Cybersecurity: The protection of digital devices and their communication channels to keep them stable, dependable and reasonably safe from danger or threat. Usually, the required protection level must be sufficient to prevent or address unauthorized access or before it can lead to substantial personal, professional, organizational, financial and/or political harm.

Digital Device: Any electronic appliance that can create, modify, archive, retrieve or transmit information in an electronic format. Desktop computers, laptops, tablets, smartphones and Internet-connected home devices are all examples of digital devices.

Cyber Crime: Any tradition crime that can happen using ICT can be regarded as a cyber-crime.

Cyber Attack: To take aggressive or hostile action by leveraging or targeting digital devices. The intended damage is not limited to the digital (electronic) environment.

Cyber Warfare: Cyberwarfare is the use of digital attacks to attack a nation, causing comparable harm to actual warfare and/or disrupting the vital computer systems. Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

Cyber Espionage: The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization. Cyber espionage is a form of cyber-attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.

Cyber Insecurity: Suffering from a concern that weaknesses in one’s cyber security are going to cause one’s personal or professional harm.

Hacker: A person who engages in attempts to gain unauthorized access to one or more digital devices.

Ethical Hacking: The process by which supportive penetration testing experts assist in finding security weaknesses and vulnerabilities.

Red Team: When testing for potential exploits affecting any critical or sensitive system, infrastructure or website, a team of penetration testers is usually used. This term (red team) is used to describe the group of penetration testers working together on this type of objective.

Ethical Hacker: An alternative name for a penetration tester.

Virus: A form of malicious software that spreads by infecting (attaching itself) to other files and usually seeks opportunities to continue that pattern. Viruses are now less common than other forms of malware. Viruses were the main type of malware in very early computing. For that reason, people often refer to something as a virus when it is technically another form of malware.

Malware: Shortened version of malicious software. A term used to describe the insertion of disruptive, subversive or hostile programs onto a digital device. These types of programs can be intentional or unintentional. Intentional versions are usually disguised or embedded in a file that looks harmless. There are many types of malwares; adware, botnets, computer viruses, ransomware, scareware, spyware, trojans and worms are all examples of intentional malware. Hackers often use malware to mount cybersecurity attacks.

Botnet: Shortened version of robotic network. A connected set of programs designed to operate together over a network (including the Internet) to achieve specific purposes. The purpose can be good or bad. Some programs of this type are used to help support Internet connections; malicious uses include taking over control of some or all of a computer's functions to support large-scale service attacks. Botnets are sometimes referred to as a zombie army.

Ransomware: A form of malicious software (malware) that prevents or restricts usage of one or more digital devices or applications or renders a collection of electronic data unreadable until a sum of money is paid. It simulates traditional ransom. For example, WannaCry (2017).

Spyware: A form of malware that covertly gathers and transmits information from the device on which it is installed. Example: Pegasus

Phishing: Using an electronic communication (for example email or instant messaging) that pretends to come from a legitimate source, in an attempt to get sensitive information (for example, a password or credit card number) from the recipient or to install malware on the recipient's device. The methods used in phishing have evolved so that the message can simply contain a link to an Internet location where malware is situated or can include an attachment (such as a PDF or Word document) that installs malware when opened. The malware can then be used to run any number of unauthorized functions, including stealing information from the device, replicating additional malware to other accessible locations, sharing the user screen and logging keyboard entries made by the user. Less complex forms of phishing can encourage the recipient to visit a fake but convincing version of a website and to disclose passwords or other details.

Spear Phishing: A more targeted form of phishing. This term describes the use of an electronic communication (for example, email or instant messaging) that targets a particular person or group of people (for example, employees at a location) and pretends to come from a legitimate source. In this case, the source may also pretend to be someone known and trusted to the recipient, in an attempt to obtain sensitive information (for example, a password or credit card number).

Spoofing: Concealing the true source of electronic information by impersonation or other means. Often used to bypass Internet security filters by pretending the source is from a trusted location.

Social Engineering Attack: It is the art of manipulating people through personal interaction to gain unauthorized access to something.

The act of constructing relationships, friendships or other human interactions for the purpose of enticing the recipient to perform an action or reveal information. The individual(s) doing the social engineering use the victim's action or information for the hidden purpose of achieving a nefarious objective, such as acquiring intelligence about the security, location or vulnerability of assets, or even gaining the person's trust to open an Internet link or document that will result in a malware foothold being created.

Denial of Service (DoS): An attack designed to stop or disrupt peoples' use of organizations' systems. Usually, a particular section of an enterprise is targeted; for example, a specific network, system, digital device type or function. These attacks usually originate from, and are targeted at, devices accessible through the Internet. If the attack is from multiple source locations, it is referred to as a Distributed Denial of Service, or DDoS attack.

Vulnerability: (in the context of cybersecurity) a weakness that could be compromised and result in damage or harm.

Vector: Another word for 'method' – as in 'They used multiple vectors for the attack.'

Exploit: To take advantage of a security vulnerability. Well-known exploits are often given names. Falling victim to a known exploit with a name can be a sign of low security, such as poor patch management.

Zero-day: It refers to the very first time a new type of exploit or new piece of malware is discovered. At that point in time, none of the anti-virus, anti-malware or other defenses may be set up to defend against the new form of exploit.

Backdoor: A covert method of accessing software or a device that bypasses the normal authentication requirements.

Threat Actors: An umbrella term to describe the collection of people and organizations that work to create cyber-attacks. Examples of threat actors can include cyber criminals, hacktivists and nation states.

