Skadden

A Practical Guide to the Role of Directors in Fighting Ransomware

Ransomware is such a major threat to businesses that directors need to take an active role overseeing cybersecurity programs.

- Boards need to take an active role overseeing cybersecurity measures.
- Directors may be held personally responsible for lapses that result in attacks.
- U.S. money laundering and sanctions rules may prohibit some ransom payments.

The biggest cyberthreat most companies face is not attacks backed by nation-states like the recent SolarWinds hacking episode. It is ransomware, a type of malware that encrypts its victims' data and holds it hostage until a ransom is paid in untraceable bitcoin.

These attacks have grown more frequent and sophisticated at the same time that more people are working remotely and are more reliant on corporate IT systems. According to BitDefender's analysis of the cyberthreats, there was a 715% increase in detected and blocked ransomware attacks in the first half of 2020 versus that period in 2019. Many of these are never publicly disclosed. In some recent attacks, sensitive data was stolen before it was encrypted, and the attackers threatened to leak it if the victims failed to pay.

Two legal developments bear directly on directors' roles in dealing with the problem:

Officers and directors may face personal liability in the event of a cyber attack. Lawsuits arising from other kinds of data breaches reflect an emerging expectation that directors must play an active role in cybersecurity planning and cannot delegate the issue entirely to management. Those cases suggest that directors may be held personally liable for (a) failing to ensure proper policies were in place to protect a company or (b) issuing misleading statements about their companies' preparedness. For example:

- A class action complaint against one company alleges that its board knew of an initial data breach whose scope only became clear two years later but "failed to act

sufficiently upon the full extent of knowledge known internally by the company's information security team."

– In litigation over the theft of consumer credit information from Equifax, a federal judge found that the company "relied upon a single individual to manually implement its [software] patching across its entire network" and that person "had no way to know where vulnerable software in need of patching was being run on Equifax's systems." That "failed to meet the most basic industry standard," the court found, and therefore "it was false, or at least misleading, for Equifax to tout its advanced cybersecurity protections" in public filings.

The implication: Directors need to take this threat seriously and play an active oversight role in implementing protections.

U.S. anti-money-laundering and sanctions laws may bar some ransom payments. Boards need to be aware that the Treasury Department requires ransomware victims and their financial institutions to perform due diligence on those to whom they plan to pay ransom. Because several prolific ransomware groups are subject to U.S. sanctions, Treasury rules may prohibit some ransom payments. That leaves the victims with no choice but to rebuild their systems from scratch and suffer the consequences of having their data disclosed publicly.

Authors

Michael E. Leiter / Washington, D.C.

Maxim Mayer-Cesiano / New York

William Ridgway / Chicago

The Growing Role of Boards in Cybersecurity Planning

25%

Share of financial services firms whose boards discussed cybersecurity more than once a year in 2017

95%

Share of those whose boards or committees discussed cybersecurity at least four times a year in 2020

48%

Share that involve their boards in cybersecurity exercises

Source: McKinsey

This article is from Skadden's ***The Informed Board***.

One Manhattan West / New York, NY 10001 / 212.735.3000

A Checklist for Managing Ransomware Risks

- ☐ **Boards should discuss cybersecurity regularly.** A recent McKinsey survey of financial services companies suggests best practices. Nearly 95% of the firms reported that one of their board committees discussed cybersecurity and technology risks four times or more per year. Almost half the companies involved the board in cybersecurity exercises, and nine in 10 provided regular updates on cybersecurity to the full board.

  Financial services firms furnish a good model because they have long been targets of attacks and have advanced cybersecurity programs. Their approach hints at what shareholders, regulators and others are likely to demand from boards in other industries.

- ☐ **Responsibilities need to be defined in advance.** The inevitable disruption of an attack can be compounded by uncertainty about who should handle different aspects of the response. For instance, CIOs/CTOs, general counsels and communications chiefs will each have roles, sometimes overlapping, so their responsibilities need to be spelled out in advance. The board should also consider pressure-testing management's plans and lay down procedures to ensure the board plays an appropriate oversight role during an incident.

- ☐ **Prepare a response playbook in advance.** Corporate networks are often disabled by ransomware. Since attackers typically demand payment within days, victims can find themselves scrambling to engage outside experts (***e.g.***, a digital forensics consultant, ransomware negotiator, outside counsel and public relations specialist) and make strategic decisions while the company's e-mail system is inoperable and vital records are inaccessible. It may be impossible, for example, to fulfill contractual obligations to notify customers about the incident because contact or contract information has been locked up by encryption.

  Procedures need to be in place to deal with such a situation. At a minimum, secure communication alternatives need to be in place, and records required to respond to a crisis must be accessible even if primary IT systems are down.

- ☐ **Cybersecurity needs to be assessed within a larger risk management framework.** Given the potentially catastrophic impact of an attack, cybersecurity risks need to be evaluated as part of a company's overall risk management. Budgets for risk mitigation need to factor in the damages an attack could cause, including its impact on customers and suppliers. Companies should find metrics to monitor their progress in mitigating cyberrisks. Objective metrics will also be needed to back up any claims the company makes about its cybersecurity practices, especially those aimed at investors.

- ☐ **Consider hiring outside vendors to test your systems and people.** A survey of directors last year by the University of California, Berkeley and Booz Allen Hamilton showed that many companies seek regular third-party advice to ensure that management is keeping up with the latest evolving threats. That may be essential for the board to fulfill its oversight role.

  Even for companies that follow established procedures, such as the National Institute of Standards and Technology's Cybersecurity Framework, third parties can help verify that those are being adhered to. For example, the American Institute of Certified Public Accountants has set standards for companywide audits of cyberrisk measures.