THE IMPORTANCE OF IMPACT ANALYSIS AND PLANNING RISK MITIGATION

Question 2 | Jason Rivers | CYSE 495

The Importance of Risk Mitigation

The importance of risk mitigation to every aspect of business cannot be understated. Even outside of the realm of cybersecurity, mitigating risk is something every business must be conscious about, and actively planning around. There is risk associated with every action anyone possibly takes, and those risks increase exponentially when running a business. For example, let's say you, as an executive of a company, decided to buy laptops for all employees who were able to work from home.

The risk associated with that action would be the cost of the laptops versus just having them work in office, plus the risk that one of those laptops should be broken, compromised, stolen, etc. and the risk associated with letting employees work from home, which opens up a new set of risks associated with efficiency, and of course security of their connection to the business network. This example is exactly why we need to put an emphasis on structured analysis, planning, and foreseeing every possible risk associated to our assets and actions, so we can properly mitigate them, or at the very least realize the risks posed to out decisions before we make them. The first step in risk mitigation is to conduct a Business Impact Analysis (BIA) to determine what risks are currently posed to an organization, and potential recovery strategies.

Business Analysis Impact

A BIA involves systematically determining risks associated with an organization. This can include regular business-related risks, financial, cyber-security, or IT related, and many other aspects. It puts an emphasis on risks that may affect critical aspects of an organization, such as

databases, e-commerce sites, financials, or vulnerabilities in a network or security apparatus. Initially in a BIA, something like an audit is conducted to analyze different aspects of an organization to identify any potential vulnerabilities or threats associated with these different aspects of it. After vulnerabilities and threats have been identified, a BIA will begin developing preemptive measures, or reactionary recovery plans to mitigate the risk posed by these threats. These recovery plans are usually tailored to each specific threat but can be compiled together to develop a sufficient incident recovery response, or disaster recovery plan which I will go in depth on later (Kirvan & Sliwa, 2022).

To before a BIA, first you need prior approval from organizational leadership, and people trained, or at least experienced enough to perform a BIA, as well as people able to plan one out; you'll basically be performing an audit of your organization. From here, you would start analyzing policies, procedures, assets, employee, and their training, as well as sending out questionnaires and interviewing members within the organization, followed by evaluating the findings of each. Highlighting critical assets and identifying threats to them is key for a BIA, as the largest impact on an organization will come from the most critical assets it uses. At this step, the creation of initial recovery effort plans begins, which will be continued, and implemented in the next part of the risk mitigation process (Kirvan & Sliwa, 2022). After this, the findings are recorded, organized, and presented to management within the organization so the ball can get rolling for the next step, which is the development of a Business Continuity Plan (BCP).

Business Continuity Plan

A BCP is a planned, organized document laying out critical assets, information, and operations needed for a business to continue operating at basic functionality. It outlines the most important assets needed for the business to continue operating, and further outlines how those essential functions need to be maintained, both in a usual everyday capacity and in the event of an emergency. These important assets can include people, locations, intellectual property (IP), assets, networks, databases, or processes needed for the business operations to continue. The main benefit of a BCP is to mitigate risk associated with catastrophic events, like natural disasters, full-enterprise ransomware attacks, total database crashes, etc. Just like a BIA, it begins with analyzing and essentially auditing the enterprise in question. Normally if you perform a BIA before a BCP, you can utilize a lot of the same information between the documents.

The first step is to analyze important assets, functions, and people within an organization. Sorting through all the processes and assets within an organization, and determining which ones are key to operational functionality, and which ones are not can be a time-consuming process, but as I stated before, you can utilize information from a prior BIA for the BCP analysis step, and several steps after this, such as the risk assessment (Brunskill, 2022).

As the name suggests, a risk assessment is when you take a closer look at your business essential assets, and the risks associated with each. For example, for an essential location such as a manufacturing plant, some risks to it may include natural disasters, supply chain issues, machines breaking down, manpower needed to conduct the manufacturing process and operate

machinery, and other similar assets needed to keep it running, albeit at reduced capacity. After analyzing and identifying risks associated with essential assets, a BCP will include a recovery plan for each potential risk, either to mitigate the associated risk partially or completely, allowing an asset to continue functioning at a reduced capacity (Brunskill, 2022).

Organizing a recovery plan is probably the most important aspect of a BCP. This could include establishing redundancies within an organization, establishing a work-from-home plan in case an office is inaccessible, off-site databases featuring routine backups from the main server, and organizing members of a workforce into a recovery team ahead of time, with pre-planned actions rehearsed so they're ready in the event of an emergency (Brunskill, 2022).

Communicating ahead of time who oversees what, pre-establishing lines of communication, and chains of command are key to pre-planning recovery. If a recovery plan must be altered or entirely abandoned in the middle of a crisis, pre-planned lines of communication, or pre-arranged chain of command can mitigate the chaos this can create. Pre-planning, training employees ahead of time, rehearsing certain recovery plans, and keeping physical copies of a BCP on hand are the final essential step to a BCP (Brunskill, 2022). A BCP is very closely aligned with a Disaster Recovery Plan (DRP), where an enterprise is concerned with recovery efforts rather than sustaining their essential operations. Making sure an enterprise can continue to conduct business, and outlining how it can recovery assets essential to its operational efficiency, are different, but have the same goal in mind: protecting the enterprise from disasters, man-made or otherwise.

