By Mark D. Podgainy

A Cyberattack and Its Aftermath: A Case Study of Survival

It is well documented that cyberattacks have the potential to cause catastrophic economic damage to individuals and businesses. In 2022, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) received 800,944 complaints of cyberattacks or cyber-enabled frauds with a potential loss of $10.2 billion.[1] Since not every incident is reported, the potential losses are probably significantly understated.

Given the economic damage generated, the potential for a cyberattack to result in a personal or business insolvency or bankruptcy filing is high. A middle-market company was recently the subject of a debilitating ransomware[2] attack that might have led to a bankruptcy filing or closure if it were not for the extraordinary efforts of the management team, the patience of the secured lender, trade vendors and customers, and cybersecurity insurance coverage.[3] This article provides an insider's view of a middle-market company reacting to and overcoming a cyberattack to give better insight as to the nature of the issues being faced, the effort that is required to overcome them, and how such an incident can endanger a company's survival.

Mark D. Podgainy
Getzler Henrich & Associates LLC
New York

Mark Podgainy is a managing director of Getzler Henrich & Associates LLC in New York. He has 25 years of experience in operational roles and turnaround consulting in a variety of industries.

Background

AeroCo is a middle-market manufacturer of aerospace components for military and civilian applications with two locations: the Midwest and West Coast. At the time of the cyberattack, AeroCo was struggling to recover from the effects of the COVID-19 pandemic due to supply-chain disruption, labor shortages, increasing labor costs and inflation. The company was operating on a cash-flow break-even basis and had available borrowing capacity on its $28 million revolving credit line.

The Attack

In December 2022, one of AeroCo's employees was contacted by a malicious actor, who informed the employee that the company's data had been encrypted by malware and that a payment of $2 million would be required to receive an encryption key to unlock the data. During an investigation by AeroCo's information-technology (IT) staff, the company determined that its shared drives, data storage, enterprise-resource-planning (ERP) system and backup had been affected. The company immediately notified the FBI, legal counsel and its insurance company, then engaged a cybersecurity forensic firm. The FBI was able to shut down the attacker's operations on the dark web, but that was small consolation considering the damage ultimately sustained by the company.

AeroCo paid the $2 million ransom to obtain the encryption key to unlock the data, which was ultimately fully reimbursed by its insurance carrier. However, when using the key, the company determined that its data had not been completely encrypted, but it had been corrupted during the encryption process. Further, the most recent backup that the company was able to restore was Nov, 23, 2022. In assessing the damage, management realized that it was faced with a situation where the company's core systems were inoperable and approximately six weeks of data had been lost, thus crippling the company's ability to perform its critical functions, such as manufacturing, shipping, invoicing, paying bills and reporting. It also imperiled its survival, and AeroCo was in a race to get back up and running quickly before it ran out of cash.

The Action Plan

AeroCo's management rapidly developed an action plan that consisted of several components.

Communication

The company created tailored messaging about the cyberattack that was shared with its key constituents, including the following:

- *Employees*: AeroCo needed its team to rally together to restore the company to a healthy status, especially considering that there were likely to be long days ahead to get there;
- *Customers:* AeroCo had to inform customers of delays in shipments, request waivers for possible late shipment fees and provide updates on timing of future shipments;
- *Vendors/trade:* Management leveraged its strong vendor relationships to request extended payment terms while continuing to accept previously scheduled shipments; and

1 FBI's 2022 Internet Crime Report.
2 Ransomware is a type of malware that blocks access to a system, device or file until a ransom has been paid. This is achieved by encrypting files on the endpoint, threatening to erase files, or blocking system access. *See* Center for Internet Security.
3 The author's firm worked with AeroCo on this matter.

• *Lender:* AeroCo had to communicate that its regular reporting (*e.g.*, financial statements, borrowing base certificates, etc.) would be delayed and that there would be a significant impact on business operations and financial performance.

Restarting Manufacturing Operations

Since AeroCo was unable to use its ERP system, it had to operate manually. This meant that the movement of raw materials, work-in-process and finished goods, and manufacturing labor and machine hours used throughout both plants had to be tracked using paper forms with related information entered into Excel spreadsheets. Management, in consultation with employees, developed appropriate procedures and processes to implement manual tracking so that core functions could restart.

Recovering Systems and Data

The company planned to work with its internal and external IT specialists to restore its ERP system, shared drives and data storage. While that was happening, employees in finance and accounting — supplemented with temporary staff — set up systems and processes to manually re-enter data, based on physical records (invoices to customers, invoices from vendors, etc.), and to maintain the books and records of the company going forward until the ERP system was operable.

Improving Cyberdefenses

Once AeroCo's operations stabilized, management planned to focus on improving its cyberdefenses, with a focus on better endpoint[4] protection, data backup and restoration, and disaster-recovery policies and procedures.

What Happened

AeroCo's employees came together as a team and swiftly executed the plan but struggled to restart production and shipments. In January, revenue was approximately 25 percent of management's plan, a shortfall of approximately $4.5 million. Further, operating manually was inefficient and costly, driving payroll costs up and margins down. Restoration of the ERP system was going slowly, but the system was finally operable in the beginning of February, enabling the company to input data from the date of the last backup in November and begin the work required to close the December books. By the end of January, the company had regained its shared drives.

