**900103-000-00-KM-01, Cyber Defence Introduction, NQF Level 4, Credits 7**

**LEARNER GUIDE**

**MODULE ONE (1)**

|  |  |
| --- | --- |
| **Module #** | 900103-000-00-KM-01 |
| **NQF Level** | 4 |
| **Notional hours** | 70 |
| **Credit(s)** | 7 |
| **Occupational Code** | 900103-000-00-00 |
| **SAQA QUAL ID** | SP - 220330 |
| **Qualification Title** | Cybersecurity Defender |

|  |  |
| --- | --- |
| **Name** |  |
| **Contact Address** |  |
| **Telephone (H)** |  |
| **Telephone (W)** |  |
| **Facsimile** |  |
| **Cellular** |  |
| **E-mail** |  |

**Note to the learner**

This Learner Guide provides a comprehensive overview of the module. It is designed to improve the skills and knowledge of learners, and thus enabling them to effectively and efficiently complete specific tasks.

**Purpose of the Module**

The main focus of the learning in this knowledge module is to build an understanding of the basics of cybersecurity including definitions, concepts, terminology and the adverse effect of cyber vulnerabilities on the safety and security of company information, data and systems. They will also understand the importance of a safe cybersecurity and threat posture of a company

The learning will enable learners to demonstrate an understanding of:

* KM-01-KT01 : Introduction to cybersecurity 30%
* KM-01-KT02 : Cybersecurity basics 20%
* KM-01-KT03 : Cybersecurity governance fundamentals 20%
* KM-01-KT04 : A cyber secure organisation 15%
* KM-01-KT05 : Basics of threat intelligence 15%

**Entry Requirements**

NQF 3 (Gr 11) with Computer Literacy, English and Math Lit

**Provider Accreditation Requirements for the Knowledge Module**

*Physical Requirements:*

* The provider must have lesson plans and structured learning material or provide learners with access to structured learning material that addresses all the topics in all the knowledge modules as well as the applied knowledge in the application modules
* QCTO/ MICT SETA requirements

*Human Resource Requirements:*

* Lecturer/learner ratio of 1:20 (Maximum)
* Qualification of lecturer (SME):

NQF 5 qualified in industry recognised qualifications with 1 years’ experience in the IT industry

Cybersecurity vendor certification

* Assessors and moderators: accredited by the MICT SETA

*Legal Requirements:*

* Legal (product) licences to use the software for learning and training
* OHS compliance certificate
* Ethical clearance (where necessary)

AM

*Physical Requirements:*

* Valid licenses software and application, including OS.
* Internet connection and hardware availability.
* Examples and information specified in the scope statement and all the case studies, scenarios and access to hardware and software implied in the scope statements of the modules.
* Remote learners: Provider must provide business IT simulation system (e.g. invoice processing).

*Human Resource Requirements:*

* Qualification of lecturer (SME):  
  o NQF 5 industry recognised qualification with 1 year relevant experience
* Assessors and moderators: accredited by the MICT SETA

*Legal Requirements:*

* + Legal (product) licences to use the software for learning and training
  + OHS compliance certificate
  + Ethical clearance (where necessary)

**Venue, Date and Time:**

Consult your facilitator should there be any changes to the venue, date and/or time.

Refer to your timetable.

**Assessments**

**Associated Assessment Criteria (AACs)**

* Basic governance principles and concepts related to cybersecurity are understood.
* Basic concepts and principles of cybersecurity are understood.
* Basic concepts and principles of cyber threats and attacks are understood.
* Basic concepts and principles of cyber defence are understood.
* Ethical considerations in ethical hacking and penetration testing are understood.
* Procedures to respond to cybersecurity incidents are understood.

**Associated Assessment Criteria (AACs)**

* User and host identities are verified.
* Mechanisms are put in place to prevent system intrusions.
* Automated tools are used to guard against intrusions.
* Network confidentiality is ensured.
* The security posture is evaluated to detect vulnerabilities and to enhance resilience.

**Associated Assessment Criteria (AACs)**

* Threats to the cybersecurity of the company are detected.
* Adversary techniques, tactics and practices (TTPs) are emulated
* using an emulation platform.
* Network traffic is monitored and analysed using a suitable platform.
* Incidents are identified, responded to and reported.

**Associated Assessment Criteria (AACs)**

* Foot-printing tools are used against a target and intelligence is gathered.
* Vulnerabilities are identified using penetration testing tools.
* Servers and devices are attacked to build better defences.
* Clients are manipulated to uncover internal threats.
* Targets are exploited to increase cybersecurity.

Antivirus and intruder detection systems (IDS) are tested

# PURPOSE OF THE QUALIFICATION

Cybersecurity Defenders are responsible for proactively protecting organisations’ systems from attacks, they are the first line of defence against cyberattacks, the first responders to cybersecurity breaches and are responsible for the hardening of the information systems of organisations ensuring compliance with legislation

# QUALIFICATION RULES

This Skills Programme consist of two components namely Knowledge/Theory component and Application component. The following are compulsory modules in each of the two components:

**Knowledge/Theory Component:**

The following Modules are compulsory:

* 900103-000-00-KM-01, Cyber Defence Introduction, NQF Level 4, Credits 7
* 900103-000-00-KM-02, Cyber Threats and Attacks, NQF Level 4, Credits 7
* 900103-000-00-KM-03, Cybersecurity, NQF Level 4, Credits 7
* 900103-000-00-KM-04, Responding to Cybersecurity Incidents, NQF Level 4, Credits 5

Total number of credits for Knowledge Component: 26

**Application Component:**

* 900103-000-00-PM-01, Protect against cybersecurity threats, intrusions and attacks, NQF Level 4, Credits 11
* 900103-000-00-PM-02, Detect cybersecurity threats, intrusions and attacks, NQF Level 4, Credits 11
* 900103-000-00-PM-03, Conduct Penetration Testing Techniques to Determine Security, NQF Level 4, Credits 12

Total number of credits for Application Component: 34

# EXIT LEVEL OUTCOMES

**Exit Level Outcomes (ELO) 1**

Demonstrate knowledge and understanding of cybersecurity, cyber

threats and attacks and cyber defence

**Exit Level Outcomes (ELO) 2**

Protect against cybersecurity intrusions and attacks

**Exit Level Outcomes (ELO) 3**

Detect cybersecurity threats and attacks

**Exit Level Outcomes (ELO) 4**

Use different penetration testing tools to identify vulnerabilities in the security posture of an organisation

# KM-01-KT01: Introduction to cybersecurity 30%

**Topic elements to be covered include:**

* KT0101 Concepts, principles and terminology
* KT0102 Definition of cybersecurity
* KT0103 What is hacking?
* KT0104 What is ethical hacking?
* KT0105 Definition of cyberattacks, incidents and data breaches
* KT0106 Definition of cyber resilience
* KT0107 Reasons for cybersecurity
* KT0108 Who is the target (of cyberattacks): Individuals, groups, organisations and governments

**KT0101 Concepts, principles and terminology**

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.

Computer security, cyber security , digital security or information technology security (IT security) is the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide.

The field is significant due to the expanded reliance on computer systems, the Internet, and wireless network standards such as Bluetooth and Wi-Fi. Also, due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is one of the most significant challenges of the contemporary world, due to both the complexity of information systems and the societies they support. Security is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance.

Cybersecurity is the practice of protecting computer systems, networks, and data from security breaches, unauthorized access, and damage caused by cyber threats such as hackers, viruses, and other malicious actors. It encompasses a wide range of concepts, principles, and terminology. Here are some key ones:

1. **Confidentiality**: Ensuring that sensitive information is accessible only to authorized individuals or entities and is protected from unauthorized disclosure.
2. **Integrity**: Maintaining the accuracy, completeness, and consistency of data and preventing unauthorized alteration or tampering.
3. **Availability**: Ensuring that information and resources are available and accessible to authorized users when needed, and minimizing downtime due to cyber attacks or technical failures.
4. **Authentication**: Verifying the identity of users or entities attempting to access a system or data, often through passwords, biometrics, or multi-factor authentication (MFA).
5. **Authorization**: Granting appropriate access privileges to authorized users based on their roles and responsibilities.
6. **Encryption**: The process of converting data into a code to prevent unauthorized access during transmission or storage. It ensures that even if intercepted, the data remains unreadable without the decryption key.
7. **Firewall**: A network security device that monitors and controls incoming and outgoing network traffic, acting as a barrier between a trusted internal network and untrusted external networks, such as the Internet.
8. **Intrusion Detection System (IDS)**: A security mechanism that monitors network traffic for suspicious activity and alerts administrators of potential security breaches.
9. **Intrusion Prevention System (IPS)**: A security device or software that actively monitors and blocks malicious network traffic or attempts at unauthorized access.
10. **Malware**: Short for "malicious software," it refers to any software specifically designed to harm or exploit computer systems or networks. Examples include viruses, worms, Trojans, ransomware, and spyware.
11. **Phishing**: A social engineering technique where attackers use deceptive emails, messages, or websites to trick individuals into revealing sensitive information, such as login credentials or financial details.
12. **Vulnerability**: A weakness or flaw in a system's design, implementation, or configuration that could be exploited by attackers to compromise its security.
13. **Patch**: A software update or fix released by vendors to address security vulnerabilities and improve system performance.
14. **Zero-Day Exploit**: An attack that targets a previously unknown vulnerability, which gives victims no time to prepare or patch before the attack occurs.
15. **Social Engineering**: The manipulation of individuals through psychological tactics to trick them into divulging sensitive information or performing actions that compromise security.
16. **Endpoint Security**: The protection of devices such as computers, laptops, smartphones, and other endpoints from cyber threats.
17. **Data Breach**: The unauthorized access, acquisition, or disclosure of sensitive information, often involving the loss or theft of data.
18. **Penetration Testing**: Also known as "pen testing," it involves authorized simulated attacks on a system to identify vulnerabilities and weaknesses in its security measures.
19. **Incident Response**: The process of handling and managing security incidents, including identifying, containing, eradicating, and recovering from cyber attacks.
20. **Security Policy**: A set of guidelines and rules that define the organization's approach to cybersecurity, including roles, responsibilities, and acceptable use of resources.

