IT Audits

Joan Pu, CISA
City Auditor's Office, City of Kansas City, MO

Vivien Zhi, CISA
City Auditor's Office, City of Kansas City, MO

AGA Monthly Meeting
August 21, 2019

Objectives

- Why do we care about IT security?
- What are IT audits?
- What can we do?

Data Breach Statistics

https://breachlevelindex.com/

DATA BREACH STATISTICS

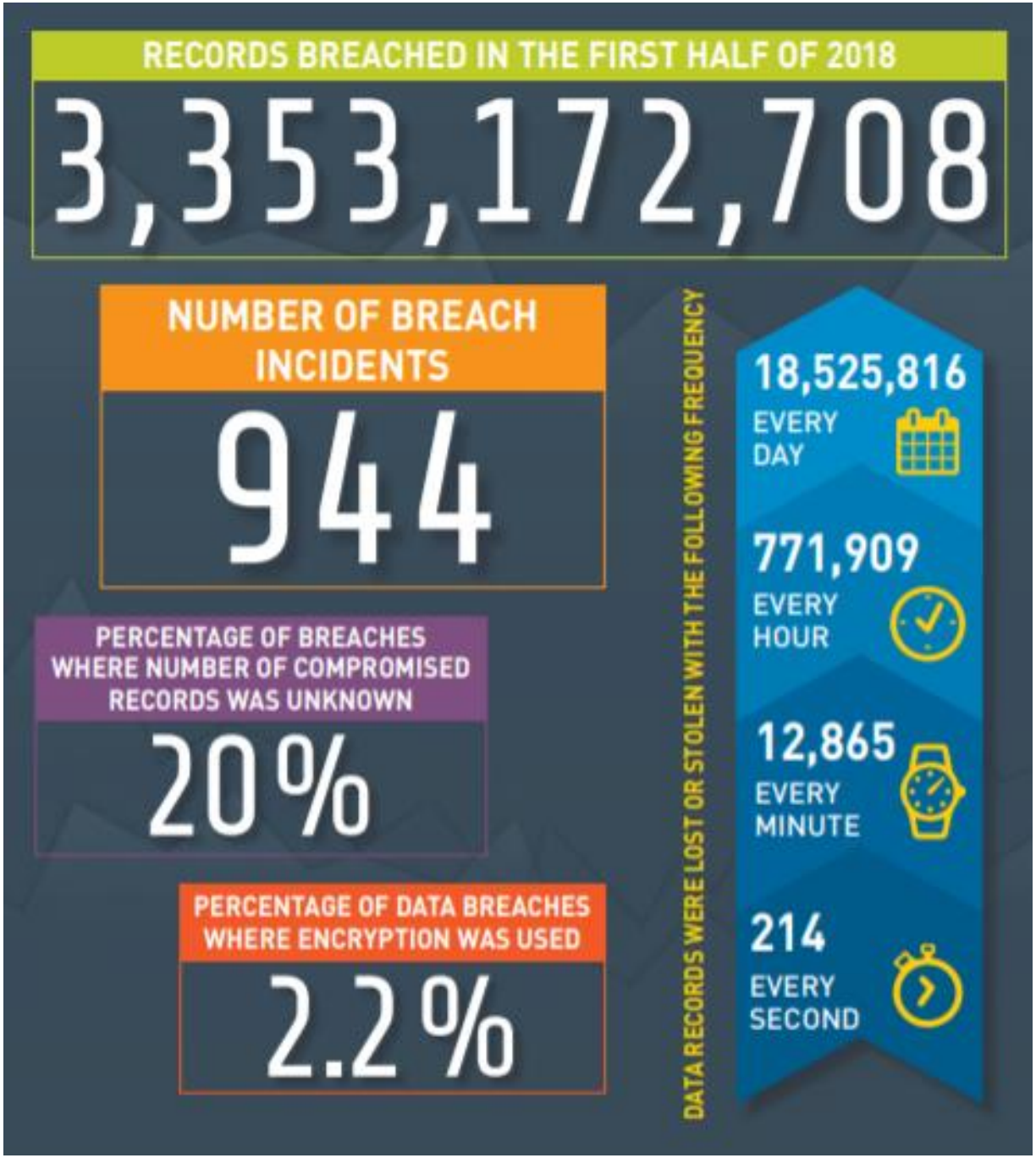
DATA RECORDS LOST OR STOLEN SINCE 2013

14,717,618,286

ONLY **4%** of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

EVERY DAY	EVERY HOUR	EVERY MINUTE	EVERY SECOND
6,079,148	253,298	4,222	70
Records	Records	Records	Records


