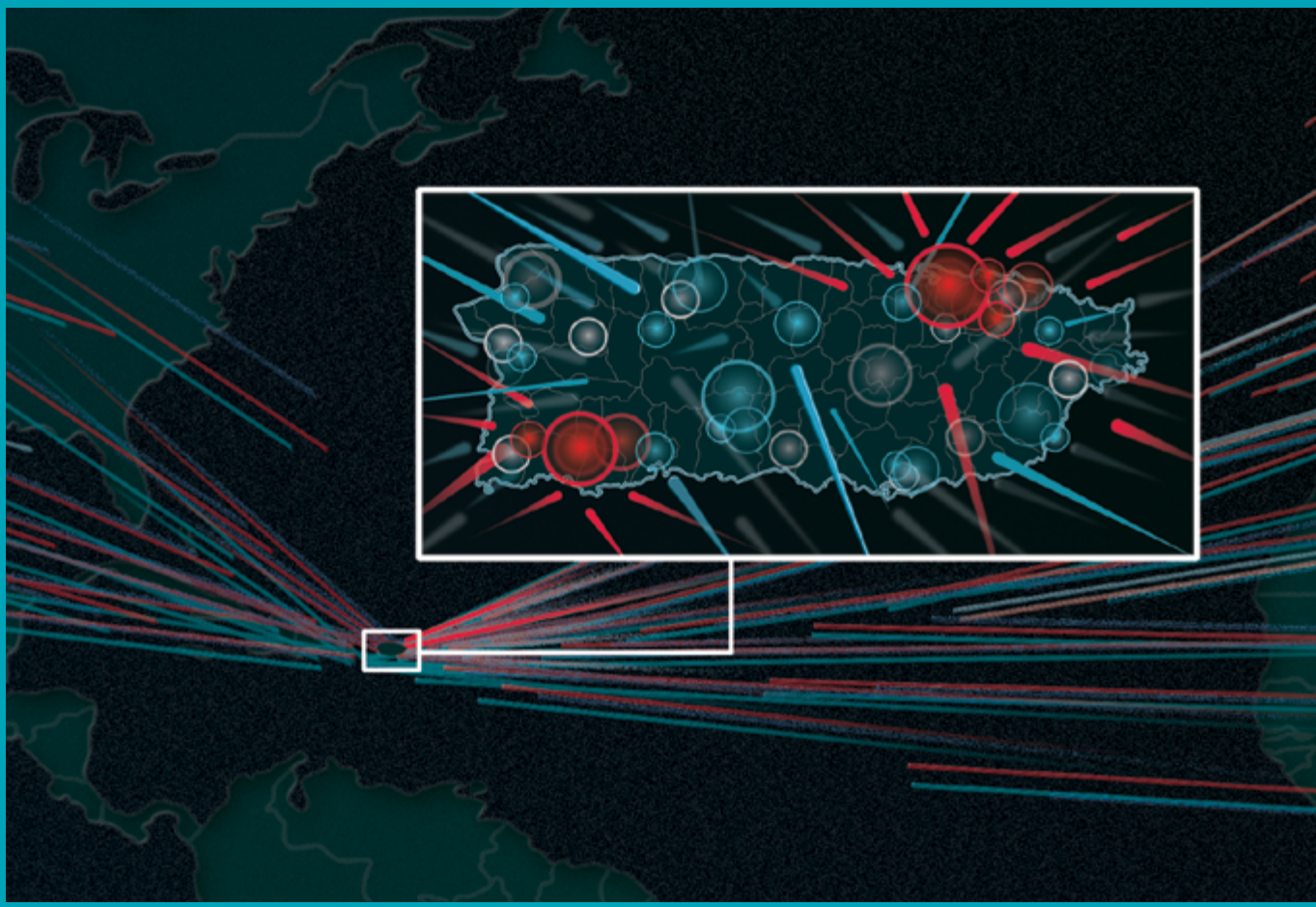
RANSOMWARE CASE STUDY

HACIENDA OF PUERTO RICO

Phone: 443-345-0503
infopr@compsecdirect.com
www.compsecdirect.com



Release Date:
June 21, 2021
Illustration: María de los Ángeles Pagán

José Fernández
President

THANK YOU

FOR VIEWING THIS STUDY

Puerto Rico faces multiple challenges that seem impossible to fix. As a Puertorrican, it is necessary to recognize our collective efforts as we attempt to improve the quality of life of its citizens. Notwithstanding we must learn from past mistakes, not to humiliate nor denigrate those involved, but instead to understand how similar situations can be avoided in the near future. Hacienda may have been hacked in 2017, yet we are all Hacienda; we are all optimistic that things will get better and we feel this is intended to show how.

151 Calle San Francisco
Suite 201
San Juan, PR, 00901

Phone: 443-345-0503
E-mail: infopr@compsecdirect.com
www.compsecdirect.com

Content: José Fernández
Design: María de los Ángeles-Pagán
Marketing and press: Ivette Rodriguez
Revisions: Oscar Fuentes

CONTENT

Special thanks: Heriberto Acosta, Giancarlo Gonzales Ascar, Fortaleza de Puerto Rico, Hacienda de Puerto Rico, BSides PR.

LIGHTING STRIKES TWICE AND

CYBER NEVER SLEEPS

CompSec Direct provided initial Incident Response efforts for the Department of Hacienda; also known as the Treasury Department of Puerto Rico.

The following Case Study illustrates how effective leadership, coordination of actions and preventative measures can prevent scenarios like the one faced by the Department of Hacienda. CompSec Direct was present in high-level briefings with the Department of Hacienda (DOH) staff, executive leadership, and the FBI during and after this engagement.

Technical information such as IDS logs, ransomware copies, network diagrams and deliverables from 3rd party providers were also shared with CompSec Direct and formulates part of our assessment in this Case-Study.

CompSec Direct provided guidance, recommendations, and action items for Hacienda to follow.

QUICK FACTS

... FOR THOSE UNFAMILIAR WITH HACIENDA

The organization is understaffed

