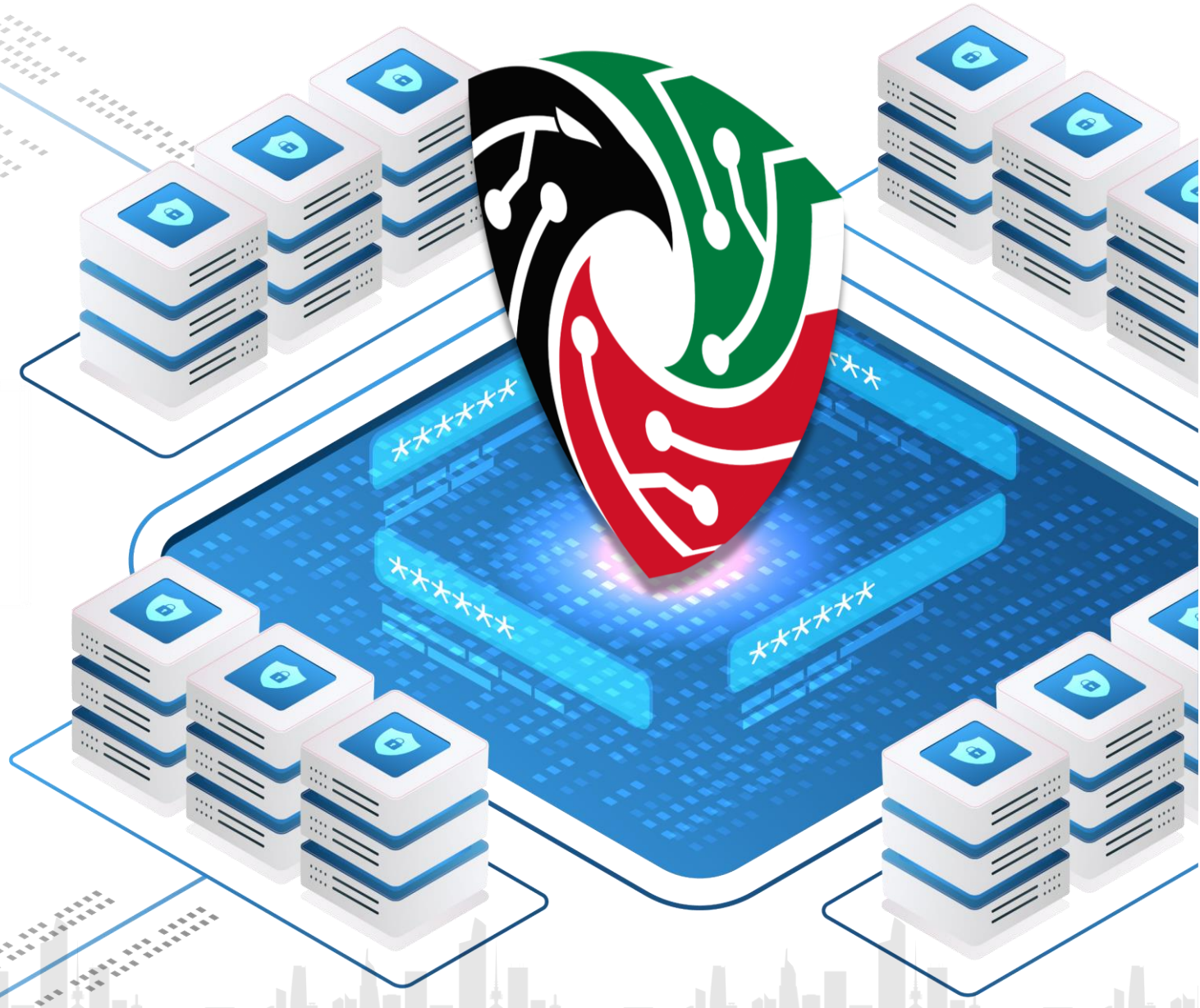
Cybersecurity in The State of Kuwait

NCSC, KW



Cybersecurity

الأمن السيبراني

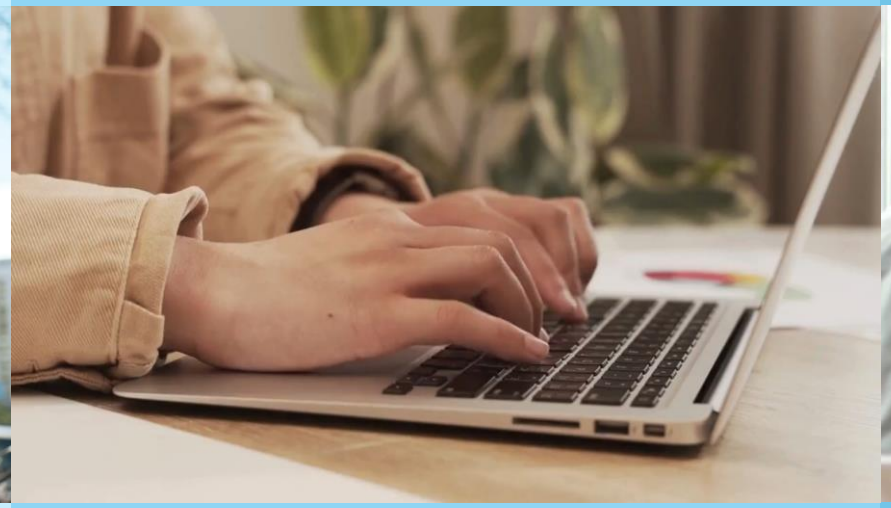
Information Security

أمن المعلومات

Types of Information

Memory Information

Electronic Information



Paper Information

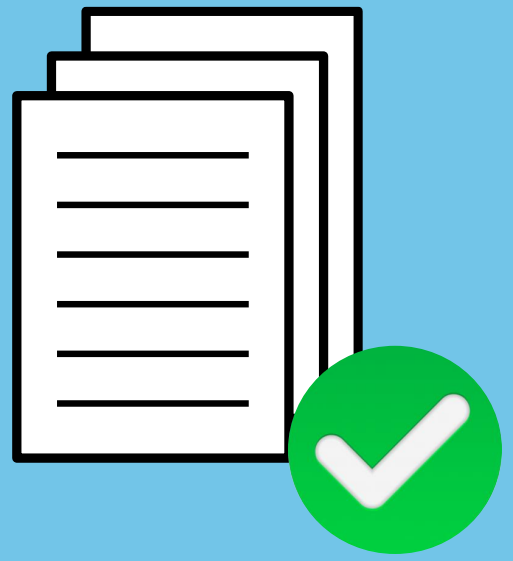
1. information Security

Information security is about protecting information in all forms (digital, non-digital).

- The information doesn't need to be online to require protection.

