DOJ updates cyber incident best practices guide

Rick L. Hindmand | Friday, October 26, 2018

Last month, the Cybersecurity Unit of the Department of Justice released its updated Best Practices for Victim Response and Reporting of Cyber Incidents, which outlines recommended steps to prepare for and respond to cyber incidents.

Preparation for Cyber Incidents

The guidance recommends the following pre-planning steps before a cyber intrusion or attack occurs:

- Educate senior management about the nature, scope and severity of cyber threats.
- Identify the critical assets and mission-critical needs of the organization, assess risks, establish cybersecurity priorities and determine how to manage the risks.
  - The guidance recommends adopting risk management practices, such as the NIST Cybersecurity Framework for protecting critical networks.
  - The HIPAA Security Rule sets forth risk assessment and management standards requiring HIPAA covered entities and business associates to perform and update risk analysis to identify risks to the privacy, security and availability of protected health information and implement safeguards to reduce the identified risks and vulnerabilities.
  - The guidance highlights the need to evaluate vulnerabilities relating to the use of contractors and vendors.
  - Ensure that those with incident response roles have access to the incident response plan.

  - The guidance expresses an expectation that the incident response plan will be ingrained through regular exercises.
- Implement incident response plans with specific, up-to-date procedures to handle cyber incidents, provide direction on how to continue operating while managing a security incident, and work with law enforcement and incident response firms.
  - The guidance identifies the following as essential issues to address in an incident response plan:
    - Who has decision-making responsibility for each incident response element
    - How to contact critical incident response personnel and, if unable to contact them, how to proceed
    - What mission-critical data, networks, assets or services warrant priority attention
    - How to contact and interact with third parties (e.g., data centers or cloud service providers) who host the organization's affected information
    - How to contact the organization's incident response firm and obtain assistance in responding
    - When and how to restore and insure the integrity of backed-up data
    - Criteria to determine who to notify, including when and how to notify law enforcement and government agencies.
- Develop relationships with law enforcement agencies, legal counsel familiar with cyber incident management, cybersecurity firms and others who can contribute to incident response.
- Implement appropriate workplace policies to ensure that personnel are familiar with the incident response plan and help prevent cyber threats and mitigate potential damage.
- Maintain basic cybersecurity policies and procedures, including patch management programs, access controls, network segmentation, password management programs, perimeter defense (e.g., firewalls), and server logs.
- Adopt technology solutions and service arrangements for response and recovery.
- Establish procedures for lawful monitoring of systems and devices for cybersecurity threats.
- Work to keep up with cyber threats by accessing information from public and private sector organizations, such as government agencies, information sharing and analysis centers (ISACs), and information sharing and analysis organizations (ISAOs).

After Detection of a Cyber Incident

The guidance describes the following steps in response to a cyber incident, and expresses the expectation that these issues will be addressed in the incident response plan:

1. Immediately assess the nature and scope of the incident
2. Implement measures to minimize continuing damage
3. Record and collect information
4. Notify appropriate points of contact within the organization, as well as law enforcement, regulators and other victims.

The guidance adds the following steps after a cyber incident appears to be resolved:

- Continue to monitor the system for signs of compromise
- Adopt measures to prevent similar attacks
- Conduct a post-incident review of the organization's performance and assess the strengths and weaknesses of the organization's incident response plan
- Note and discuss any deficiencies and gaps in the response and take remedial steps as needed.

In addition, the security incident should be analyzed to determine what notifications (if any) are required under relevant contracts and law, such as the HITECH Breach Notification Rule if protected health information (PHI) is involved, and state law.

The importance of effective incident response planning is clear from this guidance and from observations of others within private and public sectors. In particular, the Department of Health and Human Services Office for Civil Rights has identified incident response planning as a priority for HIPAA covered entities and business associates.

McDonald Hopkins LLC assists clients implement incident response plans and other cybersecurity policies and practices to address risks the privacy, security and availability of information, as well as in responding to cyber incidents and data breaches.

For more information, please contact the attorney listed below.

Rick L. Hindmand