Cyber Security

Laws

Presented By: Daniel Howard

Overview

- Gramm-Leach-Bliley Act (GLBA)
- HIPAA Privacy & Security Rules
- The Computer Fraud and Abuse Act
- Electronic Communication Privacy Act
- US Patriot Act (Sections 105, 202, 210, 216, 220)
- Sarbanes-Oxley Act
- NERC CIP
- PCI DSS

General concepts

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA) includes provisions related to the protection of consumer information held by financial institutions, it requires financial institutions to establish and maintain information security programs. These programs are designed to safeguard the confidentiality and integrity of nonpublic personal information (NPI), including sensitive financial data.

1. **Information Security Programs:** Financial institutions are mandated to develop, implement, and maintain comprehensive information security programs to protect the security and confidentiality of customer information.

2. **Risk Assessment:** GLBA requires financial institutions to conduct regular risk assessments to identify and evaluate potential risks to the security, confidentiality, and integrity of customer information.

3. **Safeguards:** Institutions must implement appropriate safeguards to control identified risks. This may involve the use of encryption, access controls, employee training, and other measures to protect customer information.

4. **Ongoing Monitoring and Adjustment:** GLBA emphasizes the importance of ongoing monitoring and adjustment of information security programs in response to changes in technology, the sensitivity of customer information, and potential internal or external threats.

5. **Third-Party Service Providers:** Financial institutions must ensure that their service providers also have safeguards in place to protect customer information. This includes assessing the security practices of third-party vendors.

6. **Incident Response:** In the event of a security incident, financial institutions are expected to have response mechanisms in place to address and mitigate the impact of the incident, as well as to notify customers and regulatory authorities as necessary.

GLBA sets the framework for financial institutions to establish and maintain effective information security programs tailored to their specific risks and circumstances. Compliance with GLBA helps protect consumer financial information and maintain trust in the financial sector.

General concepts

HippaPrivacy & Security Rules

The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules are U.S. regulations designed to protect the privacy and security of individuals' health information. Enacted in 1996, these rules apply to covered entities, which include healthcare providers, health plans, and healthcare clearinghouses.

1. **HIPAA Privacy Rule:**
   - The Privacy Rule establishes standards for safeguarding individuals' protected health information (PHI).
   - It grants patients rights over their health information, including the right to access and request corrections to their records.
   - Covered entities must obtain patients' consent for the use and disclosure of their PHI, except in certain permitted circumstances.
   - The rule outlines administrative, physical, and technical safeguards to protect the confidentiality of PHI.

2. **HIPAA Security Rule:**
   - The Security Rule focuses on the protection of electronic protected health information (ePHI).
   - Covered entities must implement security measures to ensure the confidentiality, integrity, and availability of ePHI.
   - It sets standards for administrative, physical, and technical safeguards, including risk analysis and risk management processes.
   - Covered entities are required to have security policies and procedures, conduct employee training, and implement access controls to protect ePHI.

Both rules include provisions for the reporting and investigation of breaches, with potential penalties for non-compliance. HIPAA aims to strike a balance between the need for healthcare information to be accessible for quality care and the importance of safeguarding individuals' privacy and the security of their health data.

General concepts

NERC CIP

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are a set of mandatory cybersecurity standards designed to secure the assets and information systems crucial to the reliability of the North American bulk power system (BPS).

1. **Scope:** The standards cover a range of requirements related to the security of critical cyber assets, which include hardware, software, and data that are essential to the reliable operation of the BPS.

2. **Categorization:** NERC CIP standards are organized into several categories, each addressing specific aspects of cybersecurity, such as access controls, incident response, and physical security.

3. **Compliance:** Electric utilities and entities responsible for the operation and management of the bulk power system must comply with the NERC CIP standards. Compliance involves implementing cybersecurity measures, conducting regular assessments, and reporting incidents.