These are just a few essential concepts and principles in cybersecurity. As technology and threats evolve, the field of cybersecurity continues to develop and adapt to protect against new challenges.

**KT0102 Definition of cybersecurity**

Cybersecurity, also known as computer security or IT security, refers to the practice of protecting computer systems, networks, and data from security breaches, unauthorized access, and damage caused by cyber threats such as hackers, malware, viruses, and other malicious actors. The main objective of cybersecurity is to ensure the confidentiality, integrity, and availability of information and resources, while also preventing and mitigating potential cyber attacks.

It involves a combination of technologies, processes, and practices that are designed to safeguard digital assets and defend against a wide range of threats and vulnerabilities that exist in the interconnected world of computer systems and networks. Cybersecurity measures encompass various strategies such as using firewalls, encryption, access controls, intrusion detection systems, regular software updates, employee training, and incident response protocols to effectively protect against potential cyber threats.

As the digital landscape continues to evolve, the importance of cybersecurity has grown significantly to counteract the increasing sophistication and frequency of cyber attacks. It plays a critical role in safeguarding sensitive information, critical infrastructure, financial systems, and various other aspects of modern society that rely heavily on technology and the internet.

**KT0103 What is hacking?**

Hacking is the act of gaining unauthorized access to computer systems, networks, or digital devices with the intent to manipulate, disrupt, or steal information. A person who engages in hacking is often referred to as a "hacker."

Hacking can have both positive and negative connotations, depending on the intentions and actions of the individual involved:

1. **Ethical Hacking**: Ethical hacking, also known as "white-hat hacking" or "penetration testing," involves legally and legitimately attempting to exploit vulnerabilities in computer systems or networks with the permission of the system owner. Ethical hackers aim to identify and fix security weaknesses to help improve the overall security of the target system.
2. **Malicious Hacking**: This type of hacking involves unauthorized access to systems or networks for nefarious purposes. Malicious hackers, also known as "black-hat hackers," may engage in activities such as stealing sensitive information, distributing malware, launching DDoS (Distributed Denial of Service) attacks, or causing other harm.
3. **Hacktivism**: Hacktivism combines hacking with activism, where hackers use their skills to promote a social or political cause. Hacktivists may deface websites, leak sensitive information, or disrupt online services to draw attention to their cause.
4. **Cracking**: "Cracking" is a term often used interchangeably with malicious hacking, specifically referring to attempts to bypass software security measures to gain unauthorized access or remove software protections.
5. **Script Kiddies**: These are individuals with limited technical skills who use pre-made hacking tools and scripts to launch basic attacks without fully understanding the techniques involved.

It's important to note that engaging in malicious hacking is illegal and unethical, as it violates the privacy and security of others' digital assets. Governments and organizations worldwide have laws and penalties in place to deter and punish illegal hacking activities.

However, ethical hacking plays a crucial role in cybersecurity, as it helps identify and address vulnerabilities before malicious hackers can exploit them. Ethical hackers are often employed by companies, organizations, or governments to assess their security posture and ensure that their systems and networks are adequately protected against potential cyber threats.

**KT0104 What is ethical hacking?**

Ethical hacking, also known as "white-hat hacking" or "penetration testing," is the practice of intentionally and legally attempting to exploit vulnerabilities in computer systems, networks, or applications to identify and address security weaknesses. Ethical hackers, often hired by organizations, use their skills and knowledge to assess the security posture of systems, with the ultimate goal of improving overall cybersecurity.

Key aspects of ethical hacking include:

1. **Authorization**: Ethical hackers always work with explicit permission from the system owner or organization. This ensures that their activities are legal and authorized.
2. **Identifying Vulnerabilities**: Ethical hackers systematically examine and analyze systems and networks to find potential vulnerabilities that could be exploited by malicious hackers. These vulnerabilities could include weak passwords, unpatched software, misconfigurations, or other security flaws.
3. **Testing and Exploiting**: Once potential vulnerabilities are identified, ethical hackers attempt to exploit them to demonstrate the impact of a successful attack. This step helps organizations understand the severity of the vulnerabilities and the potential consequences of a real cyber attack.
4. **Reporting and Remediation**: Ethical hackers document their findings and provide detailed reports to the organization's management or IT/security team. These reports include recommendations and steps to mitigate the identified vulnerabilities and enhance overall security.
5. **Continuous Improvement**: Ethical hacking is part of an ongoing cybersecurity strategy. As technology evolves and new threats emerge, regular assessments help organizations stay vigilant and resilient against potential cyber threats.

The benefits of ethical hacking include:

* **Enhancing Security**: By identifying and fixing vulnerabilities, ethical hacking helps organizations strengthen their security measures and protect against potential cyber attacks.
* **Compliance and Regulation**: Ethical hacking can help organizations meet compliance requirements and adhere to industry regulations regarding data protection and security.
* **Cost-Effectiveness**: Proactively addressing security vulnerabilities through ethical hacking can be more cost-effective than dealing with the aftermath of a successful cyber attack.
* **Reputation Protection**: Demonstrating a commitment to cybersecurity through ethical hacking can enhance an organization's reputation, especially when clients and customers trust that their data is handled securely.

Ethical hacking plays a crucial role in the overall cybersecurity landscape, complementing other security measures such as firewalls, encryption, and employee training. It helps create a proactive and resilient defense against cyber threats in an increasingly digital and interconnected world.

**KT0105 Definition of cyberattacks, incidents and data breaches**

1. **Cyberattacks**:

Cyberattacks are deliberate, malicious actions taken by individuals or groups to exploit vulnerabilities in computer systems, networks, or digital devices. The objective of a cyberattack is to compromise the security of the target and cause harm or gain unauthorized access to sensitive information. Cyberattacks can take various forms and may include:

* **Malware**: The deployment of malicious software, such as viruses, worms, Trojans, ransomware, or spyware, to disrupt, steal data, or gain unauthorized access.
* **Phishing**: The use of deceptive emails, messages, or websites to trick individuals into revealing sensitive information, such as login credentials or financial details.
* **Denial of Service (DoS) / Distributed Denial of Service (DDoS)**: Overloading a system or network with excessive traffic to make it unavailable to legitimate users.
* **Man-in-the-Middle (MitM)**: Intercepting and potentially modifying communications between two parties without their knowledge.
* **SQL Injection**: Exploiting vulnerabilities in web applications to gain unauthorized access to databases or execute malicious commands.
* **Zero-Day Exploits**: Targeting previously unknown vulnerabilities for which no patch or fix is available.

1. **Incidents**:

In the context of cybersecurity, an incident refers to any adverse event or suspected violation of security policies, procedures, or acceptable use policies that may compromise the confidentiality, integrity, or availability of information, systems, or networks. Incidents can be the result of cyberattacks, accidental actions, or system malfunctions. They include:

* **Security Incidents**: Events caused by unauthorized access attempts, data breaches, malware infections, or other malicious activities.
* **Operational Incidents**: Non-malicious events, such as accidental data loss, hardware failures, or software glitches, that impact the normal functioning of systems.
* **Policy Violations**: Incidents involving violations of security policies, acceptable use policies, or other guidelines set by an organization.

1. **Data Breaches**:

A data breach is a specific type of cybersecurity incident where sensitive or confidential information is exposed, accessed, or stolen by unauthorized individuals. It may involve personal data, financial information, intellectual property, or other sensitive records. Data breaches can occur due to cyberattacks, human errors, or system vulnerabilities. Once a data breach occurs, the compromised data may be sold on the dark web or used for identity theft, financial fraud, or other malicious purposes.

Organizations have a legal and ethical responsibility to notify affected individuals and take appropriate measures to mitigate the impact of data breaches when they occur.

Overall, the terms "cyberattacks," "incidents," and "data breaches" are interconnected and are crucial components of the cybersecurity landscape. Understanding them helps organizations and individuals respond effectively to security threats and protect their digital assets and sensitive information.

**KT0106 Definition of cyber resilience**

Cyber resilience refers to an organization's ability to prepare for, respond to, and recover from cyber threats, incidents, and disruptions effectively. It is a comprehensive approach that focuses on maintaining the availability, integrity, and confidentiality of information, systems, and services even in the face of cyberattacks or other adverse events. Cyber resilience goes beyond traditional cybersecurity measures by incorporating elements of risk management, incident response, business continuity, and organizational agility.

Key aspects of cyber resilience include:

1. **Preparedness**: Proactively identifying and understanding potential cyber risks and vulnerabilities within an organization's IT infrastructure, applications, and processes. This involves implementing security controls, regular risk assessments, and employee training to enhance the organization's overall security posture.
2. **Detection and Response**: The ability to quickly detect and respond to cyber incidents when they occur. This includes having advanced monitoring tools, security analytics, and incident response plans in place to minimize the impact of cyber threats and prevent further escalation.
3. **Business Continuity**: Having plans and procedures in place to maintain critical business functions and operations during and after a cyber incident. Cyber resilience ensures that the organization can continue to deliver essential services to its customers while dealing with the aftermath of a cyber event.
4. **Redundancy and Backups**: Implementing redundancy and regular data backups to ensure that critical information and systems can be restored in the event of data loss or system compromise.
5. **Adaptability and Learning**: A cyber-resilient organization continuously learns from past incidents and adapts its security measures to stay ahead of evolving cyber threats. It embraces a culture of ongoing improvement and strives to build a more robust and agile security posture.
6. **Collaboration**: Cyber resilience involves coordination and collaboration among different departments within an organization, as well as partnerships with external stakeholders, such as government agencies, industry peers, and cybersecurity experts.

