BREACH RESPONSE CHECKLIST

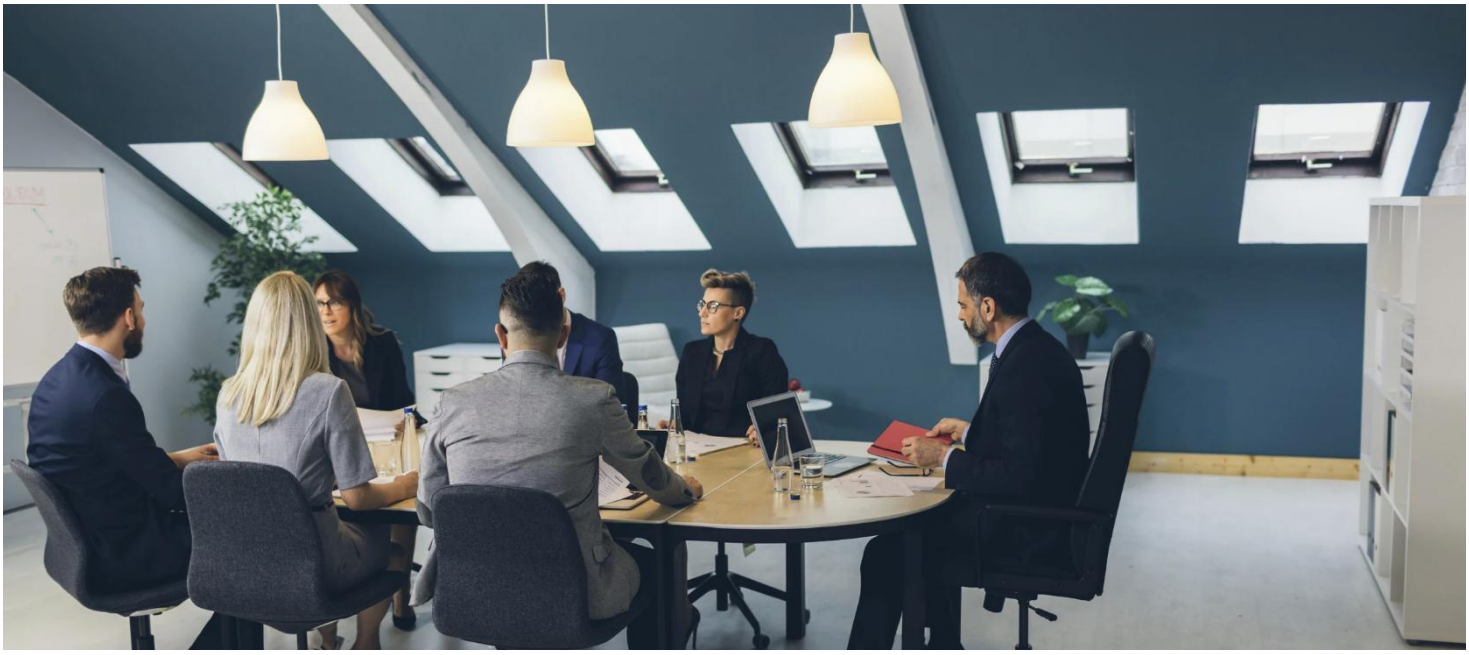
Use this checklist for data breach simulations and table-top exercises to validate your cybersecurity incident response in compliance with NIST CSF, ISO 27001:2022 and data protection legislation.