Hacienda is dependent on contractors that are over tasked and simply unable to effectively mitigate to future threats.

The IT security goals are not clear

Although it's difficult to envision the defend "everywhere, everything and always" functioning in a complex eco-system; this is the organization that collects revenue for the island and is not capable of deterrence of threats.

Stakeholders are responsible

Staff on-site was not well-equipped, organized nor prepared to deal with ransomware. Knowledge of the existing vulnerabilities and weaknesses of the IT eco-system is a responsibility of the government, who depend on contractors for valid and transparent identification of such weaknesses.

Leadership gaps in response efforts

The organization did not have a CISO when the event occurred. This is the result of talent exodus that effects hiring of skilled staff in the island. Transition period between governing parties worsened this gap for new leadership staff that lacked knowledge and dissemantion of technical debt inherited from previous administration.

EXECUTIVE SUMMARY

IMPACT FACTS

On March 5, 2017, the Department of Hacienda (DOH), Suffered outages to services that:

- Impacted state-revenue sources
- Denied the port authority of Puerto Rico to tax shipping trade
- Denied residents and companies to submit sales-tax revenue to the DOH

Sources inside of Hacienda stated that the losses exceeded $20 Million dollars a day due to outages.

The agency attempted to identify the source of outages that began occurring during an alleged maintenance period.

Link to March 6, 2017 Article from El Nuevo Dia
From: ElNuevoDia.com

EXECUTIVE SUMMARY
CONDENSED FACTS

Staff Identified Ransomware

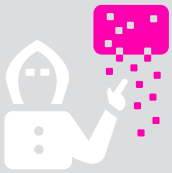
Analysis by the IT staff at Hacienda (ITSH) determined that ransomware was infecting client machines and servers in the network. The agency was overwhelmed with outages and requested the assistance of experts to remediate the problem.

Assistance to restore availability

CompSec Direct and other companies were contacted to assist Hacienda with this situation. The government of Puerto Rico also solicited help from the local talent pool of Information Security professionals that live in the island.