4. **Risk Management:** NERC CIP standards emphasize a risk-based approach to cybersecurity. Entities are required to identify, assess, and prioritize cybersecurity risks, and then implement measures to mitigate these risks.

5. **Incident Reporting:** In the event of a cybersecurity incident, entities are required to follow reporting and response procedures outlined in the standards. This includes reporting to appropriate authorities and taking necessary actions to address and recover from the incident.

NERC CIP standards play a crucial role in enhancing the resilience and security of the electrical grid by establishing a framework for protecting critical infrastructure against cyber threats and ensuring a consistent and high level of cybersecurity across the industry.

Electronic Communication Privacy Act

General concepts

The Electronic Communications Privacy Act (ECPA) is a U.S. federal law enacted in 1986 that governs the interception and privacy of electronic communications. The law was designed to extend legal protections to electronic forms of communication, such as emails, telephone conversations, and electronic data transmissions.

1. **Wiretap Provisions:** ECPA establishes rules for the interception of wire, oral, or electronic communications. It generally requires law enforcement to obtain a warrant based on probable cause before intercepting or accessing the content of electronic communications.

2. **Stored Communications:** ECPA also addresses the privacy of stored electronic communications, including emails stored on servers. It establishes rules regarding when and how the government can access stored communications, specifying different standards for obtaining different types of stored data.

3. **Pen Register and Trap and Trace Devices:** The law regulates the use of pen registers and trap and trace devices, which record metadata about communications (such as phone numbers dialed). ECPA requires court authorization to use these devices.

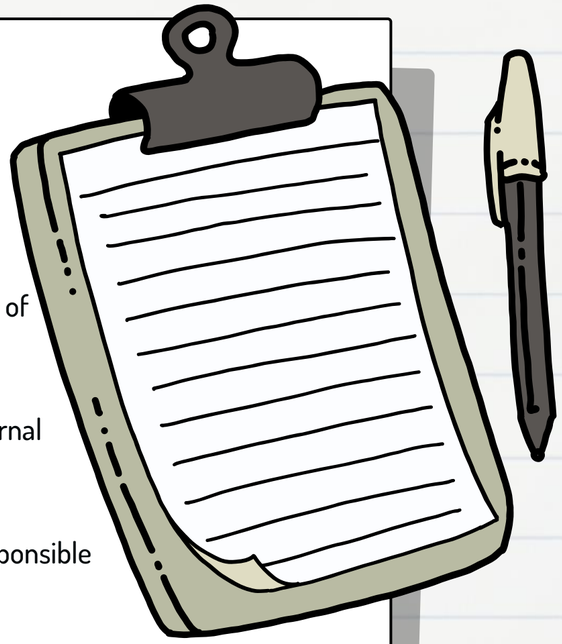
4. **Exceptions and Consent:** ECPA includes exceptions to the warrant requirement in certain situations, such as with the consent of one of the parties involved in the communication or in cases of emergency.

5. **Privacy Protections for Electronic Communication Providers:** The law includes provisions to protect the privacy of customers of electronic communication service providers, restricting the disclosure of customer records and communications.

6. **Amendments and Evolving Technology:** ECPA has been amended over the years to adapt to changes in technology. However, some aspects of the law have faced criticism for not keeping pace with the rapid evolution of electronic communication methods.

ECPA plays a crucial role in safeguarding the privacy of electronic communications, outlining legal standards for law enforcement access to such communications and balancing the need for law enforcement investigations with individual privacy rights.

Sarbanes-Oxley Act



General Concepts

1. **Corporate Responsibility:** Company executives are required to personally certify the accuracy of financial statements and disclose any significant changes in financial condition.

2. **Auditor Independence:** The act establishes guidelines to ensure independence between external auditors and the companies they audit, reducing conflicts of interest.

3. **Audit Committee Oversight:** Public companies must have independent audit committees responsible for overseeing financial reporting, internal controls, and external audits.

4. **Internal Controls:** Companies are required to establish and maintain effective internal control structures to ensure the reliability of financial reporting.

