6.2: The Information Security Triad- Confidentiality, Integrity, Availability (CIA)

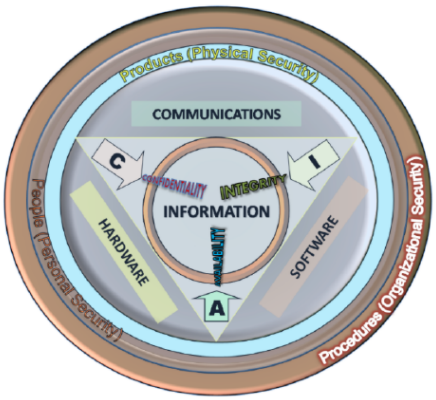

Figure 6.2.1: The Information Security triad: CIA. Image by John M. Kennedy T., is licensed under CC BY-SA

Confidentiality

Definition: Confidentiality

Confidentiality refers to restricting access to information only to authorized users.

Protecting information means you want to restrict access to those who are allowed to see it. This is sometimes referred to as NTK, Need to Know, and everyone else should be disallowed from learning anything about its contents. This is the essence of confidentiality. For example, federal law requires that universities restrict access to private student information. Access to grade records should be limited to those who have authorized access. Companies must keep sensitive data like customer records, trade secrets, and financial information confidential. A breach of confidentiality occurs when unauthorized entities access restricted data - for example, through a hack or stolen laptop. Loss of confidentiality can harm reputation, erode trust, and violate data privacy laws.

Integrity

Definition: Integrity

Integrity means maintaining the accuracy and completeness of data over its lifecycle.

Integrity is the assurance that the information being accessed has not been altered and truly represents what is intended. Just as people with integrity mean what they say and can be trusted to represent the truth consistently, information integrity means information truly represents its intended meaning. Information can lose its integrity through malicious intent, such as when someone who is not authorized makes a change to misrepresent something intentionally. An example of this would be when a hacker is hired to go into the university's system and change a student's grade. Lack of integrity undermines business decisions, compliance, and analytics.

Integrity can also be lost unintentionally, such as when a computer power surge corrupts a file or someone authorized to make a change accidentally deletes a file or enters incorrect information.

Availability

Definition: Availability

Availability ensures information systems and data are accessible by authorized users when needed.

Information availability is the third part of the CIA triad. Availability means information can be accessed and modified by anyone authorized to do so in an appropriate time frame. Depending on the type of information, an appropriate timeframe can mean different things. For example, a stock trader needs information to be available immediately, while a salesperson may be happy to get sales numbers for the day in a report the next morning. Online retailers require their servers to be available twenty-four hours a day, seven days a week. Other companies may not suffer if their web servers are down for a few minutes once in a while. Companies require high availability for critical systems - like e-commerce sites, cloud platforms, and customer databases - to maintain operations. Lengthy downtime and unreachable systems can cripple productivity, revenue, and customer satisfaction.

You'll learn about who, what, and why of cyber-attacks in this chapter. Different people commit cybercrime for different purposes. Neglecting confidentiality, integrity or availability exposes companies to significant cybersecurity risks that can impact finances, reputation, and continuity. Wise investments in CIA safeguards deliver value by reducing business disruption, preserving trust, and avoiding high recovery costs. For example, investing in Security Operations Centers that are designed to fight cybercrime. Jobs in a Security Operations Center (SOC) can be obtained by earning certifications, seeking formal education, and using employment services to gain internship experience and job opportunities.

The Danger

In chapter 5, we discussed various security threats and possible solutions. Here are a few scenarios to illustrate how hackers trick users.

Hijacked People

Melanie stopped at her favorite coffee shop to grab her drink for the afternoon. She placed her order, paid the clerk, and waited to fulfill orders' backup while the baristas worked furiously. Melanie took her phone out, opened the wireless client, and linked to what she thought was the free wireless network for the coffee shop.

Sitting in the corner of the store, however, a hacker had just set up a free, wireless hotspot "rogue" posing as the wireless network of the coffee shop. The hacker hijacked her session when Melanie logged on to her bank's website and accessed her bank accounts. The same risk can also happen to a business at a larger scale. in 2018, over 150,000 payment cards were compromised in a point-of-sale breach at coffee chain Caribou Coffee, caused by hacking into their systems via unsecured WiFi networks at some store locations. This illustrates the cybercrime risks of public WiFi use without proper IT security precautions (CBS News, 2018)

Hijacked Companies

Jeremy, an employee of a large, publicly-held corporation's finance department, receives an email from his CEO with an enclosed file in Adobe’s PDF format. The PDF regards earnings for the organization in the third quarter. Jeremy does not recall his department making the PDF. His interest is triggered, and he opens his attachment.

