Washington Lawmakers Take Aim at Cybercrime with Washington Cyber Crime Act

Julia McCandless | January 11, 2016

As technology continues to race ahead, many are struggling to keep up — including lawmakers. That's why two lawmakers in Washington proposed new legislation last week to defend against current cybercrime and swiftly prosecute cybercriminals in their state.

The Washington Cyber Crime Act, which Rep. Chad Magendanz and co-sponsor Rep. Tina Orwall plan to introduce in the 2016 legislative session, recognizes new categories of cybercrime that are not currently covered under law, including tampering, spoofing and "denial of services" attacks. The proposed bill also extends prosecution to individuals who copy or transmit data with the intent to commit a crime, but leave the original in place or unaltered.

As a former Microsoft employee, Magendanz is a seasoned expert in identifying and preventing cybersecurity threats. In fact, he was a key player on the Microsoft Security Development Lifecycle team, which developed the STRIDE Threat Model across six categories, including spoofing, tampering, repudiation, information disclosure and elevation of privilege.

His deep-rooted knowledge of cybercrime led Magendanz to push for stricter legislation that effectively targets true criminals.

“For many years, I’ve had this frustration that members of the Legislature are chasing the latest technology and then putting restrictions on its use to prevent criminal behavior,” he said. “ Behavior is what’s criminal, not the technology itself.”

Magendanz said he hopes that the Washington Cyber Crime Act will eliminate barriers for law enforcement and create a clear path to defend against diverse cybercriminals.

“It’s going to allow prosecutors to go after these criminals before they’ve stolen the data,” he said. “Giving them that window of activity is a huge advantage.”

For end users, he added, that will likely result in quicker response times and lower rates of cyberattacks.

While technology experts like Magendanz have long been aware of cybercrime, he points out that this year has been eye-opening for the general public and has put a spotlight on the importance that cybercrime holds in our nation.

“People are much more aware this year than they have been in any previous year,” he said. “Especially when you get a major company like Sony, or governor’s races that impact taxpayers with data breaches. It seems like there’s always a new breach in the private sector as well.”

So why the uptick in recent cybercrime? The short answer: money.

“The numbers tell the story; data is a lucrative target for criminals,” Magendanz explained. “This legislation would protect consumers and companies by helping the courts prosecute these cybercrimes.”

Though it’s clear that legislation will need to continually grow and evolve with technology to defend against cybercrime, Magendanz said he hopes the proposed bill will inspire positive change in the way we manage cybercrime in the future.

“This is just a first step of a larger process of raising awareness of cybercrime and giving law enforcement the tools they need to aggressively defend our data,” he said. “Looking ahead, this is the new battlefield, and it’s affecting all of our infrastructures. We need to staff up the defenders of our infrastructure in the same way we do with our military. The first step is raising awareness and giving basic tools. Then we have to make an investment to follow up.”

http://www.govtech.com/security/Washington-Lawmakers-Take-Aim-at-Cybercrime-with-Washington-Cyber-Crime-Act.html