CYBERATTACKS AND RANSOMWARE DEMANDS ON MUNICIPAL GOVERNMENTS AND SMEs

By Kamala Raghavan, CPA, CFP, CFF, CGMA

Municipal governments and small to medium (SME) enterprises are facing an escalating number of cyberattacks and ransom demands. These attacks are crippling their systems and costing them funds that could be deployed to increase stakeholder services. "Ransomware is a pandemic in the United States," said Joel DeCapua, supervisory special agent in the Federal Bureau of Investigation's cyber division referring to the malicious software deployed by hackers who are increasingly going after smaller targets.

Municipal governments and SMEs are attractive targets for the criminals due to their vulnerable technology infrastructure and weak cybersecurity protocols as compared to the corporate sector. These organizations are increasingly using loosely integrated networks of information systems to deliver services to stakeholders and are generally not prepared to combat data breaches due to limited resources. They are also relying increasingly on small third-party outsourced technology providers who are not able to protect sensitive stakeholder information.

It's hard to quantify the total impact of ransomware attacks because most are not publicly reported. This article discusses several incidents and offers a suggested preventive, detective and corrective procedures' framework for use by managers and auditors in reviewing and monitoring compliance, with the goal of avoiding expensive corrective actions after the incident.

Current Situation

While most ransomware attacks of earlier years targeted home computers, the attackers have moved to the more attractive targets of municipal governments and SMEs, which face pressure to resume services to their stakeholders quickly for their survival. The recent attacks from state-sponsored hackers have been targeting the bigger prize of the U.S. federal government to gain access to defense secrets and citizens' data more and more. So far, these attackers have not demanded ransom money but seem to be more interested in accessing the U.S. defense and research data.

This article focuses only on the lesser scope of municipal and SME security breaches for ransom money.

Following are examples of some attacks:

- Travelex, the foreign exchange shop operator, was infiltrated in January 2020 by hackers and had to pay about $2.3 million in ransom. It was attacked by a malware known as "Sodinokibi."
- In June 2019, two Florida cities, Lake City and Riviera Beach, had their 911 systems compromised and the systems could not be operated. Lake City paid $460,000 in cryptocurrency and Riviera Beach paid $600,000 in bitcoin.
- Hackensack Meridian Health in New Jersey suffered a ransomware attack in December 2019. The attack forced cancellation of surgeries and other procedures. The hospital system paid an undisclosed amount to the hackers, worked to restore its computer networks over a few weeks, and hired cybersecurity and forensic experts to investigate.
- The cyberattack on the City of Atlanta's network happened in March 2018 and a federal grand jury in Atlanta indicted two Iranian nationals in December. Both men remain wanted by the FBI. The City of Atlanta refused to pay a ransom of $51,000 in bitcoin and suffered millions of dollars in losses from the attack.
- Imperial County, California suffered a breach in April 2019, with hackers demanding payment of $1.2 million. Secure backup data helped the county avoid paying the ransom, and the county spent about $1.6 million to beef up equipment and security. The costs were largely covered by a cyber-insurance policy.

