**Incident Response**

 Jose Flores

CSOL-590-02-SU23: Cyber Incident

Professor Thomas Plunkett

May 15, 2023

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Phases/ Task | Technical Team | Coordination Team | Leadership Team | Legal Team |
| **Description** | The Technical Team consists of the IT department, forensic investigator, penetration testing, and other IT-related supportive roles. | The Coordination Team is responsible for communicating between the technical team and leadership. They are in charge of organizing, preparing, reviewing, and documenting plans developed by the technical team so they may focus on the incident. They are the liaison between the technical team and the impacted department/environment/program leadership. | The Leadership team makes decisions in the organization's best interest. They will brief the C suite with actions that are taken place or will take place. | During the incident, the Legal Team handles any legal terms and regulations related to customers, employees, stakeholders, and affected parties (Chai & Lewis, 2023). This includes disclosing information to the public to maintain a positive organizational reputation. They work closely with the financial and administrative teams. |
| **Preparation** |  |  |  |  |
| Assessments  (NIST, 2012) | Conducting penetration testing and vulnerability assessments on the systems/networks. | Preparing an asset and software list on each system. Organizing the assessments conducted by the technical team to present to the leadership team. | The leadership team assigns duties and responsibilities to the technical team members. Some team members may be given for forensics analysis, penetration testing, containment, information gathering, and other specific duties. | The legal team reviews the documents the leadership approves to ensure they comply with local, state, and federal laws. They also do their due diligence on laws and regulations such as HIPPA, GDPR, and PCI DSS. |
| Awareness and Training | The technical team will train and teach others to identify malicious activity such as phishing, tailgating, and shoulder surfing. | The coordinator team will set up meetings and time with other departments to execute the training. | The leadership team will meet with the C suite and emphasis the importance of conducting training to reduce the possibility of incidents. | The legal team would maintain documentation of employees that have complete training to have accountability. |
| **Identification** |  |  |  |  |
| Impact Level (NIST, 2012) | The technical team would design a risk assessment on which incidents are the low impact to highest impact. Example: Controlled Unclassified Information (CUI) is less risky than Top Secret information being leaked. | The coordination team will organize the risk assessment by color coding it to make it presentable to the C suite. They will add or change any information as updated by the technical team. | The leadership will present the risk assessment with the impact levels to the C suite. They will explain to the C suite the levels of impact the organization will suffer if they were a victim of specific incidents. | The legal team will work with the financial section to calculate each incident's estimated cost so the C-suite can understand the potential loss. |
| Involvement | The technical team will identify the source the incident occurred from. They will determine if it was an insider threat, external, faulty equipment, natural disaster, or other sources. | The coordinator team would ask the 5 Ws and organize it into a report. | The leadership team would present the report to the C suite and provide the next course of action to contain the incident. | The legal team would reach out to impacted parties and maintain an open line of communication with them. If another organization is involved, they will communicate with their legal team to set up meetings about legal actions. |
| **Containment** |  |  |  |  |
| Evidence Preservation  (NIST, 2012) | The technical team would filter and segregate the source of the incident. | The coordinator team would communicate with the technical team to create a network diagram of where the source is coming from. This would provide a visual aid to the leadership to brief the C suite. | The leadership would brief the C-suite on where the incident source started and the following actions used to contain it. | The legal team would create a brief to let the impacted parties know what is being done to prevent further damage. |
| Securing the System | The technical team would take the system offline to further the damage. If the incident is caused by a human factor, they would remove their credentials off every access list and systems. | The coordinator team would communicate with the point of contact to the respected environment and update them on what needs to be done. If a human factor caused the incident, the coordinator team would contact human resources and other departments the individual had access too. They would initiate getting the backups ready to be installed on a separate system to reduce downtime. | The leadership team would update the C suite on the actions to contain the short- and long-term incident. | The legal team would update the impacted parties on what data have been exposed and what actions are being taken to contain the incident. |
| **Eradication** |  |  |  |  |
| Anti Virus/ Malware Check | The technical team would conduct an in-depth virus and anti-malware scan throughout the network with two different types of software. | The coordinator team would communicate with the environmental leadership to set a date and time the technical team would conduct their anti-virus and malware scan. They would let the leadership team know when the actions will occur and the results. | The leadership team would update the C-suite on actions being taken to eliminate the threat. | The legal team would maintain the logs and reports generated by the anti-virus and malware scans. |
| Third Party Check | The technical team would work with the third party to find and eliminate the cause of the problem. | The coordinator team would contact third-party companies to coordinate when they are available. | The leadership team would get approval from the C suite to have a third party come into the organization and help eliminate the threat. | The legal team would contact the third-party legal team, set up a liability contract, and initiate a brief background and clearance check. |
| **Recovery** |  |  |  |  |
| Restoring | The technical team would restore the system to the initial setup and configuration. They would verify that proper security setups are in place and update any necessary patches/software. They would also harden the system by removing necessary drivers, programs, and using two-factor authentication. | The coordinator team would let the department leadership know what additional security steps would be implemented to ensure the systems are well protected. | The leadership team would debrief the C suite that the systems are being hardened and restored to the best-known good configuration. | The legal team would draft a letter to the impacted parties informing them of the actions to restore the data. |
| Testing | The technical team would test the system to ensure the additional security practices work correctly. An example is checking that everyone uses a 2FA method to log in. | The coordinator team would keep track of what methods are working and which are not. They would compose a report on what security practices are effective and ineffective to give to the leadership team. | The leadership would debrief the C suite and the impacted parties on what best practices are working and which are not. T | The legal team would draft a contract to let the impacted parties know they understand the risk they are taking if they do not want to implement the additional security best practices. |
| **Lessons Learned** |  |  |  |  |
| Changes | The technical teams would revise the systems and make any changes needed to improve the security. They would brief with the department/environment to talk about cybersecurity best practices. | The coordinator team would revise/update any additional document the technical team recommends that would improve the department's security. | The leadership would meet with the impacted parties and the C suite to improve our security and ensure this does not happen again. | The legal team would close out any legal suits and disclose the final outcome to the media if necessary. |
| POA&M | The technical team would recommend actions/plans that should take place to avoid another security incident. | The coordinator team would draft the POA&M to present it to the department and change anything that needs to be changed. | The leadership team would brief the C-Suite on what the POA&M consists of and what important steps we have taken to avoid an incident again. | The legal team would develop a lesson-learned report to discuss with other organizations so we may help each other maintain a strong defense. |

References

Chai, W., & Lewis, S. (2023). *Incident Response Team*. TechTarget. https://www.techtarget.com/searchsecurity/definition/incident-response-team#:~:text=Responsibilities%20of%20an%20incident%20response,for%20all%20incident%20handling%20measures.

NIST. (2012). Computer Security Incident Handling Guide - NIST. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf