Wheat Ridge vs Black Cat

LESSONS LEARNED FROM A RECENT CYBER ATTACK

Our Agenda

About Cybercrime

Wheat Ridge Experience

Lessons Learned

About Cybercrime

800,944 complaints to IC3 in 2022 (5% decrease from 2021, likely due to Russian/Ukrainian War)

- Potential total loss grew from $2.7B in 2018 to $10.2B in 2022
- Many attacks are not reported to the FBI

Cybercrime includes:

- Ransomware – 2,385 complaints with losses of more than $34.3 million affected 14 different sectors
- Business Email Compromise – 21,832 complaints with losses of over $2.7 billion
- Call Center Fraud – 44,092 victims with losses of over $1 billion

Wheat Ridge Attack

Ransomware attack
Early hours of August 29, 2022
First detected by a Wheat Ridge Police Sergeant
Ransom Note (This is an Attack!)
Shut the City Down
Notified Authorities

Organizing Our Response

- No incident response plan for this emergency
- Formed an internal Incident Response Team (modeled on Pandemic) planning, coordination and feedback
- Developed “scrappy communication methods”
- Handled critical in-the-moment tasks
- Focused on service delivery and staff needs

Insurance and Legal

- Insurance is Key!
- Cybersecurity & Data Privacy Legal Specialty
- Forensics
- Recovery and Restoration
- Regulatory
- Helped us Manage the Chaos

Threat Actor

- Black Cat
- Ransom Note
- Threat Actor Communication
- Determination Not to Pay

Personal Information

- Regulated Differently by Every State
- Timelines and Deadlines for Reporting
- Possible Impacted Population Determines Reporting

Communication

- Simple – relate to service delivery
- Project calm
- Balance transparency with legal concerns (internal/external)
- Reputation management

Restoration

- Organization and Communication!
- Regular Check-Ins
- Gaps we Had to Fill
- Help From Friends

Lessons Learned & How to Plan

- It's a Matter of When, Not If
- Coordination and Communication is Critical
- Your Help Will Have Their Own Motivations
- Your Team Needs You
- Recovery Takes Longer Than You Think
- Incident Response Plan & No Fee MSAs
- System Inventory
- Gap Analysis

Wheat Ridge's Approach to Recovery

- Complete network rebuild
- Only trusted, clean devices
- Rebuild with a security-first mindset

What to Ask Your IT Leadership

- What is our backup strategy?
- What are our Recovery Time (RTO) and Recovery Point Objectives (RPO)?
- Have we tested our network? If so, when and what did we learn?
- Does our team have the right skills to support our environment?
- What is keeping us from implementing MFA? Are our MFA settings appropriate?
- Do we have a current system inventory?

What to Ask Your IT Leadership

- What is our information governance policy?
- Do our password policies conform to best practices?
- Do we have shared accounts, especially with admin rights or old passwords?
- Who has administrative rights?
- How do we control access through our network?
- What is exposed to the Internet?
- Are our systems currently supported?

What You Can Do Right Now (For Free!)

- Start Using a Password Manager
- Join the Multi-State Information Sharing and Analysis Center (MS-ISAC) https://www.cisecurity.org/ms-isac
- Sign up with Cybersecurity & Infrastructure Security Agency (CISA) https://www.cisa.gov/
- Leverage SANS.org https://www.sans.org/free
- Turn on MFA
- KnowBe4 Training
- Find Local Cybersecurity Groups

Questions?

Patrick Goff, City Manager
PGOFF@CI.WHEATRIDGE.CO.US

Allison Scheck, Deputy City Manager
ascheck@ci.wheatridge.co.us

Marianne Schilling, Assistant City Manager
mschilling@ci.wheatridge.co.us

Jesse Dubin, IT Manager
jdubin@ci.wheatridge.co.us