



Cybersecurity: Phishing and Ransomware

Douglas Jones, City Auditor, City of Kansas City
Amanda Noble, City Auditor, City of Atlanta

Mid-America Intergovernmental Audit Forum
Overland Park, Kansas
December 5-6, 2019

Kansas City's IT/Cybersecurity Audits Since 2009

- ❖ E-Service Systems Security (Oct 2009)
- ❖ City Should Document GIS Data (Nov 2010)
- ❖ Security of the Municipal Court Docketing System (Feb 2014)
- ❖ Fire CAD System Preparedness (Oct 2014) **CLOSED**
- ❖ Employees' Response to Phishing Email Put City Information Systems at Risk (Mar 2015)
- ❖ City Should Follow Recommended Practices to Protect Personally Identifiable Information (Apr 2015)
- ❖ Mobile Device Security Risks (Nov 2016)
- ❖ Addressing IT Network Vulnerabilities (Nov 2018) **CLOSED**

How Do We Perform IT & Cybersecurity Audits?

- ❖ Standards and recommended practices guide our IT audits
 - FISCAM (Federal Information System Controls Audit Manual)
 - NIST (National Institute of Science & Technology)
 - COBIT (Control Objectives for Information Technology)
 - ISACA (Information Systems Audit & Control Assoc.)
- ❖ Knowledge and experience through certifications and performing the audits
- ❖ Focus primarily on general controls

Friday, March 27, 2015

By MARK DAVIS

The Kansas City Star

“... hackers duped 280 Kansas City Employees into opening the door to municipal computer systems sometime in the last six months, a city audit report said.

Each employee had given up log-in credentials after responding to an email that had been sent to collect just such critical information. They’d fallen for what is commonly called a phishing attack.”

“Luckily, these were would-be hackers. The attack was a fake, specifically a test conducted by city auditors.”

Is Phishing a Big Deal?

❖ 100 million customer credit card records stolen.
Target, November 2013

❖ +100 million shoppers' personal information and credit card data posted for sale on hacking websites.
Home Depot, September 2014



❖ Employees' social security numbers and email messages were stolen from the network. *Sony Pictures, November 2014*

Employees' Response to Phishing Email Put City Information Systems at Risk

- ❖ Data breaches caused by phishing scams can damage city systems, cost the city money, and shake the public's trust and confidence in city government

- ❖ Audit Objective:
Are city employees prepared to respond appropriately to phishing emails?



How'd We Do It?

- ❖ Thought like a bad guy
 - Developed a *very* enticing email
 - Set up a fake website
 - Sent emails to city employees
- ❖ Reviewed NIST cybersecurity guides
- ❖ Interviewed IT staff about how they responded to our phish and employee calls to the help desk

