Version 1.0

Date: 10/5/2019

Data Breach Checklist

1. 0 Purpose

To provide our members a checklist that can be modified and used to prepare your company for a data breach. This checklist compliments the NCSS's How-To-Guide on Data Breach Notification. The checklist guides you through the steps to prepare, respond and contain the damage of a data breach and can also be used to develop your company's own Standard Operating Procedure (SOP).

2.0 Prepare

a) Identify ownership and responsibility for the systems used by the organization.
b) Develop and maintain an up-to-date point of contact list for the software vendors that you may need to contact during a data breach.
c) Ensure security software (such as anti-virus, anti-malware, Host Intrusion Detection System (HIDS)) are up to date and enabled. Also consider using appropriate encryption software to secure sensitive information.
d) Develop a Standard Operating Procedure (SOP) for responding to a data breach for your company. In addition, consider establishing a rapid response team to quickly respond to potential data breaches.

3.0 Identify

a) Identify the type of threat and impact from the breach. For example, a compromise of the Marketing Manager's email could potentially expose details about proprietary information and company clients.
b) Notify internal staff of the breach in a discrete fashion. For example, if emails are compromised, use another method such as a phone or text to contact the team.
    i. Encrypt communication methods.
    ii. Limit communications to only those with need to know, such as the rapid response team.
    iii. Authorize or obtain additional resources for response and investigation; investigate the incident. See our Incident Response Plan.
    iv. Categorize known Severity and Impact (Low/Medium/High).
    v. Provide updates as important new information comes to light.

4.0 Contain

a) Identify all systems that may have been impacted. For example, if an email account of an employee is breached, it could potentially enable an attacker to gain access to other internal systems or involve other systems.

Data Breach Checklist

b) Collect information from your Managed Security Service Provider (MSSP) or other partner who notifies you of a potential event. Document and interview affected parties. Utilizing either your MSSP or a Forensic Investigator, assess the extent of the event. Ask your investigator to search for changes or new characteristics in files, system calls, processes, and/or network.

c) Identify and document data that may have been stolen or exposed.

5.0 Respond

a. Short term
   i. Gather evidence of the breach for further analysis. For example, using forensic imaging tools, create a bit level clone of the impacted server or computer hard drives.
   ii. Remove all malicious software from the infected systems, such as RAT (Remote Access Trojan), C+C (Command and Control), and any Backdoors.
   iii. Determine if data has been stolen and evaluate your legal requirements under either Payment Card Industry (PCI), HIPAA compliance and/or state regulatory frameworks.
   iv. Reset all administrator and user credentials.

b. Long term
   i. Assess your company's response to the data breach and develop plan for improvements.
   ii. Re-engineer systems to prevent or reduce the risk of data breaches - reevaluate access controls.
   iii. Segment critical data to more restricted areas.
   iv. Conduct quarterly checkpoints to re-evaluate the efficacy of new procedures.

6.0 Additional Resources

The NCSS has additional resources to help your company deal with a data breach:

1. ISAO Incident Reporting - report event to DHS via our AIS portal - https://nationalcybersecuritysociety.org/incident-reporting/

2. NCSS's How-to-Guide on Data Breach Notification

3. NCSS's Template to create your own Cyber Incident Response Plan

Data Breach Checklist

4. NCSS's How-To- Guide on U.S. Data Breach Laws

5. NCSS's Template to create your own Crisis Communication Plan

6. NCSS's Template to create your own IT Disaster Recovery Plan

7. SANS Incident Handling Forms - https://www.sans.org/score/incident-forms/

8. SANS Incident Handling Handbook - https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

9. CSO ONLINE - 15 Signs You've been hacked - https://www.csoonline.com/article/2457873/signs-youve-been-hacked-and-how-to-fight-back.html