Coping with Cyber Extortionists

No company is immune to ransomware attacks that seek to shut down operations and blackmail its victims. **BY PATRICIA KOCSONDY**

The recent wave of ransomware attacks like WannaCry, Goldeneye and NotPetya has turned commonly held assumptions about cyber risks and security upside down.

There are three big assumptions that media companies need to rethink, in particular.

***Assumption No. 1*:** "My business is only a target if I store information like credit card or health data that may be financially valuable to a cyber criminal. Our company doesn't really hold much of this data."

This assumption presumes that media companies lack data of interest to cybercriminals, which is not the case. Valuable material such as content, newsgathering sources and information about employees (especially high profile personalities) is susceptible to extortion tactics.

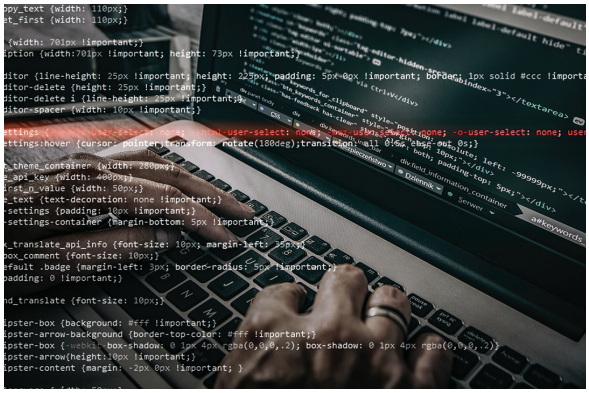
Secondly, cybercriminals understand that for a company to succeed, it must operate and serve customers on a regular basis – without business interruptions. They know that media companies are dependent on advertising and/or subscriptions, and they are financially affected if infrastructure related to either of those revenue streams is locked down.

To unlock it and resume operations, the demand is usually negligible – just a few hundred dollars, payable in an anonymous cryptocurrency like Bitcoin. For many companies, payment is often the path of least resistance.

***Assumption No. 2*:** "Cyber criminals attack only large, high profile companies. My business is too small and not well known enough to be a target."

Ransomware is indiscriminate, and the malicious code exploits vulnerabilities in all company networks – large, small and in-between. Within a day, WannaCry infected more than 230,000 computers in over 150 countries, according to ScienceAlert.com. While news reports focus on large or well-known corporate victims, countless smaller businesses are regularly attacked. Most lack the financial resources and expertise to implement high-level cybersecurity measures, which makes them susceptible to attack.

***Assumption No. 3*:** "Investing in cybersecurity is important to us, but not as important as other pressing needs, like growing the business. We feel we can hold off for the time being."



While news reports focus on large or well-known corporate victims, countless smaller businesses are regularly attacked.

Midsize and smaller media companies cannot afford to postpone cybersecurity investments. Even a brief business interruption can cause brand and reputational damage. Advertisers or subscribers may think twice about doing business with a company that appears unable to stay on the air or go to press on time.

To limit the risk of a ransomware attack, basic cybersecurity "best practices" are advisable. They include keeping software current; effective patch management; firewalls; daily offsite data backup, and network segmentation (establishing barriers between stored data files to block intrusion).

Regrettably, even the best technology-driven security measures can easily be undermined by employee mistakes. Hackers sometimes infiltrate networks by cracking passwords and/or phishing – inducing an employee to click on an infected e-mail link. Proper password hygiene (sophisticated passwords regularly changed) and training employees to recognize and report suspicious e-mails are a must.

Simply paying the ransom does not end the crisis. The decryption software may unlock only a portion of the infected data. There's also the possibility of no decryption key – the case with WannaCry.

Nagging questions in the aftermath of an attack are common: How did the cybercriminals get into the network? Did they see or take confidential information? Are they *still* in the network? Could this happen again? Must we inform advertisers, subscribers, customers, business partners and/or regulators about the attack?

Resolving these questions usually requires the assistance of a forensic investigator, legal counsel and crisis management consultants. These specialists can determine which systems and files have been accessed or corrupted. And they can assess the legal ramifications.

Specialists can also contain the media fallout through public relations support, helping to establish a call center as well as credit monitoring and identity restoration services. Among those who specialize in such services are cyber insurers.

The U.S. Department of Justice reports there were 4,000 ransomware attacks per day in 2016. All companies should take the threat seriously.

Patricia Kocsondy is senior vice president, North America financial lines, and a media professional liability product manager at Chubb. She can be reached at patricia.kocsondy@chubb.com