INCIDENT RESPONSE GUIDE

PREPARING

- Work with your organization's senior leadership and other relevant personnel to develop an incident response and business continuity plan based on the most pressing risks that have been identified in your organization's cyber risk assessment.
  - Develop threat scenarios for the kinds of incidents that relate to your organization's highest-priority cyber risks. Focus on building capacity to respond to those scenarios.
  - Identify, record, and make available within your organization a list of points of contact for incident response.
  - Identify and record contact information for relevant local and federal law enforcement agencies and officials.
  - Establish provisions specifying which kinds of incidents must be reported, when they must be reported, and to whom.
  - Establish written guidelines that outline how quickly personnel must respond to an incident and what actions should be performed, based on relevant factors such as the functional and information impact of the incident, and the likely recoverability from the incident.
  - Inform all employees to contact your technical team – most commonly this will be IT personnel and/or CISO/CIO/other comparable manager – when an incident occurs.
  - Deploy solutions to monitor employee actions and to enable identification of insider threats and incidents.
  - Include business continuity plans to coordinate how your organization will work with suppliers and primary customers during a business emergency, including how you would conduct manual or alternative business operations if required.
  - Include written procedures for emergency system shutdown and restart.
  - Develop and test methods for retrieving and restoring backup data; periodically test backup data to verify its validity.
  - Have established agreements and procedures for conducting business operations in an alternate facility/site.
  - Have in place a clear dissemination channel to all customers.

EXERCISING

- Organize small tabletop exercises with all staff or representatives from all levels of staff including organization's executives, PR/communications personnel, and legal and compliance teams.
- Identify and ideally participate in industry-wide tabletop exercises relevant for your organization.
- Establish process to ensure lessons learned from exercises are incorporated and addressed in your company's cybersecurity strategy.

RESPONDING

- Implement incident response plan actions to minimize the impact including with respect to reputational damage.
- Identify impacted/compromised systems and assess the damage.
- Reduce damage by removing (disconnecting) affected assets.
- Start recording all information as soon as the team suspects that an incident has occurred. Attempt to preserve evidence of the incident while disconnecting/segregating affected identified asset (e.g., collect the system configuration, network, and intrusion detection logs from the affected assets).
- Notify appropriate internal parties, third-party vendors, and authorities, and request assistance if necessary.
- Initiate customer notification and assistance activities consistent with laws, regulations, and inter-agency guidance.
- Use threat sharing platforms such as FS-ISAC or MISP to notify the industry about the threat.
- Document all steps that were taken during the incident to review later.

RECOVERING

- Restore recovered assets to periodic "recovery points" if available and use backup data to restore systems to last known "good" status.
- Create updated "clean" backups from restored assets and ensure all backups of critical assets are stored in a physically and environmentally secured location.
- Test and verify that infected systems are fully restored. Confirm that affected systems are functioning normally.

REVIEWING

- Conduct a "lessons learned" discussion after the incident occurred—meet with senior staff, trusted advisors, and the computer support vendor(s) to review possible vulnerabilities or recommend new steps to be implemented.
- If possible, identify the vulnerabilities (whether in software, hardware, business operations, or personnel behavior) that led to the incident and develop a plan to mitigate them.
- Develop a plan for monitoring to detect similar or further incidents related to the issues identified.
- Share lessons learned and information about the incident on threat sharing platforms such as FS-ISAC.
- Integrate lessons learned in your organization's incident response protocols.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America