“Cyber Security & Data Protection”

Kareem Ismail

Agenda

- Definition
- Why Cybersecurity?
- The Kill Chain Process
- Cyber Attacks Types
- NIST Framework
- IT-Cybersecurity Risks
- Data Protection Tools
- SAIs' Key Role in Safeguarding Cybersecurity & Data Protection

Definition

Cybersecurity is the practice of safeguarding systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction.

Why Cyber Security?

Sensitive Data Protection

increasing digitization of information, businesses, governments, and individuals store vast amounts of sensitive data online. Cybersecurity measures are necessary to safeguard this data from unauthorized access, theft, or misuse.

Prevention of Cyber Attacks

Cybercriminals constantly develop new techniques to exploit vulnerabilities in computer systems and networks. Cybersecurity measures help prevent various types of cyber attacks, such as phishing, ransomware, malware, and DDoS attacks, among others.

National Security

Cyber attacks can pose significant threats to a country's national security. Critical infrastructure, military systems, and government networks are potential targets. Strong cybersecurity measures are essential to protect these assets from cyber threats.

Financial Impact

Cybersecurity incidents can lead to significant financial losses. Businesses can suffer from disruptions in operations, legal liabilities, and costs associated with repairing the damage caused by a cyber attack. Investing in cybersecurity can mitigate these financial risks.

Why Cyber Security?

Compliance and Regulations

Many industries and sectors have regulations and compliance standards related to data protection. Adhering to these regulations, such as GDPR (General Data Protection Regulation) in Europe or HIPAA (Health Insurance Portability and Accountability Act) in the United States, is mandatory and requires robust cybersecurity measures.

Data breaches and privacy concerns

High-profile data breaches have highlighted the importance of safeguarding personal and sensitive information. Breaches not only lead to financial losses but also damage an organization's reputation, making cybersecurity a top priority for businesses and individuals alike.

Interconnectedness of Systems

increasing interconnectivity of devices and systems (Internet of Things, cloud computing, etc.) creates more entry points for cyber attacks. Securing these interconnected systems is essential to prevent widespread vulnerabilities.

Digital transformation

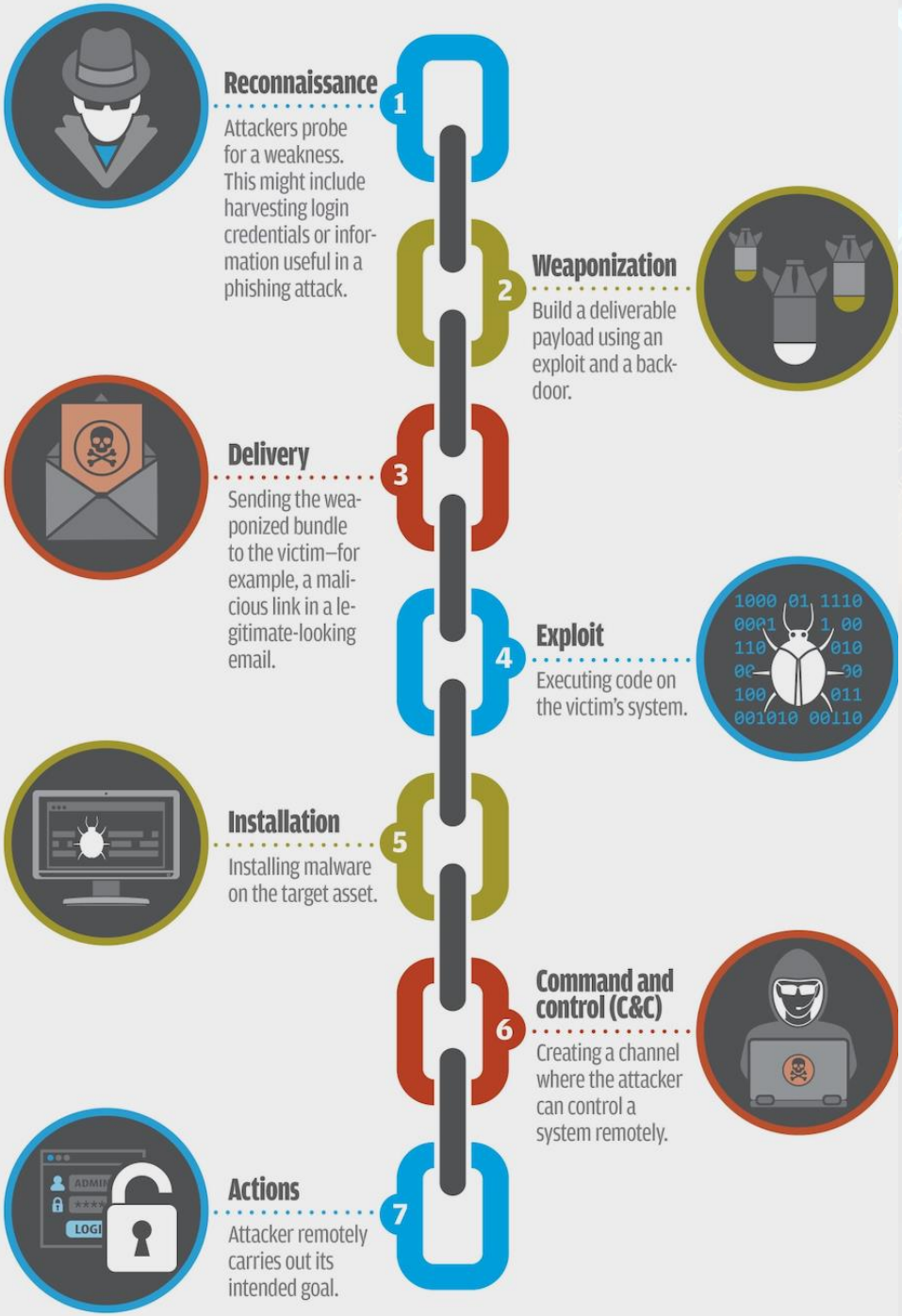
Organizations are undergoing digital transformation initiatives, moving their operations, services, and data to digital platforms. This shift amplifies the importance of cybersecurity to protect digital assets and ensure the continuity of business operations.

Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide (in trillion U.S. dollars)

As of November 2022. Data shown is using current exchange rates.

Sources: Statista Technology Market Outlook, National Cyber Security Organizations, FBI, IMF



The Kill Chain Process

As a "Cyber security defense tool"

How do the Attackers think?

The conventional mode - static defense- (e.g. intrusion detection systems and antivirus software) assumes that attackers have an inherent advantage over defenders given ever-shifting technologies and undiscovered software vulnerabilities.

Conventional defenses were insufficient to protect organizations from sophisticated "advanced persistent threats" (APTs).

Cyber Attack Types

Cyberattacks can target a wide range of victims from individual users to enterprises or even governments. The hacker's goal is usually to access sensitive and valuable company resources.

Phishing Attacks

Uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information

Ransomware Attacks

A specific type of malware, ransomware works by encrypting key files on a machine or network, then demanding a payment

IoT Attacks

Any cyberattack that targets an (IoT) device or network.

Code Injection Attacks

Injecting malicious code into a vulnerable computer or network to change its Course of action.

Spoofing Attacks

A cybercriminal disguises themselves as a known or trusted source.

AI Attacks

Use generative AI tools for phishing emails, keystroke monitoring malware, and basic ransomware code

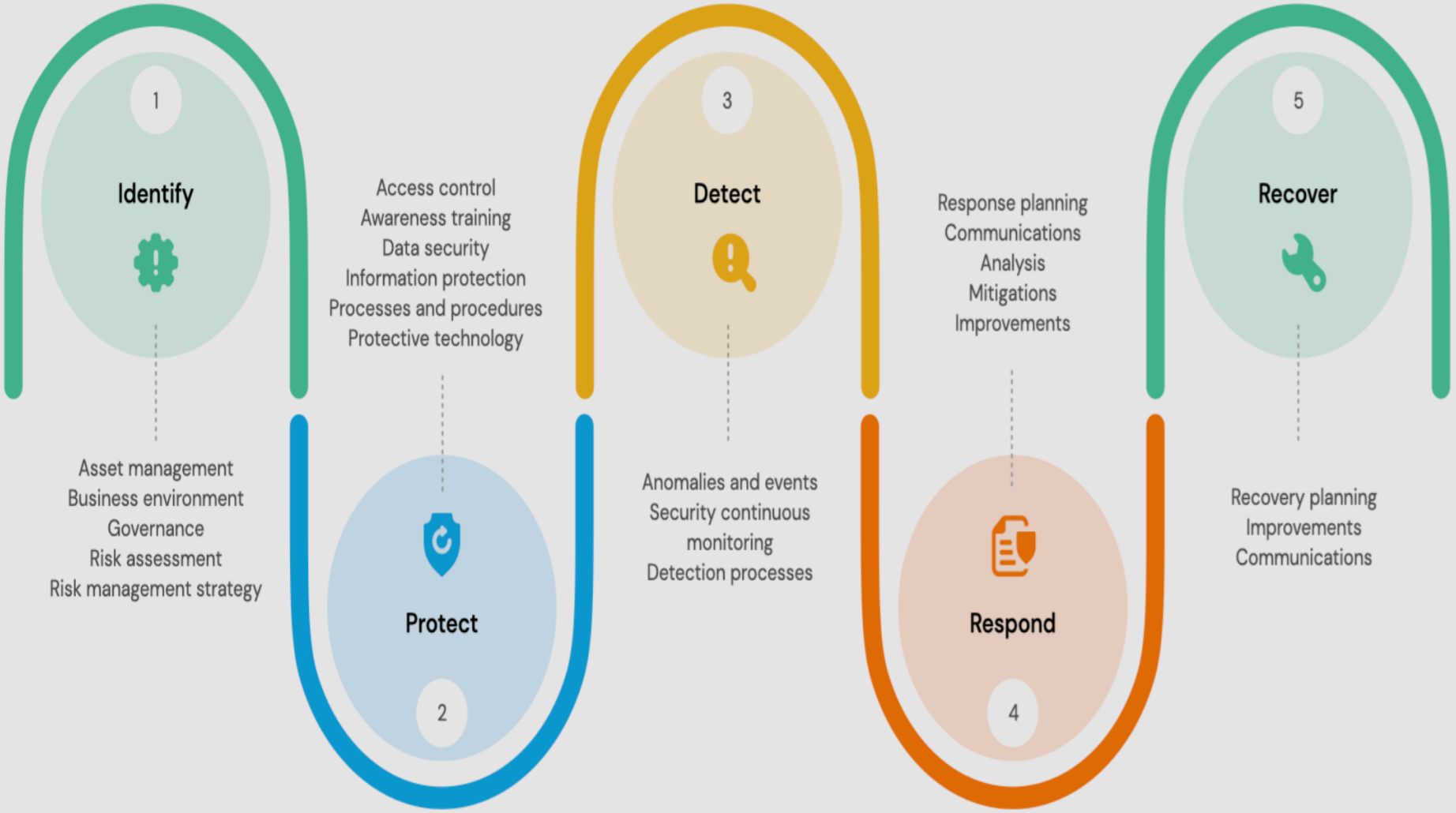
DoS Attacks

A malicious, targeted attack that floods a network with false requests to disrupt business operations.

Insider Attacks

