Information Security and Privacy - Policies and Standards

22MCS15

Dr. BASAVARAJ G.N

OUTCOME

- Syllabus & Course Outcome
- Introduction
- IA guidelines
- Paper publication 10Marks
- AAT/Assignment 10Marks

Information can be

- Printed or written on paper
- Stored electronically
- Transmitted by post or using electronics means
- Displayed / published on web
- Verbal – spoken in conversations

Characteristics of Information

- Three characteristics of information must be protected by information security:
  - Confidentially
  - Integrity
  - Availability

INFORMATION SECURITY?

- The architecture where an integrated combination of appliances, systems and solutions, software, and vulnerability scans are working together.
- Information security is all about **protecting** and **preserving** information. It's all about protecting and preserving the **confidentiality, integrity, authenticity, availability**, and **reliability** of **information**.
- Monitored 24 x7

Introduction

- Policy is the essential foundation of an effective information security program
  - "The success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing information on automated systems"

- Policy maker sets the tone and emphasis on the importance of information security

Introduction (cont'd.)

- Policy objectives
  - Reduced risk
  - Compliance with laws and regulations
  - Assurance of operational continuity, information integrity, and confidentiality

Why Policy? (cont'd.)

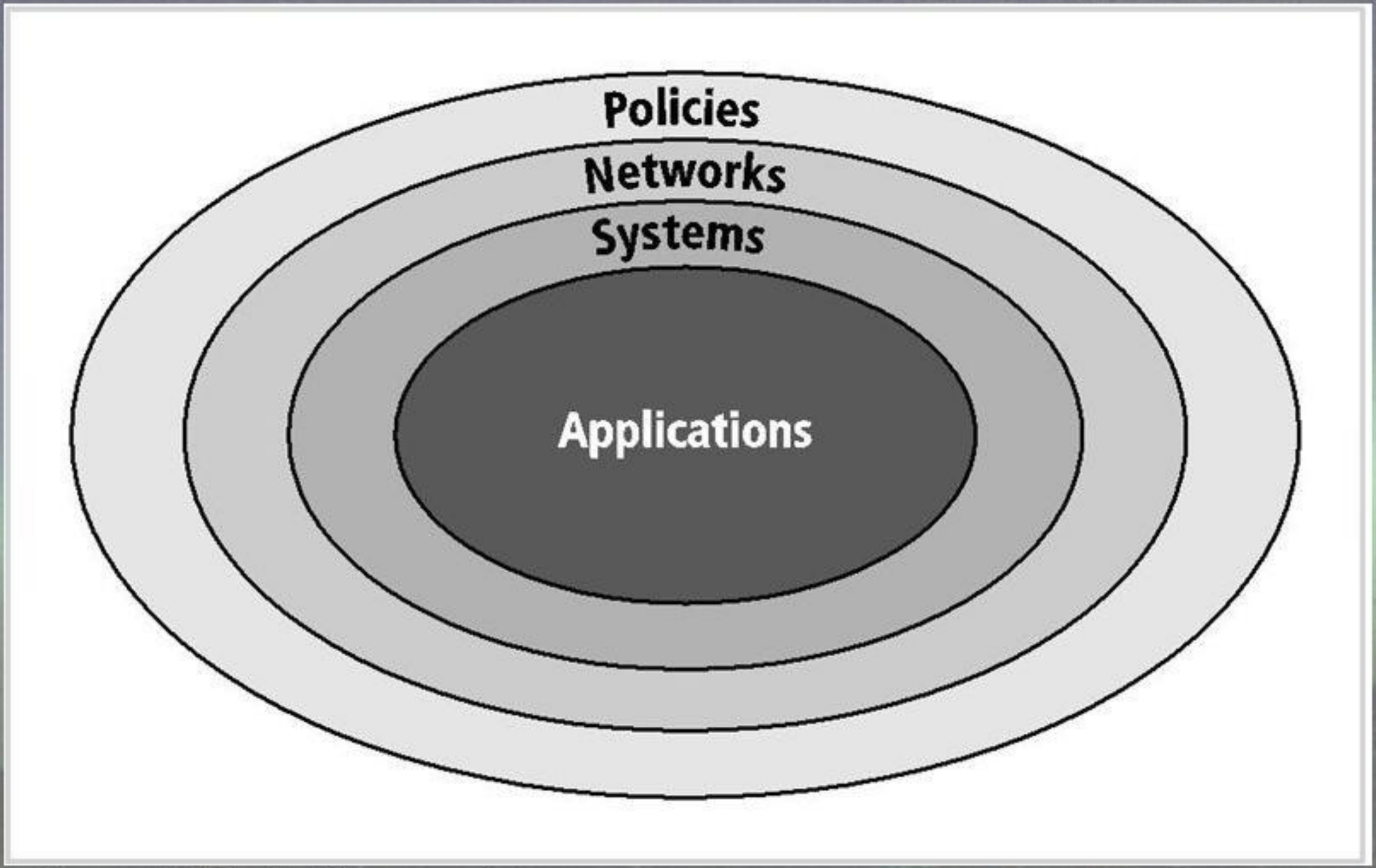


Figure 4-1 The bull's eye model

Source: Course Technology/Cengage Learning

Why Policy? (cont'd.)

