# 2-1 Journal

Joshua Merren

Southern New Hampshire University

CYB 320: Incident Response and Investigation

Professor Noah Nicholls

6 November 2024

In today's digital world, where cybersecurity threats are rampant, having an Incident Response Plan (IRP) is crucial for all organizations. An IRP is a set of detailed instructions that help IT teams effectively handle cybersecurity incidents. Its primary aim is to minimize the damage such incidents cause to an organization's operations and reputation. This plan is crucial as it safeguards sensitive information, reduces recovery costs from cyber incidents, and minimizes the damage caused by security breaches. With a well-defined IRP, an organization could avoid prolonged downtime and significant financial losses while also risking the loss of trust among customers and partners (Cassetto & Cassetto, 2024).

An IRP should include critical steps such as preparation, detection, containment, eradication, recovery, and post-incident analysis. Preparation, the first and perhaps most crucial step, involves understanding the organization’s most critical assets and setting up a cybersecurity team with clearly defined roles. Following this, the team must be capable of quickly detecting any anomalies and containing them to prevent further spread. Eradicating the threat involves removing the source of the breach and repairing any vulnerabilities. The recovery process must aim to bring systems back online safely and efficiently, while the final step, post-incident analysis, involves learning from the incident to strengthen future responses. It would help to clearly document and regularly update these steps to adapt to evolving cyber threats. (Cassetto & Cassetto, 2024).

Several factors can improve the effectiveness of an IRP, such as regularly updating and testing the plan. A plan not practiced through drills or real scenarios can become ineffective, leading to inadequate handling of incidents. Additionally, a lack of support from senior management can result in insufficient funding and resources being allocated to cybersecurity efforts, undermining the IRP's effectiveness. To ensure success, an IRP must be comprehensive, detailed, and supported by all levels of the organization, from executives to technical staff. Companies must also stay informed about advancements in cybersecurity, such as integrating Security Orchestration, Automation, and Response (SOAR) tools, which can significantly enhance their ability to respond to incidents swiftly and effectively (Cassetto & Cassetto, 2024).

# References

Cassetto, O., & Cassetto, O. (2024, September 4). *Incident Response Plan 101: The 6 phases, templates, and examples*. Exabeam. https://www.exabeam.com/blog/incident-response/incident-response-plan-101-the-6-phases-templates-and-examples/