AMERICAN BANKRUPTCY INSTITUTE
JOURNAL
The Essential Resource for Today's Busy Insolvency Professional

Cyber-U

By Wayne P. Weitz and Scott Corzine

Cyberuptcy: The Intersection of Information Security and Bankruptcy

Wayne P. Weitz
B. Riley Advisory Services; New York

Scott Corzine
B. Riley Advisory Services; Arlington, Va.

Wayne Weitz is a senior managing director with B. Riley Advisory Services and is co-head of its Restructuring and Insolvency Advisory Practice in New York. He is also a member of ABI's Board of Directors. Scott Corzine is a senior managing director and co-head of the company's Compliance, Risk and Resilience Practice in Arlington, Va.

At the dawn of the internet age, it was popular to proclaim that "[i]nformation wants to be free, accessible [and] seamless." However, that "information" has the potential to impact the bankruptcy process on both procedural and very personal bases. The move to a paperless office, sustained remote workforce and globally connected computer systems mandates preparation, monitoring and rapid real-time evolution to protect owners and subjects of the information being moved. At the same time, lockdown protection at all costs can hinder the smooth operation — or any operation — of businesses that rely on real-time exchanges of information.

We live in a hyper-connected world where everyone's data and applications are subject to compromise with only a few keystrokes, if the bad guys know the passwords and the good guys have not taken active steps to protect their systems. This article will review how cybersecurity and privacy issues intersect with insolvency issues — before, during and after a chapter 11 process. It then discusses data issues as proximate causes of filing, risks inherent in increasing the number of users who have access to systems and data, and how decisions made before and during the chapter 11 process can materially impact the ability of post-confirmation fiduciaries to pursue and achieve their goals of maximizing recoveries for creditors.

While cyberevents are not the root cause of most bankruptcies, cybersecurity is an important consideration to understand when it is at least a contributing cause, and when it complicates and adds risk to the bankruptcy process. It can be helpful to think about the risk to the three elements of information security — confidentiality, integrity and availability — when cyberincidents may precipitate a bankruptcy, during discovery and the information exchange, and afterward when access to data continues to be critical.

Systems compromises, data breaches and intentional attacks such as denial of services, malware and ransomware in and of themselves generally do not cause large or mid-market companies to seek bankruptcy protection. At the same time, cyberevents may push smaller organizations toward insolvency because such organizations are less resilient and less prepared than large organizations to weather a disruption. In addition, cyberincidents can compromise data confidentiality and integrity, or disrupt or block information availability. Certain industries, such as banking or health care, are entirely dependent on information systems to run large parts of our lives and the economy. Cyberdisruptions in these industries can have cascading effects.

Cyber-risk during bankruptcy might be caused by the sharing of information by multiple parties with distinct interests across system configurations that range from secured, collaborative data transmission and storage platforms to everyday unencrypted email exchanges. The more players at the table, the greater the risk to the confidentiality of documents and artifacts, and possibly document integrity. Document production can be impeded if eDiscovery systems are somehow compromised.

Before Distress

A 2019 article[1] acknowledges that large companies rarely declare bankruptcy immediately after suffering a cyberattack, but instead suffer financial repercussions, embarrassing disclosures, reputational impacts and senior-management purges. First-party costs associated with credit-monitoring, notice, incident response and forensics, and stakeholder communications can be meaningful to the

1 *See* Rob Black, "Cybersecurity Breach Bankruptcy: It Does Happen," LinkedIn (Jan. 23, 2019), *available at* linkedin.com/pulse/cybersecurity-breach-bankruptcy-does-happen-rob-black (unless otherwise specified, all links in this article were last visited on April 26, 2022).

extent that they exceed limits, exclusions and self-funded retentions imposed by the cybersecurity insurance policy. However, it is the contingent costs not covered by insurance that may be the more important impact: shareholder (and partner/customer) derivative lawsuits, ever-more punitive regulatory enforcement actions and penalties, disruptions of business operations, and the brand/image damage that often results in the replacement of C-suite members. It might not rise to the level of bankruptcy, but the cumulative damage can be reflected in market cap devaluation, reduced deal value in M&A, intense regulatory scrutiny, and tougher contractual demands of counterparties.

When North Korean hackers (purportedly) took confidential data from Sony Pictures in 2014, they acquired personally identifiable information, emails and executive salary data. However, that paled by comparison to the damage done by making public copies of then-unreleased films, plans for future films, and scripts — representing future enterprise value and competitive advantage. The *coup de grace* was that the attackers introduced a variant of the Shamoon wiper malware that essentially erased Sony's computer infrastructure, requiring a months-long rebuild of the entire IT environment, during which Sony Pictures was forced to revert to analog operations. In December 2014, a *Wall Street Journal* article estimated that the cost to Sony of the North Korean data breach would ultimately exceed $100 million, a figure with the potential to render many companies insolvent.

