



COMMONWEALTH OF PUERTO RICO
OFFICE OF THE COMMISSIONER OF INSURANCE

June 23, 2016

CIRCULAR LETTER NO.: CC-2016-1889-AF

TO ALL PERSONS THAT HOLD A LICENSE OR CERTIFICATE ISSUED BY THE OFFICE OF THE COMMISSIONER OF INSURANCE THAT HAVE AN ELECTRONIC INFORMATION SYSTEM

RE: CYBERSECURITY RISK

Dear Sirs and Madams

Cybersecurity should be a priority for all entities that manage information systems, particularly those with sensitive information on their insureds, providers and/or creditors. Due to the high volume of information managed by them, Insurers, Health Services Organizations, and their Intermediaries are especially vulnerable to cybersecurity risk.

The exposure to damage due to this risk includes, among other things, the loss of privileged information, extortion, unauthorized acquisition of personal information (data breach), theft or corruption of information, and interruption of operations. However, there are cybersecurity systems, which are the processes, procedures, technologies, and preventive measures used to protect information that is stored electronically from the risk of unauthorized disclosure or use.

All entities that hold a license or certificate of authority issued by this Office have the duty to control, monitor, and minimize all risks that are inherent to their operations, including cybersecurity risks. This circular letter is issued for the purpose of contributing to the efforts of our licensees to address their particular risks, for which guidelines and general recommendations are provided. The following are preventive measures and guidelines for corporate governance, administrative measures, and technical measures for the management of information system, which should be considered and implemented in accordance with the complexity of the operations of each licensee, after a careful assessment of the respective cybersecurity risk.

1. Corporate Governance:
 - a. Promote a culture of protection of information among directors, officers, administrators, and employees.
 - b. Implement an Information Security Program.
 - c. Establish policies and standards.
 - d. Annual assessment of business risk, including cybersecurity exposure.
 - e. Facilitate access to appropriate technology, in proportion to corporate needs and resources.
 - f. Formalize and empower an Oversight Committee for the Information Security Program.

2. Administrative Measures:
 - a. Establish a formal training and information access program for employees.
 - b. Assign monitoring responsibilities for the Information Security Program.
 - c. Maintain a monitoring program for service providers that have access to corporate information.
 - d. Maintain alternative programs for continuity of operations upon the occurrence of cyber events.
 - e. Identify preventively alternative methods for notifying persons that are affected by an unauthorized acquisition of personal information (data breach).
 - f. Identify proactively measures to mitigate cyber events.
 - g. Maintain liability insurance policies for risk and protection against loss of privacy, including coverage for interruption of business due to such risk.

3. All entities, as a minimum, must implement the following with regard to the information system network:
 - a. Firewall
 - b. Antivirus
 - c. Access and use of alphanumeric credentials (e.g. AD)
 - d. Internet traffic monitoring software
 - e. Inventory of electronic equipment
 - f. Legitimate licenses for all applications
 - g. Technical support/webmaster
 - h. Contingency plan
 - i. Internal security policies for network use
 - j. Backup system
 - k. Network monitoring/audit system
 - l. Control of remote connections to the systems
 - m. Perform a penetration test at least once a year
 - n. Alternate connection to internet (redundancy)

4. Encrypted portable equipment
5. The server area or communications room shall have:
 - a. Restricted physical access.
 - b. Appropriate temperature and humidity control for the equipment
 - c. Fire control system
 - d. Access log for the controlled area (date, name, purpose of the visit)
 - e. Flood-free area
6. With regard to servers:
 - a. These must have the latest patches required for their operating system
 - b. Updates must be filtered and monitored
 - c. There must be antivirus software installed
 - d. They must be behind the network firewall
 - e. They must be configured within a range of static IPs
7. With regard to confidential information:
 - a. Daily backups shall be done consistently
 - b. Ensure the security of the flow and storage of data
 - c. Restricted network access
 - d. Files containing privileged information will be encrypted

As an additional guide to the assessment of cybernetic risk, the Office recommends reading the following documents:

- Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), <http://www.nist.gov/cyberframework>
- Draft Insurance Data Security Model Law, NAIC Cybersecurity (EX) Task Force; NAIC Model Law #672 "Privacy of Consumer Financial Health and Information Regulation"; NAIC Roadmap for Cybersecurity Consumer Protections; http://naic.org/index_security_breach.htm

Very truly yours,

SIGNED

Ángela Weyne-Roig
Commissioner of Insurance