RECORDS BREACHED IN THE FIRST HALF OF 2018
3,353,172,708
NUMBER OF BREACH INCIDENTS
944
PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN
20%
PERCENTAGE OF DATA BREACHES WHERE ENCRYPTION WAS USED
2.2%
DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY
18,525,816 EVERY DAY
771,909 EVERY HOUR
12,865 EVERY MINUTE
214 EVERY SECOND

Governments are Under Attack

The first half of 2015 has shown a shift in attack targets. Health care and **government** overtook retail as the major sectors under attack with the number of compromised data records.

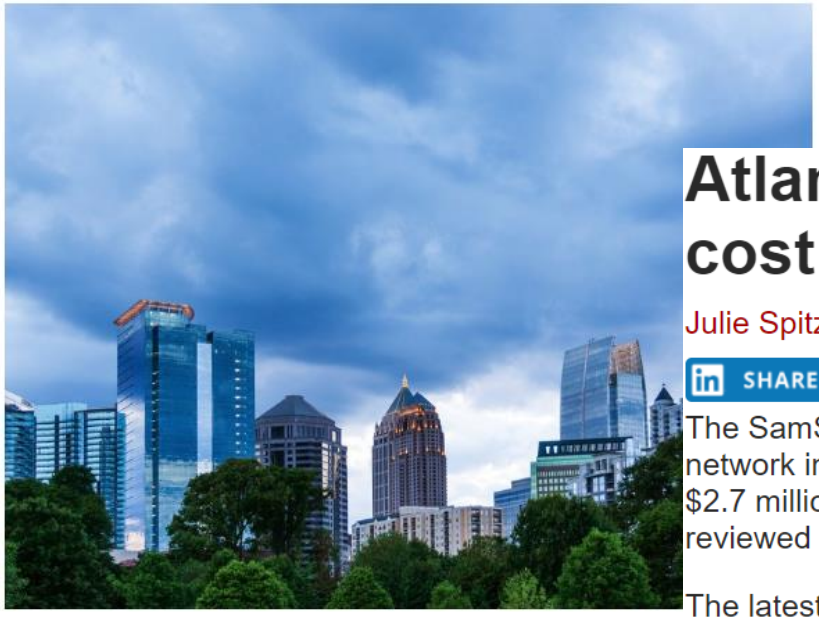
-- Gemalto, 2015 First Half Review

Ransomware Attack Hits 23 Texas Towns, Authorities Say

The state declined to say which towns were affected by the coordinated cyberattack. But one expert said it could signal more such attacks in the future.

