Denise Ng
Eric Nguyen
Dr. Deepti Singh
IS 360

GAP Analysis

An information security professional's major responsibility is to manage or carry out an information security gap analysis to identify potential security risks and vulnerabilities and to use the information to put into practice solutions to close the gaps. The objective is to continuously advance security, get closer to the desired security position, and shift security from its present state to its enhanced future state. When performing a useful gap analysis, several crucial elements in the process must always be taken into consideration. Defining the scope of the area to be evaluated, identifying the areas for improvement, setting goals, determining the present state, and developing a plan of action or measures to attain the desired future state should all be included in the process for every gap analysis.

The first step is to define the scope and choose a security standard or benchmark. This keeps the inquiry's focus sharp, offers clarity to keep everyone in line and on the course, and ultimately encourages a successful gap analysis study. Benchmarking is necessary so that the organization can make better-informed decisions. Once more, the company, the resources available, and the goals will all influence how you approach this. Additionally, conducting a gap analysis against a certain security standard is necessary to get or maintain certification. Industry standards or security frameworks can be used to compare an organization's current security program to industry security best practices. Selecting a security standard to work with, if you do not already utilize one, maybe a crucial stage in the procedure. Other benchmarking methods, however, can involve examining the activities that other firms have performed or using industry best practices. A common practice is to consider the expertise and experience of peers operating in the same field.

You will need to look at current organizational structures, organizational processes, application and data inventories, personnel interviews, and security policies, controls, and procedures. The following should be taken into consideration: inventories of hardware and software, data classifications, access restrictions, system maintenance records, program settings, and backup methods.

Security risks frequently include humans, namely human mistakes. Investigation and proper addressing of user behavior are required. Therefore, doing staff interviews is essential. You must comprehend their expertise and capability for securely adhering to the established procedures. There must be evidence for this. In this case, security control is a process rather than a technological one.

A review of already-existing documents is required. To determine the organization's risk profile with the greatest degree of accuracy, all this examination is required.
The objective is to better understand how the current security program operates through inquiry and data collection. This offers you a clear picture of the environment, the protection that is in place, and the efficiency of the security that is in place. The gaps, flaws, and vulnerabilities can be identified by contrasting the current controls with best practice controls or those suggested by the chosen standard. Additionally, any missing security measures can be found, as well as any that are insufficient.

In the company FullSoft, we must first decide what area is under consideration with this gap analysis. In this case, we are analyzing the security threats and other threats that leave the company inoperable. Next, we must decide what categories we want to improve on. We have decided to split into a natural disaster that could disable our servers and must be recovered to become functional again. We have broken it down into three natural disasters fire, earthquake, and flood. Fire is preventable while earthquakes and a flood would not. In these case we want to have a measurable goal so when can identify how we can help and the resources to do so. The fire we would like to be able to stop small fires ourselves and be able to delay long enough

so by the time the fire department arrives it will not be too late. Earthquake and a flood that could not out the power and damage the server we must have an off-site location to immediately bring back the system up again. In this case, we would like to be back up within hours.

We look at cyber security threats and the common ones we would like to focus on are specifically ransomware attacks. Denial of Service attacks, generally network security, and training of new employees. The goals we want to achieve in this gap analysis are to reduce downtime and minimize damage. The new employees should be very unlikely to affect and be able to test properly before doing anything that could affect the company.

Now that we have identified what we want to improve and the goals we would like to achieve. We must then decide on the Key Performance Indicator. These help how is the best way to determine if our goals are met and where we currently are at the moment. Currently with the company when it comes to fire. We currently have standard water sprinklers, fire alarms, and smoke detectors. In turns of recovery in the event of a flood or earthquake. We currently have a cold site which means by hand we must move all the current equipment from our current location onto the other. Which could take days to weeks. For the security threats, we have ransomware attacks we do have a cloud base back-up but could take hours to download all the information back again. DDOS attacks we only have firewalls to hopefully mitigate unwanted traffic. For updating out-of-date firmware on our devices we have IT that update it once a year or the device is no longer supported. Lastly, we do have a senior employee that oversees and double-checks the work of the juniors.

Now that have our goals, what metric we want to improve on, and where we are currently at. We can now start to develop a plan to achieve the desired goal. First-out disasters can be improved by implementing fire suppression. This is can be achieved by using carbon dioxide gas instead of water to put out fires without damaging the servers. The next step is to replace all materials that could catch on fire like insulation with fire-resistant materials. If we cannot we can at least cover it matter that will not catch on fire. For our cold side, we can make

a hybrid where it had just the bare minimum to keep the service running for a couple of days so we can have a more permanent solution. This way the customers will still be able to access their data in the event of an emergency. In the event of a ransomware attack, we need to automate an alarm system and immediate backup of the data so that the company remains completely operational. Also, careful logging of how it occurred to it does not happen again. Possibly have a test environment to check if USBs have been infected with malware. For DDOS attacks we can use third-party services like Cloud flare to be able to help deter or prevent having only one system handle an unreal amount of requests. Lastly, we can improve the security concern of new employees by of course more training. As well as have a test environment and software so that can train in a safe manner that doesn't affect the company. We can as well create a system so that multiple seniors must check the work first before it can be pushed to production code.

GAP Analysis

Area Under Consideration:	The security of the platform and customer data	
Desired	Current	Action steps
Disasters 1. Fire - Time for the fire department to arrive20 - 40 mins 2. Earthquake - Time it takes for off-site 3. servers to be operations 1 hour 4. Flood - Time to get off-site server operational 1-hour Cyber Security Threats 5. A ransomware attack - Reduce downtime and minimize damage caused 6. DDOS Attacks - reduce or prevent the time the product is down. 7. Network Security - reduce the time of updates that contain fixes to a known vulnerability. 8. New employees- limit the time production is down	1. Currently have sprinklers, smoke detectors, and fire alarms 2. Have employees who have to physically move servers to off-site locations 3. Same as above 4. Have a back-up and restore back-up before operational again. 5. No prevention for DDOS attack 6. IT staff update devices on a routine basis. 7. We have them work on a testing environment first before pushing it into production code	1.1 Have fire suppression 1.2Replace flammable material with fire-resistant Material 2.1 Have a fully operational off-site location in case one goes down. 3.1 Have a hot site on an off-site location 4.1 Have an automated way to restore and recover compromised data. 5.1 Use a 3rd party service like Cloud flare to prevent DDOS attacks. 6.1 Have documentation of all devices used and the updated software in ogre of the threat level. 7.1 Have it checked by multiple senior employees before pushing it to production 7.2 More training to spot possible scams or social engineering.