Chapter 13: Introduction to Incident Management and Response

13.1 Background on Incident Management and Response

This section discusses, in detail, concepts related to incident management and incident response as they apply at cyber defense competitions.

13.1.1 Types of Potential Incidents

When dealing with cyber threats, it can be challenging to know where to begin. A good place to start is to identify what type of threat is present. The Commonwealth of Massachusetts and the U.S. DHS's CISA provide descriptions of various different types of cyber threats [84, 85]. As noted by the Commonwealth of Massachusetts, common threat vectors include [84]:

- Malware
- Phishing
- Denial of Service
- Ransomware

In addition to the type of threat, the source of the threat should be noted. The U.S. DHS's CISA outlines multiple potential sources for cyber threats including [85]:

- Foreign Intelligence Services
- Independent Hackers
- Insiders
- Terrorists

Any of the types of attacks can be carried out by any of the potential sources.

Malware is described as malicious code or software. The individuals responsible for creating malware typically aim to compromise the overall security of the target system. Malware can range from very obviously present on a machine to extremely covert. Complex malware have the ability to steal data, compromise systems, and even take down power grids.

Phishing is a relatively new form of attack which takes advantage of email as an attack vector. Phishing attacks can be generic or targeted. An example of a generic phishing scheme is the Nigerian Prince. In this scheme, the unsuspecting user receives an email from a prince claiming to have millions in assets which they will send you if you wire them a small sum of money to be released from prison (or something similar). These schemes, while unsavory, do not necessarily have the ability to cause significant damage. Targeted phishing attacks on the other hand take advantage of information about the target which help convince the target that the sender is legitimate. These emails may appear to come from a trusted sender and typically request that you either click on a link or download a file. The unsuspecting target is unaware that the link may route them to a website which will attempt to solicit confidential information under the guise of a legitimate source such as the target's bank, or download a file which executes malicious code upon being opened.

Denial of Service (DoS) attacks perform exactly what they sound like; they attack a target such that the target is no longer accessible. In the case of a web page, DoS attacks may spam the page with so much traffic that valid users can no longer access the page. DoS attacks are a significant inconvenience to the target and require attention, which then allow malicious attackers to commit other acts such as intrusions or fraud while the response teams are distracted by the DoS attack.

Ransomware is another relatively new type of attack. Typically, the malicious actor uses malware to encrypt the targets assets or file system. The malicious actor then requires a sum of money to decrypt the assets.

13.1.2 Dealing with Insider Threats

Insider threats are those which occur internal to an organization. Three common archetypes for insider threats, according to a Sirius Edge article, are Mistake-Makers, Malicious Insiders, and Imposters [77]. Mistake makers are described as individuals within the organization who fall for phishing schemes or otherwise become an a means of access to data. This individual is not necessarily involved in the malicious act, but rather, their carelessness makes them a vulnerability. Imposters are described as malicious actors who use legitimate credentials (typically stolen) for employees of an organization to access data legitimately. The malicious insider is a current or previous employee or other related figure to the organization, such as a contractor, who exploit the fact that they have authorized access to data [77].

Insider threats are challenging to defend against, especially in the case of the malicious insider, because the behavior is normal. An authorized individual is accessing data which they access every day. Although the technical behavior is not anomalous, there are certain measures which an organization can take to help combat against insider threats.

In an article from Sage Data Security, author Becky Metivier provides four tips for detecting insider threats [76].

1. **Be Aware**: An organization needs to know where their most sensitive data is located and monitor access to that data. This means that the organization may need to perform an assessment of the data, determine what is valuable, and keep record of the location of that data. Which individuals access the data, when they access the data, and how they access the data should all be recorded.

2. **Change Things Up**: An organization needs to be modular. Criteria such as the location of data, authorized individuals and stewards of the data, and monitoring of the data should be regularly rotated. Keeping the system under constant change means that a single individual or team never has extended access to the data, which can make it easy for them to regularly exfiltrate small amounts of data so as to go under the radar.

3. **Know Indicators of Compromise**: There are many indicators of compromise which can lead to the discovery of an insider threat. One of the way that insider threats are carried out is to exfiltrate data. This can be detected by monitoring data transfer. An insider may transfer anomalous amount of data, whether it downloaded onto an external drive, sent across email, or uploaded to a file sharing service or cloud service. Monitor access logs, checking if individuals have been accessing assets anomalously (outside of normal hours, special access areas without authorization), if terminated employees are accessing organization systems, or if an individual who has been transferred internally is accessing

previously authorized assets.

4. **Implement Security Technologies**: Knowing the indicators of compromise is only valuable if there are measures in place to protect against the threat. Regularly updating employee accesses will help to prevent against a terminated or transferred employee from having residual access to previous assets. For critical assets, ensure the data is encrypted, this will keep it from being useful if exfiltrated.

