LESSONS LEARNED

THIRD-PARTY
CYBER
VENDORS

CIRMA

January 2020 | No. 16

Third-Party Cyber Vendors

SCENARIO

The municipality experienced a ransomware attack that encrypted 7 servers, 4 of the servers housed business critical information, such as Human Resource personnel and payroll information, along with 128 desk top computers. Once notification was made, CIRMA initiated its cyber response process. This included initial calls with privacy counsel and forensic investigators, and CIRMA's notification to the Connecticut Intelligence Center (CTIC).

The municipality was working with their third party I.T. provider on decryption efforts 7 days prior to contacting CIRMA. Shortly after CIRMA began its process it was determined that the municipality would be required to pay the ransom, $42,500 - 4.5 bitcoins based on the daily value at the time of the attack. Upon payment of the ransom, the municipality received a set of decryption keys and after three (3) days the municipality had all 4 business critical servers and approximately 90% of the affected desktop units decrypted. The forensic investigation lasted another 4 weeks.

INVESTIGATION AND DAMAGES/INJURY

It was stated by the municipal leadership that they only thought to contact CIRMA to determine if this would be a covered loss; specifically, if the payment of the ransom would be covered by insurance. They were unaware of the importance of contacting local law enforcement until it was discussed with them by CIRMA. Once notified, CIRMA reported the incident to CTIC as per CIRMA's cyber response protocols. During the CIRMA investigation, it was determined that this municipality utilized a third-party I.T. vendor as their Managing Service Provider (M.S.P.)

The M.S.P. and municipality had a standard third-party vendor agreement; however, the agreement was not favorable to the municipality and contained the below language:

> *"…the municipality is responsible for any and all costs, including legal fees, forensics, data restorations, and third party actions made against the municipality or "X" company for any data breach or cyber incident, including but not limited to data encryption, loss of encrypted data, damage to physical equipment, release of personally identifiable information (P.I.I.) and associated state required credit monitoring…. and holds "X" company harmless and waives its ability to seek payments for any of the acts above or any legal action resulting from the acts above… regardless of any fault by "X" that contributed to any of the above…".*

The M.S.P. was responsible for data management, regular network maintenance and security. The M.S.P. would access the municipality's network through two vectors: 1. Remote Desk Top (RDP) access, or 2. Virtual Private Network (VPN). They would run diagnostics, push updates and manage the municipalities back up protocols. Back up servers where located at the M.S.P.'s location Further forensics showed that the initial malware entered the municipality's network through the M.S.P.'s RDP address into the municipality's network. Once the malware entered the network it was able to "write itself" as an administrator and access the back up. It was determined that the malware entered the M.S.P. network through an email that contained a type of banking malware called Emotet. This was introduced into the M.S.P.'s network by one of their other clients who had downloaded a malicious file from a phishing email. Because the backups were potentially exposed, this created a very low confidence by the forensic investigators in the ability to recover from backups. The most viable back up information was approximately 9 month old. After consulting with counsel and the forensic investigators, it was determined that the ransom would need to be paid to recover the data. Contact was made with the threat actor and arrangements were made to pay the ransom. Once paid the threat actor provided several decryption keys, and after three (3) days the municipality had all 4 business critical servers and approximately 90% of the affected desk top units decrypted. The forensic investigators continued their scope of work to insure that no "Trojans" had been left on the municipality's desktop devices or on premises servers. Forensic investigators also determined that there was no exfiltration of PII. At the time of the incident, the municipality was a CIRMA Liability-Auto-Property (LAP) member, therefore the loss was a covered through CIRMA's cyber and data breach policy. The policy provides coverage for a data breach of sensitive information from intentional hacking of a computer system or through stolen information from lost or misplaced hardware, whether through the actions of an employee or an outsider.

CIRMA's Cyber Insurance policy includes coverage for notification and ID/credit monitoring expenses as outlined by the State of Connecticut's Public Act 15-142 concerning data breaches for Connecticut organizations. The policy also provides many other coverages such as:

- Forensic investigation
- Security & privacy liability
- Data recovery

- continued on back

Total cost of loss:	**$226,500**
CIRMA cyber coverage deductible	$10,000
Ransom	$42,500
Forensics & Restoration	$135,000
Privacy Counsel	$34,000
Misc. Legal Fees	$5,000

LESSONS LEARNED

- **Utilize CIRMA's contract review process when entering into third-party M.S.P. contacts.** As a best practice, CIRMA recommends that any contract your municipality enters into be reviewed by CIRMA's Contract Review Team to identify contract language that may transfer risk to you unnecessarily and to ensure that your interests are protected. Many standard form contracts that are used today contain several waivers of subrogation throughout the contract that may limit CIRMA's ability to hold responsible parties accountable for losses.
- **Identify how the M.S.P. will be accessing your networks and establish protocols for this access.** This should be clearly defined with the contractual agreement.
- **Report all incidents immediately to CIRMA, local law enforcement, and CTIC.** Local law enforcement can access resources from the State of Connecticut Intelligence Center and Connecticut State Police Cyber Crimes unit. These special departments may have additional resources that can aid in the recovery of data.
- **Ensure back up are properly protected and separated from "live" or "production" environments.** It is a risk management best practice to separate data back up from the "live" network. This reduces the likelihood of the backup network being affected by any malicious software. Having a secure back up protocol will reduce the likelihood of paying any ransom. Language should be included in third party MSP agreements as to the municipality's expectations of the process for securing and separating back up networks.

For more information on this topic, please contact your CIRMA Risk Management Consultant.