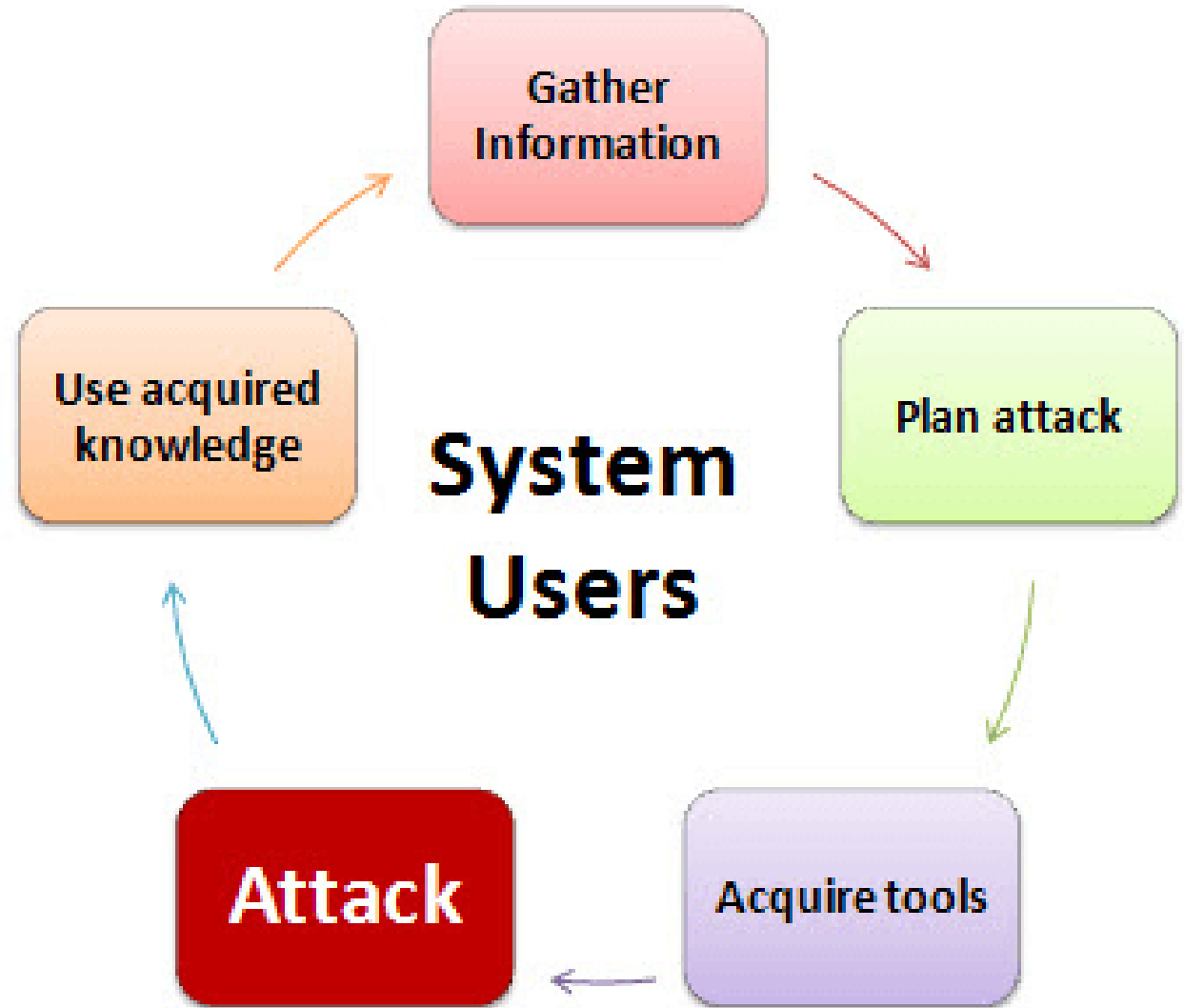


[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

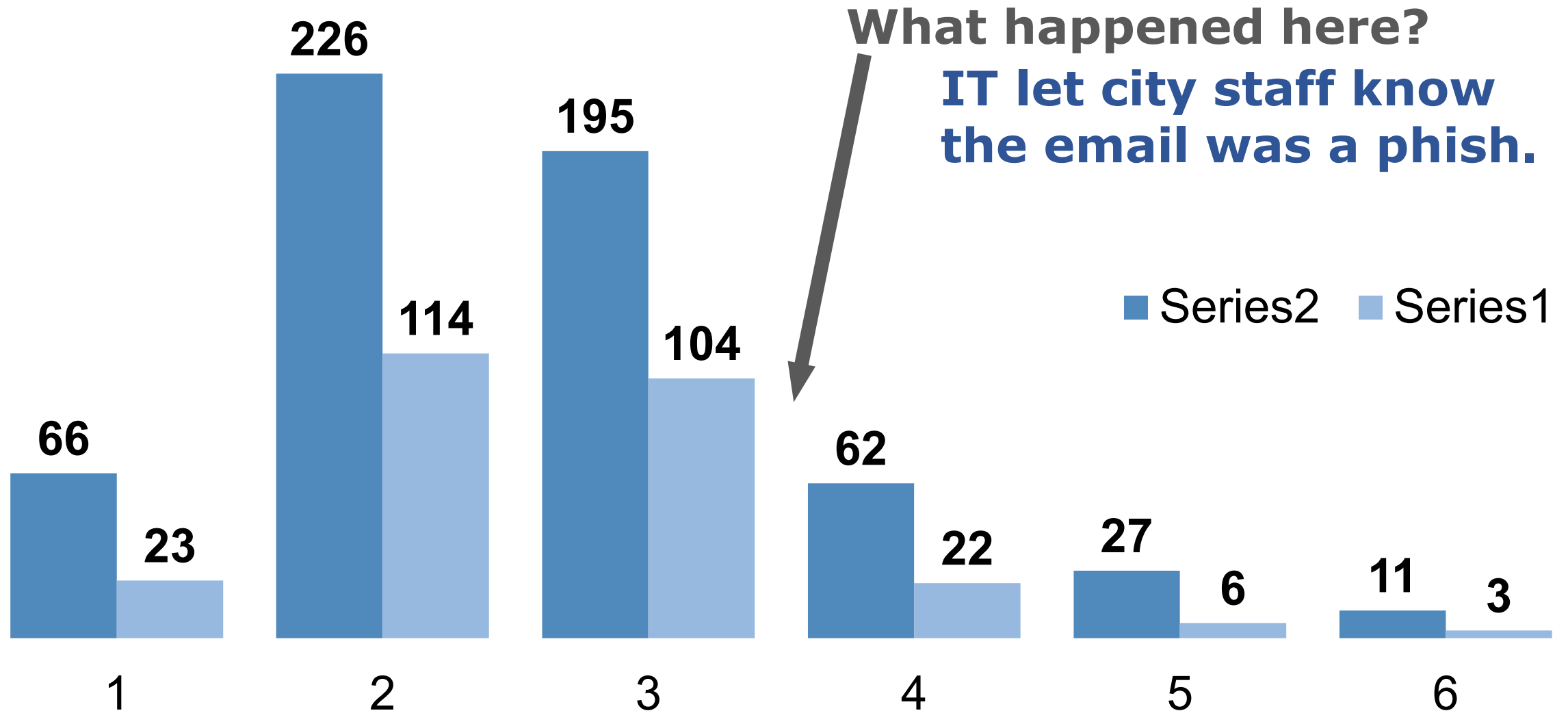
Social Engineering Works!

