Guidepost

THE RANSOM IS THE LEAST OF YOUR WORRIES

Wannacry is the latest herald of cyber-Armageddon. Countless computers all over the world were rendered useless. Data became encrypted and unavailable. Pay the ransom or kiss your data goodbye forever was the threat.

Wannacry spread around the world very rapidly, affecting service companies, manufacturers, national healthcare systems, governmental agencies and individuals. By one report, the perpetrators of Wannacry have earned about $50,000 through their ransom demands. This is not a huge payoff, but it may be enough to provide an incentive to copycat attackers.

Of course, this is not the first such incident. Just over a year ago, a hospital in California learned a hard lesson when staff lost access to the network during a ransomware outbreak. The hospital paid the $17,000 ransom after employees spent 10 days relying on fax machines and paper charts. Several digitally connected police departments in Maine fell victim to a phishing scam in April of 2015 and paid a ransom of $300 to regain access to encrypted arrest and incident records.

The truth is, despite all the turmoil and real danger created by Wannacry and its predecessors, we will survive it. The bigger question is whether we will learn anything from it. Discussions about what group launched it, who is at fault for the code, and how did it spread make great fodder for news stories, but are ultimately just diversions from the real issue. Wannacry was completely preventable. The real story here is how were we so unprepared.

Lost in the commotion are familiar prescriptions for good cyber hygiene. Use licensed and supported software. Install updates. Back up your files outside of your network. Be alert for suspicious emails.

More generally, Wannacry is the current wake-up call for everyone's need to periodically review their cybersecurity profile. Despite the ever-increasing necessity to improve security, entities of all kinds continue to fall victim to the same attacks. Whether an unwary recipient clicks on the wrong email attachment, or gets lulled into a false sense of security by a prolonged social engineering ruse, the result can be the same: data stolen, encrypted or otherwise compromised.

No business can afford to lose access to its data for long and survive. When the compromised data belongs to a healthcare provider or law enforcement agency, the health and safety of the public can be at risk. The stakes simply

cannot be higher. Cyber security assessments must become as standard a procedure as the annual safety inspection for your car.

If you do fall victim to a ransomware attack and you cannot restore your system from a backup, you do have options. Although new ransomware appears every day, the decryption keys for many of them are known and available through law enforcement or security vendors. You can consider paying the ransom if you determine there are no other viable options, but when you do, you are trusting the integrity of the attacker to provide you with the key. Even if he does, attackers have been known to share the identity of their victims and the means of their successful attack to cohorts in return for a percentage of the next ransom payment. After all, you have already demonstrated your vulnerability to attack and your willingness to pay.

Plan in advance, incorporate a ransomware scenario into your Incident Response Plan so you know what to do if your defenses fail.

JOHN TORRES

President, Security + Technology Consulting

John P. Torres is the president of the Security & Technology Consulting practice for Guidepost Solutions. John has extensive investigative and security experience. Previously, he served as the Special Agent in Charge for Homeland Security Investigations in Washington, D.C. and Virginia. His background includes more than 27 years of experience providing investigative and security management for the U.S. Departments of Homeland Security and Justice, including serving as the Acting Director and the Deputy Director of U.S. Immigration and Customs Enforcement.