Work was divided between three teams

Experts provided input towards the first 48 hours after the event that allowed DOH to collect revenue, thanks to the government leadership, ITSH and CompSec Direct.



Trust is fragmented in the organization

IT Contract disputes had occurred in the last few months. Auditing/Legal team had low confidence in ability of ITSH to safeguard sensitive communications.

The FBI made arrests related to insider crime

It is not clear if the insider crime was related to the ransomware as originally believed by the ITSH. We consider that the accused have the benefit of the doubt as to their involvement until all criminal proceedings have concluded.

We provided strategic advisory

CompSec Direct provided the initial strategic advisory needed to help DOH coordinate and mitigate the effects of malicious activity at DOH.

Link to March 7, 2017 Article from El Nuevo Dia
Author: Gloria Ruiz Kuilan @ ElNuevoDia.com

THIS COULD HAVE

BEEN AVOIDED

Proactive-Defenses

Scanning, monitoring, testing your Infrastructure before a problem occurs.

Requires outsourcing and Independent evaluations.

Perimeter Scanning

Using internal scanning helps identify your IT eco-system. External scanning would have identified how this eco-system is accessible remotely.

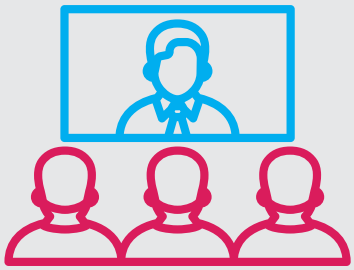
Continuous Monitoring

The IT eco-system outnumbers your staff. Without custom fitted monitoring solutions, your staff will not be able to effectively respond to incidents.

Testing

Mature organizations will test disaster recovery scenarios regularly towards recovery objective points. As more test are performed, logistical and technical gaps become reduced and refined. In house staff is already dedicated towards availability, not resilience.

OUR MAIN AREAS OF EXPERTISE RELATED TO THE INCIDENT

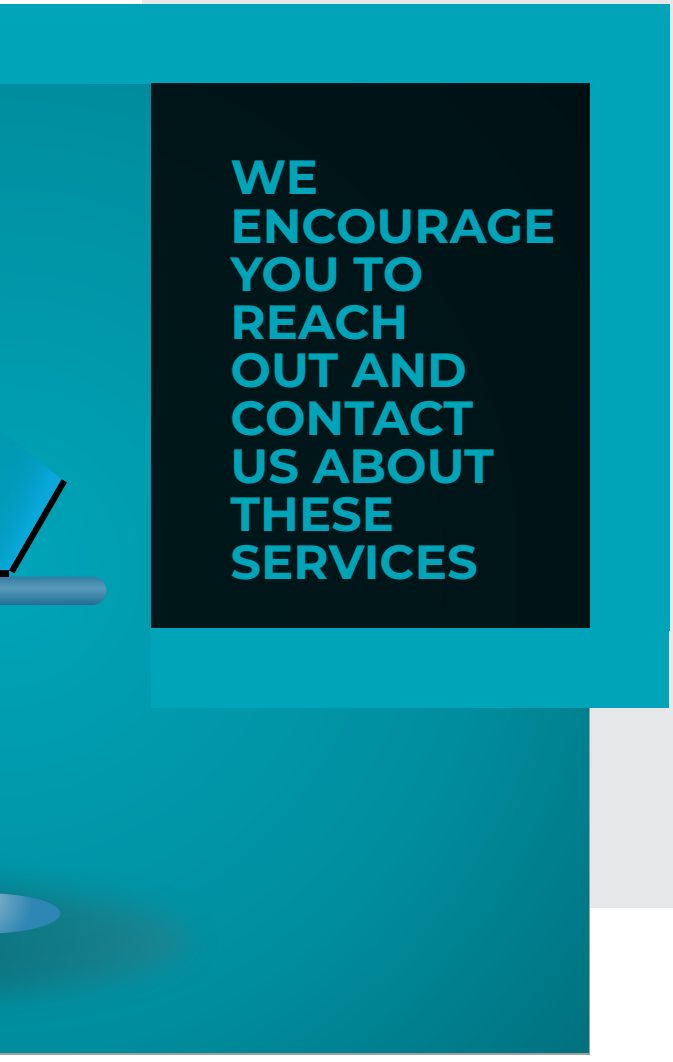


Staff Augmentation

We want to help your staff grow; we are not interested in replacing your staff. By mentoring and working with your in-house staff, we can collectively improve awareness of unknown and undetected threats.

