BEYOND DISASTER RECOVERY

Amanda Noble

SWIAF/SEIAF JOINT MEETING - AUGUST 12-14, 2019 | AUSTIN, TX

LEARNING OBJECTIVES

- Become aware of cybersecurity risks facing local governments
- Consider auditors' role in mitigating risk
- Think about your organization's plan for continuity of operations in the event of a cyberattack

ATLANTA: POSTER CHILD FOR CYBER (IN)SECURITY

2018 Atlanta cyberattac

https://en.wikipedia.org/wiki/2018_Atlanta_cyberattack

Not logged in Talk Contributions Create account Log in

Article Talk | Read Edit View history | Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

2018 Atlanta cyberattack

From Wikipedia, the free encyclopedia

This page's infobox may require expansion, verification, or otherwise need cleanup. Please make sure that the infobox meets Wikipedia's guidelines for infoboxes. There might be relevant comments on the talk page. You may also want to view the infobox template page to view the full parameter list and read guidance on usage of that infobox. *(November 2018)*

The city of Atlanta, Georgia was the subject of a **massive cyberattack** which began in March 2018.[2] The city recognized the attack on Thursday, March 22, 2018, [1][3] and publicly acknowledged it was a ransomware attack.

Due to Atlanta's national importance as a transportation and economic hub, the attack received wide attention[4] and was notable for both the extent and duration of the service outages caused. Many city services and programs were affected by the attack, including utility, parking, and court services.[5] City officials were forced to complete paper forms by hand.[6]

On November 26, a grand jury indicted two Iranian hackers, Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri, for the attack. The Department of Justice alleged that Savandi and Mansouri are part of the SamSam group; that the SamSam group is based out of Iran; and that the pair created SamSam Ransomware, the malware used in the attack. There are no affiliations with the government of Iran.[7]

2018 Atlanta cyberattack

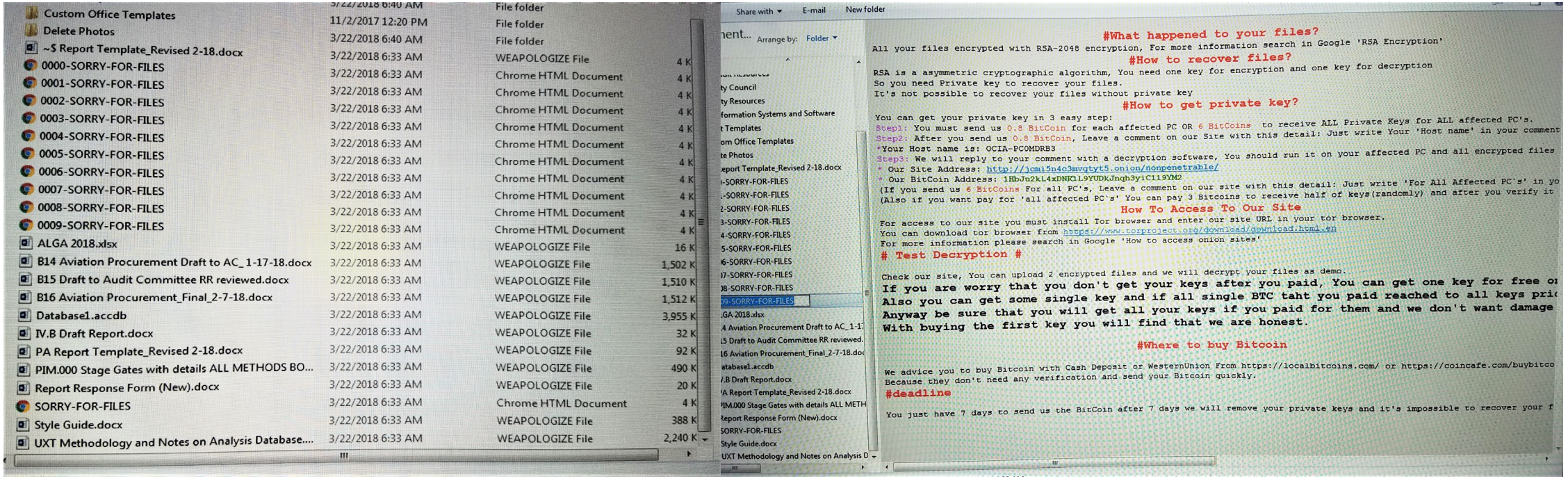
Date	22 March 2018[1]
Location	Atlanta, Georgia, United States
Type	Cyberattack
Theme	Ransomware encrypting files with $51,000 demand (via Bitcoin)
Cause	SamSam Ransomware
Outcome	Multiple municipal services down, including databases and wi-fi Years' worth of data destroyed City spends $2.7 million in recovering services

