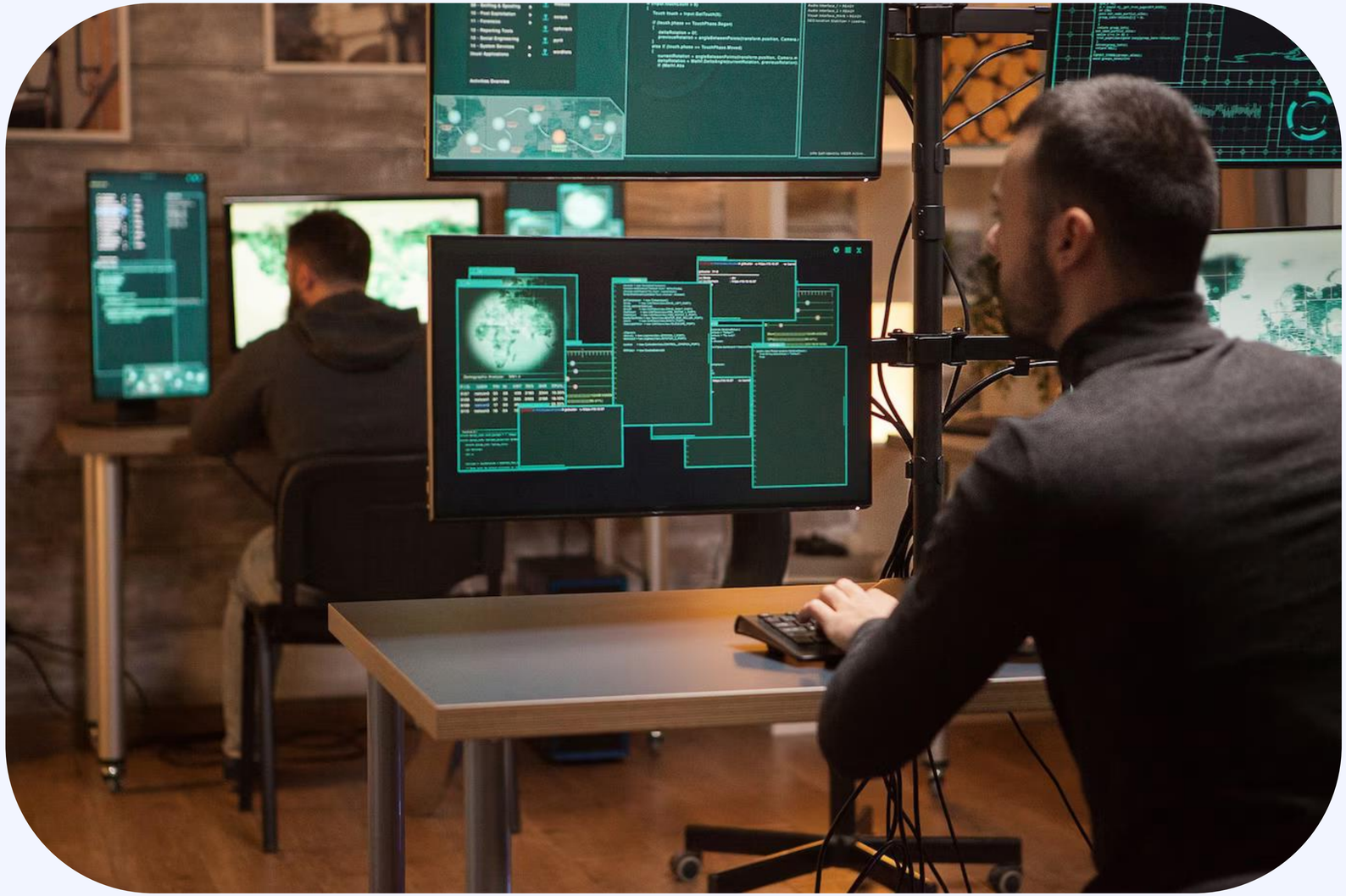
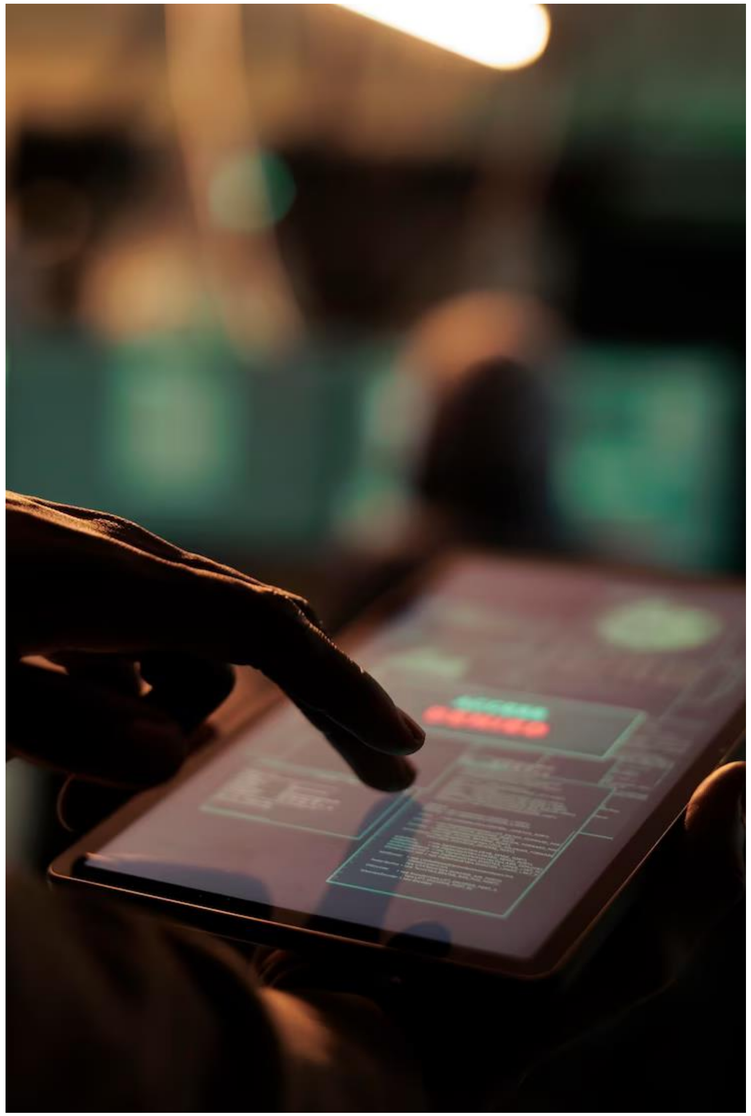
MODULE 6

