Protecting Availability of Your Systems: A CISO's Perspective

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 200T: Cybersecurity, Technology, and Society, Professor Chris Brown

February 14, 2025

Assignment:

You are the CISO for a publicly traded company. What protections would you implement to ensure availability of your systems (and why)?

Who is a CISO? What is their role and responsibility in the organization?

A CISO (Chief Information Security Officer) is a senior executive and leader responsible for overseeing an organization's information security strategy and protecting its data, networks, and IT infrastructure from cyber threats (Nieles, Dempsey, & Yan Pilli, 2017). Their responsibilities include developing, implementing, and enforcing security policies to protect critical data. They convey the organization's security mission and philosophy through their leadership and collaboration with others, both internal and external parties. The typical workday for a CISO is spent in "continuous interaction with subordinates, colleagues, and superiors, collaborating with different groups and departments to ensure all business operations mirror the security policies and procedures of the organization" (Cisco, 2025). The CISO is constantly evaluating and managing the cyber and technology risk posture of the organization, along with developing, justifying, evaluating, and allocating cybersecurity investments and resources to meet the organization's security needs.

What is 'Availability'?

It is one of three key components to the CIA Triad—the 'Holy Trinity' of cybersecurity. The acronym stands for 'Confidentiality, Integrity, and Availability' (Hashemi-Pour, 2025). Confidentiality ensures that information is accessible only to authorized personnel (e.g., encryption). Integrity ensures data remains accurate and unaltered (e.g., checksums). Availability ensures information and resources are consistently and readily accessible when needed (e.g., redundancy resources). Availability includes properly maintaining software and hardware technical infrastructure systems that store and display the information. Most organizations aim to ensure 24/7 network availability year-round— the gold standard of availability is 99.999% uptime or a maximum operational downtime of 5.26 minutes per year.

What protections would you implement to ensure the availability of your systems (and why)?

To meet the 99.999% Gold Standard, companies will employ various tools, creating a dependable and redundant technological network ecosystem. We can organize and summarize Protection and Availability tools into several categories. First, the organization will want to implement redundancy and failover systems should a specific device, network of devices, or large sections of an organization's cyber network break down. A CISO will want to deploy and use multiple backup servers, databases, and cloud replication for data preservation. The *3-2-1 Backup Strategy* is a good rule of thumb: maintain three copies of one's data, using two different storage media, and safekeeping one copy offsite (Seagate, 2025).

Second, load balancing helps distribute network traffic to prevent system overloads and failures. Should a part of the network become overloaded or fail, the other devices (i.e., servers, routers) can take over the load to continue supporting the organization's end users. It is a good rule of thumb to have more than one point of failure in an organization and several preconfigured devices 'ready-in-hand' to serve as immediate replacements in a nearby climate-controlled security room. The IT Department can easily replace any network equipment that naturally fails or becomes comprised by nefarious actors with a new and/or compatible version; in addition, organizations usually have backup configurations of current devices to transfer onto new devices, reducing the downtime status and streamlining the Mean Time to Repair process (MTR). Examples of hardware include routers, switches, media converters, and even patch cables. We can also apply the redundancy philosophy to software or application services, like paying for an additional cloud service platform that mirrors the primary vendor services in case the primary fails. Therefore, load balancing is a holistic approach that targets and includes entire networks, applications, domain name systems (DNS), servers, databases, and global traffic and communications.

Third, the CISO oversees creating, implementing, and maintaining Disaster Recovery and Business Continuity Plans. The Business Continuity Plan is the 'Umbrella or Master' document containing the organization's network and security policies for Incident Response and Disaster Recovery procedures. It is the responsibility of the CISO to create, implement, and maintain security policies and procedures in these areas; however, the CISO is also responsible for educating the organization's workforce about those policies and procedures on a regular and annual basis. The hope and goal is to prepare the workforce before incidents and natural disaster take place while remaining compliant with regulatory agencies. Incident Response plans will direct IT professionals with detail and precision: its life cycle covers Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity (Cichonski, Millar, Grance, & Scarfone, 2012).

Another example of ensuring redundancy is the Disaster Recovery Plan, which will refer IT professionals to multiple tools and methods, like having multiple sources of power for an organization to remain active during all times of the day, 'rain or shine.' The goal is to persevere against any natural storm or hostile entity should they target and effectively nullify an organization's primary energy source—e.g., a local utility company. They will use Uninterruptible Power Supplies (UPS) for day-to-day operations to prevent surges and brownouts, mobile or large stationary gas/diesel generators to supply power to organizations for more extended periods, and sometimes operating remotely using Cloud Infrastructures (Desktop/Software as a Service) or prearranged physical locations to operate as backup facility should the primary facility become compromised or destroyed (e.g., Cold Site, Warm Site, or Hot Site).

Lastly, CISOs will want to proactively monitor and maintain hardware and software within the network using real-time alerts to address issues before they escalate. It helps prevent data loss and complete network failure: CISOs will create, implement, and maintain cybersecurity measures to protect against DDoS attacks, ransomware, and other threats, both insider and external. A CISO may implement within a Security Information and Event Management (SIEM) one or more Unified Management Systems (UMS) to proactively manage multiple IT, security, and business operations in a central location. The UTMs are placed at the network's edge, acting like a first-defense tool using various firewalls, group policies, and other software protocols against external threats and preventing unauthorized data from existing in the company's network. The UTMs also monitor traffic in real-time and send records of all traffic activity to internal servers using ports like SysLog for later review. Lastly, UTMs can host anti-virus, content filtering, and VPN services. UTMs are more like Intrusion Prevention Systems (IPS) than typical Intrusion Detection Systems (IDS) because an IDS only identifies activity, records it, and sends relevant notifications to authorized administrators; UTMs do the above AND proactively stop threats from entering the network at the front end.

Conclusion

CISOs want to achieve 99.999% uptime availability for their users through myriads of methods, tools, and educating the organization's workforce. Availability helps IT professionals ensure business continuity, maintain customer trust, and uphold an organization's reputation. CISOs will create and implement a well-thought policy and strategy using redundancy at its core in its systems and network designs to overcome challenges and obstacles that can obstruct or completely prevent user access to the company's resources.

References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Recommendations of the National Institute of Standards and Technology (NIS). *Computer Security Incident Hanlding Guide*, August.

Cisco. (2025, February 10). *What Is a CISO?* Retrieved from Cisco: https://www.cisco.com/c/en/us/products/security/what-is-ciso.html

Hashemi-Pour, C. (2025, January 26). *What is the CIA Triad? Definition, Explanation, Examples*. (W. Chai, Editor) Retrieved from TechTarget: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Lazzari, Z. (2023, October 23). *Levels of Hierarchy in Business*. Retrieved from CHRON: https://smallbusiness.chron.com/levels-hierarchy-business-22635.html

Mazares, G. (2024, August 3). *Leading from Two Perspectives: The Dynamic Roles of a CEO vs. Board Member*. Retrieved from Purpose: https://www.purposelegal.io/leading-from-two-perspectives-the-dynamic-roles-of-a-ceo-vs-board-member/

Nieles, M., Dempsey, K., & Yan Pilli, V. (2017). An Introduction to Information Security. *Computer Security, NIST Special Publication 800-12 Revision 1*, 101.

Seagate. (2025, February 1). *What is a 3-2-1 Backup Strategy?* Retrieved from Seagate: https://www.seagate.com/blog/what-is-a-3-2-1-backup-strategy/