dbr DAILY BUSINESS REVIEW

Common Law Negligence and Ransomware Attacks: An Old Tool for a New Job

In the Cyber Age, legislative and regulatory bodies must play a perpetual game of catch-up, chasing dexterous bad actors whose evolving tactics and capabilities outpace the legal response.

By Meaghan Goldstein
November 3, 2020

Meaghan Goldstein, associate with Kozyak Tropin Throckmorton in Coral Gables. Courtesy photo

In the Cyber Age, legislative and regulatory bodies must play a perpetual game of catch-up, chasing dexterous bad actors whose evolving tactics and capabilities outpace the legal response. Victims are often left stranded in extremely vulnerable positions, seemingly without recourse. A strong and willing plaintiffs' bar may be the victims' best, or only, option for recovery.

And the lawyers' best tool is often one that already exists—common law negligence.

On Sept. 17, hackers paralyzed a German hospital with a ransomware attack, requiring the transfer of critically ill patients to another nearby hospital. Tragically, and avoidably, one patient died en route. Her death was a direct and foreseeable consequence of the cyberattack, but also of the hospital's failure to safeguard its systems. German cybersecurity authorities determined that the hackers exploited a vulnerability in the hospital's VPN software, which allowed the ransomware to enter the network.

Ransomware is a type of network attack that hijacks the targeted computer systems and re-encrypts them, denying the owner access to, and use of, stored data. Once an attack is executed, usually by embedding malware in an email or attachment, the perpetrators hold the system hostage, demanding ransom in exchange for a decryption key to unlock it. Often, the ransom must be paid in cryptocurrency, frustrating attempts to trace the payment and identify and prosecute the hackers. Academic institutions and government agencies, who typically possess large volumes of sensitive personal information, have long been popular target. But the German hospital attack exemplifies the hackers' alarming new focus on healthcare systems.

Our health care system, like most aspects of our lives, depends heavily on internet-based infrastructure. Charts, test results, medication schedules—all are online. Radiologists review X-rays and scans remotely with equipment that runs online. A hostile shutdown of internet and systems access hamstrings health care providers and administrators alike, delaying life-saving care to patients.

Hackers who disable hospitals arguably have the most powerful leverage imaginable. In a typical data breach, personal data like Social Security numbers and credit card numbers may fall into the wrong hands. In a health care ransomware attack, *human lives* are at stake, providing hackers with the ultimate collateral. A principled refusal to "negotiate with terrorists" while law enforcement attempts to hunt down the perpetrators is an unaffordable luxury. By the time the ransom is paid and decryption keys are handed over, patients and health systems have suffered damages that, in some cases, are irreparable.

The attack in Germany is far from an isolated event. Last week, Universal

Health Services (a network of more than 400 health care centers) was held hostage by ransomware, forcing a temporary return to paper-and-pen records. Of course, paper records lack all of the instant cross-checking, real-time updating, and portability upon which modern hospitals rely to provide appropriate and timely care.

Similarly, earlier in September, one Cleveland-area hospital was forced to postpone all elective surgeries in order to concentrate resources on the most urgent cases during a similar ransomware attack. The Ashtabula County Medical Center was offline for more than a week while grappling with the attack. That was at least the 53rd incident of health care ransomware in the United States in 2020 alone.

State and federal legislative initiatives to impose stiffer penalties for ransomware attacks offer little benefit or consolation to patients harmed by such attacks. According to the National Conference of State Legislatures, more than 280 cybersecurity bills and resolutions have been introduced across the country in 2020. But only three states have successfully enacted measures related to ransomware—and none of them creates a private cause of action for victims.

For a patient who has suffered bodily injuries, increased medical bills, and potential loss of life, the knowledge that the hacker may be charged with a felony rather than a misdemeanor may be a moral victory. But their only tangible redress is a financial award to cover additional medical expenses and the attendant pain and suffering.

What recourse exists, then, for the patients' whose medical care is compromised in the meantime? *Common law negligence.*

Organizations who possess sensitive data have a duty to act with reasonable care in establishing and maintaining their digital systems. A breach of that duty, leading to foreseeable damages, is a textbook case of common law negligence.

Common law negligence thus fills a void that has thus far been unaddressed by legislative and regulatory bodies. It offers a remedy for patients who are otherwise caught in a Bermuda triangle between bad actors with the capacity to wreak havoc around the globe, and the legislators and some healthcare institutions who struggle to keep pace with them.

Meaghan Goldstein *is an associate at Kozyak Tropin Throckmorton focusing on complex litigation and class actions with experience litigating claims involving fraud and Ponzi schemes, deceptive and unfair trade practices, product defects, and business torts. She can be reached at:* ***mgoldstein@kttlaw.com****.*