CYBER SECURITY AND DATA PRIVACY



Introduction



Cybersecurity is the practice of protecting computer systems, networks, and data from digital attacks, theft, damage, or unauthorized access. As our reliance on digital technologies continues to grow, cybersecurity has become a critical component in safeguarding individuals, businesses, governments, and organizations from the evolving threat landscape of cybercrime. The primary goal of cybersecurity is to ensure the confidentiality, integrity, and availability of information and systems

Confidentiality, Integrity, and Availability (CIA)

These three principles form the foundation of cybersecurity: Confidentiality: Ensures that sensitive information is accessible only to authorized individuals.

Integrity: Guarantees the accuracy and trustworthiness of data, preventing unauthorized modifications.

Availability: Ensures that systems and data are available and accessible when needed.

Threats and Vulnerabilities

Cybersecurity threats and vulnerabilities encompass a wide range of risks that can potentially compromise the confidentiality, integrity, and availability of information systems and data. Understanding these threats and vulnerabilities is essential for developing effective cybersecurity strategies

Malware:

Malicious software (malware) includes viruses, worms, trojans, ransomware, and spyware. Malware is designed to infect systems, steal data, or disrupt operations.

Phishing:

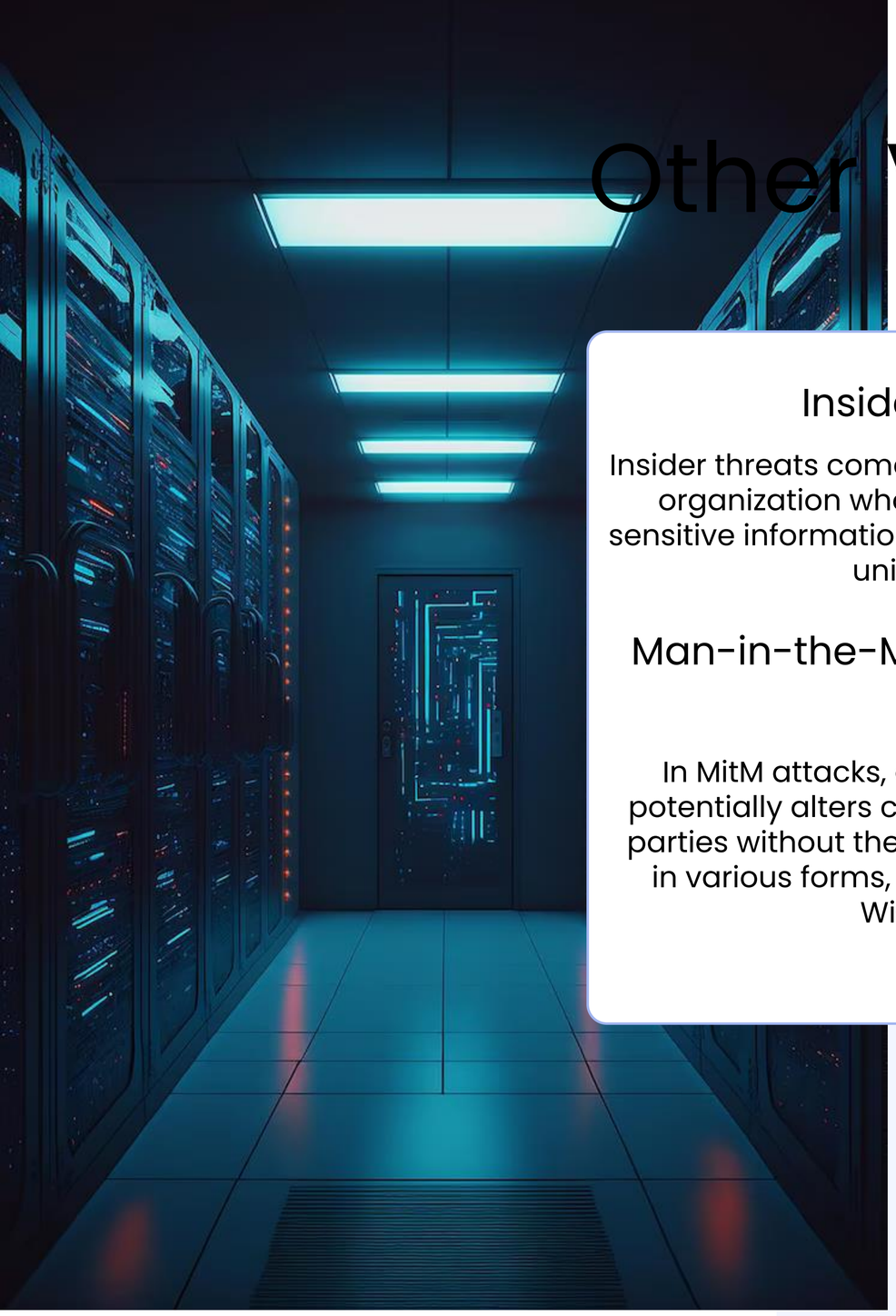
Phishing is a social engineering attack where attackers trick individuals into providing sensitive information such as usernames, passwords, or financial details by pretending to be a trustworthy entity.

Ransomware:

Ransomware encrypts a user's files or entire systems, rendering them inaccessible. Attackers demand a ransom for the decryption key, often in cryptocurrency.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:

DoS attacks flood a system or network with traffic to overwhelm and disrupt services. DDoS attacks involve multiple compromised systems working together to amplify the impact.



Other Vulnerabilities

Insider Threats:

Insider threats come from individuals within an organization who misuse their access to sensitive information. This can be intentional or unintentional.