Most vendors, while not happy about the situation, were willing to extend payment of invoices, which provided a crucial lifeline while production and shipments got back on track. Similarly, customers worked with the company's estimated revised shipment dates and did not cancel orders, with some customers later agreeing to accelerate payments. The lender was initially patient with AeroCo, but by the end of January, since the company still could not certify a borrowing base, grew concerned about the value of the collateral supporting the loan and the company's liquidity requirements. The lender issued a default notice due to AeroCo's failure to provide certified borrowing base certificates and, as a defensive measure, put an availability block on the borrowing base, effectively reducing AeroCo's borrowing capacity. Further, the lender requested that the company retain a financial advisory firm to independently review the company's 13-week cash-flow forecast and borrowing base and assess the company's financial reporting capabilities in light of the cyberattack.

March

By the beginning of March, AeroCo had made slow but steady progress in getting its data into the ERP system and catching up on reporting. The company had closed the books for December, had entered data through mid-February and was working on closing the books for January. However, sales, transactions and general activity were still largely manually maintained. The company was producing borrowing base certificates using the same inventory and accounts receivable ineligibles values as of month-end November, but would not certify them since it was unable to verify all of the data.

With the assistance of its newly retained financial advisor, AeroCo completed and presented a cash-flow projection to its lenders at the beginning of March, which indicated that it would burn through almost $12 million of cash through the end of May and would only start generating cash in June. This would require the loan balance to increase from $11 million to $23 million and result in an overadvance, which was forecasted to peak at $6.6 million by the end of May.

Once the lender had visibility into the cash flow and borrowing base, it adopted a collaborative approach and worked with AeroCo to resolve the issues related to the loan, including a verbal agreement to eliminate the $4 million availability block, which lowered the overadvance hurdle. Along the same lines, AeroCo and its financial advisor identified several opportunities to reduce or eliminate the forecasted overadvance, including (1) reducing capital expenditures to a "maintenance only" level; (2) repatriating excess cash from its foreign subsidiary; (3) obtaining more favorable payment terms from certain customers on a temporary basis; (4) identifying and executing short-term sales opportunities to drive revenue; (5) selling slow-moving inventory; (6) obtaining a minority equity investment from a third party; and (7) investigating a sale/leaseback of a piece of retail estate to inject cash into the business.

AeroCo was particularly concerned about further deferring vendor payments, as management believed that vendors were stretched as much as possible, and that further concessions might impair future performance and relationships. The forecast included an increase in vendor payments in April to reduce the pressure from payments that were deferred in January and February, and the company was not willing to go back to the vendors to seek help in reducing the overadvance.

Meanwhile, the IT staff, with the assistance of outside consultants, was revamping its approach to cybersecurity. First, AeroCo replaced its endpoint protection vendor and added capabilities so that it could not only detect malware and other typical threats, but detect more advanced threats

4 Endpoints are entry points of end-user devices such as desktops, laptops and mobile devices. Endpoint security is viewed as the front line of cybersecurity. *See* Trellix.

continued on page 54

from page 17

(*e.g.*, fileless malware, polymorphic attacks, etc.) and also respond to threats. Second, it replaced its legacy backup system with daily cloud backups. Finally, the company established disaster-recovery procedures should it experience another cyberattack, and began testing recovery of daily backups to ensure that its data could be fully restored.

May

By the beginning of May, AeroCo had completed all data entry and resumed using its ERP system. The finance and accounting staff had closed the books for March and was far along in closing April. A physical inventory had been conducted at the beginning of April, with cycle-counting subsequently implemented, which gave management confidence in its inventory numbers for the first time since December. Management was now in a position to certify borrowing base certificates for the first time since the cyberattack.

Throughout April, management had been hard at work negotiating a forbearance agreement with the lender, which was executed in early May. The agreement required AeroCo to provide monthly financial statements since the cyberattack according to a set schedule, provide weekly rolling cash forecasts and borrowing base certificates, and retain an investment banker to investigate strategic options, including a sale or refinancing, that would lead to payment of the outstanding loan balance in full. In return, the lender agreed to reduce the reserves under the borrowing base and stop testing the fixed-charge coverage ratio, which was a covenant in the credit agreement.

By the end of May, five months after the ransomware attack, AeroCo's operations were almost restored to their pre-attack state. In addition, management eliminated the overadvance by implementing many of the aforementioned ideas and obtaining the lender's cooperation in reducing the borrowing base reserves.

Post-Mortem

It took six months for AeroCo to fully recover operationally from the ransomware attack. In the first three months following the attack, it lost approximately $6 million in sales and incurred approximately $4.5 million of incremental costs. AeroCo avoided running out of cash thanks to the strong relationships that management had maintained over time with its lender, vendors, customers and employees, and an effective cybersecurity policy that reimbursed the company for $3 million of the costs it incurred. Though an outcome of its lender's requirement in the forbearance agreement that the company repay its outstanding loan may be that the company ceases to remain independent, AeroCo was fortunate to survive the ransomware attack.

One of the key lessons learned was related to the company's legacy backup system and procedures. First, AeroCo had relied on a backup system that was susceptible to a cyberattack. Second, the company had never walked through restoration of its data using the backup system, which resulted in significant time, effort and money expended in the restoration process.

Conclusion

In theory, companies operate every day with the risk of a cyberattack, and management should put processes, systems and people in place to minimize that risk. However, understanding an actual cyberattack and its aftermath brings to life just how fragile companies are and how close they can come to bankruptcy or closure, and can help management teams and professionals be better equipped to plan and respond. abi