New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 258—NO. 40
MONDAY, AUGUST 28, 2017

Outside Counsel

Expert Analysis

Cyber Ransoms: Mr. Smith Attacks HBO's Loot Train

By **Thomas G. Rohback**

And **Brooke Oppenheimer**

The recent cyber-attack on HBO should be a wakeup call to both businesses and insurers. While the amount sought by the hackers called "Mr. Smith"—roughly $6 million in bitcoin—is not a huge amount for HBO, it is significantly more than the amounts that have typically been demanded in recent cyber extortion demands. Over the last two years, the average ransom amount demanded in ransomware attacks was only between $100 and $2,000. Accordingly, approximately 70 percent of all ransomware demands have been paid. Datto, "Datto's State of the Channel Ransomware Report" (2016).

While underwriting for many aspects of cyber insurance faces significant challenges—particularly since many data breach cases and claims thus far have foundered on the lack of standing or actual damages where personally identifiable information (PII) has been accessed but not used—ransomware attacks have been substantially under-reported. Id. Ransomware attacks involve introducing a software into a company's computer system that allows data to be temporarily encrypted (and made unusable) until a ransom demand is paid. Absent faulty technology (or fake ransomware), the data is typically only exfiltrated, deleted or destroyed if the ransom demand is not met. In the past two years, the volume of ransomware-infected email has increased by 6,000 percent resulting in more than 1.5 million systems being infected with ransomware. Limor Kessem, "Ransomware: How Consumers and businesses value their data," IBM Security (Dec. 14, 2016). But the relatively modest ransom prices have been quickly paid, thereby making this payment appear more like a cost of doing business rather than an event requiring an insurance claim to be filed. In terms of business interruption, the duration of interruption is relatively short, and coverage periods do not necessarily begin at the first moment a system is shut down. The average small business loses $8,581 for every hour of downtime

> For businesses and their insurers, either ransoms will be paid or the hackers will be stopped. Either way, "Winter is coming."

THOMAS G. ROHBACK *is a partner and* BROOKE OPPENHEIMER *is an e-discovery attorney at Axinn, Veltrop & Harkrider.*

with the average minimum downtime being two days. Robert Bready, "Downtime and Data Loss: How Much Can You Afford?," Aberdeen Group (August 2013). Yet, less than 25 percent of businesses even report the incident, let alone file an insurance claim. Datto, "Datto's State of the Channel Ransomware Report," (2016). Even though the highly publicized "WannaCry" attack hit more than 200,000 computer systems in May and June, many insurers failed to notice any significant change in cyber claims. Advisen, "WannaCry ransomware virus has little effect on demand for cyber insurance in the UK, says survey," citing Insurance Newslink; Iann Sherr, "WannaCry ransomware: Everything you need to know," CNET (May 2017).

But the HBO attackers did not encrypt the data so that it became unusable until a ransom was paid. They took the data (among other things, the script for an episode of Game of Thrones) and then threatened to release it (and much more). Here, unlike the typical, low-cost high-volume ransomware attacks of the last couple of years, these hackers invested a great deal of time and money gaining access to the data prior to making any ransom demand; and their demand of a greater amount reflects that investment. While the Sony data ransom of 2014 created a stir, it was viewed as a costly aberration: a politically motivated attack by a rogue regime. There, no ransom was sought; it was retribution, pure and simple. Likewise, the Ashley Madison demands of 2015 were apparently motivated by ethical concerns. With the HBO incident, the apparent motive is money, bringing these hackers into the more traditional mode of cyber-crime.

With more than $4 billion in premiums from written cyber policies to date, insurers are aggressively marketing cyber insurance policies as a "comprehensive" approach "to protect against all your cyber needs." See *P.F. Chang's China Bistro v. Federal Insurance Company*, 2016 WL 3055111 (D. Ariz.). Ransom attacks often trigger either the cyber-extortion or network interruption portions of these "comprehensive cyber policies." Cyber extortion coverage generally focuses on the costs of (1) assessing the credibility of a ransom demand, (2) obtaining cryptocurrency (e.g., Bitcoin, Ripple), and (3) paying the ransom. Since most attacks are resolved promptly, the loss covered by business interruption insurance is generally limited. With coverage waiting periods ranging from 12 hours to 48 hours on average, roughly half the attacks will not result in payments from the policy.