Source: The New York Times, 8/20/19

ATLANTA SPENT $2.6M TO RECOVER FROM A $52,000 RANSOMWARE SCARE



Atlanta's ransomware attack may cost the city $17M

Julie Spitzer - Monday, August 6th, 2018 Print | Email

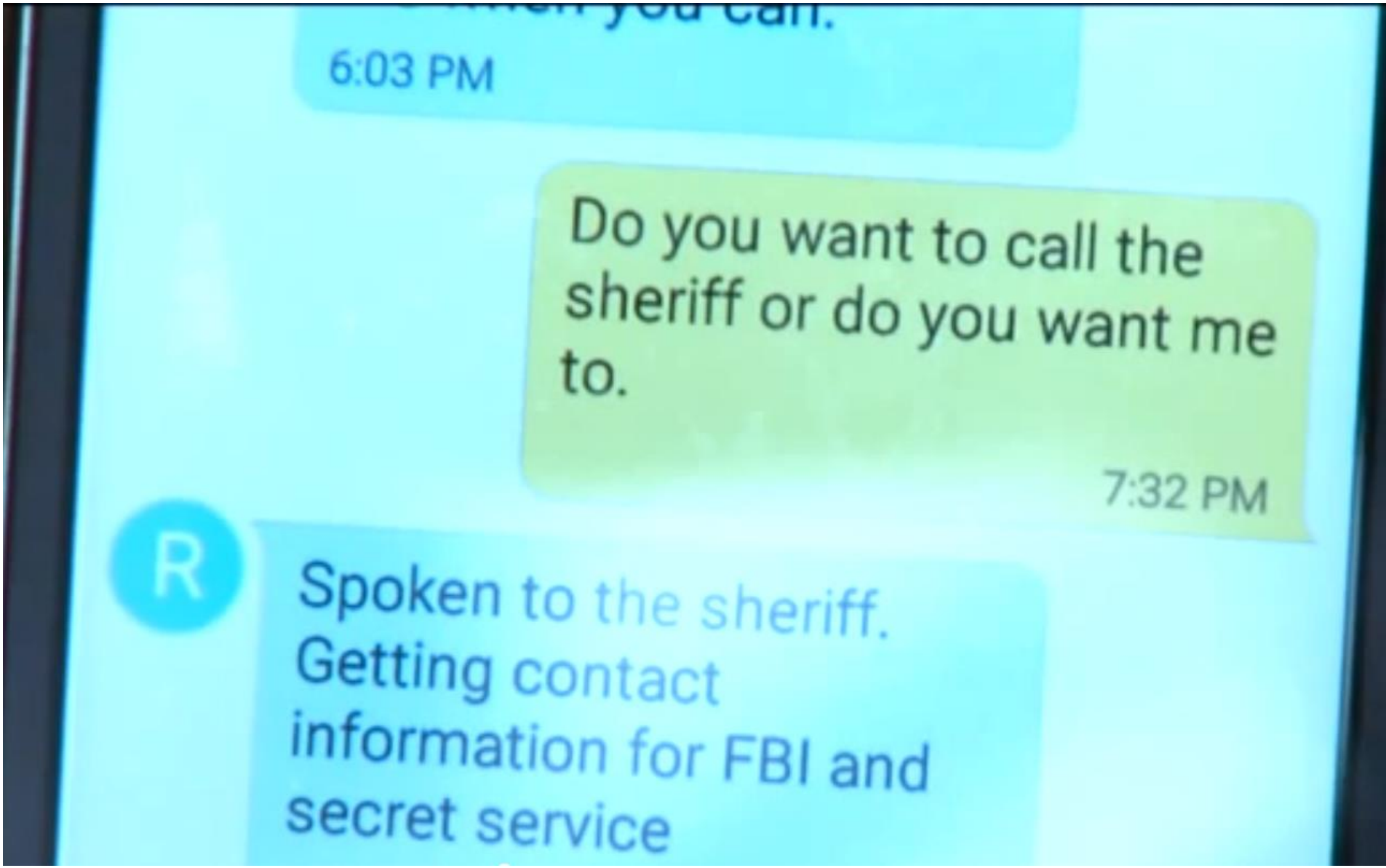
The SamSam ransomware attack that took down the city of Atlanta's computer network in March could cost taxpayers $17 million — up from earlier estimates of $2.7 million, according to a "confidential and privileged" seven-page document reviewed by *The Atlanta Journal-Constitution* and *Channel 2 Action News.*

The latest cost estimate includes about $6 million in existing contracts for security services and software upgrades and $11 million in potential costs associated with the attack, including new desktops, laptops, smartphones and tablets. This would mark one of the U.S.' costliest cyberattacks affecting a local government in 2018, despite city officials declining to pay the ransom demanded by the hackers.

"We are pleased with the progress of the recovery efforts. In addition to responding to the criminal attack against the city of Atlanta, we are using this opportunity to make the city more secure," a city spokesperson told the publications in an email statement. "Unfortunately, in today's world, governments are seeing an increase in cyber attacks … As you already know, the city is insured against cyberattack (sic). We continue to work through that process for the most cost-effective outcome for our residents."

“Many of us think that sort of thing is just not going to happen to us. You may be one of the lucky ones, but it’s less and less likely that you’re going to be one of the lucky ones every day.”

-- Kevin Haley, Symantec


6:03 PM
Do you want to call the sheriff or do you want me to.
7:32 PM
R
Spoken to the sheriff. Getting contact information for FBI and secret service

Truman Medical Center 'hit with ransomware' Tuesday

Maggie Holmes

Posted Aug 6, 2019 | 0

Cyber Attack Archive
Week of Aug. 12th

https://www.seculore.com/cyber-attack-archive

Latest Additions to the Archive: Week of August 12th

Public Safety

- New Jersey – Essex County
- Oregon – Crook County

Local Government

- Kentucky - Jefferson County
- Texas - Smith County

Medical

- *No attacks this week*

Education

- Pennsylvania – Elk County
- Florida – Alachua County

Park DuValle Community Health Center, Jefferson County

Breach Type – Unknown Ransomware

WDRB

July 25th, 2019

- Nearly $70,000 was given to hackers in the hopes that the data of around 20,000 patients would be released back to the center
- It has been several months without any sign of the data being restored as operations run on pen and paper
- This was the second attack that the center has faced forcing DuValle to lose over $1 million in attempts at restoration