Ransomware Protection

Prevention is less expensive than remediation of an incident. Ransomware is not solved by turn-key vendor products. We can help your staff identify and manage risk before its too late.



Hunt as a Service

By actively defending your IT eco-system, we can deploy dedicated staff to remotely hunt for adversaries within your network. This is a long-term commitment to enable active monitoring using digital and human resources.

Incident Response

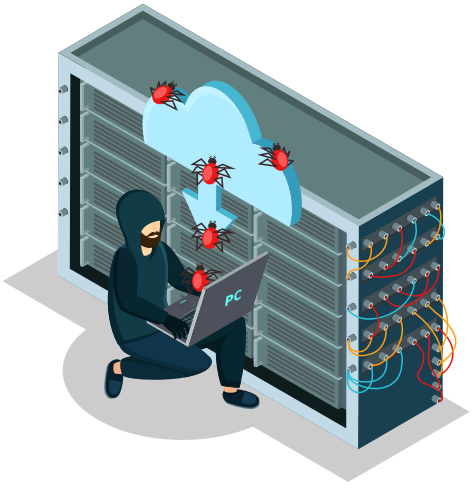
Timing is critical and after a breach is detected you need to call experts to reduce the impact this will have on your staff. Having pre-established relationships with multiple response vendors reduces pre-start paperwork and enables vendors to work on the problem; your breach and not your procurement process.

SUMMARY OF EVENTS

QUICK STRATEGIC EXECUTION

- **COORDINATION AMONG GROUPS WAS NOT EFFECTIVE NOR IN UNISON**
- **DOH LEADERSHIP SHARED INSIGHT INTO A MULTI-YEAR INVESTIGATION OF POSSIBLE MALICIOUS INSIDERS AS A CAUSE FOR ATTACK.**
- **THE GOVERNMENT OF PUERTO RICO MOVED AWAY FROM MALICIOUS INSIDER THEORY AND NOW CLAIM CHINA IS BEHIND THE ATTACK.**

CompSec Direct provided actions plans for Network and Windows® staff members to utilize during the ransomware.



The FBI arrests two employes at Hacienda for corruption

"The men are accused of extortion and taking bribes."

Link March 9, 2017 Article from El Nuevo Dia

Author: Frances Rosario @ ElNuevoDia.com

DATA BREACH, RANSOMWARE,

Summary of events from Mar 7, 2017 to Mar 9, 2017

- THE P.R. CIO REQUESTED AN IMMEDIATE PLAN AND COORDINATION EFFORT AMONG THREE FUNCTIONAL GROUPS:

> Incident response group - CompSec Direct
> Internal monitoring group - DOH Staff
> Malware analysis group - 6th Element Group; now FiberWolf

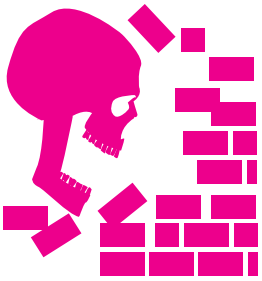
- COMPSEC DIRECT IDENTIFIED THAT TWO MEMBERS OF THE ITSH WERE ULTIMATELY RESPONSIBLE FOR SECURITY WITHIN DOH, FOR A USER BASE OF OVER 5,000 EMPLOYEES.

