Implementing a comprehensive Incident Response Plan is vital for any organization, especially when managing cybersecurity incidents within a supply chain. This plan provides a systematic approach to addressing and mitigating the impact of security breaches and cyberattacks. By ensuring that your organization is prepared to swiftly detect, respond to, and recover from incidents, the plan minimizes potential disruptions and reduces the risk of cascading effects throughout the supply chain.

A well-structured Incident Response Plan facilitates effective decision-making, ensures adherence to legal and regulatory requirements, and reinforces the organization's overall cybersecurity posture by identifying and addressing vulnerabilities not only within its own systems but across its entire supply chain network.

We are committed to maintaining the highest standards of security and operational resilience, and we are pleased to share an overview of our Incident Response Plan, specifically tailored to protect our supply chain operations, safeguard our stakeholders, and uphold our dedication to excellence and security.

Volvo Group Incident Response Plan

Step 1: Preparation – Establish and maintain incident response capability, including policies, tools, and training.

This step is the most important in the incident response process because being unprepared can lead to delayed or chaotic responses during incidents which may exacerbate damage and prolong recovery times.

Examples of Actions Taken:

- Develop an incident response policy
- Train security staff
- Ensure necessary tools and resources are available
- Develop a communication plan
- Establish methods for users to report potential or confirmed security incidents

Responsible Party: IT Management

Step 2: Identification – Detect and determine the nature of the incident.

The incident (external or internal) should be reported through predetermined channels so the appropriate actions can be performed. Timely and accurate information will allow for an effective response, minimizing damage, and preventing further impact.

Listed below are a few examples of the information that should be gathered during this step.

- What type of cyberattack is it?
- How was the attack discovered?

- Is it a personal data breach? Has any information been stolen?
- Is the email environment safe? Can we trust the supplier's contact to verify this?
- What supplier email domains are affected (e.g., @suppliername.com)?
- Are there any current or anticipated impacts on production?

Examples of Actions Taken:

- Monitor systems for unusual activity
- Investigate user reported anomalies
- Analyze alerts
- Confirm the incident

Responsible Party: Incident Response Team

Step 3: Containment – Limit the impact of the incident to prevent further damage.

Effective containment activities help protect critical assets and maintain operational integrity while the incident is addressed. This step typically includes short-term containment measures put in place to quickly manage the incident that will lead to long-term containment strategies to ensure that the issue is fully controlled.

Examples of Actions Taken:

- Isolate the affected systems
- Block affected domains
- Revoke account access
- Prevent the spread of the incident

Responsible Party: Security Operations Center

Step 4: Eradication – Eliminate the root cause of the incident.

This step focuses on identifying and removing the root cause of the security incident to ensure that the threat is fully eliminated. Depending on the scope and impact of the incident, it may be necessary to engage third-party security teams to help with the removal of the threat.

Examples of Actions Taken:

- Remove any malware
- Address vulnerabilities
- Clean affected systems
- Document all findings and remediation steps taken

Responsible Party: Security Operations Center

Step 5: Recovery - Restore and validate system functionality.

Proper recovery is crucial to prevent recurring or residual issues, maintain business continuity, and rebuilding stakeholder trust by demonstrating that security incidents can and will be addressed effectively.

Examples of Actions Taken:

- Restore systems from backups
- Validate system integrity
- Unblock domains
- Restore external account access
- Monitor for any signs of the incident reoccurring

Responsible Party: Security Operations Center

Step 6: Lessons Learned - Review the incident and improve future responses.

After all systems and services have been restored to normal operations, review and analyze the incident and response actions to identify successes and areas for improvement. This reflection will help shape and enhance future response efforts, prevent similar issues, and strengthen overall security practices.

Examples of Actions Taken:

- Conduct a post-incident review
- Document findings
- Update the incident response plan

Responsible Party: Incident Response Team

This incident response plan can be tailored to fit the specific needs of your organization. Steps can be combined or expanded based on your company's size, industry, and resources. For example, in smaller companies, the same individual might perform multiple roles, while larger organizations may have specialized teams for each step. Customizing the plan ensures that it's practical, effective, and aligns with the unique requirements and capabilities of your organization.