Cyber Security Incident Response

This paper will define a cyber security incident response (IR) methodology that both resolves the cyber security incident as well as provides many different stakeholders with the information regarding the incident that they need. By providing the incident details (facts), the methodology helps cyber security incident responders get up-to-speed and engaged quickly. The many third- parties who benefit from both receiving the incident information and participating in the IR process include cloud service providers, incident response firms, legal professionals, communications professionals, crisis communication stakeholders etc. The growth in cloud computing usage necessitates active participation of the 3rd parties in the incident response process for each enterprise.

I implemented the following approach at seven large industry-leading enterprises over the last few decades. Following published standards for IR is a solid and appropriate practice for cyber security professionals. This approach is additive to existing standards.

Facts:

- Facts should be in bullet point format using concise language (fewer words is better)
- Ideally, they should be in chronological order in how they were discovered
- They may include references to specific log files but not all the detailed information from the log file is necessary to include
- Using a different colored font is one technique for adding facts to the incident summary as they are identified
- You may also want to use version numbers in the document to track changes

Business Impact:

- This should include current impact stakeholders (customers, employees, board members, etc.) and the potential stakeholders in the future that may be impacted
- One customer impacted currently but there could be hundreds of customers impacted soon

Root Cause:

- The root cause of the incident may or may not be confirmed early in the incident response work effort
- If the root cause is not known yet, identify a hypothesis for what it is
- The goal is to either prove or disprove the hypothesis with more facts
- “A privileged user’s user ID and password was harvested by a threat actor”
- An SMS one time passcode was intercepted by a threat actor bypassing the second authentication factor

Corrective Actions:

1. These are tasks that are part of the recovery/containment process defined in simple terms

2. Each one should identify an owner (a person or team) that is accountable for conducting the work effort and sharing results
3. Each task should identify a target completion time (1 hour, 4 hours, 8 hours, 1 day, 3 days, 1 week, etc.)
4. The log file analysis for the specific APIs are being analyzed by the SOC analysts and results are expected within 8 hours

Lessons Learned:

- There is no need to wait until after the incident to capture lessons learned
- IR standards call for a review process after the incident has been resolved often referred to as a post-mortem review- I choose to identify lessons learned as we learn them as part of the IR process so that an enterprise can apply the lessons learned as quickly as possible
- Identifying lessons learned immediately (during an IR) represents a behavior supporting cyber resilience at enterprise scale
- Never use lessons learned to place blame on individuals or functions- the key is for all IR participants to focus on opportunities to improve
- "The call center voice recognition and authentication process for customers was fooled by an LLM generated synthetic voice prompt so we need to add a filtering capability to identify synthetic voice signatures going forward."

Background:

This format is more than a reporting format. The goal of this approach to cyber incident response is to capture information essential to the many stakeholders of the incident as soon as possible while focused on the critical path of recovery and minimizing the business impact. There are many stakeholders for cyber incidents including but not limited to:

1. Cyber security staff
2. IT staff
3. Employees
4. Customers
5. Legal staff
6. Privacy staff
7. Executive leadership
8. Board members
9. Internal Auditors
10. External Auditors
11. Regulators
12. Potential customers

One of the benefits to this approach is to make the incident process more efficient for those engaged with the process. I can't tell you how many thousands of times I joined a conference call for an IT incident where a few participants shared critical information in the first few minutes of the call. As others joined the call, they would announce themselves and then wait for someone to describe the facts which never came. As a result, they would often try to contribute to the resolution or corrective actions only to discover they were missing a key piece of information that was discussed before they joined the call. The only time that the facts were shared in summary form on calls was when the CIO joined (a rare occurrence) and the facts were summarized for his/her benefit.

Starting with the core facts when someone joins the call helps everyone both understand and the current situation and contribute to the recovery process. One technique is to share a screen with the facts identified in bullet form that each participant can read when they join the video conference. Productivity improves and collaborative work effort improves.

It is very common not to have all the information in a cyber incident as the incident response process is initiated. Using this approach ensures that the information that is known at that point in time is captured along with what is not known and needs to be known. The latter provides a clear indication of what information is necessary to fully understand both recovery and remediation scope. Cyber incident response requires collaboration across organizational boundaries within an enterprise and external to the enterprise. This approach enables facilitation of the essential information while sharing it with both incident responders and the key stakeholders.

This approach represents a set of behaviors that are core to cyber resilience. That includes the recognition that every enterprise (large and small) has cyber incidents and IT outages. Practicing the right incident response behaviors is a positive step toward cyber resilience. As an example, it is bad practice to assign blame to an organization or individual during a cyber security incident. Capturing facts is essential. Therefore, it is imperative to practice the cyber security incident response process and enable contributors to practice the behaviors that make it more effective. This includes practicing with third party vendors/suppliers that provide services core to IT infrastructure or part of the incident response capabilities (incident responders, legal professionals, crisis communication service providers, etc.).

The proliferation of cloud infrastructure service providers along with ERP cloud SaaS and PaaS providers supporting enterprises today means that practicing incident scenarios with these partners offers a rich set of opportunities for improvement based on the learning from the practice incidents. In other words, practice synthetic incidents with third parties and you will be surprised at some of the assumptions made by third parties that fail to understand the customer's expectations in an incident. The Cloud Security Alliance (CSA) published an incident response framework in May of 2021 that offers a starting point for understanding incident response from a cloud service provider's perspective. It includes a few scenarios for simulation testing. https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework

I prepared this information knowing that there are a few clear differences with conventional practices for cyber security incident response. One difference is the incorporation of lessons learned into the core process rather than doing a "post-mortem" analysis after the fact. Recreating incident context after the incident was resolved and closed is cumbersome and often avoided by top technical talent that focus on the current set of problems not on participating in post-mortem exercises. Another difference is the use of an incident facilitator [lead] that pulls the facts and other relevant information out of the participants in the incident response process. This is often someone in the SOC but frankly can be anyone who understands meeting facilitation techniques. The facilitator controls who share information in the incident call/meeting and ensures the five step process is applied to the session. The third difference is to separate remediation work effort beyond 90 days from the actual incident report. If a corrective action or the application of a lesson learned will take over 90 days to implement, then the tracking for that activity should be transferred from the incident report to another reporting/governance process/tool. This allows incidents to be closed once the information is completed. The last difference is the use of version control or different colored fonts on incident reports to add a temporal dimension to the incident response documentation. Most of the major cyber incidents I led took weeks and sometimes months to complete.

I encourage you to apply this approach to cyber incident response and then make it better through incremental improvement. I welcome feedback and especially ways you improve the approach.