Incident Response Plan

Abramek, Inc. has a company-wide plan for responding to incidents, along with policies and procedures that explain how to protect and manage different kinds of data. If there's a cybersecurity or data security problem, these documents also outline the steps to take. The policies and procedures specify who is responsible for responding to incidents and how to communicate with important people involved.

February 4, 2024
Incident Response Plan Version 1.0.0

Goals of Incident Response

In the digital age, security incidents are a reality, but at Abramek, Inc., we're ready. Our commitment to safeguarding our systems, data, and people is the driving force behind our comprehensive security incident response plan.

1. Confidentiality: We protect the integrity and availability of systems, networks, and entrusted sensitive information.
2. Swift Recovery, Business as Usual: When incidents occur, we prioritize a quick and seamless recovery, minimizing disruptions to our operations.
3. Unified Against Threats: We stand strong against threats with a coordinated response, deploying effective measures to neutralize risks and safeguard our data.
4. Clear and Timely Communication: Key to our plan is prompt initial reporting of incidents and ongoing updates to keep stakeholders well-informed.
5. Navigating Legal Compliance: Committed to legality, we work with qualified professionals to address cyber-related legal issues effectively, minimizing potential liabilities.
6. Collaborative Response: Collaboration is at the core of our response. We leverage external Computer Incident Response Teams and law enforcement for efficient resolution.
7. Reputation is Priority: Throughout the response process, we prioritize protecting Abramek, Inc.'s reputation.

Purpose and Scope

This plan introduces a dedicated incident response team with clearly defined roles, responsibilities, and communication channels. It's not just limited to cyber incidents; this flexible approach also covers data breaches unrelated to computers, guaranteeing a smooth response for any situation.

Incident Response Team (IRT)

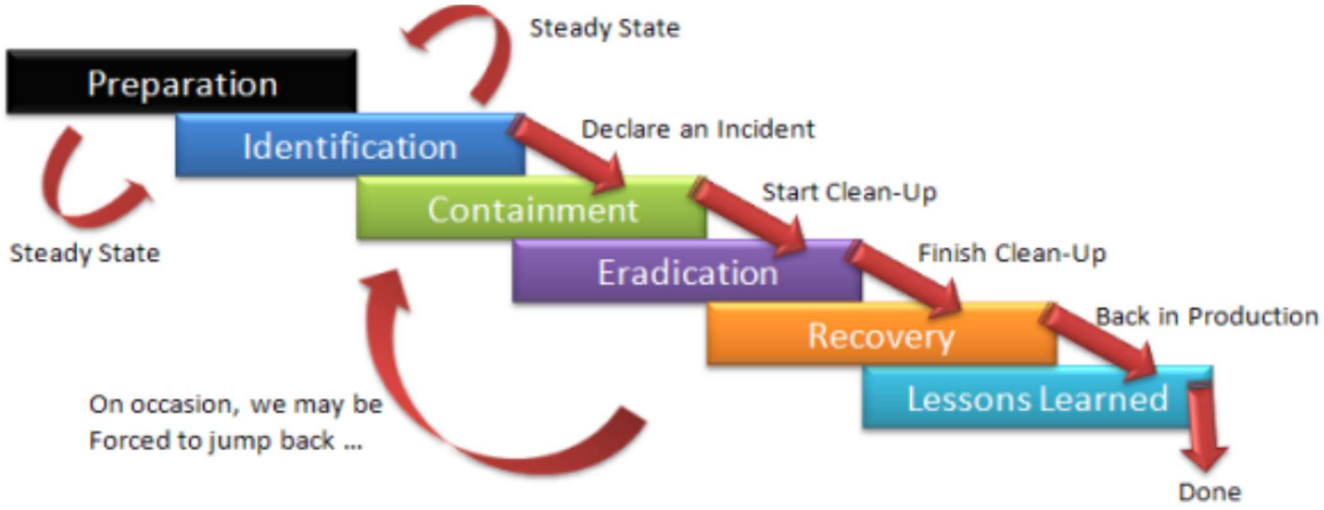
Abramek's Incident Response Team is prepared to handle any situation, with access to Subject Matter Experts (SMEs) for specialized guidance. An Incident Response Manager (IRM) coordinates our efforts, working closely with the Global Privacy Office when personal data is involved. Our plan includes clear steps for remediation and mitigation, addressing both internal and third-party data management.

Incident Response Life Cycle Process

Handling incidents is an ongoing cycle, like a continuous journey. The Incident Response Plan is made up of specific elements that guide us through this process, ensuring a well-rounded approach.

