Ransomware Attack and Business Continuity Planning (BCP)

By: Gerald Rigdon - 2023

Case Study Questions:

How would the potential for ransomware attacks affect a data backup strategy?

Due to the popularity of cloud services, many companies have abandoned on premise data centers in favor of cloud service providers. For many companies, it's simply a financial decision. However, operating in the cloud comes with its own set of security risks. In any case an important consideration would be to make sure your primary data center is not your only data center. Having a second location containing full copies of all the data is certainly a good strategy for dealing with potential ransomware attacks. Furthermore, per (*6 Business Continuity Plan Best Practices*, n.d.), the minimum recommended distance for a secondary data center is 150 miles from your primary. While this strategy is based primarily on a distance that is beyond the radius of most natural disasters, I think it is also sound for cybersecurity attacks.

The Atlanta attack was a virus in the SamSam family which encrypts data and basically locks user access unless a key is provided by the threat actor. Therefore, having all your data stored in a separate secondary location which is inaccessible to the attacker is a good mitigation strategy. There are many good cloud backup providers, but I would be looking for a strategic partner that not only secures the backed-up data, but also provides the most secure and efficient mechanisms for the recovery process. My over-arching strategy is to assume that your business will be the subject of a ransomware attack one day. Having this mindset is helpful when planning for these events which involves both the preservation and restoration of data.

Why should the Recovery Time Objective or RTO always be shorter than the Maximum Tolerable Downtime or MTD?

RTO identifies the planned recovery time for a system and focuses on restoration goals. MTD represents the total amount of downtime that can occur without significant impact to the mission of a company. Hence, when applied in Business Continuity Planning, these terms help identify important events along a timeline (Horn, R., 2020). For example, if a cyber-attack prevented business operations where the MTD was 5 business days, the RTO would need to be less than 5 days. Thus, when used in practice, MTD is determined by various financial inputs and the RTO is the metric used by the Information Technologists. Once the RTO number is established, it becomes a requirement for IT personnel and establishes the timeline for use in the Incident Response process. With the RTO

requirements, a cybersecurity group can then analyze various complicated scenarios based on current use cases and determine the possible situations where RTO might not be met. All this information is part of the risk management process where a business must determine whether the likelihood and impact (the risk) is acceptable. This can be challenging in cases where the MTD is a short amount of time and hence the even shorter RTO constraints would likely result in expensive recovery solutions.

What business continuity planning best-practices would be recommended to the City of Atlanta following their cyber-attack?

Given the City of Atlanta is government, I would start with compliance with ISO 22301 (*What are the 5 key components of a business continuity plan*, 2020) where the key components of a business continuity plan are identified:

1. Understanding risks and potential business impact
2. Planning an effective response
3. Roles and responsibilities
4. Communication
5. Testing and training

Additionally, at Ready.gov there is a Business Continuity Plan template (Rock, T. 2022), which includes program administration, continuity organization, impact analysis, strategy and requirements, manual workarounds, incident management, training testing and exercising, program maintenance and improvement.

With these governing objectives and a template to work from, I would further recommend (Burke, A., 2018) the following 7 best practices:

1. Take the time to realistically assess enterprise vulnerabilities
2. **Understand the difference between disaster recovery and business continuity**
3. **Incorporate new (cloud) technologies**
4. Pay attention to third-party risks
5. Test the business continuity plan often
6. **Get employees involved**
7. Bring in expert help when needed

One of the best practices identified above helps a city in crisis to proceed with step-by-step protocols. For example, during a cyberattack **understanding the difference between disaster recovery and business continuity** enables you to have specific protocols that address each separately. Per the continuity plan, the city wants to ensure it can continue to operate while the disaster recovery steps focus on the restoration of the data and other specific technology components.

Getting employees involved cannot be overstated. People are often the weakest link in cybersecurity and so continuous training helps with awareness. The City of Atlanta should therefore take advantage of FedVTE, which is a free training program for all government workers. As noted in (*How to Train Government Workers on Cyber Security Threats*, n.d.), "Local governments with outdated IT technology are easy targets for a ransomware attack or malware infection. As a result, hackers will hit underprepared government officials with email phishing scams, stolen passwords, or malware to break in and steal confidential and important government data or lock up critical systems needed for operations and services."

Finally, given this expressed sentiment on outdated IT, I would recommend the movement away from any on premise data centers and **incorporate new cloud technologies** as more secure alternatives.

Should the City of Atlanta have paid the ransom? Why or why not?

Whether or not to pay ransomware attackers is a hotly debated topic. One strongly held view (Moore, S., 2021) is that this is a business decision, one that should be made by stakeholders in the company at the board level instead of the leaders in security risk management. Moreover, from (Freed, n.d.) we are given three reasons for not paying:

1. There is no guarantee your organization with regain access to their data

   Research (Freed, n.d.) found 46% of respondents regained access to their data post-payment while 3% got nothing in return.

