Tishk International University
Faculty of Applied Science
Cybersecurity Department

Lecture 10 : Cybersecurity in Business & E-commerce

CBS221/A : Ethics and Legal Issues in Cybersecurity

Week 11 : 14-18/12/2025

Instructor: Prof. Dr. Qaysar Salih Mahdi

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Cybersecurity in Business & E-commerce

- **Objectives:**
- 1. Understand cybersecurity challenges in business and e-commerce
- 2. Explore ethical issues in financial data protection
- 3. Identify liability considerations for businesses handling sensitive data
- 4. Apply cybersecurity frameworks and best practices

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Introduction to Business & E-commerce Cybersecurity

- - Importance of cybersecurity in business and e-commerce
- - Diagram: E-commerce Cybersecurity Overview
- Link: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
- - Explanation: Interaction between web apps, payment systems, data storage, and security controls

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Introduction to Business & E-commerce Cybersecurity

IT governance has become a common theme within enterprises, as made evident by the inclusion of governance as a key component of the COBIT® 2019 framework[1] and the publication of innumerable articles addressing the importance of implementing in-house governance frameworks.[2] However, various forms of governance are relevant when reviewing current trends.[3] Cybersecurity risk management governance takes a front seat in the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, released in late February 2024.[4] A review of NIST CSF 2.0 from an agency theory perspective provides cybersecurity and governance professionals with a conceptual understanding of how governance can be extended to cybersecurity risk management.[5] This level of understanding allows decision makers the opportunity to identify the potential motivation of organization members, predict where potential conflicts of interest may occur, and address cybersecurity risk management governance to reduce these issues.

Governance

To "govern" is to conduct the policy, actions, and affairs of a state, organization, or people.[6] Therefore, governing involves acting on another's behalf with the implied intent of adding value for those being governed or those affected by the governing policies and actions. NIST CSF 2.0 (figure 1)[7] elevates "govern" from an identity function category to the newest and most important function in the cybersecurity risk management framework. NIST CSF 2.0 states, "The govern function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five functions in the context of mission and stakeholder expectations."

FIGURE 1

NIST CSF 2.0 Govern Function and Categories

Function	Categories
Govern: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	• Organizational Context • Risk Management Strategy • Roles, Responsibilities, and Authorities • Policy • Oversight • Cybersecurity Supply Chain Risk Management

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Theoretical Principles

- - CIA Triad: Confidentiality, Integrity, Availability
- - Ethical Principles: Privacy, Consent, Transparency
- - Legal Principles: Compliance with GDPR, PCI DSS, ISO 27001
- - Link: https://www.iso.org/isoiec-27001-information-security.html
- - Explanation: Technical principles (CIA) guided by ethics and enforced by law

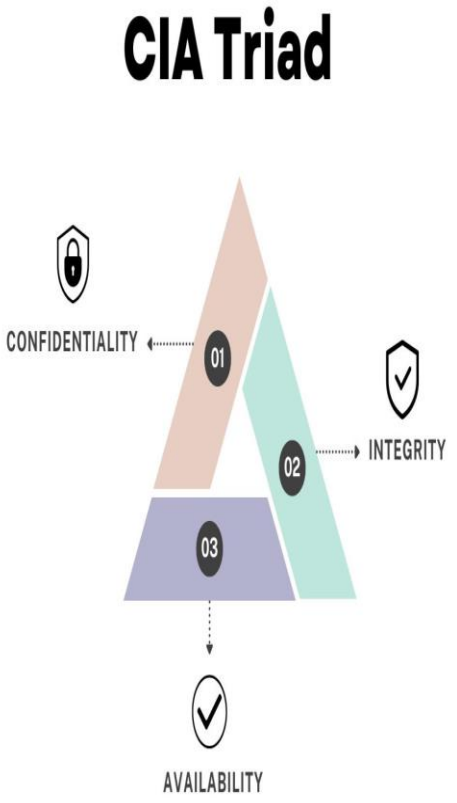
Tishk International University
Faculty of Applied Science
Cybersecurity Department

What is the CIA Triad?

The CIA Triad is a foundational information security model. It helps organizations to protect their sensitive data and systems. Its explicit formulation as a core triad gained prominence in the 1980s and 1990s, with roots as old as the 1972 Anderson Report. It has three core principles:

- **Confidentiality -** Confidentiality ensures that the data is only accessible to authorized individuals and not to unauthorized parties.
- **Integrity -** Integrity means to maintain the accuracy and trustworthiness of data and protect it from unauthorized alteration or corruption.
- **Availability -** Availability ensures that authorized users can access the information whenever needed.

These three pillars together act as the backbone of cybersecurity. It helps organizations to evaluate risks, implement controls, and build resilient systems. NIST SP 800-12 Rev 1 defines the CIA Triad as an essential component to protect information and ensure operational continuity in digital systems.



Tishk International University
Faculty of Applied Science
Cybersecurity Department