- Policies are important reference documents
  - For internal audits
  - For the resolution of legal disputes about management's due diligence
  - Policy documents can act as a clear statement of management's intent

Policy, Standards, and Practices

- Policy
  - A plan or course of action that influences decisions
  - For policies to be effective they must be properly disseminated, read, understood, agreed-to, and uniformly enforced
  - Policies require constant modification and maintenance

Issue-Specific Security Policy (ISSP)

- Provides detailed, targeted guidance
  - Instructs the organization in secure use of a technology systems
  - Begins with introduction to fundamental technological philosophy of the organization
- Protects organization from inefficiency and ambiguity
  - Documents how the technology-based system is controlled

Issue-Specific Security Policy (cont'd.)

- Protects organization from inefficiency and ambiguity (cont'd.)
  - Identifies the processes and authorities that provide this control
- Indemnifies the organization against liability for an employee's inappropriate or illegal system use

Issue-Specific Security Policy (cont'd.)

- Every organization's ISSP should:
  - Address specific technology-based systems
  - Require frequent updates
  - Contain an issue statement on the organization's position on an issue

Developing Information Security Policy (cont'd.)

- Policy development projects should be
  - Well planned
  - Properly funded
  - Aggressively managed to ensure that it is completed on time and within budget
- The policy development project can be guided by the SecSDLC process

Developing Information Security Policy (cont'd.)

- Investigation phase
  - Obtain support from senior management, and active involvement of IT management, specifically the CIO
  - Clearly articulate the goals of the policy project
  - Gain participation of correct individuals affected by the recommended policies

Developing Information Security Policy (cont'd.)

- Investigation phase (cont'd.)
  - Involve legal, human resources and end-users
  - Assign a project champion with sufficient stature and prestige
  - Acquire a capable project manager
  - Develop a detailed outline of and sound estimates for project cost and scheduling

Developing Information Security Policy (cont'd.)

- Analysis phase should produce
  - New or recent risk assessment or IT audit documenting the current information security needs of the organization
  - Key reference materials
    - Including any existing policies

Developing Information Security Policy (cont'd.)

Figure 4-8 End user license agreement for Microsoft Windows XP

Source: Course Technology/Cengage Learning

Developing Information Security Policy (cont'd.)

- Design phase includes
  - How the policies will be distributed
  - How verification of the distribution will be accomplished
  - Specifications for any automated tools
  - Revisions to feasibility analysis reports based on improved costs and benefits as the design is clarified

Developing Information Security Policy (cont'd.)

- Implementation phase includes
  - Writing the policies
    - Making certain the policies are enforceable as written
    - Policy distribution is not always straightforward
    - Effective policy is written at a reasonable reading level, and attempts to minimize technical jargon and management terminology

Developing Information Security Policy (cont'd.)

- Maintenance Phase
  - Maintain and modify the policy as needed to ensure that it remains effective as a tool to meet changing threats
  - The policy should have a built-in mechanism via which users can report problems with the policy, preferably anonymously
  - Periodic review should be built in to the process

Approach to Policy Development

- Overview: Scott Barman emphasizes the importance of strategic timing and a structured methodology in policy development for effective information security

When to Develop Policies

Timing is Key: Policies should be developed proactively, ahead of system implementations, to integrate security measures seamlessly

Response to Threats: Policies should evolve in response to emerging cyber threats to maintain resilience

Compliance Alignment: Develop policies to align with regulatory requirements and industry standards

Methodology Overview

- Risk Assessment: Conduct thorough risk assessments to identify and prioritize areas for policy development
- Stakeholder Engagement: Involve key stakeholders for diverse insights and policy alignment
- Policy Drafting: Craft clear policies outlining roles, responsibilities, and procedures for safeguarding information assets

