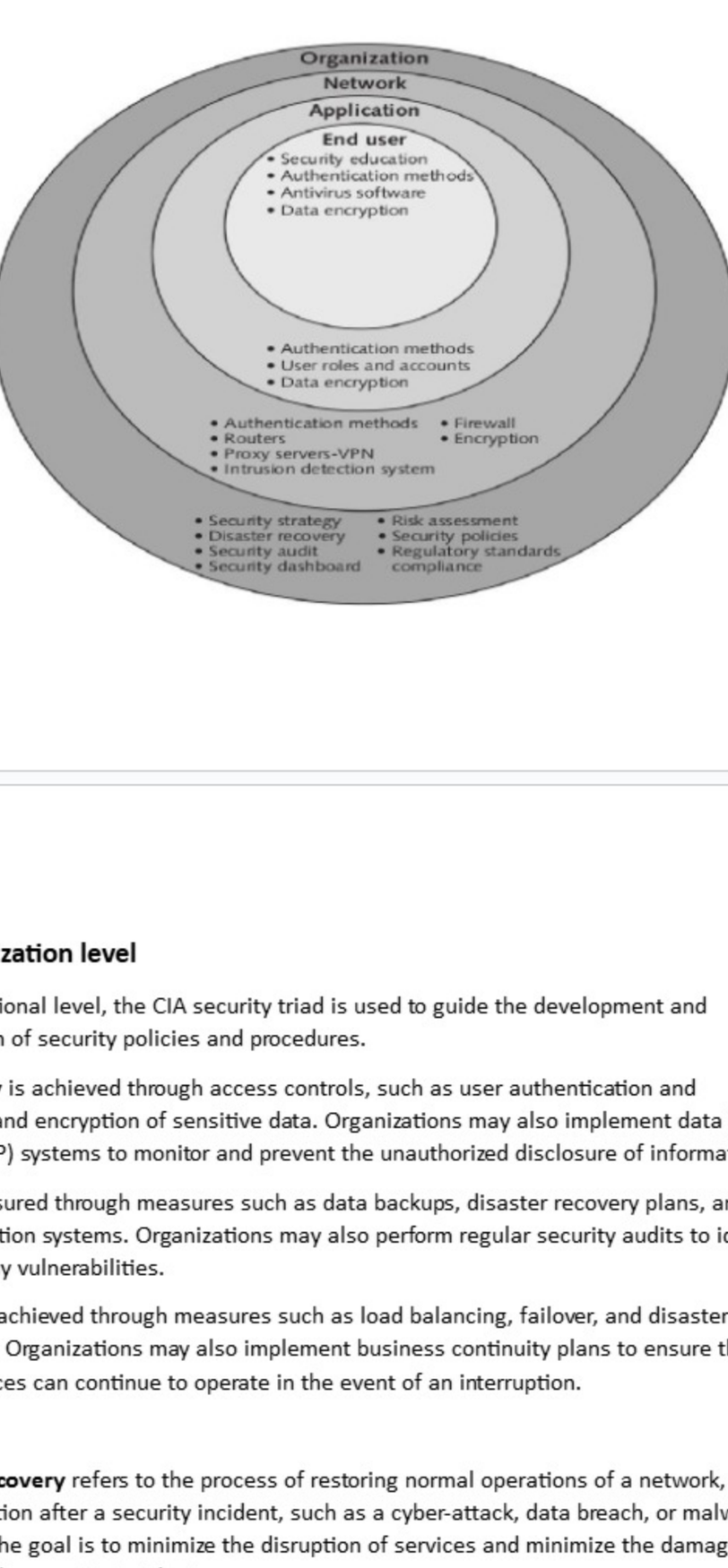
SQL injection: This type of exploit involves injecting malicious code into a website's database through a vulnerability in the website's code.

Man-in-the-middle (MitM) attacks: This type of exploit involves intercepting and modifying communication between two parties without their knowledge.

