Incident Response Plan

Levi Overstreet

University of Advancing Technology: NTS405

Incident Response Plan

An incident response plan for cyber security is a set of instructions to help IT staff detect, respond to, and recover from network security incidents. These types of plans address issues like cybercrime, data loss, and service outages that threaten daily work. I will give a look into my thoughts on how an incident response plan should be set up to handle general security events.

The Company

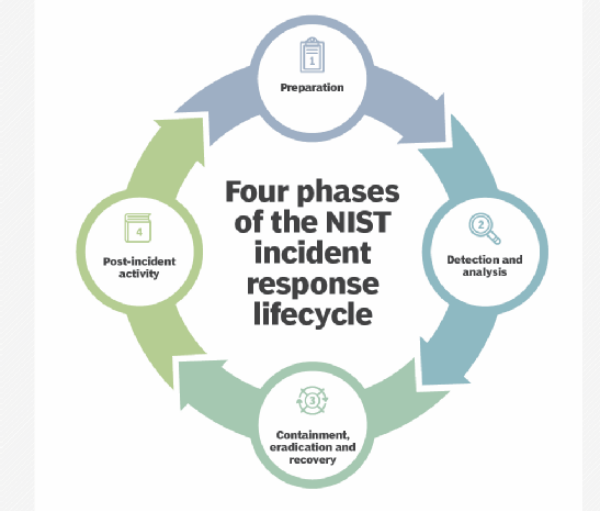
My company is a reginal online data processing company called Local Bytes. It has around 130 employees making it a medium sized enterprise. As a data processing company, it handles the extraction of relevant information from many sources and processes it into an easily comprehendible and convenient manner to be accessed as a digital format for its respective clients. It handles several high-profile contracts such as a contract for the local government, one for a billing processer, and another for a medical provider. With high-profile clients, this makes Local Bytes a target for data breaches and ransomware attacks.

The Scenario

In this scenario, I show what I believe to be a typical series of events for most companies that collect and or store vast amounts of sensitive data. According to Risk Based Security, based on a 2020 end of year report on data breaches, an overall decline in breach events (security incidents) was observed but the number of breached records grew dramatically (Lohrmann, 2021). There were 3,932 publicly reported breach events, a 48% decline compared to 2019. Despite 1,923 breaches (49%) without a confirmed number of records exposed, the total number of records compromised in 2020 exceeded 37 billion, a 141% increase compared to 2019 and by far the most records exposed in a single year. This also leads into the other arm of my scenario, ransomware. In 2020, there was an increase in ransom attacks, these kinds of attacks were up

150% over the previous year, and the amounts paid by the victims of these attacks had increased more than 300% in the same year (Sharton, 2021). According to Hiscox, Ltd., 43% of the more than 6,000 companies it surveyed had suffered a cyberattack in 2020, up 38% in the 12 months before, and one in six of those attacks was a ransom attack. In 2020, the amount of ransom demanded grew to the mid to high seven-figure ranges. At the end of 2020 and into 2021, they have seen some ransom demands reaching into the tens of millions of dollars. With these kinds of attacks either being on the rise or appearing to be the norm, I will be showing how my incident response plan handles such an event.

The Plan



The purpose of an incident response plan is for overall preparation and responding to physical and electronic information security incidents. Guidelines for response plans can be found on the NIST website, where documents such as 800-61 outline industry best practices. (Michigan.gov) Preparing an SOP outlining the plan is critical to a company's operation because it defines the roles and responsibilities of the response team and stakeholders, the definition of an incident, procedures, and reporting requirements. Outlined below are high-level documentation of a response plan and a few of the key terms defined.

Event: Any exception to the standard operating procedure, not all events are incidents.

Incident: An event that violates the agency's policies as it relates to physical or IT security. The management or Risk Management team defines the categories these incidents fall within and their risk to the organization. The risk is on a scale of 0-5, 0 low risks, and 5 Extreme risk.

Samples of incidents include:

- Malware/viruses/trojans
- Phishing
- Ransomware
- Data breaches

Responding Authorities: The responding authorities' contact information is included in the plan by jurisdiction. For example, local authorities, such as police response, may respond to lower threats, whereas the FBI or CIA will respond to all Extreme risk incidents.

