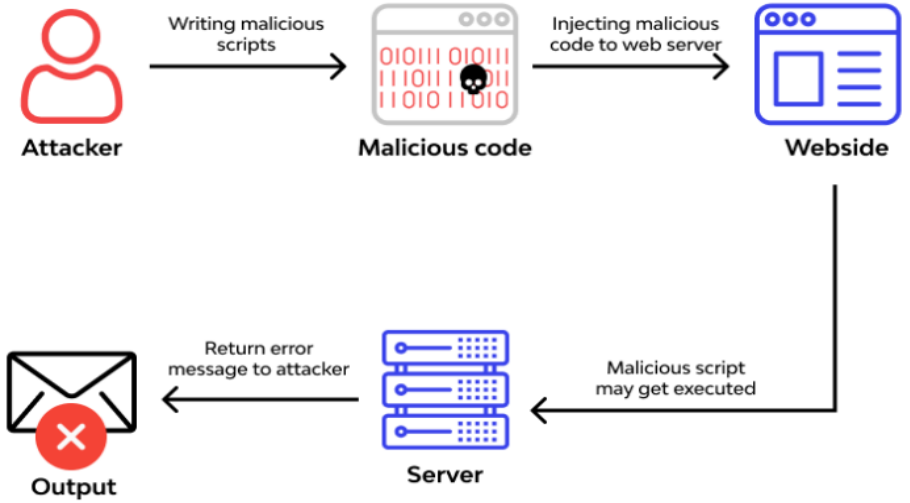
Cybersecurity:
New Challenges for Supervision and the Market

Prepared by:
Alexander S. Adams Vega, Esq., MPA
Puerto Rico Insurance Commissioner

OFICINA DEL COMISIONADO DE SEGUROS DE PUERTO RICO

Most detected forms of cyber attack in Latin America

- According to the report prepared by Fortinet, the Latin America and Caribbean region suffered 137 billion attempted cyberattacks between January and June 2022.
- The most detected form of cyber attack in the Latin American region was related to the vulnerability known as "Remote Code Execution".



Example of RCE vulnerability

Cyber Attacks on Critical Infrastructure

A WATER TREATMENT FACILITY IN PUERTO RICO. IMAGE: PUERTO RICO FISCAL AGENCY AND FINANCIAL ADVISORY AUTHORITY

Jonathan Greig
March 24th, 2023

News Industry

FBI, CISA investigating cyberattack on Puerto Rico's water authority

The agency that manages Puerto Rico's water supply has called in the FBI to investigate a cyberattack that occurred last week.

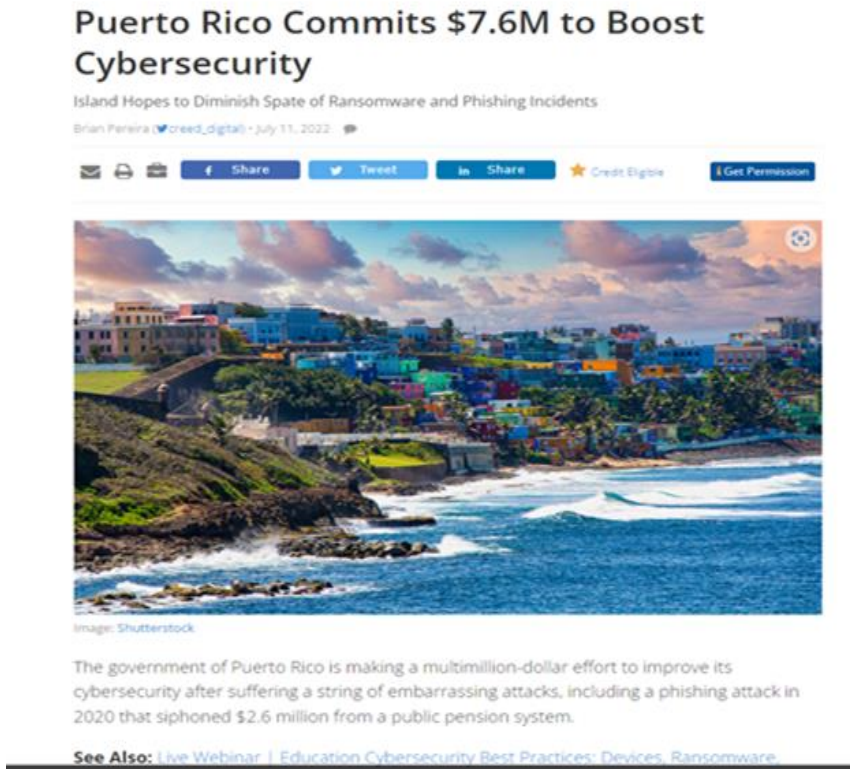
The investigation into the attack on the Puerto Rico Aqueduct and Sewer Authority (PRASA), which was announced on March 19, found that customer and employee information was compromised in the incident. But officials noted that the authority's critical infrastructure was not affected by the incident due to network segmentation.