CIA security triad

The CIA security triad is a model for guiding information security policies and practices. It consists of three components: confidentiality, integrity, and availability.

- **Confidentiality** refers to ensuring that sensitive information is only accessible to authorized individuals.
- **Integrity** refers to ensuring that information is accurate and has not been tampered with.
- **Availability** refers to ensuring that authorized individuals have access to the information when they need it.



CIA at organization level

At an organizational level, the CIA security triad is used to guide the development and implementation of security policies and procedures.

Confidentiality is achieved through access controls, such as user authentication and authorization, and encryption of sensitive data. Organizations may also implement data loss prevention (DLP) systems to monitor and prevent the unauthorized disclosure of information.

Integrity is ensured through measures such as data backups, disaster recovery plans, and intrusion detection systems. Organizations may also perform regular security audits to identify and address any vulnerabilities.

Availability is achieved through measures such as load balancing, failover, and disaster recovery plans. Organizations may also implement business continuity plans to ensure that essential services can continue to operate in the event of an interruption.

Methods:

- **Disaster recovery** refers to the process of restoring normal operations of a network, system, or organization after a security incident, such as a cyber-attack, data breach, or malware outbreak. The goal is to minimize the disruption of services and minimize the damage caused by the security incident.
- **Risk assessment:** It is used to identify and understand the potential risks to an organization's assets, including its people, information, and physical infrastructure, in order to develop and implement effective security measures to mitigate or manage those risks.
- **Security policies** are needed to guide employees to follow recommended processes and practices to avoid security-related problems.
- **Security Audits:** Another important prevention tool is a security audit that evaluates whether an organization has a well-considered security policy in place and if it is being followed. For example, if a policy says that all users must change their passwords every 30 days, the audit must check how well that policy is being implemented.

CIA at network level

At a network level, the CIA security triad is used to guide the design, implementation, and maintenance of security controls for a network infrastructure.

Confidentiality is achieved through network segmentation, which involves dividing a network into smaller subnets and applying different security controls to each subnet. This can be done through the use of firewalls, virtual private networks (VPNs), and other network security devices. **Encryption** can also be used to protect data as it travels over the network.

Integrity is ensured through measures such as intrusion detection and prevention systems (IDPS), which monitor network traffic for signs of malicious activity and can block or alert on such activity. Network integrity can also be ensured through the use of network access control (NAC) systems, which limit access to a network based on user identity and device compliance.

Availability is achieved through the use of network redundancy, load balancing, and failover mechanisms. This allows for the continued operation of network services even in the event of a failure or disruption. Network monitoring can also be used to identify and address issues that could affect availability.

Methods:

- **Firewalls:** A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.
- **VPN:** VPNs provide an encrypted connection between a remote user and the enterprise network. This protects against eavesdropping and reduces the risk that the remote user will be infected with malware.
- **Intrusion Detection and Prevention Systems (IDPS):** are security systems that monitor and analyze network traffic or system activity to identify and prevent unauthorized access or malicious activity. They combine the capabilities of intrusion detection systems (IDS) with the ability to take action to prevent intrusions.
- **Network redundancy** is the practice of implementing multiple, independent systems or components in a network infrastructure to provide a backup in case of failure or disruption. This helps to ensure the availability of network services, even in the event of a failure or disruption.
- **Load balancing** is the practice of distributing network traffic across multiple servers or resources in order to ensure that no single server or resource becomes overloaded. This helps to ensure the availability and performance of network services.

CIA at application level

- ➢ Authentication methods, user roles and accounts, and data encryption are key elements of the application security layer.
- ➢ These elements must be in place to ensure that only authorized users have access to the organization's applications and data and that their access is limited to actions that are consistent with their defined roles and responsibilities.