The concept of cyber resilience acknowledges that cyber threats are inevitable and that no organization can be completely immune to attacks. Therefore, it focuses on reducing the impact of cyber incidents and ensuring a timely recovery to minimize downtime and financial losses. By embracing cyber resilience, organizations can better protect their assets, reputation, and customer trust in an ever-changing and challenging cybersecurity landscape.

**KT0107 Reasons for cybersecurity**

Cybersecurity is essential for several reasons, as the digital world becomes increasingly interconnected and dependent on technology. Here are some of the key reasons for cybersecurity:

1. **Protection of Sensitive Information**: Cybersecurity safeguards sensitive data such as personal information, financial records, intellectual property, trade secrets, and confidential business data from unauthorized access, theft, or misuse.
2. **Prevention of Data Breaches**: Cybersecurity measures help prevent data breaches, where large amounts of sensitive information can be compromised and exposed to unauthorized individuals, potentially leading to identity theft, financial fraud, and other malicious activities.
3. **Defense Against Cyber Attacks**: Cybersecurity protects computer systems, networks, and digital devices from various cyber threats, such as malware, ransomware, phishing attacks, and denial-of-service (DoS) attacks, which can disrupt operations and cause significant financial and reputational damage.
4. **Safeguarding Critical Infrastructure**: Cybersecurity is crucial for protecting critical infrastructure, including power grids, water systems, transportation networks, and communication systems, from cyber attacks that could have severe consequences for public safety and national security.
5. **Preservation of Business Continuity**: Cybersecurity measures help maintain business continuity by preventing disruptions to operations caused by cyber incidents. Recovering from cyber attacks can be time-consuming and expensive, making prevention and preparedness essential.
6. **Compliance with Regulations**: Many industries have specific cybersecurity regulations and data protection laws that organizations must adhere to. Implementing strong cybersecurity measures ensures compliance with these regulations and avoids potential legal consequences.
7. **Protection of Intellectual Property**: Cybersecurity helps safeguard intellectual property, such as patents, trade secrets, and proprietary technology, from theft or unauthorized access, which can have significant financial implications for businesses.
8. **Preservation of Customer Trust**: Demonstrating a commitment to cybersecurity instills confidence in customers and clients that their sensitive information is being handled securely. Maintaining trust is crucial for businesses to thrive in today's digital economy.
9. **National Security**: Cybersecurity is essential for protecting a nation's critical infrastructure, government systems, and military networks from cyber threats launched by nation-states or other malicious actors.
10. **Prevention of Reputation Damage**: A successful cyber attack can lead to negative media coverage and damage an organization's reputation. Cybersecurity helps avoid such incidents, protecting an organization's brand and public image.

Overall, cybersecurity is a vital investment for individuals, businesses, governments, and organizations of all sizes to protect against cyber threats and ensure the safe and secure use of technology in our increasingly digital world.

**KT0108 Who is the target (of cyberattacks): Individuals, groups, organisations and governments**

Cyberattacks can target various entities, including individuals, groups, organizations, and governments. The motives behind cyberattacks can vary widely, ranging from financial gain and data theft to political activism and espionage. Here's how each of these entities can be the target of cyberattacks:

1. **Individuals**: Individual users are often targeted through techniques like phishing, social engineering, or the use of malicious software (malware). Cybercriminals may try to steal personal information, financial data, login credentials, or even gain access to personal devices and accounts.
2. **Groups and Organizations**: Businesses, non-profit organizations, and other groups can be targets of cyberattacks. These attacks can aim to steal sensitive business data, disrupt operations, extort money through ransomware attacks, or gain a competitive advantage through corporate espionage.
3. **Governments**: Governments and their agencies are attractive targets for cyber attacks due to the potential impact on national security, critical infrastructure, and sensitive government data. State-sponsored attacks can target other nations for espionage or sabotage purposes.
4. **Critical Infrastructure**: Critical infrastructure, such as power grids, water supply systems, transportation networks, and healthcare facilities, is a prime target for cyberattacks. Disrupting these systems can have severe consequences for public safety and national security.
5. **Financial Institutions**: Banks, financial services, and payment processors are often targeted by cybercriminals seeking to steal financial information, commit fraud, or launch large-scale attacks to disrupt financial operations.
6. **Healthcare Sector**: The healthcare sector is a valuable target for cybercriminals due to the value of patient records and sensitive medical data. Ransomware attacks on healthcare providers have become increasingly common.
7. **Academic Institutions**: Educational institutions may be targeted for various reasons, including stealing research data, personal information of students and staff, or to disrupt operations.
8. **Political and Activist Targets**: Cyberattacks against political entities, activists, or government opponents may aim to gather intelligence, spread disinformation, or disrupt their activities.

It's important to note that the motivations behind cyberattacks can vary widely, and the targets may change based on the attackers' objectives. Regardless of the target, the importance of cybersecurity measures and practices cannot be overstated, as cyber threats continue to evolve and pose significant risks to all entities operating in the digital realm.

***Internal Assessment Criteria and Weight***

* IAC0101 Cybersecurity concepts and principles are explained using correct terminology.
* IAC0102 The aim and function of cybersecurity and cyber resilience are described.
* IAC0103 The impact of cyberattacks, incidents and data breaches on companies is analysed.
* IAC0104 Reasons for attacking specific targets are given.

***(Weight 30%)***

# KM-01-KT02 : Cybersecurity basics 20%

**Topic elements to be covered include:**

* KT0201 Understanding cyber threats (internal vs external)
* KT0202 Threats that impact cybersecurity
* KT0203 Understanding that threats materialise into attacks
* KT0204 Different types of hackers
* KT0205 How individuals are targeted by hackers
* KT0206 Man-in-the-middle attack

**KT0201 Understanding cyber threats (internal vs external)**

Understanding cyber threats involves recognizing the sources and origins of potential attacks, with two primary categories being internal threats and external threats:

1. **Internal Threats**:

Internal threats refer to cybersecurity risks that originate from within an organization or entity. These threats can arise from current or former employees, contractors, or anyone with authorized access to the organization's systems and data. Internal threats can be intentional or unintentional and can pose significant risks to an organization's security.

Examples of internal threats include:

* **Insider Threats**: These involve employees or individuals with privileged access who misuse their authority or intentionally sabotage systems, data, or operations. Insider threats can result from malicious intent, disgruntlement, or unintentional mistakes.
* **Human Error**: Accidental actions by employees, such as clicking on phishing emails, mishandling sensitive data, or misconfiguring security settings, can lead to security vulnerabilities.
* **Data Leakage**: Unauthorized sharing or leaking of sensitive information by employees can expose the organization to reputational damage and legal consequences.
* **Privilege Abuse**: Misuse of administrative privileges or excessive access rights by employees can lead to unauthorized access to critical systems or data.

1. **External Threats**:

External threats refer to cybersecurity risks that come from outside the organization. These threats are posed by individuals, groups, or automated tools seeking to exploit vulnerabilities or gain unauthorized access to systems, networks, or data.

Examples of external threats include:

* **Hackers and Cybercriminals**: Malicious actors attempt to breach an organization's defenses to steal sensitive data, disrupt operations, or extort money through ransomware attacks.
* **Phishing and Social Engineering**: Cybercriminals use deceptive emails, messages, or phone calls to trick individuals into revealing sensitive information, such as login credentials or financial details.
* **Advanced Persistent Threats (APTs)**: Sophisticated and persistent attackers, often state-sponsored or well-funded groups, target specific organizations for espionage or long-term data theft.
* **Botnets and DDoS Attacks**: Botnets are networks of compromised computers controlled by attackers, often used for launching Distributed Denial of Service (DDoS) attacks to overwhelm websites or networks.
* **Zero-Day Exploits**: Attackers exploit previously unknown vulnerabilities in software before a patch or fix is available.
* **Supply Chain Attacks**: Threat actors compromise the supply chain, infecting software or hardware during the manufacturing or distribution process to infiltrate the target organization.

It's crucial for organizations to be aware of both internal and external threats and implement a comprehensive cybersecurity strategy that addresses these risks. This includes implementing access controls, training employees, regularly patching and updating systems, deploying intrusion detection systems, and having incident response plans in place to mitigate the impact of potential cyber threats.

**KT0202 Threats that impact cybersecurity**

Cybersecurity faces a wide range of threats that can impact the confidentiality, integrity, and availability of data and systems. These threats are constantly evolving, and new attack vectors emerge as technology advances. Here are some of the most common threats that impact cybersecurity:

1. **Malware**: Malware is malicious software designed to harm systems, steal data, or gain unauthorized access. It includes viruses, worms, Trojans, ransomware, spyware, and adware.
2. **Phishing**: Phishing attacks use deceptive emails, messages, or websites to trick individuals into revealing sensitive information, such as login credentials, financial details, or personal data.
3. **Ransomware**: Ransomware encrypts a victim's files or locks them out of their system, demanding a ransom payment in exchange for restoring access.
4. **Denial of Service (DoS) / Distributed Denial of Service (DDoS)**: DoS and DDoS attacks overwhelm systems or networks with excessive traffic, making them unavailable to legitimate users.
5. **Insider Threats**: Insider threats involve employees or individuals with privileged access who misuse their authority or intentionally sabotage systems and data.
6. **Advanced Persistent Threats (APTs)**: APTs are sophisticated and persistent attacks launched by well-funded adversaries, often aiming to steal sensitive data or gain long-term access to a target.
7. **Zero-Day Exploits**: Zero-day exploits target newly discovered vulnerabilities for which no patch or fix is available.
8. **SQL Injection**: SQL injection attacks manipulate databases through input vulnerabilities in web applications.
9. **Man-in-the-Middle (MitM)**: MitM attacks intercept and potentially modify communications between two parties without their knowledge.
10. **IoT Vulnerabilities**: Security weaknesses in Internet of Things (IoT) devices can be exploited to gain access to networks or cause disruptions.
11. **Social Engineering**: Social engineering techniques manipulate individuals into revealing sensitive information or performing actions that compromise security.
12. **Password Attacks**: Password attacks involve attempts to guess or crack passwords to gain unauthorized access to accounts or systems.
13. **Data Breaches**: Data breaches involve unauthorized access to sensitive information, potentially exposing personal or financial data.
14. **Supply Chain Attacks**: Threat actors compromise the supply chain, infecting software or hardware to infiltrate the target organization.
15. **Brute Force Attacks**: Brute force attacks try all possible combinations to guess passwords or encryption keys.
16. **Cross-Site Scripting (XSS)**: XSS attacks inject malicious scripts into websites, potentially compromising users' browsers.
17. **Eavesdropping**: Eavesdropping attacks intercept and monitor communications to capture sensitive information.
18. **Web Application Vulnerabilities**: Flaws in web applications, such as code injection or insecure direct object references, can be exploited to gain unauthorized access.
19. **Fileless Malware**: Fileless malware operates in memory, making it challenging to detect with traditional antivirus software.
20. **Physical Attacks**: Physical attacks on hardware or facilities can lead to data theft or system compromise.