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

In MitM attacks, an attacker intercepts and potentially alters communication between two parties without their knowledge. This can occur in various forms, such as eavesdropping on Wi-Fi networks.

SQL Injection:

SQL injection attacks involve injecting malicious SQL code into input fields to manipulate a database and gain unauthorized access to data.

Zero-Day Exploits:

Zero-day exploits target vulnerabilities in software or hardware that are not yet known to the vendor. Attackers exploit these vulnerabilities before a patch or solution is available.

Threats

Advanced Persistent Threats (APTs):

APTs involve sophisticated and prolonged attacks by well-funded adversaries, often with specific targets in mind. These attacks aim to remain undetected for an extended period.

IoT (Internet of Things) Vulnerabilities:

Insecure IoT devices can be exploited to gain unauthorized access to networks. Weak security in devices such as smart cameras and home automation systems poses significant risks.

Common Vulnerabilities

Unpatched Software and Systems

Failure to apply security patches and updates leaves systems vulnerable to known exploits. Regular patch management is crucial for addressing vulnerabilities

Weak Authentication and Passwords

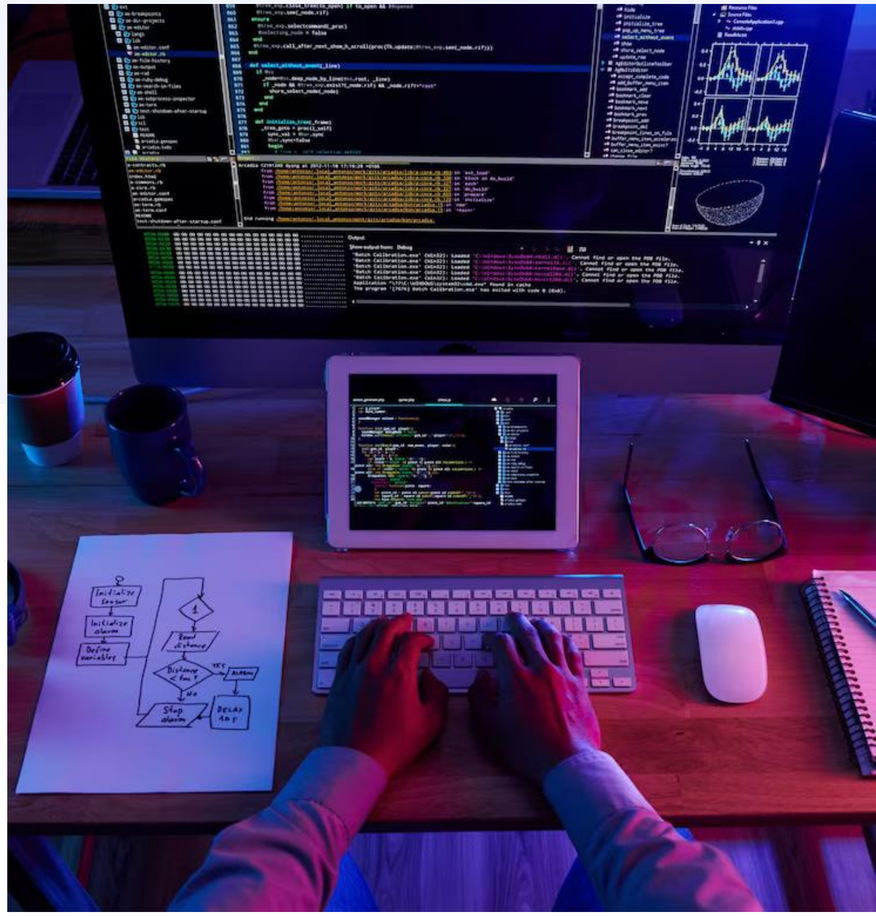
Weak or easily guessable passwords, as well as insufficient authentication measures, can lead to unauthorized access. Multi-Factor Authentication (MFA) helps mitigate this risk.

Lack of Encryption

Failure to encrypt sensitive data, both in transit and at rest, increases the risk of data breaches. Encryption helps protect information even if unauthorized access occurs.

Social Engineering

Social engineering exploits human psychology to manipulate individuals into divulging sensitive information or taking actions that may compromise security.



Common Vulnerabilities

Insecure Configurations:

Improperly configured systems or network devices can expose vulnerabilities. Regular security audits and configuration reviews are essential.