Memory Information

Electronic Information

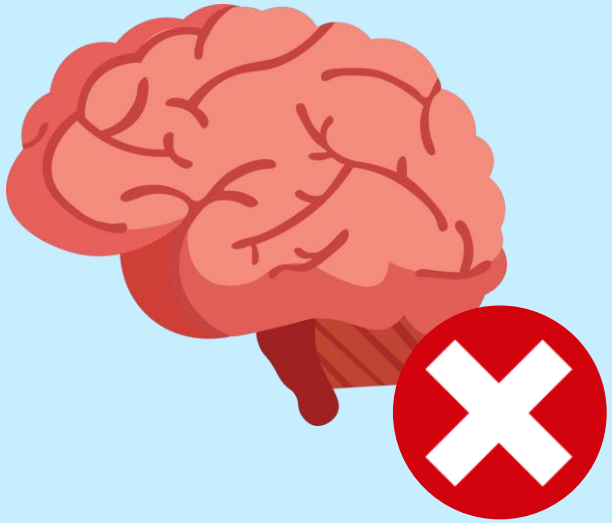


Paper Information

2. Cybersecurity

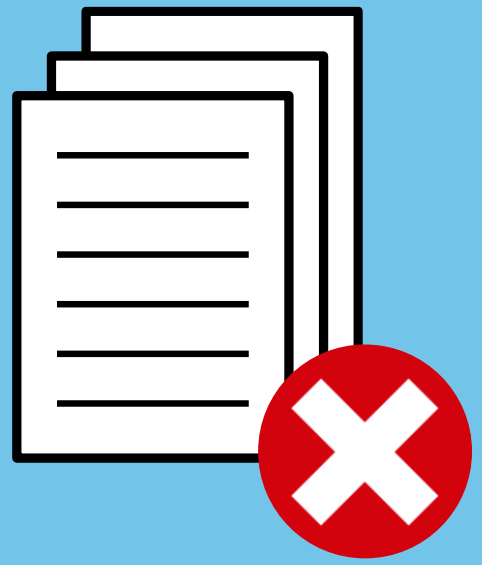
Cybersecurity is the protection of computer systems, networks, and data from unauthorized access, cyber attacks, theft or damage.

ensuring the confidentiality, integrity, and availability of information.



Memory Information

Electronic Information



Paper Information

2. Cybersecurity

Cybersecurity is the protection of computer systems, networks, and data from unauthorized access, cyber attacks, theft or damage, ensuring the confidentiality, integrity, and availability of information.

- Cybersecurity is a branch of information security.
- Transitioning data from paper-based (non-digital) formats to digital data formats increases the risk of cyberattacks on institutions.
- It is essential to implement the necessary measures to protect data and combat cybercrime.

Importance of Cybersecurity

Minimizes Internal Risks:
Helps reduce threats from within the organization, whether caused by accidental mistakes or intentional actions by employees.

Safeguards National Security:
Protects critical infrastructure and national systems.

Fights Cybercrime:
Defends against hacking, phishing, and malware attacks.

Protects Sensitive Data & Privacy:
safeguards both organizational and personal data, ensuring confidentiality and preventing unauthorized access.

Prevents Financial Loss:
Reduces financial damage from cyberattacks.

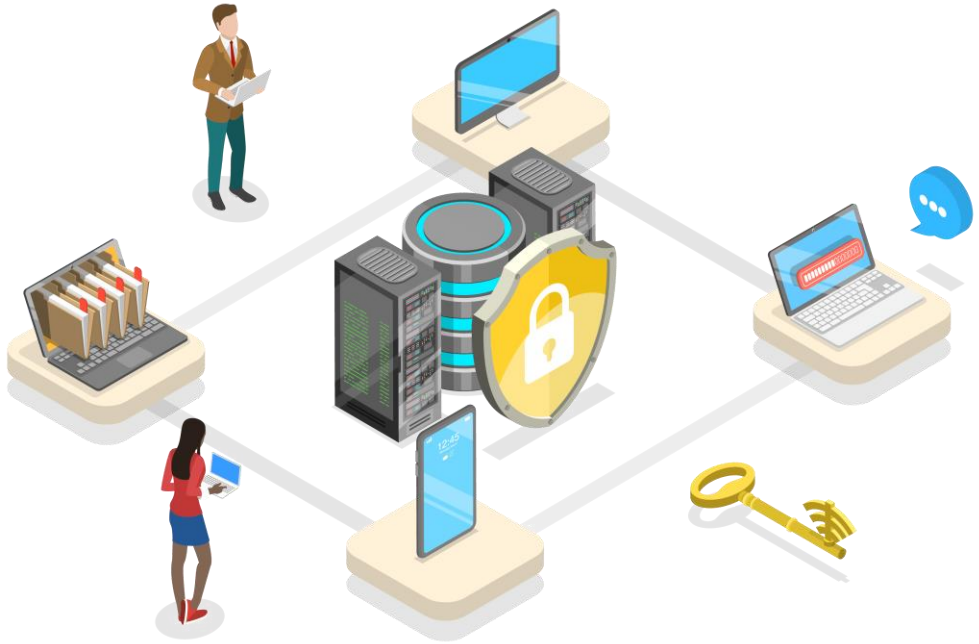
Supports Regulatory Compliance:
Helps organizations comply with legal and regulatory requirements, avoiding penalties and reputational damage.

Scope of Cybersecurity

People:
Security awareness training and monitoring to prevent insider threats.

Processes:
Implementing security frameworks and incident response plans.

Technology:
Using tools like firewalls, encryption, and antivirus software.



Access Controls:
Managing secure access through multi-factor authentication.

Data Security:
Protecting data with encryption and secure storage.