Policy Components

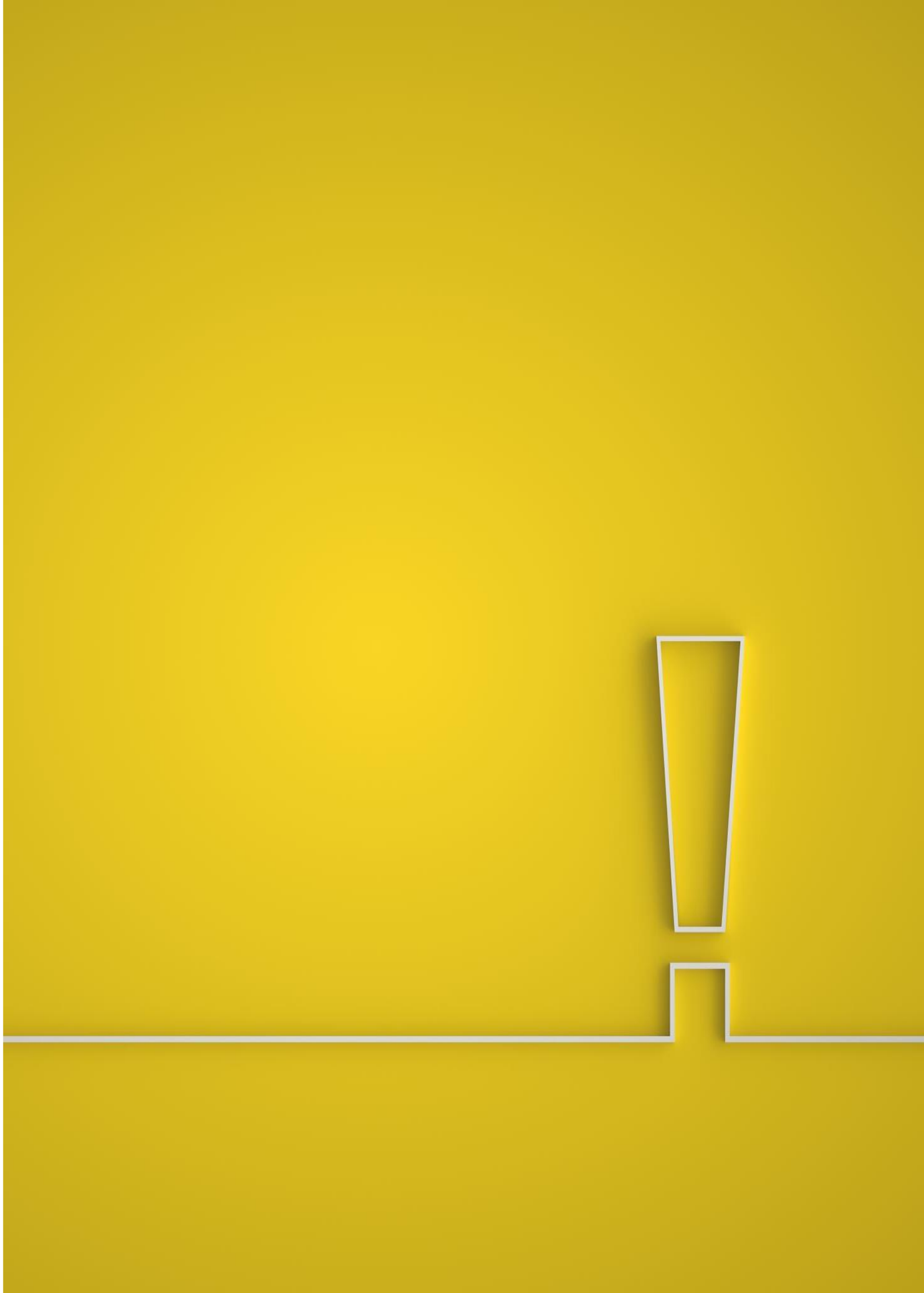
- Access Control: Define procedures for granting, monitoring, and revoking access to sensitive data and systems
- Data Protection: Establish guidelines for encryption, backup, retention, and secure disposal
- Incident Response: Outline protocols for detecting, reporting, and responding to security incidents

Training and Awareness

- Employee Training: Provide comprehensive training to educate employees on security policies and best practices
- Awareness Campaigns: Launch initiatives to reinforce security awareness and foster a culture of cybersecurity

Compliance and Auditing

- Monitoring Compliance: Implement mechanisms to monitor and enforce policy compliance, conducting regular audits
- Regulatory Alignment: Ensure policies align with regulations like GDPR, HIPAA, or PCI DSS, and update them as needed



Conclusion

- Strategic Approach: Barman's approach prioritizes proactive risk management, stakeholder engagement, and compliance
- Key Takeaways: Develop policies ahead of system implementations, in response to threats, and to meet compliance standards

SEMESTER – I
Information Security and Privacy - Policies and

Dr. Basavaraj G.N

Course Code 23MCA1C1

Introduction

- Title: Safeguarding Data and Intellectual Property: Essential Practices
- Welcome to our presentation on protecting data and intellectual property.
- Overview of topics: Data security, backups, archival storage, data disposal, and intellectual property rights.

- **Data Security Considerations**
  - Definition: Ensuring the confidentiality, integrity, and availability of data.
  - Example: Encryption of sensitive information during transmission (e.g., HTTPS).
  - Who and What is Protected: Personal data, financial records, and company trade secrets.
  - Considerations: Strong passwords, access controls, and regular security audits.