As cyber threats continue to evolve, organizations must stay vigilant, implement robust security measures, and regularly update their defenses to protect against potential attacks. A proactive and comprehensive cybersecurity strategy is essential to safeguarding sensitive information and maintaining the trust of customers and stakeholders.

**KT0203 Understanding that threats materialise into attacks**

Cyber threats are potential risks or vulnerabilities that exist in computer systems, networks, or digital environments. When these threats are exploited or leveraged by malicious actors, they materialize into cyber attacks. In other words, an attack occurs when a threat is realized and exploited by an individual, group, or automated system with malicious intent.

For example, a common threat is the existence of a software vulnerability, such as an unpatched security flaw in a web application. If a hacker identifies this vulnerability and uses it to gain unauthorized access to the application or compromise its data, it becomes a cyber attack. The hacker exploits the existing threat (the unpatched vulnerability) to launch the attack.

Threats can come from various sources, including external attackers, insiders (such as disgruntled employees or contractors), or even accidental actions by users. Different cyber attack techniques are used to exploit different types of threats, aiming to achieve specific objectives such as data theft, service disruption, financial gain, or espionage.

Understanding the connection between threats and attacks is crucial for cybersecurity professionals to proactively identify and mitigate vulnerabilities, implement robust security measures, and respond effectively to incidents. By staying ahead of potential threats and taking proactive security measures, organizations can reduce the risk of successful cyber attacks and protect their digital assets and sensitive information.

**KT0204 Different types of hackers**

Hackers come in various types, and they are often categorized based on their intentions, skills, and activities in the cybersecurity landscape. Here are some common types of hackers:

1. **White Hat Hackers**: Also known as ethical hackers or penetration testers, white hat hackers work legally and with permission to identify and fix vulnerabilities in systems, networks, or applications. Their goal is to improve cybersecurity by helping organizations strengthen their defenses.
2. **Black Hat Hackers**: Black hat hackers are the malicious actors who engage in unauthorized and illegal activities to compromise computer systems, steal data, or cause harm. They are motivated by personal gain, financial rewards, or simply causing disruption and chaos.
3. **Gray Hat Hackers**: Gray hat hackers operate between white hat and black hat hackers. While they may identify and report vulnerabilities, they do so without explicit permission, which can still be illegal. Their intentions may not always be malicious, but they don't follow ethical guidelines strictly.
4. **Script Kiddies**: Script kiddies are individuals with limited technical skills who use pre-made hacking tools and scripts without a deep understanding of how they work. They rely on ready-made exploits to launch attacks, often without fully comprehending the techniques involved.
5. **Hacktivists**: Hacktivists are hackers motivated by political or social causes. They use their skills to launch cyber attacks or deface websites to advocate for their beliefs or raise awareness about specific issues.
6. **State-Sponsored Hackers**: Also known as APT (Advanced Persistent Threat) groups, state-sponsored hackers are backed by governments and work to conduct cyber espionage, steal sensitive information, or disrupt other nations' critical infrastructure.
7. **Insider Threats**: Insider threats are individuals within an organization who misuse their authorized access to systems or data for malicious purposes or unintentionally cause security breaches.
8. **Cyber Criminals**: Cyber criminals are hackers who engage in criminal activities for financial gain. They may conduct ransomware attacks, steal sensitive data for sale on the dark web, or commit other cybercrimes.
9. **Hacktivist Collectives**: These are groups of hacktivists who join forces to advocate for particular social or political causes. Examples include Anonymous and Lizard Squad.
10. **Nation-State Hackers**: Nation-state hackers are state-sponsored groups primarily focused on carrying out cyber operations on behalf of their country's government. Their targets often involve intelligence gathering, disruption of rival nations, or conducting cyber warfare.

It's important to note that hacking is a broad term, and individuals within these categories may have varying skill levels, motivations, and levels of sophistication. While ethical hacking can serve a valuable purpose in improving cybersecurity, malicious hacking is illegal and poses significant risks to individuals, organizations, and society as a whole.

**KT0205 How individuals are targeted by hackers**

Individuals are targeted by hackers through various methods and techniques, each designed to exploit vulnerabilities and gain unauthorized access to personal information or digital assets. Here are some common ways in which individuals are targeted by hackers:

1. **Phishing Attacks**: Hackers send deceptive emails, messages, or website links that appear to be from legitimate sources, tricking individuals into revealing sensitive information such as login credentials, passwords, or financial details.
2. **Social Engineering**: Social engineering involves manipulating individuals through psychological tactics to convince them to perform certain actions or disclose confidential information. This can be done through phone calls, impersonation, or exploiting trust.
3. **Malware**: Hackers use malicious software (malware) to infect individuals' computers or mobile devices. Common types of malware include viruses, worms, Trojans, ransomware, and spyware, which can steal information or control the device remotely.
4. **Drive-By Downloads**: Hackers exploit vulnerabilities in websites or ads to automatically download malware onto individuals' devices without their knowledge or interaction.
5. **Credential Stuffing**: Hackers use username and password combinations obtained from data breaches on other websites to try and gain unauthorized access to individuals' accounts on different platforms.
6. **Public Wi-Fi Exploitation**: Hackers may set up fake public Wi-Fi hotspots to intercept data transmitted by users on unsecured networks, potentially capturing sensitive information.
7. **USB Dropping**: In public places, hackers may leave infected USB drives or other media devices hoping that someone will pick them up and connect them to their computer, unknowingly introducing malware.
8. **Watering Hole Attacks**: Hackers compromise websites that are frequently visited by individuals with a specific interest or profile, infecting the visitors' devices with malware.
9. **Spear Phishing**: A targeted form of phishing where hackers personalize their attacks to exploit specific individuals or organizations, increasing the chances of success.
10. **Social Media Exploitation**: Hackers use information publicly available on social media platforms to craft personalized attacks or to gain access to personal data.
11. **Fake Websites and Apps**: Hackers create fake websites or mobile apps that mimic legitimate ones to deceive users into providing personal information or downloading malware.
12. **SMS and Phone Call Scams**: Hackers send deceptive SMS messages or make phone calls to manipulate individuals into revealing sensitive information or making financial transactions.

To protect against these threats, individuals should be cautious and vigilant when interacting online. This includes being wary of suspicious emails, messages, or requests, using strong and unique passwords, keeping software and devices updated, avoiding unsecured Wi-Fi networks, and using reputable security software and services. Additionally, being aware of common cyber threats and regularly educating oneself about cybersecurity best practices is essential for staying safe in the digital world.

**KT0206 Man-in-the-middle attack**

A Man-in-the-Middle (MitM) attack is a type of cybersecurity attack in which a malicious actor secretly intercepts and possibly alters communications between two parties who believe they are directly communicating with each other. The attacker positions themselves between the sender and the receiver, essentially "eavesdropping" on the communication without the knowledge or consent of either party.

Here's how a typical Man-in-the-Middle attack works:

1. **Interception**: The attacker gains access to the communication channel between the two parties. This can be done through various means, such as compromising a router, exploiting weaknesses in Wi-Fi networks, or using specialized tools like Wireshark to sniff network traffic.
2. **Impersonation**: Once the attacker has control over the communication channel, they may impersonate one or both of the parties involved in the communication. For example, the attacker might pose as the sender to the receiver and vice versa, pretending to be each party.
3. **Monitoring and Alteration**: With the ability to intercept the communication, the attacker can now monitor the messages exchanged between the two parties. They can also modify the content of the messages, inserting malicious content or modifying data.
4. **Forwarding**: In some cases, after intercepting and modifying the communication, the attacker may then forward it to the intended recipient to maintain the illusion that everything is functioning as normal.

MitM attacks can occur in various scenarios, including:

* **Public Wi-Fi Networks**: Hackers can set up rogue Wi-Fi hotspots with names similar to legitimate ones to intercept data transmitted by unsuspecting users.
* **ARP Spoofing**: Attackers can use Address Resolution Protocol (ARP) spoofing to redirect traffic intended for one device to their own, allowing them to intercept communications.
* **DNS Spoofing**: DNS (Domain Name System) spoofing involves redirecting users to fake websites that mimic legitimate ones, allowing attackers to intercept login credentials and other sensitive information.
* **SSL Stripping**: Attackers can attempt to downgrade secure HTTPS connections to unsecured HTTP, making it easier to intercept data.

MitM attacks pose significant risks as they allow attackers to steal sensitive information, such as login credentials, financial details, or personal data. They can also facilitate other types of cyberattacks by altering communications or injecting malicious content.

To protect against Man-in-the-Middle attacks, users should use secure and encrypted communication channels whenever possible, avoid connecting to untrusted Wi-Fi networks, verify the authenticity of websites and digital certificates, and be cautious when sharing sensitive information online. Employing strong encryption methods, like SSL/TLS, can also help prevent data interception and manipulation during transmission.

***Internal Assessment Criteria and Weight***

* IAC0201 Cybersecurity as an escalating global pandemic is reasoned.
* IAC0202 Types of hackers are differentiated.
* IAC0203 The man-in-the-middle attack is understood.

