Kristopher Adams

Chris A Noffke

Intro to Cyber Security

7 April 2025

Respond to Cybersecurity Disruptions

Responding to any type of incident within cyber security is extremely time sensitive. Especially when under high-pressure, we want to ensure that the situation does not worsen. If there is no plan in place for handling these situations, it may progress further and cause confusion. When an organization responds to a cyber security incident, they must have a plan in place to avoid confusion that will only worsen the situation. During an active disruption, an immediate response with critical thinking is needed so a smooth recovery can happen.

If an entry-level cyber security professional takes a wrong action to stop a security incident due to poor planning, this could cause larger confusion within the organization. This confusion could end up spiraling into situations like data-loss, or extended downtime. To avoid situations like this, the organization should implement a BCP to ensure the critical business functions can run without disruption, especially during a disruption. Another recommendation for the organization is to have a DRP in place to ensure that the infrastructure, for normal business operations, is able to be restored. To avoid confusion the DRP should be extremely detailed on exactly how to recover the infrastructure. After implementation, the plans must stay up to date to ensure there is no confusion caused due to out of date documentation. This can be done by reviewing the BCP, and DRP regularly. Once a review procedure is in place the last recommendation is to train employees on how to plan and test a BCP and DRP. This can be good for the employees to ensure they are trained properly and understand how the plans will work when a disruption occurs.

When a disruption occurs within an organization, critical thinking and ethics can both help choose the best course of action. Critical thinking can help you isolate the disruption faster. Instead of thinking ethically about what the consequences would be if you accessed the data, you find the disturbance faster.Ethics can help an organization find longer term solutions to problems that may cause a disturbance. So instead of fixing the disturbance quickly with the possibility of it happening again, you find a solution to ensure it does not happen again. Although preventing the disturbance from happening is more important than critical thinking. The ethics stage can be completed after the disturbance is resolved. If any poor judgement is given, it could escalate a disaster. Therefore, Critical thinking is more important when it comes to real-time disturbance recovery.

Organizations should always have a DRP and a BCP in place that is constantly kept up to date. If a organization experiences a disturbance they can easily recover from it and get back up and running. When resolving the issue, critical thinking is much more important to the situation than ethical thinking. The speed of the recovery is always put to the highest priority. An organizations preparedness is required to be successful when any disturbances happen.

Works Cited

Learning, Jones & Barlett. “Lesson 10.” *Lesson 10. Lecture 1.Pptx*,

uwplt.instructure.com/courses/739957/files/89573470?module\_item\_id=26890839 . Accessed 6 Apr. 2025.