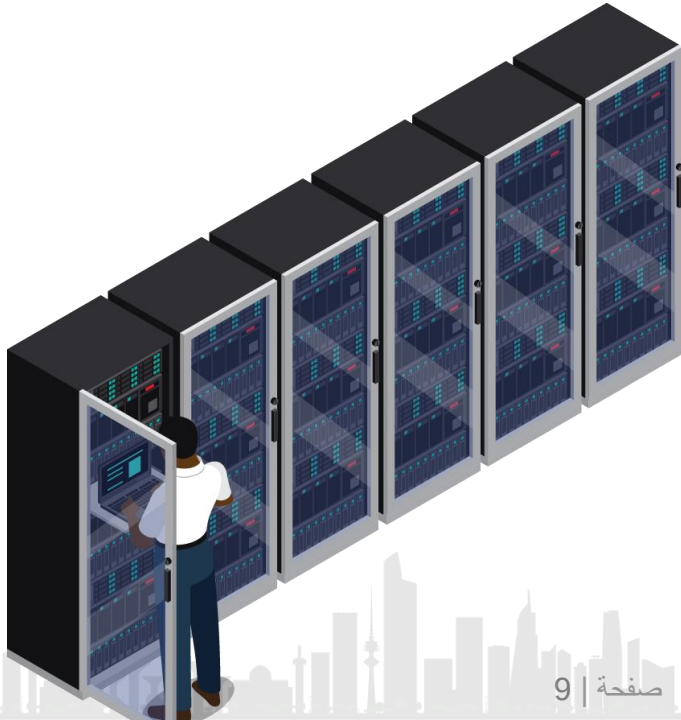
Incident Response:
Detecting, responding to, and recovering from cyber incidents.

IT Department:

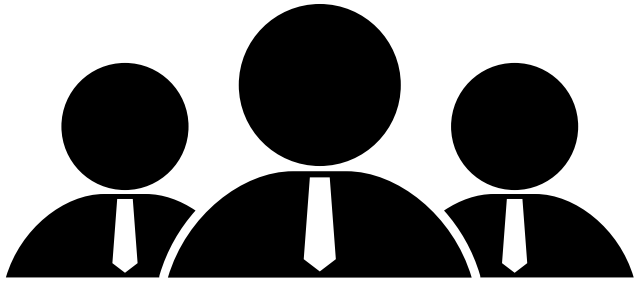
In the past, all countries around the world relied on IT departments, which were responsible for using technology to support and improve the working environment within an organization.

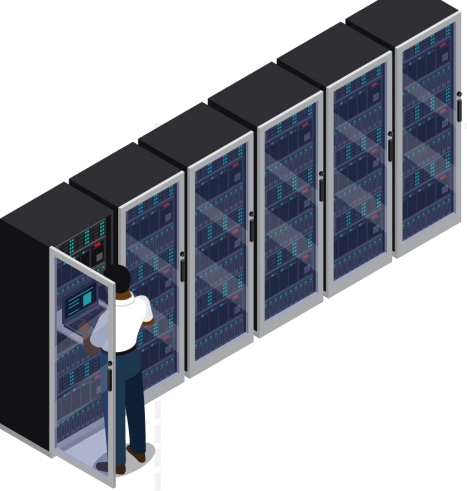
Some of their key responsibilities include the following:

- Providing Technical Support
- System Administration
- Organization Infrastructure and Network Management
- Backup and Disaster Recovery
- IT Policy Enforcement & etc.



Why is it essential for every government entity in Kuwait to have a dedicated Cybersecurity Department?





The Main Reasons For Establishing Cybersecurity Departments In Organizations:

- The IT department needs to focus on innovating and improving the organization's infrastructure.
- Kuwait's future vision for digital transformation by 2035.
- The rise in cyberattacks and breaches calls for a specialized team to protect digital infrastructure.

المركز الوطني للأمن السيبراني
National Cyber Security Center

Cybersecurity Department

The department is responsible for implementing protective measures to ensure that information and communication systems are secure, confidential, and always available. Its main duties include:

- **Analyzing and Monitoring Activities:**

  Regularly reviewing network traffic and smart devices and keeping a detailed log of all activities performed by users within the organization.