The same scenario occurs around the company as thousands of other workers are enticed to click on the PDF attachment successfully. As the PDF opens, ransomware is mounted on the workers' computers, including Jeremy’s, and the process of storing and encrypting corporate data begins. The attackers' target is financial gain, as they keep the company's ransom data until they get paid. As with Jeremy's case, the consequences for opening an attachment in a spam mail or from an unfamiliar address could be disastrous. In 2017, shipping giant Maersk suffered a destructive cyber attack that disabled IT systems across its global operations for weeks. This disruption to critical business systems cost Maersk an estimated $300 million in lost revenues. (Reuters, 2017)

Targeted Nations

Some of today's malware is so sophisticated and expensive to create that security experts believe that it could be created only by a nation-state or group of nations. This malware can be designed to attack vulnerable infrastructures, such as the water network or electric grid.

This was the aim of the Stuxnet worm, infecting USB drives. The movie World War 3.0 Zero Days tells a story of a malicious computer worm called Stuxnet. Stuxnet has been developed to penetrate Programmable Logic Controllers (PLCs) from vendors-supported nuclear installations. The worm was transmitted into the PLCs from infected USB drives and ultimately damaged centrifuges at these nuclear installations. China's APT10 hacking group allegedly stole IP from managed IT service providers to access customer data from firms in aviation, biotech, and other industries. Victim companies lost competitiveness. (US Department of Justice, 2018)

Threat Actors

Threat actors include amateurs, hacktivists, organized crime groups, state-funded groups, and terrorist organizations. Threat actors are individuals or a group of individuals conducting cyber-attacks on another person or organization. Cyberattacks are intentional, malicious acts intended to harm another individual or organization. The major motivations behind cyberattacks are money, politics, competition, and hatred.

Known as script kiddies, amateurs have little or no skill. They often use existing tools or instructions to start attacks found on the Internet. Some are only curious, while others seek to show off their abilities by causing damage. While they use simple methods, the outcomes can often be catastrophic.

Hacktivists

A hacktivist can act independently or as a member of an organized group. Hacktivists are hackers who rage against many social and political ideas. Hacktivists openly demonstrate against organizations or governments by publishing articles and images, leaking classified information, and crippling web infrastructure through distributed denial of service (DDoS) attacks with illegal traffic. A denial of service (DoS) attack is one of the most powerful cyberattacks in which the attacker bombards the target with traffic requests that overwhelm the target server in an attempt to crash it. A distributed denial of service (DDoS) attack is a more sophisticated version of DoS in which a set of distributed computer systems attacks the target.

Financial Gain

The financial gain motivates much of the hacking activity that constantly threatens our security. Cyber Criminals are people who utilize technology for their own malicious intentions, such as stealing personal information to make a profit. Cybercriminals want access to our bank accounts, personal data, and everything else they can use for cash flow generation.

Trade Secrets and Global Politics

In the past few years, several reports have seen nation-states hacking other nations or intervening with internal policies. National states are also keen to use cyberspace for industrial spying. Intellectual property theft can give a country a considerable advantage in international trade.

Defending against the consequences of state-sponsored cyberespionage and cyber warfare will continue to be a priority for cybersecurity professionals.

How Secure is the Internet of Things

The Internet of Things (IoT) is rapidly expanding all around us. The internet of things is a network of physical objects that collect and share data over the internet. We're now beginning to enjoy the IoT rewards. There is a constant creation of new ways of using connected things. The IoT helps people link items so they can enhance their quality of life. Smart security systems, smart kitchen appliances, smartwatches, and smart heating systems are few examples of the IoT products available today.

For starters, many people now use connected wearable devices to monitor their fitness activities. How many devices do you currently own that link to the Internet or your home network?

How safe are those devices? For instance, who wrote the software to support the embedded hardware (aka firmware)? Has the programmer been paying attention to the security flaws? Are your home thermostats connected to the internet? Your Electronic Video Recorder (DVR)? When there are security bugs, can the firmware be patched in the system to fix the vulnerability? The new firmware will not update many computers on the Internet. For updating with patches, some older devices were not even developed. These two conditions put the users of such devices to face threats and security risks.

References

World War 3 Zero Days (Official Movie Site) - Own It on DVD or Digital HD. Retrieved September 6, 2020, from www.zerodaysfilm.com

Caribou Coffee President: Customer Data Exposed In Security Breach (2018). Retrieved September 10, 2023, from https://www.cbsnews.com/minnesota/news/caribou-coffee-president-customer-data-exposed-in-security-breach/

Reuters. (2017). Maersk says global IT breakdown caused by cyber attack. **https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO**

US Department of Justice. (2018). Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information. **https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion**

This page titled 6.2: The Information Security Triad- Confidentiality, Integrity, Availability (CIA) is shared under a CC BY 4.0 license and was authored, remixed, and/or curated by Ly-Huong T. Pham and Tejal Desai-Naik (Evergreen Valley College) .

- **6.2: The Information Security Triad- Confidentiality, Integrity, Availability (CIA)** by Ly-Huong T. Pham, Tejal Desai-Naik, Laurie Hammond, & Wael Abdeljabbar is licensed CC BY 3.0.