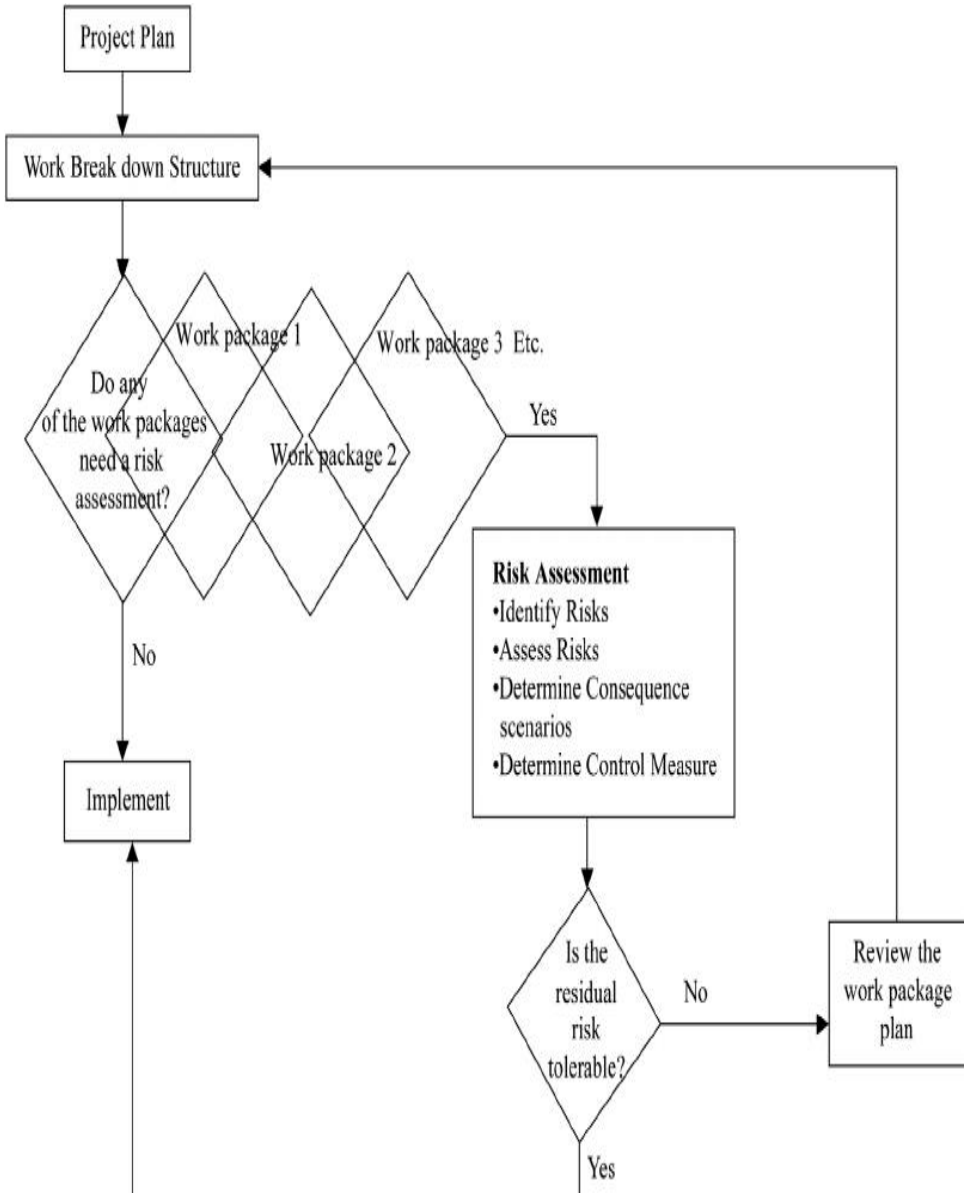
Mathematical Principles & Equations

- 1. Compliance Risk Score: CR = (I × V) / C
- I = Impact, V = Vulnerability, C = Controls
- 2. Probability of Financial Breach: P(B) = 1 - (1 - P_t)^n
- - Link: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/measuring-cybersecurity-risk
- - Explanation: Estimates risk and breach probability

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Financial Risk Calculation Flowchart

Financial risk, as one of the most influential and destructive risks in business, will make enterprises unable to escape the fate of bankruptcy if not warned and prevented in time. In the paper, we conducted research on the financial risk early warning of listed companies. A total of 250 companies were randomly selected from the Chinese A-share .

