No System is Secure
Using the CIA Triad to Prevent Catastrophe
Introduction

You are a modern human. Working 45 hours a week, at your remote, work-from-home job. You order your groceries from Amazon, your laundry gets picked up, cleaned, and folded by a dry-cleaning service, and a maid comes to clean your apartment once-a-week. When you don’t want to cook, you order food from GrubHub. When you want to go out to eat, you get in your car, which suggests restaurants based on a blend of curated recommendations and sponsored advertisements. You have signed up for a new bank account, but have never met a live human.

To what do we owe all these spectacular conveniences? Data. Personal, and highly sensitive data entrusted to algorithms, and less-than-secure information systems.

Businesses face the same struggle. How can business leaders improve efficiency, reduce costs, and increase revenue? The answer, is (you guessed it) data. The trouble with data, however, is that it needs to be stored. Data needs to be secured, but at the same time, data needs to be available to those business entities that need it. So how do businesses leverage the most advanced and interconnected technologies, while maintaining critical standards of data privacy and ethicality?

Early information security (IS) scribes point to the “CIA” triad as ‘the’ IS framework, the purpose of which is to minimize information security risks. The CIA triad includes three key pillars: Confidentiality, Integrity, and Availability. Each pillar represents a unique information security threat category. While the true origin of the CIA triad is unknown, the three pillars of the framework have stood the test of time as the core threat areas for information systems.

The paper will provide in-depth examples and supporting research around each of the three security risks (Confidentiality, Integrity, Availability). This paper will also outline potential solutions, to show that by utilizing the CIA triad, information security risks can be significantly minimized for individuals and businesses if emphasis is put on mitigating all three risk types. The paper includes opinions and solutions posed by Bruce Schneider, author of Click Here To Kill Everybody.

Confidentiality

Confidentiality, the first pillar of the CIA triad, primarily affects privacy. Privacy concerns affect every single person on the planet. Anyone who has ever taken an embarrassing photo,
sent an email, or even written down their daily notes in a diary is at risk of a confidentiality breach. Confidentiality attacks can include threats like espionage and data theft.

A recent example of a major Confidentiality breach is the 2017 Equifax data breach, which exposed the personal and financial information of 145.5 million Americans (nearly half the population of the U.S.). Hackers exploited a key vulnerability in the Equifax website to gain access to this sensitive data. The hackers extracted the personal information from the 145.5 million U.S. consumers, including names, Social Security numbers, birth dates, addresses, and driver's license numbers. This data could be used to steal identities and attain victims’ medical histories, bank accounts, and employee accounts.

According to CNBC, as of February 2019, the stolen Equifax data has not been found or seen on any underground black market. Though security experts agree that the breach occurred and personal information from almost nearly the US population was stolen, no one expert can pinpoint where the data is currently. The data was also never found to be used in any of the expected illegal ways, such as identity theft scams and unauthorized account usage. Consumer data is typically put up for sale on the dark web immediately after it is stolen in an attempt to make sales before detection. Once detected, victims and institutions can quickly make changes or flag the data rendering it useless.

In the case of the Equifax breach, attackers exploited a critical vulnerability in the Apache web server software within the website. Equifax did not patch the vulnerability until months later, not before the attackers used the vulnerability to breach the network (despite being notified by Apache, US-CERT, and the Department of Homeland Security). One of Schneier’s ten high-level design principles for improving security and privacy of devices is extremely applicable here: Make the software patchable, patch quickly once vulnerabilities are discovered, and regularly check for patches.

In 2013-2014, Yahoo reported the biggest Confidentiality breach of the 21st century, compromising all 3 billion of its user accounts, and impacting its sale price by an estimated $350 million during merger negotiations with Verizon. Names, email addresses, telephone numbers, birth dates, hashed passwords, and even account security questions, were compromised and found on the underground web. According to Alex Holden, the founder of Hold Security, which has been tracking the flow of the stolen Yahoo data on the underground web: “The stolen Yahoo data is critical because it not only leads to a single system but to users’ connections to their banks, social media profiles, other financial services and users’ friends and family.”
Solutions

To mitigate confidentiality breach risks, Schneier emphasizes the necessity of a shift towards engineering security throughout the development process, rather than treating security as a rushed add-on at the very end of development for compliance. In terms of securing confidential data, Schneider offers security principles surrounding data and databases to organizations, which are often prime targets for attackers. Schneider poses suggestions like minimizing data collection to only what is absolutely necessary, minimizing data use, transparent data collection, use, storage, and deletion and anonymizing data whenever possible. Schneider also suggests allowing users to access, inspect, correct, and delete their data, and deleting data when it is no longer necessary. Schneier also argues for a mixture of individual and collective expenditures when it comes to improving Internet security. Individual expenditures include security programs for computers and firewalls for networks while collective expenditures include police investigations of cybercrime and investments in Internet infrastructure.