Authentication methods

Authentication is the process of verifying the identity of a user, system, or device. There are several different authentication methods that can be used to accomplish this, including:

- ➢ password or PIN.
- ➢ Location-based authentication, such as confirming the location of the device or user through GPS or IP address.
- ➢ Multi-factor authentication, which combines two or more of the above methods for added security.
- ➢ Biometric Authentication, which uses a unique physical trait of the user, such as a fingerprint, facial recognition, iris scan, etc.
- ➢ Knowledge-based authentication, which is based on something only the user knows, such as answers to personal questions.

User roles and accounts

In a computer system or network, user roles and accounts are used to control access to resources and perform specific tasks.

- **User roles:** These are the different types of users within a system, each with a specific set of permissions and responsibilities. Examples of user roles include administrator, user, guest, and superuser.
- **User accounts:** These are the individual records that are created for each user in the system. Each account contains information such as the user's name, password, and permissions.

User roles and accounts are used together to control access to resources and perform specific tasks. For example, an administrator may have full access to all resources and the ability to perform all tasks, while a guest may have limited access and the ability to perform only certain tasks.

Data encryption

CIA at user level

Security education, authentication methods, antivirus software, and data encryption must all be in place to protect what is often the weakest link in the organization's security perimeter—the individual end-user.

Security education
It is the process of educating individuals, employees, and organizations about the importance of information security and how to protect against security threats. The goal of security education is to raise awareness of security risks and to empower individuals to take the necessary steps to protect themselves and their organizations.

Data encryption

Major enterprise systems such as enterprise resource planning (ERP), customer relationship management (CRM), and product lifecycle management (PLM) access sensitive data residing on data storage devices located in data centers, in the cloud, or at third-party locations.

Data encryption should be used within such applications to ensure that these sensitive data are protected from unauthorized access.

Authentication methods

Antivirus Software

Antivirus software should be installed on each user's personal computer to scan a computer's memory and disk drives regularly for viruses.

Antivirus software scans for a specific sequence of bytes, known as a virus signature, that indicates the presence of a specific virus.

RESPONSE TO CYBERATTACK

- **Incident notification**
  It is the process of informing relevant parties about a security incident or potential incident. This can include both internal and external parties, depending on the nature and scope of the incident. The goal of incident notification is to ensure that appropriate action can be taken to contain, investigate, and respond to the incident in a timely manner.
  Internal incident notification typically involves informing key personnel within the organization, such as IT staff, security teams, and management. This may include activating incident response teams and activating incident response plans.
  External incident notification may be required when the incident has the potential to affect other organizations or individuals, such as when personal data of customers or employees is involved or when the incident is likely to cause reputational damage.

- **Protecting evidence and activity logs**
  is an important aspect of incident response and forensic investigations. Evidence and activity logs can be used to identify the cause of an incident, establish the scope of the incident, and determine the appropriate response.
  To protect evidence and activity logs, organizations should follow best practices for securing and preserving digital evidence, such as:
  Isolating the affected systems: To prevent further damage or alteration of evidence, systems should be isolated as soon as possible after an incident is detected.
  Creating a forensic image: A forensic image of the affected systems should be created to preserve the evidence in its original state.
  Securing the evidence: Evidence and activity logs should be stored in a secure location, such as a tamper-evident container or a secure server, to prevent unauthorized access or alteration.
  Managing access to evidence and activity logs: Access to evidence and activity logs should be restricted to authorized personnel, and any access should be logged and audited.
  Maintaining chain of custody: The chain of custody of the evidence and activity logs should be maintained to ensure the integrity of the evidence and to demonstrate that the evidence has not been tampered with.
  Following legal and regulatory requirements: Organizations should comply with any legal or regulatory requirements related to the collection, preservation, and handling of digital evidence.

- **Incident containment**
  It is the process of isolating and controlling an incident to prevent it from spreading or causing further damage. It is a critical step in incident response, as it helps to minimize the impact of an incident and reduce the overall recovery time.

- **Eradication**
  Eradication is the process of removing an incident from a system or network. It is a critical step in incident response, as it helps to restore normal operations and prevent the incident from recurring. There are several steps involved in incident eradication, including:

  Identifying and removing malicious files: Any malicious files or software that were used to exploit a vulnerability or gain unauthorized access should be identified and removed. This may involve using anti-virus software, malware scanners, or other tools.