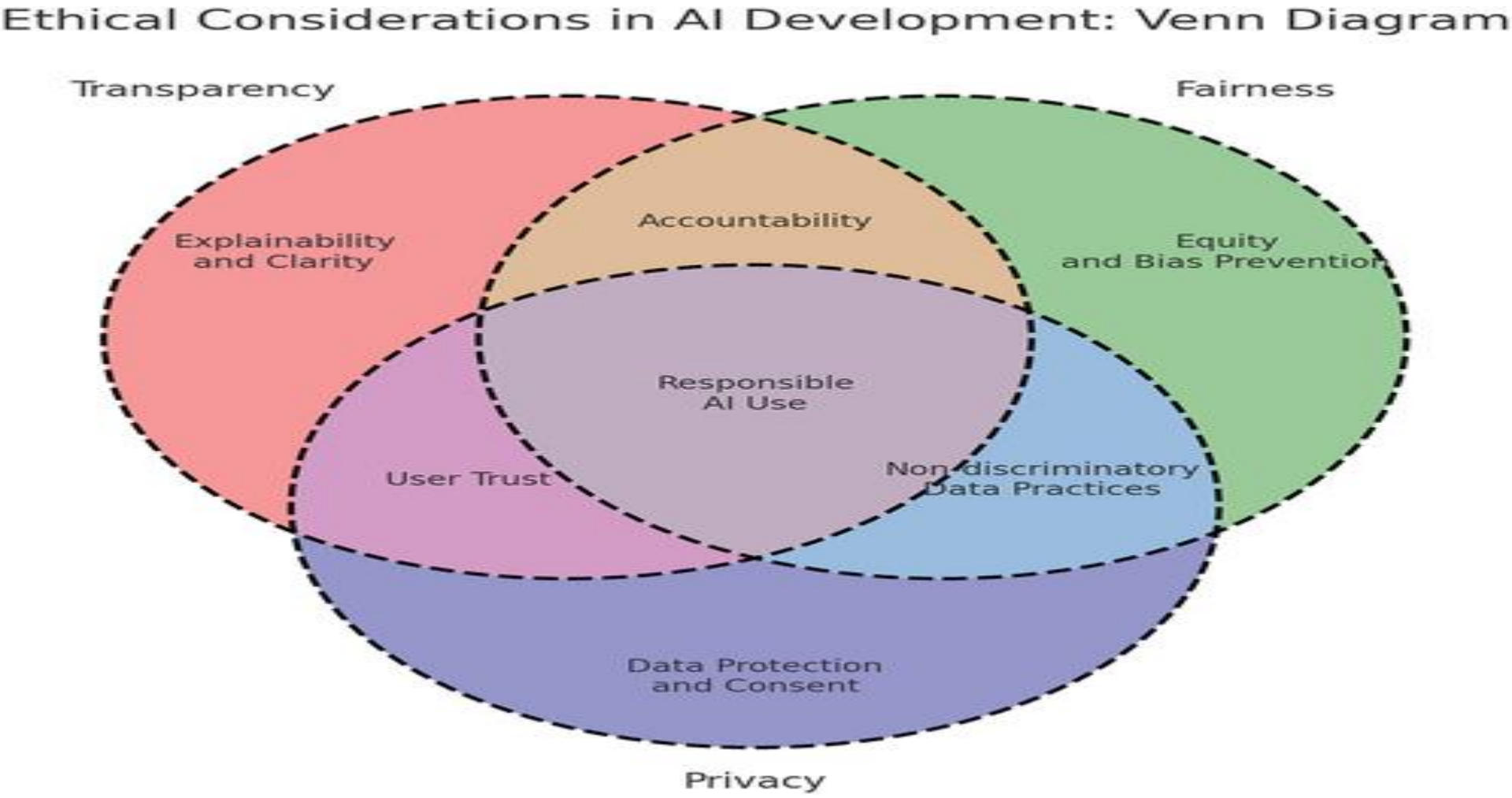


Tishk International University
Faculty of Applied Science
Cybersecurity Department

Ethical Issues in Financial Data Protection

- - Topics: Unauthorized access, insider threats, phishing, ransomware
- - Diagram: Financial Data Protection Ethics Flowchart
- Link: https://www.pwc.com/gx/en/services/forensics/cybersecurity-data-protection.html
- - Explanation: Stepwise process to ensure ethical handling of customer data

Tishk International University
Faculty of Applied Science
Cybersecurity Department



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Liability in Cybersecurity

- Legal responsibilities for protecting customer data

Link: https://www.abi.org.uk/products-and-issues/topics-and-issues/cyber-insurance

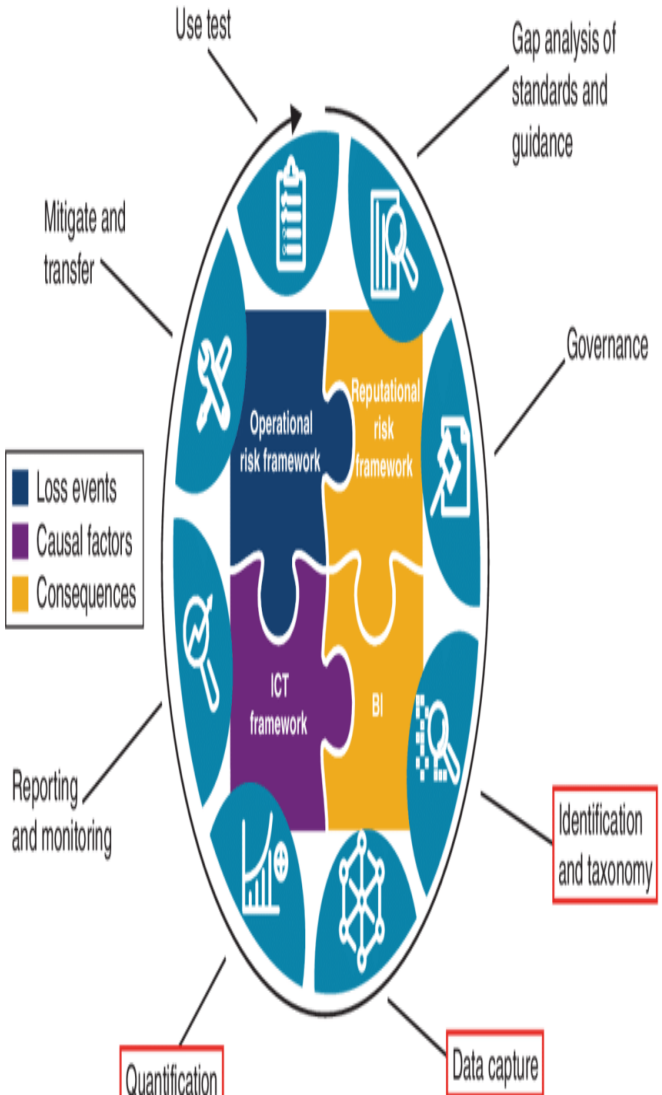
- - Explanation: Legal obligations, insurance, and compliance

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Cyber, or technology, risk is a growing area of concern in almost every industrysector.

1. The Bank of England's Systemic Risk Survey (June 2018) ranked cyber risk as the joint second-most-cited source of risk for the UK financial system; the criminal organization behind the Cobalt malware alone is said to be responsible for causing over €1 billion worth of losses in banks in more than forty countries.
2. The rapid rate of growth of cyber-related incidents has made it exceedingly difficult to keep up with the associated cyber threats, owing in no small part to the continual advances in complexity and interconnectivity of the technology landscape.

As a testament to its high profile, not a month goes by without us hearing of a head-line breach, a cyber crime, a software malfunction or a hardware failure that incurs substantial costs for the affected organizations and victims, including the subsequent regulatory fines that are imposed.



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Cybersecurity Frameworks for E-commerce

What is a cybersecurity framework?

A cybersecurity framework is a structured set of standards, guidelines, and best practices designed to help organizations manage and reduce cybersecurity risks. These frameworks provide a comprehensive roadmap for assessing, monitoring, and mitigating potential threats. By establishing consistent processes and controls, they help organizations implement a proactive security strategy, manage regulatory requirements, and facilitate communication among security professionals and stakeholders.

