The Walls Have Been Breached! (Now What?)

What do you do when the CEO calls about a ransomware demand?

BY DOUG RAYMOND AND AMELIA BRETT

Imagine this thought experiment: You're the board chair or lead director of a public company. Everything is quiet as you head to your beach house for the long holiday weekend. But then your cellphone rings. It's your CEO and the general counsel. They frantically tell you that the company has been hit by a ransomware attack. Its core systems are frozen and they've been sent to a website where a multimillion-dollar ransom (payable in cryptocurrency) is being demanded to restore functions. You know that these first hours can be critical, but what do you do? Friday night is chaos as management struggles to get a handle on what happened, what systems and operations have been compromised, and what — if anything — still functions.

Your first action item is to convene the board — but the hackers may have been inside the company's systems for weeks. They might have infiltrated its internal communication systems, including management's emails and the integrated phone system. If you use ordinary communication channels, the hackers could invite themselves to the meeting. Instead, you fall back on "out-of-band" communication methods, such as encrypted communication (e.g., encrypted smartphone apps) or an old-fashioned phone tree, to avoid exposing sensitive information about the company's response plan to the hackers.

Once you get the board together over a secure link, it must quickly assess the situation, understand the scope of the attack to the extent management can do so and decide on next steps. This is not the time for pointing fingers or second-guessing initial steps taken. However, the general counsel should advise on what, if any, cybersecu-

rity and ransomware insurance coverage is in place and notify the insurer as soon as possible. The board and management will also need to quickly obtain extremely sophisticated advice from a variety of experts, who will have hours — not days — to get up to speed.

- Lawyers, including the company's existing trusted counsel, as well as counsel with deep experience in similar attacks and (maybe) insurance coverage counsel
- A forensic network security firm that can ensure that the company's systems are locked down and that the attackers are out of the system, and can then investigate the scope and implications of the attack
- A crisis communications firm
- A negotiating team that specializes in negotiating with cybercriminals and has navigated this situation many times before, typically consisting of former law enforcement officers with access to enough cryptocurrency (e.g., Bitcoin) to facilitate a ransom payment

The board will then need to turn to arguably its most important decisions — whether to pay the ransom and whether (and when) the company needs to notify others, such as customers, suppliers, employees and the FBI. And your general counsel will remind you that the SEC will require almost immediate public reporting of the attack if it is determined to be material. The board will be understandably reluctant to negotiate with the bad actors, and some may want to delay reporting the attack until it can be accompanied by some better news. Unfortunately, the board may have little choice but to negotiate if they want to restore crucial operations and avoid the ballooning financial and reputational costs associated with the attack and the potential disclosure of highly sensitive data. Time is definitely not on the board's side.

If the board decides to negotiate and pay up, the hackers should provide a decryption key that will allow the company to decrypt and regain control of its systems and data. And if the company can "trust" the cybercriminals involved, the company's stolen data should not become public and you will be told that the hackers have destroyed the data. On the other hand, if the company can use backups to bring its core systems back online within an acceptable time frame, maybe the company can refuse to pay the ransom or negotiate a significant reduction. But companies that fail to "play ball" with the cybercriminals or drag their feet too long will probably find increasing amounts of their data posted online, including the most sensitive information the hackers were able to steal. In the end, it seems that many — if not most — companies conclude that the best option is to pay the ransom to minimize downtime and to avoid public exposure of sensitive information.

Through this whole process, the board and the executive team must work closely with the company's crisis communications firm to develop a communications strategy. The messaging should be transparent but carefully crafted to protect — to the extent possible — the company's reputation, reassure customers and suppliers that their data is safe and that the company is (or will be shortly) back to normal operations, and it should comply with any SEC and other legal disclosure obligations. Depending on the nature of the stolen data, the company may be required to notify affected customers, employees or clients and should also prepare statements to address press and other inquiries as they arise. The company will also need to quickly evaluate what data breach notice requirements may exist in its customer and other third-party agreements, which often can mandate that the company provides prompt notice of any data breach in as little as 48 hours. Completing this evaluation in a very short time frame will be a tall order if the company has not previously cataloged these notice obligations.

These decisions — and the ones that follow — must be guided by the board's fiduciary duties to act in the best interests of the corporation (and, in Delaware, its stockholders), after investigating the relevant information, with opportunity for reflection and informed, deliberative decision-making based on all material information reasonably available. But under the circumstances, these critical judgments will be made under extreme pressure and on a very tight timeline, with the knowledge that shareholder (and other) litigation and government investigations almost always follow these intrusions.

Knowing the significance — and some would say inevitability — of a ransomware attack, the very short time frames involved, and the potential customer, stockholder and reputational ramifications, the board should not build this airplane while trying to fly it. And leaving aside the board's *Caremark* duties to provide effective oversight of risks, this is not a situation any director wants to find themselves trying to navigate for the first time during an actual attack. Boards should expect such an attack to occur and run real-time practice scenarios to battle-test their readiness and ability to respond to even the most hostile attack. ■

Doug Raymond *and* ***Amelia Brett*** *are partners at Faegre Drinker Biddle & Reath LLP (www.faegredrinker.com). They can be reached at douglas.raymond@faegredrinker.com and amelia.brett@faegredrinker.com, respectively.*