CIA Triad & Authorization vs. Authentication

CIA consists of three concepts: confidentiality, integrity, and availability. Authentication and Authorization are not twins, and authentication always comes first.

CIA Triad

The CIA Triad is a concept within cybersecurity that intends to keep data, systems, and hardware: accurate, trusting, secure/private, and confidential. CIA translates to confidentiality, integrity, and availability (Chai, 2022). The CIA Triad may not hold a single author, but it is a pillar for effective cybersecurity. Some examples of effective cybersecurity in the three areas are:

Example Confidentially (Chai, 2022):

Data storage on hard copy
Biometric verification

Example Integrity (Chai, 2022):

Cryptographic checksums
Detecting changes to data via EMP

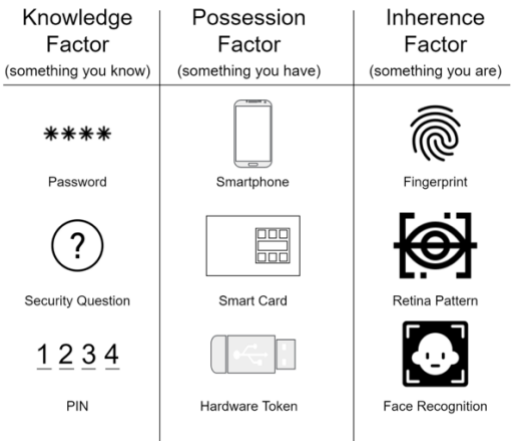
Example Availability (Chai, 2022):

Ensuring bandwidth speeds
Disaster recovery

Authentication

Firstly, “authentication (AuthN) is a process that verifies that someone or something is who they say they are” (Authentication Vs. Authorization: What is the Difference? | OneLogin, n.d.), for example, if we were to look at a square amazon box, how do we know its actually what it presents itself as; we most likely make this determination based on its coloring, script, and shape. In IT, more often than not, three factors determine authentication for Authorization.

3 Authentication Factors



(Authors, 2021)

Example REST API, OAuth 2.0 (Gupta, 2022)

Creates secure access tokens and refreshes these tokens. It also can create specific tokens depending on request or permission type. Finally, another feature in OAuth 2.0 is JSON Web Tokens.

Authorization

Thinking back to the previous example of an amazon box, now that we can determine it is indeed an amazon box, we can move on to determining who can open it. It is essential to note the phrase, "Authorization is the security process that determines a user or service's level of access [and] authentication always comes before Authorization (Authentication Vs. Authorization: What is the Difference? | OneLogin, n.d.). An example below details RBAC and ABAC.

Example

Role-Based Access Control (RBAC) gives permission assignment to roles versus individual users like attribute-Based Access Control (ABAC) does.
Attribute-Based Access Control. Using our previous example of an amazon box, five people receive five pairs of scissors to open the box; this is ABAC. RBAC, on the other hand, would give one pair of scissors to the entire group of five people; each person can access the scissors to open the box. RBAC becomes easier because system managers can deal with uses and permission in bulk" (What Is Authorization? - Examples and Definition - Auth0, n.d.). In other words, we will only need to keep track of one pair of scissors versus five in the above example.

Difference between Authentication and Authorization

In the web article, the between Authenticating and Authorizations sums up beautifully, "[authentication] verifies the identity of a user or service before granting them access, while [Authorization] determines what they can do once they have access (Authentication Vs. Authorization: What is the Difference? | OneLogin, n.d.). Another concept often referred to as access control is part of Authorization, not authentication as many assume.

Conclusion

In sum, the CIA triad is the three-concept idea of confidentiality, integrity, and availability servings as a pillar for effective cybersecurity. Arguably another foundation is Authorization and Authentication. Authentication usually involves three concepts to review a system or person's identity. At the same time, Authorization comes after in ways such as RBAC and ABAC to give access to requested data or systems.

References

Authentication vs. Authorization: What's the Difference? | *OneLogin*. (n.d.). Retrieved September 13, 2022, from https://www.onelogin.com/learn/authentication-vs-authorization#:%7E:text=Authentication%20and%20authorization%20are%20two,authorization%20determines%20their%20access%20rights.