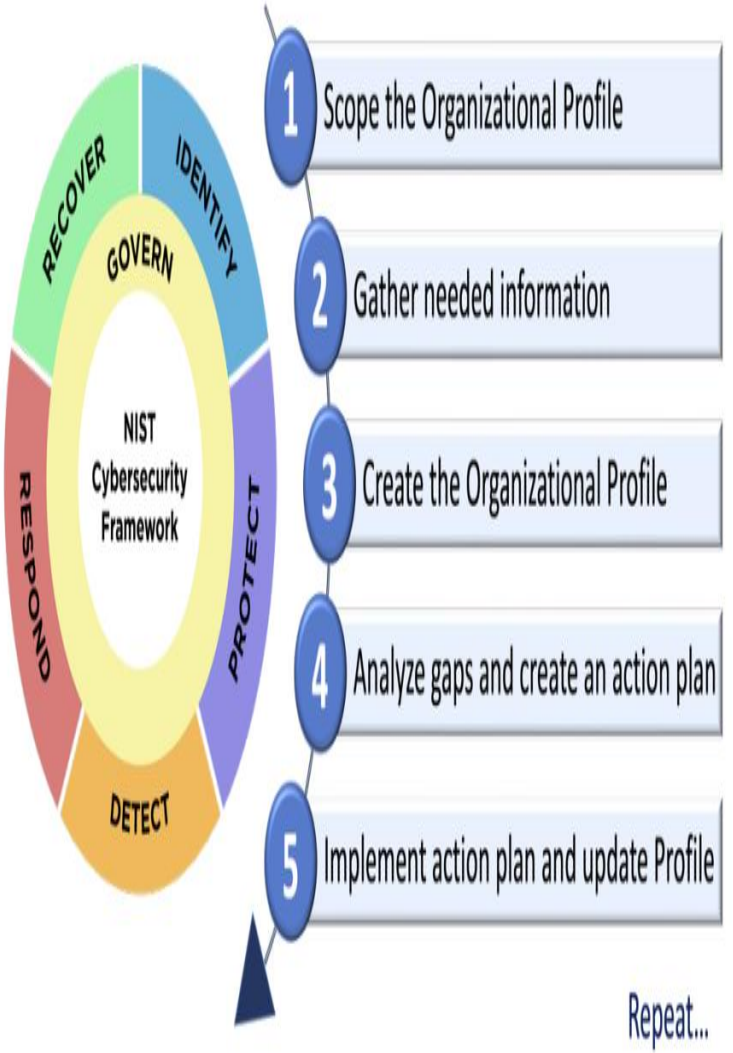
Cybersecurity frameworks are critical for aligning security efforts across different teams, industries, and countries. They enable security leaders—such as CISOs, risk management teams, and IT leadership—to effectively assess their own security posture as well as that of third-party vendors, ensuring a unified approach to threat mitigation.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

1. NIST 2.0 Framework

The NIST Cybersecurity Framework was established in response to an executive order by former President Obama — Improving Critical Infrastructure Cybersecurity — which called for greater collaboration between the public and private sector for identifying, assessing, and managing cyber risk.

While compliance is voluntary, NIST has become the gold standard for assessing cybersecurity maturity, identifying security gaps, and meeting cybersecurity regulations.



Tishk International University
Faculty of Applied Science
Cybersecurity Department

2. ISO 27001 & ISO 27002 Frameworks

Created by the International Organization for Standardization (ISO), ISO 27001 and ISO 27002 certifications are considered the international cybersecurity standard for validating a cybersecurity program — internally and across third parties.

With an ISO certification, companies can demonstrate to the board, customers, partners, and shareholders that they are doing the right things with cyber risk management. Likewise, if a vendor is ISO 27001/2 certified, it's a good indicator (although not the only one) that they have mature cybersecurity practices and controls in place.

The downside is that the process requires time and resources; organizations should only proceed if there is a true benefit, such as the ability to win new business. The certification is also a point-in-time exercise and could miss evolving risks that continuous monitoring can detect.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

3. SOC2 Framework

Service Organization Control (SOC) Type 2 is a trust-based cybersecurity framework and auditing standard developed by the American Institute of Certified Public Accountants (AICPA) to help verify that vendors and partners are securely managing client data.

SOC2 specifies more than 60 compliance requirements and extensive auditing processes for third-party systems and controls. Audits can take a year to complete. At that point, a report is issued which attests to a vendors' cybersecurity posture.Because of its comprehensiveness, SOC2 is one of the toughest security frameworks to implement — especially for organizations in the finance or banking sector who face a higher standard for compliance than other sectors. Nevertheless, it's an important security framework that should be central to any third-party risk management program.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Compliance

Read our guide to SOC2 compliance for requirements, types of SOC reports and standards, leadership recommendations, and a complete SOC2 compliance checklist.

Bitsight Vendor Risk Management's latest enhancement – Instant Insights – leverages AI to surface and summarize the most important details from vendor-provided SOC 2 reports. With Instant Insights, GRC teams can work more efficiently through the vendor onboarding and assessment process, ultimately responding to requests from business stakeholders more quickly.

4. NERC-CIP Framework

Introduced to mitigate the rise in attacks on U.S. critical infrastructure and growing third-party risk, the North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) is a set of cybersecurity standards designed to help those in the utility and power sector reduce cyber risk and ensure the reliability of bulk electric systems.

The NERC-CIP security framework requires impacted organizations to identify and mitigate third-party cyber risks in their supply chain.

NERC-SIP stipulates a range of controls including categorizing systems and critical assets, training personnel, incident response and planning, recovery plans for critical cyber assets, vulnerability assessments, and more. Read more about effective strategies for achieving NERC-CIP compliance.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

5. HIPAA Framework

The Health Insurance Portability and Accountability Act (HIPAA) is a cybersecurity framework that requires healthcare organizations to implement controls for securing and protecting the privacy of electronic health information.Per HIPAA, in addition to demonstrating compliance against cyber risk best practices — such as training employees — companies in the sector must also conduct risk assessments to manage and identify emerging risk.HIPAA compliance remains a keen challenge for healthcare organizations, as Bitsight research suggests.

6. GDPR Framework

The General Data Protection Regulation (GDPR) was adopted in 2016 to strengthen data protection procedures and practices for citizens of the European Union (EU). The GDPR impacts all organizations that are established in the EU or any business that collects and stores the private data of EU citizens — including U.S. businesses.The security framework includes 99 articles pertaining to a company's compliance responsibilities including a consumer's data access rights, data protection policies and procedures, data breach notification requirements (companies must notify their national regulator within 72 hours of breach discovery), and more.Fines for non-compliance are high; up to €20,000,000 or 4% of global revenue, and the EU is not shy about enforcing them.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

7. FISMA Framework

The Federal Information Security Management Act (FISMA) is a comprehensive cybersecurity framework that protects federal government information and systems against cyber threats. FISMA also extends to third parties and vendors who work on behalf of federal agencies.