The 2019 article's analysis identified three notable companies that ceased operations due in large part to years of intellectual property (IP) theft that destroyed enterprise value: Westinghouse, Nortel Networks and SolarWorld. A pernicious form of cyberthreat, IP theft can happen in a single large data theft, but it is usually a slower and more insidious death. The theft of essential IP destroys value by compromising the basis of competitive advantage as an initial — but not exclusive — root cause of failure. IP theft brazenly impacts the confidentiality of information due to any one or a combination of several cybersecurity compromises, from insider theft to malware, each of which points to holes in access control, logging and monitoring, lack of segmentation or a zero-trust architecture, poor data-at-rest encryption, etc. In a world where well over 80 percent of enterprise assets today are digital, hoping the past is prologue is bad strategy. Whether IP theft or compromise of other digital assets, boards and management teams of companies must coldly assess their cyberposture and close the gaps, then address the risks, so that they do not join the ranks of the previously mentioned three companies.

While large organizations typically have better security posture, practices and maturity than smaller firms, material gaps still plague big companies to a surprising extent, given the demonstrable ubiquity of successful cyberattacks on companies everywhere by threat actors using sophisticated tradecraft. But smaller, resource-constrained organizations continue to bear the greatest risk. As one article pointed out,[2] smaller organizations lack the resources, expertise, breadth of operations and markets, and management buy-in typically found in large companies. Smaller companies may view cyberprotection as an unaffordable luxury rather than a core cost of doing business. As a result, significant cyberevents can be the root cause of a failure that eventually leads to bankruptcy.

While IP theft may result in economic damages from which large companies can recover over time, the loss of computer systems and data can cause the demise of some organizations. In 2019, Texas-based steel structure manufacturer United Structures of America Inc. was the victim of a ransomware attack that left its financial systems locked and inaccessible. Although the company paid the ransom, they were unable to decrypt the data, began a wind-down process and ultimately filed for bankruptcy.[3]

However, not all companies are able or willing to acknowledge the extent of the risk, and in some cases the cost of adopting mitigation procedures and systems may itself be incompatible with a company's ability to operate profitably. As a practical example, consider the U.S. defense industrial base, comprised of more than 300,000 companies, most of which are small secondary or tertiary subcontractors to large prime contractors. The recent imposition of reasonable new-contract acquisition and compliance requirements for better cybersecurity, designed to protect national defense, met with a material objection from smaller contractors, united in opposition to new rules that amount to basic, sound cybersecurity.

These small contractors took the position that cybersecurity is too expensive to implement. Not surprisingly, nation-state theft and compromise of data from these small companies was the policy predicate for the new regulations in the first place. Many of these small defense contractors that resist reasonable controls risk insolvency should they be hacked, and they further jeopardize the prime contractors that depend on them, and in some cases national security.

For a chapter 11 debtor, the process itself creates risk in the areas of treatment and protection of confidential data, access to and maintenance of data and application servers on an ongoing basis to support the business and the case, and preservation of data for use once the formal bankruptcy case is resolved or a plan is confirmed.

Electronic Data Rooms: A Convenience Fraught with Risk

During bankruptcy, a due-diligence process associated with a sale under § 363 or pursuant to a plan typically requires that the debtors make confidential information available to potential suitors. In the pre-connected age, sellers would set up physical data rooms containing file cabinets full of paper information, and buyers would visit these rooms in person. Access was tightly controlled, and documents generally were not permitted outside the secure location.

Connectivity and digital access have long been a double-edged sword. By allowing potential buyers to evaluate a target remotely, the universe of potential buyers increases. However, the act of making information available over an internet connection greatly increases the risk of problems, including confidentiality breaches. Electronic data rooms or virtual data rooms have become the norm to address this risk, but debtors must be satisfied that the security proto-

2 Robert Johnson, III, "60 Percent of Small Companies Close Within 6 Months of Being Hacked," *Cybercrime Magazine* (Jan. 2, 2019), *available at* cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked.

3 *In re United Structures of Am.*, 22-30104 (Bankr. S.D. Tex.).

cols employed by the vendor are adequate. When systems are being accessed remotely, security is only as good as the weakest connected system and the security habit of users.

