

11.4: Information Security Issues

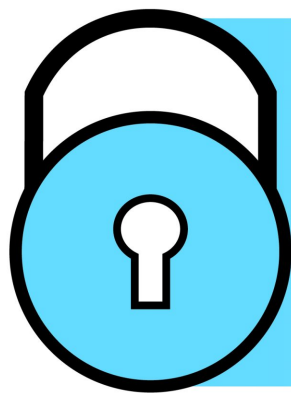
Information security is one of the fastest growing areas of the law affecting businesses today. Any business that collects, uses, and stores personal information about employees and customers is subject to these laws. Businesses are also increasingly targeted by hackers who seek to steal private information on a large scale.

Security Analysis

A simple but widely-used security model is the **CIA Principle** or **CIA Security Rule**, which stands for Confidentiality, Integrity and Availability. The principle is applicable across points of contact from access to a user's internet history to security of encrypted data across the Internet.

Figure 21.2 CIA Principle

Security Rule



- Confidentiality
- Integrity
- Availability

Confidentiality is the ability to hide information from those without authorization to view it. While perhaps the most obvious principle, it is usually the one that is attacked most often. Cryptography and Encryption are methods used to protect confidentiality of data transferred across the Internet.

Integrity is the ability to ensure that data is an accurate and unchanged representation of the original information. One common security attack is to intercept some important data and make changes to it before sending it on to the intended receiver.

Availability is the ability to make information readily accessible to authorized users at all times. Some security attacks attempt to deny access to appropriate users, either to inconvenience them or to achieve another goal such as redirecting business to a competitor.

As discussed in Section 21.3 above, HIPAA's Security Rule requires covered entities to implement the CIA principle to protect PHI.

Data Breaches

According to the Pew Research Center, almost eighty-five percent of individuals in the US shop online. And most retailers collect customer's personal and financial data. If a customer uses a form of payment other than cash, then the customer's personal and financial information will be shared with the business.

Rather than pickpocket an individual consumer, thieves today are targeting businesses to collect personal and financial information of entire consumer sets. Data breaches affect all industries, such as retail, credit bureaus, hospitals, and government agencies. In the first half of 2019, there were over 4.1 billion compromised documents reported as part of only 3,800 disclosed data breaches.

Cybersecurity experts advise that cyber criminals run automated online scripts looking for unsecured databases. While some larger businesses are particularly targeted, cyber criminals are the most successful when targeting small to medium-sized businesses that are unaware of the threat or do not want to spend adequate resources on cybersecurity.

Businesses should be aware, though, that approximately sixty percent of data breaches are the result of human error rather than outdated or insufficient technology. Therefore, by adequately training employees, many data breaches may be avoided. For example, breaches often result from sending emails to the wrong person, responding to phishing attacks, sharing passwords, and leaving computer screens open.

Another big risk is when people use the same password for multiple accounts, such as email accounts, bank accounts, and social media. If the password is obtained by cyber criminals and added to the database of passwords, all the accounts will be at risk.

Big Data

In addition to financial data, businesses collect personal information about consumers and their habits. This is called **big data**. Consumer information is very valuable because businesses can search the data to identify spending habits to target marketing to likely customers. This reduces costs and increases profit for businesses, especially as e-commerce increases the number of competitors across industries.

Another benefit to mining the data available about consumers is businesses can make more profitable decisions. For example, health insurance companies are heavily invested in big data because they want information about the lifestyle habits of the people they insure and potentially insure. If they know someone is a smoker, eats a lot of sugary foods, or has a sedentary lifestyle, then they can adjust premiums accordingly to minimize their risk. Insurance companies look for trends not just for individuals but also regions, types of occupations (including those with the highest risk of addiction or obesity), and socio-economic status.

Big data is also connected to the Internet of Things. The **Internet of Things (IoT)** is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. In other words, the IoT includes everyday devices connected to the internet, including medical devices, appliances, vehicles, and buildings.

As more businesses seek big data about consumers and sell IoT items to consumers, privacy rights are impacted. Data collection in public spaces, such as billboards tracking who stops to read them, may be lawful. However, the location and manner of data collection involves different expectations of privacy. For example, businesses argue that by purchasing and installing "smart home" appliances and products, consumers have consented to surveillance and data collection. Consumer advocacy groups argue that purchasing goods for a particular use does not give consent to businesses to invade consumer privacy in their homes. These issues will be heavily litigated in the years to come.

Transborder Data Transfers

As discussed previously, the EU has a comprehensive set of privacy laws and regulations. The EU has strict limits on the export of all human resources data and consumer information to the US, even when the data export occurs within the same business. To help US businesses comply with the EU laws, the US Department of Commerce negotiated a "safe harbor" of data protection practices that the EU approved. If a US business can certify its compliance with the Safe Harbor Principles, then the EU will approve data transfers to that business.

Security Incident Preparation and Response

Businesses are not able to prevent all data security breaches. However, businesses need to take steps to protect against known and reasonably anticipated threats to confidential information. For businesses without sufficient in-house cybersecurity staff or

expertise, **Managed Security Service Providers (MSSPs)** offer a wide range of security services, including setting up security infrastructure and incident response.

Although federal and state laws vary regarding legal requirements, a business should have a written cybersecurity program that conforms to their industry's recognized cybersecurity framework.

In general, a cybersecurity program should:

- Protect the security and confidentiality of all electronically stored records containing an employee or customer's social security number, driver's license number, state identification card number, credit and debit card information, dates of birth, passwords, and personal information;
- Protect against any anticipated threats or hazards to the security or integrity of the confidential information;
- Provide for reliable and accurate backups of data; and
- Protect against unauthorized access to and acquisition of information likely to result in an employee or customer being exposed to a material risk of identity theft or fraud.

Many laws, including HIPAA, have cybersecurity regulations with which businesses must comply. Certain industries have also issued their own security standards. For example, the Payment Card Industry (PCI) Security Standards Council has issued standards for the safety of credit and debit cardholder data across the globe.

Businesses wanting information about implementing cybersecurity programs that are appropriate for their industry should consider the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity. The mission of NIST is to help organizations understand and improve their management of cybersecurity risks. It is an excellent place to start when analyzing cybersecurity issues.

11.4: Information Security Issues is shared under a [not declared](#) license and was authored, remixed, and/or curated by LibreTexts.

- **21.4: Information Security Issues** by [Melissa Randall and Community College of Denver Students](#) is licensed [CC BY 4.0](#). Original source: <https://introductiontobusinesslaw.pressbooks.com>.