# WEEK 1: MODULE ONE

# CYBERSECURITY FUNDAMENTALS

## SESSION ONE: INTRODUCTION TO CYBERSECURITY

Cybersecurity is an emerging field with a high demand for experts from around the globe. With the ever-increasing globalization, security issues in information and critical infrastructure are becoming vital. In this course, the reader will learn what cybersecurity is like, how to gain the necessary skills, and where to find work. Focus on the sector's basic operations and key ideas.

It is also worth making a brief contribution and understanding the place of cyber security within information security before proceeding to a new career in this stream. Information security may also protect information and information systems from threats against unauthorized access, use, disclosure, disruption, modification, or destruction. Cybersecurity is implementing the concept of information protection from cyber threats that can affect computer networks, devices, aware applications, etc.

**Security policies and procedures:** This is also known as an information security policy, which refers to an organization's standard or framework for safeguarding its information and systems. It embraces concepts like access control, handling information security incidents, and data categorization.

### The Key concept and components of cybersecurity

**Confidentiality, Integrity, and Availability (CIA) Triad:** These are the three elements of information security. Confidentiality pertains to protecting data from disclosed individuals; integrity pertains to safeguarding data's veracity and safeguarding the ability of authorized persons to access data and systems at the right time.

The basic concept of **defense-in-depth** is to use layers of barriers to protect information and systems from unauthorized access. This means that whether one layer is violated, there are others to minimize the chances of intrusion or destruction.

Cybersecurity comprises many factors that form adequate digital information and system security measures. Amongst these components, the following can be regarded as some of the most important ones:

Network security is, therefore, the protection of networks and the traffic passing through them from being accessed or tampered with maliciously. Some network security methods are firewalls, intrusion detection, and cryptographic solutions.
As the name suggests, **Application Security** deals with the security of applications or software that hackers might target. Application security can be defined as secure coding practices, vulnerabilities, and patching vulnerabilities.
**Endpoint or terminal protection** refers to protecting devices such as desktops, laptops, and mobile devices, which are the last link in the organizational security structure and can easily be attacked. Endpoint protection **is** called antivirus and firewalls and is instrumental in managing the device.

**Identity and Access Management (IAM):** includes the procedures and tools used to manage user identity and grant and restrict helpful access to information and other systems. IAM comprises identification, entitlements, and users.

**Incident response and recovery:** involve planning and executing measures to respond to cybersecurity incidents, such as data breaches or malware attacks. The information is followed by the desire to reduce the consequences, bring things back to as close to 'normal' as possible, and avoid similar events in the future.

**Cloud security protects:** data, applications, and structures in the cloud computing environment. Since modern organizations' business operations and information are mainly conducted and kept in cloud environments, protecting cloud assets has emerged as one of the primary strategic challenges of businesses in the field of cybersecurity. Some of the perspectives of cloud security are identity and access management, encryption, data transmission, and conformity to rules and regulations.

**Zero Trust:** is based on the principle that no one should be trustworthy, whether a user, device, Position, or Network. This approach involves constantly validating the user account details, the device's status, and adherence to the security standards that the device and its user must meet, thus decreasing the vulnerability to intruders and information leakage.

**Extended Detection and Response (XDR):** formerly EDR, this approach unites several highlighted solutions, including Endpoint Detection and Response, Network Traffic Analysis, or Security Information and Event Management tools, to present a larger and more active wall against possible threats.

**Privacy-enhancing technologies:** Due to the threat of data privacy and government regulations, technologies like differential privacy and homomorphic encryption are more widely used. They also allow users to maintain confidentiality in their communications, making it possible to process data with such systems without violating, for example, the GDPR.
Studying these subdomains and attending to their updates will help enhance knowledge in cybersecurity and familiarize one with the growing and rather acute problem of personal protection from dangers in the virtual world.

## Threat Landscape

The ever-changing risks posed by hackers, cybercriminals, and other malevolent entities targeting people, companies, and governments are called the cybersecurity threat landscape.

