BRACEWELL

INSIGHTS

Ransomware: An Enterprise Risk for the Unprepared

January 20, 2022

By: ***Jason G. Cohen***

For a company with robust data protection and recovery practices, a ransomware attack may cause a few extra headaches, but it won't wipe the company out. Companies without those protections in place, however, risk allowing ransomware to bankrupt their entire enterprise.

United Structures of America, Inc. ("United Structures"), a Houston-based steel manufacture and design company, was worth $100,000,000 at the height of its business, but due to a ransomware attack in May 2019, the company has now filed for Chapter 11 protection in the U.S. Bankruptcy Court for the Southern District of Texas.

Unfortunately, the United Structures case is also one in which paying the ransom didn't secure the restoration or return of United Structures' data. The FBI has long ***advised*** that "[p]aying a ransom doesn't guarantee you or your organization will get any data back." The loss suffered by United Structures was so catastrophic that United Structure has been "methodically winding down its operations" ever since. United Structures first ***announced*** its intention to shut down its Houston facility and lay off all 79 of its employees in 2019.

According to court filings, the May 2019 ransomware attack wiped out United Structure's "data relating to accounts receivable, accounts payable, current orders, customer information, current CNC machinery files, along with essentially all of its business data." Debtors in bankruptcy are ordinarily required to provide the kinds of financial data destroyed in the May 2019 ransomware attack in various forms with their bankruptcy petitions, to creditors upon request, and in their schedules of assets and liabilities, statements of financial affairs, and disclosure statements. United Structures qualified to file under subchapter V of Chapter 11, so while it will still be required to file schedules and a statement of financial affairs, United Structures was able to avoid the petition-date filing requirements by submitting a statement under oath explaining its lack of financial information.

United Structures can also expect to benefit from subchapter V's debtor-friendly plan confirmation process. As a debtor filing under subchapter V, United Structures can confirm a plan of liquidation without the approval of any creditors, who may be frustrated with the lack of information regarding United Structures' finances. Additionally, United Structures may avoid the requirement of filing a disclosure statement, in which debtors are typically required to provide adequate information for creditors to make an informed decision about the debtor's plan to exit bankruptcy.

Victims of ransomware attacks considering bankruptcy who do not qualify for subchapter V protection are not without recourse under the Bankruptcy Code. These companies may still file for Chapter 11 bankruptcy protection, but a company with no historical financial data attempting to comply with Chapter 11's disclosure requirements would be navigating uncharted territory. These debtors should expect the lack of historical financial data to increase the time, expense, and difficulty of a bankruptcy filing, as efforts to notify creditors of the filing and provide creditors with due process will still be required.

Recommendations:

Over the past few years, ransomware has become one of the most efficient attack types for hackers seeking profit as well as one of the most destructive on the target organizations. Encrypting business files until a ransom is paid can often result in a complete disruption of business operations, and that downtime can cause large-volume financial losses for some companies. Companies must become more proactive in ensuring that their disaster recovery procedures are able to handle such sophisticated attacks. Companies should consider the following:

- To avoid enterprise-ending losses due to a ransomware attack, be proactive: implement industry best-practice data security measures, data protection policies, employee data security training, and data backup procedures.

- Policies specific to ransomware should be prepared in advance of a ransomware attack, bearing in mind that paying ransom does not guarantee that data will be restored or returned.

- If a catastrophic ransomware attack occurs before industry best-practice procedures can be implemented, consider whether your business qualifies for subchapter V protection under the bankruptcy code, which could provide a relatively low-cost path to liquidation and dissolution.

In the immediate wake of a ransomware attack, companies should reach out to trusted outside counsel and forensic vendors. But taking proactive steps to ensure that your company is prepared for a ransomware attack is always best-practice. As the United Structures case demonstrates, failing to prepare for a ransomware attack can be a fatal and costly mistake. Bracewell attorneys are ready and able to help companies prepare for and respond to ransomware and cyberattacks of all kinds.