Security Essentials Plan

By Andrew Waddell

12 February 2023

NTS 201 Security Essentials

INFOSEC

When it comes to the aspect of security, what does one imagine? Perhaps a tall fence with razor wire sitting atop, surrounding a specific building. Much like one would see of a prison or a military base. Or does one imagine something more simplistic? Such as a simple safe where they can keep valued items like jewelry, passports, and even firearms. What about a complex system that incorporates both types perhaps? Every description listed above could be considered a type of physical security. However, could cybersecurity mimic many of the same aspects as those mentioned only digitally? Instead of a tall fence that surrounds a building it could be a digital set of ones and zeros that creates a complex firewall system for a network of computers. Successful security has to be a multilayer operation like that of a prison or, more specifically, a military base or even The Pentagon or CIA HQ.

For example, to even access a military base, a person has to have a specific type of ID Card that has been created and validated by the federal government granting them access to a federal installation. Even after access is granted to the general area of the base, like the Base Exchange, Commissary, and even the gym or barracks, there are still more layers of security that requires additional restricted area badges that only select personal can have access to depending on their Military Occupational Specialty, or Air Force Specialty for those in the Air Force and Space Force. However, that is only one type of a multilayer security operation of a military base. So, let us call those special IDs Common Access Cards (CAC), being that is a name for military IDs. On top of the CAC access, military installations have intrusion detection in many different forms that fall under the entire security policy of keeping the base safe and secure. But how do we incorporate these into the digital realm or even into the private sector such as a data center?

Well, first off there has to be a limited amount of access. Imagine, if you will, we have a data center for and organization. Let us give them the name of “The Conglomerate.” They have a new data center, we will call it, “Site X-Ray.” The Conglomerate has asked a new company, us, called “Badger Security,” to implement a Information Security, INFOSEC, Plan. They have informed us that no expense will be spared for Site X-Ray. So far, as mentioned above, we have already started with a way to limited physical access to the data center. The less people that have access to the information stored there, the more secure that specific data will be. Let us say, for ease of creation, that the security stored there is of the Top Secret Classification. This data site is a third-party site for the Defense Department. So, obviously, with it holding highly classified data that can potentially compromise national security, we definitely need to limit the authorized users who have access to the site physically. This type of authorization will fall under the umbrella of a security policy that has overarching branches.

Branch one will consist of the Common Access Card access, for physically entering the site, to a limited access roster, we will call it a “Controlled Access Roaster.” This list will be authenticated by the highest levels of The Conglomerate and DoD to allow a select number of people physical access to the site. Since there will almost always be a need for a physical presence at the center there will be a need to limit access to those who truly need to be there. The easiest way to implement this first security policy will be to surround the entire complex with two layers of fencing, coupled with outward facing razor wire. The fence style will mimic the same style as one would see in specific secured locations on a military installation or prison. From there, we will have an access gate that will allow access to the complex. The gate will be a four-lane gate, two for personal and two for contracting, like building maintenance, construction, etc.

The DoD and third-party corporations/contractors will not want to suddenly have their building come crashing down due to lack of maintenance. To add onto that, server maintenance will be of high importance since this site will be used to house Top Secret data. Once inside the complex there will be two-way traffic to and from the parking lot. The outbound gate lane will controlled by barriers and limited to one way with everyone being subject to search at any time leaving the complex. Random searches will be conducted daily. Those that are there for contracting, construction, shipment deliveries, etc. will follow the well created signs to the shipping/receiving area under escort by the security personal. The gate guard security shack will be anything other than a ramshackle shack. It will be an octagonal shape with multiple armed security personal. It will be a control center for access. Foot traffic will also be controlled by a one-way spinning gate that requires a person to badge in to “unlock” the spin gate. Those that choose to drive will also have to badge in to open the gate under the supervision of the security personal. If the gate becomes unfunctional, security personal will have digital scanners that they will use to scan in and scan out personal.

Moving on from the “Main Gate,” area, the parking lot will also be fenced off for staff parking with a single point of ingress/egress that can be blocked off by security personal in the event of a physical or digital breach. Entry will be controlled with a specific restricted area badge that will be number coded as well as digitally encoded with the areas that that specific person has access too. This will be controlled by the “Master Controlled Access Roaster.” The reception area will control the foot traffic in and out of all areas beyond. All personal will surrender all electronic devices before proceeding beyond into the offices, server room, etc. No personal flash media or anything of the sort will be connected to any of the terminals inside the complex.