Nannette Martínez, executive director of the Puerto Rico Aqueduct and Sewer Authority's (PRASA) office of innovation and technology, said the agency had activated "security protocols" following the attack.

"It should be noted that once the incident was detected and from the first moment we have

- On March 2023, the information of customers and employees of the Puerto Rico Aqueduct and Sewer Authority was compromised in a cyber attack incident, in which fortunately the authority's critical infrastructure was not affected by the incident.
- The attack is being investigated by state and federal agencies, "Cyber Division of FBI" and "Cybersecurity and Infrastructure Security Agency" (CISA), pointing out as possible responsible for the attack a "criminal organization" nationwide.

Puerto Rico Government Response



Puerto Rico Commits $7.6M to Boost Cybersecurity

Island Hopes to Diminish Spate of Ransomware and Phishing Incidents

Brian Pereira (@creed_digital) • July 11, 2022

Share Tweet Share Credit Eligible Get Permission

Image: Shutterstock

The government of Puerto Rico is making a multimillion-dollar effort to improve its cybersecurity after suffering a string of embarrassing attacks, including a phishing attack in 2020 that siphoned $2.6 million from a public pension system.

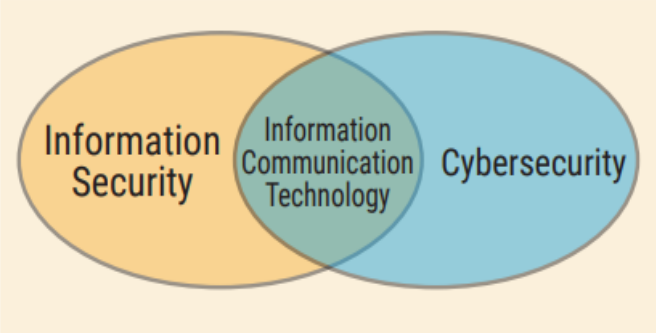
See Also: Live Webinar | Education Cybersecurity Best Practices: Devices, Ransomware

- The government of Puerto Rico announced a $7.6 million investment to strengthen cybersecurity measures at public agencies with the Multi-State Information Sharing Analysis Center (MS-ISAC), a component of the Center for Internet Security (CIS), the entity designated by the US Department of Homeland Security for the prevention and management of cyber threats for state and territory governments.

- The agreement provides Endpoint Detection and Response services to minimize or prevent the impact of any phishing/ransomware type cyber-attack that the government of Puerto Rico may experience.

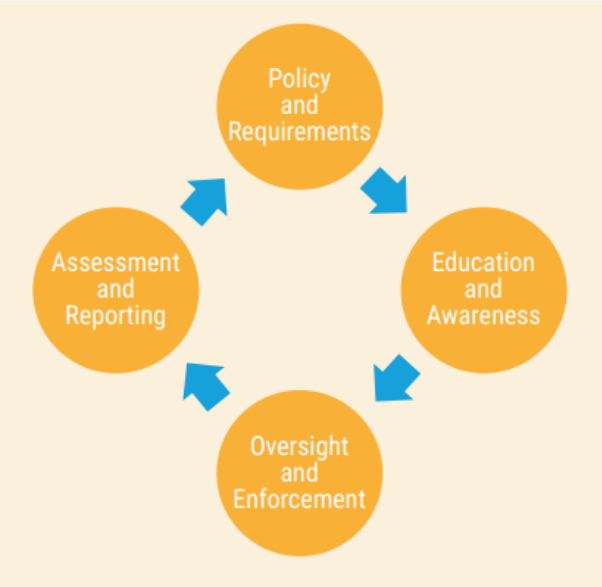
ASSAL-IAIS COSTA RICA 2023

Insurance Sector Regulation



- Insurance regulators have a critical role in protecting consumers' personal information.
- Puerto Rico seeks to adopt the regulatory scheme of the "National Association of Insurance Commissioners" (NAIC), under the "Insurance Data Security Model Law", as a legal framework to require insurers to implement a cybersecurity program.
- Cybersecurity program shall include:
  - ✓ Adequate cybersecurity testing criteria,
  - ✓ Board of Directors involvement,
  - ✓ Incident response plans, and
  - ✓ Specific incident reporting procedures

Cyber Security Program Benefits



Protecting infrastructure, information systems and information from unauthorized access or other malicious acts will enable the insurer to:

- Identify Risks.
- Protect nonpublic information.
- Detect and respond to cybersecurity events.
- Recover from the event.
- Notify the event as appropriate.
- Restore normal operations and services.

An effective cybersecurity plan is essential to minimize the possible negative impacts of cyber attacks.

THANKS!

ASSAL Asociación de Supervisores de Seguros de América Latina

aii access to insurance initiative

SUGESE Superintendencia General de Seguros República de Costa Rica

IAIS International Association of Insurance Supervisors

Financial Stability Institute | BIS