  Patching vulnerabilities: Any vulnerabilities that were exploited by the incident should be patched to prevent the incident from recurring. This may involve applying software updates, configuring security settings, or implementing other security controls.

  Restoring from backups: If necessary, systems and data can be restored from backups to ensure that they are in a known good state.

  Monitoring the systems: After eradication, the systems should be continuously monitored to detect any signs of the incident recurring.

  Documenting the incident: It's important to document the incident and the eradication steps taken, to provide an accurate record of the incident and serve as a reference for future incident response.

- **Using an MSSP**

An MSSP (Managed Security Service Provider) is a third-party company that provides a range of security-related services to organizations. These services can include:

Network security: MSSPs can provide a range of network security services, such as firewall management, intrusion detection and prevention, and vulnerability scanning.

Threat intelligence: MSSPs can provide organizations with threat intelligence, such as information on the latest threats, attack methods, and vulnerabilities.

Compliance: MSSPs can help organizations to meet compliance requirements, such as HIPAA, PCI-DSS, and SOC 2.

Incident response: MSSPs can provide incident response services, such as incident management, forensic analysis, and incident follow-up.

Security Operations Center (SOC): MSSPs can provide SOC as a service, which will monitor the organization's network and assets for security threats and respond to incidents.

Using an MSSP can provide several benefits for organizations. These include:

Cost-effective: Outsourcing security services to an MSSP can be more cost-effective than building and maintaining an in-house security team.

Expertise: MSSPs typically have a team of security experts who can provide specialized expertise and knowledge.

Scalability: MSSPs can provide a range of services that can be scaled to meet the organization's changing security needs.

24/7 monitoring: MSSPs can provide 24/7 monitoring and incident response, ensuring that security threats are detected and responded to in a timely manner.

Compliance: MSSPs can help organizations to meet compliance requirements, which is critical for many businesses.

- **Computer Forensics**

Computer forensics is the process of collecting, preserving, analyzing, and presenting digital evidence in a manner that is legally admissible. It is a branch of digital forensics which specifically deals with the examination of digital devices, including computers, servers, mobile devices, and storage media.

- ➢ **Database forensics:** Retrieval and analysis of data or metadata found in databases
- ➢ Email forensics: Retrieval and analysis of messages, contacts, calendars, and other information on an email platform
- ➢ **Mobile forensics:** Retrieval and analysis of data like messages, photos, videos, audio files, and contacts from mobile devices
- ➢ **Memory forensics:** Retrieval and analysis of data stored on a computer's RAM (random access memory) and/or cache
- ➢ **Network forensics:** Use of tools to monitor network traffic like intrusion detection systems and firewalls

- **Incident follow up**

The purpose of incident follow-up is to assess whether supports and services were being provided as required immediately before, during, and after the incident, and to determine whether any further action should be taken to ensure the safety of the participant and others or reduce the frequency and severity of incident.

Provision of Cyber Law and Electronic Transaction Act of Nepal

- ➢ The first cyber law was the Computer Fraud and Abuse Act (CFAA), which was enacted in 1986.
- ➢ On the 30th Bhadra, 2061 B.S., a cyber law was developed to tackle computer crime and violence.
- ➢ In 2004, Nepal passed the much-awaited Electronic Transaction and Digital Signature Act Ordinance known as Cyber Law of Nepal. The government also passed the Electronic Transactions Act (ETA), 2063 (2008), and Electronic Transaction Regulations (ETR) in 2064 (2007).