- **Backups**
  - Definition: Creating copies of data to prevent loss in case of system failures or cyber attacks.
  - Example: Automatic daily backups of a company's database to an offsite server.
  - Who and What is Protected: Business data, customer records, and intellectual property.
  - Considerations: Regular backup schedules, redundant storage, and testing restoration procedures.

- **Archival Storage**
  - Definition: Long-term preservation of data for historical, legal, or research purposes.
  - Example: Digital archives of historical documents by libraries and museums.
  - Who and What is Protected: Cultural heritage, scientific research, and institutional records.
  - Considerations: Metadata management, data integrity verification, and accessibility standards.

- **Disposal of Data**
  - Definition: Proper removal or destruction of data to prevent unauthorized access.
  - Example: Shredding physical documents containing sensitive information.
  - Who and What is Protected: Personal data, obsolete records, and proprietary information.
  - Considerations: Secure deletion methods, compliance with data protection regulations, and documentation of disposal processes.

- **Intellectual Property Rights**

  - Definition: Legal rights protecting creations of the mind, such as inventions, literary works, and trademarks.
  - Example: Patenting a new invention to prevent others from using it without permission.
  - Who and What is Protected: Innovations, artistic creations, and brand identities.
  - Considerations: Understanding IP laws, registration processes, and enforcement mechanisms.

- **Copyright**
  - Definition: Protection granted to original works of authorship, such as books, music, and software.
  - Example: Licensing of a photograph for use in advertising campaigns.
  - Who and What is Protected: Creative works, literary compositions, and digital content.
- Considerations: Fair use exceptions, copyright duration, and infringement claims.

- **Trademarks**
  - Definition: Symbols, words, or designs used to identify and distinguish goods or services.
  - Example: Registration of a company logo to prevent others from using a similar design.
  - Who and What is Protected: Brand names, logos, and product packaging.
  - Considerations: Trademark searches, brand consistency, and renewal requirements.

- **Patents**
  - Definition: Exclusive rights granted to inventors for new inventions or processes.
  - Example: Patenting a unique technology to prevent competitors from copying it.
  - Who and What is Protected: Technical innovations, pharmaceutical compounds, and manufacturing methods.
  - Considerations: Patentability criteria, patent infringement litigation, and patent expiration.

- **: Trade Secrets**
  - Definition: Confidential information that provides a competitive advantage to its owner.
  - Example: Formula for a popular soft drink kept confidential by the manufacturer.
  - Who and What is Protected: Business strategies, customer lists, and research data.
- Considerations: Non-disclosure agreements, access controls, and employee training on trade secret protection

- **University IP Policies**

  - Definition: Institutional guidelines governing the ownership and commercialization of intellectual property.
  - Example: Research institution policies on faculty inventions and discoveries.
  - Who and What is Protected: Faculty research, student innovations, and university-generated intellectual property.
  - Considerations: Royalty sharing agreements, technology transfer processes, and academic freedom.

- **Ethical Considerations**

  - Definition: Moral principles guiding the responsible use and protection of data and intellectual property.
  - Example: Respecting copyright laws by citing sources in academic research papers.

- Who and What is Protected: Privacy rights, academic integrity, and cultural heritage.
- Considerations: Transparency, accountability, and balancing competing interests.

- **Compliance and Regulation**
  - Definition: Adherence to laws and regulations governing data protection and intellectual property rights.
  - Example: Compliance with the European Union's General Data Protection Regulation (GDPR).
  - Who and What is Protected: Personal data privacy, consumer rights, and fair competition.
  - Considerations: Data breach notification requirements, copyright infringement penalties, and regulatory audits.

- **Case Studies**

  - Example 1: Sony Pictures Entertainment Hack (2014) - Data security breach resulting in leaked emails and sensitive employee information.
  - Example 2: Apple vs. Samsung Patent Dispute - Legal battles over smartphone design and software patents.
  - Example 3: Disney's Protection of Mickey Mouse Trademark - Vigilant enforcement of trademark rights to safeguard brand integrity.
  - Example 4: IBM's Patent Portfolio - Strategic use of patents to protect innovations and generate revenue through licensing.
  - Example 5: Harvard University's Technology Transfer Office - Facilitating the commercialization of university research through IP licensing and startup incubation.

- **Conclusion**

  - Recap of key points on safeguarding data and intellectual property.
  - Importance of implementing robust security measures, adhering to IP laws, and promoting ethical practices.
  - Encouragement for ongoing education and vigilance in protecting valuable assets in an increasingly digital world.