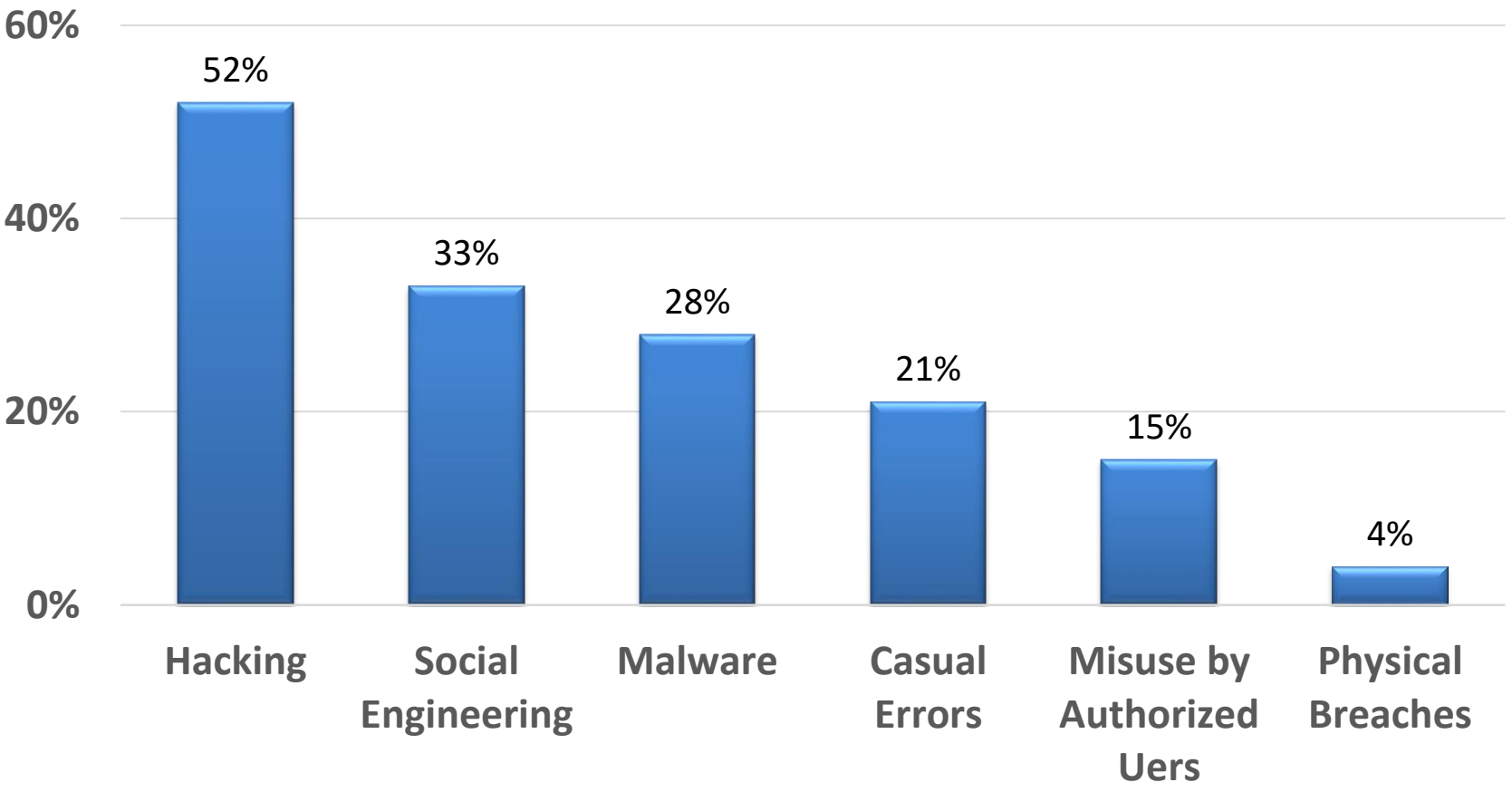
Read More

Cities in general approach cybersecurity like private companies do. But at the government level, you have fewer resources and also fewer skilled people, which makes things more difficult. You also have to deal with politics, and security is something invisible, particularly if people perceive that there aren't that many attacks.