Authors, R. (2021, December 13). *What Are the Three Authentication Factors?* Rublon. Retrieved September 13, 2022, from https://rublon.com/blog/what-are-the-three-authentication-factors/#:%7E:text=The%20three%20authentication%20factors%20are,something%20you%20are%2C%20e.g.%2C%20fingerprint

Chai, W. (2022, June 28). *confidentiality, integrity and availability (CIA triad)*. WhatIs.com. Retrieved September 13, 2022, from https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Gupta, P. (2022, May 23). *5 fundamental strategies for REST API authentication*. SearchAppArchitecture. Retrieved September 13, 2022, from https://www.techtarget.com/searchapparchitecture/tip/5-fundamental-strategies-for-REST-API-authentication

OneLogin: Market-Leading Identity and Access Management Solutions. (n.d.). Retrieved September 13, 2022, from https://www.onelogin.com

What is Authorization? - Examples and definition - Auth0. (n.d.). Auth0. Retrieved September 13, 2022, from https://auth0.com/intro-to-iam/what-is-authorization/#definition-of-authorization-using-authorization-strategies

Risks & Solutions Involving Hospital Boiler SCADA Systems

The critical infrastructure system, hospital boilers, and SCADA systems address staffing and energy audit risks. While there are risks associated with SCADA systems itself, these risks are being addressed.

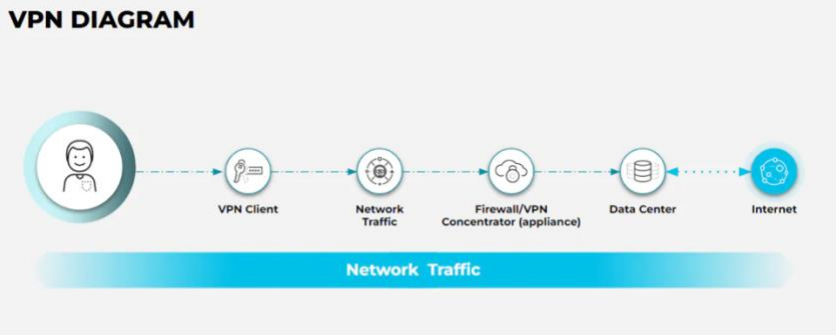
Critical Infrastructure System: Why boilers in Hospitals matter

When "the entire sterilization process inside a hospital begins with its system of industrial boilers, [and] are what allow the hospital to function" (Eklind 2020), protecting this process is crucial. Hospitals are vital, from lifesaving procedures to preventative care for humanity. Therefore using SCADA systems to ensure a fully functioning hospital outweighs SCADA risks, especially in times of crisis. Below are common risks to the SCADA systems as a whole. From there, we will next jump to two common risks that plague hospital boilers and how SCADA applications have decreased these risks.

Risks to SCADA System & Solutions

A common risk is an unsanctioned access to SCADA system software and packet access; both are actively being mitigated with VPNs and firewalls (*SCADA Systems)*.

Example:



(What Is Zero Trust Network Access (ZTNA), n.d.)

Risks to Hospital Boilers & SCADA Applications to Decrease Risk

Among the most common SCADA systems for boilers are "energy audits, [and] boiler automation (2022, RakHOH); outlined below are common risks associated with steam boilers in a hospital setting and SCADA applications to decrease said risk.

Risk	SCADA Application	Type	Example
Not enough staffing for supervisory control.	Supervisory computer equipped with HMI software.	Automation	Unsafe condition occurs, alarm sounds, and HMI

			software takes care of problem (Automatedo, 05:20). Intervention by operator no longer required.
Impact: Quicker reaction time, less required manpower, overall efficiency increase.			
Risk	SCADA Application	Type	Example
Energy Audits to long and complex, not available instantly.	SCADA Server (SQL) Mobile HMI (Automatedo, 03:26).	Data Communication Automation	Upcoming Weather Advisory occurs, access data from device to ensure proper functions. Also, based on the data, possibly have a safety protocol activated. Cloud storage of data if Boilers malfunction. (MetroCloud)
Impact: Real-time access for monitoring and weather advisory solutions.			

Conclusion

Hospital boilers with SCADA systems decrease staffing and energy audit risks. Risks associated with SCADA systems itself are being addressed with VPNs and firewalls. Therefore implementing SCADA systems within a Hospital Boiler is justified.

