**. Introduction**

* **Brief overview** of the importance of effective incident response in cybersecurity.
* **Contextualize** how high-pressure situations (e.g., ransomware attacks, natural disasters) can lead to confusion without clear guidance.
* **Thesis Statement**: When responding to cybersecurity incidents, organizations must establish clear protocols to avoid improper responses from entry-level professionals, and in active disaster scenarios, critical thinking is more vital than ethics due to the need for immediate, logical decision-making.

**II. Addressing the Missteps of Entry-Level Cybersecurity Staff**

**A. The Consequences of Poor Process Guidance**

* Example: Entry-level employee taking incorrect action (e.g., pulling the plug on a system, deleting files, ignoring protocol).
* Resulting issues: Escalation of attack, data loss, reputation damage.

**B. Recommendations to the Organization**

* Develop and document clear, step-by-step **Incident Response Plans (IRPs)**.
* Conduct **regular training and simulation exercises** for all staff, especially new hires.
* Appoint mentors or assign experienced staff as **incident response coaches** for junior personnel.
* Emphasize a **communication hierarchy** to prevent impulsive actions.

**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.