Evidence Preservation: All evidence gathered in response to the incident must be preserved by following state and federal regulations. Evidence preservation is necessary to analyze the risk and identify any potentially compromised sectors of the system, isolate and repair those sectors and create an operating plan moving forward to mitigate future breaches.

Staffing: Organizations must have the staffing necessary to monitor and address threats. These teams including a monitoring team (internal or third-party), cyber incident response team, and management (decision managers)

Tenants of the plan:

Monitoring and Detection: A team is staffed 24/7 to monitor the networks for anomalies and respond to alerts triggered by the notification system. This team is trained to collect and analyze data for events, trends, and patterns of behavior. (Michigan) In an attack, the monitoring team

will continue to data gathering and report details to the decision-maker. The decision-maker will make the final "Declaration of Incident."

The Response

Following the "Declaration of Incident," the response is transitioned to the Cyber Incident Response Team; the monitoring team will remain engaged by watching the networks and gathering all additional data for the Cyberteam.

The Cyber team will perform an initial risk assessment as previously defined by the SOP and risk management team. The risk assessment identifies the data breach in more detail, including its threat level and immediate response tasks. Once the risk is assigned a threat level, actions are taken to contain the attack and close off the appropriate systems, such as the location of the data breach and any connected networks. The goal is to isolate the breach and quickly assess any other vulnerabilities to be addressed. These initial response steps are part of the active security process.

Gravity of cyber incident	Corresponding level from U.S. Cyber Incident Severity Schema	Impact assessment	Is the incident an "armed attack" under the UN Charter's Article 51?
Level 5: *Situation of Extreme Emergency*	Level 5: *Emergency*	Extreme Impact	Possible; to be assessed on a case-by-case basis
Level 4: *Major Crisis*	Level 4: *Severe*	Major Impact	Unlikely, but actions corresponding to these levels could nonetheless constitute unlawful acts under international law (intervention, infringement on sovereignty, inappropriate use of force, and so forth.)
Level 3: *Crisis*	Level 3: *High*	Strong and Broad Impact	
Level 2: *Serious Incident*	Level 2: *Medium*	Strong and Narrow Impact	
Level 1B: *Incident*	Level 1: *Low*	Medium and Narrow Impact	
Level 1A: *Event*		Low Impact	
Level 0: *Minor Event*	Level 0: *Baseline*	Negligible Impact	

Sample Cyberthreat matrix (Toucas, 2018)

Once contained, the team will move forward with breaking the breach down into critical components vulnerability that led to the incident, response lessons learned, and possible adjustments required for the operating plan or incident response plan. Not all threats are the same; thus, a different decision may not all be standard; these are lessons the team can learn from to improve processes in the future.

A plan is only as good as the team that can work together to execute it. Ultimately, the thing that makes an incident response plan work is the people who are tasked with working on each part. Having proper training and the resources to do their jobs is key. If an organization can back up a security team with proper training and the resources, then any plan will be more likely to succeed.

References

Chapple, M. (2019). 5 critical steps to creating an effective incident response plan. TechTarget. Retrieved on https://searchsecurity.techtarget.com/feature/5-critical-steps-to-creating-an-effective-incident-response-plan

Lohrmann, D. (2021). 2020 Data Breaches Point to Cybersecurity Trends for 2021. Retrieved from https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-data-breaches-point-to-cybersecurity-trends-for-2021.html

Michigan.gov. Example incident response plan. Michigan.gov. Retrieved from https://www.michigan.gov/documents/msp/Example_Incident_Response_Policy_666657_7.pdf

Sharton, B.R. (2021). Ransomware Attacks Are Spiking. Is Your Company Prepared? Retrieved from https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared

Toucas, B. (2018). With its new 'White Book', France looks to become a World-Class player in Cyber Space. Ware on the Rocks. Retrieved from https://warontherocks.com/2018/03/with-its-new-white-book-france-looks-to-become-a-world-class-player-in-cyber-space/