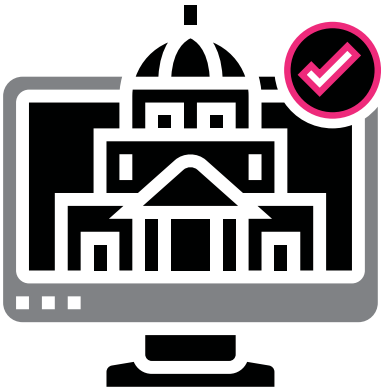
- THE DOH LEADERSHIP BELIEVED ASKING THE FBI TO ASSIST IN INVESTIGATION WOULD HELP FIX EXISTING ISSUES... DURING AND AFTER THE CRISIS.

- A LEAD INTERNAL AFFAIRS (IA) INVESTIGATOR FOR DOH, MENTIONED THAT ITSH MEMBERS POSSIBLY READ IA EMAILS AND BECAME AWARE OF AN INVESTIGATION REGARDING BRIBES AND KICKBACKS.

WHY DID THIS HAPPEN?

HISTORICAL EVENTS PRIOR TO BREACH

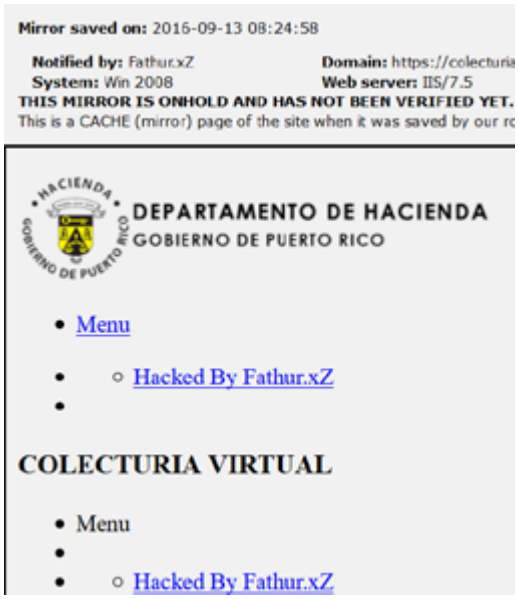




Puerto Rico has a long-standing history of insecurity among public service offerings.

Despite this, it has been able to provide value added services to residents and commercial entities as part of the much needed digitalization of government services.

The DOH and other state officials minimized the impact of this breach, despite being clearly hacked and stated that no records were leaked.



The DoH also had contract disputes with a well-established IT service provider in the island that may or may not have not lead to contract work-role reductions in the face of bankruptcy and economic insecurity among residents.

The DoH publicly acknowledged a web-site defacement in September 2016

The defacement was allegedly executed by a hacker known as **Fathur.xZ**

This hacker handle is associated with the Indonesian Cyber Freedom crew.

THREAT ACTOR PROFILE FATHUR.XZ

Possible Twitter account:
fathur Xz'aliDce-AOH
@fathurAOH

Over 2,900+ hacks claimed on Zone-H

Known member of the Indonesian Cyber Freedom crew

High confidence on Attribution.

Made/Sold t-shirts on **TeeSpring**

Design By Fathur.xZ With Backtrack Dragon High confidence on Attribution.

Breach Analysis:

DOH was most likely hacked due to lack of security on the CMS portal by leaving the default Install Wizard exposed.

Actor is perhaps taking risks by not compartmentalizing online identities and activities.

Targeting was **random** and **not directed** against DOH

TeeSpring is a valid attributable source to this individual via access logs associated to this account.

IT CHALLENGES THAT IMPEDED HACIENDA FROM PREVENTING RANSOMWARE AND DIMINISH CYBER SECURITY EFFECTIVENESS

01
Contract disputes
Allegedly and despite high levels of unemployment, the organization over- relies on contractors.

02
No CISO
No champion for security concerns voiced by staff and contractors

03
Technical Debt
Multiple systems; both modern and legacy that increases sustainment operations and impedes changes towards risk reduction.

04
Lack of boundary monitoring and controls
Hacienda was exploited by not reducing attack surface.

05
No security operations
No internal staff, independent from IT, dedicated to hunt and incident response.
An out sourced SOC is not suitable for this organization given point #1 and barriers that occur when contractors direct government staff on prevention and remediation efforts.