Electronic Transaction Act 2063

Electronic Transaction Act 2063 has 12 chapters:

1. Preliminary Statement
2. The provisions related to electronic records and digital signatures
3. Provisions relating to Dispatch, Receipt, and Acknowledgement of Electronic Records.
4. Provisions relating to controller and Certifying Authority
5. Provisions relating to Digital Signature and Certificates
6. Functions, Duties and Rights of Subscriber
7. Electronic record and government use of digital signature
8. Provisions relating to network service
9. Offence relating to computer
10. Provisions relating to Information Technology Tribunal
11. Provisions relating to Information technology Appellate Tribunal
12. Miscellaneous

All laws and acts regarding Cybercrime and penalties in Nepal are according to the Electronics Transaction Act 2063 (2008).

Section 48: Piracy, Destruction, and Alteration of the Computer source code is a big offense. The punishment for a crime under this act can be up to 3 years of conviction or a maximum penalty of Rs 2,00,000 or both.

Section 45: Unauthorized access in Computer Material by any person who is not supposed to access the equipment, program, code is also punishable. The punishment is the same maximum 3 years imprisonment or maximum 2 Lakh rupees fine.

Sec. 47: Publication of Illegal Material in electronic form. This is the biggest and wide act. If anyone publishes any content that does defamation, creates hate, destroys the public image, does public shaming or shares derogatory content can be punished. There is provision for 5 years prison and a fine up to Rs 1,00,000.

Section 48: Confidentiality to Divulge. Under this, if anyone destroys the confidentiality of records, information, logs, letter, memo, archive, etc. by disclosing to any unauthorized person is punishable. The punishment is maximum of 2 years in jail or Rs 10,000 fine or both.

Section 49: To Inform False Statement – Maximum fine is Rs 1,00,000 and jail time is 2 years.

Section 52: Computer Fraud: It encompasses crimes regarding ATM, digital signature certificate, fraud and publishing illegal content. Maximum Punishment can be Rs 1 Lakh fine or 2 years imprisonment or both.

Sec. 56: Government can confiscate any electronic device like computer, router, modem, smartphone, tablet, laptop, etc. which has been involved in crime or is evidence.

Section 55: If any offence is committed outside of Nepali land which affects the computer and network system inside Nepal, it is also punishable under law.

Different cyber laws in Nepal

1. **The Electronic Transactions Act, 2008**

This was Nepal's first cyber law. Cybercrimes were dealt with under the Country's criminal code before this law came into force. Since the cases of cybercrime increased, it became necessary to enact a separate law.

Chapter 9 of the Act deals with offences relating to computers, the main highlights of which are as follows:

- ➢ Pirating or destroying any computer system intentionally without authority carries imprisonment for three years, or a fine of two hundred thousand rupees, or both.
- ➢ Accessing any computer system without authority results in imprisonment for three years, or a fine of two hundred thousand rupees, or both.
- ➢ Intentional damage to or deleting data from a computer system carries imprisonment for three years, or a fine of two hundred thousand rupees, or both.
- ➢ Publication of illegal material in electronic form carries imprisonment for 5 years, or a fine of one hundred thousand rupees, or both.
- ➢ Commission of a computer fraud carries imprisonment for two years, or a fine of one hundred thousand rupees, or both.

2. **The Children's Act, 1992**

- ➢ The aim of this Act is to protect and uphold the rights of children.
- ➢ It also prohibits child pornography.
- ➢ Section 16(2) of the Act prohibits individuals from capturing any immoral picture of a child.
- ➢ Section 16(3) of the Act prohibits the publication and distribution of any such photographs of children.

3. **The Copyright Act, 2002**

- ➢ This act protects the copyright of ideas, including a computer program.
- ➢ It prohibits people from copying and modifying the original work of others and using it for their own advantage or economic benefits.

4. **The Individual Privacy Act, 2018**

- ➢ This act is the first legislation in Nepal to protect the right to privacy of its people and define personal information.
- ➢ It protects the privacy of the body, family life, residence, property, and communication. It puts the responsibility on public entities to protect the personal data of individuals.
- ➢ They cannot transfer such data to anyone without the consent of the owner.
- ➢ The Act prescribes a general punishment for violation of privacy as three years of imprisonment, or a fine of NPR 30,000, or both.