5. **Whistleblower Protection:** SOX provides protection for employees who report potential misconduct, fraud, or violations of securities laws within their companies.

6. **CEO/CFO Certification:** The CEO and CFO of publicly traded companies must personally certify the accuracy of financial statements in their periodic reports to the Securities and Exchange Commission (SEC).

SOX has had a significant impact on corporate governance practices and has increased transparency in financial reporting. While it imposes additional compliance costs on companies, it is viewed as a crucial measure to restore investor confidence in financial markets.

PCI DSS

General Concepts

1The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure the secure handling of credit card information during payment transactions. Developed by the Payment Card Industry Security Standards Council (PCI SSC), the standard aims to protect cardholder data and strengthen payment card transaction systems.

1. **Scope:** PCI DSS applies to any organization that stores, processes, or transmits credit card information. This includes merchants, financial institutions, and service providers involved in payment card transactions.

2. **Security Requirements:** The standard outlines a set of security requirements and controls across various categories, including data encryption, access controls, network security, and regular monitoring and testing of security systems.

3. **Data Protection:** PCI DSS focuses on protecting sensitive cardholder data, such as credit card numbers, expiration dates, and verification codes. The goal is to prevent unauthorized access and reduce the risk of data breaches.

4. **Compliance Levels:** Merchants and service providers are categorized into different compliance levels based on the volume of transactions they process. The higher the transaction volume, the more stringent the security requirements.

5. **Validation and Compliance:** Organizations must undergo regular assessments and validations to demonstrate compliance with PCI DSS. This may involve self-assessment questionnaires or on-site audits by qualified security assessors.

6. **Penalties for Non-Compliance:** Non-compliance with PCI DSS can result in financial penalties, restrictions on card processing capabilities, and damage to an organization's reputation.

PCI DSS aims to create a secure environment for payment card transactions, protecting both consumers and businesses from the risks associated with the unauthorized access and misuse of sensitive cardholder information. Compliance helps maintain trust in the payment card industry and reduces the likelihood of data breaches.

The Computer Fraud and Abuse Act

General Concepts

The Computer Fraud and Abuse Act (CFAA) is a U.S. federal law that addresses computer-related crimes and unauthorized access to computer systems. Enacted in 1986 and subsequently amended, the CFAA establishes legal penalties for various offenses related to unauthorized access, computer fraud, and the misuse of computer systems.

1. **Unauthorized Access:** The CFAA prohibits unauthorized access to protected computer systems. This includes intentionally accessing a computer without authorization or exceeding the authorized access to obtain information.

2. **Data Theft:** It criminalizes the theft of information from protected computers. This includes accessing computer systems with the intent to steal, copy, or alter data.

3. **Computer Fraud:** The CFAA addresses fraudulent activities involving computers, such as manipulating data, introducing viruses or malware, and causing damage to computer systems.

4. **Denial of Service Attacks:** It criminalizes actions that result in the impairment or disruption of the availability of computer systems, commonly known as denial of service attacks.

5. **Trafficking in Passwords:** The CFAA prohibits the trafficking of passwords or similar authentication credentials to gain unauthorized access to computer systems.

6. **Penalties:** Violations of the CFAA can lead to criminal and civil penalties, including fines and imprisonment. Penalties vary based on the severity of the offense and the damages incurred.

7. **Amendments:** The CFAA has undergone multiple amendments to adapt to evolving technology and address emerging cyber threats. These amendments have expanded its scope and updated its provisions to reflect the changing landscape of computer-related crimes.

The CFAA is a key legal tool for prosecuting individuals who engage in unauthorized and malicious activities related to computer systems. It plays a crucial role in deterring cybercrimes and protecting the integrity and security of computer networks and data.

International Organization for Standardization (ISO) 27001 and 27002

General Concepts

ISO 27001 and ISO 27002 are international standards that focus on information security management systems (ISMS). They are developed and published by the International Organization for Standardization (ISO) to provide a framework for organizations to establish, implement, maintain, and continually improve their information security practices.

