By Mark A. Carter and Cathy Mulrow-Peattie

Boards of Distressed Enterprises: The Cyberattack "Buck" Stops Here

Mark A. Carter
Hinshaw & Culbertson LLP; Chicago

Cathy Mulrow-Peattie
Hinshaw & Culbertson LLP; New York

Mark Carter is a partner in Hinshaw & Culbertson LLP's Business and Commercial Transactions Practice Group in Chicago, with a focus on corporate governance, mergers and acquisitions, and business restructurings. Cathy Mulrow-Peattie is a partner in the firm's New York office, with a focus on privacy, security and artificial intelligence.

The increasing use of data, technology and artificial intelligence (AI) to streamline business operations creates significant opportunities. However, with this opportunity comes increased risk of threat by bad actors who attack the technology and extract personal data to harm the enterprise, usually for profit.

Nearly one-fifth of U.S. and EU companies are believed to face economic crisis and bankruptcy due to the costs of ransomware and other cybersecurity incidents.[1] Here are some of the cybersecurity vectors that companies are currently facing:

- Ransomware attacks occur when malware infiltrates an organization's computer systems and encrypts the data to hold the organization hostage. When this happens, the company's impacted servers often are inaccessible, meaning that there can be no billing, customer data, access to records, financial reporting or access to any services.
- Social-engineering attacks occur when a hacker uses valid company access to obtain or give away sensitive information.[2] Hackers frequently pretend to be employees to obtain credentials, often to execute large financial transactions. Bad actors, often from outside the U.S., are using AI's large language models for social engineering attacks.
- Supply chain attacks have been continuous attack vectors to infiltrate companies from the outside, especially leveraging third-party software.

To be effective, a company's board of directors must set clear cyberrisk-tolerance levels for key assets of the enterprise. As discussed herein, these obligations and cybersecurity concerns are amplified in the context of an insolvent enterprise.[3]

Duties of a Distressed Enterprise's Board

As with all acts or omissions by board members, the board's approach to cybersecurity matters will be evaluated under the governance framework of the law of the state of the entity's formation. Under the laws of most states, board members owe fiduciary duties of care and loyalty to the enterprise and its owners.[4] Absent conflicted board members, which gives rise to duty-of-loyalty concerns, a board's actions will be presumed to be proper under the business judgment rule unless the directors were "recklessly uninformed" or acted "outside the bounds of reason."[5]

For example, under Delaware law, the presumption may be overcome if a board's "decision was the product of an irrational process or [if] directors failed to establish an information and reporting system reasonably designed to provide the senior management and the board with information regarding the corporation's legal compliance and business performance."[6] Board members must become informed on cybersecurity issues and insist upon the installation of processes that protect against the risk.

To be clear, depending on the applicable state law, entities may provide for exculpatory provisions in their formation documents that limit or waive the fiduciary duties of board members.[7] Yet, even with effective waivers, the board might become involved in resource-draining litigation as a result of a cyberattack.[8]

For insolvent companies, the group of stakeholders to whom the board members' fiduciary duties are owed generally expands to include the creditors of the enterprise.[9] In a chapter 11 case, the board's fiduciary duties of care and loyalty continue to apply, but with an additional focus on preserving the company's assets and maximizing their value.[10] The limits that various state laws impose or permit regarding breach-of-fiduciary-duty actions are, in most cases, supplanted by insolvency and bankruptcy law. For example, many jurisdictions recognize the derivative standing of a creditors' committee to

1 "Cyber Attacks Throw One-Fifth of Businesses in Europe and the U.S. into Bankruptcy," Kron Techs. (May 29, 2022), *available at* krontech.com/cyber-attacks-throw-one-fifth-of-businesses-in-europe-and-the-us-into-bankruptcy; Simon Hendery, "FBI: Cybercrime Cost Americans over $12.5B in 2023," SC Media, *available at* scmagazine.com/news/fbi-cybercrime-cost-americans-over-12-5b-in-2023 (unless otherwise specified, all links in this article were last visited on Sept. 27, 2024).

2 *See* "Defining Insider Threats," Cybersecurity & Infrastructure Sec. Agency, *available at* cisa.gov/defining-insider-threats.