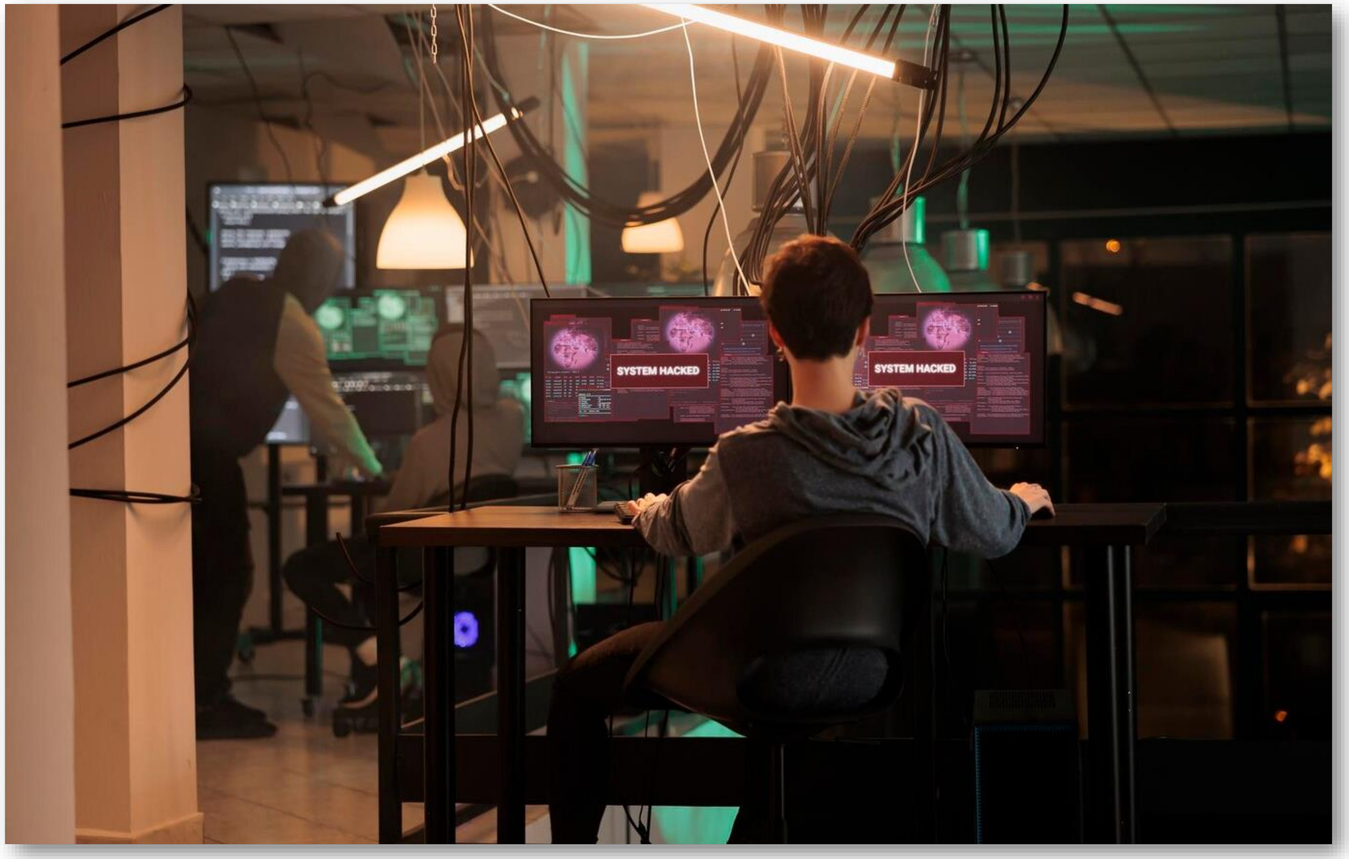
Lack of User Training and Awareness

Users who are unaware of cybersecurity best practices are more susceptible to falling victim to phishing, social engineering, and other attacks.

Insufficient Incident Response Plans

Lack of a well-defined incident response plan can result in delayed or ineffective responses to security incidents.

Understanding the dynamic nature of cybersecurity threats and vulnerabilities is crucial for organizations to implement proactive and comprehensive security measures. Regular risk assessments, security awareness training, and the adoption of industry best practices are essential components of a robust cybersecurity strategy.



Cybersecurity Breach

Cybersecurity breaches refer to incidents where unauthorized individuals or entities gain access to computer systems, networks, or data, leading to the compromise of confidentiality, integrity, or availability. These breaches can have severe consequences, including the theft of sensitive information, financial losses, damage to reputation, and disruption of business operations.

Equifax (2017)

One of the largest and most impactful breaches, Equifax, a major credit reporting agency, suffered a cyberattack that exposed the personal information of approximately 147 million people. The breach included names, Social Security numbers, birthdates, and addresses.

Yahoo (2013-2014)

Yahoo experienced two major breaches in 2013 and 2014. The 2013 breach affected all three billion user accounts, exposing names, email addresses, and hashed passwords. The 2014 breach involved the theft of personal information and led to a significant impact on Yahoo's business and reputation.

Target (2013)

Target, a retail giant, faced a data breach during the holiday shopping season in 2013. Attackers gained access to customer data, including credit card information, of around 40 million Target customers.

WannaCry Ransomware (2017)

The WannaCry ransomware attack spread globally, affecting hundreds of thousands of computers in more than 150 countries. It exploited a vulnerability in Windows systems and encrypted users' files, demanding a ransom in Bitcoin for decryption.

Marriott (2014-2018)

Marriott International experienced a data breach that exposed the personal information of around 500 million guests. The breach occurred through the Starwood guest reservation system and included details such as names, passport numbers, and payment card information.

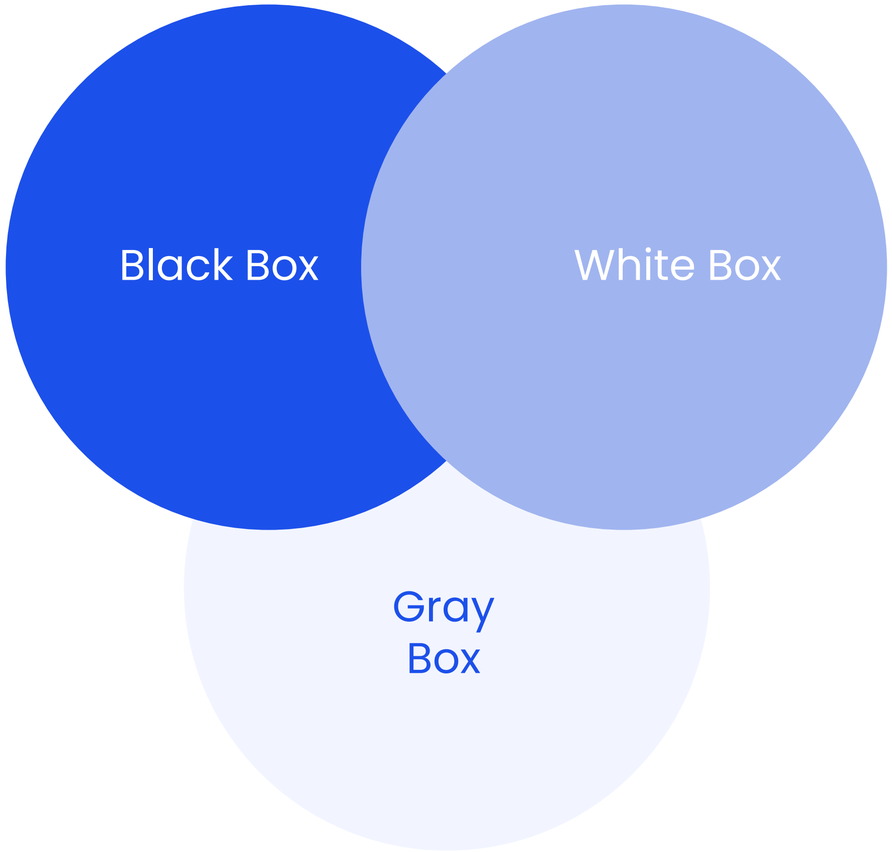
Captial One (2019)

Capital One suffered a data breach that exposed the personal information of over 100 million customers. The breach was a result of a misconfigured web application firewall, allowing an attacker to gain unauthorized access to sensitive data.