New dangers and attacks based on artificial intelligence are emerging because understanding these threats helps create better security tactics.

The increase in digitalization and automation in companies' and industries' capacities is a new source of targets and tactics for cybercriminals. The three challenges require organizations to develop proactive measures, embrace better protection technologies, and work together and set international criteria to protect innovation and security. Thus, they can realize AI's benefits and avoid harm.

## The main threats arising from or enhanced by the development of AI:

- **Automated and advanced phishing. Ransomware:** attackers use AI to create more sophisticated and personalized phishing campaigns, for example, to generate convincing messages aimed at specific malicious targets or to obtain sensitive data through deception.

- **Identity theft. Spoofing:** Low-cost, easy-to-use generative AI tools make it easier than ever for cybercriminals to impersonate the voice or image of a CEO, CFO, or company manager, developing deception strategies to induce subordinate employees to carry out specific actions through email, calls, or voice or video messages.

- **Deep fakes:** AI makes it possible to create hyper-realistic, manipulated content with the aim, among other things, of spreading false information that affects decisions or reputations.

- **Malware. N-Day and Zero-Day vulnerabilities:** AI-powered to adapt to the victim's environment and avoid detection: "Evasion techniques," which change their behavior or signature in real-time, or "Polymorphic malware," which constantly reconfigures itself to make it challenging to identify and exploit newly discovered vulnerabilities.

- **Targeted denial-of-service (DoS):** attacks identify system vulnerabilities and coordinate more effective attacks. AI provides cybercriminals with tools to generate advanced code that scans for vulnerabilities, bypasses DDoS protections, or enables the dynamic organization of botnets for distributed denial-of-service attacks.
- **Generative AI misuse refers to the use of AI-powered content generation technologies:** On the one hand, the growing Trust in such tools means that the results are not verified or reviewed, which can lead to the exfiltration of sensitive information. Above all, the use of malicious or ethically questionable activities is worrying.

## Attack Vectors

An attack vector is the method or pathway cybercriminals use to infiltrate a system. Common attack vectors include:

- **Email & Phishing Links:** Social engineering tactics trick users into revealing credentials.
- **Software Vulnerabilities:** Unpatched applications exploited by hackers.
- **Unsecured Networks:** Public Wi-Fi and weak encryption allow data interception.
- **Supply Chain Attacks:** Targeting third-party vendors to compromise an organization.

Artificial intelligence (AI) employs machine learning and intelligent algorithms to improve cyber threat identification, prevention, and response. AI can thus assist cybersecurity program structures in analyzing large volumes of data, finding trends, and reaching choices more quickly and efficiently than humans. Ensuring the safety, reliability, and moral application of AI systems is the focus of AI assurance. Crucial elements consist of:

- Transparency & Trust ensuring AI decisions are explainable and fair.
- Security in AI Models protecting AI from adversarial attacks, data poisoning, and model theft.
- Compliance & Governance following AI risk management frameworks (e.g., NIST AI RMF, ISO 42001).
- Bias Mitigation implementing measures to reduce AI discrimination and ensure fairness.
- A proactive approach to cybersecurity, combined with strong AI assurance principles, helps mitigate risks and safeguard digital assets from evolving threats.

### New cyber defense tools and services to reduce cyber attack

The range of options and services to improve security and reduce the risk of cyberattacks has expanded significantly.

### We mention some of the services and technologies that are beginning to be deployed:

- **AI-based detection systems:** Using defensive AI to identify anomalous behavior and threats in real-time. AI-based cybersecurity solutions provide a more sophisticated and practical means of identifying and thwarting online threats such as ransomware, malware, and phishing attempts. AI-based technologies help businesses respond to insider threats more quickly and effectively by analyzing user behavior and identifying anomalies and suspicious activity.

- **Multi-factor authentication (MFA):** Reduce the possibility of phishing attacks by making it difficult to access applications or platforms by introducing access control systems that require combined validation from the user through different methods, applications, and devices.