As the connection point for internet access, Schneier points to ISPs as another potential method for improving security on the internet. He believes that ISPs should provide users with a secure connection, scan for malware, block potential phishing emails and web pages attempting to steal information. As companies that connect users to the internet, ISPs should take steps to educate consumers about internet threats and warn users when their devices or connections are compromised.

Outside of Schneider’s suggestions there are many other preventative measures that can be taken to ensure confidentiality, and to prevent sensitive information from being accessed by unauthorized users. Some basic examples include enforcing strong password practices, and multi-factor authentication. More advanced examples include biometric verification, security tokens, data encryption, monitoring all database access activity and usage patterns to detect data leakage, blocking malicious web requests, and authentication protocols for communications over the internet.

Integrity

While confidentiality cyber-attacks have been the most widely publicized, it is the second category of cybersecurity threats that is the most dangerous of all: attacks of integrity. As the name suggests, these aim to compromise the integrity of systems they affect. They are much harder to detect and deter, and because of this, have the potential to cause large, widespread
damage. “A confidentiality breach in your car means someone learns your driving habits,” says Mike Gault, founder of cyber-security company Guardtime, “An integrity breach means they could take over your brakes.” (Gault)

Security experts warn that there are three major areas where integrity attacks would be particularly devastating. Russia has proven this in their exploits of Ukrainian critical infrastructure such as power grids and water supplies. Threats of this kind are also in line with Russian military doctrine *maskirovka* (meaning “camouflage, concealment, and deception”). Given the current political dynamic between the U.S. and Russia, military application of these cyber-attacks is of extreme relevance. Lastly, attacks on the stability of the global financial system could be the most catastrophic of all.

On April 23, 2013, a tweet from the Associated Press said that President Barack Obama had been injured after explosions occurred at the White House. Within minutes, $136 billion was erased from the Standard & Poor’s 500 Index. Just as fast as value was lost, US indices rebounded as the tweet was proven to be the result of a hack.

The AP Twitter hack highlights the substantial risk that integrity cyber-attacks pose to the stability of the global financial system. According to a research report by IBM, the financial sector was attacked 65% more often than other industries. Due to the increasing interconnectedness of modern finance, misinformation can cascade through these systems, snowballing into potentially devastating effects down the line. In the case of this flash crash, we are lucky that the integrity breach was caught quickly enough that it did not cause much lasting damage. But as cyber-attacks become more sophisticated, quick thinking humans cannot be what is relied on in the future to keep financial systems stable.

A white paper published by the Institute for International Finance (IIF) specifically identified a data integrity attack as one of the four most likely and far-reaching threat scenarios. If a large-value payment system, such as one that settles transactions between major financial institutions, were to suffer an integrity breach, the resulting liquidity issues would proliferate throughout the globe. The IIF also mentions central securities depositories (CSDs) and custodian banks as particularly vulnerable targets. If multiple CSDs and custodians were to be attacked at once, securities data reconstruction may not be fully possible, causing widespread loss of confidence in the financial system.

Defense against, and use of, integrity attacks plays a key role in national security and military operations. In a 2015 testimony before Congress, James Clapper, then the Director of National Intelligence, noted the threat of “cyber operations that will change or manipulate
electronic information in order to compromise its integrity (i.e., accuracy and reliability) instead of deleting it or disrupting access to it... Decision-making by senior government officials, corporate executives, investors or others will be impaired if they cannot trust the information they are receiving.” (Clapper)

Due to the sensitive nature of military operations, there is only one public example of a U.S. integrity cyber-attack: Stuxnet. First uncovered in 2010, Stuxnet is regarded as the first true cyber-weapon, having caused physical damage to over a thousand machines, most notably ruining one fifth of Iran’s nuclear centrifuges. In his technical report on the malware, Ralph Langner, a cyber-defense expert, details how Stuxnet was able to spread to over 200,000 computers and specifically seek out the Iran's centrifuges’ control units before destroying them through over-pressurization and speeding up rotors to their critical (resonance) speeds.

In his conclusion, Langner’s notes that the “future is burdened by an irony: Stuxnet started as nuclear counterproliferation and ended up to open the door to proliferation that is much more difficult to control: The proliferation of cyber weapon technology.” (Langner)

Russia has taken the lead on the use of cyber-attacks against critical infrastructure, most notably in Ukraine. Two days before Christmas in 2015, a quarter-million Ukrainians were without power due to a Russian cyber-attack on three energy distribution companies. Two years later, a Kiev transmission station was knocked out by a virus later identified as CrashOverride, the first automated malware found since Stuxnet designed to destroy physical infrastructure.