- ❖ Social engineering is an attack designed to obtain sensitive or confidential information
- ❖ Our phishing test proves social engineering works

Social Engineering Cycle



Employee Visits to Phishing Website & Credentials Provided



What Was the Final Result?

CAO Phishing Test Results (2014)		
Delivered Emails	3,115	
Link Clicks	634	20.4%
Credentials Provided	283	9.1%

- ❖ IT took appropriate steps to address phishing email
- ❖ Some employees did not change their passwords after instructed to do so

Recommendations

- ❖ Implement an IT security awareness training program
- ❖ Develop a comprehensive cyber security incident response plan



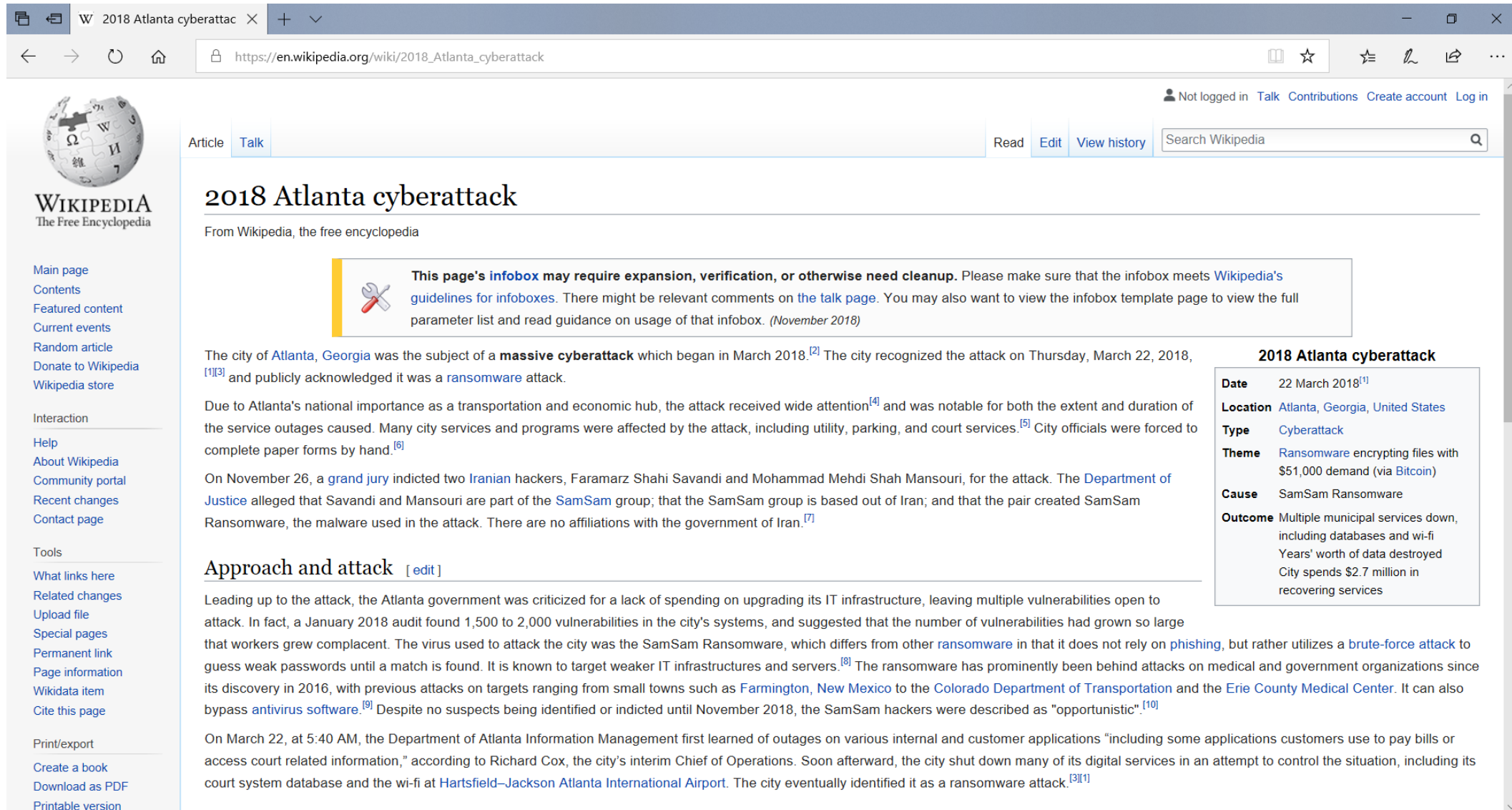
[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

