Cyber Liability

Lessons From the Colonial Pipeline Breach

One of the nation's largest pipelines was forced to shut down in early May 2021 after falling victim to a ransomware attack. The 5,500-mile pipeline is operated by Colonial Pipeline and carries refined gasoline and jet fuel from Texas to New York. This pipeline transports 45% of the east coast's fuel supplies.

The attack—carried out by DarkSide ransomware—resulted in gas shortages along the east coast due to Colonial Pipeline halting their operations in an effort to contain the breach. DarkSide reportedly stole 100 gigabytes of data from Colonial Pipeline and allegedly threatened to leak portions of it to the public unless a $5 million ransom was paid. This method, known as double extortion, involves cybercriminals not only encrypting stolen data and making it inaccessible but also threatening to release it.

Key Takeaways

The shutdown served as a reminder and warning of the catastrophic impact ransomware can have on businesses—especially those with aging IT infrastructure—and people. There are a few key takeaways from the breach, including:

- **The threat of ransomware-as-a-service (RaaS)**—DarkSide ransomware operates as RaaS, meaning cybercriminals subscribe to their tools to execute ransomware attacks. This is significant because, in the past, hackers had to have coding expertise to be successful. With RaaS, however, users don't need to be skilled or experienced to carry out sophisticated attacks. RaaS empowers novice hackers by providing them with an easy-to-use system for deploying ransomware.
- **The impact of double extortion**—Double extortion increases the stakes of a ransomware attack. Rather than only deleting data if the ransom isn't paid, cybercriminals threaten to leak it. Since Colonial Pipeline did have backup data available to them, it would have been possible to wipe and restore their infrastructure without paying the ransom. However, they paid the ransom to keep their data from being exposed.
- **The risks posed by aging infrastructure**—Old and obsolete operating systems may be easier for cybercriminals to infiltrate. By exploiting vulnerabilities in the outdated network, cybercriminals can gain access to sensitive data and hold it for ransom.

Preventive Measures

Organizations can take the following actions to ensure that ransomware attacks don't compromise their operations and data:

- **Conduct a security risk evaluation.** Take time to identify which critical systems and assets are most appealing to cybercriminals. By doing this, businesses can get a better idea of how to prioritize protection.
- **Keep systems up to date.** Update operating systems, applications and software regularly. Applying the latest updates improves systems, fixes problems and corrects any security issues discovered by developers.
- **Maintain data backups.** The Multi-State Information Sharing and Analysis Center reports that backing up important data is the most effective way for organizations to recover from a ransomware attack. Backups should be stored offline, out-of-band or in a cloud service so attackers can't target them. They should also be tested regularly for efficacy.
- **Train the team.** Some of the most damaging cyberattacks occur due to human error. Training employees on the importance of cybersecurity and how to identify scams can help organizations reduce the likelihood of becoming a victim of ransomware attacks.

- **Install antivirus software.** Antivirus software protects against many cyberthreats, including viruses, spyware, malware, Trojans, phishing attacks, rootkits and spam attacks.

If an attack occurs, organizations should have an incident response plan ready with defined roles and communications that can be shared during an attack. Organizations that are overly cautious and plan proactively may be able to minimize damage.

For additional risk management guidance and insurance solutions, contact us today.

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.