The FISMA security framework is aligned closely with NIST cybersecurity standards and requires agencies and third parties to maintain an inventory of their digital assets and identify any integrations between networks and systems.

Sensitive information must be categorized according to risk and security controls must meet minimum security standards as defined by FIPS and NIST 800 guidelines. Impacted organizations must also conduct cybersecurity risk assessments, annual security reviews, and continuously monitor their IT infrastructure.

Cybersecurity frameworks are vital guideposts

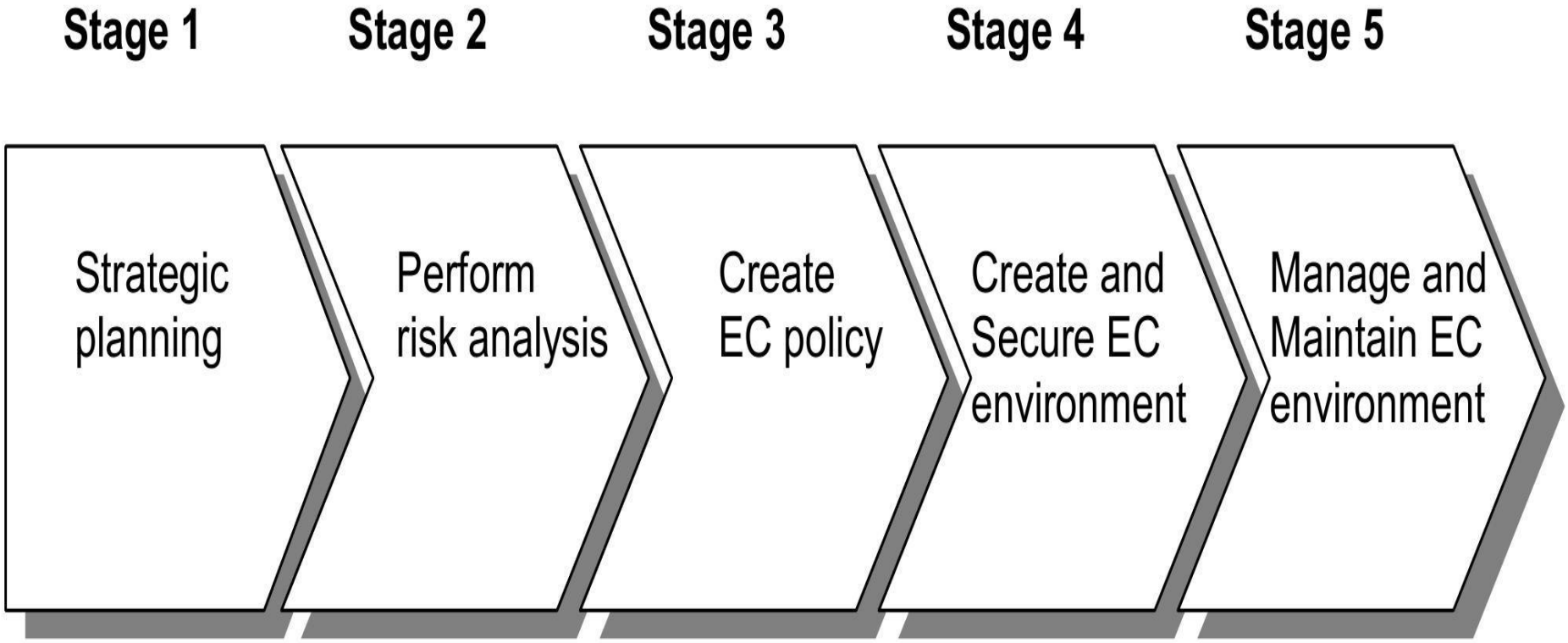
Cybersecurity frameworks provide a useful (and often mandated) foundation for integrating cyber security risk management into your security performance management and third-party risk management strategy.

With a security framework as your guidepost, you'll gain vital insight into where your highest security risk is and feel confident communicating to the rest of the organization that you're committed to security excellence.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