-- Linda Poon, CityLab

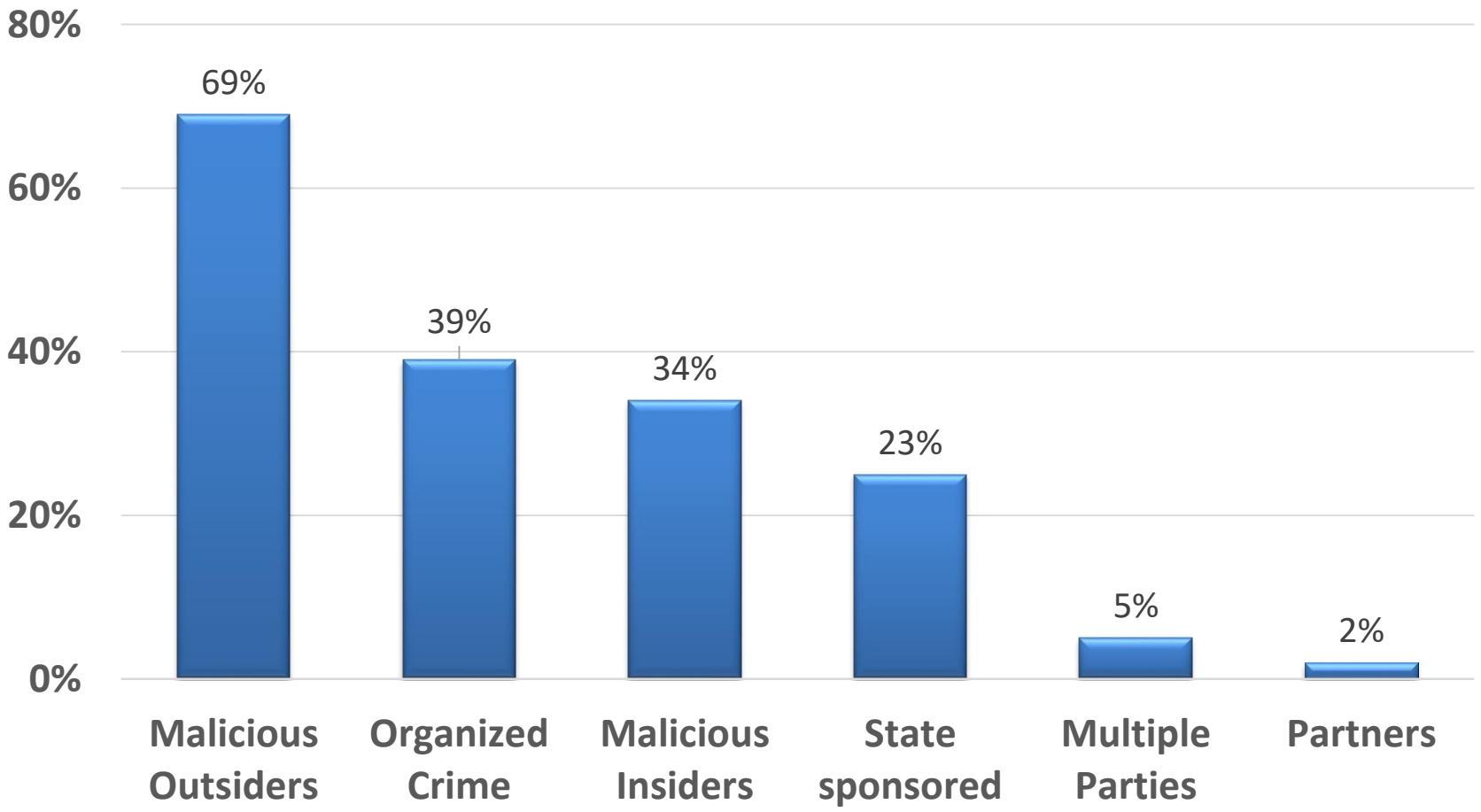
Purposes of Cyber Attacks

Tactics Used



Source: Verizon 2019 Data Breach Investigations Report

Leading Sources of Attackers



Source: Verizon 2019 Data Breach Investigations Report

Public Sector Breaches in a Glance

- 330 public sector entities had confirmed data disclosures.
- Cyber-Espionage, miscellaneous errors, and privilege misuse represent 72% of public sector breaches.
- 75% of public sector breaches are from malicious outsiders.