#auditimpact

- ❖ IT created an IT Security Team and named a chief information security officer
- ❖ IT started conducting online cybersecurity training and refresher training
- ❖ IT has gone phishing a couple of times since the audit

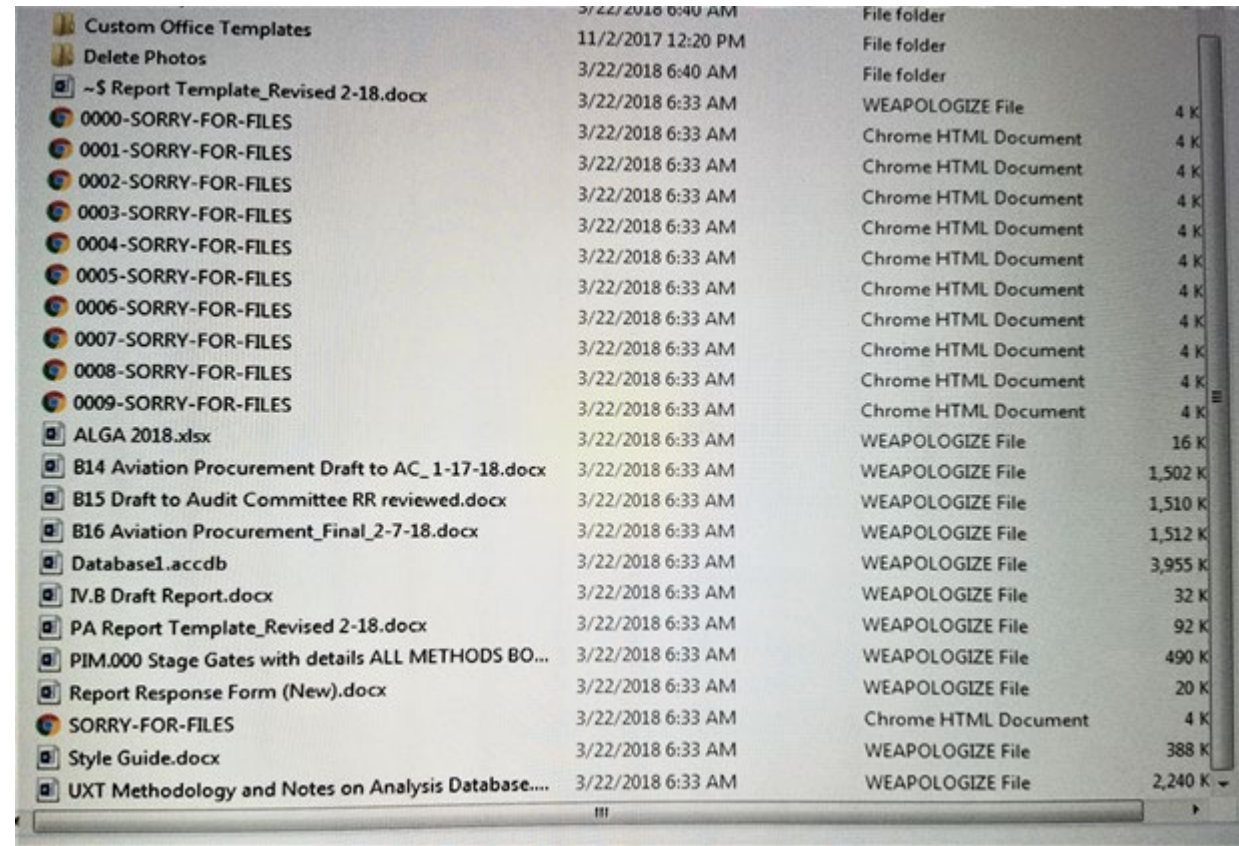
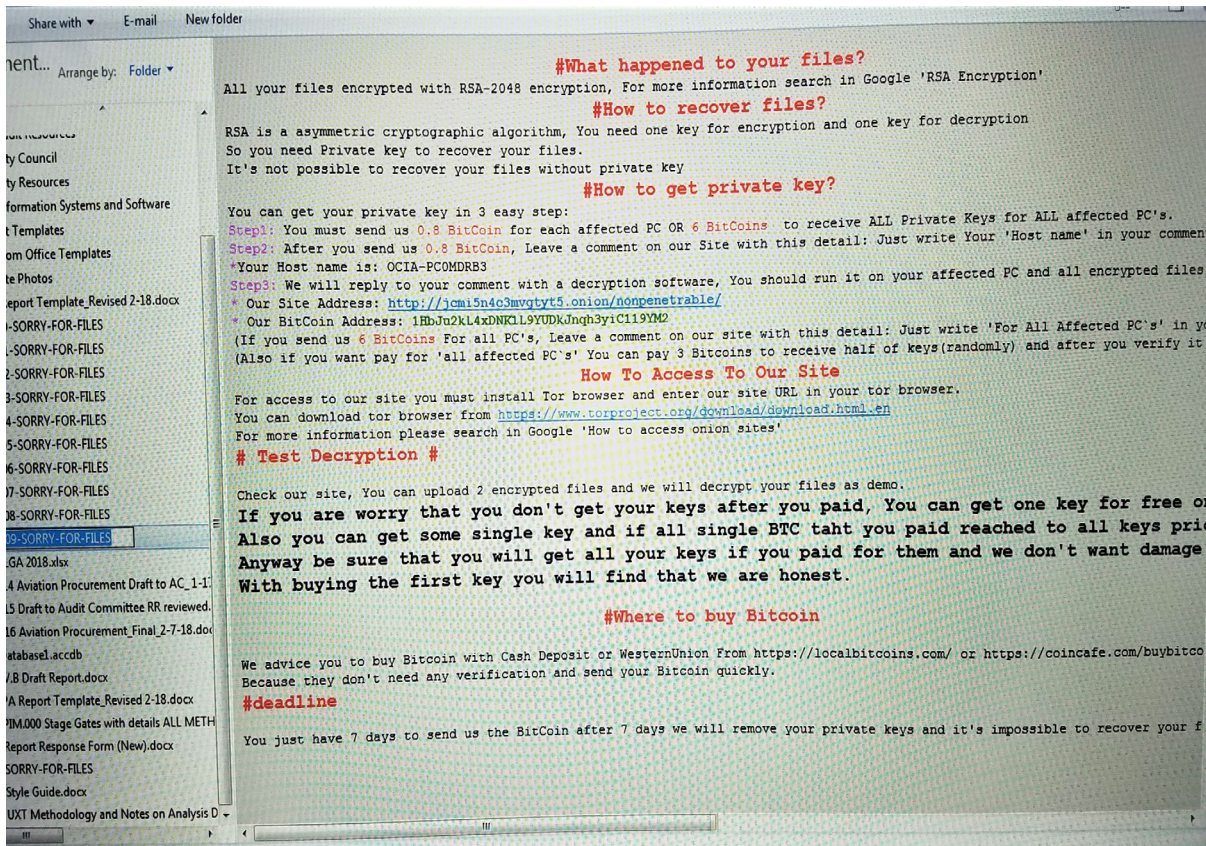
	CAO Phishing Test (48 hours in 2014)		IT Phishing Test (8 days in 2019)	
Delivered Emails	3,115		3,266	
Link Clicks	634	20.4%	576	17.6%
Credentials Provided	283	9.1%	119	3.6%