Disaster Recovery Plan

As I stated before a DRP is very closely related to a BCP, but they differ significantly in their main functions, primarily where a BCP's main function is to outline business operations continuing in some capacity, a DRP outlines how to recovery primarily IT, and database related assets or restart operations that are important to the business, regaining operational efficiency, and smoothing the transition from sustaining operability to recovering totally operational capacity. The process of developing a DRP is also very similar to a BCP, but the steps are usually in a different order. For starters, a DRP is normally initiated by outlining a Disaster Recovery Team (DRT), comprised of members within an enterprise (and occasionally outside of it) who oversees not only conducting disaster recovery efforts in the event of one, but also formulating, outlining, and ensuring the viability of recovery efforts. One common recovery, or risk mitigation effort is utilizing backups and safe, off-site backup databases (Berke et al., 2014).

Once a DRT has been comprised, and informed of their individual duties, they begin assessing the risk posed by various disasters to different aspects of their enterprise. Just like with the BIA and BCP, information collected from those can be utilized here if it is available for use, same as with the next step involving identifying critical assets, information, and locations. Assets that are critical to operations are prioritized, followed by important yet non-critical assets, which are categorized by importance. The more important the asset, the higher up on the priority list is. Higher propriety assets are also more likely to have redundancies, or backups, such as central databases, financial systems, IP assets, and the like. Finally, just like with a BCP, practice runs,

rehearsals, and table-top simulations of disasters are run to make sure that the team has at least some experience and knowledge of their roles and what to do prior to an actual disaster occurring. Now that we've established more serious disaster risk mitigation plans, let's look at risk mitigation planning revolving around non-catastrophic, or at least pre-catastrophic situations (Berke et al., 2014).

Computer Incident Response Team Plan

A Computer Incident Response Team Plan (CIRTP), or more commonly known as simply an Incident Response Plan (IRP) is a document outlining how a cybersecurity, IT team, or information assurance team plans to handle a variety of situations. When an incident begins, or a problem arises, an Incident Response Team (IRT) is formed to begin investigating, first starting with identifying the issue, checking logs, and diagnosing what the issue could be. Containing and minimizing the issue at this stage is key to mitigate the risk of it blowing up and becoming a full-blown disaster. At the same time, evidence is collected either from logs, corrupted filed, surveillance tapes, and many other forms of evidence gathering, up to and including forensics post-incident (Ruefle et al. 2014).

After the incident has been contained, classified, and the evidence collected, the IRT will begin recovery efforts. This could include bringing back up systems that have gone down, accessing, and utilizing backups or redundant systems, clearing a device or database of corrupted, or suspicious files, and overall trying to get systems back to working order as they were pre-incident. Finally, a follow-up is conducted to make sure the incident was logged

properly and communicated clearly to organizational leadership. The cause will be discussed, and remedies to the issue that led to it will be introduced, whether it be policy changes, technical adjustments, or someone being fired. The incident is, all evidence, and any remedial efforts are logged, and in most cases stored so that in case any future issues arise related to the incident, they have a record of everything that happened during it (Ruefle et al. 2014).

Incident Response is a very important step below Disaster Recovery, and often it can prevent an incident from becoming a situation where Disaster Recovery is required. It minimizes the risk early enough that while damage will be done, it will be contained enough to where the entire organization isn't crippled by it. Just like with Disaster Recovery however, a wide array of pre-planned response plans, and trained individuals must be ready ahead of time for such incidents. Seeing as how Incident Response is more common than Disaster Recovery, or Business Continuity, Incident Response team members will normally have more hands-on experience from dealing with actual incidents. Raw experience in dealing with incidents, coupled with a well-trained, organized team with a pre-planned response can ensure not only that the incident is discovered, contained, and resolved before it becomes a big issue, but it also ensures that damage and risk posed to an organization is minimized as much as possible.

Conclusions

Risk mitigation planning within an organization must include situations ranging from a simple port or IP malfunction to a full-blown DoS, ransomware attack, or otherwise on an organization. Planning around an incident happening before it ever occurs can mitigate much of

the risk from it and reduces the damage it can cause by applying not only preventative and deterrent measures, but reactionary responses as well. Recognizing who oversees what, what members of an organization have the most experience, and making sure they know their duty, and how to do it will reduce the chaos an incident or disaster can cause, possibly saving an organization despite being put into such a precarious situation. It's a well-known fact that no organization can eliminate risk, or the chance of disaster striking them in whatever form. The key to being resilient and mitigating risk is not to focus on eliminating risk, but to mitigate it while making sure you're prepared to respond if any potential risks or threats ever come to fruition.

References:

Berke, P., Cooper, J., Aminto, M., Grabich, S., & Horney, J. (2014). Adaptive Planning for Disaster Recovery and Resiliency: An Evaluation of 87 Local Recovery Plans in Eight States. *Journal of the American Planning Association*, *80*(4), 310–323. https://doi.org/10.1080/01944363.2014.976585

Brunskill, V.-L. (2022, May 19). *What is a business continuity plan (BCP)?*. Disaster Recovery. https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity-action-plan

Kirvan, P., & Sliwa, C. (2022, May 23). *What is a business impact analysis (BIA)? definition from whatis.com*. Storage. https://www.techtarget.com/searchstorage/definition/business-impact-analysis

Ruefle R., Dorofee A., Mundie D., Householder A. D., Murray M. and Perl S. J., (2014, October 22) "Computer Security Incident Response Team Development and Evolution," in *IEEE Security & Privacy*, vol. 12, no. 5, pp. 16-26, Sept.-Oct. 2014, doi: 10.1109/MSP.2014.89