Tips for Protecting Sensitive Data Before, During, and After a Cyber Incident or Breach

I. **Before the Attack**: IT systems supporting government organizations are inherently at risk. Cybersecurity experts now state “it is not if, but when” a cyberattack will occur. Without proper safeguards, these systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, and launch attacks against other computer systems and networks. Thus, government organizations need to effectively manage their cybersecurity risks and respond when incidents or breaches occur. The best time to plan such a response is *before* the attack occurs. Organizations can and should take the following steps to protect their IT resources and plan for cyberattacks.

1. Identify mission critical data and assets
2. Implement appropriate security and privacy controls to protect your assets
3. Ensure contracts specify contractor responsibilities for responding to incidents
4. Establish a cyber incident response team
5. Create and test an actionable incident response plan
6. Establish relationships with key external partners

II. **During the Attack**: Even with reasonable security controls, government organizations can and do fall victim to cyber-attacks and incidents. A quick, effective response to these incidents is essential to minimizing the resulting harm and expediting recovery. Taking prompt action and effectively executing a well thought-out and actionable plan can help to contain the scope of the incident or breach and limit its impact on organization operations and information. Organizations can and should take the following steps during a cyber-attack.

1. Make an initial assessment
2. Implement measures to minimize continuing damage
3. Recover and restore operations

III. **After the Attack**: When a cyber incident or breach occurs, limiting its effect on affected parties is a primary concern. Additionally, assessing the underlying causes of the incident and organization’s response can identify opportunities for improving the security controls as well as the planning and execution of the incident response plan. The lessons learned can assist organizations with taking the necessary steps to reduce the likelihood and impact of future incidents. Organizations can and should take the following steps after a cyber-attack.

1. Assess and mitigate risk to affected parties
2. Conduct post-incident reviews
3. Implement corrective/preventive measures

Tips for Protecting Sensitive Data Before, During, and After a Cyber Incident or Breach

Before the Attack

I.1. Identify mission critical data and assets:

- Identify what and who is connected to your network – maintain inventory of IT systems, networks, facilities, and services; remote connections; and vendors/3rd parties
- Identify the key data/information and business practices that enable your organization to achieve its mission
- Assess their relative importance – Identify your "crown jewels"
- Assess cyber risks (consider threats, vulnerabilities, consequences, likelihood of attack/incident)
- Determine organization's risk tolerance
- Develop cybersecurity risk strategy

I.2. Implement appropriate security and privacy controls to protect your assets:

- Limit and manage access to physical and logical assets and associated facilities to authorized users, processes, and devices
  - Uniquely identify each authorized device, user, and process.
  - Grant access using principles of least privilege and separation of duties
  - Use multifactor authentication and complex passwords to verify identity of each user, device, and other assets
  - Segment network to isolate high value/sensitive data
- Secure data consistent with organization's risk strategy
  - Encrypt data-at-rest and data-in-transit
  - Implement data leakage protections
  - Use integrity checking mechanisms to verify software and information integrity
  - Separate development and testing environments from production environment
- Configure strong security settings on firewalls, routers, switches, servers, and endpoints.
- Apply patches and keep applications and operating systems current
- Document and maintain security and privacy policies, processes, and procedures used to manage protection of information systems and assets, including Privacy Act required routine use statements in SORNs

- Provide computer security awareness and role-based training to organization's personnel and partners
- Continuously monitor network devices for vulnerabilities and compliance with configuration policies
- Implement security incident and event management systems to audit and log network activity
- Back-up systems software, applications, and data on a regular basis and store off-site.

I.3. Ensure contracts specify contractor's responsibilities for responding to incidents. Require contractors to:

- Cooperate and exchange information with agency personnel during audits and investigations
- Provide training to their personnel on incident response procedures
- Report suspected or confirmed cyber incidents to agency personnel promptly
- Allow for government inspection and forensic analysis of contractor-operated systems

I.4. Establish an incident response team:

- Identify roles, responsibilities, and contact information of specific officials who comprise incident response team. The team should include a senior executive, senior agency official for privacy, chief information officer, and officials from the following offices: IT security, procurement, budget, general counsel, and public affairs
- Train employees on roles and responsibilities for incident response and perform regular exercises to ensure employees understand their roles and responsibilities.

1.5 Create and test an actionable incident response plan:

- Identify what mission critical data and networks should be prioritized for greatest protection
- Specify procedures for preserving data related to the intrusion/incident for forensics and investigation
- Identify reporting requirements and procedures to DHS CISA, IG, law enforcement, Congress
- Identify factors for assessing the risk of harm to affected individuals and notifying these individuals
    - Nature and sensitivity of PII compromised by a cyber incident or breach
    - Likelihood of access and use of PII
    - Type of breach or incident

- Identify logistical and technical support needed to respond to cyber incident or breach
    - Senior agency official for privacy – call centers, prepare and deliver notices
    - Chief information officer / IT security – technical remediation and forensic analysis
- Conduct table top exercises and review response plan

I.6. Establish proactive relationships with key external partners including internet service providers, DHS Cybersecurity and Infrastructure Security Agency (CISA), law enforcement agencies, and cybersecurity firms whom you may call upon in the event of a cyber incident.

During the Attack

II.1. Make an initial assessment of the nature and scope of the incident:

- Assess whether incident is malicious or a technological glitch
- Identify which networks, systems, and applications are affected by the incident or breach
- Identify which tools the attackers are using and which vulnerabilities they are exploiting
- Assess potential impact of incident to prioritize incident response activities
- Notify appropriate internal personnel, consistent with the incident response plan
- Notify DHS CISA, law enforcement, and other external parties, consistent with the incident response plan

II.2. Implement measures to minimize continuing damage:

- Remove affected devices from the network or logically quarantine infected computers
- Avoid powering down infected systems as you may inadvertently destroy system logs files
- Disable compromised accounts and mobile device service
- Reroute network traffic to isolate affected network segments
- Delete malicious software
- Collect and preserve data related to the incident

II.3. Recover and restore operations:

- Replace compromised devices

- Upload backup versions of systems software, applications, and data, as needed
- Upgrade software or apply patches as needed
- Change passwords to all accounts
- Continue to monitor network for anomalous activity

After the Attack

III.1. Assess and mitigate risk to affected parties:

- Assess likely risk of harm to affected individuals based on factors in incident response plan
- Notify affected individuals, consistent with the incident response plan
- Offer assistance to affected individuals, if appropriate and consistent with incident response plan

III.2. Conduct post-incident reviews:

- Analyze the incident:
    - Identify deficient security processes and technical controls that facilitated the incident
    - Determine underlying causes of the deficiencies
    - Identify remedial actions
- Analyze the incident response – what went right, what went wrong
- Identify lessons learned and corrective action steps

III.3. Implement corrective/preventive measures:

- Implement remedial actions to prevent recurrence of incident
- Monitor and assess effectiveness of corrective actions over time
- Update incident response plan to incorporate lessons learned

Tips for Protecting Sensitive Data Before, During, and After a Cyber Incident or Breach

For additional information, see the following resources:

DHS CISA – https://www.dhs.gov/cisa/cybersecurity

Federal Trade Commission – https://consumer.ftc.gov/topics/privacy-identity-online-security

NIST Computer Security Resource Center -- https://csrc.nist.gov/

Center for Internet Security – https://www.cisecurity.org