Atlanta: Poster Child for Cyber (In)Security

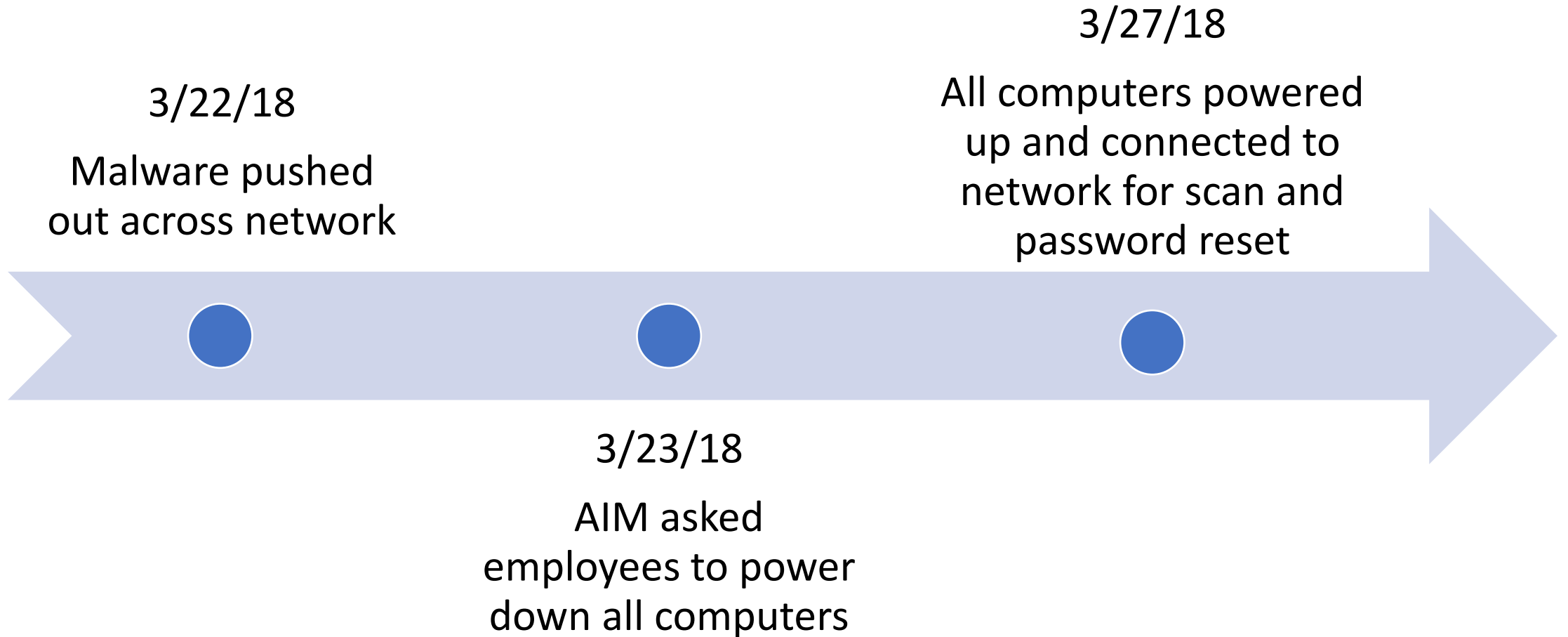


The screenshot shows a web browser window displaying the Wikipedia article for the 2018 Atlanta cyberattack. The browser's address bar shows the URL https://en.wikipedia.org/wiki/2018_Atlanta_cyberattack. The article title is "2018 Atlanta cyberattack". A notice at the top of the article content states: "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 main text of the article begins with: "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." A sidebar on the right contains