- **Verifying Authorized Users:**

  Ensuring that only authorized individuals can access the system and verifying their permissions to ensure compliance.

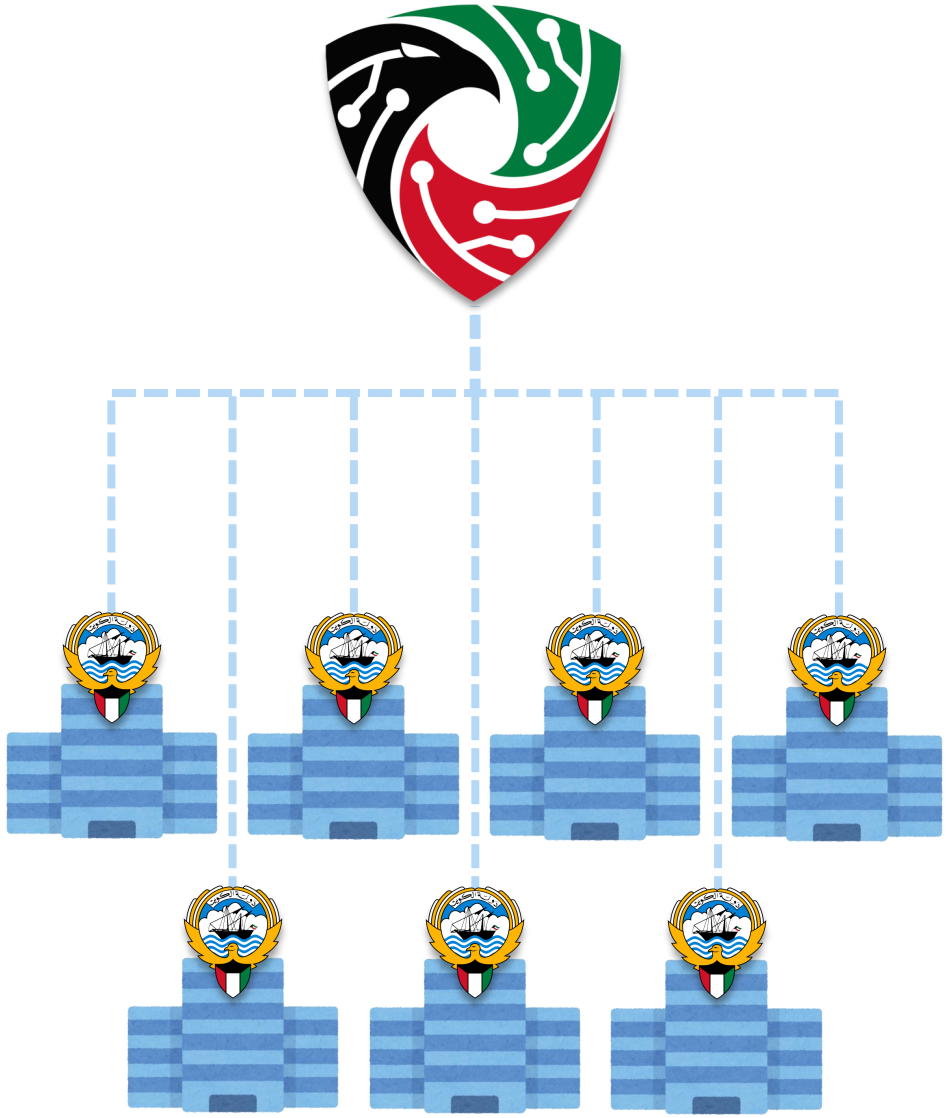
- **Detecting Cyber Incidents:**

  Proactively identifying any potential threats or breaches in the organization's systems.

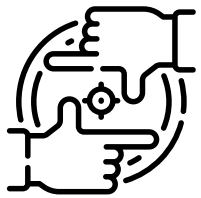
National Cybersecurity Center

Highest authority responsible for protecting the country's infrastructure, economy, and citizens from cyberattacks.

- The center oversees relevant state entities by coordinating communication, cooperation, and training of their staff to enhance cybersecurity.



