July 2016

Is your Covered Entity or Business Associate Capable of Responding to a CyberSecurity Incident?

Computer security incident response is an important element of an information technology program. It can assist Covered Entities and Business Associates in promptly detecting breaches, decreasing loss and damage, mitigating the weaknesses that were exploited, protecting the confidentiality, integrity, and availability of data, and restoring IT services back to normal.

*HIPAA defines **security incidents** as attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. HIPAA also identifies **breaches** as, generally, an impermissible acquisition, access, use, or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information.*

According to a survey recently conducted, 43% of the survey respondents lack formal incident response plans and procedures, and 55% percent of them lack formal incident response teams. Also, 61% of these respondents have experienced a data breach in over the past two years, which included unauthorized access, denial of service, or malware infection. Cybersecurity-related attacks have continued to rise and become more destructive and disruptive. According to a different study, in 2014 the average cost to a company suffering a data breach affecting personally identifiable information (PII) was $3.5 million, with an average cost of $145 per individual.

With the constant upsurge of security breaches that involve cyberattacks and as required by the HIPAA Security Rule, Covered Entities and Business Associates should have security incident response capabilities established. Although effective incident response planning can be a complex task, it should be one of Covered Entities' and Business Associates' priorities.

When establishing incident response capabilities, Covered Entities and Business Associates should consider:

- ***Developing incident response policies , plans, and procedures***

An incident response policy assists Covered Entities and Business Associates in having a proper, concentrated, and coordinated approach to responding to incidents. The incident response plan should provide a roadmap for implementing the entity's incident response capabilities. The plan should also meet the Covered Entities' and Business Associates' distinctive requirements that relates to their mission, sizes, structures, and functions, and identify the necessary resources and management support. Incident response policies and plans should be approved by management and reviewed on an annual basis.

The incident response procedures should be based on the incident response policy and plan. Incident response procedures are outlines of the specific technical processes, tools, techniques, and forms that are utilized not only by the incident response team, but also by staff who need to report an incident. These procedures should include the entity's processes for:

- preparing for incidents;
- detecting and analyzing incidents;
- containing, eradicating and recovering from incidents; and
- conducting post-incident activities and reviews.

➢ ***Building relationships and setting up plans for communicating with internal and external parties regarding incidents***

Building relationships and lines of communication between the incident response team and other groups, both internal and external can be challenging. Covered Entities and Business Associates should plan the communication with these groups before an incident occurs.

Before establishing incident response policies and procedures, the incident response team should first develop relationships and lines of communication with internal groups within its organization, such as the IT department, public affairs office, legal department, internal law enforcement, and management.

Also, the incident response team should discuss with its entity's public affairs office, legal department, and management about sharing information with external groups. Covered Entities and Business Associates are often required to communicate with external parties regarding an incident and should comply whenever applicable. External parties could consist of federal agencies, law enforcement, media, internet service providers (ISPs), vendors, or other incident response teams.

- ***Staffing and training***

  Covered Entities and Business Associates should staff their incident response team with people who have the appropriate skillsets. These skills could include network administration, programming, technical support, intrusion detection, and CyberSecurity forensic analysis; team members should also possess teamwork and communication skills.

Furthermore, incident response team and staff members should be provided with the necessary training to be effective in their roles, and to carry out their responsibilities during an incident or when an incident is suspected.

Resources:

National Institute of Standardization and Technology (NIST):
http://csrc.nist.gov/publications/PubsSPs.html - *(Special Publication 800-61, Computer Security Incident Handling Guide)*

Office for Civil Rights (OCR): http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html - *(HIPAA Breach Notification guidance)*

This is an announce-only list, a resource to distribute information about the HIPAA Privacy and Security Rules. For additional information on a wide range of topics about the Privacy and Security Rules, please visit the OCR Privacy website at http://www.hhs.gov/ocr/privacy/index.html. You can also call the OCR Privacy toll-free phone line at (866) 627-7748. Information about OCR's civil rights authorities and responsibilities can be found on the OCR home page at http://www.hhs.gov/ocr/office/index.html.