an infobox titled "2018 Atlanta cyberattack" with the following details: 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. The left sidebar of the Wikipedia page includes navigation links such as "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", and "Printable version".

What Happened?



Timeline: Investigation and Containment



Timeline: Recovery

4/2/18

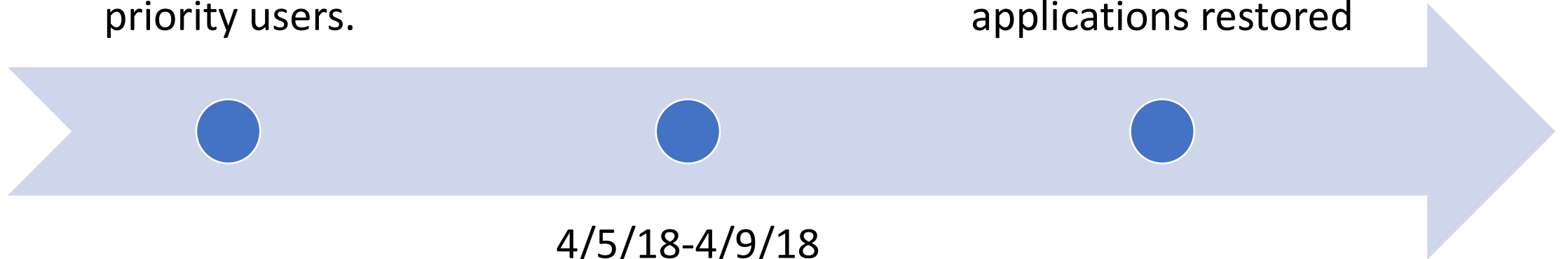
AIM configured and distributed loaner devices to 115 priority users.

4/14/18

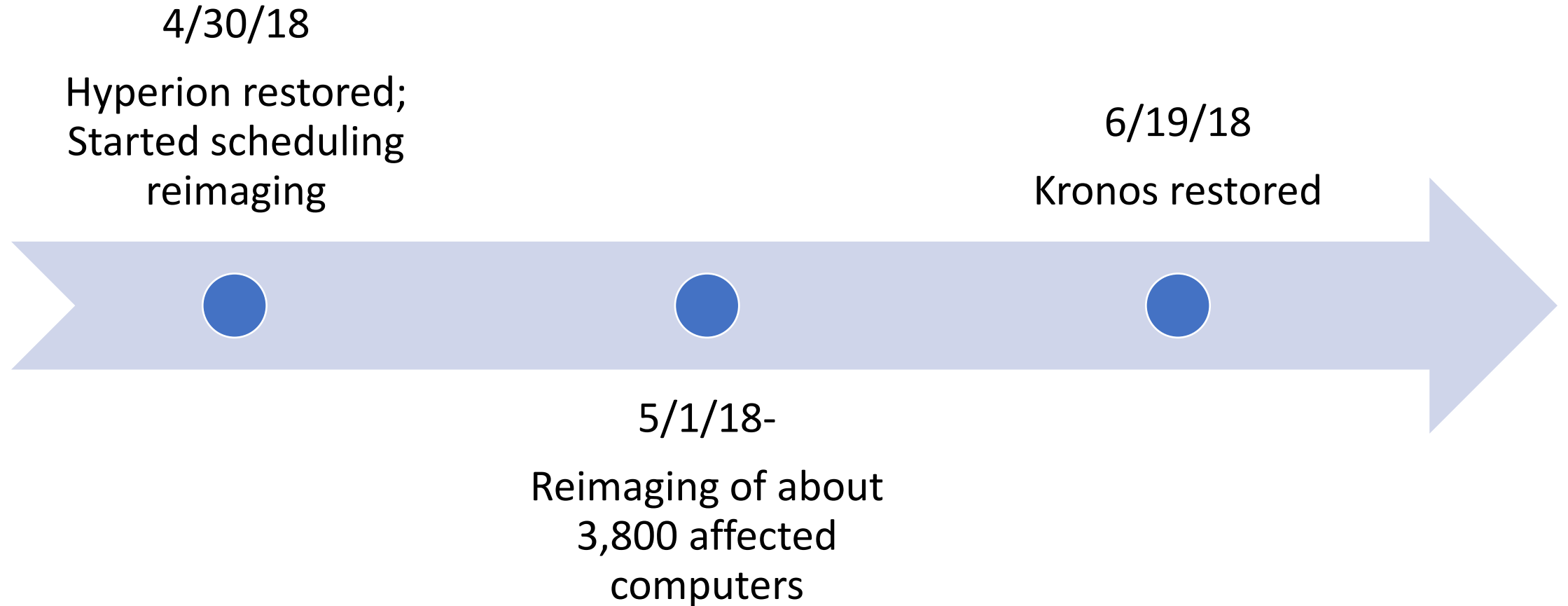
Pilot reimaging; 34 applications restored