1. **ISO 27001: Information Security Management System (ISMS):**
   - ISO 27001 is the primary standard that outlines the requirements for establishing, implementing, maintaining, and improving an Information Security Management System (ISMS).
   - The standard provides a systematic approach to managing sensitive information, ensuring the confidentiality, integrity, and availability of information assets.
   - ISO 27001 is designed to be adaptable to various types and sizes of organizations and focuses on a risk-based approach to information security.

2. **ISO 27002: Code of Practice for Information Security Controls:**
   - ISO 27002, formerly known as ISO 17799, complements ISO 27001 by providing a detailed set of security controls and best practices.
   - It offers a comprehensive catalog of security controls and guidelines that organizations can use to implement specific measures to address information security risks.
   - ISO 27002 covers various areas, including information security policies, organization of information security, human resource security, asset management, access control, cryptography, physical and environmental security, and more.

Together, ISO 27001 and ISO 27002 help organizations establish a robust information security management system, implement effective security controls, and manage risks systematically. These standards are widely adopted globally and are often used as a benchmark for demonstrating an organization's commitment to information security best practices. Organizations that achieve ISO 27001 certification have demonstrated compliance with a recognized international standard for information security.

General concepts

US Patriot Act (Sections 105, 202, 210, 216, 220)

Section 105 of the USA PATRIOT Act mandates the Director of the United States Secret Service to establish a nationwide network of electronic crime task forces, modeled after the New York Electronic Crimes Task Force. The objective is to proactively address and investigate electronic crimes, including those with potential links to terrorist activities targeting critical infrastructure and financial payment systems. This initiative aims to enhance the nation's capabilities in preventing, detecting, and responding to diverse forms of electronic threats.

Section 202 amends Section 2516(1)(c) of Title 18, United States Code. The amendment expands the authority to intercept wire, oral, and electronic communications concerning computer fraud and abuse offenses. It specifically includes felony violations of Section 1030, which pertains to computer fraud and abuse, alongside existing provisions related to mail fraud. This modification broadens the legal scope for law enforcement to conduct interceptions in cases involving computer-related offenses.

Section 210 covers the amendment to Section 2703(c)(2) of Title 18, United States Code, broadens the scope of subpoenas for electronic communication records. It expands the information that can be collected from an entity regarding a subscriber, encompassing details such as the subscriber's name, address, telephone connection records, session times, service types, instrument number, and payment details. The revision eliminates redundant language and provides law enforcement with a more comprehensive set of data, enhancing their ability to investigate and gather information related to electronic communications.

Section 216 of the USA PATRIOT Act introduces amendments to Section 3121(c) of Title 18, United States Code, concerning the use of pen registers and trap and trace devices. The modifications expand the scope of authorized information collection, including details such as names, addresses, telephone connection records, and payment information of subscribers. Additionally, it refines the procedures for court-issued orders, specifying criteria for granting ex parte orders and mandating record maintenance for devices used on data networks. The amendments also enhance the contents of orders, outlining attributes of communications covered. The section includes provisions related to nondisclosure requirements and introduces adjustments to definitions for terms such as 'pen register' and 'trap and trace device.'

Section 220 amends Chapter 121 of Title 18, United States Code, specifically focusing on sections 2703 and 2711. The amendment expands the authority for the nationwide service of search warrants for electronic evidence. It replaces the phrase 'under the Federal Rules of Criminal Procedure' with 'using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation' in section 2703. Additionally, section 2711 is amended to include a definition of 'court of competent jurisdiction,' aligning it with the meaning assigned by section 3127, and extending to any Federal court within that definition, without geographical limitations. A conforming amendment in section 2703(d) removes the reference to section 3127(2)(A). These changes enhance the legal framework for obtaining electronic evidence search warrants on a nationwide basis.

Thank's For Watching