References

Automatedo. (2022, September 27). *SCADA Explained | Supervisory Control and Data Acquisition* [Video]. YouTube. Retrieved October 15, 2022, from https://www.youtube.com/watch?v=7kTJA69EzMc

Eklind, A. (2020, August 11). *The Role of Boilers in Hospital Steam Sterilization - Miura America*. Miura Boiler. Retrieved October 15, 2022, from https://miuraboiler.com/the-role-of-boilers-in-hospital-steam-sterilization/

MetroCloud. (2022, August 10). *Cloud SCADA Hot Water & Steam Temperature Monitoring*. MetroCloud | Cloud SCADA Water Monitoring Systems. Retrieved October 15, 2022, from https://metrocloud.us/hot-water-steam-temperature-monitoring-cloud-scada/

RakHOH. *A Guide to PLC and SCADA Automation in Steam Boilers*. (2022, February 10). Boilers and Steam Boiler Manufacturer in Maharashtra, Pune. Retrieved October 15, 2022, from https://rakhoh.com/en/a-guide-to-plc-and-scada-automation-in-steam-boilers/

SCADA Systems. (n.d.). SCADA Systems. http://www.scadasystems.net

What Is Zero Trust Network Access (ZTNA). (n.d.). Palo Alto Networks. Retrieved October 18, 2022, from https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust-network-access-ztna

Balancing Cyber Security and Additional Hardware: Budget Suggestions

There will be trade-offs while balancing both training and technology expenditures. The best course of action begins with acknowledging the importance of balancing training and tech and then taking advantage of free cybersecurity training and tax deductions.

Importance of Balancing Training with Tech

To put in context our present reality, cyber-attacks account for over $400 billion globally, with 35% being due to human error and 47% of IT/CS professionals reporting poor collaboration in mitigating such risks (Fissea, 2021).

According to Digital McKinsey and Global Risk Practice, our primary concerns training employees and purchasing new technology, should "go beyond technical controls to build a holistic program that protects the enterprise, engage the full set of stakeholders to ensure appropriate support and decision-making, Integrate cybersecurity with business strategy to build trust and create value" (2019).

Subject	Importance
Our World	$400 Billion loss globally We don't want to lose profit/investment
Plan of Action	Create a framework that considers everyone's input to form trust & understanding of good cybersecurity. Good cybersecurity = Good business

Free Cyber Training Resources

SANS, accessible continually updated sources (Cyber Aces Free Cyber Security Training Course | SANS Institute, n.d.) to facilitate the previously mentioned topic, Good cybersecurity = Good business. Additionally, possible ways to encourage Good cybersecurity = Good business includes turning "virtual happy hours into monthly security AMAs, free resources from SANS and federal government, security office holding weekly office hours, deputizing volunteer security leads for each department, [and] dedicating team channel to all things security" (5 Ways to Level up Security Awareness Training Without Breaking the Bank, 2021).

Subject	Importance
Training Cost	Free resources = >less expenditure =>increased profit.

Tax Deductions

Consider tax deductions for business computers, such as Section 179 (York, 2022). Additionally, other possibilities include tax deductions for advertising and promotion, auto expenses, bank fees, business licenses and permits, charitable contributions, commissions, costs of goods sold, education, equipment purchases, events, furniture and décor, gifts, home internet, home office expenses, business insurance, interest expense, leasehold improvements, meals (not entertainment), merchant processing fees, payroll expense, professional, fees, office expenses (software), rent, repairs and maintenance, and lastly development costs (Just a Moment., n.d.-b).

Subject	Importance
Tax Deductions	Training, software, development less expenditure =>increased profit.

Conclusion

There are tax deductions and free cybersecurity resources to utilize and balance our tech and cybersecurity budgets. Understanding the importance of both sides in facilitating good business is also essential.

References

Cyber Aces Free Cyber Security Training Course | SANS Institute. (n.d.). https://www.sans.org/cyberaces/

Fissea. (2021). *Cybersecurity-The human factor*. https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf

Just a moment. . . (n.d.-b). https://gusto.com/blog/taxes/tax-deductions-tech-startups

Perspectives on transforming cybersecurity. (2019, March). McKinsey. https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

York, E. S. A. (2022, February 16). *Self-Employed Computer Tax Deductions: The Ultimate Guide*. https://www.keepertax.com/posts/self-employed-computer-tax-deduction

5 Ways to Level Up Security Awareness Training Without Breaking the Bank. (2021, July 19). Tugboat Logic. https://tugboatlogic.com/blog/five-low-budget-ways-improve-security-awareness-training/