Approach and attack [edit]

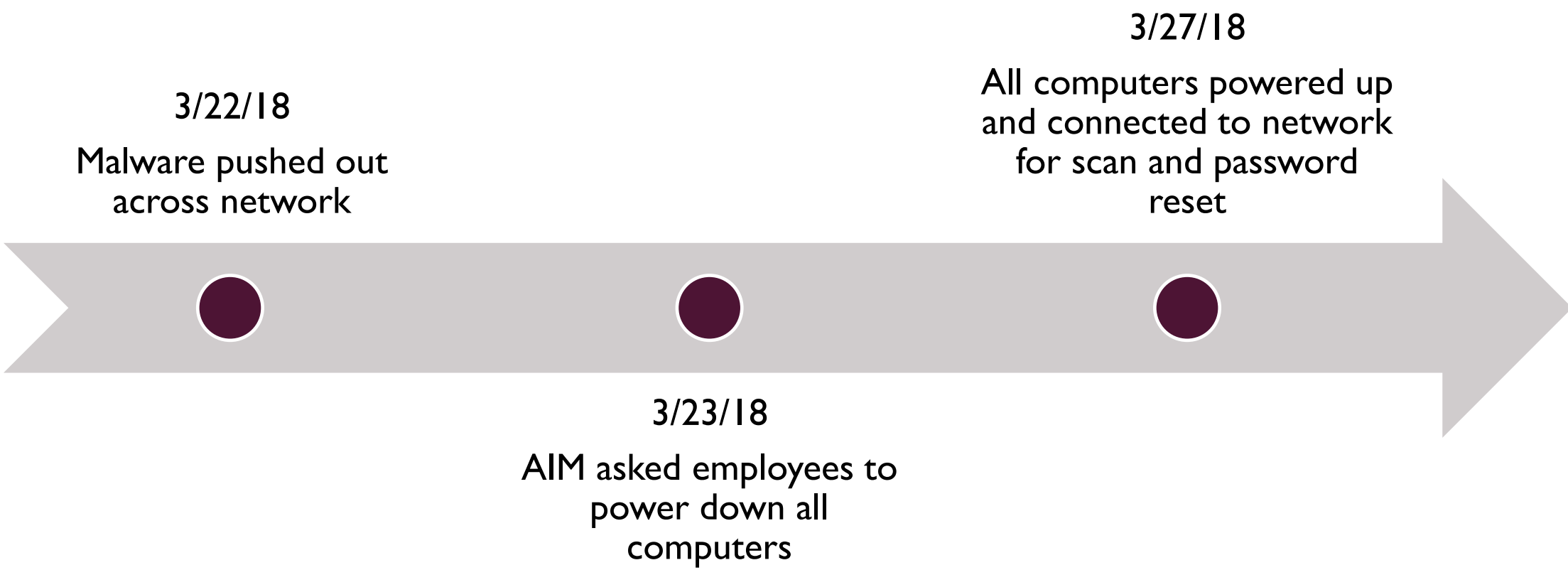
Leading up to the attack, the Atlanta government was criticized for a lack of spending on upgrading its IT infrastructure, leaving multiple vulnerabilities open to attack. In fact, a January 2018 audit found 1,500 to 2,000 vulnerabilities in the city's systems, and suggested that the number of vulnerabilities had grown so large that workers grew complacent. The virus used to attack the city was the SamSam Ransomware, which differs from other ransomware in that it does not rely on phishing, but rather utilizes a brute-force attack to guess weak passwords until a match is found. It is known to target weaker IT infrastructures and servers.[8] The ransomware has prominently been behind attacks on medical and government organizations since its discovery in 2016, with previous attacks on targets ranging from small towns such as Farmington, New Mexico to the Colorado Department of Transportation and the Erie County Medical Center. It can also bypass antivirus software.[9] Despite no suspects being identified or indicted until November 2018, the SamSam hackers were described as "opportunistic".[10]

