Drill – Actions in Response to a Cyberattack

Task: Organize security and response operations in the aftermath of a cyberattack or intrusion to agency/organization/business' cyber systems.

Condition: Given the agency/organization/business has:

1. Established an identified Incident Cyber Response Team
2. Established pre-developed cyber response protocols specifically tailored to that agency/organization/business
3. Recognized the agency/organization/business is or has been the target of a cyberattack or cyber intrusion to its system(s).

Standards: Rapidly mobilize the entity's Incident Response Team to secure physical areas, stop additional data loss, fix vulnerabilities, report and investigate the attack, determine legal requirements and notify appropriate parties.

Performance Measures:

Upon recognition of a cyberattack or intrusion, mobilize the Incident Cyber Response Team to:

1. **Conduct an Initial Threat Assessment**. Make an initial assessment of the threat. Assess its nature and scope. Determine whether it is a malicious act or technological difficulty. This will help determine the type and extent of damage and mitigating and remedial solutions needed. This will also provide insight as to the type and expanse of any assistance needed. The assessment should seek to determine:

   a. Affected computer systems

   b. The apparent origin of the incident, intrusion, or attack

   c. Any malware used in connection with the incident

   d. Any remote servers to which the data was sent (if information was exfiltrated)

   e. Identify of any other victim organizations, if such data is apparent in logged data

2. **Make a Forensic Image of the Affected Computers**. As soon as possible after the incident is detected:
   a. Make a forensic image of the affected computers in order to preserve a record of the system for future analysis.
   b. Safeguard and restrict access to these materials from possible malicious insiders.
   c. Establish a formal chain of custody as this Forensic Image may serve as potential evidence in subsequent criminal trials.

3. **Enact the organization's Cyber Incident Response Plan**. Follow previously developed protocols tailored to the agency/organization/business to thwart the Cyberattack and restore operating systems.

   (Note: Exact response will vary depending upon the nature of the breach and structure of the agency/organization/business)

In general, this response should:

a. Identify the type of cyber attack

b. Secure the network

(1) Secure physical areas related to the breach. Lock them and change access codes

(2) Stop additional data loss. Do not turn machines off – but take all equipment affected equipment offline immediately.

(4) Update credentials and passwords of authorized users

(5) Wherever possible, replace affected equipment with "clean" machines

c. Report and investigate

(1) Notify appropriate points of contact within the agency/organization/business

4. **Report the Cyberattack/Incident**

a. **Report to US-CERT.** The US-CERT Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to US-CERT. This system assists analysts in providing timely handling of cybersecurity incidents as well as the ability to conduct improved analysis. Use the form found at https://www.us-cert.gov/forms/report. Provide as much information as possible in answering these questions so US-CERT may better understand the incident.

b. **Call NCCIC** for guidance. Provide a report of the cyberattack/intrusion using the format at https://www.us-cert.gov/forms/report.

c. **Notify the FBI** through eGuardian (https://www.fbi.gov/resources/law-enforcement/eguardian) or US Secret Service. FBI will investigate – but typically does not mitigate the impacts of the attack/intrusion.

d. **Notify local Law Enforcement.** Report potential risk for identity theft.

e. **Notify the Department of Homeland Security (DHS) Cybersecurity Advisor**

5. Determine Legal Requirements in the Aftermath of a Cyberattack

a. Determine any legal requirements specific to a breach of your agency/organization/business

b. Designate an informed point of contact from the affected agency/organization/ business authorized to release information and address queries

c. Notify affected businesses

d. Notify impacted individuals

References:

Federal Trade Commission. (May 2019) *Data Breach Response: A Guide for Business.* Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business