If suspicion rises that an organization may have an insider threat, formal investigative work will need to be done. Accusing an employee of being a potential insider can not come lightly. Documentation, logs, evidence are key; if approaching a potential insider, leading with evidence will help support any claims made [76].

13.1.3 Responding to Cyber Incidents

Incidence response is not a new topic, nor is it poorly documented; various organizations have explicit response plan steps. An article from AlienVault lists the steps that NIST and SANS use for incident response [62]. Both have very similar models, including the following steps:

1. Prepare for an Incident
2. Identify and Analyze an Incident
3. Contain the Incident
4. Eradicate the Incident
5. Recover from the Incident
6. Perform an Analysis Post Incident

Exabeam lists best practices for incident response plans [72]. The best practices include using automation, leveraging playbooks, and testing the incident response plan [72]. In a time where there is so much data, it can be difficult to perform effective data analysis to detect anomalous activity which may be an incident. Using automation can help cut out some of the noise, making it easier to identify the anomalous events.

Hacking groups, nation state actors, and other malicious actors tend to follow similar patterns on low profile attacks. Playbooks can be used to prepare a response to incidents which perform a series of steps on a prospective malicious incident.

As with any plan, an incident response plan needs to be tested to determine its efficacy. Carry out a mock incident and determine how the incident response plan fared against the mock incident.

A proper incident response plan will help ensure that an organization is prepared for incidents and can swiftly minimize the impact. Other sources for incident response plans include the U.S. Department of Homeland Security's National Cyber Incident Response Plan [59] and NIST's Computer Security Incident Handling Guide (SP 800-61 rev.2) [60].

13.1.4 Documenting Cyber Incidents

As with anything else in life, documentation is critical. Having detailed and accurate cyber incident documentation will help the response team to perform their role swiftly and effectively. There are many quality resources which walk through cyber incident reporting and documentation.

One suggestion, from a Turn Key Technologies article, is to build up a tiered reporting process [70]. Author Tony Pugielli explains that having separate reporting procedures for different groups within an organization can lead to confusion regarding which procedure to follow and may slow the documentation process [70]. By using a comprehensive documenting procedure which applies to all groups within the organization, response teams can quickly document any necessary information, following the universal documentation process.

Having a cyber incident documentation template can help ensure that all appropriate information is recorded. Any necessary evidence from the incident can also be collected. In the event that the incident requires legal dispute, having proper documentation is crucial, according to a Digital Guardian article [71]. A template will help ensure that critical information, such as the time the incident was detected or the systems impacted, are noted. The template could be based on an organization wide policy for incident documentation which ensures that sufficient information is record to be presented in a legal court [71].

In a Computer Weekly article, author Dinesh Bareja provides a list of best practices for security incident management [73]. Bareja suggests having a policy and procedure in place to ensure that as information becomes available, it is documented in a specific way, including specific details. It is also suggested there are clearly defined roles for individuals in the incident documenting procedure. Bareja notes that carrying out regular training with sample incidents can help ensure that an organization's employees stay sharp on the skills and allow management to assess if any employees need clarity on their role in the reporting process [73].

Having clear and defined information which should be collected and a template will ensure that employees do not leave out necessary information or include unnecessary information. An organization can develop its own incident report template or adopt pre existing templates. Two existing templates for incident reporting are the U.S. Department of Homeland Security's FEMA form ICS 201 [58] and the U.S. Department of Homeland Security's US-CERT Incident Reporting System [61].

13.1.5 Briefing Appropriate Audiences on Cyber Incidents

Organization suffer from cyber incidents, it is inevitable. However, how an organization documents the incident, responds to the incident, and briefs the appropriate audiences will determine the long term impact of the incident on the organization. Audiences can range from a small group within an organization to the public; regardless of the size of audience, an appropriate briefing of the event is necessary. Consider the following suggestions when preparing a briefing.

In a document from the Massachusetts Institute of Technology titled *Guidelines for Effective Briefings*, it is suggested that the presenter determine the medium for the briefing [82]. Consider the audience for whom the briefing is being prepared. Common mediums for briefings include spoken, email, and pre-recorded video. Another tip is to follow an organized script of topics.

A suggested order for topics is to begin with background and context of the incident, follow up with an appropriate amount of detail regarding the organizations response, and finish with a conclusion of the current state of the incident and what the organization has done to prevent a similar incident in the future [82].

In a Chron article, author Jackie Lohrey stresses the importance of an effective Q&A period. After an incident, the audience will surely have questions. Lohrey notes that the distinguishing factor of a successful briefing is an effective question and answer session. There may be some common questions which can be anticipated, such as the source of the incident, affected systems, what it means for clients, etc. The organization should prepare well thought out answers to these common questions. For the more challenging or random questions, an organization should ensure that the individual giving the briefing is able to articulate well, possesses strong stage presence, and speaks with assurance [83]; even if the question cannot be answered directly, these qualities will speak to the audience.