On March 22, at 5:40 AM, the Department of Atlanta Information Management first learned of outages on various internal and customer applications "including some applications customers use to pay bills or access court related information," according to Richard Cox, the city's interim Chief of Operations. Soon afterward, the city shut down many of its digital services in an attempt to control the situation, including its court system database and the wi-fi at Hartsfield–Jackson Atlanta International Airport. The city eventually identified it as a ransomware attack.[3][1]

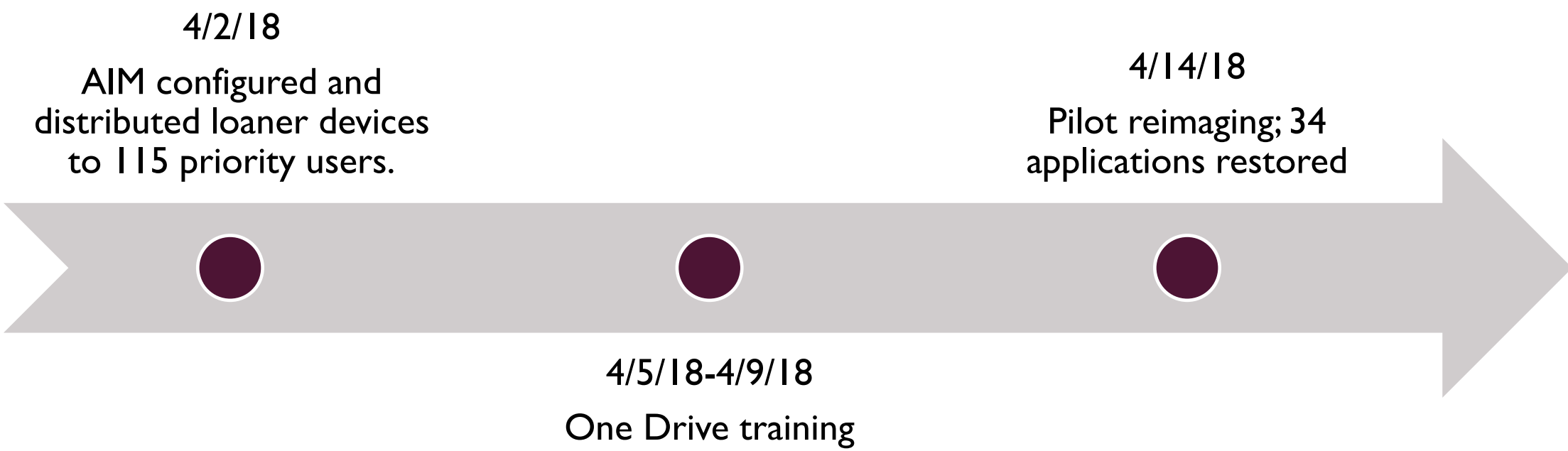
WHAT HAPPENED?



TIMELINE: INVESTIGATION AND CONTAINMENT



TIMELINE: RECOVERY



TIMELINE: RECOVERY

4/30/18

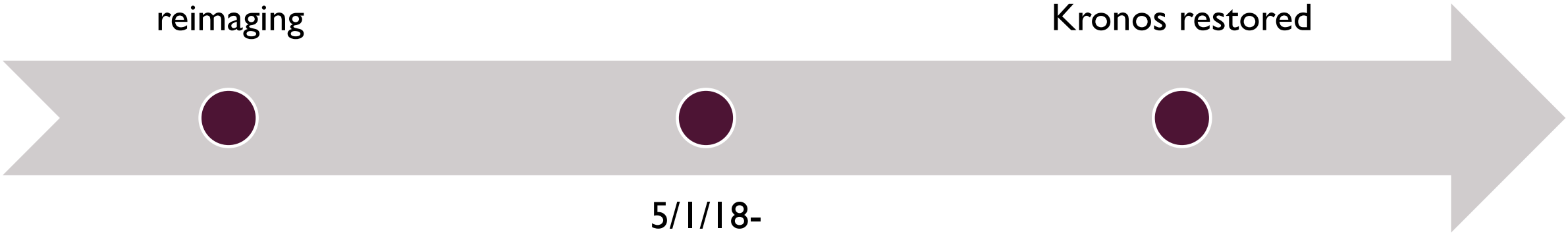
Hyperion restored; Started scheduling reimaging