- **Continuous 360 monitoring. AI-based SIEM:** Deploy advanced tools to track and analyze activities on networks and systems with the detection of system behavior anomalies and intelligent correlation of security events

- **SOAR Platforms:** Security orchestration, automation, and response technology refers to how work involving multiple people and assets is orchestrated and completed.

- **Training and awareness:** Train users to identify signs of phishing or deep fakes.

## SESSION 2: SECURITY POLICIES AND PROCEDURES

This session concludes that organizations should increase their defense against cyber occurrences because they are progressive and evolving daily. Cyber incidents are invaluable assets that help businesses implement the proper measures and strategies regarding security and exercise the level of security consciousness in an organization.

Cyber security policies refer to several rules and practices an organization implements to guard its computer-based systems and reduce the likelihood of cyber risks. These policies define the standards and best practices that must be followed to ensure the security of information assets and business continuity. Businesses are exposed to cyberattacks, especially Small and medium-sized businesses (SMEs), which are increasingly vulnerable to cyberattacks. SMEs frequently lack the funding or skilled staff to implement cybersecurity policies and procedures.

The rising degree of digitization has made it necessary for businesses in every nation to have security measures for their data.

**IN THIS SESSION,** I will discuss laws and measures every business organization should adopt to counter cybercrimes.

**1. Make regular backups:** It is critical to have backups to restore the business's operations in case of a cyber-attack. Therefore, backups should always be current and kept safe. Regular testing is also necessary to ensure that backups are recoverable.

**2. Establish strong password policies:** Passwords are the first line of defense against cyberattacks. In addition to establishing secure password policies that include the creation of complex passwords and the obligation to change them periodically, it is essential to train the rest of the human capital so that they are aware of the dangers and the different methods that hackers use to violate the company's cybersecurity, using their terminals and accounts as a means of access. Ensure that you do not use a password that has been used before for any other website or app. However, you should also note that using MFA is a good practice as it can enhance the security of your accounts.

**3. Limit access to systems:** This is one of the main reasons why it is stated that only the workers who require access to the System should be allowed to use it. The System should provide suitable user privileges, monitor access privileges to prevent abuses and track abnormal system usage.

**4. Update systems and software regularly:** Software updates are crucial and applicable to the System, and device protection has become evident. They commonly apply new features and repair noted weaknesses and threats to the System's security. As we have seen, it is necessary to update the software periodically so as not to leave the opportunity to invade attackers.

**5. Raising awareness among employees about cybersecurity:** Cybersecurity is everyone's problem; employees can be the weakest link in your security chain. Make sure your team is trained to identify and report suspicious activity and is aware of the role they play in the importance of cybersecurity.

**6. Monitor and analyze network activity:** Monitoring and analyzing network activity is essential to detect and prevent potential cyber-attacks. A monitoring and analysis system must be established to detect suspicious activity and respond immediately.

**7. Implement privacy and data protection policies:** Remember that data protection and privacy are critical issues for any company. Implementing clear privacy and data protection policies is the quickest way to ensure compliance with applicable regulations and standards and prevent the company from becoming a victim of cyber threats.

While implementing these cybersecurity policies and procedures may seem expensive and complex, the cost of recovering from a cyberattack can be much greater than the cost of implementing preventative security measures.

The business world faces increasing cyber risks, and establishing cybersecurity measures can minimize cyber-attacks and protect the integrity and continuity of your business.

## RISK MANAGEMENT AND VULNERABILITY ASSESSMENT

### Risk Management

Cybersecurity risk management is the systematic procedure of recognizing, evaluating, assessing, and controlling risks connected with information security. It also implements options or measures to prevent threats and successfully minimize them.

Risk management is present in all company areas to a greater or lesser extent. However, what is common to all is that those in charge understand which risks lie ahead and can compromise the set goals.