3 *Cf.*, Jonathan Trimble, "Beware: Restructuring Is an Opportunity for Cybercriminals," XLI *ABI Journal* 4, 24-25, April 2022, *available at* abi.org/abi-journal.

4 *Cf.*, *Bayou Steel BD LLC v. Black Diamond Capital Mgmt. LLC (In re Bayou Steel BD Holdings LLC)*, 651 B.R. 179 (Bankr. D. Del. 2023).

5 *Id.* at 184-85.

6 *Hurwitz v. Mahoney (In re Space Case)*, No. 22-10657, 2024 Bankr. LEXIS 902*, 2024 WL 1628440, *15 (Bankr. D. Del. April 15, 2024).

7 *CML V LLC v. Bax*, 28 A.3d 1037 (Del. 2011).

8 *See Firemen's Ret. Sys. of St. Louis v. Sorenson*, No. 2019-0965-LWW, 2021 Del. Ch. LEXIS 234*, 2021 WL 4593777, at *13 (Del. Ch. Oct. 5, 2021); *Constr. Indus. Laborers Pension Fund v. Bingle*, No. 2021-0940-SG, 2022 Del. Ch. LEXIS 223*, 2022 WL 4102492 (Del. Ch. May 13, 2022), *aff'd*, 297 A.3d 1083 (Del. 2023). While both cases were dismissed, they provide examples of what a board should and should not do with regard to cybersecurity preparedness.

9 *Cf.*, *Quadrant Structured Prods. Co. v. Vertin*, 102 A.3d 155 (Del. Ch. 2014); *In re Doctors Hosp. of Hyde Park Inc.*, 474 F.3d 421, 426 (7th Cir. 2007); *Caufield v. Packer Grp. Inc.*, 2016 IL App. (1st) 151558, 56 N.E. 3d 509.

10 *See, e.g.*, *Holywell Corp. v. Smith*, 503 U.S. 47, 117 L. Ed. 2d 196, 112 S. Ct. 1021 (1992); *In re Schipper*, 933 F.2d 513 (7th Cir. 1990).

bring actions, such as fiduciary duty claims, on behalf of the bankruptcy estate.[11] Even in the context of a limited liability company (LLC) with full waivers of fiduciary duties in its governance documents, courts have declined to enforce such waivers under "pre-emption" theories under the Bankruptcy Code.[12] Therefore, board members could be subjected to creditors' prosecution of fiduciary duty claims in bankruptcy, notwithstanding the presence of fiduciary duty waivers in governance documents.

The circumstances under which the board of a distressed company finds itself add to the risks of a cyberattack. Management's focus then changes to conserving resources. Accordingly, the board of an insolvent company faces heightened vulnerability to a cyberattack and an expanded group of potential "plaintiffs" that would not be present were the company in strong financial health.

The Growing Regulatory Environment

Boards and senior management often fail to recognize that there are regulatory requirements for companies to maintain sufficient cybersecurity protections, such as the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, U.S. Securities and Exchange Commission (SEC) cybersecurity regulations for public companies, New York's Department of Financial Services (NYDFS) Part 500, and Federal Trade Commission (FTC) and state security and data-protection requirements for reasonable security standards. These standards apply to companies whether in or outside of bankruptcy.

Adding to this regulatory concern is the fact that the FTC also has remained active in targeting companies that fail to implement reasonable data-security measures to protect consumer data. In 2022 and 2023 alone, the FTC announced or finalized enforcement actions against Global Tel*Link (required change in management processes as part of the settlement when security systems change), Drizly (FTC settlement against the company and its chief executive officer (CEO) for, among other things, failing to have written information security policies, multifactor authentication (MFA) and access controls — the order requirements followed the CEO to his next organization), Chegg (failed to implement encryption and MFA) and CafePress (failed to have reasonable security controls to protect sensitive information such as MFA and encryption) for data-security failures.[13]

In 2024, the FTC settled an action against Blackbaud for its data breach, citing its repeated failures to have appropriate cybersecurity controls in place, such as MFA or software patches, to delete data, and its misstatements about its security practices.[14] Similarly, all 20 comprehensive state privacy laws require reasonable security standards with sufficient administrative, organizational and technical controls, and these newer regulators will be watching organizations for weaknesses. In addition, California allows data owners to sue organizations directly with a private right of action, and state attorneys general are beefing up compliance staffing to hold organizations responsible for their security requirements and promises.