**Solutions**

The road to defeating advanced malicious programs such as Stuxnet, CrashOverride, and the countless others that haven’t been uncovered won’t be easy, but it is imperative that it becomes a priority. The majority of the cyber-security industry has been focused on a singular task: keeping bad actors and software out of the systems they’re protecting. This is necessary, but not sufficient; it is the equivalent of only securing your most valuable possessions with a lock and key. Once past these perimeter defense mechanisms, attackers can run rampant within a system, often without the notice of the owner.

Integrity-specific cyber-security solutions are the equivalent to an alarm system: if anything is changed unexpectedly, even from seemingly friendly sources, an alert is triggered. There are multiple of these integrity schemes being researched and developed, but significant challenges still exist in efficiently deploying them. This is where Mike Gault, Guardtime CEO, believes that the security community should be focused on: “Once the security community moves
beyond the mantras “encrypt everything” and “secure the perimeter,” it can begin developing intelligent prioritization and response plans to various kinds of breaches - with a strong focus on integrity. We can no longer count on keeping the hackers out. Let’s work on ensuring we can catch them once they break in.”

**Availability**

Listed last in the triad, availability breaches occur when users can no longer access a service and control their data. Unlike confidentiality breaches, availability threats don’t initially seem as dangerous. However, as computers become more prevalent and essential to society throughout the world, denial of service (DoS) quickly becomes catastrophic and doesn’t just affect property, but also safety and human life. Examples of this include disabling an internet connected car, hacking into factories and power plants to shut them down, or denying access to satellites. These are just a few of the many technologies that are vulnerable to availability threats.

Take the findings of researchers Billy Rios and Jonathan Butts presented at the 2018 BlackHat security conference. By replicating the cloud infrastructure of Medtronic’s pacemaker software delivery system, Rios and Butts identified vulnerabilities that would allow attackers to inflict fatal harm to patients. They identified that the pacemaker’s program updates and communicates with support equipment rather than the pacemaker itself, therefore providing more access opportunities to hackers. Through these vulnerabilities, attackers could tamper with vital accessories, reach the pacemakers, and shut them down. The system also ultimately lacked “digital code signing”, which validates the legitimacy of the software itself along with its subsequent updates. Attackers then had the ability to control the supporting equipment, subsequently allowing them to reach the pacemaker and turn it down.

Medtronic responded by fixing the data privacy issues Rios and Butts discovered in their demonstrations, but there were no other mitigation attempts for the vulnerabilities that could kill their users. They stated that the findings “revealed no new potential safety risks” and that the issues weren’t “exploitable remotely”. Butts and Rios debated fitting a pig with Medtronic’s pacemaker to demonstrate that they could kill it with their iPhone, but ultimately decided against it. Similar to the pacemakers, they were able to expose availability vulnerabilities that provided the opportunity for attackers to disable the pump and harm or even kill the patient.
Solutions

Increasing security and safety against availability breaches consists of several strategies. For example, the software transmission system in Medtronic’s pacemakers and insulin pumps simply needed to be secured with code signing. A solution Schneier suggests is to move towards less centralization and more towards distributed systems, making these systems more robust and fail-safe if others shut down. This is similar to the approach of data centers and distributed cloud systems, which host data in multiple locations. If a system in California goes down, the data is still available. When a system does go down, proper response time is essential to preventing malicious effects to the system that’s down. Another mitigation strategy Schneier suggests is software actually policing itself, therefore creating a fail-safe and validation process to weed out threats and inauthentic users.

As with the two other types of security risks, a large component of combating and preventing accessibility issues is finding them quickly and testing often. In addition to this, availability vulnerabilities need to be taken much more seriously than they have been. They aren’t just precursors to other types of risks, but provide an opportunity for far greater and more dangerous implications than currently perceived.

Conclusion

As systems and technologies become more complex and interconnected, data security and privacy quickly becomes one of the most pressing issues facing modern technological progress. Convenience and ease-of-use must not be the policy when setting up complex information systems. Systems now need to be built from the ground up with information security principles and frameworks in mind. Specifically, understanding the CIA triad framework, and its core pillars (Confidentiality, Integrity, Availability), will help individuals and businesses developing IS solutions to keep security in mind throughout the Software Development Life Cycle (SDLC).

By evaluating the CIA triad framework, understanding previous cases of major data breaches, and learning how to implement preventative IS security measures, individuals and businesses may be able to mitigate future IS catastrophe.
Sources


Fazzini, Kate. "The stolen Equifax data has never been found, and experts suspect a spy scheme." CNBC. 14 Feb. 2019. CNBC. 15 Mar. 2019


Schneier, Bruce. Click Here to Kill Everybody. Frechen: MITP, 2019.