Employees will need to utilize their restricted area badges and a personal PIN to access the office space beyond reception. This area will be a Secured Compartmentalized Information Facility, or SCIF. Once inside, employees will be free to move about the hallways, break areas, restrooms, etc. The server room will be another SCIF within the SCIF. Only authorized users will have access to this room. Those users, being specific security personal, network technicians, etc. Network techs will be responsible for maintaining the integrity of the data, as well as the network itself. A select number of servers will be needed for redundancy as well as backup. In the event of a catastrophic network failure, all data will be downloaded to specific flash media and kept under lock and key by a select few network techs with armed security. This data will not be permitted to leave the complex unless under the express authorization of the DoD and CEO of The Conglomerate. This will be done through use of DoD couriers authorized to handle classified information. Maintenance will be done by the way of contractors, whom will be escorted by armed security personal. At no point will security not have eyes on unauthorized users. Shipping/receiving areas will be under the same scrutiny.

The security office, located inside the actual data center, will house no less than four armed security personal at any given time. This office will be a secured and locked location with a mini reception area for employees to be able to talk to the security personal in the event of an issue. This office will also be the command-and-control center for all the security concerns for this complex. There will be high-definition cameras located throughout the complex, mimicking the style that one would be in high end casinos in Las Vegas, also known as the “Eye in The Sky.” Obviously, there will be no cameras located in the restrooms as that is a violation of privacy. However, cameras will be located by the entrances, and the walls will be reenforced to prevent any attempts to access the server rooms. So, branch one is complete with CAC and Restricted Area Badge (RAB) access, controlled by a Master Controlled Access Roaster that is authenticated by upper management of the DoD and The Conglomerate. This is coupled with the physical presence of armed security personal, and command-and-control area, physical barriers, and traffic flow control through a single point entry system.

Since the DoD is a vast and huge entity spanning all over the world, access to this new data site will also have to be through the realm of cyberspace. However, we do not want just any employee to have digital access to this data center, just like we do not want any person off the street to be able to waltz right up to the front door of the data center. Here is where we bring in branch number two with specific security policies. This branch will incorporate virtual user access. This type of access will be limited, much like physical access. The users who will be authorized to access the information stored in the data center will have to use special computers attached to a specific inter agency network completely isolated from the regular internet. These users will need to request access through a security management team, and must use specific computers which reside in secured rooms much like vaults, called a Secured Compartmentalized Information Facility, that they will need special access to by way of Restricted Area Badge access. These users will have to fill out various forms to allow them access to both the needed computers and SCIFs. All user access will be reevaluated biannually, and users will need to maintain cyber awareness training every year to continue to have limited access to the terminals needed to access the data. Any information that is needed in paper format will be extremely controlled and not be permitted to leave the SCIF unless under direct authorization from the highest levels of management and the DoD.

All information will be subject to the rules and regulations governing classified material per DoD instructions and local military guidance. These specific policies help compartmentalize the information and create a loyalty and need to know basis for access to the information. With these policies in place, this will limit access to the information as well as keep a very in depth, authenticated, record of members who have the clearance level and need to know basis for access.

However, because we live in a digital world, there will always be a threat to cyber-attacks, to include insider threats. While an isolated inter agency network can help mitigate outside threats, it is not completely invulnerable. Thus, we bring in branch number three. Anti-virus software and tools along with firewalls. These two should be used in conjunction with each other. This suite of software and tools will help keep digital machines clean of malicious software and give another layer of security to breaches by threat actors. The implementation of these tools will also incorporate intrusion detection. Because, nothing digital is completely secure when it connected to a network, there has to be a way to detect intrusions and lock those computers down. The hardest thing to detect, in something this complex, is the insider threat. The insider threat has the easier capability to sabotage or access information to nefarious purposes. All employees will be subject to background checks at the highest level, mental health evaluations, even credit checks and polygraphs. All foreign travel, foreign contacts must be disclosed to security management within 72 hours before or after. Users will not be permitted to discuss their daily job duties outside of Site X-Ray, discuss in-depth of Site X-Ray, or anything relating to it. Because we can never fully vet those that would become an insider threat, we can mitigate it as much as possible with these steps.

Security is something the DoD takes very seriously. As you can see there are multiple layers of security that are needed to keep things out of the hands of the wrong people, whether it is a lone wolf actor or a peer to peer threat. Limiting access is the first big step of keeping things secure. There does not need to be thousands of personal coming and going to a data center that houses highly classified information, or even proprietary intellectual property. There for common access cards are the simplest, and most cost effective, way to limit access. Couple with a Master Controlled Access Roaster and physical security with armed guards with gates and fences. Access can be limited and controlled. On top of physical, digital access is just as important. So implementing secured access through SCIFs and specific terminals keeps things in specific locations where only authorized users have access to. These are the types of security measures that one can see every day in the DoD and are commonly used in the private sector as well.

References

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage.

*Department of Defense Manual - Dodig*. (n.d.). Retrieved February 12, 2023, from https://www.dodig.mil/Portals/48/Documents/Policy/520001\_vol3.pdf