Responsibilities of the National Cybersecurity Centers:



Developing a National Cybersecurity Strategy including policies & national standards

Training the National Cyber Incident Response Team

International Cooperation in Cybersecurity

Protecting National Networks and Systems against cyber threats

Training the National Cyber Incident Response Team

Supporting partnerships between the public and private sectors in cybersecurity.

One of the key objectives of the NCSC according to Decree No. 37 of 2022:

1. Building and developing national cadres specialized in the field of cybersecurity.

2. Enhancing the culture of cybersecurity that supports the safe and proper use of cyberspace.

3. Protecting and monitoring critical assets, national infrastructure, and information, as well as the national information network in the country.

4. Enhancing cooperation & coordination, as well as the exchange of information between various local and international entities, to raise the level of cybersecurity readiness in the state.

International Cyber Diplomacy

International Cyber Diplomacy

Cyber diplomacy involves the use of diplomatic tools and initiatives to achieve objectives in the complex and continuously evolving uncharted territory of cyberspace.

Key aspects of international cyber diplomacy include the following initiatives:

1. Building trust through cooperation in the field of cybersecurity.
2. Setting standards for collaboration between nations.
3. Developing agreements to prosecute cybercrimes.
4. Strengthening cybersecurity capacities.

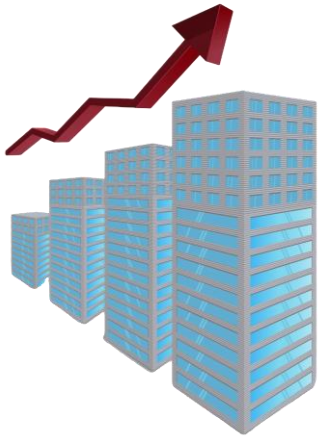
Benefits of Cyber Diplomacy

Global Partnerships

Cyber diplomacy facilitates global partnerships that help secure information systems.

Secure Systems

Cyber diplomacy plays a critical role in protecting systems.



Economic growth

Cyber diplomacy fosters secure cyberspaces which enable economic growth through international cooperation and secure networks

Some Key Players in Cyber Diplomacy

World Economic Forum
(WEF)

European Union
(EU)

Cooperation Council for the Arab States of the Gulf
(GCC)

League of Arab States
(AL)

International Telecommunication (ITU) Union

United Nations
(UN)

IT

Trends 2024

Artificial Intelligence (AI) and Machine Learning (ML):

Increasing use in automating tasks, enhancing decision-making, and improving user experiences.

IT

Trends 2024

Internet of Things (IoT):

Increasing connectivity of devices, leading to smarter homes, industries, and healthcare systems.

IT

Trends 2024

Cloud Computing Expansion:

Growing adoption of hybrid and multi-cloud environments for scalability, cost-efficiency, and flexibility.

IT

Trends 2024

Blockchain Technology:

Continued expansion in sectors beyond cryptocurrency, such as supply chain management, identity verification, & smart contracts.

Most Popular Cyber Attack Techniques

Trends 2024

Phishing Attacks:

Deceptive emails or messages designed to trick users into providing sensitive information or downloading malware.

Most Popular Cyber Attack Techniques

Trends 2024

Ransomware Attacks:

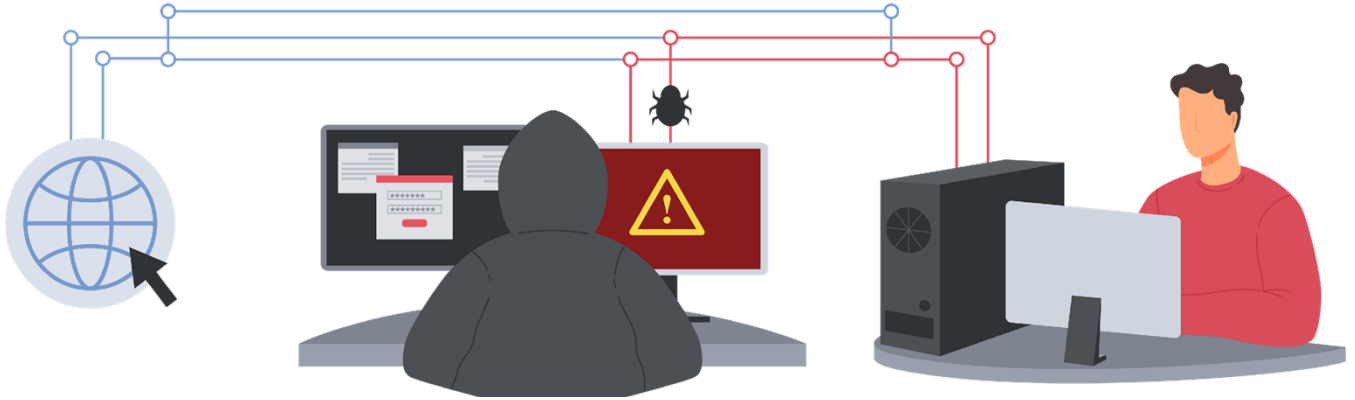
Malware that encrypts a victim's data and demands payment for decryption, with increasing sophistication in targeting critical infrastructure.

