What Should You Do When You're Hit by a Cyberattack?

By John M. McNichols, *Litigation News* Associate Editor

Prompted by the Russian invasion of Ukraine, the Biden administration recently warned of "evolving intelligence," that the Russian government was exploring options for potential cyberattacks against the United States. While U.S. military departments and federal intelligence agencies might seem the most likely targets for such attacks, the president made clear that no one is immune and that attacks on certain private businesses—banks, for example—could be just as damaging to U.S. infrastructure as an attack on its military. Accordingly, he urged all private companies, large and small, to harden their cyber defenses by implementing the "best practices" of the "Shields Up!" initiative of the federal Cybersecurity and Infrastructure Security Agency.

Left unanswered, however, is an important question: What happens if a company, despite taking all reasonable precautions, finds itself the victim of a cyberattack that puts at risk not merely the company's own private data but that of its customers as well? At present, there is no generally applicable federal law requiring private companies to report such events so that affected persons can take protective measures.

That may change, however, and soon. In March 2022, the U.S. Senate passed the Strengthening American Cybersecurity Act, which would require that private companies report a data breach within three days. If passed by the House of Representatives, the act will complement existing state statutory law governing responses to cyberattacks and align federal law with European law under the General Data Protection Regulation (GDPR).

What Is a Cyberattack or Data Breach?

A cyberattack is broadly defined as any attempt to gain unauthorized access to someone else's computer network to manipulate the information housed there. Although the word "cyberattack" is of recent vintage, Americans' popular awareness of electronic intrusion dates at least to the 1983 film *WarGames*, in which a teenage hacker inadvertently penetrates a U.S. military base and nearly starts World War III.

Real-world cyberattacks are less dramatic, but nevertheless consequential. A hacker who obtains access to another's information can use it for his or her own purposes—as intelligence, for example—or to deprive the owner of its use through "ransomware." Infiltration methods can take many forms, the most well-known of which is the "phishing" email, which lures the recipient to click on a hyperlink that will allow the email's sender to access the recipient's system.

The most common consequence of a successful cyberattack is a data breach, which occurs when hackers obtain and then

Published in *Litigation News* Volume 47, Number 4, Summer 2022.

disclose their target's private information, as happened in 2016 when Cozy Bear and Fancy Bear, agents of the Russian intelligence services, penetrated the Democratic National Committee's system. Notwithstanding heightened awareness of such incidents and measures like the "Shields Up!" initiative, data breaches may become more common in the future as businesses increasingly transition their electronic data from self-contained servers to the externally hosted environment known as "the cloud." Despite the sophistication and preparedness of cloud service providers, data stored in the cloud may be more vulnerable than data in a company's own servers, given that nearly anyone can open an account with a cloud service provider and thereby gain access to its environment.

According to recent data from the security firm Panorays, the average cyberattack costs nearly $200,000 to remediate. While that is not a huge sum for a Fortune 500 company, it may be a crippling liability for a small business. And small businesses cannot take comfort in the idea that they are unlikely to become victims. More than 40 percent of all cyberattacks target small businesses, with law firms being a particularly attractive target given their perceived slowness to adopt cyber defense technology and the potential sensitivity of information in their possession. In 2016, the security company TruShield reported that the legal industry was among the most targeted of all industry sectors, with small law firms the most heavily targeted of all.

More than 40 percent of all cyberattacks target small businesses, with law firms being a particularly attractive target.

What Laws Govern Cybersecurity Incidents?

The legal landscape governing cyberattack responses is rapidly changing. As recently as 2017, the *ABA Journal* reported that only four states had enacted legislation requiring that information on cyberattacks be made available to residents whose personal data may have been compromised. In the five years since, nearly all states have imposed such reporting requirements when a data breach occurs. In Europe, meanwhile, the European Union adopted the GDPR, which since May 2018 has imposed a continent-wide reporting mandate in the event of cyber intrusion.

Although the United States presently has no uniform federal mandate analogous to the GDPR, new legislation may change that. The Strengthening American Cybersecurity Act is an amalgam of multiple prior proposals. Title II of the act is the most consequential for private companies, as it designates 16 categories of businesses as "critical infrastructure"—including the financial services, telecommunications, energy, and healthcare industries—and requires companies in those industries report any "substantial cyber incident" to the federal government within three days and any ransomware payment within one day. To assist the federal government's response—and to enable other companies to avoid the same fate—the act's required reporting would include, among other things, a description of the vulnerabilities exploited and the hackers' tactics to defeat existing defenses.

To encourage compliance, the act includes significant penalties for the failure to report but also prevents a company's incident report from being used against it. Among other things, information submitted pursuant to the act would be protected as proprietary information and, therefore, exempt from disclosure under public access laws. In addition, a covered entity that submits compliant reports would be entitled to immunity from civil lawsuits based on its report, and regulatory agencies would not be able use the information submitted for enforcement actions against the covered entity.

What Can Private Sector Businesses Do?

Because an ounce of prevention is worth a pound of cure, most of the protective measures outlined by cybersecurity experts are proactive in nature, in that they require taking action before a cyberattack occurs. One controlling principle is that the less information that an organization possesses, the less vulnerable it is to a breach. Hence, most experts recommend deleting data not currently in use. When that is not an option—because of company retention policies or preservation duties imposed by litigation, for example—other measures can be taken, such as applying encryption or moving data to a repository that prevents easy access. And to prevent unauthorized access in the first place, companies are encouraged to segregate and silo data and adopt two-factor authentication. But the most important step is not merely hardening defenses; it is getting a response plan in place for when an attack succeeds.

The first 24 hours after a cyberattack are critical, and any delay can be costly both in time and money. For this reason, cybersecurity experts recommend that, as part of their incident response plans, companies identify in advance the service providers who will support their remediation efforts when an attack occurs. Such providers necessarily include a computer forensics firm, but many are less obvious, such as a crisis communications firm or a ransomware negotiator. And as with all forms of misfortune, insurance is increasingly becoming a must, to cover both the remediation costs and potential liabilities to third parties whose data may be put at risk. LN

RESOURCES

- Julie Sobowale, "Law Firms Must Manage Cybersecurity Risks," *ABA J.* (Mar. 1, 2017).
- Eric Lipton, David E. Sanger & Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *N.Y. Times* (Dec. 13, 2016).
- Lamar Johnson, "CISA Tells CI Operators 'Shields Up,' Warns of State-Sponsored Attacks," *MeriTalk* (Feb. 21, 2022).
- Hunton Andrews Kurth LLP, "U.S. Senate Unanimously Passes Cybersecurity Legislation Requiring 72 Hour Cyber Incident Notification," 12 *Nat'l L. Rev.* 112 (2022).
- Andrew Serwin, Deborah R. Meshulam, Edward J. McAndrew & Leila Javanshir, "US Senate Unanimously Passes the Strengthening American Cybersecurity Act," *DLA Piper* (Mar. 14, 2022).