Secretly unsecure

Why companies stay silent when hit with big-time cyberattacks

BY SABRINE BRISMEUR
Cooper City High School

A global cyberattack hit a company in Miami's main cargo port last month. Beyond that, the details begin to thin.

Microsoft accused a Ukrainian software firm of being the primary source behind the attack, but nothing is certain. The hacking tool might have belonged to the NSA, but the government hasn't issued a statement confirming it.

Perhaps the virus has a kill switch, but no one knows for sure. And if they do, they're not talking.

One of the businesses hit was South Florida Container Terminal.

"The company's systems had not been upgraded for a while before the attack, which is not unusual," said Don Wrinkle, a PortMiami representative. "Going forward, they will have to bring up the old system before being able to update their software. But the company is working on changes to improve their security now."

The affected company itself, however, was not so forthcoming with information concerning the attack. South Florida Container Terminal is a partner of APM Terminals and a subsidiary of A.P. Moller-Maersk out of Denmark. APM Terminals acknowledged – sort of – that its Florida partner was the victim of a cyberattack.

"It is still too early to determine the impact," said Thomas Boyd, APM director of external communications, in an email. "Right now we are focused on our terminal operations and keeping cargo moving."

Boyd did not respond to a request for a follow-up interview. South Florida Container Terminal likewise declined an interview request. And Miami Police. In fact, PortMiami's public-spirited response was an anomaly.

A pattern was developing. When it comes to cyberattacks, facts are hard to come by.

"A lot of information about cyberattacks is kept private and hidden from the general public," said Christopher Sanchez, cybersecurity consultant at Enterprise Risk Management in Coral Gables.

But considering that Florida is the third most vulnerable state to such infiltrations, a better understanding is becoming increasingly essential.

Florida is a hotspot for cyber crime because of its lack of state income tax, transient population and vulnerable senior citizen population, according to John Breyault, vice president of the Consumers League.

"We are somewhat responsible ourselves – our own behavior – for leaving ourselves open this way to cyberattacks," said Burton Rosenberg, a University of Miami computer science professor.

"It's always people. In the end, it's always people."

But while individuals might be somewhat responsible for leaving themselves vulnerable to cyberattacks, companies certainly aren't helping them learn about better security measures.

Albert Caballero, director of information security at HBO Latin America, is under a typical non-disclosure agreement that prevents him from discussing specifics about his company's cybersecurity.

"I can certainly discuss the general types of technology we use," he said. "I can't give you product names, however."

Kerry Enfinger, an "ethical hacker" and the owner of White Hat Defenses in South Florida, specializes in vulnerability assessments. He said that by implementing policies that prevent employees from discussing cybersecurity, companies protect themselves and their image.

For the public, though, keeping quiet about attacks prevents people from learning more about their own vulnerabilities in cyberspace and, more important, how to protect themselves.

"The least amount of information you give – no information – is the best," Enfinger said.

But other cybersecurity experts don't always agree on the reasons for the secrecy.

"Don't let people tell you they're silent about cyberattacks because it keeps them safe," Caballero said. "They want to save face and they don't want people to know they've been hacked."

Ambiguity with the public also serves as a cover-up for outdated security systems and faulty software. For many, an attack could have been avoided by updating software immediately or by training employees to exercise caution when receiving emails with links or files, security experts say.

"Usually, if [companies] don't want to give out information, it means they're lax," Enfinger said. "And they don't want you to know how lax they are. I'm sure their policy states they can't give out that kind of information, too, but it's been proven over and over by the types of attacks that most companies are less than secure."

Rosenberg agreed.

"It's hard to get facts. An institution that has been hit by a cyberattack is not very anxious to talk about it in detail… It's very sensitive and difficult to get to the bottom of things."

For many South Floridians, company disclosure will remain far more obscure for the foreseeable future.

"You're never going to get that type of information out of companies," said Enfinger. "They just won't talk."



Photo by Alley Robertson

HARBOR HACK: A container company in PortMiami is recovering after a devastating cyberattack.