2020

Creating an Incident Response Plan

Brayden Scott
Grand Valley State University

Brayden Scott

Professor Kalafut

CS

April 24, 2020

Creating an Incident Response Plan

In any organization, it is important to be prepared in the event of a major incident that might impact and impede critical operations. The best practice that an organization can take to ensure that such an incident may be handled well is to develop a plan in preparation for such an event. In order to aid my organization in preparing for adverse incidents, I have worked to create an incident response plan based on our organization. This plan is developed to cater to our manufacturing organization with 4 major locations and an IT team of about a dozen individuals. By having an incident response plan developed, we can be more effective at managing any incidents that might occur.

My organization is Adrian Steel company, which has its headquarters in Adrian, Michigan. We are a manufacturing organization which fabricates shelving, drawers and accessories that can be installed in utility vehicles. Our customers include Internet Service Providers, Electricians, Delivery Companies, etc. Our largest customers will have fleets of over 100 vehicles, and we also have a number of customers who distribute our product for retail purposes to smaller companies local to their area, such as plumbers, and local ISPs.

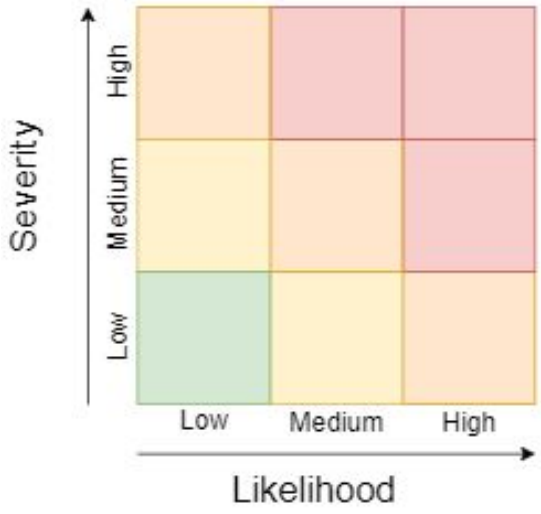
The first step I took in creating the response plan was to meet with the director of IT at my organization. I outlined with him what an Incident Response Plan consists of, including each of the phases involved with the plan. Although he approved of the project, he was not familiar with incident response plans. One concern that he had brought up was the question of determining whether a plan was working or not, for our organization we would like to know if we are "winning" or "losing". If we have an incident response plan in place, we would like to be able to demonstrate that when an incident occurs, the plan is helping us to win. To do this, we would want to identify what metrics we are using to measure this.

A second bit of feedback that he offered was that he was not sure that it would be more valuable to create a plan for incident response as opposed to strengthening our current defenses. Wouldn't the best Incident Response Plan be to bring the number of incidents that occur down to zero? I clarified that that goal is in the same spirit of the preparation phase of an incident response plan, however, the importance of having a plan is to partially recognize that while we want to minimize the possibility of an incident, there is no way to remove the risk of an incident occurring, which is why the other phases are valuable. Following up on this, he felt that in addition to having the phases to the plan laid out, then, it would also be valuable to our organization to look at the plan in terms of the OSI model. We would like to be able to assess the risks that are present at each of those layers, if that would work with the plan.

Using this framework was helpful in categorizing the incidents that I included in the plan and gave an outline for the preparation and detection phases. Another point that I began to emphasize was how the seven phases align with the Plan-Do-Check-Act method. I categorized Preparation, Detection, and Analysis as phases in the planning step, and Containment,

Eradication, and Recovery under the Do Step, and the Lessons Learned phase equates to the Check Act, and also ends in the Act phase which reevaluates the "Preparation" phase. Because the PDCA methodology is already embraced by our organization, this helped me to demonstrate further how an Incident Response Plan aligns with our organization.

The best tool that I incorporated into our plan was a set of checklists for the do phases. For our company, we wanted to have a thorough method of verifying that everything that we needed to have done was completed during the containment, eradication, and recovery phases for our responses to specific attacks that we needed to include in the plan. These are effective in giving step-by-step instruction to our team members, and allow our team leader to quickly see where we are at on the way towards recovery. In order to determine these, we took a number of incidents, and used a Hazard-Risk Matrix (below) to identify what incidents were most important to include.



I also included “winning” and “losing” metrics in the Incident Response Plan. While where available, we can evaluate our handling of incidents to past experiences and determine whether we were better at responding more quickly and effectively in terms of business impact, we don’t always have previous experiences with some incidents or documentation to allow us to compare effectively. In the absence of more measurable goals, we would rely on feedback from our incident response team with regards to how they felt the plan supported their effectiveness in responding to the incident. We added a questionnaire to our Lessons Learned phase of the plan that includes suggestions from each of the team members about what they would add to the plan to support future response team members in their same role.

The major difficulty that I faced during this project was that this was a project of my own initiative, rather than being a project initiated by my company. Because of this, while I could prioritize my project, others would not be able to. Essentially, creating the incident response plan competed with other projects for time and resources within my organization. For the first part of the year, our entire company was very busy, we were expecting a major increase in sales, and so all departments were needed to both facilitate the new orders, and to also ensure that we maintained customer satisfaction for our continuing business as well. Because of this, even I had to prioritize other projects over my own, and used weekends to make the most progress.

The onset of the Covid-19 pandemic also impeded my ability to complete the project. Our company is within the automotive industry, and once the Big Three began to stop manufacturing due to the pandemic, we were not able to meet our expected sales. Since there were no new vehicles being produced, our customers had to cancel their purchases. As a result of this, our department became very busy with supporting the sudden change of direction. The

priority for us was to enable employees who needed to work remotely to do so and to enable our helpdesk to keep supporting them. Covid-19 has also prevented our department from engaging in a roundtable excercise for the plan, but I am hoping that in the coming months, we will be able to get more feedback from it.

Covid-19 also gave us opportunity to look at our organizations needs, and what our capabilities are. We were able to get input from the department heads about which employees are critical, and what functions are critical for them. This gave us great insight into how we would want to prioritize for any incident that forces us into supporting our operations when users cannot be on site.

Currently, the Incident Response plan is focused on our IT department, and we will try using it internally. I look forward to being able to use the plan, and to especially encounter situations that allow us to improve the plan. I also think that it will be valuable to encounter new incidents, so that we can make the plan more specialized overall. Once we are able to better demonstrate the plan's value for our organization as a whole, I am hoping that we will be able to get more input from other departments to improve our plan and to get buy offs from all our organization's leaders.