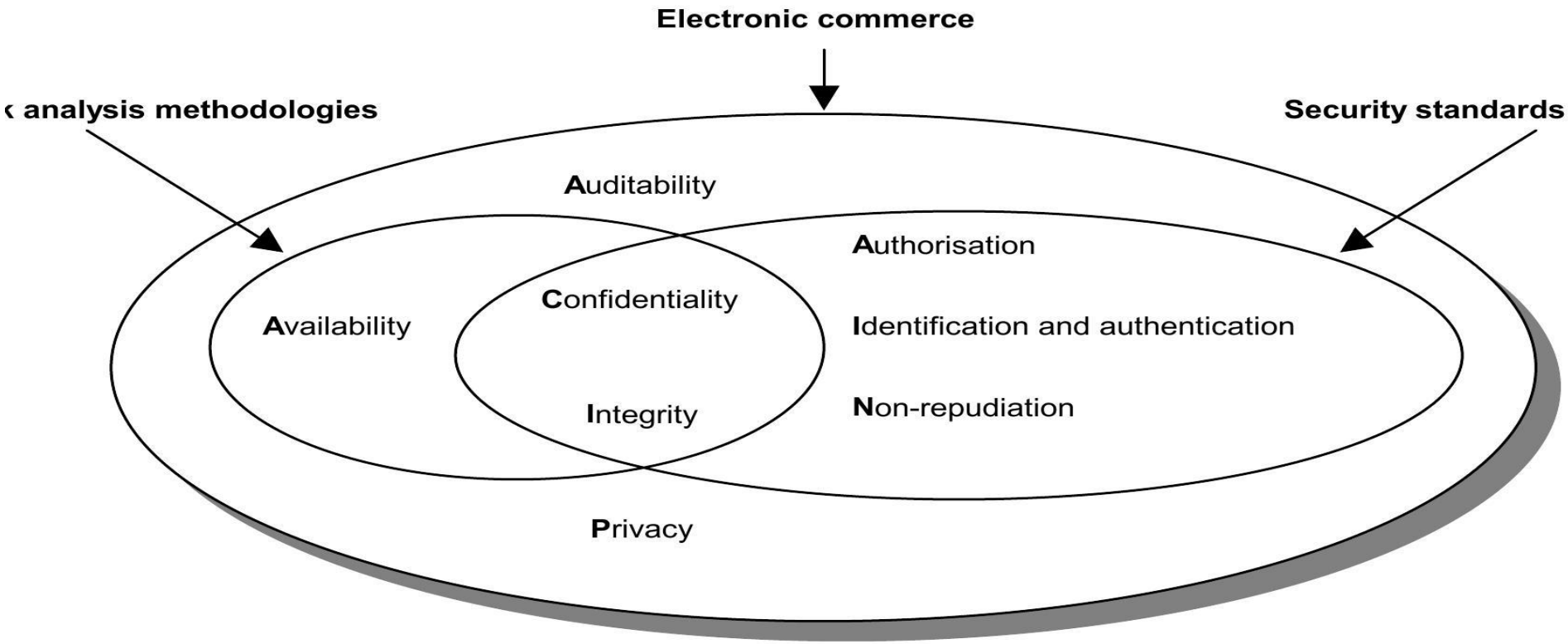
Stages in electronic commerce

electronic commerce environment consisting of the following [ERNS98]:
Figure 1 — Stages in electronic commerce



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Security requirements for electronic commerce environment security requirements and how they fit together to form the electronic commerce secur



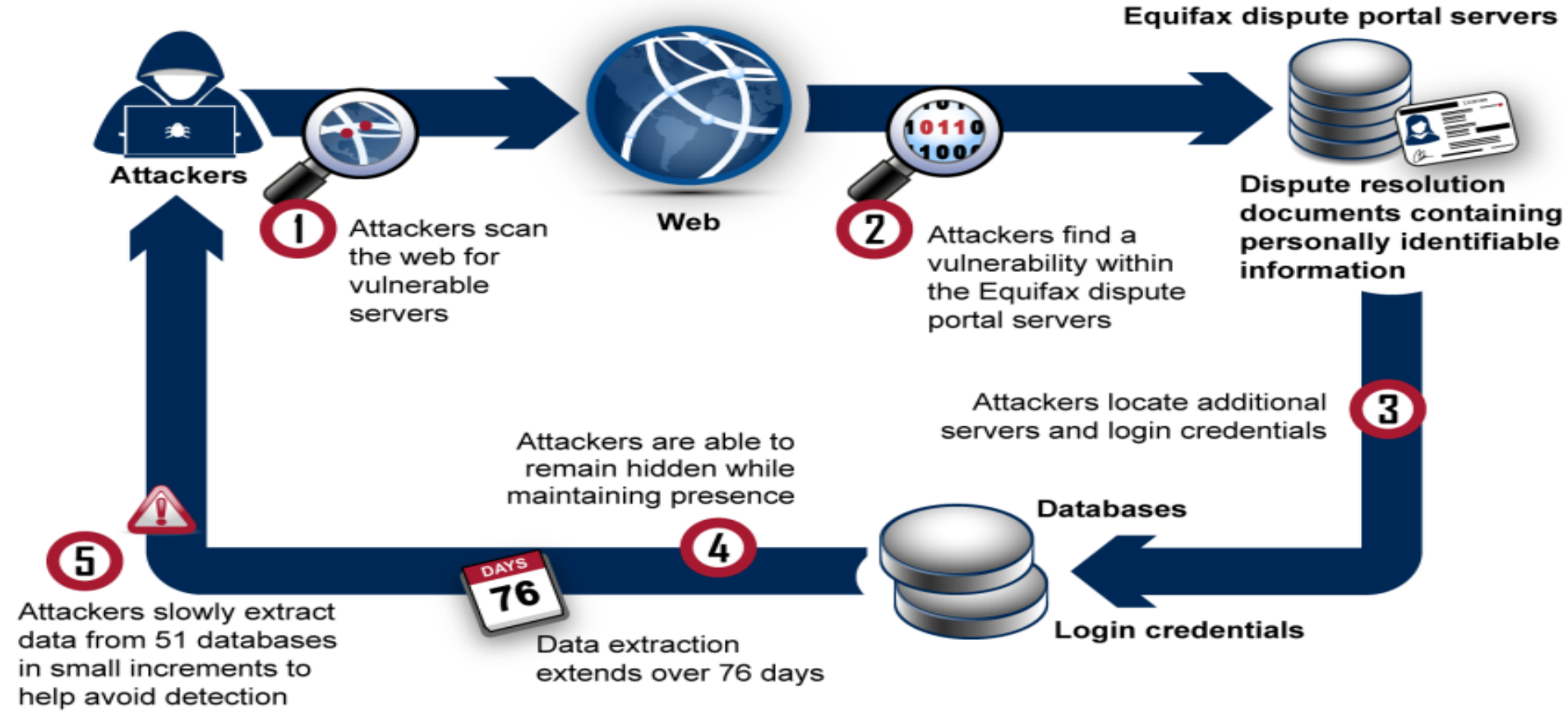
Tishk International University
Faculty of Applied Science
Cybersecurity Department

Case Study 1: Financial Data Breach

A financial data breach case study, such as the Capital One breach, involves a security incident where sensitive customer data is exposed due to a cybersecurity vulnerability, such as a misconfigured firewall. These breaches result in financial, legal, and reputational consequences for the company, including costs from remediation, fines, and loss of customer trust, and highlight the need for improved security measures like patching, network segmentation, and strong access controls

Tishk International University
Faculty of Applied Science
Cybersecurity Department

How Attackers Exploited Vulnerabilities in the 2017 Breach, Based on Equifax Information



Source: GAO, based on information provided by Equifax. | GAO-18-559

Tishk International University
Faculty of Applied Science
Cybersecurity Department

A Case Study of the insider threat cases

The notorious insider threat cases, analyze their outcomes, and investigate how these attacks happened. We'll also see how these internal data breach examples could have been prevented.