Pen Testing

Penetration testing, often referred to as ethical hacking, is a proactive cybersecurity approach designed to identify vulnerabilities in computer systems, networks, and applications. The goal is to simulate a real-world cyberattack to discover weaknesses that malicious actors could exploit. Penetration testing follows a systematic methodology to ensure a comprehensive assessment.

Types of Pen Testing



Black Box

Testers have no prior knowledge of the target system. This simulates an external attacker with limited information.

White Box

Testers have full knowledge of the target system, including source code and architecture. This simulates an insider threat or an advanced attacker with extensive information.

Grey Box

Testers have partial knowledge of the target system, simulating a scenario where an attacker has some insider information.

Pen testing Methodologies

1. Information Gathering (Reconnaissance):

Collect information about the target, including domain names, IP addresses, and network infrastructure. This phase involves passive reconnaissance to gather data without directly interacting with the target.

2. Scanning

In this phase, active reconnaissance is conducted to discover live hosts, open ports, and services running on the target. Tools like Nmap or Nessus may be used.

3. Enumeration

Enumerate services and identify potential vulnerabilities. This involves extracting information about users, shares, and system configurations.

Pen testing Methodologies

4.Vulnerability Analysis

Analyze the vulnerabilities discovered in the previous steps. This includes assessing the severity of each vulnerability and prioritizing them based on potential impact.

5.Exploitation

Attempt to exploit identified vulnerabilities to gain unauthorized access or escalate privileges. This phase involves using various tools and techniques to simulate real-world attacks.

7. Reporting

Compile a detailed report documenting the findings, including vulnerabilities, exploited paths, and recommended remediation measures..

6. Post-Exploitation

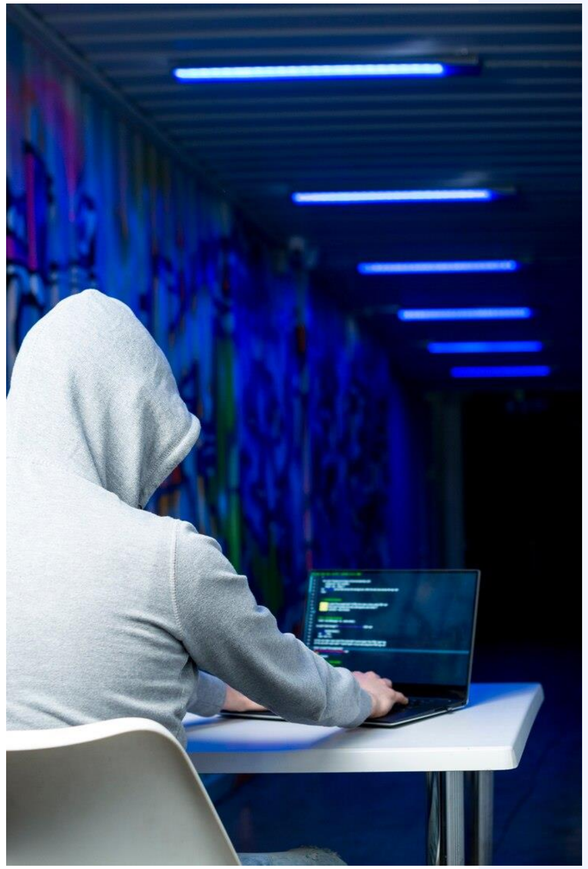
If successful, assess the extent of the compromise and identify opportunities for further exploitation. This phase helps understand the potential impact of a successful attack.

This report is crucial for stakeholders to understand and address security weaknesses

Vision

Profit

Tools Used In Pen Testing



Nmap

Network mapping tool used for host discovery and service enumeration.

Metasploit

Framework for developing, testing, and executing exploits. It aids in automated penetration testing.

Burp Suite

Web application security testing tool for discovering and exploiting vulnerabilities in web applications.

Wireshark

Network protocol analyzer for capturing and analyzing network traffic.

OWASP Zap

Open-source security testing tool for finding vulnerabilities in web applications.

John the Ripper

Password cracking tool used for testing weak passwords.

Common Practices of Pen testing

01

Red Team vs. Blue Team

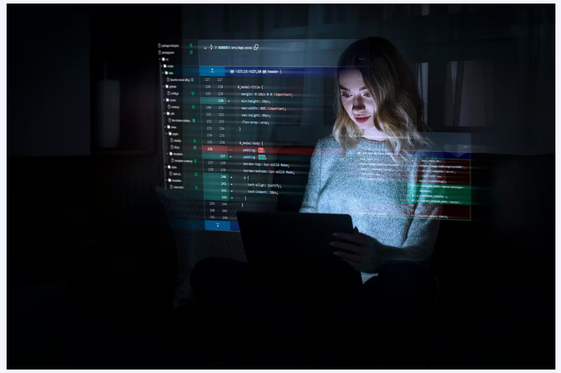
- Red Team: Simulates attackers to identify vulnerabilities.
- Blue Team: Defends against simulated attacks, testing the organization's detection and response capabilities

Penetration testing is an essential component of a robust cybersecurity strategy, helping organizations identify and address security weaknesses before malicious actors can exploit them. It is part of a broader security posture that includes preventive, detective, and corrective measures to ensure the resilience of an organization's information systems.

Frameworks and Standards for Cyber Security

NIST Cybersecurity Framework

Developed by the National Institute of Standards and Technology (NIST), the framework provides a set of voluntary guidelines, standards, and best practices for managing and improving an organization's cybersecurity risk management processes. It consists of five core functions: Identify, Protect, Detect, Respond, and Recover.



ISO/IEC 27001

The ISO/IEC 27001 standard is an internationally recognized framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It provides a risk-based approach to information security and is accompanied by ISO/IEC 27002, which offers a set of security controls.

