Licensing and Copyrights
copyright@americanbar.org

ABA Publishing
321 North Clark Street
Chicago, Illinois 60654

Periodical Author Permission Grant
Permission is granted for reprint of the final printed version of the article subject to the terms and conditions below:

Terms

- Permission is granted free of charge.
- If any material in the work has been licensed by another source, authorization from that source must have already been obtained or must be obtained.
- Usage does not include the right to license the final printed version of the article, individually or as it appears in the publication, or to grant others permission to photocopy or otherwise reproduce the final printed version.
- The ABA requests that, if and when you republish, you credit the ABA publication in which your article first appeared and include the article title and the name of the ABA publication, including volume, issue, and date, and the copyright notice as it appeared in the ABA publication. E.g.:

  "©2016. Published in The Business Lawyer, Vol. 71, No. 4, Fall 2016, by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association or the copyright holder."

- If the PDF already contains the reprint line, please leave as is.
- Use of the final printed article is granted on a non-exclusive basis and is valid throughout the world in the English language only.
- Permission is granted to make versions for use by blind or physically handicapped persons, provided that no fees are charged.

Uses

- Article may be posted to author's law firm or organizational web site.
- Article may be included in author's print or electronic law firm or organizational newsletter.
- Article may be posted to SSRN.
- Author can provide a link to the article on the ABA website. Please keep in mind that many of the ABA's publications are password-protected and cannot be accessed by non-ABA members.

Responding to the not so hypothetical cyber incident

Claudia Rast

Claudia Rast is a shareholder at Butzel Long in Ann Arbor, Michigan. Ms. Rast is a past-chair of the Section and current member of the ABA Cybersecurity Legal Task Force.

Whereas few haven't read, or at least been warned about, the threats posed by hackers and the malware they plant, less common are the stories told from inside the cyber incident as it unfolds. Of particular interest to the SEER lawyer is a recent *Wall Street Journal* article warning of hackers targeting U.S. public utilities. R. Smith, *Cyberattacks Raise Alarm for U.S. Power Grid*, Dec. 30, 2016, Wall St. J. (describing how hackers remotely disconnected circuit breakers until an electrical substation in Ukraine was completely disabled). This article will describe a hypothetical cyber incident with the hope of accomplishing two goals: first, illustrate what the mayhem—and it can truly be mayhem—is like when the cyber event occurs and, second, outline the series of scalable best practices that small- to medium-sized organizations can incorporate into their day-to-day operations to mitigate such an incident when one happens.

The early stages of the "hack"

During the test of a company server, an employee modifies certain server settings. One of those settings allows open access to the Internet. At the conclusion of his work, the setting is not closed. The now open Internet-facing server becomes vulnerable to an opportunistic malware attack that moves through the company's firewall and into the company's IT network, where it plants itself, unseen and undetected. **Note:** *The company's firewall has no geolocation blocks in place, there is no intrusion detection and prevention equipment, and the anti-virus software has not seen this particular malware before.*

The malware includes both the ransomware virus and a "backdoor" agent. This is common: The ransomware virus provides an immediate attack threat by encrypting the target company's data and demanding bitcoin currency before it will send the decryption keys. It is also a diversionary tactic. The ransom—if paid—gives the hacker a quick payday. Meanwhile, the backdoor agent can lie dormant, and often undetected, providing a means for the bad guys to get back into the company's network.

The ransomware virus takes hold

The ransomware traverses the IT environment, encrypting servers and work stations as it goes. An early shift employee notices the immediate effect as the tell-tale screen announces that his data is now inaccessible and encrypted, and a count-down clock posts a 24-hour deadline to meet its bitcoin demand. The employee notifies the IT department, which notifies company management. Both the state police and the FBI are called. IT staff attempt to clean and rid the

Published in Trends May/June 2017, Volume 48, Number 5,

unencrypted areas of the network of any trace of the malware. **Note:** *While the instinct may be to bring in one or more enforcement agencies right away, this can be a mistake. This decision should be made in consultation with an experienced cyber attorney. Further, the company needs to forensically collect and preserve relevant evidence before steps are taken that will eliminate or taint it. Without functioning communications (e-mail or fax), the logistics of negotiating the engagement of cyber counsel and a forensic team can be difficult. With an Incident Response Plan in place, this is pre-negotiated, and cyber counsel can be onsite and available immediately. In addition, the Plan will have pre-vetted forensic experts so that there are no delays in getting a team on the ground and assessing the situation immediately.*

Show me the "bitcoins"

Conducting a bitcoin transaction while working against a countdown clock and communicating with an anonymous hacker who revels in the idea of creating mayhem is unnerving at best. Bitcoin ATM locations are not found in safe locations such as next to police stations or near well-trafficked shopping areas. The transactions are performed by feeding cash to the bitcoin ATM, where the cash is deposited in the account of a pre-negotiated intermediary willing to sell bitcoins (for between $400 and $1100 per bitcoin). The newly purchased bitcoins are then transferred to the hacker's "wallet." This may be only the first of several transactions, as the hacker will hold back some encryption keys for more bitcoins and the company must test the decrypt keys to make sure that they work. Having thousands if not tens of thousands of dollars in cash available for such a transaction and taking it to a not-so-pleasant neighborhood in the early morning should be planned in advance. While bitcoins are a digital currency, their purchase often requires a trip to a physical ATM, thus being accompanied by security is advisable.

Next time: The Incident Response Plan

Asset Inventory. One of the more tedious, time-consuming, and vitally necessary activities in the wake of a cyber incident is the inventory and assessment of all devices that may have been connected to the infected network. (Of course, it doesn't help if both the network diagram and the device inventory are on the encrypted network and unavailable.) Thus, the Incident Response Plan should be updated regularly and be available in a physical, written format.

Legal Obligations. A designated "Incident Commander" and the executive team should consult with counsel about whether there are sufficient indicators to notify external authorities. Certain industries (energy, health, financial, etc.) have regulatory control and notification requirements depending on the nature and type of digital records or processes that may have been compromised. Industry records show that when reported too early—before the forensic team is satisfied with all the details necessary for an informed report—companies pay more per compromised record than those companies who wait to make a more informed report. In cases involving data breaches, state statutes generally allow for investigative time, with an average

requirement of 30 days or so from the date when the breach was determined. State notice triggers and filing requirements vary widely, so it is vital to determine early on what types of records might have been compromised, where the owners of these records reside (state law governs) and how many of these owners reside in each implicated state. Further, calling the state police or FBI before the forensic team has a chance to collect and preserve relevant data makes it difficult, if not impossible, to correctly identify "patient zero" or to determine what digital records are involved. (Commonly, the source individual within a company that the hacker successfully targeted. Finding the patient zero is a priority that can lead to better understanding of how the hacker gained entry.) Thus, gather facts quickly and carefully and know in advance the underlying laws implicated by the results of the hacker's activities.

Notice to Insurance Carrier. For those companies with cyber liability coverage, it will save much time later if the impacts and consequences of the incident are sorted out early on according to the carrier's coverage requirements. Keeping track of impacts—and resulting damages—may be important to later claims in litigation if the hacker is identified and subject to jurisdiction in the United States. Sadly, this is infrequently the case. Thus, it is advisable to consult with the company's insurance broker and cyber counsel on these coverage issues.

The likelihood of something similar to the above-described scenario happening to one of our clients/companies is high. The best advice is preparation: assess the risks, protect the assets, implement a response plan, and have knowledgeable counsel at the ready.