Post-Incident Response Checklist

- Conduct a blameless post-mortem analysis to identify the root cause of the breach and evaluate the effectiveness of your incident response.
- Develop a list of actionable recommendations based on the findings from the post-mortem review.
- Update your incident response playbook to incorporate lessons learned from the incident.
- Apply patches to all affected systems, and update all systems enterprise-wide with the latest security updates.
- If the attacker moved laterally, implement network segmentation improvements to prevent similar ease of movement in the future.
- Brief employees on what happened and how to reinforce security best practices, using anonymized scenarios from the incident as a learning story.
- Establish clear, consistent, and transparent communication channels for all stakeholders.
- Immediately identify all relevant internal stakeholders (management, IT teams, employees) and external stakeholders (clients, suppliers, media, regulators).
- Craft transparent and timely notifications that detail what happened, what data was affected, what the organization is doing, and what actions individuals should take.
- Own the narrative by proactively communicating with the public to protect your organization's reputation.
- Have your public relations team collaborate with security professionals to manage messaging.
- Ensure compliance with all applicable data breach notification laws, such as GDPR, HIPAA, and CCPA.
- Report the incident to the appropriate authorities, such as the FBI or CISA in the U.S., within the required timeframes.
- Ensure that all digital evidence is handled using forensically sound methods and that a clear chain of custody is maintained for legal admissibility.

- Review your cyber liability insurance policy to understand your coverage for costs associated with the attack, including legal fees, forensic investigations, and regulatory fines.
- Leverage your cyber insurance firm's panel of pre-approved experts for support with legal counsel and forensics.
- Assess the damage and determine the financial loss caused by the attack.
- Review and update security policies to reflect the new threat landscape.
- Enhance monitoring and detection capabilities to prevent similar attacks from going undetected.
- Communicate with clients and customers who may have been impacted, offering support and transparent updates.
- Conduct a final security audit to ensure all vulnerabilities have been addressed and the environment is secure.
- Publish a public report or a blog post to share lessons learned, reinforcing your organization's commitment to security.
- Provide support and resources for employees who may be experiencing stress or burnout from the incident.
- Update emergency contacts in your incident response plan, including internal teams and external stakeholders.
- Review and update all user access privileges, enforcing the principle of least privilege post-breach.
- Audit all accounts for unusual activity and reset credentials for any that were compromised.
- Formalize relationships with third-party vendors who assisted during the breach.
- Conduct a technical debrief with security and IT teams to review tools and procedures.
- Analyze the attack's financial impact to inform future budget requests for security.
- Update security awareness training with specific examples from the attack.
- Review legal and regulatory requirements for breach notification to ensure compliance.

- Engage in thought leadership by publishing insights about the incident response to rebuild trust.
- Reinforce the security culture by celebrating employees who reported suspicious activity.
- Implement a continuous improvement program for your security posture.