5/1/18-

Reimaging of about 3,800 affected computers

6/19/18

Kronos restored



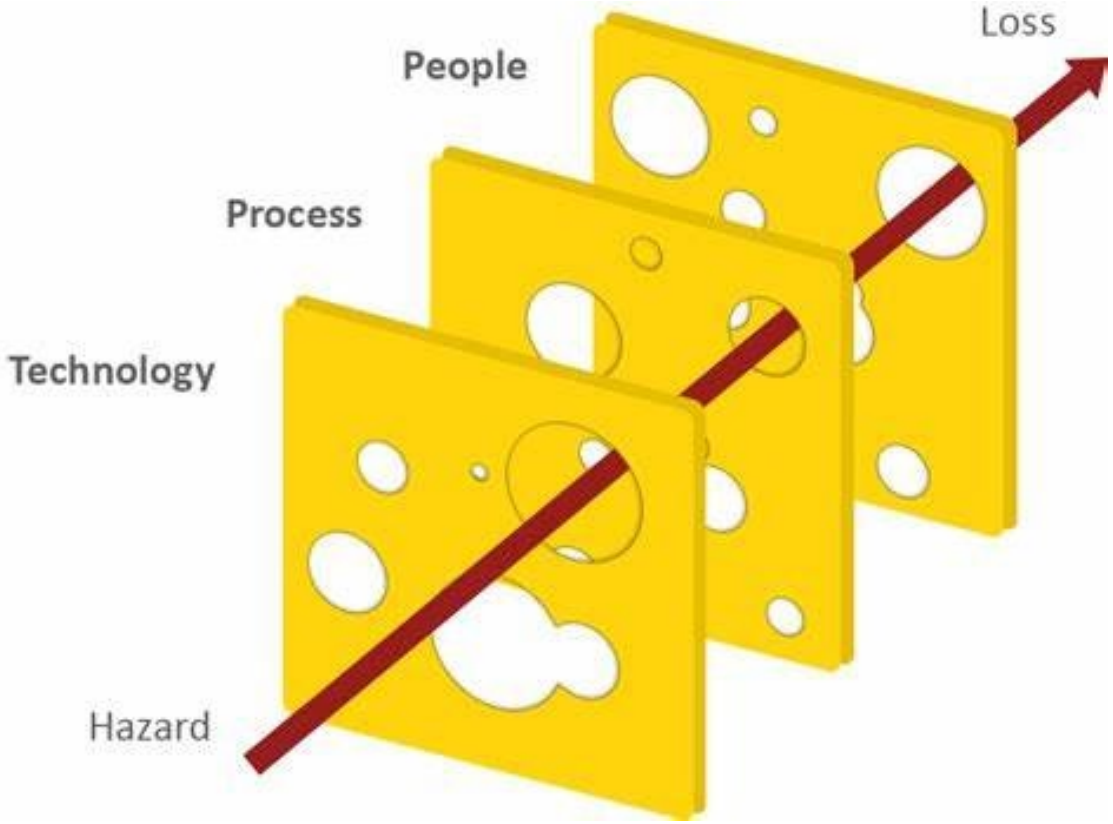
FINAL TALLY

- $17 million unofficial estimated cost for recovery and rebuild
- 77 "critical systems" affected
- Loss of productivity

SOME GOOD NEWS

- Network segmentation protected critical public safety systems
  - Airport
  - Water treatment and distribution
  - 911
- No evidence that sensitive employee, vendor, or citizen data was accessed
- Cyber insurance policy in effect
  - City has received $5.1 million reimbursement; expects $5-$6 million more

WHY IS CYBERSECURITY HARD?