2. Your organization could incur penalties from the U.S. government for paying threat actors who may reside or operate out of countries subject to U.S. sanctions

   OFAC or the Office of Foreign Asset Control, can impose penalties based on strict liability meaning an organization can be held liable even if it did not know it was engaging in transaction with a threat actor in a sanctioned country.

3. You are sending the wrong message

   Bowing to the wishes of a threat actor suggests that extortion will be tolerated, which opens the door for subsequent attacks. Research (Freed, n.d.) found that 80% of organizations who paid a ransom incurred future attacks.

In this case the city of Atlanta refused to pay the $50,000 in Bitcoin and in the end spent millions of dollars to recover. I agree with this decision because even though it was costly and a major disruption to many services, the Atlanta 911 system, emergency response, and major utilities were unaffected. Moreover, I contend this was a great learning experience that may not have occurred had the payment option been taken. A good long-term view is to understand that such attacks will never stop, and the cost of the disruption may likely be worth it assuming maturation of the approach to cybersecurity.

What can other city governments learn from the incident at the City of Atlanta?

1. Prepare for the inevitable (Sneed, A., 2019).
   - Newark New Jersey paid $30,000 to ransomware attack in 2017
   - Baltimore Maryland computer systems went down in 2019 for refusing to pay an $80,000 ransom
   - Etc.

2. Have a solid incident response plan.
   Obviously, if Atlanta had a better plan the recovery process would have likely been faster and less expensive. Atlanta CIO Gary Brantley who was hired after the attack said: “It’s less about the attack for me, and more about your ability to respond when it happens.” (Sneed, A., 2019).

3. Have a cyber insurance policy.
   Atlanta had a policy in place which is a good example to follow. (Douglas, T., 2018).

4. Have security zones. (Douglas, T., 2018).
   Atlanta could have benefited from security zones. This prevents an attacker from lateral movement following the compromise of one system. This also enables you to take the infected machine offline and isolate from the network.

5. Collaborate with other city governments. (*CISOs make a case for more state-local cybersecurity collaboration*, 2020)
   Since not all local governments have the same capabilities and resources there is an opportunity to collaborate and build relationships. Sharing and learning from others is a great way to break out of silos which can be targets for threat actors.

6. Determine the MTD for city operation and investigate which attack vectors could result in RTO not being met.

7. Perform security audits and do something with the findings.
   According to (*Cyber Security Lessons: City of Atlanta Ransomware Incident*, 2021), an audit performed two months before the Atlanta incident identified between 1500 to 2000 total vulnerabilities.

References:

6 Business Continuity Plan Best Practices (n.d.). techadvisory.com https://www.techadvisory.com/business-continuity-best-practices/

Burke, A. (2018, June). 7 business continuity strategy best practices. questsys.com. https://questsys.com/partner-blog/7-business-continuity-strategy-best-practices/

CISOs make a case for more state-local cybersecurity collaboration. (2020, October). statescoop.com. https://statescoop.com/radio/cisos-make-a-case-for-more-state-local-cybersecurity-collaboration/

Cyber Security Lessons: City of Atlanta Ransomware Incident. (2021, November). pasins.com. https://www.pasins.com/blog/cyber-security-lessons-city-of-atlanta-ransomware-incident

Douglas, T. (2018, October/November). *What Can We Learn From Atlanta?* govtech.com. https://www.govtech.com/security/what-can-we-learn-from-atlanta.html

Freed, A. (n.d.). *Three Reasons Why You Should Never Pay Ransomware Attackers.* cybereason.com. https://www.cybereason.com/blog/three-reasons-why-you-should-never-pay-ransomware-attackers

Horn, R. (2020, August). *What is the difference between RPO, RTO, and MTD?* tandem.app. https://tandem.app/blog/what-is-the-difference-between-rpo-rto-mtd

How to Train Government Workers on Cyber Security Threats (n.d.). govpilot.com. https://www.govpilot.com/blog/how-to-train-government-workers-on-cyber-security-attacks

Moore, S. (2021, October). *When it Comes to Ransomware, Should Your Company Pay?* gartner.com. https://www.gartner.com/en/articles/when-it-comes-to-ransomware-should-your-company-pay

Rock, T. (2022, March). *9 Critical Business Continuity Plan Objectives*. invenioit.com. https://invenioit.com/continuity/business-continuity-plan-objectives/

Sneed, A. (2019, October). *What Cities Can Learn From Atlanta's Cyberattack*. bloomberg.com. https://www.bloomberg.com/news/articles/2019-10-29/what-cities-can-learn-from-atlanta-s-cyberattack

What are the 5 key components of a business continuity plan? (2020, June). qmsuk.com. https://www.qmsuk.com/news/what-are-the-5-key-components-of-a-business-continuity-plan