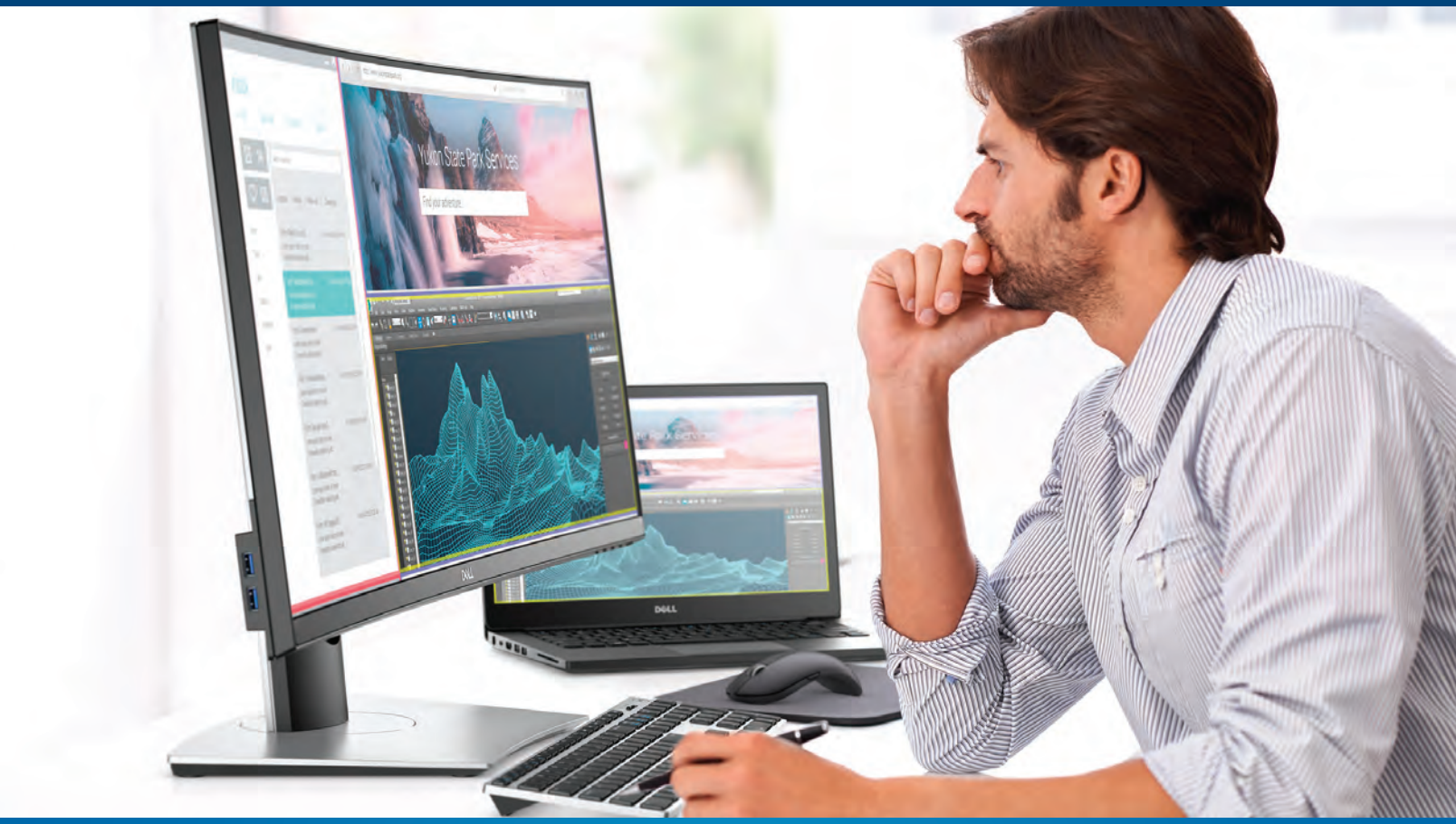
Table 1.

Preventive, Detective and Corrective Procedures to Monitor – Management

- ✔ Ensure collection and correlation of data across sources.
- ✔ Train a talented workforce.
- ✔ Keep systems, network and malware definitions up to date.
- ✔ Invest in staff training, especially in cybersecurity.
- ✔ Follow a strict data protection process, including analyzing system vulnerabilities frequently, keeping systems updated and data files backed up regularly.
- ✔ Promote data-driven decision-making.
- ✔ Install software for regularly scanning systems for viruses and malware.
- ✔ Monitor cybersecurity assessment and conduct frequent cybersecurity audits.
- ✔ Communicate with stakeholders.
- ✔ Ensure that tape and disk-based backups are encrypted to deter easy access to data, and that offline and online backups of critical data are kept.
- ✔ Implement multifactor authentication for all crucial data and login protocols.
- ✔ Have an incident response team in place with a team leader designated and an incident response plan. Keep a hard copy of the incident response plan available and have a predesignated site for the incident response team to gather.
- ✔ Have a public relations and communication plan to inform law enforcement and other interested parties.
- ✔ Ensure that internal auditors are trained to provide guidance on best practices to protect the organization moving forward.

Article continues on page 17

Dell Technologies is excited to offer TXCPA members exclusive benefits.



TXCPA Members save an extra 5-10% off! Contact Dell's Account Executive for TXCPA, Amy, at **Amy_Henry@Dell.com** or call **855-900-5548** to speak with a Small Business Advisor.

DELL Technologies

- The City of Baltimore suffered an attack on May 7, 2019, with more than one group breaching the computer network. The attack delayed home sales and prevented the city from issuing water bills. The computer and email access for some employees was restored after a few months. Baltimore refused to pay a $76,000 ransom but estimated that the attack cost $18.2 million in losses and restoration expenses.

Risk Factors and Surveys

Municipal governments and SMEs operate networks of disparate and loosely connected information systems to deliver services to stakeholders efficiently but have limited cybersecurity talent and financial and software resources. Most ransomware attacks happen when an employee unknowingly opens a link or an attachment in a phishing email or are the result of a vulnerable cybersecurity system. The ransomware blocks data files and the attackers send demands for the files to be unlocked in return for a payment, typically in cryptocurrency.

An Accenture security survey of more than 2,600 security professionals from 355 companies in 11 countries in various industries found that the average annual cost of cybercrime per company jumped from $11.7 million in 2017 to $13 million in 2018. The study included four categories of internal activity: cybercrime discovery, investigation, containment and recovery. The authors estimated the total value at risk from cybercrime in the next five years at $5.2 trillion.