***(Weight 20%)***

# KM-01-KT03 : Cybersecurity governance fundamentals 20%

**Topic elements to be covered include:**

* KT0301 Basic introduction to legislative framework:

Cybercrimes Act

Governance, confidential information and the POPI Act

Electronic Communication and Transactions Act

* KT0302 Cyber security policy - the foundation of protection
* KT0303 The role of the IT department in preventing vulnerabilities

**KT0301 Basic introduction to legislative framework:**

**Cybercrimes Act**

**Governance, confidential information and the POPI Act**

**Electronic Communication and Transactions Act**

As of my last update in September 2021, there is no specific "Cybercrimes Act" that applies universally across all countries. However, many countries have enacted laws and regulations that address cybercrimes and cybersecurity issues. These laws are designed to combat various forms of cybercriminal activities and protect individuals, organizations, and governments from cyber threats.

The content and scope of cybercrime legislation can vary significantly from one country to another, but some common elements found in such laws include:

1. **Definition of Cybercrimes**: Cybercrime laws typically define various cyber offenses, such as unauthorized access to computer systems, data theft, hacking, identity theft, online fraud, cyberbullying, distribution of malicious software, and denial-of-service attacks.
2. **Penalties and Punishments**: Cybercrime laws prescribe penalties and punishments for offenders found guilty of committing cybercrimes. These penalties may include fines, imprisonment, asset forfeiture, or other appropriate legal actions.
3. **Jurisdiction and Extradition**: The laws often address issues related to jurisdiction, especially in cases where cybercrimes are committed across borders. Provisions for extradition of cybercriminals may also be included.
4. **Investigation and Law Enforcement Powers**: Cybercrime laws may grant law enforcement authorities the necessary powers to investigate cybercrimes, obtain electronic evidence, and conduct cyber forensics.
5. **Data Protection and Privacy**: Some cybercrime laws incorporate provisions related to data protection, privacy, and the handling of personal information to safeguard individuals' rights.
6. **Reporting Obligations**: The laws may require certain entities, such as internet service providers (ISPs) or critical infrastructure operators, to report cyber incidents or cooperate with law enforcement agencies during investigations.
7. **International Cooperation**: Cybercrime laws often encourage and facilitate international cooperation between countries in addressing cyber threats and prosecuting cybercriminals.

It's important to note that cybersecurity legislation is continually evolving to keep pace with the ever-changing cyber threat landscape. Countries may update or amend their cybercrime laws as new challenges and risks emerge.

If you have specific inquiries about the Cybercrimes Act of a particular country or region, I recommend consulting the relevant government or legal sources to access the most up-to-date and accurate information regarding cybercrime legislation in that jurisdiction.

Governance, confidential information, and the POPI Act are interconnected concepts related to data protection and privacy in the context of South Africa. Let's explore each of these aspects:

1. **Governance**:

Governance refers to the system of rules, practices, and processes by which an organization is directed, controlled, and operated. In the context of data protection and privacy, governance encompasses the policies, procedures, and practices that an organization implements to ensure the responsible handling of personal and confidential information.

A robust data governance framework includes:

* **Data Protection Policies**: Clear and comprehensive policies that outline how personal data will be collected, processed, stored, and shared.
* **Data Privacy Officer (DPO)**: Appointing a designated individual or team responsible for overseeing data protection and privacy matters within the organization.
* **Data Access Controls**: Implementing access controls to ensure that only authorized individuals have access to sensitive data.
* **Data Retention Policies**: Establishing guidelines for how long personal data should be retained and when it should be securely deleted.
* **Data Breach Response Plan**: Having a plan in place to respond promptly and effectively in case of a data breach or security incident.

1. **Confidential Information**:

Confidential information refers to sensitive data or knowledge that is not publicly available and is intended to be kept secret. This can include proprietary business information, trade secrets, customer data, financial records, and any other data that has value and should be protected from unauthorized access or disclosure.

Ensuring the confidentiality of sensitive information is essential for maintaining trust with customers, business partners, and stakeholders. Organizations must implement security measures, access controls, and data protection mechanisms to safeguard confidential information from internal and external threats.

1. **POPI Act (Protection of Personal Information Act)**:

The Protection of Personal Information Act (POPI Act) is a comprehensive data protection and privacy law in South Africa. It aims to regulate the processing of personal information by public and private organizations and to provide individuals with certain rights concerning their personal data.

Key provisions of the POPI Act include:

* **Data Subject Rights**: The Act grants data subjects (individuals whose personal data is being processed) various rights, including the right to access their information, the right to correct inaccurate data, and the right to object to certain types of processing.
* **Consent**: Organizations must obtain explicit and informed consent from data subjects before collecting, using, or disclosing their personal information.
* **Security Measures**: The Act requires organizations to implement appropriate security safeguards to protect personal data from unauthorized access, loss, or destruction.
* **Data Breach Notification**: Organizations are required to report data breaches to the Information Regulator and affected individuals promptly.
* **Cross-Border Transfers**: Personal data can only be transferred outside of South Africa if the receiving country has adequate data protection laws or if the data subject has given consent.
* **Data Protection Officer (DPO)**: Certain organizations may need to appoint a DPO to oversee compliance with the POPI Act.

Compliance with the POPI Act is crucial for all organizations handling personal data in South Africa. Non-compliance can result in significant fines and reputational damage.

In summary, governance practices, including data governance, play a vital role in ensuring the responsible and secure handling of confidential information, particularly when complying with data protection and privacy laws like the POPI Act in South Africa. Organizations must prioritize data protection and implement appropriate measures to safeguard personal information and maintain compliance with relevant regulations.

The Electronic Communications and Transactions Act (ECT Act) is a legislation enacted in South Africa to provide a legal framework for electronic communications, electronic transactions, and the use of electronic signatures. The Act was introduced to facilitate e-commerce and promote the use of electronic means in conducting various business and communication activities. It was signed into law in 2002 and has been amended since then to adapt to technological advancements and changes in the digital landscape.

Key aspects and provisions of the Electronic Communications and Transactions Act include:

1. **Legal Recognition of Electronic Transactions**: The Act grants legal recognition to electronic transactions and contracts, making them as legally binding and enforceable as traditional paper-based transactions.
2. **Electronic Signatures**: The ECT Act recognizes electronic signatures as valid and legally binding, provided they meet certain requirements specified in the legislation.
3. **Data Messages**: The Act defines data messages as electronic messages, including emails, SMS, and other forms of electronic communication. It ensures that data messages are legally recognized and enforceable as documentary evidence.
4. **Consumer Protection**: The Act contains provisions to protect consumers engaging in e-commerce transactions, including requirements for businesses to provide certain information to consumers before concluding an online transaction.
5. **Liability of Service Providers**: The ECT Act includes provisions that protect internet service providers and other intermediaries from liability for third-party content or information transmitted through their systems, under certain circumstances.
6. **Unsolicited Commercial Communications (Spam)**: The Act addresses the sending of unsolicited commercial communications (spam) and provides requirements for obtaining consent from recipients before sending such messages.
7. **Privacy and Data Protection**: While the ECT Act primarily focuses on electronic communications and transactions, it also aligns with South Africa's broader data protection laws, including the Protection of Personal Information Act (POPI Act).
8. **Digital Signatures and Certificates**: The Act establishes provisions for the use of digital signatures and digital certificates in electronic transactions, providing a secure way to authenticate parties and ensure data integrity.

The ECT Act has been crucial in enabling and promoting e-commerce and other electronic transactions in South Africa. It provides legal certainty and consumer protection while encouraging the growth of the digital economy. It is essential for businesses and individuals engaged in electronic communications and transactions to understand and comply with the provisions of the Electronic Communications and Transactions Act to ensure legal compliance and facilitate secure and reliable electronic interactions.

**KT0302 Cyber security policy - the foundation of protection**

A cyber security policy is a fundamental and essential document that serves as the foundation of protection for an organization's digital assets, data, systems, and networks. It outlines the guidelines, principles, and rules that govern the organization's approach to managing and mitigating cyber risks. A well-crafted cyber security policy provides a framework for safeguarding against cyber threats, ensuring data confidentiality, integrity, and availability, and promoting a culture of security awareness within the organization.

Here are some key aspects of how a cyber security policy serves as the foundation of protection:

1. **Risk Management**: The policy defines the organization's risk appetite and risk management strategies. It identifies potential cyber threats and vulnerabilities, assesses their impact, and establishes measures to mitigate risks effectively.
2. **Data Protection and Privacy**: The policy outlines procedures for handling and protecting sensitive data, both internally and when shared with external entities. It aligns with data protection and privacy laws and sets guidelines for data retention, access controls, and data sharing.
3. **Access Control and Authentication**: The policy establishes rules for granting access to information systems and networks. It defines authentication methods, password policies, and user account management practices to ensure that only authorized individuals can access sensitive data.
4. **Incident Response and Reporting**: The policy outlines procedures for responding to and reporting cyber incidents, including data breaches and security breaches. It includes protocols for notifying relevant stakeholders, authorities, and affected individuals promptly.
5. **Employee Training and Awareness**: The policy emphasizes the importance of security awareness among employees. It mandates regular cybersecurity training and education programs to ensure that employees understand their roles and responsibilities in maintaining a secure environment.
6. **Technology Guidelines**: The policy sets guidelines for the use and configuration of technology resources, such as computers, mobile devices, and software applications, to maintain a secure and consistent computing environment.
7. **Third-Party Risk Management**: If applicable, the policy addresses the management of cyber risks associated with third-party vendors, partners, or contractors that have access to the organization's systems or data.
8. **Compliance and Governance**: The policy ensures that the organization complies with relevant cybersecurity regulations, industry standards, and best practices. It provides a framework for governance and oversight of cyber security measures.
9. **Business Continuity and Disaster Recovery**: The policy establishes protocols for business continuity and disaster recovery in the event of a cyber incident or other disruptive events.
10. **Audit and Monitoring**: The policy outlines procedures for conducting periodic security audits and monitoring of the organization's IT environment to identify potential vulnerabilities and weaknesses.

