Chad Ballay

**Week 1 – CIA**

Confidentiality, Integrity, and Availability are the three components of the CIA triad. These three foundational principles of information security can be secured through the various applications of network controls. This risk reduction and management is at the core of the learning efforts we are pursuing.

* **Confidentiality** – ensuring that information is not made available or disclosed to unauthorized individuals, entities, or processes
* **Integrity** - maintaining and assuring the accuracy and completeness of data over its entire lifecycle.
* **Availability** – ensuring that the information is readily accessible to those that have need.

(Information Security, n.d.)

The defense for breaches of the confidentiality leg of the triad will usually occur through defense in depth. Incoming email is checked for trojans or phishing links. Passwords are required to be rotated and complex. SSH keys are rotated frequently. Network segmentation is implemented. Etc, etc…. For each of these layers the end goal is to act as a bulwark against an attacker’s wish to gain access. Much of the mitigation will come from process review and implementation. Requirements being listed and then programmatic tools implemented to enforce these requests. My favored solution for the aforementioned SSH key rotation is automating the the CI/CD pipeline to also generate/push a new SSH key as requested. See this link for a rough outline. (<https://hackernoon.com/ssh-key-rotation-b0877fbd75c2>) When automation removes the stress and pain of following the required process, you ensure it will be done often and consistently executed.

For integrity the focus is ensuring that the data is not altered in any way. Either maliciously or inadvertently. For instance, an attacker gaining access to the order database and updating their order/cost entries to not reflect reality. File hashes and audit logs are two straightforward examples. For file hashes this helps ensure that the data remains the same in transit. Audit logs and the infrastructure accounting is needed by the admins of the systems. This gives them the ability to understand changes to their system and to be able to identify unplanned events. (How NIST can protect the CIA triad, including the often overlooked ‘I’ – integrity, n.d.) A clear and unambiguous chain of custody is the name of the game here.

Finally, the Availability leg of the triad often times becomes an architectural design issue. DDoS based attacks will have to be mitigated by firewalls and possibly with load balancers and caches. Data center outages will require redundant deployments and network routing changes. Of the three, availability is usually a cost/benefit conversation about how expensive of a solution is prudent. Each nine gets progressively harder to achieve. (Betsy Beyer, 2018)

A screenshot of a cell phone

Description automatically generated

In closing, if any leg in this triad buckles the whole contraption falls. Whether this failure is maliciously induced, negligence, or an act of god the end result is significant impact. The lanes of traffic have to stay clear, be unaltered, and always open. This same analogy flows to the traffic infrastructure as well as to the network infrastructure. Without this interconnectedness the system falls apart.

# Bibliography

Betsy Beyer, J. P. (2018). *Site Reliability Engineering: How Google Runs Production Systems.* O'Reilly Media. Retrieved from https://landing.google.com/sre/sre-book/chapters/availability-table/

*How NIST can protect the CIA triad, including the often overlooked ‘I’ – integrity*. (n.d.). Retrieved from It Governance USA: https://www.itgovernanceusa.com/blog/how-nist-can-protect-the-cia-triad-including-the-often-overlooked-i-integrity

*Information Security*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Information\_security