MITIGATING RISK

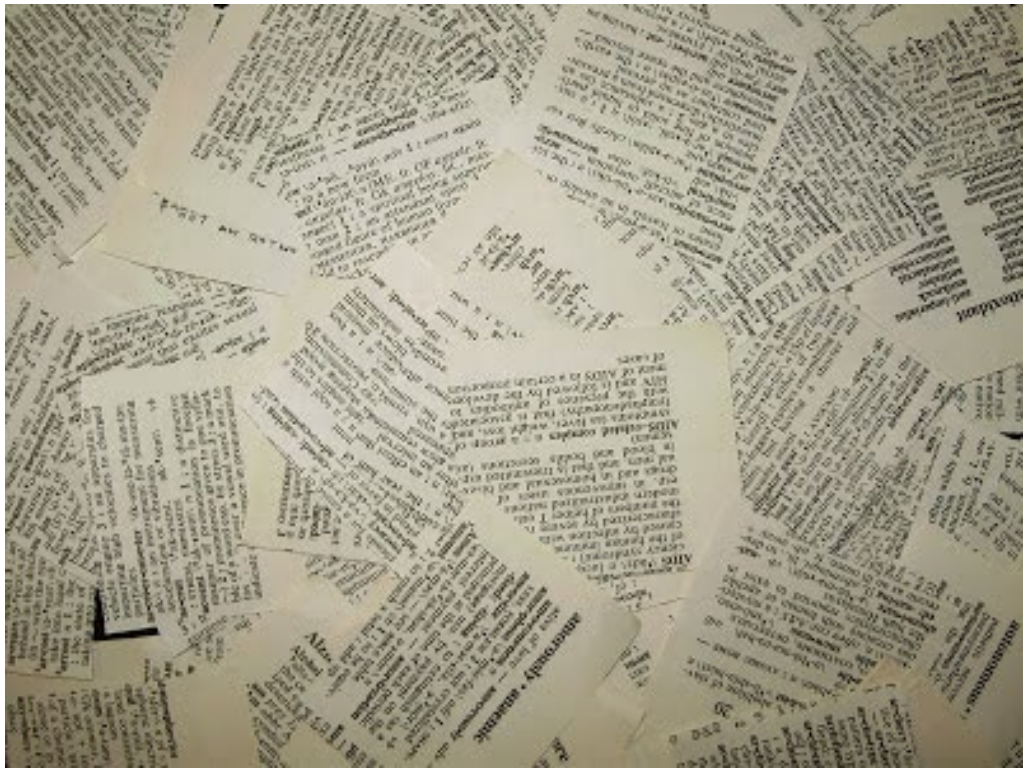
- DHS and FBI recommend:
  - Audit network for systems that use RDP; disable if not needed
  - Patch management
  - Verify cloud-based virtual machine instances with public IPs have no open RDP ports
  - Strong passwords and account lockout policies to defend against brute force attacks
  - Two-factor authentication
  - Regular system and software updates
  - Good backup strategy
  - Enable logging
  - Minimize network exposure for all control system devices
  - Restrict user permissions to install software

WHAT'S THE ROLE OF THE AUDITOR?

- An audit is a snapshot in time. Cybersecurity is continuous.

"… THE CITY RECEIVED YEARS OF WARNINGS ABOUT SECURITY WEAKNESSES"

"In one case," the audit said, "monthly vulnerability scan results indicated the presence of 1,500-2,000 severe vulnerabilities in the scanned population, with a history that went back over a year with no evidence of mitigation of the underlying issues."



"Confidential Report: Atlanta's cyber attack could cost taxpayers $17 million," Stephen Deere, The Atlanta Journal-Constitution, August 1, 2018

8 HEADLINES THAT DEFINED 2018 FOR INTERNAL AUDIT

Internal Audit Findings Could Have Prevented Atlanta's Ransomware Attack

Not all of 2018's headlines were about internal audit failings. Indeed, news reports indicated that Atlanta's ransomware attack could have been avoided had city leaders acted on internal audit recommendations to address serious cyber vulnerabilities.

The city's auditor laid out dire shortcomings in Atlanta's IT department and forewarned that there were basically no formal plans in place to protect the city from cyber threats. The audit report warned that complacency and severe resource shortages in IT created a "significant level of preventable risk exposure to the city," and it concluded the city had "no formal processes to manage risk."

https://global.theiia.org/news/Pages/Blog-%E2%80%8B8-Headlines-That-Defined-2018-for-Internal-Audit.aspx

QUESTIONS?