The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 5 March 8, 2017

RANSOMWARE

Preparing For Ransomware Attacks As Part of the Board's Fiduciary Duty

By Jill Abitbol

Managing the enterprise risk of cybersecurity is a key obligation of a company's general counsel and board of directors. Ransomware attacks, which are an evolving and increasingly pervasive threat to companies, are subsumed within that risk. Debevoise partner Jim Pastore spoke with The Cybersecurity Law Report about what GCs and boards need to know about ransomware and how they can fulfill the board's cyber-related fiduciary duty to the company.

Pastore spoke to CSLR in advance of the Skytop Strategies Cyber Risk Governance conference on March 16, 2017, at the High Line Hotel in New York, where he will be a panelist.

"Ransomware continues to be one of the most common forms of cyber attack," Pastore said. Ransomware is an extortion-based category of cyber crime that uses encryption to block access to select files on a compromised endpoint. In most cases, the only way to retrieve the encrypted files is to restore them from a pre-existing backup, or pay a ransom, which can vary from hundreds to thousands of dollars, depending on the victim organization's size and ability to pay. Its prevention represents a significant security challenge because ransomware constantly evolves as cyber criminals refine their tools, techniques and procedures.

[See also "*How In-House Counsel, Management and the Board Can Collaborate to Manage Cyber Risks and Liability (Part One of Two)*" (Jan. 20, 2016); *Part Two* (Feb. 3, 2016).]

CSLR: How is the threat of ransomware attacks evolving?

Pastore: The evolution of ransomware is interesting. We are seeing a migration away from a broad scale volume-based attack, where the idea was to affect as many victims as possible, charge them relatively insignificant sums so that they would be incentivized to pay and then faithfully decrypt in response to payment. In fact, some of these guys would have you refer them as reliable decrypters to future victims because the entire idea was to get people to say "pay." It's only $300, $500 or $1000, " pay and you will successfully decrypt your data." They actually made the price so low that it was more cost-effective to decrypt than to restore.

What we are now seeing is command-line ransomware, where the bad guys carry out an intrusion and systematically target the backup files. Only then do they encrypt and they do that on specified data targets as opposed to using a volume-based approach. They look to see where they can send the malware, and they then demand much higher ransoms.

[See also "*Technology Leader Discusses How to Deal With the Growing Threat of Ransomware*" (Jul. 6, 2016).]

CSLR: Are certain industries targeted more than others? Are middle management or C-level executives more likely to be targeted?

Pastore: Attacks have most prominently been targeting the healthcare industry. I say "most prominently" because healthcare is one of the few areas where, based on HHS guidance, ransomware is a reportable cyber incident for a hospital. So they have been forced to report and the ransoms have not been reported to be multi-million dollars. They have been in the tens of thousands of dollars, which is potentially not an insignificant amount for a hospital, depending on which hospital is hit. Not surprisingly, the financial services industry also is heavily targeted.

I have not seen a trend in attacks being specifically targeted to any certain level of employees.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 5 March 8, 2017

CSLR: What level of understanding do boards and general counsel need about this risk?

Pastore: At the board level, the number-one question to understand and ask is "If we are hit by ransomware, how much business data do we lose?" In other words, "What is the recovery point? Am I backed up daily or weekly?" Number two, "Does that match my risk tolerance?"

If you are, for example, a private equity sponsor, you very well may be able to tolerate a one-day loss of data because a lot of your most critical documents are, in fact, held by your third-party service providers or at least copies are held by those providers. So, for instance, if you are in the middle of a deal or fundraising, your lawyers will have copies of the relevant deal or subscription documents. Obviously there will be some data loss, but it won't necessarily be catastrophic. If, on the other hand, you are a hospital, you can't be down for 24 hours and if you lose a day's worth of patient data, that's potentially very significant. So, it's not only important to know the company's back-up plan and how easy is it to restore data but also whether that actually matches the risk tolerance.

CSLR: Operationally, does the board look itself or should there be a team including the GC looking at what is needed and what the risk tolerance is and then briefing the board on it?

Pastore: Exactly right. As a day-to-day management issue, it is the general counsel in conjunction with the tech team figuring out what the steps are going to be. What the board can do is take more of that detached risk oversight view of "I've now been briefed and I understand that at a minimum we lose 12 hours of data, depending on when the ransomware hits," But then it needs the broad-gauge perspective: "Does that data loss actually match our risk appetite?" This will allow the board to ensure that whatever plan management has put in place has been thought through and matches the enterprise's overall risk appetite.

[See also "*A CSO/GC Advises on How and When to Present Cybersecurity to the Board*" (Feb. 22, 2017).]

CSLR: What is the ideal role of a general counsel in preparing for, preventing and responding to these attacks? Does it depend on the size and corporate structure of the company?

Pastore: It is worth thinking in advance about whether the company would ever pay a ransom and, if so, under what conditions it would pay. The FBI has said different things at different times about whether to pay ransoms. Most recently, Director Comey came out strongly against it. But there have been instances in which the FBI admitted that companies have paid ransoms, and that the FBI is unlikely to prosecute companies for doing so.

The other thing to be aware of is that there are instances in which ransomware is used by organizations that you would not want your money to be going to. So, even if you are contemplating paying the ransom, there is a question of whether and how to involve law enforcement to make sure the money is not going to people you wouldn't want it to go to.

[See also "*How to Prevent and Manage Ransomware Attacks (Part One of Two)*" (Jul. 15, 2015); *Part Two* (Jul. 29, 2015).]

CSLR: What is your advice regarding to pay or not to pay? What factors go into deciding?