Best Practices for Board Oversight and Senior Management Implementation

As the board and senior management[15] plan for a restructuring or acquisition of a distressed target, they need to recognize the continuing importance of cybersecurity controls and act to ensure that processes are in place to adequately address cyber-risk consistent with their fiduciary duties. What key practices should the board of a distressed enterprise consider — or an acquirer look for — with regard to a company's cybersecurity preparedness?

Assess and Bolster the Board's Cybersecurity Protocols and Controls

Where time permits, the company's cybersecurity structure should be reviewed and improved. The board and senior management should ensure (1) effective protocols regarding communication between board members and senior management; (2) information-sharing among the board members, any relevant committees and management; and (3) that risk-escalation criteria are in place. At the very least, the chief information security officer (CISO) should be reporting material cyber-inadequacies and material compliance directly to the board on an ongoing basis.

Focus on the Key Assets

The board and senior management should identify and understand on what platforms the enterprise's greatest personal data, information and intellectual property assets are maintained and stored. Not all cyber-risk is the same, as a balance of risks and rewards needs to be made. It is critical to establish clear cyber-risk protections for the enterprise's critical assets, including having the applicable cybersecurity controls protecting those key areas of the business.

Revisit/Establish the Incident-Response Plan

Federal and state regulators have cybersecurity incident-notification requirements. A written "incident response plan" (IRP) setting forth the individual roles, responsibilities and processes for managing a cyberattack should be updated or, if not prepared, established for the company. It is critical that the IRP identify any required data-breach notification regulatory requirements and contact information for law enforcement.

The IRP should also contain a section explaining attorney/client privilege in the security-breach environment for all players. It should also expressly reference and set forth the particular roles of at least the CEO, chief information officer (CIO), CISO, inside counsel, public relations lead, human resources lead (if any) and outside counsel. The contact information for such players should

11 *See In re Smart World Techs. LLC*, 423 F.3d 166, 176 (2d Cir. 2005); *Fogel v. Zell*, 221 F.3d 955, 965-67 (7th Cir. 2000).

12 *In re Pack Liquidating LLC*, 658 B.R. 305 (Bankr. D. Del. 2024). *See also In re HH Liquidation LLC*, 590 B.R. 211 (Bankr. D. Del. 2018) (Delaware LLC Act precludes derivate actions by creditors in bankruptcy).

13 "FTC Releases 2023 Privacy and Data Security Update," Fed. Trade Comm'n (March 28, 2024), *available at* ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update.

14 *In the Matter of Blackbaud Inc.* (a corporation), FTC Decision and Order (May 20, 2024).

15 While this article has discussed the board's obligations regarding cybersecurity protections in an organization, regulators are increasingly bringing actions against senior management, claiming that they are responsible for failures in cybersecurity controls and failing to report cyberincidents.

continued on page 59

from page 21

exist outside of the organization's computer system. Also critical to any IRP is that it covers a critical third-party platform breach.

Stress-Test the IRP: Practice Makes Perfect (Almost)

The organization should maintain stress-testing of the IRP from both a technology and "tabletop" exercise perspective, as new players will be involved in any incident. An exercise is a role-playing activity in which players respond to hypothetical threat/actor scenarios presented by one or more facilitators. Participants usually play their own role of CEO, CIO, CISO, in-house counsel, outside counsel, human resources lead and communications lead, but they can also play other roles to fill in gaps.

Insurance Coverage and Scope of Protection Need to Be Reviewed

Many companies are underinsured from a cybersecurity-incident perspective. The average cost of a data breach in 2023 was $9.48 million.[16] Most organizations have cyber- and data-breach insurance policy limits in the range of $1 million to $3 million. It is critical for the board and senior management to maintain cybersecurity insurance coverage during any restructuring and to understand what the organization's insurance policy covers and what it does not (*i.e.*, what are the exclusions).