IBM's "Cost of a Data Breach Study" by the Ponemon Institute in 2018 found that the average cost of a data breach globally increased 6.4% year over year to $3.68 million. With one million records breached, the average total cost from the incident is $40 million and with 50 million records, the cost becomes $350 million. The likelihood of a recurring breach is 27.9%. The Ponemon Institute survey estimates that 70% of small and medium sized businesses report experiencing a cyber-attack.

Verizon's 2019 Data Breaches Investigation Report found that 43% of cyber-attacks are targeted at small businesses. And in its report entitled "Seven Hidden Costs of a Cyber-attack," Deloitte listed the following as costs: investigation, cost from loss of customer confidence, regulations, legal costs, public relations, hardware and software changes, insurance, reputational loss, debt and equity costs, contract losses, etc.

In addition, reconciliation and remediation costs can run quite high even after paying the ransom.

Government organizations and SMEs face tough decisions when it comes to balancing crippled operations to stakeholders versus paying off hackers to try to limit damage. There is no guarantee that payment of ransoms will lead to recovery of data. The global survey by Cyber Edge in 2018 found that 40% of victims that paid a ransom did not get their data back.

Many of the ransomware attacks exploit the weaknesses in the systems of Managed Service Providers (MSP) used by municipal governments and SMEs to reduce costs. While many MSPs offer reliable support and data storage, they provide a convenient pipeline for hackers to infect many computers in a single attempt.

A typical example was the attack on 23 Texas cities and towns using the vulnerabilities in their MSP, TSM Consulting Services. One town was hit with ransomware twice in the past year through TSM. MSPs that are lax with clients' backup and their own cybersecurity protocol end up paying ransoms to the attackers, thereby rewarding the attackers. Attackers have capitalized on preventable security weaknesses such as weak passwords and lack of two-factor authentication in the MSP's operations.

The most widely used malware Ryuk is based on the source code of an earlier ransomware called Hermes found in Russian cybercrime forums. Ryuk is deployed through a multistep campaign to get deep into the organizations' systems using remote access, gathering information and releasing ransomware.

Ryuk's victim list includes Onondaga County Public Libraries, the Syracuse public school system, the Butler County federated library system in Pennsylvania, and Collierville, Tennessee. The list is expanding due to the poor cybersecurity protocol at smaller organizations, their MSPs and lack of in-house technology professionals.

Ransomware attacks are also exposing the weaknesses in state-owned enterprises' systems as witnessed by the 2019 attack on the

CONGRATULATIONS TO DR. KAMALA RAGHAVAN ON BEING ELECTED TO THE FULBRIGHT ASSOCIATION BOARD OF DIRECTORS!

Table 2.

Preventive, Detective and Corrective Measures to Monitor – Audit

- ✔ Review organization chart of management and certifications of IS personnel.
- ✔ Review minutes of board governance, technology and audit committees.
- ✔ Review IS operating policies, including due diligence in vendor management and core software vendor release updates.
- ✔ Review insurance policies on equipment and facilities, business interruption and fraud.
- ✔ Review contracts with third party data processor, software and hardware service providers.
- ✔ Review the disaster recovery programs and testing of the above vendors.
- ✔ Review policies for software update installations and test compliance.
- ✔ Review management of software licenses.
- ✔ Test and verify acquisition of new and existing technology equipment and software, and the development of data mining and reports.
- ✔ Review separation of duties and permissions granted to personnel.
- ✔ Review and test information security and risk management programs.
- ✔ Review controls on network access, firewalls, reports and documentation.
- ✔ Test, or at a minimum review, reports on vulnerability assessments.
- ✔ Review and test physical security measures.
- ✔ Review documentation on standards and policies and ensure that they are updated.
- ✔ Review business continuity plans, including hot site readiness and vendor agreements.

state-owned oil and gas company, Petroleos Mexicanos, disrupting its billing systems and affecting supply chain operations. Norse Hydro ASA, Saudi Aramco and Rosemont PJSC were also attacked.

Such attacks on state-owned entities make one wonder if their safety procedures are worse than their corporate counterparts.

Risk Reduction Strategies

Preventive and detective steps can deflect ransomware attacks and minimize the damages to organizations. Preventive steps include purchasing cyber insurance, hiring technology talent including artificial intelligence (AI), and training of staff in basic system hygiene.

Many large U.S. cities and SMEs have purchased cyber insurance. For example, Houston has purchased a $30 million cybersecurity insurance policy with $471,400 annual premium, while Boston, Nashville, Dallas, Denver, Detroit, San Diego, San Jose, and Washington D.C. are in the process. However, cyber insurance can act as a double-edged sword by providing a false sense of protection and encouraging the hackers to increase the attacks aggressively.