ACTIONS FROM THE FIELD

Key Findings and recommendations

- Preserve future evidence by disconnecting LAN cables and employing firewall rules on local and cloud Infrastructure to preserve dynamic evidence vs powering off affected systems.

IT Staff must continue supporting their roles and not become forensic analysts

- When incidents such as this occur, its difficult to convince staff to resume normal duties since they feel responsible to fix and address problems at the moment.
- We informed the staff that if we provoked the actors, the problem could become worse than it already was. This also involved denying any press interviews as the situation was not contained.

EFFECTS FROM OF OUR INVOLVEMENT ON DAY 1 AND LIMITATIONS OF ACTIONS

- **CompSec Direct helped Hacienda to resume generating income for Puerto Rico.**
- We helped steer initial success of response of backup responsibility across respective platforms since lighting would strike twice.

RECOMMENDED BACKUP/REMEDIATE AND HARDEN STRATEGY

TIME-LINE OF OUR INVOLVEMENT: DAY 02

- The staff reported that additional malware had executed within the organization.
- We provided the DoH a list of action items for the Windows Admins and the Firewall admins, these were rated in criticality and forensic importance in two parts, by 12:00 PM.

"BLOOD IN THE WATER" occured as an influx of vendors began offering services and giving presentations despite having no technical background, expertise, or knowledge related to incident response, system hardening, or disaster recovery which Hacienda needed...

DAY 2 PROPOSAL DELIVERY

CREATION OF SOLUTION

COMPREHENSIVE RESPONSE

plan to conduct the response, harden the network and gather forensic evidence to assist law enforcement.

COST EFFECTIVE SOURCING

information for software purchases necessary to remediate existing problems while being respectful to economic debt.

A BETTER PROPOSAL

from the services delivered to customer by Microsoft since response services from this vendor do not include comprehensive system modifications in conjunction with long-term Proactive-Defenses.

> “Incident response is the equivalent of paying someone for your organizations lack of preparation and vision. We go in, remove the problems we can find, enable continued visibility for a certain period to double check the things we missed and offer no assurances that you will ever be more secure since we were there. It’s expensive, perishable and always preventable.”
> **Preparation, training and strategic outsourcing are the enemies of incidents.**

EXIT FROM ENGAGEMENT

TIMELINE OF INVOLVEMENT: DAY 2 END OF DAY

We recommended that the organization should consider paying one bitcoin (approx. $1,200) to decrypt the one machine that had the backups they were missing as cost-effective and not cost-inhibitive as opposed to a costly response with data decryption efforts that are not guaranteed.

DAY 3 –DISCUSSIONS WITH FBI

THE BURDEN OF DISCOVERY AND LAW ENFORCEMENT EXPECTATIONS

Leadership was convinced the FBI would fix problems

The lack of cyber-professionals within the federal government has created a backlog of cases. We reminded leadership that the FBI does not secure victim networks.

CompSec Direct briefed the FBI to reduce fact-discovery period

After attending an executive pre-brief meeting, we helped articulate actions performed to date and limited discussions to facts relevant to this case to assist any future investigations.