when the danger arises internally. Confidential data that should be safeguarded might be disclosed by employees, which competitors could exploit.

NIST Cyber Security Framework



IT-Cybersecurity Risks

- **Confidentiality:** “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** “Guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity…” A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** “Ensuring timely and reliable access to and use of information…” A loss of availability disrupts access to or use of information or an information system.

Data Protection Tools

Encryption

Encryption is the process of converting data into a code that can only be read by authorized parties

Access Control

Each user, application, and so on should be granted only the access rights required for its business role.

Backup & Recovery

A backup and recovery solution helps organizations protect themselves in case data is deleted or destroyed.

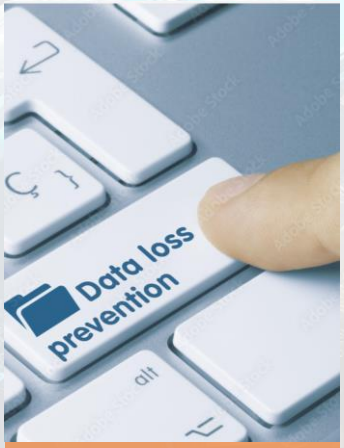
Anti-Malware

Antivirus solutions help detect and remove trojans, rootkits, and viruses that can steal, modify, or damage your sensitive data.

Data Protection Tools

Data Masking

a way to create a fake, but realistic version of your organizational data.



Data Loss Prevention

monitor workstations, servers, and networks to help make sure that sensitive data is not deleted, removed, moved, or copied.

Firewalls

Firewalls are one of the first lines of defense for a network because they prevent undesirable traffic from passing from one network to another

SIEM

Security information and event management: provide real-time analysis of security logs collected by network devices, servers and software applications.

SAIs' Key Role in Safeguarding Cybersecurity and Data Protection

Thank You