West Jordan Cyber Attack

Korban Lee, CAO

WHAT HAPPENED?

In late May, 2023, West Jordan City servers were infected with ransomware

Infection came in through an old account that none of our current staff were aware existed

The infection came on to the system in May, but did nothing for a couple of weeks.

- This allowed the infection to get transferred onto our backups and our air-gapped backups

What Happened?

Wednesday, June 14, 4:00 a.m. – started encrypting our servers and locking us out of our servers

IT Staff were alerted and immediately started taking defensive actions

Ransomware group also started trying to exfiltrate our data

- Didn’t get very far

We had started upgrading our cybersecurity software and believe that is what triggered the attack at that day and time

Starting to Worry

Initially, we were not too worried. We have backups, and we have air gapped backups of our backups.

However, we soon realized that all our backups were also encrypted.

Result:

We were locked out of everything that was on a local server

- Phone system, Financial system, GIS, Asset Management and Permitting, Public Safety Records, etc.

Anything that was hosted on the Cloud or through a 3rd party was fine

- Website, Credit Card Data and Payments, Court Software, Dispatching, Employee Benefits, etc.

RESPONSE:

Initially, worked with our cybersecurity software company only

Cyber Insurance

- We didn’t immediately notify our cyber insurance company as we thought we could quickly restore through backups
- We notified our cyber insurance company as soon as we realized we wouldn’t be able to restore our systems quickly, on our own
- Insurance brought on a team of national experts

- Also used our Cybersecurity Software Company for Digital Forensics and Security Upgrades

RANSOMWARE:

$2+ million ransomware demand

Three parts to their strategy

- Encryption – locking you out of your own systems
- Exfiltration – taking your confidential files and selling or sharing the data
- Reputational damage

Time is on your side

- The less desperate you look, the less they can hold you hostage, possibly lowering the ransom demand

RESPONSE:

Philosophy: Prioritize paying trusted partners for support and assistance over any payment to the threat actor

Abandoned some older systems we were thinking of replacing anyway

- New phone system
- New software in a few areas

RESPONSE:

Manual processes to buy us some time

Help from our friends

- Public Safety Records

Eventually found a way to restore data

- With restored data, could start rebuilding systems

RESULTS:

Stood up new systems
- Bumpy, not without its problems

Restoring data and systems
- Also bumpy
- Some abandonment
- Some restoration is still in progress

Did not pay anything to the threat actors
- Additional attacks

WHAT WOULD WE DO DIFFERENT?

Diversify Digital Holdings

- More on the cloud, different systems on different clouds
  - If you lose a server or system, only one function is affected

- If you are hosting on-site, make sure you are considering your cybersecurity position

- Think through the trade offs
  - customization of a locally hosted system

  vs.

  - security of a cloud but less customizable

What would we do different?

Be very aware of your cyber insurance policy & limitations

- Call your cyber insurance company early, even if just suspect an attack
- Understand your buckets of coverage under the broader policy
- Have reserves and/or plans for risks that exceed your policy

Additional Lessons Learned

It’s not if, but when….

Have a Cybersecurity Incident Action Plan and Exercise It

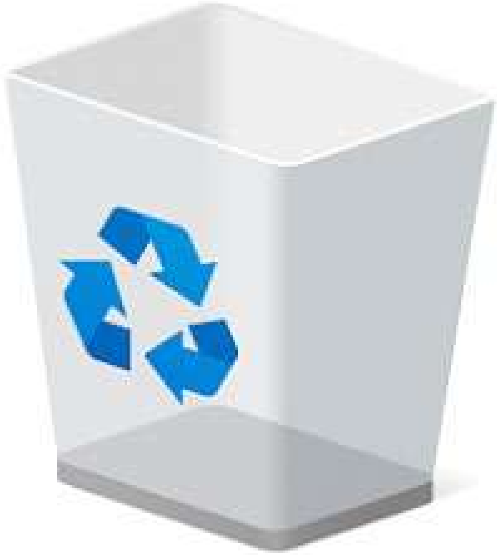
- Understand what things may require a manual process and plan for it

Additional Lessons Learned

Account life cycle – purge old accounts, access to old systems

- Audit accounts on a regular basis

Have a 3rd party cybersecurity partner



If possible, don't store personal data

Don't keep too much extra data

Additional Lessons Learned

Balance communicating with different stakeholders and the need for confidentiality

- Elected Officials
- Employees
- The Public

Form relationships and partnerships

Understand your cyber vulnerabilities and how they may change over time

Questions?

Korban Lee
Chief Administrative Officer
City of West Jordan
385-315-9910
korban.lee@westjordan.utah.gov

WEST
JORDAN
UTAH