

# The Virgin Islands Consortium

## V.I. Government Vulnerable to Cyber Attacks As Only 2 Percent of Employees Are Trained by B.I.T. in Identifying Phishing Scams

Government / **Published On July 09, 2021 06:48 AM /**

Kyle Murphy **July 09, 2021**



Cybersecurity is one of the most pressing issues facing governments and companies alike worldwide, and attacks “happen every day” in the Virgin Islands, according to Rupert Ross, director of the V.I. Bureau of Information Technology, speaking during a Senate hearing Thursday. Mr. Ross also revealed that only 2 percent of government employees have received training from B.I.T. to avoid phishing scams.

Senator Marvin Blyden, chairman of the Committee on Housing, Transportation and Telecommunications in which Thursday's hearing was held, said it was important to

"understand the security of digital data and of computer and telecommunication networks."

He used examples of cyber attacks ranging from when over \$2 million [was allegedly from the Water and Power Authority locally](#), to international events such as Russian cyber criminals' forcing over 800 supermarkets to close in Sweden last weekend.

Mr. Ross was asked by the committee chairman whether he had identified cybersecurity deficiencies in the government and what was the greatest vulnerability. "There are a lot of vulnerabilities in the cybersecurity of the Virgin Islands... one of our biggest problems is the segmented way we go about trying to secure our systems and people... If I'm supposed to point to one big item, the culture of security has not really permeated our enterprise," he said.

Mr. Ross said B.I.T. has been trying to rectify the matter, leading Mr. Blyden to question the training efforts of B.I.T. and whether those efforts included the avoidance of phishing scams and other cybersecurity risks.

Mr. Ross explained that B.I.T.'s training process "goes through the baseline setting where we send out simulated phishing emails." He said this strategy helps B.I.T. identify individuals that are "most susceptible."

Mr. Ross also revealed that to date only 2 percent of V.I. gov't employees have been trained to detect attacks, bringing into focus the long road ahead even as attacks become more sophisticated.

Senator Samuel Carrion asked Mr. Ross whether there were any cyber attacks since he started his position. "I don't want to scare anyone but cyberattacks happen on a daily basis," he said. "I wish I could tell you differently but the answer is yes."

Mr. Carrion sought to learn whether there was any way to determine the magnitude of an attack. Zakee Abdurrasheed, B.I.T. chief information security officer, explained, "We rate or gauge the different escalation levels or protocols for any cyber incident regarding their impact or scope. We have a low, medium, and high impact level and we have a low, medium and high scope and then based on those they fall into a tier ranking." Mr. Ross revealed that the territory has been affected by both medium and high-level attacks in the last two years.

Mr. Ross later proposed a solution that could curtail cybersecurity problems in the Virgin Islands. "What we need to do is we need to establish enterprise operations and work with agencies to relinquish some of their responsibilities as it relates to I.T., so that we can be able monitor their equipment and identify when those equipment have problems."

Senator Novelle Francis said the question's not if but when, "because every single day there are individuals out there really navigating the cyber and just looking for ways to hack, impede or jam the system."

Mr. Francis then asked Mr. Ross how many attacks have occurred on the government network. "We track about five million pieces of information a day... I would say that on a regular basis we get about 12 alerts a week," he responded.

Senate President Donna Frett-Gregory sought answers on whether the government had secured cybersecurity insurance. Mr. Ross said the government had not, at which point she urged him to explore the options. "I would strongly suggest that the government look into the cost of cybersecurity [insurance], particularly for the agencies that impact the most," she said.