Information Security and Privacy - Policies and Standards

Dr. BASAVARAJ G.N

MODULE 1…

RECAP:

Incident Response

Forensics

- Forensics involves the systematic gathering, examination, and analysis of digital evidence to understand and mitigate security incidents
- Real-world Example: The forensic analysis conducted after the 2016 Democratic National Committee email leak, which helped identify the intruder and their methods

Management Responsibilities

- Management holds the responsibility for setting cybersecurity policies, allocating resources, and overseeing compliance efforts
- Real-world Example: The fallout from the 2017 Equifax data breach, where poor management decisions and inadequate security practices led to significant financial and reputational damage

Role of Information Security Department

- The Information Security Department is tasked with implementing security measures, monitoring for threats, and responding to incidents
- Real-world Example: The proactive measures taken by the security team at Google to prevent and mitigate cyber attacks, such as the 2017 WannaCry ransomware outbreak

Incident Response and Forensic Readiness

- Effective incident response plans incorporate forensic readiness, ensuring that digital evidence is collected and preserved properly
- Real-world Example: The forensic investigation following the 2014 Sony Pictures hack, which uncovered the extent of the breach and informed response efforts

- Collaboration between management, IT teams, and the Information Security Department is crucial for a cohesive cybersecurity strategy
- Real-world Example: The collaborative efforts between government agencies and private sector organizations to combat cyber threats, such as the sharing of threat intelligence
- Continuous training and education are essential for keeping cybersecurity professionals updated on emerging threats and best practices

Incident Response and Forensic Readiness

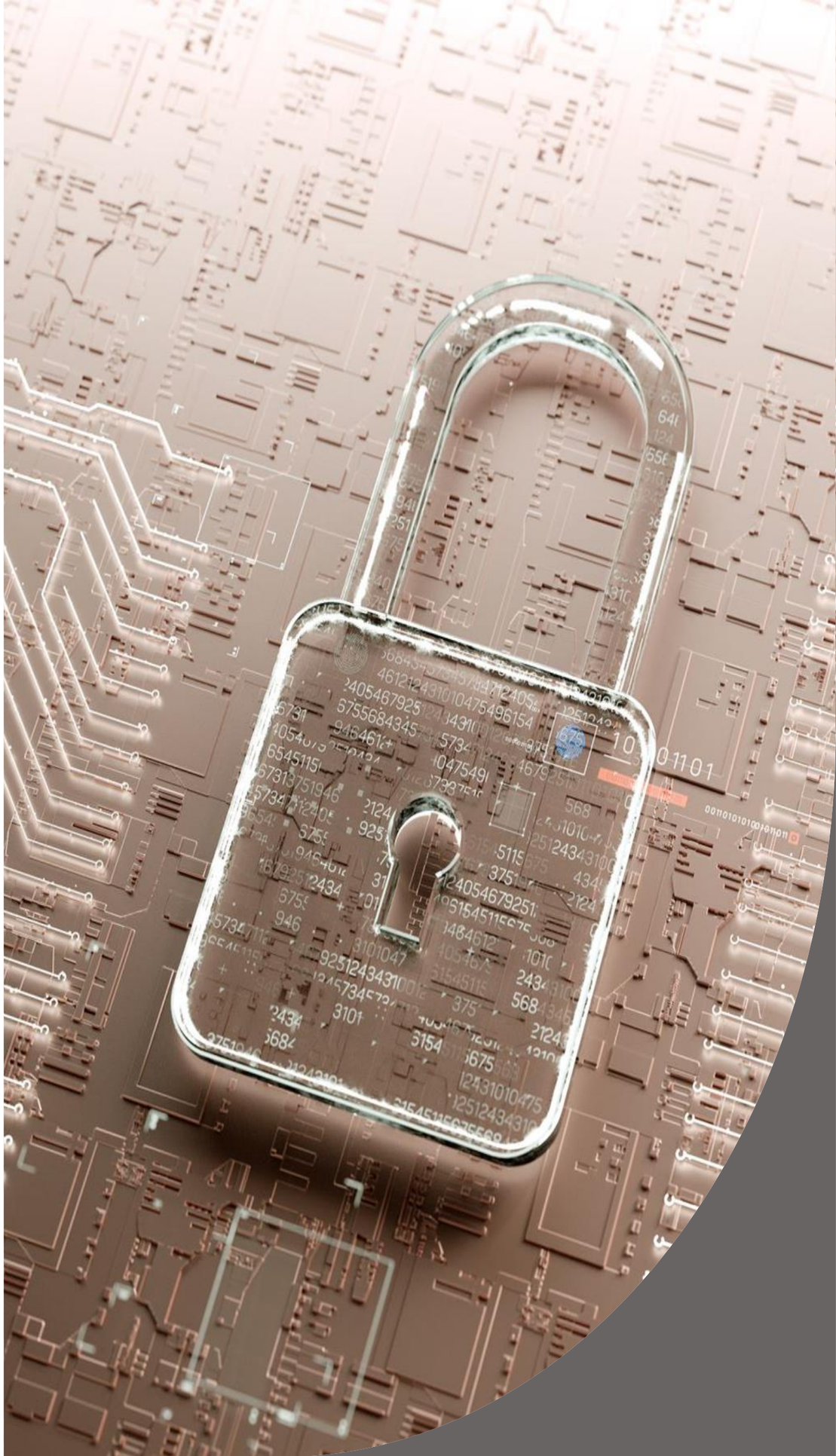
- Real-world Example: The cybersecurity training programs offered by organizations like Cisco and Microsoft to enhance the skills of their employees and partners
- Compliance with regulations and standards is necessary to ensure the security and privacy of data
- Real-world Example: The impact of the European Union's General Data Protection Regulation on global businesses, prompting them to strengthen their data protection measures