A well-implemented cyber security policy is a proactive approach to cybersecurity, empowering organizations to anticipate and defend against cyber threats effectively. It creates a unified and consistent approach to security across the organization, ensuring that everyone understands their role in safeguarding sensitive information and digital assets. Regular updates and reviews of the policy are essential to keep pace with evolving cyber threats and technology advancements.

**KT0303 The role of the IT department in preventing vulnerabilities**

The IT department plays a crucial role in preventing vulnerabilities and enhancing the overall cybersecurity posture of an organization. Their responsibilities extend beyond managing day-to-day IT operations to actively identifying, mitigating, and addressing potential security risks. Here are some key roles and actions that the IT department takes to prevent vulnerabilities:

1. **Security Infrastructure Management**: The IT department is responsible for managing and maintaining the organization's security infrastructure, including firewalls, intrusion detection/prevention systems, antivirus software, encryption tools, and other security solutions.
2. **Patch Management**: The IT department ensures that all software, operating systems, and applications are up-to-date with the latest security patches and updates. Timely patching helps prevent known vulnerabilities from being exploited by attackers.
3. **Network Security**: IT professionals implement and monitor network security measures, such as segmenting networks, configuring secure access controls, and conducting regular network vulnerability assessments.
4. **User Access Controls**: The IT department sets up and manages user access controls, ensuring that employees have the appropriate level of access to data and systems based on their roles and responsibilities.
5. **Authentication and Password Policies**: IT enforces strong authentication methods and password policies to prevent unauthorized access to systems and accounts.
6. **Secure Configuration Management**: IT configures systems and applications securely, following industry best practices and security guidelines to reduce the attack surface.
7. **Security Awareness Training**: The IT department educates employees on cybersecurity best practices through regular security awareness training. Educated employees are better equipped to recognize and avoid potential security threats.
8. **Monitoring and Incident Response**: IT teams monitor network and system activities to detect potential threats or suspicious behavior. They develop incident response plans and are prepared to respond promptly to security incidents.
9. **Penetration Testing**: The IT department may conduct periodic penetration testing to identify vulnerabilities in the organization's infrastructure and applications. This helps proactively identify weaknesses before malicious actors can exploit them.
10. **Vendor and Third-Party Risk Management**: IT professionals assess and manage the cybersecurity risks associated with third-party vendors and service providers who have access to the organization's data or systems.
11. **Encryption and Data Protection**: IT ensures that sensitive data is appropriately encrypted and protected throughout its lifecycle, both in transit and at rest.
12. **Continuous Monitoring and Improvement**: IT continually reviews and improves the organization's security measures, staying up-to-date with the latest cybersecurity trends and threats.

Overall, the IT department plays a central role in preventing vulnerabilities by implementing robust security measures, educating employees, proactively identifying weaknesses, and promptly responding to security incidents. Their efforts are vital in maintaining the confidentiality, integrity, and availability of an organization's information and digital assets in today's rapidly evolving cyber threat landscape.

***Internal Assessment Criteria and Weight***

* IAC0301 Compliance with legislation is understood.
* IAC0302 The aim and function of various governance tools are understood.
* IAC0303 The importance of the IT department in preventing vulnerabilities is justified.

***(Weight 20%)***

# KM-01-KT04 : A cyber secure organisation 15%

**Topic elements to be covered include:**

* KT0401 Assessing the exposure
* KT0402 Security posture
* KT0403 Installation weaknesses and vulnerabilities
* KT0404 Ethical considerations related to different types of software licenses

**KT0401 Assessing the exposure**

Assessing the exposure of a cyber-secure organization involves evaluating its susceptibility to potential cybersecurity threats and vulnerabilities. It aims to identify weaknesses in the organization's security measures and practices, assess the potential impact of cyber incidents, and determine the effectiveness of existing security controls. Here are key steps to assess the exposure of a cyber-secure organization:

1. **Risk Assessment**: Conduct a comprehensive risk assessment to identify and prioritize potential cybersecurity risks. This involves analyzing the organization's assets, data, systems, and processes to understand the threats they face and the potential impact of security incidents.
2. **Vulnerability Assessment**: Perform a vulnerability assessment to identify weaknesses and security gaps in the organization's IT infrastructure, including networks, systems, applications, and endpoints. This assessment helps pinpoint areas that may be prone to exploitation by attackers.
3. **Penetration Testing**: Conduct penetration testing (ethical hacking) to simulate real-world attacks and assess the organization's ability to detect and respond to different types of cyber threats. This helps reveal potential vulnerabilities and weaknesses that might not be apparent in routine assessments.
4. **Security Controls Evaluation**: Review and evaluate the effectiveness of the organization's existing security controls and measures. This includes assessing the implementation of access controls, encryption, incident response plans, employee training, and other security practices.
5. **Compliance and Standards Review**: Ensure that the organization complies with relevant cybersecurity regulations, industry standards, and best practices. Assess the alignment of security measures with frameworks such as ISO 27001, NIST Cybersecurity Framework, or CIS Controls.
6. **Third-Party Risk Assessment**: Assess the cybersecurity risks associated with third-party vendors, suppliers, and service providers who have access to the organization's data or systems.
7. **Security Awareness and Training**: Evaluate the effectiveness of the organization's security awareness training programs for employees. An educated workforce is a critical line of defense against cyber threats.
8. **Incident Response Readiness**: Assess the organization's incident response capabilities, including its ability to detect, contain, and recover from cybersecurity incidents. Test the incident response plan through tabletop exercises or simulations.
9. **Continuous Monitoring**: Implement continuous monitoring of the organization's IT environment to detect and respond to security events in real-time.
10. **Breach Simulation**: Conduct breach simulation exercises to test the organization's response to a simulated cyber breach, helping identify areas for improvement in incident response and crisis management.
11. **Data Protection and Privacy**: Assess the organization's data protection and privacy practices to ensure compliance with relevant regulations and the protection of sensitive information.
12. **Business Continuity and Disaster Recovery**: Evaluate the organization's business continuity and disaster recovery plans to ensure the ability to recover from cyber incidents effectively.

By conducting these assessments, organizations can gain valuable insights into their cybersecurity posture and identify areas for improvement. Regular assessments and proactive security measures are crucial for maintaining a strong defense against cyber threats in an ever-evolving digital landscape.

**KT0402 Security posture**

A security posture in the context of cybersecurity refers to an organization's overall approach, readiness, and effectiveness in protecting its information assets, data, systems, and networks from cyber threats. It reflects the organization's level of preparedness and resilience against potential cyberattacks and its ability to defend against, detect, and respond to security incidents. A strong security posture is essential for safeguarding sensitive information, maintaining business continuity, and preserving customer trust.

A comprehensive security posture encompasses several key elements:

1. **Risk Management**: The organization identifies, assesses, and prioritizes cybersecurity risks to make informed decisions on resource allocation and security measures.
2. **Security Policies and Procedures**: A well-defined set of security policies and procedures govern how the organization handles data, access controls, incident response, employee security awareness, and other security-related aspects.
3. **Security Culture**: A security-conscious culture is promoted throughout the organization, emphasizing the shared responsibility of all employees in maintaining cybersecurity.
4. **Access Control**: Robust access controls are implemented to ensure that only authorized users have appropriate access to systems and data.
5. **Endpoint Security**: Measures are in place to protect endpoints (e.g., workstations, laptops, mobile devices) from malware, unauthorized access, and data breaches.
6. **Network Security**: The organization deploys firewalls, intrusion detection/prevention systems, and other network security measures to protect against unauthorized access and cyber threats.
7. **Data Protection**: Sensitive data is encrypted, and proper data classification and handling procedures are followed to protect data confidentiality and integrity.
8. **Incident Response**: The organization has a well-defined incident response plan to quickly and effectively respond to and mitigate security incidents.
9. **Security Awareness Training**: Employees receive regular security awareness training to recognize and respond to potential cyber threats effectively.
10. **Vendor Risk Management**: Cybersecurity risks associated with third-party vendors are assessed and managed to ensure they meet security standards.
11. **Monitoring and Detection**: Continuous monitoring of network and system activities allows for the timely detection of potential security incidents.
12. **Business Continuity and Disaster Recovery**: The organization has plans in place to ensure business continuity in case of a cyber incident or disaster.
13. **Compliance**: The organization complies with relevant cybersecurity regulations, industry standards, and best practices.

A strong security posture is a dynamic and ongoing effort that requires constant evaluation, updates, and improvements to adapt to evolving cyber threats. Regular security assessments, penetration testing, and vulnerability management play crucial roles in maintaining and enhancing the security posture of an organization. By continually investing in cybersecurity measures and staying vigilant, organizations can reduce the likelihood of successful cyberattacks and protect their critical assets and reputation.

