Sample Cybersecurity Incident Response Template

EXIGENT

Creating a cybersecurity breach incident response plan is crucial for effectively managing and mitigating security incidents. While we can provide you with a basic template for guidance, you should tailor it to your specific organization's needs and consult with cybersecurity experts for the best results. Here are key elements to plan for and consider:

Define Incident Response Team

- Identify team members and their roles.
- Establish communication channels for the IRT.
- Create a protected and documented location for a physical copy of all elements of the incident response policy and plan.

Incident Classification

- Develop a classification system for incidents based on their severity.
- Clearly define what constitutes a security incident.

Incident Detection & Reporting

- Identify the methods for detecting security incidents (e.g., intrusion detection systems, log analysis).
- Establish reporting procedures for employees and external parties.
- Establish communication responsibilities and escalation cascade for notifications and reporting both internal and external.

Initial Identification & Response

- Create procedures for confirming the incident, including investigation techniques.
- Detail the immediate actions to be taken upon incident confirmation, coordinating as needed with technology and insurance partners, as well as law enforcement.
- Ensure preservation of evidence.

Containment & Eradication

- Outline the steps to isolate and eliminate the threat.
- Consider the impact on operations during containment, including investigation requirements that could take days to weeks to complete and could entail a full pause in your operations.

Recovery

- Define the process for restoring affected systems to normal operation, keeping in mind that investigative delays may require a separate, fully independent restoration environment, depending on the type and severity of a cyber attack.
- Prioritize systems and data for recovery.

Communication

- Establish communication protocols for internal and external stakeholders.
- Prepare templates for incident notifications, including target lists for emails, media contact rosters, and information for each audience you expect to update.
- Again, create a protected yet accessible physical copy of all resources.

Documentation & Reporting

- Maintain detailed records of any incident, response actions, and outcomes. Designate a secure repository for those records, and leverage them for improvements and/or expansion of your incident response plan.
- Report incidents to appropriate authorities as required, including local, state, and federal authorities.

Sample Cybersecurity Incident Response Template

Training & Awareness

- Provide ongoing training for incident response team members.
- Educate employees about security awareness and reporting incidents, and make sure they are aware of both the IRT plans and their role in the case of cybersecurity incident.
- Additionally, update the information within your incident response protocols on a regular basis, including refreshing contact details.

Legal & Compliance

- Ensure your incident response team understands and is in compliance with relevant laws and regulations (e.g., GDPR, HIPAA).
- Engage with legal counsel if necessary.

Vendors & Third-Parties

- Include third-party service providers in your incident response planning, such as your insurance provider, IT services provider, key vendors, and others.
- Ensure they have their own incident response plans and meet regularly to compare, update and synchronize your strategies for seamless execution if an incident occurs.

Testing & Drills

- Schedule regular tabletop exercises and simulated incident scenarios, making sure to balance between IRT-specific tests and those that involve your entire organization.
- Evaluate the effectiveness of the incident response plan after each drill and update as needed. Continuous improvement is essential to stay on track with a quickly evolving threat landscape.
- After any incident, review and update the plan to improve your incident response strategy.

PR & Crisis Communications

- Prepare for potential public relations challenges and responses, considering both internal and external audiences.
- Maintain a consistent message to the public and media, and have a process for looping in your employees so they are aware and in sync with external messaging.

Remember that this is a simplified template/checklist, and you should adapt it to your organization's needs, resources, and regulatory requirements. Additionally, work closely with a cybersecurity expert or your managed IT services provider to ensure your plan is comprehensive and effective.