But, as both the HBO and WannaCry attacks suggest, substantial business losses are possible, and these potential losses present the underwriting challenge and the litigation risk. For example, Amazon reported that it would lose $60,000 a minute if services were stalled. Kelly Clay, "Amazon.com Goes Down, Loses $66,240 Per Minute," Forbes, (Aug. 19, 2013). Though some policies reduce the waiting period to four hours, significant damage can result in this period. Presumably, insureds could bargain for a shorter waiting period, but that would come with a price, just as a lower deductible would result in higher premiums. Moreover, even if a cyber policy provided a large amount in total coverage, the business interruption coverage might have a far lower sublimit. Therefore, there may be some disconnects between the expectations of the insured and the terms of the policy.

In the case of HBO, it may be that there is no covered business interruption; i.e., HBO can still put on an episode of Game of Thrones, even if the script has been disclosed in advance. Likewise, the business might not be interrupted if embarrassing emails of top HBO

executives are published, as was the case in Sony, even if there are other types of business losses incurred.

Cyber ransom attacks capture the public's attention when the fate of mythical fire-breathing dragons hangs in the balance, but what about human lives in the event of a ransom attack on a hospital? These have occurred, and fortunately the ransoms were not exorbitant and were quickly paid. Russell Brandom, "UK hospitals hit with massive ransomware attack," The Verge (May 12, 2017). But what will happen if the ransom becomes enormous and the lives of patients are at risk? The consequences go beyond the scope of business interruption insurance, and bodily injury is frequently excluded in cyber insurance and business interruption insurance. The implications for liability from third-party negligence claims, as well as shareholder and regulatory litigation are staggering in the event that a hospital or any enterprise that provides critical services—not simply entertainment—is shut down for some period of time.

Insurance offers a variety of coverage options for business interruption, release of PII, theft of trade secrets, extortion, cost of identifying and repairing a network exposure. Extortion coverage might cover the amount of the ransom to be paid, but it might not cover the business losses resulting from the disclosure. Likewise, the policy might cover the amount of the ransom, but if the insurer offers to pay the ransom, while the insured refuses to accede to the extortion, there may be no coverage. Insurers and insureds will have to look closely at the changing landscape to determine whether a particular attack is covered, and whether there are quantifiable and recoverable damages directly caused by an attack.

Just a few days ago, HBO reported through its partner, Star India Private Limited, that four individuals associated with Prime Focus Technologies were in India arrested in connection with the attack. Steven Trader, "HBO Partner Says 4 Arrested for 'Game of Thrones' Leak," Law360. (Aug. 15, 2017). Although these hackers were identified and apprehended quickly, that may be of little practical benefit if the hackers lack the resources to satisfy a judgment to reimburse the hacked company for its losses. Unlike the theft of tangible property or cash (which in many cases can be recovered once the criminals are caught), the publication of confidential information or trade secrets is not something that can readily be undone. Moreover, these four may not be the only individuals who have participated in the cyber-attack on HBO. Id.

Taking a stand, HBO has announced that it is not going to negotiate with the cyber-terrorists who have allegedly stolen up to 1.5 terabytes of data from HBO. Lifars, "HBO Refuses to Pay Hackers as Leaks Continue," Lifars. (Aug. 14, 2017). In many instances, law enforcement would urge hacked companies not to give into ransom demands; in choosing to fight, however, those companies incur the financial damage of prolonged business interruption or losses stemming from the disclosure of commercially valuable, confidential information. For businesses and their insurers, either ransoms will be paid or the hackers will be stopped. Either way, "Winter is coming."