Most Popular Cyber Attack Techniques

Trends 2024

Man-in-the-Middle (MITM) Attacks :

Interception of communication between two parties to steal data or inject malicious content.



Most Popular Cyber Attack Techniques

Trends 2024

Distributed Denial of Service (DDoS) Attacks :

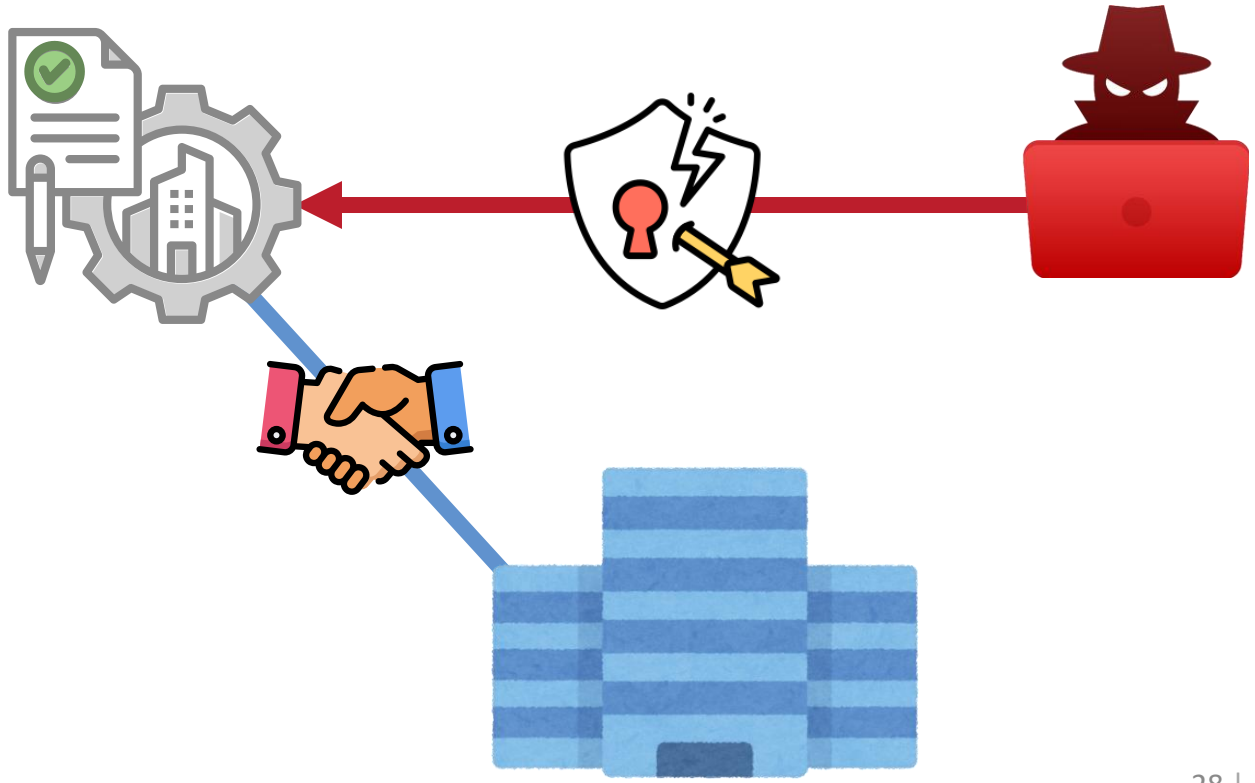
Overloading a network or website with traffic to disrupt services, often used as a distraction while other attacks take place.