Pastore: It is really a situational decision, company by company. I don't think there is a one-size-fits-all answer. You might take into account a number of different factors: (1) the confidence level that you are going to get an effective decryption key; (2) the confidence level that the money you might pay is not going to a truly bad enterprise; and (3) the relative damage to the company of not decrypting and how much data is actually going to be lost. If we are being realistic about it, it is a very difficult situation for certain companies to be in.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 5 March 8, 2017

CSLR: What should employees be instructed to do upon discovering a ransomware attack?

Pastore: It is absolutely critical to internally report it immediately because, if you do, even though it might be somewhat embarrassing for the individual whose computer was infected, the company can take systems offline and keep the ransomware from spreading. The most common forms of ransomware attacks are self-propagating – they spread to whatever the person is connected to. So it is very important that, as quickly as possible, the attacker be taken off the network.

The attack is typically first reported to the helpdesk. It then needs to be escalated as quickly as possible to the people who have the ability to shut the machines off – which may mean going to an employee's office and physically removing the infected machine.

CSLR: Given its fiduciary duty to operate in the best interests of the company, do any shareholder derivative suits to date provide insight into the board's legal obligation in connection with cybersecurity?

Pastore: There have been claims brought against boards of public companies in the wake of breaches. To date, none have been successful. The plaintiffs in these cases have generally pled some form of a duty of care violation in the form of a shareholder derivative suit, alleging that the board completely abdicated its responsibility to oversee cybersecurity. That is an extremely high standard. The courts have not been receptive to those claims to date.

The reality is, like all duty-of-care cases, the facts would have to be pretty egregious for there to be a finding that the board breached the duty of care, whether it is cyber or something else. It just doesn't happen all that much. It's not like other areas that have well-defined best practices.

CSLR: What facts or scenario would give rise to potential board liability for breach of those fiduciary duties?

Pastore: This may be one area where the noise around cybersecurity may not be helpful. Cybersecurity is a business risk to be managed and boards are quite familiar with the level of care that they need to exercise to discharge their duty around business risks. If you approach it as a business risk, boards will then naturally come to understand the level at which they need to engage.

Having said that, the difficulty in cyber is knowing the right questions to ask. For example, a board member may ask, "Do we have multi-factor authentication in place?" Management might truthfully answer, "Yes." But, it may turn out the company only has multi-factor authentication for remote access to systems. Or, it has multi-factor authentication for all of its systems except one legacy system where its sensitive data happens to reside. So, boards really need to think about those granular issues and make sure they are asking the right questions.

CSLR: How does the board ensure it is asking the right questions?

Pastore: We have generally seen two different approaches. Either the board hires someone to advise them, such as an outside expert akin to an auditor, or companies have increasingly been looking for board members with technical expertise. There have been bills proposed in Congress (which haven't gone anywhere) that would require the board to identify one of its members as the person responsible for cybersecurity issues.

CSLR: Is there any regulation or law that requires a company to hire an outside expert?

Pastore: Currently pending is an Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards from the federal banking agencies that actually contemplates imposing additional legal requirements around this.

Certainly, there is some indication that we might wind up there but there is not currently a specific regulation that requires a company's board to hire an outside expert to advise them on cybersecurity.

CSLR: What is the GC's role in ensuring the board fulfills its fiduciary duty to the company on cybersecurity?

Pastore: Don't be afraid to get under the technical hood, so to speak, and dig and ask the important questions. Because it is a specialized field, general counsel may, in some instances, abandon their sense of curiosity or their ability to interrogate. But they shouldn't. Just because the technical side of cybersecurity involves funny acronyms or lots of numbers, general counsel should not shy away from asking the granular questions about encryption and other technical aspects of cybersecurity as they would for any potential business risk.

General counsel also shouldn't be afraid to have candid conversations with the tech team about what security measures are and are not being implemented, and whether it might be reasonable to not do certain things.

CSLR: Once general counsel gains that understanding, is it then reported to the board?

Pastore: Yes. The general counsel has to make an assessment in the first instance with the tech team and general counsel should be encouraging that discussion. If the tech team tells the GC they are doing everything that could be done, you've got a problem, because that is never true. The business reality is that you can never truly do everything that should be done. It's all about risk management. You can have the most secure system in the world but you'd never be able to run the business, so there has to be a balancing of priorities.

CSLR: Is it typically the general counsel who reports to the board on cybersecurity?

Pastore: Ideally, the general counsel is involved in that presentation but in practice, it is not always true. It is often the domain of the CISO, or the CTO or CIO. At the same time, breach issues are becoming fundamentally legal events because there almost inevitably is litigation following any significant breach event. We are at the point where breach events are legal events.

CSLR: So do the CISO and GC need to work together for the most effective results?

Pastore: Absolutely. For example, you might get a technical assessment and if it is not done under privilege and without the involvement of lawyers, you potentially get hyperbolic language in the report from the vendor about how awful your cybersecurity is. Then, that shows up in litigation and winds up in the plaintiff's hands, and it's not a good day. Whereas, if the lawyer was a team member from the start, you first might succeed in keeping that report privileged and, second, there might be more sensitivity to ensuring the results are reported in a way that is sensitive to potential litigation risks, while still remaining accurate and actionable.

This is an example of where viewing cyber as a business risk as opposed to some scary technological thing that lawyers are incapable of understanding goes a long way.

CSLR: How often should the board address cybersecurity or receive a cybersecurity briefing at its meetings?

Pastore: To the extent there is any regulatory consensus, it is coalescing around a minimum of annually and, in practice, we are starting to see companies move more towards quarterly airtime for cyber at board meetings. Sometimes it's not with the full board. The quarterly discussion might be with an audit committee, but cyber often is getting some airtime with some portion of the board every quarter.