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 After implementation, the plans must stay up to date to ensure there is no confusion caused due to out of date documentation.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.

**III. Critical Thinking vs. Ethics During a Disaster**

**A. The Role of Critical Thinking**

* Definition: Assessing the situation logically, analyzing available information, choosing the best course of action.
* Example: Prioritizing system isolation to contain ransomware instead of debating ethical data access questions.

**B. The Role of Ethics**

* Ethics ensures responsible behavior (e.g., honesty, data protection, legal compliance).
* Can guide long-term decisions, but may not always be immediately actionable in a crisis.

**C. Which Is More Important – And Why**

* **Argument**: Critical thinking takes precedence in real-time disaster response; ethics are foundational but not always practical in the heat of the moment.
* Reasoning: A wrong action due to poor judgment can escalate a disaster, while ethical decisions without situational awareness may delay necessary action.

**IV. Conclusion**

* Reiterate the need for structured incident response processes to guide less experienced cybersecurity personnel.
* Emphasize that **critical thinking is the key skill** during an active incident, supported by ethical frameworks after immediate danger is resolved.
* Final thought: Preparedness, training, and sound judgment are the pillars of effective cybersecurity crisis management.