Expert walks Worcester through the economics of internet secrets

SAM BONACCI

Aaron Portnoy addresses the Worcester Economic Club Wednesday.

In the world of cyber security, an entire industry has materialized around selling information about vulnerabilities in programs, alternately offering the ability to protect against these flaws in the programs and allowing them to be used as cyber weapons.

"You can make a significant career out of this," cyber security expert Aaron Portnoy told the audience at a meeting of the Worcester Economic Club where he was a guest speaker Wednesday night. "The market is blowing up."

Throughout any computer program there are vulnerabilities, which like tunnels under the castle walls, open up the program and its users to threats from the outside. When a company or individual discovers these vulnerabilities, they can use them, sell them to a high bidder or kindly inform the program's creator. Portnoy, who attended Mass Academy and got into trouble for hacking WPI's system while attending the high school attached to the college, has

made a career, and now business with his company, Exodus Intelligence of Austin, Texas, in trading in these secrets.

"I actually hacked WPI twice, they only caught me once," Portnoy said in a first-time public admission.

In the early 2000's, these vulnerabilities had little value other than boosting a kind of internet street cred for the finder, but as more vital information has been put on the internet, the value has jumped with some individual vulnerabilities in major programs being valued at over $1 million to the right, if not always moral bidder.

That is where ethics come into the equation, said Portnoy. When someone finds these ways into a program, they can choose to sell that knowledge to governments (which rest at the top of the internet hacking food chain), the company that created the program or one that that will sell it back to that company, or hackers on the black market.

"By far the highest bidder is still governments," he said explaining that they will not inform the creators or programs but exploit them.

Governments and agencies like the Federal Bureau of Investigation will use these vulnerabilities for espionage – such as Stuxnet where the U.S. and Israeli governments allegedly attacked Iranian nuclear facilities – or to track down criminals. Other countries, including Russia and China, are alleged to be involved in cybercrimes against companies and individuals in the United States, Portnoy said. Those allegedly working on China's behalf have been targeting U.S. companies including Apple, Google and Lockheed Martin to get trade secrets to avoid investing in the research and development themselves, he said.

"They are targeting health care, pharmaceuticals – anything of economic value," Portnoy said. "They are going for economic espionage."

This has led to an increasing need for businesses to focus on security, he said. Internet criminals are not just going after money, the protection of which is actually highly regulated, but those trade secrets. The larger the business, the larger a target they become, he explained.

The response businesses must take depends on what kind of information they deal with, as well as what resources they can put into security, he said. Banks and other financial organizations are highly regulated, but for other industries it depends on each company. There are consultants that will come in to help set up security, but it is something most companies should be thinking about, even if they decide to outsource their security, Portnoy said.

There is very little regulation around the sale of vulnerabilities right now. The Wassenaar Arrangement has been adopted by most countries and includes a list of 26 countries not to sell to that include Iran and North Korea. His company also consults with military and government contacts to determine whether potential buyers may be selling to these countries. Much of this is left up to the individuals or companies at this point, though. Portnoy expects

legislation to come forward that may regular these secrets like the dangerous things they can be.

"These things that are being developed are digital weapons," he said.

Portnoy's entire speech will be available on the Worcester Economic Club website. The organization has upcoming speakers that include Robin Chase, the co-founder of Zip Car, and Stephen Dubner, the co-author of Freakonomics.

Source: wbjournal.com