Source: Verizon 2019 Data Breach Investigations Report

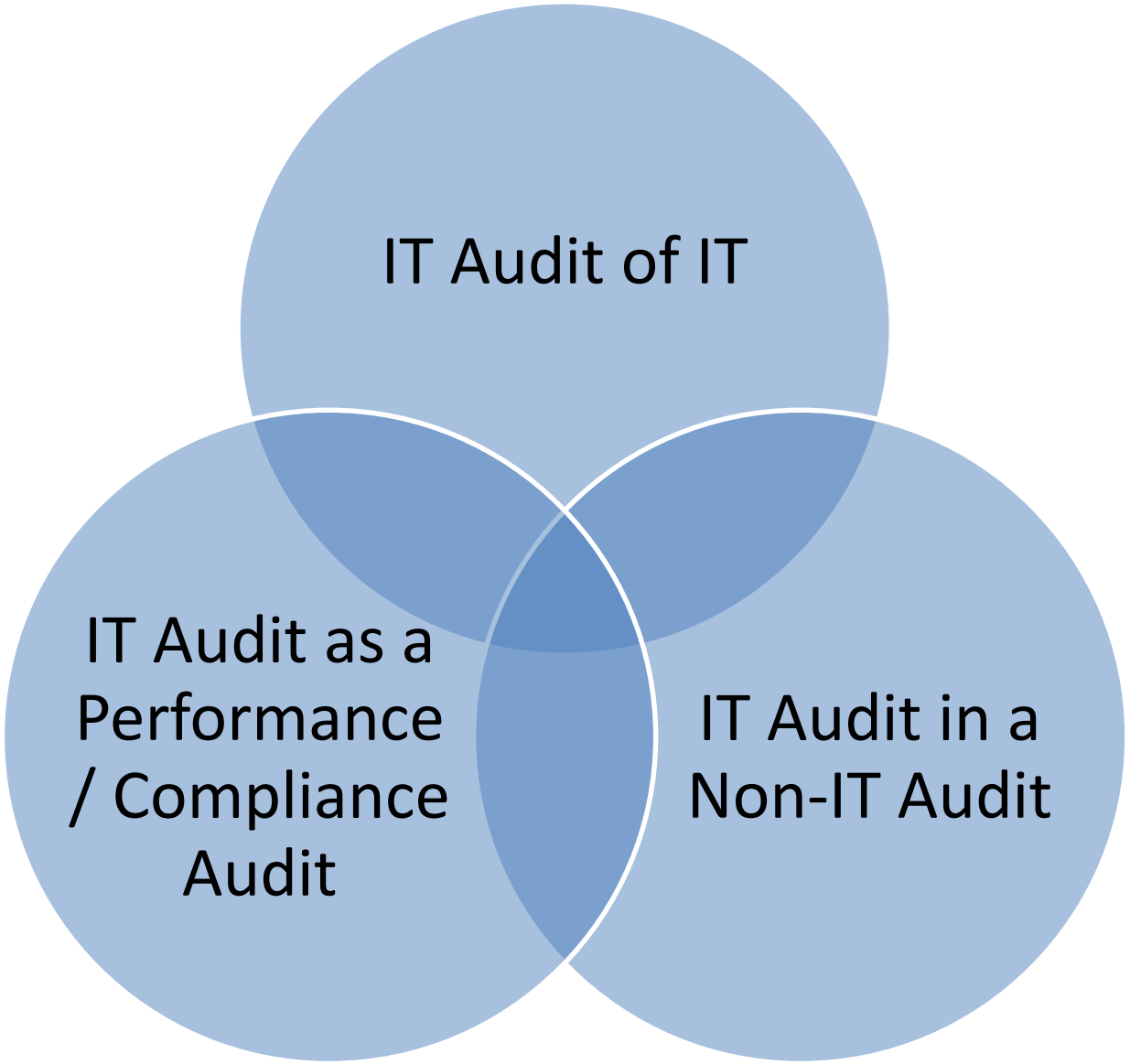
Types of Attack Vectors

- External/removable media
- Attrition
- Web
- Email
- Improper usage
- Loss or theft of equipment
- Other

Impacts of Security Incidents or Data Breaches

- Public trust and confidence
- Reputation
- Financial consequences
- Legal liability

What are IT Audits?