Most Popular Cyber Attack Techniques

Trends 2024

Supply Chain Attacks :

Targeting vulnerabilities in third-party suppliers or partners to compromise larger organizations.



Most Popular Cyber Attack Techniques

Trends 2024

Zero-Day Exploits:

Taking advantage of unknown or unpatched vulnerabilities in software before the developer can release a fix.

Most Popular Cyber Attack Techniques

Trends 2024

Social Engineering:

Manipulating individuals into divulging confidential information or performing actions that compromise security.

Challenges Faced by Nations

Shortage of Skilled Cybersecurity Professionals

Lack of adequately trained cybersecurity professionals to fill open positions in the entites.

Limited Budgets

Insufficient funding affects the ability to recruit, train, & retain cybersecurity staff, impacting their competence in representing their roles and missions as they need to stay updated with evolving technologies.

Low Awareness of Cybersecurity Careers

Limited promotion of cybersecurity career paths reduces interest and understanding of the field, leading to fewer individuals pursuing this field.

Lack of Specialized Training Programs

Absence of cybersecurity-specific educational and training initiatives to develop required skills.

High demand from critical infrastructure sectors

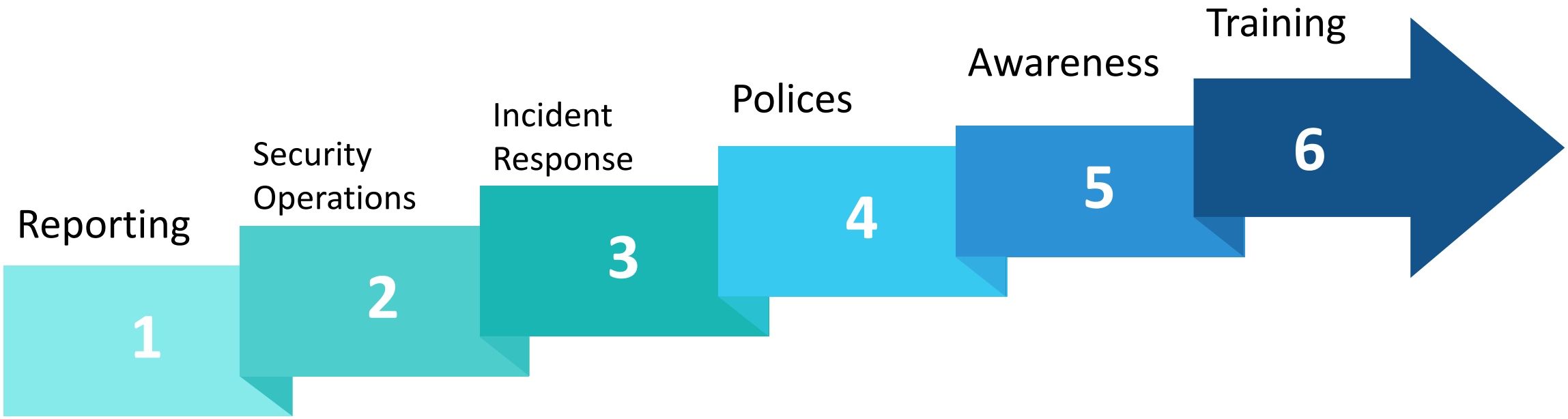
Kuwait Vision 2035's focus on digital transformation has significantly increased the demand for cybersecurity talent across all sectors.

Insufficient Qualifications of Applicants

Candidates often lack the advanced certifications needed for technical cybersecurity roles.

Future Vision

Assure a secure and resilient cyber space to safeguard the national interests of Kuwait.



Achieving Cyber Resilience

To strengthen national cyber resilience, a comprehensive cybersecurity strategy is key. This includes:

- Effective incident response plans
- Crisis management exercises
- Capacity-building programs

By implementing robust awareness programs & training initiatives, we can foster a a cyber-aware culture across both public and private sectors.

Thank You

NCSC Instagram

NCSC X