Anti-malware: It is a computer program designed to look for specific files and behaviors (signatures) that indicate the presence or the attempted installation of malicious software. If or when detected, the program seeks to isolate the attack (quarantine or block the malware), remove it, if it can, and also alert appropriate people to the attempt or to the presence of the malware. The program can be host-based (installed on devices that are directly used by people) or network-based (installed on gateway devices through which information is passed). Older forms of this software could detect only specific, pre-defined forms of malicious software using signature files. Newer forms use machine learning and make use of additional techniques including behavior monitoring.

Signatures: Signatures (in the context of cybersecurity) are the unique attributes – for example, file size, file extension, data usage patterns and method of operation – that identify a specific computer program. Traditional anti- malware and other security technologies can make use of this information to identify and manage some forms of rogue software or communications.

Defense in Depth: The use of multiple layers of security techniques to help reduce the chance of a successful attack. The idea is that if one security technique fails or is bypassed, there are others that should address the attack. The latest (and correct) thinking on defense in depth is that security techniques must also consider people and operations factors and not just technology.

Incident Response: A prepared set of processes that should be triggered when any known or suspected event takes place that could cause material damage to an organization. The typical stages are

- verify the event is real and identify the affected areas,
- contain the problem (usually by isolating, disabling or disconnecting the affected pieces),
- understand and eradicate the root cause,
- restore the affected components to their fixed state and
- review how the process went to identify improvements that should be made.

Breach Notification Procedure: Some types of information, when suspected or known to be lost or stolen, must, by law, be reported to one or more authorities within a defined time period. The required notification time period varies by regulator, but is often within 24 hours. In addition to reporting the known or suspected loss, the lead organization responsible for the information (referred to as the data owner) is also required to swiftly notify those affected, and later on, to submit a full root cause analysis and information about how they have responded and fixed the issues. To meet these legal obligations, larger companies usually have a pre-defined breach notification procedure to ensure that the timelines are met. The fines for data breaches are usually increased or decreased based on the adequacy of the organization's breach and incident response management.

Secure Configuration: It is a process ensuring that when settings are applied to any item (device or software), appropriate steps are always taken to ensure

- default accounts are removed or disabled,
- shared accounts are not used and
- all protective and defensive controls in the item use the strongest appropriate setting(s).

Penetration Test: Checks and scans on any application, system or website to identify any potential security gaps (vulnerabilities) that could be exploited. Once the vulnerabilities are identified, this process then goes on to identify the extent to which these vulnerabilities could be leveraged in an attack (the penetration possibilities). Usually, these checks are performed in a test area and emulate the same techniques that could be used by an attacker. This is to prevent any inadvertent operational disruption. The checks are typically conducted before any application or site is first used, and also on a periodic (repeating) basis; for example, each time the program is updated or every 6 months. Any significant gaps must be addressed (fixed) in a timeframe appropriate to the scale of the risk. Not to be confused with the term vulnerability assessment, which only identifies gaps without examining how they could be leveraged. Penetration tester is the person who performs simulated attempts at attack on a target system or application on behalf of the organization that owns or controls it.

Vulnerability Assessment: The identification and classification of security gaps in a computer, software application, network or other section of a digital landscape. This is usually a passive identification technique that aims only to identify the gaps, without exploring how those gaps could be used in an attack. This should not be confused with a penetration test, which may include information from a vulnerability assessment, but which will go on to explore how any vulnerabilities can be exploited.

Business Continuity Plan: An operational document that describes how an organization can restore its critical products or services to its customers, should a substantial event that causes disruption to normal operations occur.

Technical Disaster Recovery Plan: An operational document that describes the exact process, people, information and assets required to put any electronic or digital system back in place within a timeline defined by the business continuity plan.

Patch Management: A controlled process used to deploy critical, interim updates to software on digital devices. The release of a software 'patch' is usually in response to a critical flaw or gap that has been identified. Any failure to apply new interim software updates promptly can leave open security vulnerabilities in place. As a consequence, promptly applying these updates (patch management) is considered a critical component of maintaining effective cybersecurity.

Firewall: It is hardware (physical device) or software (computer program) used to monitor and protect inbound and outbound data (electronic information). It achieves this by applying a set of rules. These physical devices or computer programs are usually deployed, at a minimum, at the perimeter of each network access point. Software firewalls can also be deployed on devices to add further security. The rules applied within a firewall are known as the firewall policy. Advanced firewalls are often equipped with other defensive features typical of more unified threat management.

Chief Information Security Officer (CISO): A single point of accountability in any organization for ensuring that an appropriate framework for managing dangers and threats to electronic and physical information assets is operating and effective.

Policy:

- A high-level statement of intent, often a short document, that provides guidance on the principles an organization follows. For example, a basic security policy document could describe the intention for an enterprise to ensure that all locations (physical and electronic) where information for which they are accountable must remain secure from any unauthorized access. A policy does not usually describe the explicit mechanisms or specific instructions that would be used to achieve or enforce the intentions it expresses; this would be described in a procedure.
- Alternatively, it can also be used to mean the settings (including security settings) inside a software program or operating system.

Risk: A situation involving exposure to significant impact or loss. In formal frameworks, risk can be quantified using probability (often expressed as a percentage) and impact (often expressed as a financial amount). Other parameters for risk can include proximity (how soon a potential risk may be encountered, and information about which assets, services, products and processes could be affected).

Jurisdiction: Power of a court to adjudicate cases and issue orders. Territory within which a court or government agency may properly exercise its power.

It is also known as the authority given by law to a court to try cases and rule on legal matters within a particular geographic area and/or over certain types of legal cases. It is vital to determine before a lawsuit is filed which court has jurisdiction. State courts have jurisdiction over matters within that state, and different levels of courts have jurisdiction over lawsuits involving different amounts of money.