**KT0403 Installation weaknesses and vulnerabilities**

Installation weaknesses and vulnerabilities in the context of cybersecurity refer to security gaps and flaws that can be exploited during the setup or deployment of software, applications, systems, or networks. These weaknesses can expose organizations to potential cyber threats and increase the risk of unauthorized access, data breaches, or system compromise. Identifying and addressing installation vulnerabilities is crucial for maintaining a strong cybersecurity posture. Some common installation weaknesses and vulnerabilities include:

1. **Default Settings**: Many software and hardware products come with default settings that are not secure or appropriate for specific environments. Failure to change default passwords or configurations can leave systems vulnerable to unauthorized access.
2. **Outdated Software**: Installing outdated or unpatched software can expose systems to known vulnerabilities that have been addressed in newer versions. Regularly updating software with security patches is essential to mitigate such risks.
3. **Insecure Protocols**: The use of insecure communication protocols during installation, such as unencrypted connections, can lead to data interception and eavesdropping.
4. **Lack of Secure Bootstrapping**: During initial installation, secure bootstrapping procedures are essential to ensure that the software or system is genuine and has not been tampered with or replaced by malicious versions.
5. **Weak Authentication**: Weak or inadequate authentication mechanisms during installation can lead to unauthorized access to critical systems or administrative controls.
6. **Inadequate Access Controls**: Failure to implement proper access controls during installation can result in users or applications having unnecessary privileges or permissions, making it easier for attackers to escalate their access.
7. **Incomplete Logging**: Insufficient logging during installation can hinder the detection of suspicious activities or security incidents.
8. **Missing Security Configurations**: Failing to configure security settings properly, such as firewall rules, can expose systems and services to external threats.
9. **Open Ports and Services**: Unnecessary open ports and services during installation can provide potential entry points for attackers to exploit.
10. **Insecure Data Transmission**: Transmitting sensitive data in clear text during installation can expose confidential information to eavesdropping and interception.
11. **Unvalidated Input**: During the installation process, failing to validate user input can lead to injection attacks, such as SQL injection or cross-site scripting (XSS).
12. **Weak Encryption**: Insecure or weak encryption algorithms used during installation can compromise the confidentiality of sensitive data.

Addressing these installation weaknesses and vulnerabilities requires a proactive approach to cybersecurity. Organizations should follow best practices and security guidelines during installation, conduct regular security assessments, and ensure that all software and systems are kept up-to-date with the latest security patches. Additionally, comprehensive security policies and procedures should be in place to guide secure installation practices and minimize potential risks.

**KT0404 Ethical considerations related to different types of software licenses**

Ethical considerations related to different types of software licenses are essential for both software developers and users. Various software licenses govern the terms and conditions under which software can be used, distributed, and modified. Understanding the ethical implications of these licenses helps promote responsible and fair use of software and fosters a collaborative and respectful software development community. Here are some ethical considerations related to different types of software licenses:

1. **Open Source Licenses**:
   * **Sharing and Collaboration**: Open-source licenses promote the sharing of software source code and encourage collaborative development. Ethical considerations here involve giving proper credit to original authors and contributing back improvements to the community.
   * **License Compliance**: Developers using open-source code should ensure compliance with the specific license terms. This includes providing attribution, sharing derivative works under the same license, and making the source code available when required.
   * **Avoiding License Conflicts**: Ethical developers should be aware of license compatibility issues when combining code from different open-source projects to avoid legal disputes.
2. **Proprietary (Closed Source) Licenses**:
   * **Respect for Intellectual Property**: Ethical considerations related to proprietary licenses involve respecting the intellectual property rights of software creators and adhering to the terms and restrictions set by the license.
   * **Avoiding Piracy**: Users must avoid unauthorized distribution or use of proprietary software to ensure fair compensation for developers' efforts.
   * **Privacy and Data Collection**: Ethical software developers should be transparent about data collection practices and protect users' privacy when using proprietary software.
3. **Free Software Licenses (e.g., GNU General Public License - GPL)**:
   * **Software Freedom**: Free software licenses emphasize user freedom, including the freedom to use, modify, and distribute software. Ethical developers should support these freedoms and avoid restrictive practices.
   * **Contributions to the Community**: Ethical users of free software should consider contributing back to the community, whether through code improvements or supporting the projects financially.
4. **Commercial Licenses**:
   * **Fair Pricing**: Ethical considerations related to commercial licenses include offering software at fair prices, ensuring accessibility for all potential users, and avoiding price gouging.
   * **Transparency**: Commercial software developers should be transparent about the features, limitations, and licensing terms of their products.
5. **Dual Licensing Models**:
   * **License Clarity**: When software is dual-licensed, ethical considerations include providing clear information to users about their rights and obligations under each license.
   * **Avoiding Misuse**: Ethical users should respect the terms of the chosen license and avoid exploiting loopholes or trying to use the more permissive license in ways unintended by the software creators.

In summary, ethical considerations related to different software licenses revolve around respect for intellectual property rights, fair use, transparency, compliance with license terms, and contributions to the software community. Being aware of and adhering to the ethical implications of software licenses fosters a culture of trust, collaboration, and responsible software development and usage.

***Internal Assessment Criteria and Weight***

* IAC0401 The characteristics of a cyber secure organisation are listed.
* IAC0402 The importance of a resilient cybersecurity posture is reasoned.
* IAC0403 The importance of ethics in cybersecurity is justified.

***(Weight 15%)***

# KM-01-KT05 : Basics of threat intelligence 15%

**Topic elements to be covered include:**

* KT0501 Threat intelligence concept and definition
* KT0502 Trends in attackers’ ever-evolving TTPs
* KT0503 How is threat intelligence collected?
* KT0504 Purpose and benefits of threat intelligence
* KT0505 Who benefits from threat intelligence?

**KT0501 Threat intelligence concept and definition**

Threat intelligence is a cybersecurity concept that refers to the knowledge and information gathered about potential or existing cyber threats and the actors behind them. It involves collecting, analyzing, and interpreting data to understand the tactics, techniques, and procedures (TTPs) used by threat actors and the vulnerabilities they exploit. The goal of threat intelligence is to enable organizations to make informed decisions and implement effective security measures to protect their assets from cyber threats.

The primary components of threat intelligence include:

1. **Data Collection**: Threat intelligence relies on collecting vast amounts of data from various sources, including security logs, network traffic, social media, forums, dark web, and specialized threat intelligence feeds.
2. **Analysis and Processing**: The collected data is then analyzed and processed to identify potential threats, trends, and patterns. Security analysts use various tools and techniques to make sense of the data and extract meaningful insights.
3. **Attribution**: Threat intelligence aims to identify the origin and identity of threat actors, which is known as attribution. This involves determining the individuals, groups, or nation-states responsible for specific cyberattacks.
4. **Contextualization**: Threat intelligence contextualizes the information by assessing the potential impact and relevance of threats to the organization's specific environment and industry.
5. **Actionable Intelligence**: The most valuable threat intelligence is actionable, meaning it provides guidance on how to prevent or mitigate specific threats effectively.

Threat intelligence can be categorized into different types based on its sources, scope, and relevance:

1. **Strategic Threat Intelligence**: This type of intelligence focuses on understanding long-term trends, motivations, and capabilities of threat actors. It helps organizations develop a proactive cybersecurity strategy.
2. **Tactical Threat Intelligence**: Tactical threat intelligence focuses on specific cyber threats, their methodologies, and indicators of compromise (IOCs). It aids in detecting and responding to ongoing or imminent cyber threats.
3. **Operational Threat Intelligence**: Operational threat intelligence is more technical and assists security teams in managing and mitigating security incidents and vulnerabilities.
4. **Internal Threat Intelligence**: Internal threat intelligence is based on an organization's own data and insights into potential vulnerabilities, insider threats, and unusual behaviors within the organization's network.
5. **External Threat Intelligence**: External threat intelligence is gathered from external sources, such as cybersecurity vendors, government agencies, and industry-specific threat intelligence feeds.

Threat intelligence is a vital tool in the fight against cyber threats, allowing organizations to proactively defend against potential attacks, strengthen their security measures, and respond effectively to incidents. It helps organizations stay ahead of cybercriminals, making their cybersecurity efforts more proactive and effective.

**KT0502 Trends in attackers’ ever-evolving TTPs**

Attackers' Tactics, Techniques, and Procedures (TTPs) are continually evolving as they adapt to changes in technology, security measures, and the cybersecurity landscape. To stay ahead of defenders and evade detection, attackers often innovate and adopt new strategies. Here are some trends in attackers' ever-evolving TTPs:

1. **Fileless Malware**: Attackers increasingly use fileless malware, which resides in memory and does not leave traces on the victim's disk. Fileless malware can be challenging to detect by traditional antivirus solutions.
2. **Living off the Land (LoL) Techniques**: Attackers utilize legitimate tools and built-in OS functionalities for malicious purposes, making it harder to distinguish between malicious and legitimate activities.
3. **Ransomware-as-a-Service (RaaS)**: Ransomware operators offer their malicious software as a service, making it easier for less skilled cybercriminals to launch ransomware attacks.
4. **Supply Chain Attacks**: Attackers target the supply chain to compromise software vendors, gaining access to a broader range of potential victims through tainted software updates.
5. **Zero-Day Exploits**: Sophisticated attackers use zero-day vulnerabilities (previously unknown and unpatched) to gain initial access to systems, making detection and prevention more challenging.
6. **Phishing and Social Engineering**: Phishing attacks remain prevalent, with attackers increasingly using social engineering tactics to trick users into revealing sensitive information or downloading malicious content.
7. **AI-Powered Attacks**: Attackers leverage artificial intelligence and machine learning techniques to create more sophisticated and targeted attacks.
8. **Cloud-Based Attacks**: As organizations move data and services to the cloud, attackers focus on exploiting cloud misconfigurations and vulnerabilities to gain unauthorized access.
9. **Cryptojacking**: Attackers target computers and devices to use their computational power for cryptocurrency mining, potentially causing performance issues and increasing electricity costs for victims.
10. **IoT Exploitation**: With the proliferation of Internet of Things (IoT) devices, attackers find new opportunities to exploit vulnerabilities in connected devices.
11. **Living-off-the-Land Binaries (LOLBins)**: Attackers leverage legitimate command-line tools for malicious purposes to evade detection.
12. **Physical Cyber Attacks**: In addition to digital threats, there is a rising concern about physical cyber attacks targeting critical infrastructure and industrial control systems.
13. **Targeted Attacks on Critical Sectors**: Attackers are increasingly targeting critical infrastructure, healthcare, government, and financial sectors, where the impact of a successful attack can be significant.
14. **Deepfakes and Cyber Deception**: Sophisticated deepfake technologies allow attackers to create realistic fake audio and video content to deceive and manipulate targets.
15. **Mobile Device Exploitation**: Attackers focus on exploiting vulnerabilities in mobile devices and applications to compromise sensitive data and gain unauthorized access.

