CIA triad in practice

Jordan Morris

The CIA Triad, also known as the Confidentiality, Integrity, and Availability triad, is a fundamental cybersecurity framework. Chai (2022) notes that this framework is centered around the concepts of confidentiality (private knowledge of unauthorized users), integrity (preservation of informational accuracy), and availability (system accessibility when needed). Despite its ubiquity and seeming simplicity, the CIA Triad significantly impacts system design, threat mitigation, and organizational risk analysis. In my opinion, the CIA Triad accurately describes basic components of cybersecurity but lacks the nuance to understand modern cybersecurity threats. Cybersecurity has become a more intricate field with every connected system.

To start, confidentiality has traditionally been maintained through technological tools like encryption, authentication software, and access controls. Chai (2022) emphasizes that confidentiality is particularly important in modern systems because these systems store a wide variety of sensitive information about individuals, finances, and organizational data. However, confidentiality is not always violated due to technological vulnerabilities. Many recent cybersecurity breaches have succeeded primarily through social engineering or phishing. Although technological systems may be secured, people are still susceptible to manipulation. In that way, confidentiality also contributes to a culture of privacy in organizations. Larger collections of private user data create tension between companies that want to collect data and users that do not want their privacy violated.

Integrity and availability are two sides of the same coin, defining whether people can trust a computer system. Without both of these elements, users will be unable to rely on informational accuracy or access their systems when necessary. Integrity is often attacked by malware, ransomware, hackers, or anyone that could manipulate informational accuracy for personal gain. Alternatively, availability is primarily attacked by denial-of-service or ransomware attacks that make it impossible for users to access systems until a price is met. For example, several major cities have faced ransomware attacks that took energy, hospitals, and other critical infrastructure offline until large sums of money were paid. This is important because it demonstrates how cybersecurity can have tangible effects on real-world safety. Simultaneously, there are many instances where integrity and availability are at odds; additional security controls may reduce availability whereas availability increases security risks.

The CIA Triad is clearly demonstrated in SCADA architecture. SCADA stands for supervisory control and data acquisition systems and often refers to infrastructure that connects physical processes with computer programs. Examples of this include water filtration plants, power grids, pipeline logistics, manufacturing processes, and more. Programmable logic controllers (PLCs), remote terminal units (RTUs), and supervisory control are commonly used programs that interact with real-world sensors to provide access to these systems. Confidentiality matters in SCADA systems because a hacker could steal proprietary information about physical processes or understand how the system operates if they gain access. Integrity matters in SCADA systems because incorrect information from a sensor could cause the system to take the wrong course of action and damage physical infrastructure. Finally, availability is most important in SCADA systems because these systems typically provide public services. If the power grid

goes down, people cannot access electricity. If water pipelines go down, people cannot access clean water. Every SCADA system provides a public service that people rely on, which is why these systems cannot afford extended periods of downtime.

SCADA provides an excellent example of what fails about the CIA Triad. The reason SCADA systems are vulnerable to cybersecurity attacks is because they are intimately connected. A vulnerability in the control software can be catastrophic, but a vulnerability in the third-party vendor, communication software, or hardware can be just as destructive. Cybersecurity is not inherently about hardening a single system against attacks. It is about managing risk across a network of external dependencies. This example demonstrates one of the largest issues with cybersecurity; while most cybersecurity frameworks are great at explaining risks of the current world, they often have short arms when it comes to the future. Once a system is deployed, cybersecurity teams have very little control over how threats will evolve to target their products.

While the CIA Triad may not fully encapsulate cybersecurity, I do not believe it is outdated. However, I do believe there are important lessons to take from its limitations. The most important concept to take away is that cybersecurity is not simply a technical issue. There are major factors of human behavior, organizational structure, and decision-making that contribute to cybersecurity failures. As a result, companies should not solely focus on hardening their technological tools. Employees should be trained to prevent risky behavior, management should be incentivized to supply cybersecurity resources, and systems should be continuously monitored for vulnerabilities. Many cybersecurity issues are not because of holes in our cybersecurity

framework; they are because people fail to account for humans and system complexity. This also begs the question: should cybersecurity ever evolve past technical frameworks into socio-technical models that define people as part of the system?

To summarize, the CIA Triad provides three pieces of the cybersecurity puzzle, defining what cybersecurity is meant to protect: confidentiality, integrity, and availability. However, cybersecurity today is not as simple as protecting these three principles. Threats are becoming more complex by the day, whether they are connected SCADA systems, human behavior, or legacy hardware. Cybersecurity requires system-level thinking and a certain degree of uncertainty in how threats will evolve both in the present and the future.

Works cited:

Chai, W. (2022, June 28). What is the CIA Triad? Definition, Explanation, Examples.

“Supervisory Control and Data Acquisition (SCADA).” *SCADA Systems*, n.d., http://www.scadasystems.net.