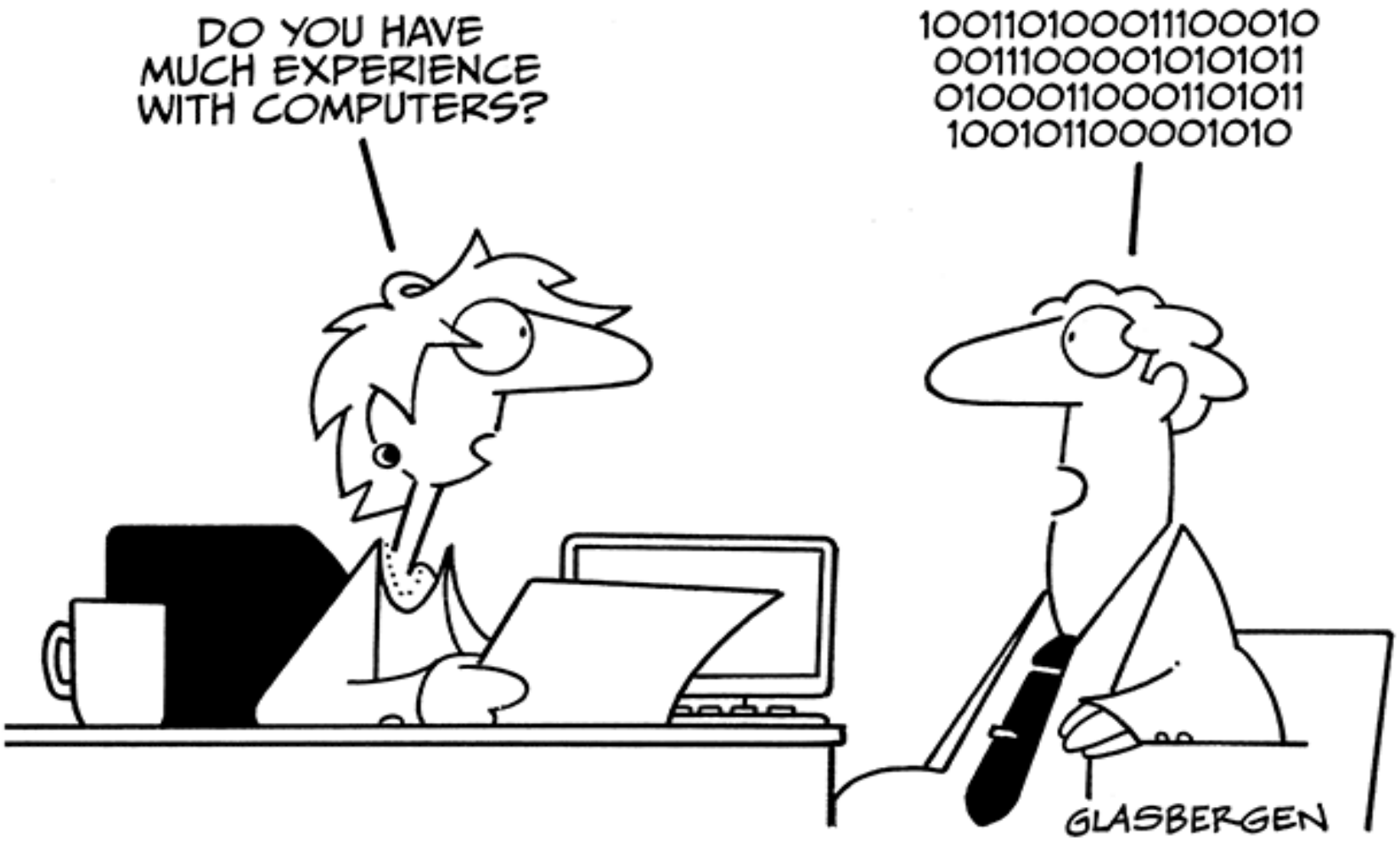


What are IT Audits?

IT audit is the process of **collecting and evaluating evidence** of the management of controls over an organization's information system, practices, controls and operations. The evaluation of evidence obtained through the IT audit process determines if the information systems are **safeguarding assets**, **maintaining** data **integrity**, and **operating effectively to achieve the organization's goals and objectives**.