1. **Preparation:** Enhance response readiness continually by securing systems, training employees, and conducting simulations.
2. **Identification**: Swiftly confirm, categorize, and prioritize suspected incidents.
3. **Containment**: Minimize damage by stopping attackers and managing communication.
4. **Eradication**: Eliminate the threat and secure affected systems.
5. **Recovery**: Restore operations, repair damage, and communicate updates.
6. **Lessons Learned**: Learn from incidents and refine security measures and response plans.

Figure 1 source: www.playbooks.flexibleir.com



Communication Methods

During a major attack, if our regular communication channels are down, the Incident Response Team (IRT) switches to pre-determined backup methods on external systems listed in the IRT contact list. This ensures clear communication even when internal systems are compromised.

Incident Response Exercises

Every year, our Incident Response Team (IRT) conducts simulations, known as "tabletop exercises." These exercises simulate real incidents, helping everyone understand their roles and promoting smooth teamwork and communication. This way, we ensure a quick and coordinated response when an actual attack occurs.

Summary

This plan should serve as a guide for handling security attacks and data breaches. It covers identification, containment, eradication, and communication steps. We'll adjust these steps to fit different situations, ensuring an effective response.

Appendix A – Abramek, Inc. Incident Response Team (IRT)

*****NOTE ABOUT CONTACT INFORMATION*****

Contact information details of the IRT team are distributed to the teams separately due to confidentiality reasons.

Primary Team Members

1. Head of Information Technology – Brian Hegstad
    a. Detects and verifies security incidents
    b. Provides updates to the IRM team
    c. Coordinates computer forensic and technical remediation activities
    d. Implements corrective actions

2. Incident Response Manager (IRM) – Kevin Strong
    a. In charge of communications within the IRM team

3. Finance Manager – Martha Brown
    a. Assess financial impact and leaked financial data

4. Public Relations – Monica Costa
    b. News media management
    c. External and internal communication

5. Building Security Manager – Patric Corn
    a. Manges building access and control

Appendix B – COMMON INCIDENT DEFINITIONS

Incident Type	Type Description
Unauthorized Access	Unauthorized access occurs when someone gains unauthorized logical or physical entry to a company's network, system, application, data, or other resources.
Denial of Service (DoS, DDoS)	Exhausting resources, a successful attack impairs the normal authorized functionality of networks, systems, or applications.
Malicious Code	Infecting an operating system or application, successful installation of malicious software like a virus, worm, Trojan horse, or other code-based malicious entity occurs.
Improper or Inappropriate Usage	When a person violates acceptable computing policies, including unauthorized access or data theft.
Suspected PII Breach	Suspected access to Personally Identifiable Information (PII) defines the incident.
Suspected loss of Sensitive Information	Involving unauthorized access, malicious code, or improper use, an incident occurs with suspected loss of sensitive information, where the cause is unknown.

Appendix-C Incident Response Strategies

Incident Type	Incident Response
Unauthorized Access	Strengthen access controls, change passwords, conduct a security audit, and provide additional user training. Restore affected accounts from backups if necessary.
Denial of Service (DoS, DDoS)	Implement network rerouting, deploy DDoS mitigation tools, and work with the Internet Service Provider (ISP) to filter malicious traffic. Ensure redundancy and failover mechanisms are in place.
Malicious Code	Isolate infected systems, run antivirus scans, remove malicious code, and restore affected systems from clean backups. Educate users on safe online behavior.
Improper or Inappropriate Usage	Review and enforce acceptable use policies, conduct employee training, and monitor user activities. Implement access controls and take appropriate disciplinary actions.
Suspected PII Breach	Activate an incident response plan, conduct a thorough investigation to confirm the breach, notify affected individuals, and provide credit monitoring if necessary. Enhance security measures to prevent future breaches
Suspected loss of Sensitive Information	Isolate affected systems, conduct a forensic analysis, identify the extent of the loss, and notify relevant parties. Implement security improvements and update policies to prevent similar incidents in the future.

Appendix-E IRT Incident Record Form

Incident: _____

Discovery Date: _____

Recorded By: _____ Page _____ of _____ Pages

Recorded Information and Events

Date/Time	Detail

Document Version History

Version	Date	Changes/Notations
1.0	February 4, 2024	Initial release

References

Cyber and Data Security Incident Response Plan Template. (n.d.). https://cdn.fedweb.org/fed-34/2/Cyber-Security-Incident-Response-Template.pdf

Cybersecurity. Leidos. (n.d.). https://www.leidos.com/company/trust/cybersecurity

FlexibleIR. (2020, April 25). *Incident response : Phases & understanding them better*. - Get and contribute to Incident Response playbooks !! https://playbooks.flexibleir.com/incident-response-phases-best-practices/