Building Resilience

- Organizations must focus on building resilience to quickly recover from cyber attacks and minimize their impact
- Real-world Example: The resilience demonstrated by organizations during the COVID-19 pandemic, where remote work and heightened cyber threats necessitated adaptive security measures

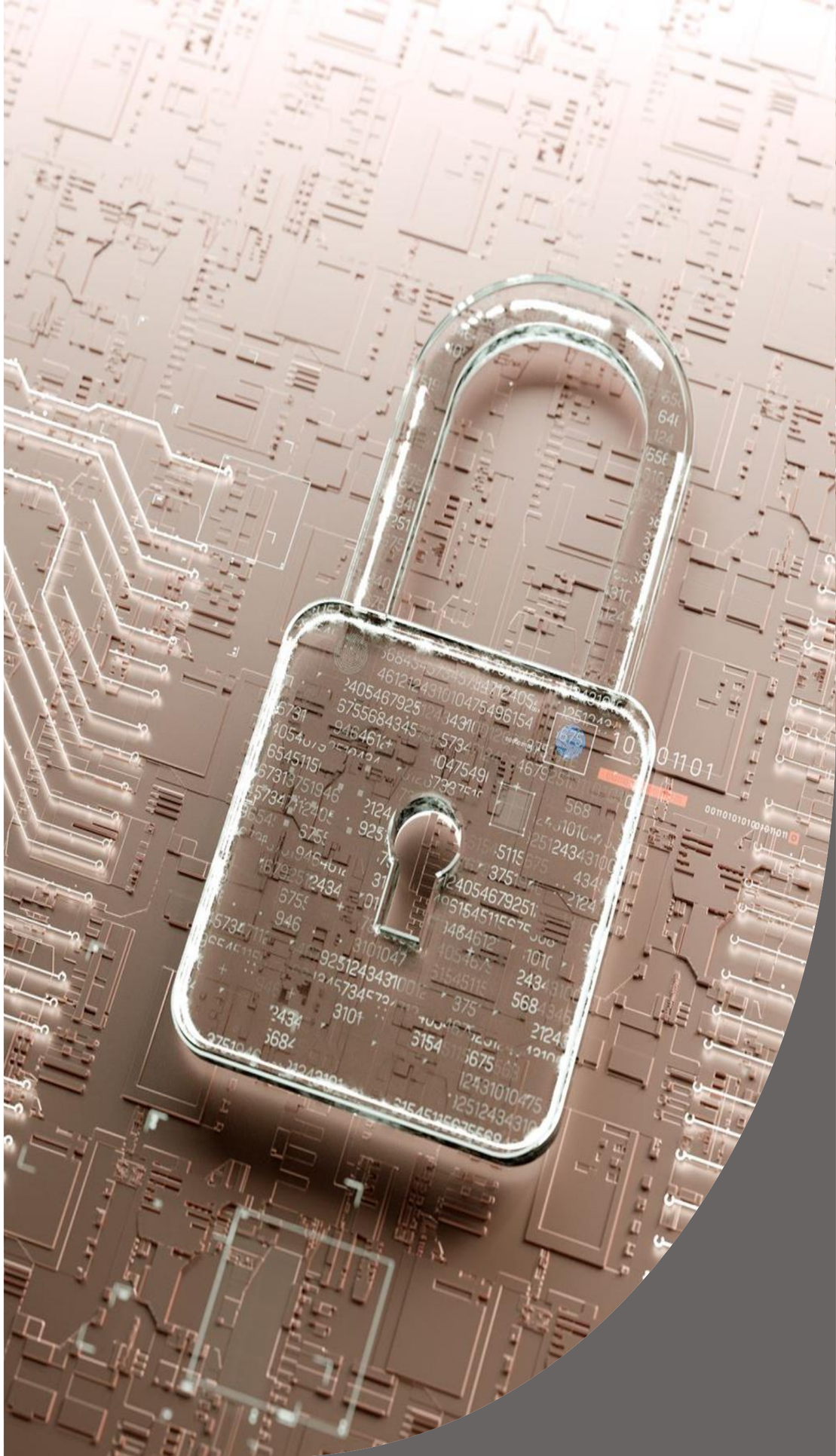
Conclusion