4/5/18-4/9/18

One Drive training



Timeline: Recovery



Final Tally



**WANTED
BY THE FBI**

SAMSAM SUBJECTS
Conspiracy to Commit Fraud and Related Activity in Connection with Computers;
Conspiracy to Commit Wire Fraud; Intentional Damage to a Protected Computer;
Transmitting a Demand in Relation to Damaging a Protected Computer



Mohammad Mehdi
Shah Mansouri



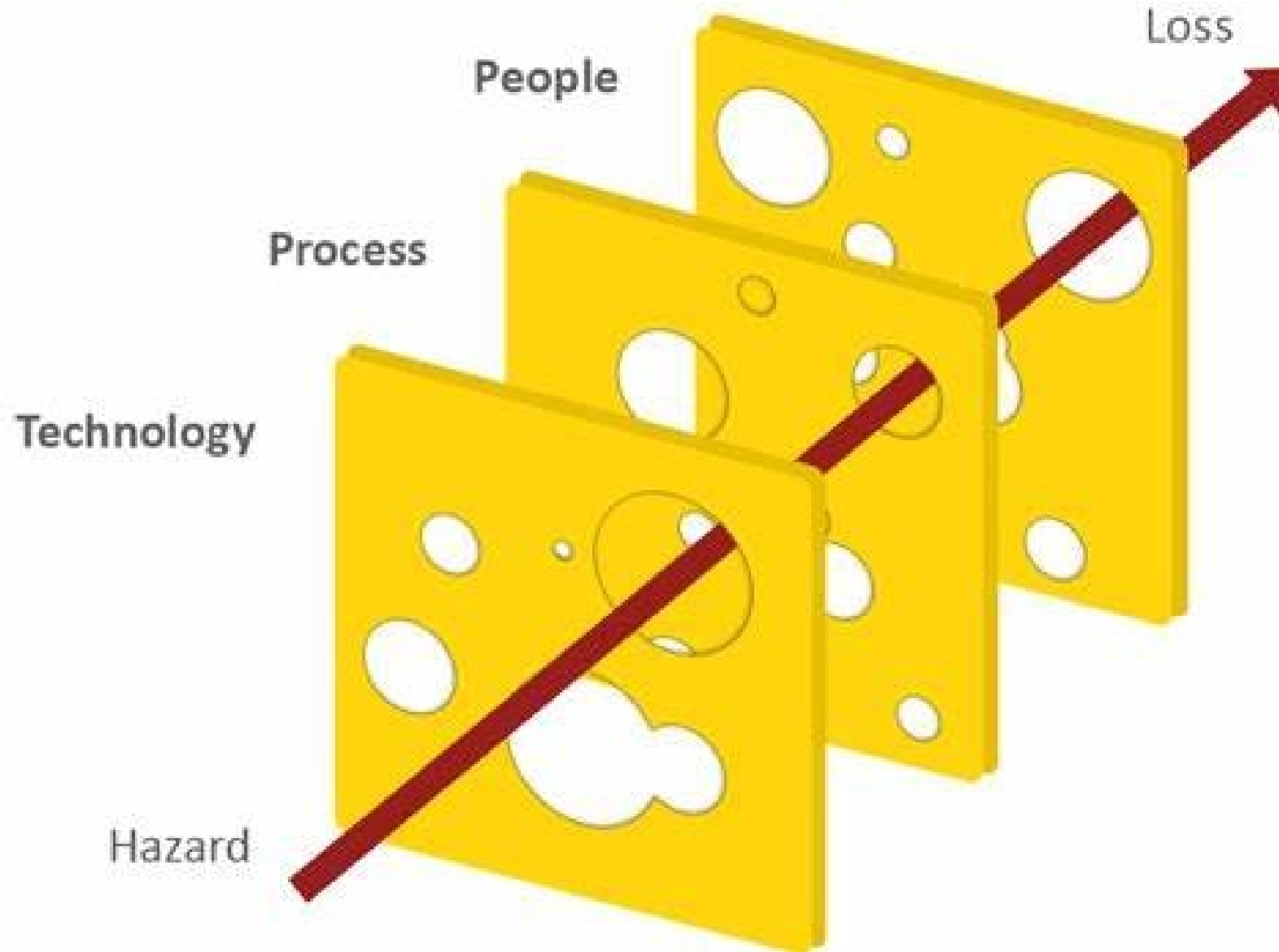
Faramarz Shahi Savandi

- ❖ \$17 million unofficial estimated cost for recovery and rebuild
- ❖ 77 “critical systems” affected
 - Timekeeping
 - Water bill payments
 - Municipal Court ticket payments
 - Inmate processing at Corrections
 - City Council Legislative system
- ❖ 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.