A strong cybersecurity policy covers the material risks like incident-response costs (such as an incident-response manager), legal and regulatory costs (covering the cost of legal fees and responding to a regulatory investigation), information and security forensic costs (information security external support, hiring of an external forensic investigator and remediating the event), crisis-communication costs (engaging a public relations consultant and having media training to respond to the event), privacy breach management costs (notifications to consumers, call centers, credit-monitoring services and translation services), income loss and extra-expense reimbursement (to reimburse organization for the losses and costs directly arising from the attack), network security liability and regulatory fines, and any related litigation costs (such as follow-up data-breach class-action lawsuits). To better understand these issues and be prepared in the event of a security incident, the insurer and the company's insurance agent can provide valuable information on such plans.

One more cautionary note is warranted: As part of the new or renewal cybersecurity and privacy policy application process, insurance companies often require organizations to have standard cybersecurity controls in place to obtain or continue coverage. Organizational officers as part of the application or renewal process certify that these controls exist.

If these controls change as part of the restructuring process and you fail to notify the carrier to revise your application, you could be denied coverage in the event of a security incident if the failure to have these controls caused the security incident. Carriers might not allow for the reduction in security controls, as these controls are wisely implemented to avoid known cyberattacks.

Update Information Security Program Based on a Written Risk Assessment

The slide of a distressed enterprise toward a restructuring process could involve or result in a material change to the business's operations. This material change, especially if publicly reported, could make the organization a target for cybercriminals and not controlled for regulatory investigation.

As a matter of cybersecurity best practices, and as required under the NYDFS Part 500 and the GLBA Safeguards Rule, "risk assessments" of an organization's information systems should be reviewed and updated when there is a material change in the business or technology that causes a material change to a company's cyber-risk, and annually even if there is no change.

A "risk assessment" refers to the process of identifying, estimating and prioritizing risks to organizational operations, assets, individuals, customers and critical infrastructure resulting from the operation of an information system. Risk assessments incorporate threat and vulnerability analyses and consider mitigations provided by security controls planned or in place.[17] SEC cybersecurity regulations and NYDFS cybersecurity regulations Part 500 both require that the board and senior management are responsible for ongoing cybersecurity risk assessments and compliance obligations.

Accordingly, the board should ensure that senior management identifies foreseeable internal and external risk to the security, confidentiality and integrity of information that could result in the unauthorized disclosure, misuse, alteration, theft or compromise of the organization's key assets, and implement a plan to address it.[18]

Maintain Qualified Individuals to Implement and Supervise the Information-Security Program

Information-technology or security teams should generally not be included in planned workforce reductions in any restructuring plan. If such reductions find their way into a restructuring, the board needs to identify alternatives, such as contracting for information security.

16 Ani Petrosyan, "Average Cost of a Data Breach in the United States from 2006 to 2024," Statista (Sept. 11, 2024), *available at* statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach (subscription required to view data).

17 23 N.YC.R.R. 500.1(p).

18 First American Bank was fined $1 million by NYSDFS for failing "to adequately maintain and implement an effective cybersecurity policy related to access controls and based on its risk assessment. 23 NYCRR §§ 500.3(b), (d), and (m)." *In the Matter of First Am.*, NYDFS Consent Order, Nov. 27, 2023.

continued on page 60

from page 59

There has been a growth of virtual CISO or virtual information security technology staff as part of COVID-19 workforce changes. A virtual CISO and information security staff are skilled and experienced cybersecurity professionals who provide the same level of expertise and guidance as an in-house CISO, but typically on a remote, on-demand basis. However, as your existing information-security team moves on, ensure that there is knowledge transfer as part of their separation agreement to a virtual CISO or information-security contractor. For public companies in particular, it is critical to have experienced CISOs, as they are required under the SEC regulations to disclose management's role and expertise in assessment and managing material cybersecurity threats.[19]

Conclusion

The need for proper assessment of cyber- and data-security risks is heightened in special situations, both in terms of the vulnerability of the assets of the company and the potential claimants to enforce claims. Whether planning for a restructuring or an acquisition of a distressed enterprise, boards and their advisors need to consider cybersecurity best practices to protect their enterprise, employees and key relationship parties. abi

19 Regulation S-K Item 106(c).