As municipalities and SMEs struggle to deal with ransomware attacks, many of them are looking at AI as the tool to quickly detect the malware and stop it from spreading. Detective procedures are being developed by vendors using AI to detect abnormal usage patterns and deflect the attacks quickly.

The city of Las Vegas has added AI to the city's cyber defenses over the past three years to detect and respond to threats. AI tools can detect irregular network behavior and automatically quarantine an infected device before the malware has a chance to compromise other equipment. AI can automatically take control and react to the threat instantly to prevent extensive damage.

The coordinated ransomware attack on 23 municipalities in Texas led to the Texas State government ordering "Level 2 Escalated Response." However, the most important lesson to be learned

from the incident is the vigilance in thwarting the ransomware attacks by Lubbock County, where the in-house technology personnel shut down the affected computers and prevented major losses in services and time. In contrast, the other 22 cities, including Borger, Keene and Wilmer, suffered major damage to their services due to lack of the preventive measure.

If they do not take actions, there are indications that the risk will be factored into increased cost of their debt by the capital markets and increased regulatory oversight.

In the future, stakeholders can and will hold auditors of these organizations accountable for reviewing and monitoring compliance with the cybersecurity framework.

IT IS STILL HARD TO QUANTIFY THE TOTAL IMPACT OF RANSOMWARE ATTACKS BECAUSE MOST ARE NOT PUBLICLY REPORTED.

Table 1 and Table 2 show some basic preventive, detective and corrective procedures to be adopted by management and audit to minimize the threat and cost to stakeholders.

The framework of procedures for management and audit discussed in Tables 1 and 2 are meant to be the minimum level of protection to be implemented by municipal governments and SMEs. The size and complexity of the organization should determine additional procedures to be considered.

Attractive Targets

Municipal governments and SMEs are attractive targets to fraudsters and hackers to launch ransomware to infect many users quickly. Due to their vulnerable cybersecurity infrastructure planning, these organizations struggle to counter the threats and recover to a normal state. Such attacks are increasing and depleting precious funds that could be deployed on services to stakeholders.
Managers must implement the preventive, detective and corrective procedures quickly and consistently.

ABOUT THE AUTHOR:

Dr. Kamala Raghavan is professor and interim department chair for Finance and Accounting at Texas Southern University's Jesse H. Jones School of Business. She was elected to the Fulbright Association Board of Directors under the leadership of Executive Director Dr. John Bader. The mission of the Fulbright Association is to advocate for the Fulbright program and promote international education. She began her three-year term January 1, 2021. Contact Dr. Raghavan at kamala.raghavan@tsu.edu.

REFERENCES

Adamek, Drew. (2019). Here's how much cybercrime can cost your company, *FM Magazine*, May 03.

Axelrod, Jason (2019) Digital defense. The Pittsfield Aug 05.

Axelrod, Jason (2019) How local governments can harness; American City & County; The Pittsfield Aug 12.

Barker, B (2019). The battle against cybercrime. *Texas Banking*. 108(10) 8-11.

Eyal Benishti, Eyal. (2018) Email phishing attacks: A significant threat to America's cities and counties, American City & County. Apr 04.

Calvert, Scott and Jon Kamp. (2019) Hackers Won't Let Up in Their Attack on U.S. Cities; Baltimore is still recovering month after more than one group breached its network, *Wall Street Journal* (Online); New York, N.Y. June 7.

Calvert, Scott and JM Kamp. (2018) U.S. Cities Brace for 'Inevitable' Hackers; Majority of top 25 U.S. cities have, or are looking to buy, cybersecurity insurance, Wall; New York, N.Y, Sep 04.

Kamp, Jon and Scott Calvert (2019). Hackers Strike Another Small Florida City, Demanding Hefty Ransom; Lake City officials agree to pay $462,000; *Wall Street Journal* (Online); New York, N.Y. June 26.

McAfee Labs (2016). Ransomware-Locky-McAfee Labs threat advisory. Available at: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sep-2016.pdf.

Snell, E. (2016). CO clinic Healthcare Ransomware case affects 6800 patients. Available at http://healthitsecurity.com/news/co-clinic-healthcare-ransomware-case-affects-6800-patients.

Tariq, Nida (2018), "Impact of Cyberattacks on Financial Institutions," *Journal of Internet Banking and Commerce*, Vol. 23, No. 2.

Wertheim, Steven (2019) "What to Do in the Event of a Cyberattack," *The CPA Journal* (https://www.cpajournal.com/2019/11/22/what-to-do-in-the-event-of-a-cyberattack/ Accessed on 1-23-2020)