“Before the attack, 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.”



8 Headlines That Defined 2018 for Internal Audit



INTERNAL
AUDITOR

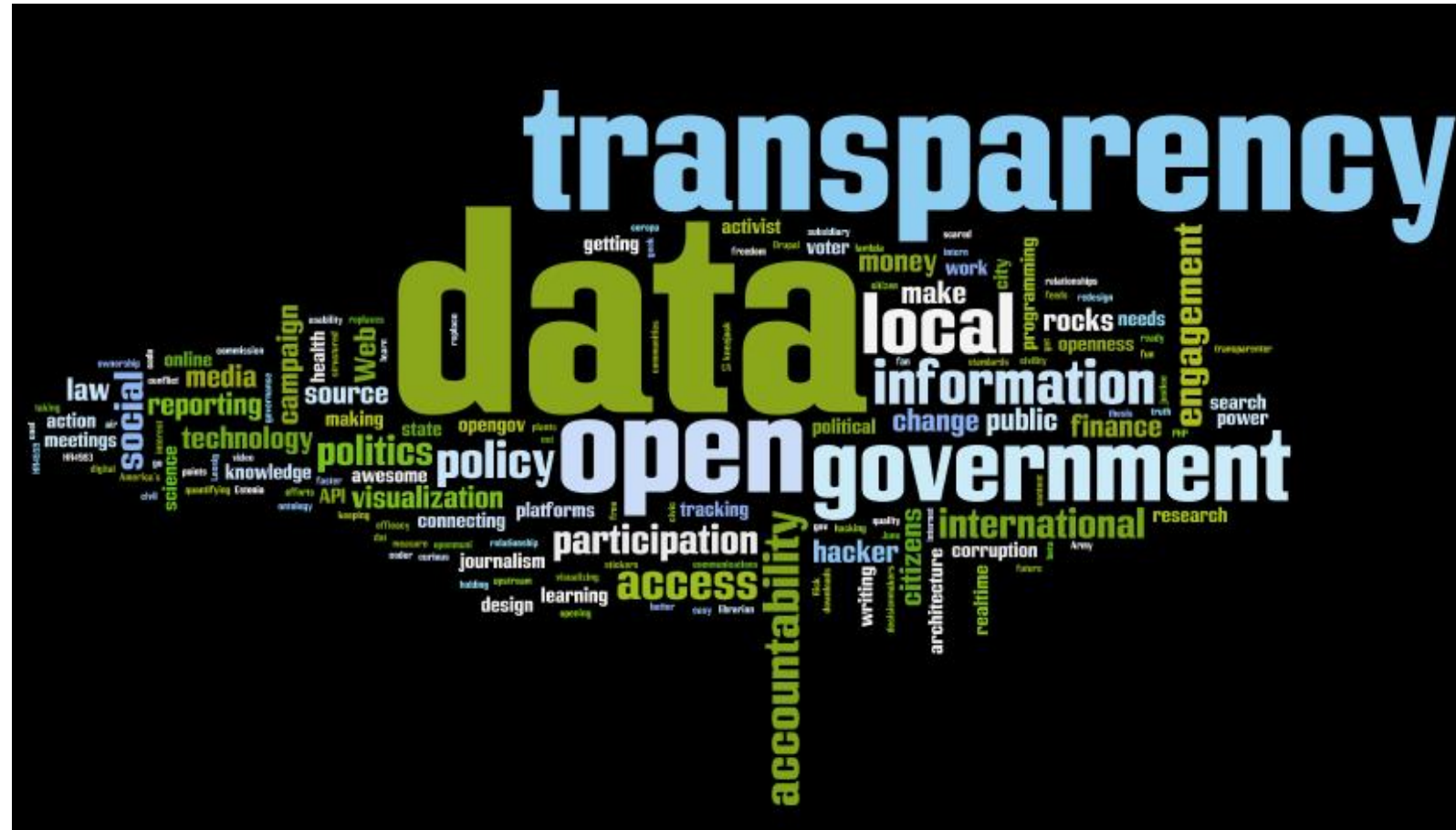
Internal Audit Findings Could Have Prevented Atlanta's Ransomware Attack

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."

IT Audits & Public Transparency OR *Things That Make You Go Hmmmmm*

- ❖ Does the public have a right to know?
- ❖ Value in public reporting?
- ❖ What is the right amount of public reporting?



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

