Incidence Response playbook: Data Theft

Phase 1: Initial Detection and Assessment

1. Upon detecting a potential data theft incident, the incident response team should be notified immediately through established communication channels, such as a dedicated incident response hotline or email.
2. The team should assess the nature and scope of the incident, including the type of data that may have been stolen, the potential impact, and the affected systems or applications.
3. The team should gather relevant information, such as timestamps, logs, and other forensic data, to support the investigation and response.

Phase 2: Containment and Mitigation

1. The incident response team should take immediate steps to contain the incident and prevent further data loss. This may involve isolating affected systems or networks, disabling user accounts, or implementing temporary security measures.
2. The team should change all relevant passwords, revoke access to compromised accounts or systems, and update security controls to prevent further unauthorized access.
3. Backups of affected systems or data should be checked for integrity and used to restore any lost data or systems, if available.
4. The team should work closely with internal IT and security teams, as well as external stakeholders, such as law enforcement or legal counsel, to ensure proper handling and mitigation of the incident.

Phase 3: Investigation and Analysis

1. The incident response team should conduct a thorough investigation to determine the cause and extent of the data theft incident. This may involve analyzing logs, examining network traffic, and reviewing system configurations.
2. The team should identify the entry point, the methods used by the attackers, and any indicators of compromise (IOCs) to understand the attack vector and the scope of the incident.
3. Forensic analysis should be conducted to collect evidence, preserve chain of custody, and document findings for potential legal or regulatory purposes.
4. The team should coordinate with internal or external resources, such as a digital forensics team or a threat intelligence provider, to gain additional expertise and insights.

Phase 4: Notification and Communication

1. The incident response team should communicate the details of the data theft incident to relevant stakeholders, including senior management, legal counsel, public relations, and affected parties, as required by law or company policy.

2. Communication should be timely, accurate, and coordinated to ensure a consistent message and to manage potential reputational, legal, or regulatory risks.
3. The team should prepare and distribute internal and external notifications, including data breach notifications, incident reports, or media statements, based on established procedures and legal requirements.

Phase 5: Recovery and Remediation

4. The incident response team should work with relevant teams to implement necessary controls, patches, or updates to prevent similar incidents in the future.
5. The team should conduct a comprehensive review of security controls, policies, and procedures to identify any gaps or weaknesses that may have contributed to the data theft incident.
6. Lessons learned from the incident should be documented and used to update the incident response playbook, as well as to improve security practices and awareness across the organization.
7. The team should conduct post-incident monitoring and follow-up to ensure that all security measures are effectively implemented, and the incident is fully resolved.

Phase 6: Post-Incident Analysis

5 After the incident is resolved, the incident response team should conduct a post-incident analysis to assess the effectiveness of the response efforts and identify any areas for improvement.

6 The team should review the timeline of events, actions taken, and outcomes to identify any deviations from the incident response playbook and to identify potential improvements.

7 The team should document the findings and recommendations for future incidents and share the analysis with relevant stakeholders for further action or awareness.

Please Note: The above incident response playbook is a general outline and should be customized to fit the specific needs and requirements of each organization. It should be reviewed and updated regularly to reflect changes in the threat landscape, technology, and business processes. Additionally, it's important to involve.

Second option

Per https://github.com/certsocietegenerale/IRM/blob/main/EN/IRM-11-InformationLeakage.pdf

1. Preparations: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: Remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process.

1 Preparations: Get Ready to Handle the Incident

1. Establish an incident response team with clear roles and responsibilities.
2. Develop and maintain an up-to-date inventory of critical data assets and their locations.
3. Implement proper access controls and monitoring mechanisms to detect unauthorized access or data exfiltration.
4. Establish communication protocols and contact information for key stakeholders, including senior management, legal, IT, and public relations.

2 Identification: Detect the Incident

1. Monitor for unusual activity and anomalies in system logs, network traffic, and user behavior.
2. Deploy security tools such as intrusion detection systems (IDS), security information and event management (SIEM) systems, and data loss prevention (DLP) solutions to detect potential data theft incidents.
3. Conduct regular security audits and vulnerability assessments to identify potential vulnerabilities that could be exploited for data theft.

3 Containment: Limit the Impact of the Incident

1. Isolate the affected systems or networks to prevent further data loss or compromise.
2. Change passwords and revoke access credentials of users or systems involved in the incident.
3. Collect and preserve evidence for legal and forensic analysis while maintaining chain of custody.
4. Implement temporary mitigations, such as disabling compromised accounts, blocking suspicious IP addresses, or applying patches to vulnerable systems.

4 Remediation: Remove the Threat

1. Conduct a thorough investigation to determine the scope and extent of the data theft incident.
2. Identify and address the root cause of the incident, including vulnerabilities or misconfigurations that were exploited.
3. Remove malware or other malicious elements from affected systems.

4. Apply necessary patches and updates to prevent future similar incidents.
5. Review and update security policies and procedures based on lessons learned from the incident.

5 Recovery: Recover to a Normal Stage

1. Restore data and systems from secure backups or trusted sources.
2. Verify the integrity and confidentiality of recovered data.
3. Conduct thorough testing and validation of restored systems to ensure they are functioning properly.
4. Gradually restore access to affected systems and networks in a controlled manner, following established procedures and approvals.

6 Lessons Learned: Draw Up and Improve the Process

1. Conduct a post-incident review to identify gaps and areas for improvement in the incident response process.
2. Document lessons learned and shared them with the incident response team, IT staff, and other relevant stakeholders.
3. Update incident response procedures, policies, and training based on the findings and recommendations from the post-incident review.
4. Conduct regular drills and simulations to practice and refine the incident response process.
5. Share best practices and lessons learned with the wider organization to raise awareness and improve overall security posture.

Please Note: The above playbook is a general guideline and should be customized to the specific needs and requirements of the organization. It's recommended to involve legal and compliance teams in the incident response process to ensure compliance with relevant laws and regulations.