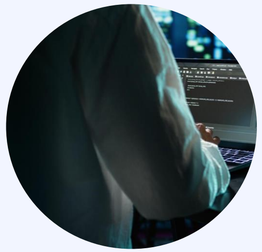
CIS Critical Security Controls (CIS Controls)

Developed by the Center for Internet Security (CIS), the CIS Controls are a set of best practices designed to help organizations prioritize and implement key cybersecurity actions. The controls are organized into three implementation groups, providing a roadmap for organizations to enhance their security posture.

Frameworks and Standards for Cyber Security

COBIT (Control Objectives for Information and Related Technologies)

COBIT, developed by ISACA, is a framework that provides a comprehensive governance and management system for enterprise IT. It helps organizations align their IT strategies with business objectives and ensures effective IT governance, risk management, and compliance.



FISMA (Federal Information Security Management Act)

FISMA is a U.S. federal law that defines a comprehensive framework for securing government information and systems. It outlines requirements for federal agencies to develop, document, and implement information security programs.

PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. It is mandated for organizations involved in payment card transactions

Other Frameworks

2015

HIPAA (Health Insurance Portability and Accountability Act)

HIPAA establishes standards for the privacy and security of protected health information (PHI). It applies to healthcare providers, health plans, and healthcare clearinghouses, as well as their business associates.

2016

GDPR (General Data Protection Regulation)

GDPR is a European Union regulation that focuses on data protection and privacy for individuals within the EU. It sets guidelines for the collection, processing, and storage of personal data and imposes strict requirements on organizations handling such data.

2017

ITIL (Information Technology Infrastructure Library)

ITIL is a set of practices for IT service management (ITSM) that aligns IT services with the needs of the business. While not specific to cybersecurity, ITIL includes processes and controls that contribute to overall IT security.

2018

NIST Special Publications (SPs)

In addition to the NIST Cybersecurity Framework, NIST publishes various Special Publications that provide detailed guidance on specific topics such as risk management (NIST SP 800-37), security controls (NIST SP 800-53), and incident response (NIST SP 800-61).

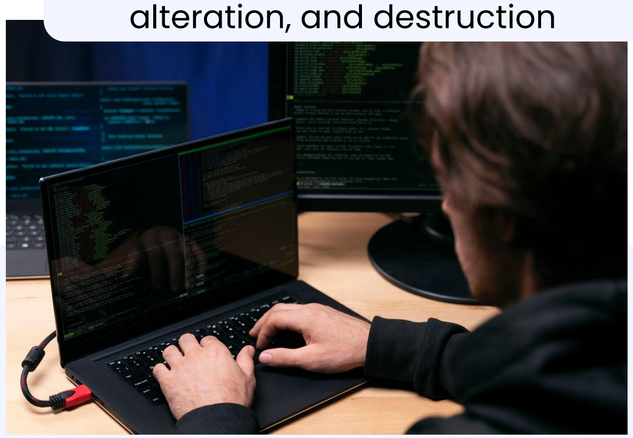
Privacy Meets Security – Data Protection

The intersection of privacy and security, particularly in the context of data protection, is crucial for maintaining the confidentiality, integrity, and availability of sensitive information while respecting individuals' privacy rights. Both privacy and security play essential roles in safeguarding data, and various regulations and frameworks emphasize the importance of balancing these concerns.

Privacy and Security as Complementary Goals

Privacy: Focuses on the appropriate collection, use, and sharing of personal information, ensuring that individuals' rights are respected.

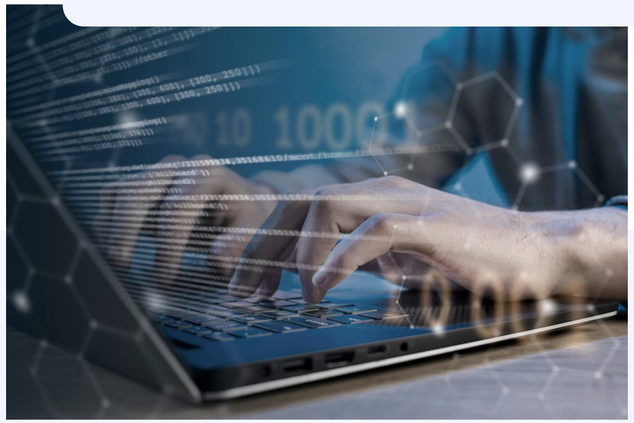
Security: Focuses on safeguarding information from unauthorized access, disclosure, alteration, and destruction



Legal Frameworks

GDPR (General Data Protection Regulation):

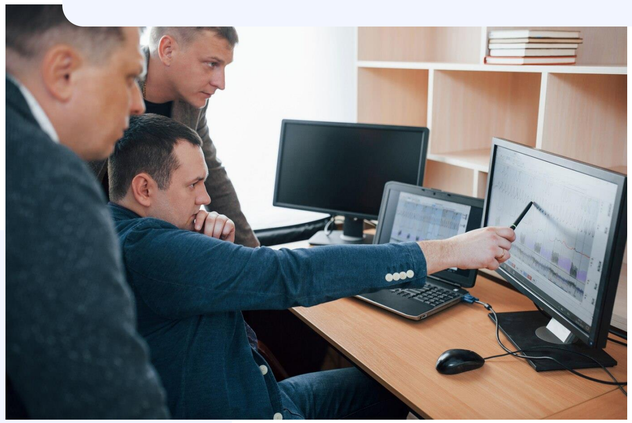
HIPAA (Health Insurance Portability and Accountability Act):



Data Minimization and Purpose Limitation

Privacy Aspect: Collect only the data necessary for the intended purpose and avoid unnecessary data processing.

Security Aspect: Implement access controls and encryption to limit access to data based on the principle of least privilege.



Data Protection Best Practices

15%

Consent Management:

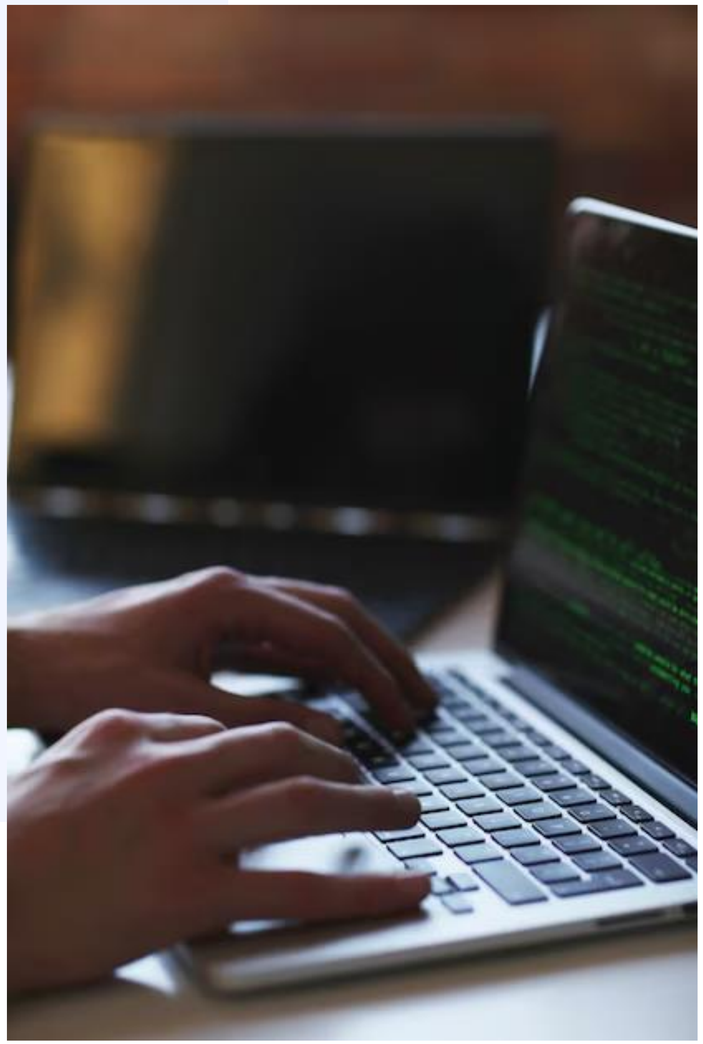
Obtain informed consent from individuals before processing their personal data for specific purposes

85%

Data Breach Response:

Promptly notify affected individuals and relevant authorities in the event of a data breach

Have robust incident response plans and security measures to prevent, detect, and mitigate data breaches.



Anonymization and Pseudonymization:

Anonymize or pseudonymize data to reduce the risk of identification and protect individuals' privacy.

Security Awareness Training

Ensure employees are aware of privacy policies and understand the importance of handling personal information responsibly.

Privacy Policies

Definition

Privacy policies are legal documents that inform individuals about how an organization collects, uses, processes, and protects their personal information. These policies are essential for building trust with users and ensuring compliance with privacy laws and regulations

Information Collected

Specify the types of personal information collected, including categories such as names, contact details, payment information, and any other relevant data.

Methods of Collections

Explain how the organization collects personal information, whether it's through websites, mobile applications, forms, or other means.

How to define privacy policy?

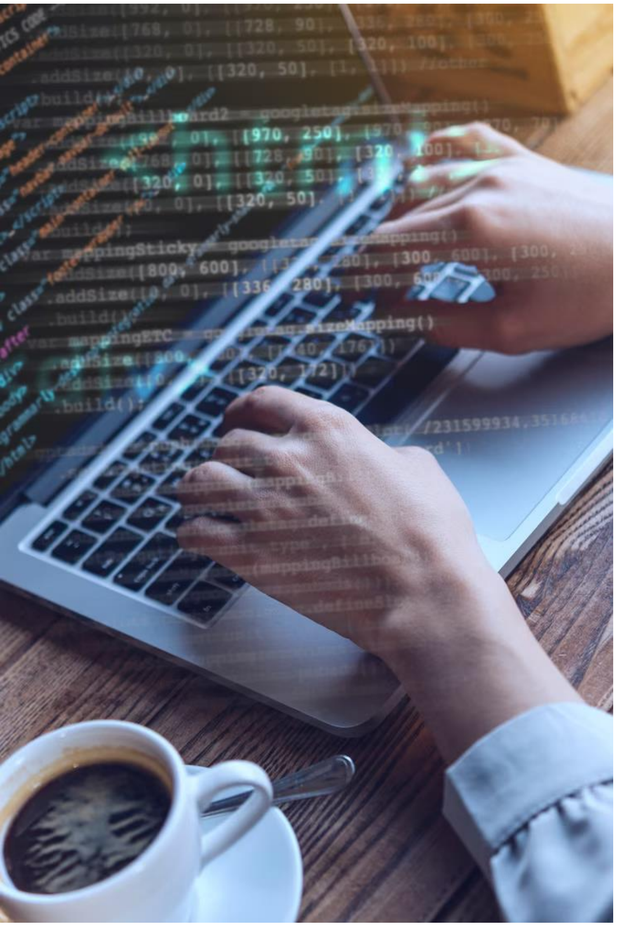
Define key terms used in the privacy policy to ensure clarity and a common understanding of terms such as "personal information," "processing," and "data controller."

Purpose of Processing

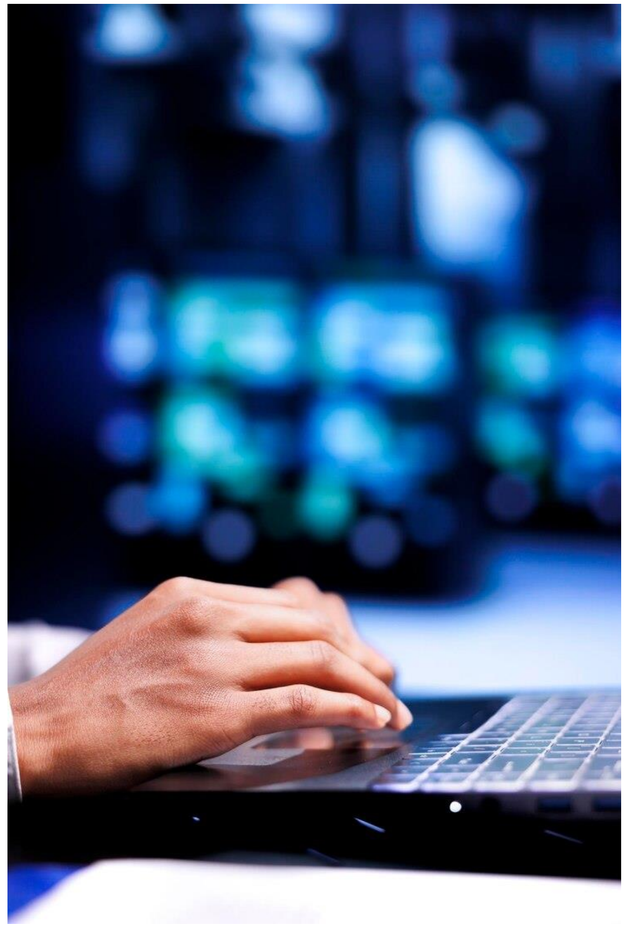
Clearly outline the purposes for which personal information is collected and processed. This could include fulfilling contracts, providing services, marketing, and improving user experience.