STRATEGIC RECOMMENDATIONS

RESULTS ARE POSSIBLE DESPITE ECONOMIC PROBLEMS

Use internship programs for 6-12 month Gov Jobs

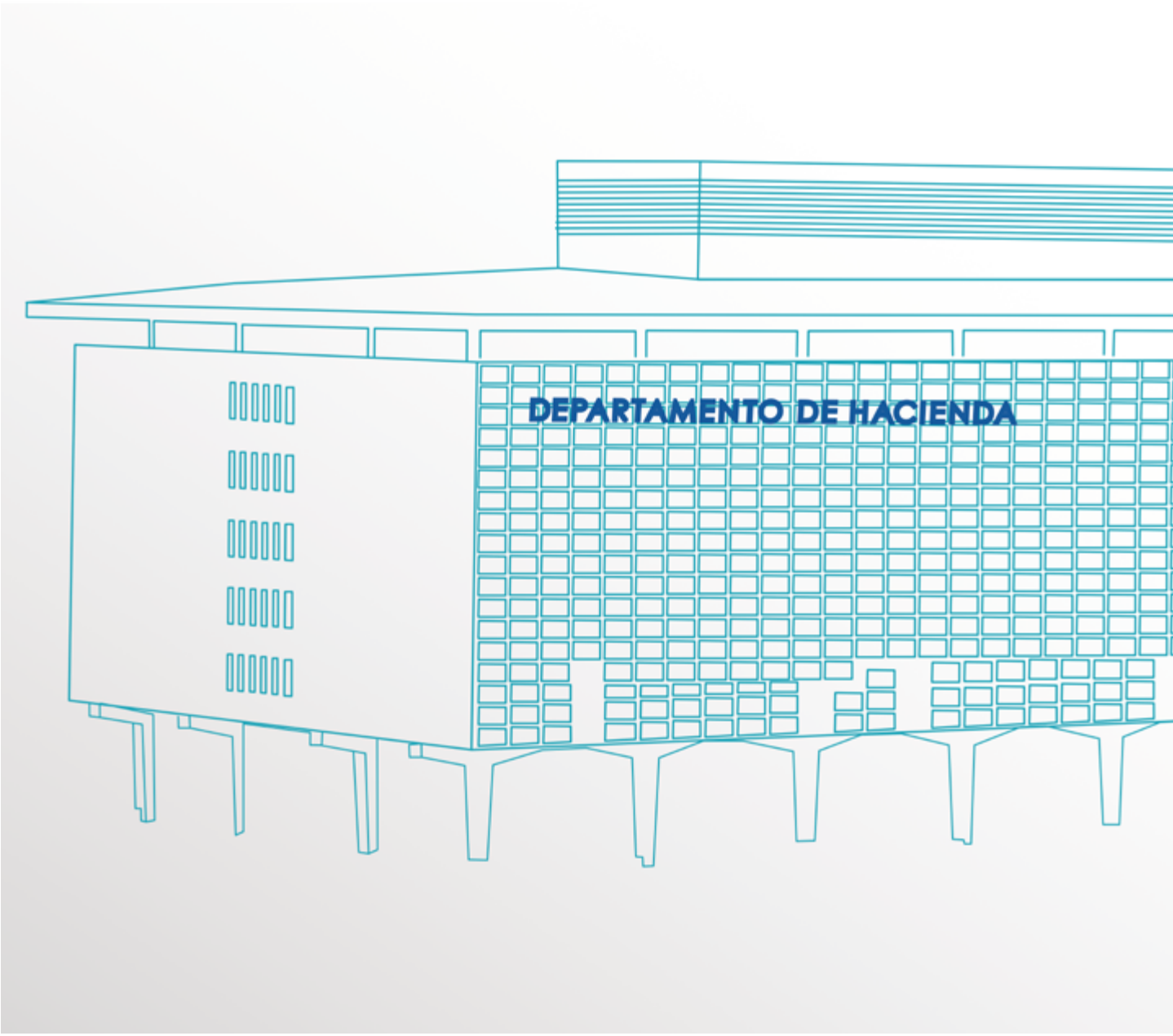
Computer Security focused hires in local universities and open recruiting fairs in events like BSides PR

Develop & test DR process

Backup/recovery scenarios to test effectiveness of disaster recovery strategy.

Develop and train senior IT staff members

Augment senior staff members on proper pre-incident response actions and reporting without using existing contractor base; which admittedly helped cause this breach. If no investment is made into senior staff roles, their skills stagnate and they may leave for better compensation elsewhere with little regard to continuity of action and knowledge sharing prior to departing.