- - Incident description, impact, lessons learned
- - Link: https://www.verizon.com/business/resources/reports/dbir/
- - Explanation: Identifies gaps in ethical handling and risk mitigation

Common Attack Tactics Carried Out in SWIFT Hacks

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Case Study 2: E-commerce Cyber Attack

Case Study 1: LuxeCart Inc.

Overview:

LuxeCart Inc. operates in the eCommerce sector, specializing in luxury goods. The company, with a workforce of 300, serves over one million customers globally and generates approximately $200 million in annual revenue. Known for its premium service and high-quality products, LuxeCart has established a significant online presence.

Summary:

- **Date of Incident: March 15, 2023**
- **Type of Attack: Ransomware**
- **Point of Entry: Phishing email targeting an employee**

Incident Report:

The cybersecurity breach at LuxeCart Inc. was initially detected through the company's network monitoring tools, which identified abnormal outbound traffic patterns. This anomaly was picked up less than four hours after the breach, signaling an efficient detection system. The attack was traced back to a phishing email that an employee inadvertently opened, which deployed ransomware across the network.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

The ransomware quickly encrypted vital data, including customer transaction histories and credit card information, and demanded a ransom paid in cryptocurrency. The attack threatened the integrity and confidentiality of LuxeCart's data and posed severe reputational risks.

Immediate Response Actions:

1.The incident response team was swiftly activated to assess and address the situation.

2.Compromised systems were quickly isolated to prevent the ransomware from spreading further.

3.Law enforcement and cybersecurity experts were notified to aid in the response and potential pursuit of the perpetrators.

Communication Strategy:

LuxeCart adopted a transparent communication approach in response to the crisis. The company informed its customers and stakeholders through direct emails and issued press releases to manage the public narrative. Updates were also consistently provided via LuxeCart's social media platforms, ensuring all parties were informed of the situation and the steps taken.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Resolution and Post-Incident Actions:

LuxeCart decided against paying the ransom despite the pressure. Instead, the company restored its data from backups that were fortunately unaffected by the attack. After the incident, LuxeCart comprehensively reviewed its cybersecurity policies and systems. This led to:

1.The implementation of more stringent access controls and the introduction of multi-factor authentication for all internal systems.

2.A comprehensive cybersecurity training program was implemented company-wide to educate employees on best practices and phishing prevention.

3.Regular audits and updates to the company's cybersecurity infrastructure were scheduled to prevent future incidents.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Impact Analysis:

•Short-Term: The attack's immediate aftermath saw LuxeCart's online operations shut down temporarily, resulting in a direct financial loss of around $5 million. Additionally, the company faced several lawsuits filed by customers whose data was compromised.

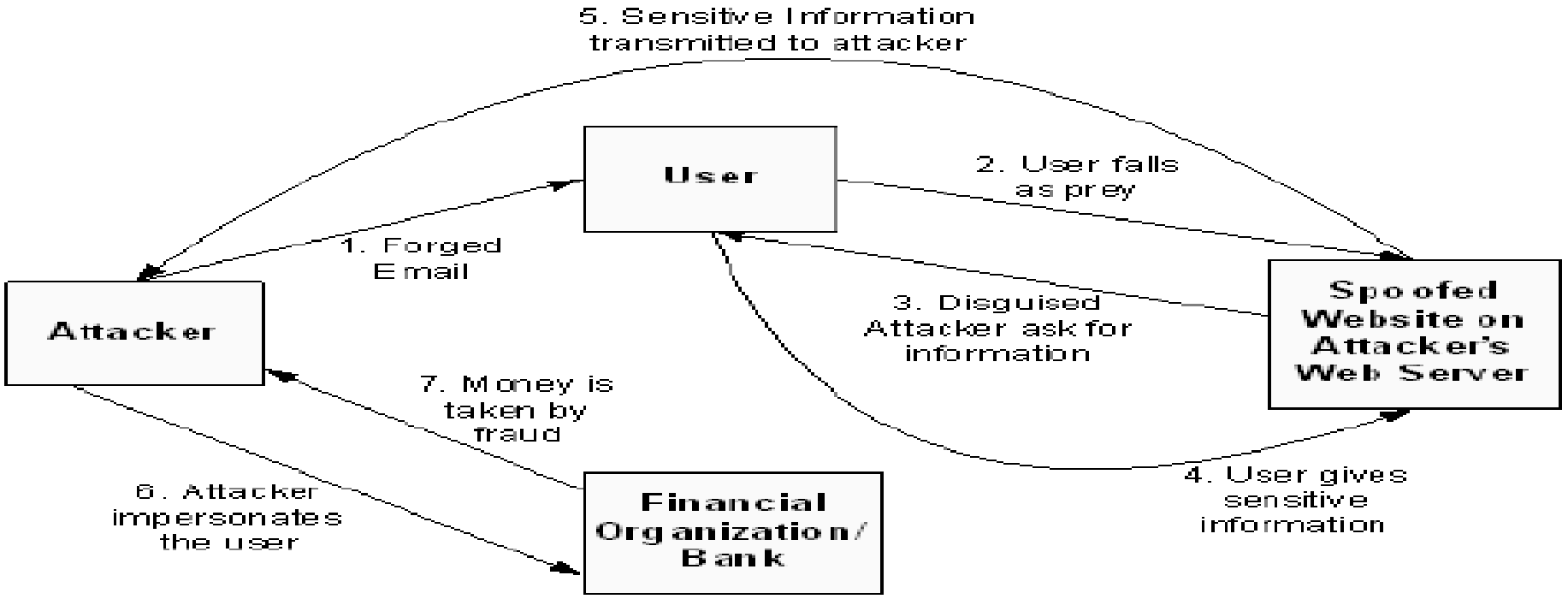
•Long-Term: LuxeCart invested heavily in overhauling its cybersecurity measures and rebuilding its reputation. These actions gradually restored customer confidence and positioned LuxeCart as a leader in responsible data management within the eCommerce industry.