Furthermore, administrative and access rights, which are controlled by the debtor or its agent (often, an investment banker) must be set up carefully to provide only the level of access intended: read/write, edit, download, etc. Access logs should be scrutinized regularly by the debtors' advisors in order to monitor what information has been downloaded and by whom. It should go without saying that anyone accessing confidential data should be bound by an appropriate confidentiality or nondisclosure agreement. Bankruptcy-driven sales have the propensity to attract visitors that do not intend to buy, just to learn, akin to neighbors visiting an open house of a for-sale property "just to see."

Where Is the Company's Data?

Another area that creates cyberaccess confidentiality risk and practical challenges is cloud storage. As personal computers became widely used, companies established centralized file servers and often application servers, generally located in a data closet in the main office. The storage center is maintained by company employees, and backups might not be performed regularly and rarely validated, thus creating a risk of loss of data (and a false sense of security, until it is too late).

In response to these risks, and with the introduction of ubiquitous internet access, the market for cloud storage and remote application execution developed. Leaders in this field include Microsoft Azure and Amazon Web Services. Companies have transitioned to storing data "in the cloud" on servers owned by third-party providers.

While adding flexibility for remote access to data and applications by employees and customers, reliance on cloud storage presents particular challenges in a bankruptcy environment. While healthy, a company using a cloud storage solution will have a service contract with one or more such hosting companies, addressing use and access of the data. These contracts, which can carry high monthly fees, typically permit the provider to cut off access to data, and in many cases delete data, for nonpayment of bills. The contracts are normally executory in nature and do not easily permit security negotiations.

To Accept or Reject the Executory Contract?

At some point in the case, whether upon the closing of a § 363 sale or confirmation of a liquidation or reorganization plan, the contract with the data provider will need to be assumed or rejected. Prior to making this decision, and cost considerations aside, it is critical that the relevant parties thoroughly consider the fate of the data, which may be needed by a buyer, a reorganized debtor or a post-confirmation trustee.

For example, a financial advisor to a liquidating trustee may have to figure out what data lies where, including accounting records, email correspondence, general files (Word documents, Excel spreadsheets, etc.) and other business-related information. There may be a situation where the debtors had contracts with hosts like Microsoft and Amazon Web Services, and the successor chose not to assume these contracts. Although ownership of the data might never be in question, if it becomes the property of the liquidating trustee in accordance with the confirmed plan, questions could arise as to access, ownership, ongoing storage and costs. If a contract is rejected hastily, post-confirmation fiduciaries could lose access to data that is critical to their pursuit of recoveries and could be deemed negligent.

Furthermore, simply assuming a contract is often not an option for a post-confirmation trust that is not generating revenues, has limited initial funds generally, and is protecting its fiduciary duty to beneficiaries by minimizing costs. The existing data contract likely was written to accommodate the debtor's pre-filing business and may be both onerous in operation and expensive to maintain.

Post-Confirmation Preservation and Access

Once upon a time, immediately upon confirmation, the liquidating trustee would arrange for physical transfer, or at least a mirror image, of a server, hard drive or similar storage device from the debtor's offices or data center, and all information would be preserved so that it could be accessed for future litigation purposes. This includes emails, which can be a treasure trove of information in D&O litigation, and general ledger information that is critical for analysis of preferences, solvency and other financial transactions. Timing is also paramount here, as large hosting organizations can be slow to assist in the transition process, particularly if they know their contract is going to be (or has been) rejected.

Therefore, it is recommended that a liquidating trustee or financial advisor to a trustee (1) identify all servers and service provider contracts of the debtor; (2) identify data that should be preserved (remember, the post-confirmation trustee will not be running the debtors' websites or business applications); (3) negotiate short-term agreements or settlements with the hosts to provide a window of continued access sufficient to download relevant data; and (4) work with IT specialists to download data and identify an appropriate and cost-effective host for storage, maintenance and access. In some cases, it may even be necessary to obtain court orders to prevent data hosts from taking action that jeopardizes the data, though with proper, thoughtful pre-confirmation planning, this should be avoidable.

Conclusion

In this era of over-reliance on connected systems and virtual storage, businesses must be acutely aware of the risks posed by such connectivity. Failure to properly protect and secure cyber-related assets can be a direct (ransomware and system freezes) or indirect (data breach liability) cause of financial distress, destruction of economic value, and even business failure. The bankruptcy process itself creates additional exposure, from making private, confidential or strategic information available to a wider audience, and from making such data available over a remote communication system. Finally, how and where a company's data is stored creates hurdles for the preservation and access of information that might be critical in the post-confirmation period. abi

Reprinted with permission from the ABI Journal, Vol. XLI, No. 6, June 2022.