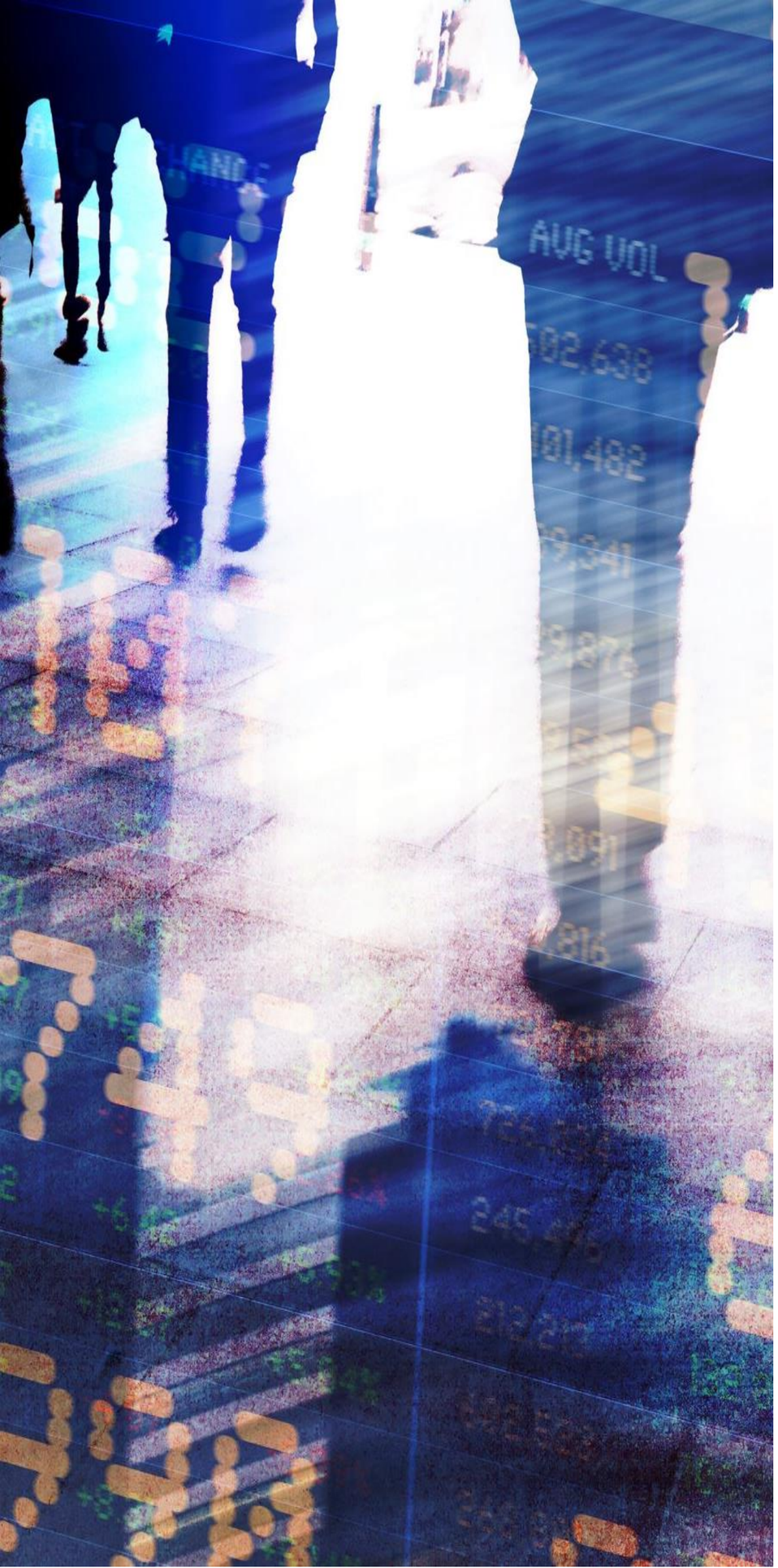
- Understanding the roles of forensics, management responsibilities, and the Information Security Department is crucial for effective information security.



Recap

- Understanding the roles of forensics, management responsibilities, and the Information Security Department is crucial for effective information security.