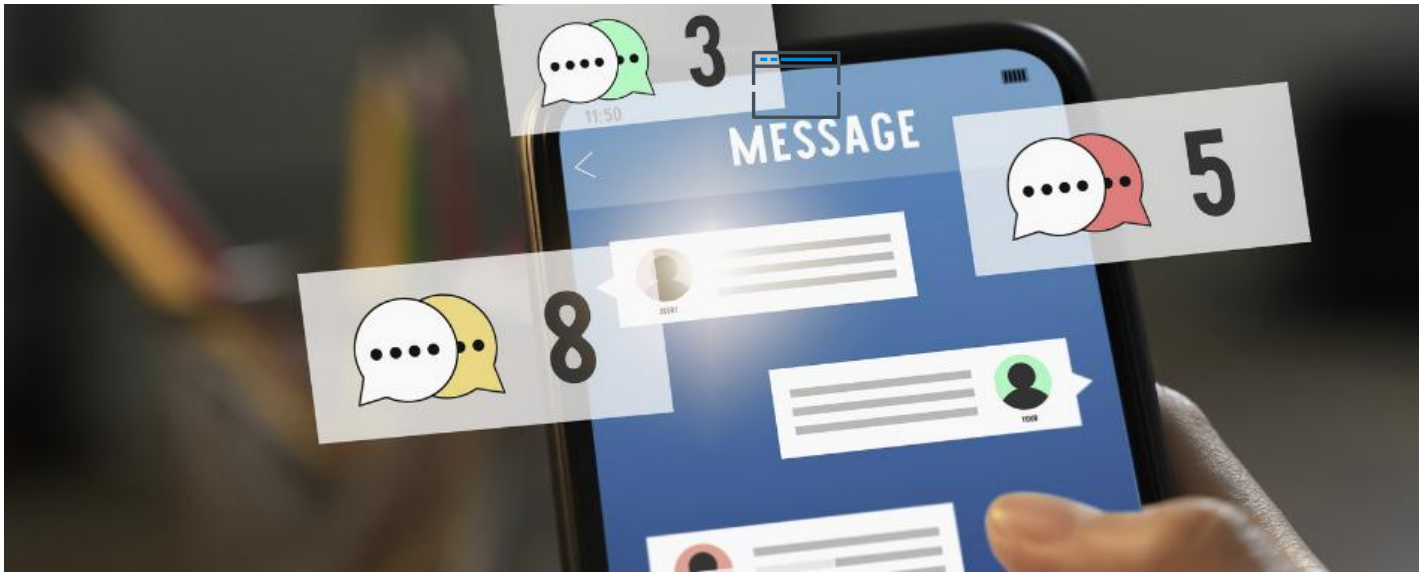
2. Immediate Containment and Investigation.

A. Isolate Affected Systems: Quickly disconnect affected systems from the network to prevent the spread of the breach.

B. Preserve Evidence: Ensure that all logs and evidence related to the breach are preserved for forensic analysis.

C. Conduct a Preliminary Assessment: Determine the scope and nature of the breach to understand what data and systems were compromised.





2. Notification and Communication.

A. Internal Notification: Inform key stakeholders and response teams within the organization immediately.

B. External Notification: Notify affected individuals and relevant authorities as required by law and regulations.

C. Transparent Communication: Provide clear and transparent communication to all stakeholders about the breach and the steps being taken to address it.

3. Mitigation and Recovery.

A. Remediation Actions: Implement measures to close vulnerabilities exploited in the breach and strengthen security controls.

B. Data Recovery: Restore lost or compromised data from secure backups, ensuring that the restored data is clean and safe.

C. Post-Incident Review: Conduct a thorough review of the incident to identify lessons learned and prevent future breaches.

Other Recommendations for Effective Cybersecurity Incident Response

- **Regular Patching**: Ensure all software is regularly updated and patched to protect against known vulnerabilities.
- **Password Security**: Enforce strong password policies, including the use of complex passwords and regular password changes.
- **Multifactor Authentication (MFA):** Implement MFA for all critical systems and applications to add an extra layer of security.
- **Employee Training:** Continuously educate employees about cybersecurity best practices and how to recognize phishing and other social engineering attacks.
- **Network Segmentation**: Use network segmentation to limit the spread of malware and unauthorized access within the network.
- **Incident** Response Plan Testing: Regularly test and update the incident response plan to ensure it is effective and current.

These steps will help enhance your organization's readiness and response to data breaches and other cybersecurity incidents.

Let's Build and test your incident response plan.
https://www.incidentmanagement.ca