Case Study: City of Portsmouth IT and Cybersecurity Turnaround A Partnership with Neoscope

Client: City of Portsmouth, New Hampshire

Challenge: An Emotet virus-infection brought the entire City network down for an extended period of time early in 2018. The City needed a Cybersecurity focused Managed Services Provider to ensure the long-term stability of their IT.

Solution: Implement a multi-pronged containment plan over a two-month period followed by a Managed IT and Cybersecurity Services offering for the City from Neoscope.

Results: The emergency partnership between the City of Portsmouth and Neoscope succeeded in eliminating the Emotet virus within a few weeks. Longer-term, Neoscope stabilized critical infrastructure, applications, security solutions and networking components resulting in a healthy computing environment, robust availability and network security. Neoscope also aided in pro-active longer-term planning of the City's infrastructure culminating in the City, as required by law, going out to bid for Managed IT services. Neoscope won the bid among over a dozen other local and national IT providers.

"Within weeks, Neoscope transformed a destructive network security situation into a manageable and then healthy one. They stepped in after we had discovered the Emotet infection and tried and failed to eradicate it. The Neoscope team provided immediate analysis and an action plan with on-sight, proactive service going forward. We are confident that we are getting prompt, thoughtful attention and good advice from Neoscope. Their professional-level security platform has made a difference for the City of Portsmouth."

-Alan Brady, Director of IT, City of Portsmouth

OVERVIEW

In April 2018, the Portsmouth Herald reported that the City of Portsmouth was enacting "remediation efforts against a virus that infected the city-wide computer system have cost more than $100,000 to date, while attacks against it remain ongoing."

Portsmouth was not alone in dealing with Emotet, a malicious file virus that intercepts and logs outgoing network traffic sent from a browser and can potentially lead to compromised sensitive data. First discovered by European computer scientists in Europe, Emotet has attacked systems vigorously in the United States for more than three years. In 2016, Emotet was suspected of causing data breeches at the Concord, NH school system and the New Hampshire Dept. of Health and Human Services.

Excluding the police and fire departments which are segregated from the city's network, Brady said the system serves more than 400 users in departments spread across the city.

"In my 17 years as an IT manager we had never seen anything as ferocious as Emotet," Brady said. "We were told that if you're infected with Emotet, you're a goner as some cities had been hit quite hard with it. We worked for weeks with our previous managed services provider to employ anti-virus solutions but they didn't work. We needed a fresh set of eyes. That is when Neoscope reached out to us and we brought them on board."

"We had heard about the attack and contacted deputy city manager Nancy Colbert Puff to lend our assistance," said Tim Martin, the CEO and president of Neoscope. "Our team along with our Chief Information Security Officer understands and knows how to confront attacks and responses. We offered to help the City of Portsmouth first to contain the event, and then to eventually cleanse, re-engineer, and rebuild the entire system."

KEY CHALLENGES

In addition to eliminating Emotet, the initial assessment by the Neoscope security team determined the City of Portsmouth had a wide range of cyber-infrastructure issues including:

- Multiple firewalls and networks configured in non-standard configurations;
- Lack of Cybersecurity Awareness Training;
- Lack of DNS, anti-virus, and network protections;
- Lack of 2-factor authentication for remote access;
- Lack of e-mail archiving, continuity encryption, or anti-Spam/Phish/Malware;
- Inefficient and ineffective licensing of workstation and server software;
- Lack of remote monitoring, access management, and patching of endpoints.

The wide range of security and non-security network issues, Brady said, added to the challenge of bringing in a new security partner after working with the previous MSP for almost three decades. “With so much going on, there was also the institutional gravity to not make necessary changes,” he explained. As it has done for a wide range of public and private clients, Neoscope seamlessly integrated its people and solutions suite with the immediate needs and priorities of the City of Portsmouth.

EMPLOYING LONG TERM SOLUTIONS AND PRACTICES

Neoscope signed an initial three-phase, 9-week contract to integrate the multi-vendor plan and oversee Emotet elimination. It was the first step to put the system back on a healthy, sustainable track. Tim Martin said Neoscope carefully handled the “emergency” situation quickly.

“It was an IT environment with more than 20 years of accumulated obsolete assets (hardware and software) and processes that needed to be updated and refreshed,” Martin explained. “In this cyber threat environment, you need multiple layers of security and unfortunately for the City of Portsmouth, in the current threat landscape they had too few layers and too many of holes. Our first task, which we completed within three weeks, was to contain and eliminate the virus and while also reducing the risk of reinfection at the city.”

Neoscope put personnel onsite daily to implement its solutions. Additionally, a 15 point program including DNS protection, phishing protection and most importantly, a cybersecurity awareness training program for all employees.

PROJECT ASSESSMENT

“I know and appreciate what they’ve done,” Brady explained. “There was so much going on and the transition of everything like server replacement went pretty smoothly. Working with Craig Taylor, we get great reports and ticketing response, and have a better understanding about what’s happening. Their cybersecurity training to assist end users has already paid off. We’ve had four to five instances of people flagging suspicious email and one in particular telling me they remembered the training video.”

“With our focus on cyber security, we have learned by listening to and working with our clients that in many cases people don’t know what they don’t know,” Martin said. “Security solutions are much easier to use and employ when everyone in an organization is rowing in sync.”

FOLLOW UP

A few months after the original contract, the City of Portsmouth signed a contract to continue the Managed Security IT partnership. The City of Portsmouth has benefited from a flat-rate, predictable IT for short- and medium-term IT planning. The contract included Neoscope’s standard of fully-staffed IT for helpdesk support and 24x7 critical infrastructure support. Additionally, Neoscope has monitored and managed the following items:

- Servers
- Routers/Switches
- Firewalls
- Wireless
- Desktop Computers
- User Support
- Vendor Management
- Documentation Services

“The city of Portsmouth has been able to focus on its core missions to serve the public without the burden of managing IT and security,” Martin said. “We want to see every firm manage their technology with best practices, kept their data secure and their employees educated. We believe City of Portsmouth’s network security has evolved further during the past ten months than in past 20 years and we are proud to be their partner in that endeavor.”