Keeping up with these evolving TTPs is a significant challenge for cybersecurity professionals. Organizations must continuously update their security strategies, invest in advanced threat detection and prevention solutions, and promote a culture of cybersecurity awareness among employees to stay resilient against evolving cyber threats.

**KT0503 How is threat intelligence collected?**

Threat intelligence is collected through various methods and sources to gather information about potential or existing cyber threats and the actors behind them. This process involves continuous monitoring, analysis, and research to understand evolving cyber threats and vulnerabilities. Here are some common methods of collecting threat intelligence:

1. **Security Logs and Event Data**: Collecting and analyzing logs from various security devices, such as firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint security solutions, provide insights into potential security incidents and suspicious activities.
2. **Network Traffic Analysis**: Analyzing network traffic helps identify anomalous patterns and potential signs of cyber threats, such as malware infections, command-and-control (C2) communication, or data exfiltration.
3. **Honeypots and Honeynets**: Honeypots and honeynets are intentionally vulnerable systems designed to attract and collect data on attackers. By analyzing the activity on these systems, threat intelligence can be gathered on the techniques used by attackers.
4. **Threat Intelligence Feeds**: Subscribing to commercial or open-source threat intelligence feeds provides organizations with up-to-date information on known threats, indicators of compromise (IOCs), and malicious IP addresses and domains.
5. **Dark Web Monitoring**: Monitoring activity on the dark web can provide insight into cybercriminal forums, marketplaces, and discussions related to potential threats and attacks.
6. **Vulnerability Databases**: Keeping track of vulnerability databases and security advisories helps identify potential weaknesses in software and systems that threat actors may exploit.
7. **Malware Analysis**: Analyzing malware samples and their behavior provides valuable information about attack techniques and potential vulnerabilities targeted by threat actors.
8. **Open-Source Intelligence (OSINT)**: Collecting intelligence from publicly available sources, such as websites, social media, and forums, helps understand threat actors' motivations, tactics, and potential targets.
9. **Collaboration and Information Sharing**: Sharing threat intelligence with trusted partners, industry peers, and government agencies helps create a collective defense against cyber threats.
10. **Incident Reporting and Sharing**: Encouraging employees and users to report security incidents and potential threats can provide valuable data for threat intelligence analysis.
11. **Security Research and Publications**: Research papers, blogs, and publications from cybersecurity experts and researchers can offer insights into new attack techniques and emerging threats.
12. **Threat Hunting**: Proactively searching for signs of potential threats or indicators of compromise within an organization's network helps detect and respond to threats before they cause significant damage.

Effective threat intelligence requires a combination of automated tools, manual analysis, and human expertise. Organizations can use threat intelligence platforms to aggregate and process data from various sources, facilitating a proactive and holistic approach to cybersecurity. By continuously collecting and analyzing threat intelligence, organizations can stay informed about the latest cyber threats, enhance their security posture, and respond promptly to emerging threats.

**KT0504 Purpose and benefits of threat intelligence**

Threat intelligence serves as a valuable asset for organizations in their cybersecurity efforts. It provides valuable information and insights about potential or existing cyber threats and the actors behind them. The purpose and benefits of threat intelligence are as follows:

**Purpose of Threat Intelligence:**

1. **Proactive Defense**: Threat intelligence enables organizations to adopt a proactive approach to cybersecurity by identifying potential threats and vulnerabilities before they can be exploited.
2. **Understanding Threat Landscape**: It helps organizations gain a comprehensive understanding of the evolving threat landscape, including emerging attack techniques and tactics used by threat actors.
3. **Incident Response and Mitigation**: Threat intelligence aids in incident response by providing critical data on attack indicators, enabling organizations to detect, respond to, and mitigate security incidents effectively.
4. **Risk Management**: Threat intelligence allows organizations to assess cybersecurity risks accurately, prioritize security measures, and allocate resources more effectively to address potential threats.
5. **Vulnerability Assessment**: Organizations can use threat intelligence to identify vulnerabilities in their systems and applications that threat actors might exploit.
6. **Enhanced Decision Making**: Informed by threat intelligence, decision-makers can make data-driven decisions when formulating security strategies and policies.
7. **Adapting Security Measures**: It helps organizations adapt their security measures to keep pace with evolving cyber threats, reducing the risk of successful attacks.

**Benefits of Threat Intelligence:**

1. **Early Threat Detection**: Threat intelligence provides early warnings about potential threats, giving organizations a head start in defending against attacks.
2. **Improved Incident Response**: It enhances incident response capabilities by providing actionable information about the nature of an attack and its potential impact.
3. **Real-time Updates**: Continuous monitoring and analysis of threat intelligence ensure that organizations stay up-to-date with the latest threats and vulnerabilities.
4. **Contextual Information**: Threat intelligence offers context-specific information about threats, allowing organizations to prioritize actions based on their unique environment and risk profile.
5. **Reduced Dwell Time**: With threat intelligence, organizations can reduce the time it takes to detect and remediate security incidents, minimizing the damage caused by cyberattacks.
6. **Threat Hunting**: Threat intelligence supports proactive threat hunting activities, allowing organizations to search for signs of potential threats in their network.
7. **Collaboration and Sharing**: Sharing threat intelligence with trusted partners and peers promotes collective defense and fosters a sense of community against cyber threats.
8. **Regulatory Compliance**: For organizations subject to cybersecurity regulations, threat intelligence can aid in meeting compliance requirements and reporting incidents to regulatory authorities.
9. **Business Continuity**: Effective threat intelligence contributes to better risk management and business continuity planning, reducing the likelihood of disruptive cyber incidents.

In conclusion, threat intelligence plays a vital role in helping organizations strengthen their cybersecurity posture, identify and respond to potential threats proactively, and stay resilient in the face of an ever-evolving cyber threat landscape. By leveraging threat intelligence effectively, organizations can significantly enhance their ability to protect their assets, data, and reputation from cyber threats.

**KT0505 Who benefits from threat intelligence?**

Threat intelligence provides valuable information about potential or existing cyber threats and the actors behind them, benefiting various stakeholders in the cybersecurity ecosystem. The following entities and individuals benefit from threat intelligence:

1. **Organizations**: Businesses and organizations of all sizes benefit from threat intelligence. It helps them understand the evolving threat landscape, assess cybersecurity risks, and implement proactive defense measures to protect their systems, data, and reputation.
2. **Security Teams**: Security teams within organizations benefit significantly from threat intelligence. It empowers them with actionable information to detect and respond to security incidents promptly and effectively.
3. **IT Administrators**: Threat intelligence aids IT administrators in identifying and addressing vulnerabilities in their systems and applications to strengthen the organization's security posture.
4. **CISOs and CIOs**: Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) benefit from threat intelligence as it informs their decision-making when formulating security strategies and allocating resources to protect the organization's assets.
5. **Government Agencies**: Government entities, such as cybersecurity agencies and law enforcement, benefit from threat intelligence to monitor and respond to cyber threats affecting national security, critical infrastructure, and public services.
6. **Security Vendors**: Companies providing cybersecurity products and services leverage threat intelligence to enhance the capabilities of their solutions and offer better protection to their customers.
7. **Threat Researchers**: Cybersecurity researchers and analysts use threat intelligence to study new and emerging threats, tactics, and techniques, contributing to the broader knowledge of the cybersecurity community.
8. **Security Consultants**: Security consulting firms utilize threat intelligence to assist their clients in understanding their cyber risk and developing tailored security strategies.
9. **Information Sharing Communities**: Threat intelligence sharing communities and platforms facilitate the exchange of actionable threat intelligence among organizations and enhance collective defense against cyber threats.
10. **General Public**: Although indirectly, the general public benefits from threat intelligence efforts when it helps prevent large-scale cyber incidents that may impact critical services, public safety, or personal data privacy.

By benefiting these stakeholders, threat intelligence plays a crucial role in fostering a collaborative and well-informed cybersecurity ecosystem. It enables stakeholders to make data-driven decisions, enhance their incident response capabilities, and stay ahead of cyber threats, ultimately contributing to a more secure and resilient digital environment.

***Internal Assessment Criteria and Weight***

* IAC0501 The importance of threat intelligence is reasoned with reference to:

Shedding light on the unknown.

Revealing adversarial motives and their tactics, techniques, and procedures (TTPs).

Helping security professionals better understand the threat actor’s decision- making process.

***(Weight 15%)***

# REFERENCES

1. *Kianpour, Mazaher; Kowalski, Stewart; Øverby, Harald (2021). "Systematically Understanding Cybersecurity Economics: A Survey". Sustainability.*
2. *Stevens, Tim (11 June 2018). "Global Cybersecurity: New Directions in Theory and Methods" (PDF). Politics and Governance.*
3. *Misa, Thomas J. (2016). "Computer Security Discourse at RAND, SDC, and NSA (1958-1970)". IEEE Annals of the History of Computing.*
4. *A. J. Neumann, N. Statland and R. D. Webb (1977). "Post-processing audit tools and techniques" (PDF). nist.gov. US Department of Commerce, National Bureau of Standards. pp. 11-3–11-4. Archived (PDF) from the original on 10 October 2016. Retrieved 19 June 2020.*
5. *Irwin, Luke (5 April 2018). "How NIST can protect the CIA triad, including the often overlooked 'I' – integrity". www.itgovernanceusa.com. Retrieved 16 January 2021.*
6. *Perrin, Chad (30 June 2008). "The CIA Triad". techrepublic.com. Retrieved 31 May 2012.*
7. *Stoneburner, G.; Hayden, C.; Feringa, A. (2004). Engineering Principles for Information Technology Security (PDF) (Report). csrc.nist.gov.*
8. *Yost, Jeffrey R. (April 2015). "The Origin and Early History of the Computer Security Software Products Industry". IEEE Annals of the History of Computing.*
9. *Nakashima, Ellen (26 January 2008). "Bush Order Expands Network Monitoring: Intelligence Agencies to Track Intrusions". The Washington Post. Retrieved 8 February 2021.*