BRUSH CREEK PARTNERS
benefits • risk management • personal lines • retirement

bcptech white paper | august 2019

Ransomware Attacks & Best Practices

Ransomware has quickly developed into one of the most significant and lethal threats to companies today. This summer, ransomware attacks have hit all industries but cities, towns, and government organizations have received the most attention.

Ransomware Defined

Ransomware is a type of malicious software, also known as malware, that allows attackers to extort companies for financial gain. They do this by blocking access to files on a computer or network until the company pays the ransom demand. This type of malware generally is self-proliferating and encrypts data on the network, rendering it inaccessible and essentially useless. In order to de-crypt the data, companies must pay the attacker a ransom or attempt to recreate or restore the data from backups. It's also not a given that you'll get your data back in full after paying a ransom.

During this process, companies also suffer extended disruptions in their operations, and will likely deal with litigation and regulatory inquiries following the incident. Once public, the reputational impact can be long-lasting.

Recent Attacks

According to recent reports, ransomware attacks have increased by 195% from the fourth quarter of 2018 to the first quarter of 2019. And no industry is immune: higher education, healthcare, municipalities, and shipping companies have all been hit. The ransomware attacks on local and state governments have been so prevalent that the U.S. Conference of Mayors agreed it will no longer pay ransom demands from hackers, hoping to discourage continued attacks.

The resolution, which is not legally binding, states in part, "the United States Conference of Mayors has a vested interest in de-incentivizing these attacks to prevent further harm, therefore be it resolved that the United States Conference of Mayors stands united against paying ransoms in the event of an IT security breach." The resolution aligns the group with the FBI, which dissuades victims from paying the hackers.

However, the attacks don't seem to have slowed down. Just last week, 23 Texas towns were hit by a coordinated ransomware attack, according to the state's Department of Information Resources. The attacks started the morning of August 16th, and the Governor order a "Level 2 Escalated Response" following the incident. The Governor also deployed cybersecurity experts to affected areas to assist with response.

The attacks in Texas follow recent state and local ransomware attacks in New York, Louisiana, Maryland, and Florida over the course of the summer.

In July, the Governor of Louisiana declared a cybersecurity state of emergency following a series of attacks on school districts throughout the state. The declaration allowed Louisiana to access resources from the state's national guard, technology office, state police, and other organizations. According to the declaration, the state of emergency will remain in place until August 21 unless terminated sooner. This is only the second time a state of emergency has been declared related to a cyber incident; Colorado declared one in 2018 after the Colorado Department of Transportation was hit with a ransomware attack.

> *"According to recent reports, ransomware attacks have increased by 195% from the fourth quarter of 2018 to the first quarter of 2019"*

To Pay or Not to Pay?

In June, Lake City, Florida suffered a ransomware attack that crippled their systems for nearly two weeks. They ultimately decided it would be cheaper and more effective to pay the hackers the 42 Bitcoin (approximately $462,000) demanded. Riviera Beach, Florida also made the decision to pay the almost $600,000 demand after experiencing nearly two weeks of down time following a ransomware attack. Based upon reports, both cities had insurance policies that covered the payment.

In contrast, the city of Baltimore refused to pay the $76,000 demand after they suffered a similar ransomware attack in May that resulted in a nearly month-long IT outage. Recent reports indicate the attack cost the city an estimated $18M, and it will still be months before Baltimore's systems are fully functional. It is unclear whether Baltimore had insurance that would have covered a potential payment.

According to research by Sentinel One, 45% of organizations pay at least one ransom when hit by ransomware attacks. The FBI discourages payment of the ransom demands, however, the determination whether to pay is ultimately a business decision. Regardless, the FBI should be consulted during a ransomware attack. In addition to providing resources, the FBI can gather intelligence about who's conducting these activities, and hopefully that information can be used to apprehend the responsible individuals.

Ideally, the decision to pay or not pay will never come to fruition, but in reality, a company cannot completely prevent a cyberattack, and should be prepared to respond. A number of "best practices" can be followed to reduce the risk of suffering an attack, and the consequences if one occurs.

Preventative Measures

- Regular Backups

Regularly backing-up systems greatly reduces the impact of a ransomware attack. If a company is able to access the backups during an attack, the company can restore the encrypted data and files without having to pay the ransom. The backups need to occur regularly, and should be isolated from the company's primary network, so the infection cannot spread and infect the backups. It's also important to make sure you know how to restore your data from a backup.

- Patching

Because ransomware often takes advantage of software and computer vulnerabilities, it's imperative companies keep all systems patched and up to date.

- Education and Training

Human error is a leading cause of cyberattacks as the criminals prey on a user's inattentiveness or lack of knowledge. Employees should be able to recognize the signs of a phishing attack. Links and attachments should be examined to confirm they are from reliable sources, and employees should never give out company or personal information in response to an email, letter, or phone call. In addition to proactive education, employees should know who to alert and how to respond to a suspected ransomware attack. Immediate response is necessary to limit the potential harm.

Conclusion

Even with the implementation of best practices, it's likely a company will fall victim to a ransomware attack. As part of a wholistic risk management strategy, companies should consider purchasing a cyber liability insurance policy that can help them respond to a ransomware attack. The policy will also help cover the financial impacts associated with such an attack beyond simply paying the ransom.

Any one of the bcp.tech team members would be happy to discuss your technology or cyber liability insurance needs. Please reach out with any questions.

Your bcp.tech team

Travis Holt, Partner

- Mobile: 210.896.3101
- Email: travis.holt@brushkc.com

Stephen Bowen, Partner

- Mobile: 913.486.3509
- Email: stephen.bowen@brushkc.com

Emily Short, Vice President of Technology Risk

- Mobile: 913.593.9006
- Email: emily.short@brushkc.com

Kyle Kelley, Account Executive

- Direct: 816.768.8243
- Email: kyle@brushkc.com

Maria Blando, Account Manager

- Direct: 816.768.8242
- Email: maria@brushkc.com

Jake Durham, Risk Consultant

- Mobile: 432.556.1698
- Email: jake.durham@brushkc.com

About Brush Creek Partners

Brush Creek Partners offers risk management and insurance solutions to mid enterprise businesses across many industry verticals, with a particular focus on technology, venture capital, and private equity risks. Brush Creek's technology and cyber experts assist in determining how to transfer risk through contracts and insurance to help quantify technology risk on the balance sheet. With deep industry and product experience, our experts are able to deliver solutions for each client's unique risk profile.

Visit us at bcptech.co