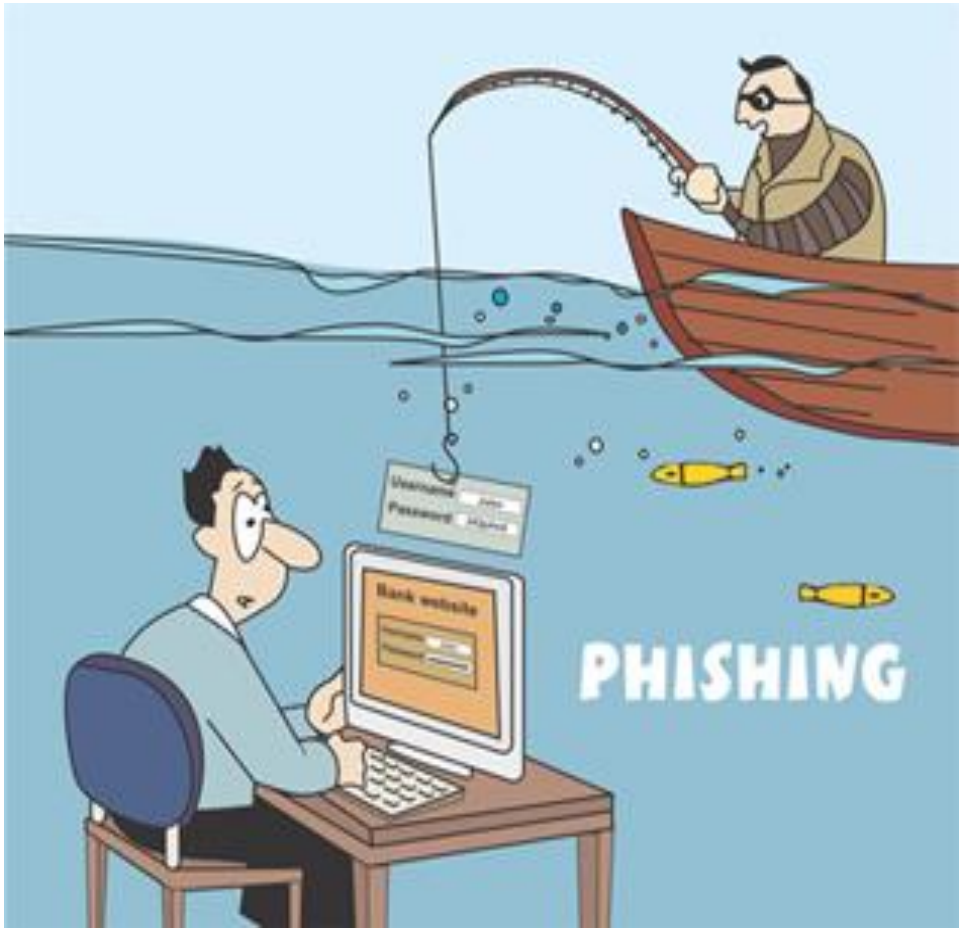
(Source: Protiviti, https://info.knowledgeleader.com/what-is-it-audit)

Conduct IT Audits Without Nerd-Level Knowledge



Audits

Employees' Response to Phishing Email Put City Information Systems at Risk (March 2015)



Identifying Phishing Emails

The email has poor spelling or grammar.

The email requests personal information. Legitimate businesses will not ask users to send their personal information through email.

The email seems too good to be true or the content places any kind of urgency.

The email is sent with a generic greeting such as “Dear Customer” or “Dear Member.”

The email contains attached files. The majority of banks and retailers will not send attachments via email.

Audits

Mobile Device Security Risks (November 2016)

DO

- Password protect your device
- Activate screen lock
- Encrypt the device
- Keep operating system and apps up-to-date
- Check app permission requests before downloading
- Disable location services when not in use
- Turn off Bluetooth when not in use
- Immediately report lost or stolen devices

DON'T

- Remove restrictions imposed by device's operating system
- Download apps from untrusted third-party app stores and markets
- Leave your mobile device unattended in public
- Connect your device to unknown Wi-Fi networks or hotspots

Symantec Guides to Scary Internet Stuff - Phishing

https://www.youtube.com/watch?v=v3JGY2L8NK4


Q
&
A

Contacts

Joan Pu

joan.pu@kcmo.org

816-513-3310

Vivien Zhi

vivien.zhi@kcmo.org

816-513-3321