### Stages of Cybersecurity Risk Management

**Thus, cybersecurity risk management can be divided into four steps**

**1. Risk recognition:** First and foremost, an organization has to have an idea or be aware that such risks are present. Therefore, the first step in the cybersecurity risk management process is to assess an organization's IT environment and security infrastructure to determine the risks that may be present and need to be managed.

**2. Evaluate:** It was argued that various risks affect an organization's operation differently. For instance, those attacking key resources, such as the corporate database server, will be considered more dangerous than the internal employees' workstations and other less significant systems. Risk can be measured depending on the probability and severity of the threat, and threats can be accordingly prioritized by degree, where degree is a combination of likelihood and severity.

**3. Mitigate:** An organization can tackle these risks after preparing a list in order of priority. Risk management may adopt four general approaches: remediation, mitigation, transfer, and acceptance.

**4. Review:** an organization should evaluate and monitor all risks and assess the efficiency of existing controls from time to time. This enables a firm to update risk priorities and adapt to the fact that some controls are failing or have emerged as new risks.

## The vulnerability management process

Because new vulnerabilities can emerge anytime, security teams approach vulnerability management as a continuous lifecycle rather than a one-time event. The five ongoing and overlapping workflows comprise this lifecycle: detection, classification and prioritizing, resolution, reassessment, and reporting.

**1. Recognition:** The detection process involves vulnerability assessment, identifying known and potential weaknesses of the organization’s IT assets. Generally, the security team performs this task through the help of a vulnerability scanning tool. Some vulnerability scanners use agents installed in the laptops, routers, and other endpoints to provide information about the various gadgets. In contrast, others make network scans comprehensive within a particular time, usually at regular intervals. Penetration testing is also conducted to perform episodic vulnerability assessment where other types of vulnerability can be identified, like those that a scanner does not detect.

**2. Categorization and prioritization:** Once known, they are categorized based on the vulnerability category (for instance, device misconfigurations, encryption issues, exposure of sensitive data) and the level of the risks. After this process, the rating of severity, exploit, and likelihood of an attack regarding every vulnerability is determined.

Threat intelligence is also typically used to determine the severity of known vulnerabilities on a scale of 0 to 10, using the Common Vulnerability Scoring System (CVSS), an open-source industry standard. The other two widely used intelligence sources are MITER's CVE list and the National Vulnerabilities Database, which NIST maintains.

**3. Resolution:** Once the vulnerabilities are prioritized then, the security teams can address them in three ways;

- **Remediation:** Partly manage a risk so that it may be utilized, for instance, by fixing a software glitch or removing an endangered asset. Some vulnerability management tools contain remediation aids in patch downloads, patch testing, and network and device configuration misconfiguration from the vulnerability management office or portal.
- **Mitigation:** involves making a vulnerability less easy to access and decreasing the harm that results from doing so without eliminating the vulnerability. An example of mitigation is making the vulnerable device connected to the Internet but separate from all the other devices. Mitigation is usually done when a patch or another remedy has not yet been developed.
- **Acceptance:** Failure to deal with a vulnerability. Lower risk factors with simple criticality ratings are often accepted, as they are unlikely to be attacked or, if they were attacked, would not result in severe consequences.

**4. Reassessment:** After vulnerabilities are fixed, a new vulnerability scan verifies that the security team's fix did not create new holes.

**5. Reports:** Vulnerability management solutions commonly offer dashboards management solutions frequently provide dashboards for reporting data such as mean. Many systems additionally save databases of vulnerabilities fundable to security teams from monitoring the vulnerability remediation and previous vulnerability management initiatives. Many security teams may use these reporting tools to track program effectiveness over time and provide a baseline for continuing vulnerability control efforts. Reports can also help pass information to the rest of the security and other IT personnel who may handle asset management but not the vulnerability management process.

## LAB: CONDUCTING A BASIC VULNERABILITY SCAN (USING NESSUS/OPENVAS)

## MATERIALS: LAB GUIDE, VULNERABILITY SCANNER ACCESS