HACIENDA

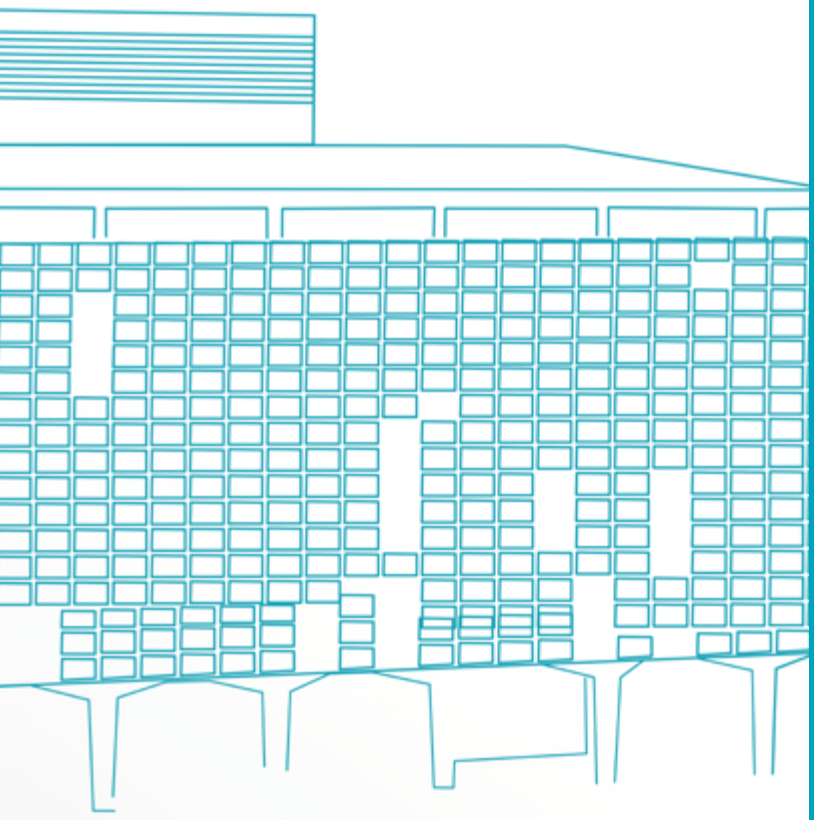
CLOSING THOUGHTS

Conclusions

All the warning signs for the Department of Hacienda were present:

1. Past breach.
2. Contract disputes with IT contractors.
3. Suspicion of privileged users abusing business activity.
4. Leadership change resulting from elections.

- ☑ The problems Hacienda had before this event may still exist.
- ☑ We are all Hacienda; no organization is impervious to sabotage by insiders and long-term exploit campaigns.
- ☑ Disaster recovery planning and testing has to be redundant since storage costs are low.
- ☑ Cloud is not a suitable Hot-Site when backups are over 1 Tb and your uplinks are not designed for speed.
- ☑ The PR government needs true experts from specialized cyber providers for help.



WE ENCOURAGE YOU TO CONTACT US FOR LONG-TERM STRATEGIC SOLUTIONS AND PRICING OPTIONS

www.compsecdirect.com
infopr@compsecdirect.com

(443) 345-0503

151 Suite 200, San Juan, PR 00901

Recommendations

We advised Hacienda on which systems could be restored to resume business operations and helped Puerto Rico generate millions of dollars by doing so.

Coordinate with FBI to determine operators of bitcoin wallets used in campaign.

Coordinate through FBI to determine operators of Tor nodes used for ransomware registrations as evidence of serious crime has occurred.

CompSecDirect is a C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) security firm that specializes in Information / Cyber Security. We are a service-disabled veteran owned company with an incredible talent pool comprised of former DoD network operators within different sectors of the federal government. The majority of our employees have undergone intensive background-checks by Federal Agencies within the last two years, making them trusted individuals within the intelligence community and private sector. Trusted Individuals is one of our main differentiators to other organizations.

Publishers Note: We caution and caveat the information enclosed as our professional opinions and observations during this engagement and does not attempt to represent the views of the Puerto Rican government. The contents of this case study are not authorized for use in the press, is not suitable for referencing nor serves as testimonial evidence for use in legal preceding's without the expressed notification, consent and approval from Comp Sec Direct LLC.