THE NATIONAL LAW REVIEW

Is Your Business Prepared To Survive A Ransomware Attack In 2019?

BARNES & THORNBURG LLP

Article By Scott N. Godes
Jason A. BernsteinTodd G. Vare
Brian J. McGinnisBarnes & Thornburg LLP

Data Security and Privacy and
EDiscovery, Data & Document
Management Law
Communications, Media & Internet
Criminal Law / Business Crimes
All Federal

Friday, June 14, 2019

Last month, the global cyber risk and insurance company Beazley reported a dramatic increase in ransomware attacks. According to their tally of insurance claims and data analytics, ransomware attacks increased a whopping 105% in the first quarter of 2019 over the first quarter 2018 statistics.

Further, PhoenixNAP Global IT Services predicts that a new organization will suffer a ransomware attack every fourteen seconds in 2019. The financial losses due to an attack can be staggering; though a rarely reported point is that while data, computers, servers, and more are inaccessible, businesses are losing revenues and spending money to bring their systems back up to speed. As such, total financial damage due to ransomware is expected to top $11.5 billion in 2019.

Ransomware is a type of malware in which a computer system is encrypted by the hacker preventing the owner from accessing their own files. The term “ransomware” was coined because the hacker typically demands a ransom payment to release the files back to the owner. The first three months of 2019 revealed a $224,871 average ransom payment, representing a 93% increase in the payment demand over the 2018 average demand.

Despite the efforts of cybersecurity companies to detect and respond to ransomware attacks, cyber hackers continue to develop new variants that can elude security software. The latest resurgence in ransomware is due to new variants like GandCrab and SamSam, which prey on remote desktop users to gain access to a company’s entire network.

Phishing emails also continue to be a huge source of vulnerability for businesses. Hackers con employees by sending a phony email that looks very real. The email contains a link, and when the employee clicks on the link, the malware is released. Ryuk and Bitpaymer are sophisticated ransomware variants that can be launched into a company’s network by unsuspecting employees that fall victim to phishing emails.

There have been a number of high-profile ransomware attacks in recent months, such as the Delaware Guidance Services for Children and Youth, in which the records of 50,000 children were compromised, and the City of Baltimore, which estimates an $18 million loss due to an attack. Private companies such as Norsk Hydro, a worldwide aluminum producer, and Arizona Beverages, one of America’s largest beverage suppliers, have also become victims of the surge in ransomware attacks.

Beazley reports that hackers are targeting larger organizations and demanding higher ransom payments. The highest payment demand reported in 2018 was $8.5 million; the highest payout was $935,000. The decision whether to pay a ransom is made on a case-by-case basis, by the individual organization being impacted. Factors to consider in the decision include: whether there is a recent and uninfected data backup, the amount of the demand, the likelihood of the hacker returning the data, the impact of potential data loss or exposure to the company and its customers, and the organization’s stance on making a payout to a criminal. An IBM study indicates that 25% of businesses would pay more than $20,000 to retrieve stolen data, but another study shows that less than one-third of those who pay the ransom receive all of their data back.

But what rarely is reported is the true financial impact on businesses of ransomware beyond the cost of the ransom or the consideration of:

- How much revenue would your organization lose if it was unable to access data, computers, servers, and more during a week-long outage?
- How much would your organization have to pay to forensic consultants, lawyers, and others to bring the networks back up to speed and ensure that the systems are clean?
- How much will the organization pay to clean machines—if they can be cleaned quickly and effectively (often they cannot)—or to replace infected and damaged machines?
- Will third parties, such as customers, vendors, or consumers, make claims or file suits against the victim organization, seeking damages as a result of their losses?

With such potentially significant financial impact on an organization, it is critical to consider your financial risk transfer, both through insurance coverage and business contracts:

- Does your organization carry insurance coverage for a ransomware event?
- Are your organization's contracts structured to address the consequences of a third party's involvement with a ransomware event that affects your organization?

The potentially devastating effects of a ransomware attack make it clear that best defense is a strong offense. Here are some questions your organization should be asking to shore up your offensive game plan against ransomware attacks.

1. **Incident Response Plan:** Do we have an incident response plan and have we exercised it? Does our incident response plan have a playbook for what to do in the event of a ransomware attack?
2. **Backups:** Do we back up all critical information? How frequently? Are the backups stored offline or on the cloud? Have we tested our ability to revert to backups during an incident? If we are hit with a ransomware attack, are our backups frequent enough to enable us to restore without unmanageable loss of data? Will our backups be affected by the ransomware? Are our providers able to provide backups in the way that they promised? What happens if they cannot?
3. **Network Access:** Have we segregated and minimized access to critical data? Are we using VPNs for wireless network access? How secure is our remote access system? Are we using two-factor authentication? Do we have an account lockout procedure?
4. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
5. **Staff Training:** Have we trained staff on cybersecurity best practices?
6. **Vulnerability Patching:** Have we timely implemented appropriate patching of known system vulnerabilities?
7. **Application Whitelisting:** Do we allow only approved programs to run on our networks?
8. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
9. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?
10. **Insurance Coverage:** How would our insurance program respond to a ransomware event? Do we have insurance coverage for the costs of paying a ransom, hiring a forensic investigator, hiring legal counsel to coordinate the response, for remediation, for lost revenues, for defending against and paying to resolve third party claims, for a customer resolution program, and other expenses resulting from an attack?
11. **Business Contracts:** How do we structure our contracts with customers and business partners? Do we have indemnification clauses that would address a ransomware event?

Source URL: https://www.natlawreview.com/article/your-business-prepared-to-survive-ransomware-attack-2019