Data Retention

Specify how long the organization will retain personal information. Clearly outline the criteria used to determine the retention period.



Security Claims Privacy Seal Programs



Security claims privacy seal programs, often referred to as certification or seal programs, are initiatives that aim to provide assurance to users and consumers regarding the privacy and security practices of a product, service, or organization. These programs typically involve an assessment or audit of the entity's privacy and security measures against established standards or criteria. Upon successful completion, the organization is awarded a "seal" or certification that can be displayed to signal adherence to certain privacy and security standards.

When considering participating in a security claims privacy seal program, organizations should carefully review the program's requirements, assess its relevance to their industry and operations, and weigh the potential benefits against the costs and responsibilities associated with certification. Additionally, users and consumers should be aware of the significance and scope of different certification programs to make informed decisions about the products and services they use.

Key aspects of Security claims privacy seal programs

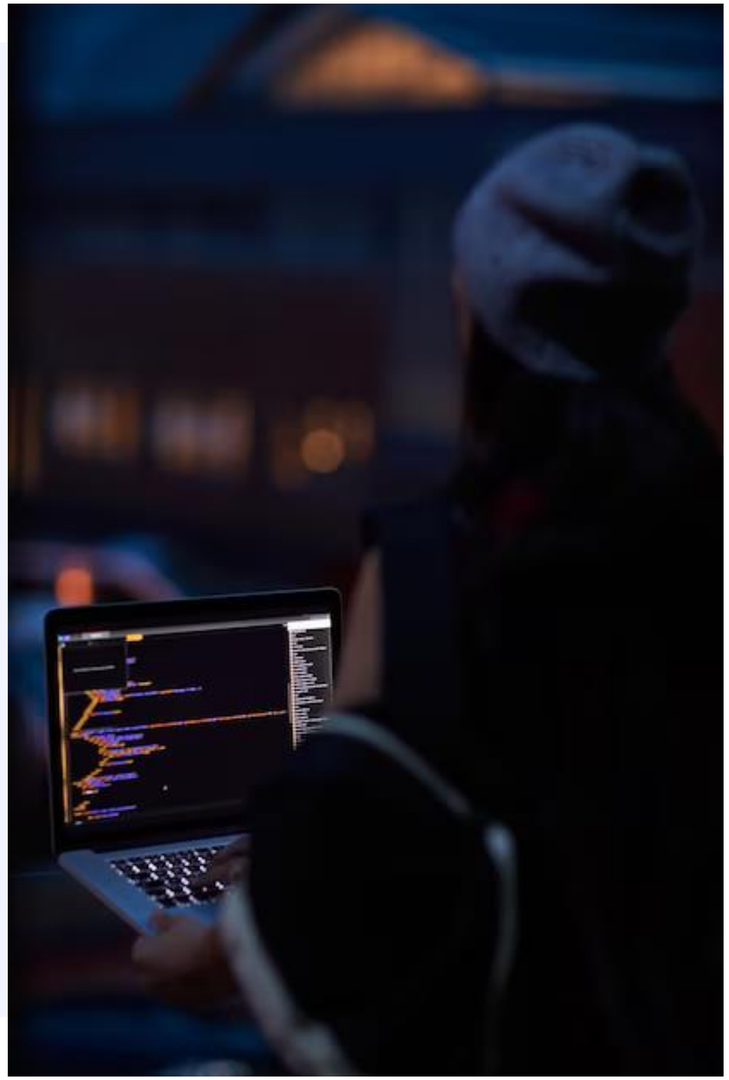
Certification Programs

Common Criteria: Programs often follow established criteria or standards, such as ISO/IEC 27001 for information security management or Privacy by Design principles for privacy. Certification may also be sector-specific, like the Payment Card Industry Data Security Standard (PCI DSS) for the payment industry.

Privacy Seals

TRUSTe (now TrustArc): TRUSTe was a well-known privacy certification and compliance organization. TrustArc, its successor, provides certification and privacy management solutions.

EU-US Privacy Shield: While not a seal program in the traditional sense, the EU-US Privacy Shield was a framework for data transfer between the European Union and the United States. Organizations adhering to its principles were considered compliant.



20%

55%

30%

Key aspects of Security claims privacy seal programs

Benefits for Organizations:

Consumer Trust: The seal serves as a visible symbol of a commitment to privacy and security, fostering trust among users and customers.

Market Differentiation: Certification can be a competitive advantage, differentiating a product or service in the market.

Legal and Regulatory Compliance: Certification may help organizations demonstrate compliance with privacy and security laws and regulations.

Security Seals

Common Criteria Certification: Common Criteria is an international standard for the certification of information technology products, particularly those related to security. It evaluates the security features and capabilities of products.

FIPS (Federal Information Processing Standards): FIPS are standards issued by the National Institute of Standards and Technology (NIST) and are often a requirement for products used in U.S. government systems.

Independent Assessments

Many programs involve third-party assessments or audits by independent organizations. This adds credibility to the certification process and assures users that the evaluation is unbiased.

Thanks for your attention!

Listen to Cheri Cheri Lady by Modern Times and you will almost forget the fact that you haven’t gotten laid ever