Lessons Learned:

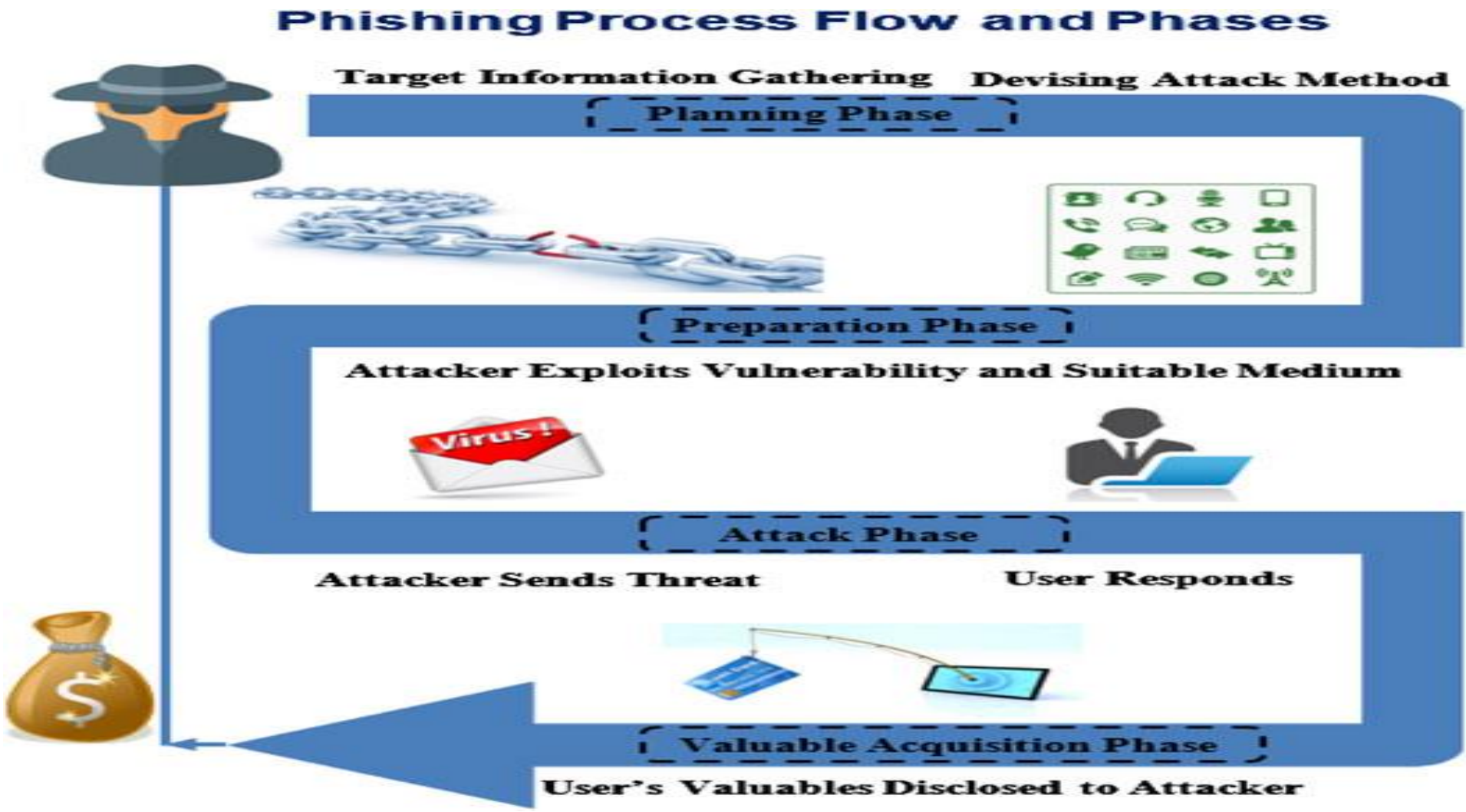
The LuxeCart incident underscores the critical importance of proactive cybersecurity measures, especially in eCommerce sectors where consumer data is a prime target. Regular employee training, robust monitoring systems, and an effective incident response plan are indispensable components of a comprehensive cybersecurity strategy. Moreover, the incident highlights the value of having resilient data recovery processes to ensure business continuity in the face of cyber threats.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

- - Example: Phishing attack on online retail
- - Diagram: Attack Vector Flowchart and Mitigation Steps
- - Link: https://www.cisa.gov/uscert/resources
- - Explanation: Stepwise mitigation process and lessons learned



Tishk International University
Faculty of Applied Science
Cybersecurity Department



Tishk International University
Faculty of Applied Science
Cybersecurity Department

Practice Problems

- 1. Calculate compliance risk: I=9, V=5, C=3 → CR=?
- 2. Estimate probability of breach: n=1000, P_t=0.002 → P(B)=?
- 3. Scenario-based ethical dilemma: How to respond if employee exposes customer data
- - Step-by-step solutions included in notes

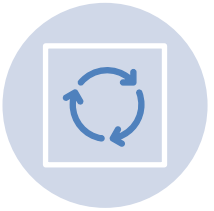
Tishk International University
Faculty of Applied Science
Cybersecurity Department

Key Takeaways & Conclusion

- Ethical handling protects reputation and reduces liability

- Compliance frameworks reduce risks in financial transactions

- Continuous monitoring and employee training are essential



- Diagram: Continuous E-commerce Security Cycle

- Link: https://www.sans.org/white-papers/continuous-monitoring/

- Explanation: Ongoing monitoring, risk assessment, and compliance steps

References

- 1. NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
- 2. ISO/IEC 27001: https://www.iso.org/isoiec-27001-information-security.html
- 3. PCI DSS: https://www.pcisecuritystandards.org
- 4. GDPR: https://gdpr-info.eu
- 5. Verizon DBIR: https://www.verizon.com/business/resources/reports/dbir/
- 6. SANS Continuous Monitoring Whitepaper: https://www.sans.org/white-papers/continuous-monitoring/

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Thank you for your listening