Understanding Security Management

- **Definition: Security management involves the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events.**
- **Real-life Example: Let's consider the security measures implemented in airports worldwide.**
- **Definition: Law enforcement refers to the system by which laws are enforced and upheld within a society**
- **Real-life Example: The collaboration between local police departments and federal agencies in combating organized crime syndicates highlights the critical role of law enforcement in maintaining societal order and safety**

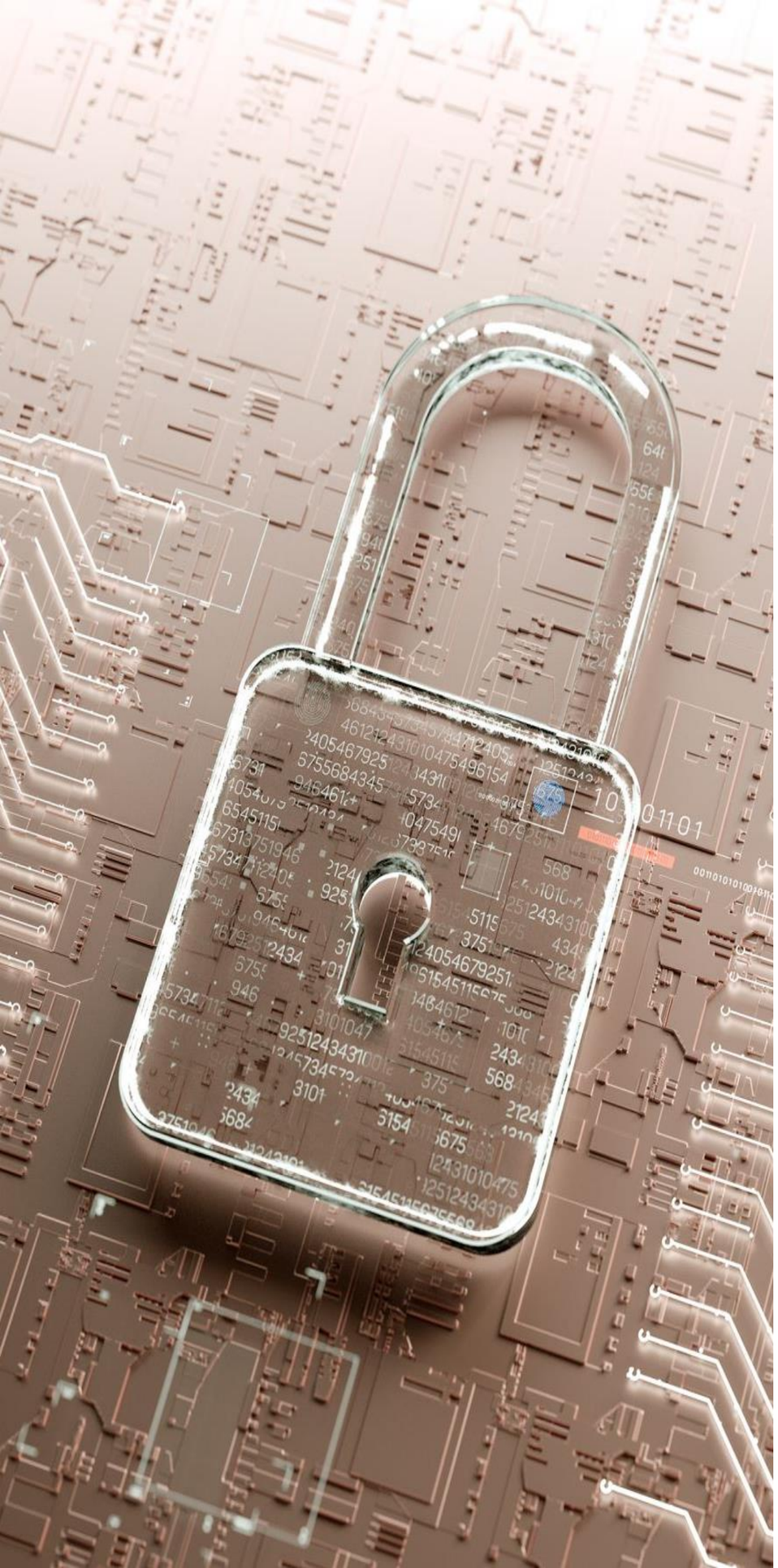
Security Awareness Training and Support

Definition: Security awareness training aims to educate individuals about potential security threats and best practices to mitigate risks

Real-life Example: Consider a corporate setting where employees undergo regular cybersecurity awareness training sessions

Enhancing Organizational Resilience: By encouragement a culture of security awareness, organizations can empower employees to become proactive stakeholders in safeguarding sensitive information and assets

Mitigating Insider Threats: Educating personnel about the risks associated with insider threats helps preempt malicious actions and fosters a sense of accountability among employees



Security Awareness Training and Support

- Overview: The Equifax data breach exposed the personal information of approximately 147 million individuals due to vulnerabilities in the company's security infrastructure
- Lessons Learned: This incident underscores the criticality of robust security measures, comprehensive risk assessments, and continuous monitoring to prevent cyber threats

Conclusion

- Recap: Today, we explored the fundamentals of security management, the pivotal role of law enforcement, and the significance of security awareness training
- Takeaway: As future engineers, it's essential to recognize the interdisciplinary nature of security management and law enforcement, incorporating these principles into our professional endeavors to uphold safety and integrity in an ever-evolving landscape