Cyberterrorism: Attack on the Core Infrastructure

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Arnett Carbis Toothman llp
CPAs & Advisors

September 14, 2021

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Information and Cybersecurity

Everyone's Responsibility

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Presenter

Chris Joseph, CPA, CISA, CRISC, CITP

Partner, Arnett Carbis Toothman LLP

- IT Auditing
- IT Security
- Risk Assessment

Certified Public Accountant
Certified Information Systems Auditor
Certified in Risk and Information Systems Control
Certified Information Technology Professional

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Objectives

- **Why Cyberterrorism**
  - Purpose
  - Cyberterrorism defined
  - The shift
  - Hit where people live
- **Targets**
- **Types of Attacks/Threats**
- **Attacks on the Infrastructure**
- **Attacks – Health Care Industry**
- **Controls**
- **Questions**

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Why Cyberterrorism

Crazy Times!!!

Cyber Events

- Increasing
- Alarming (but not surprising) rate
- Targets have been changing
  - Not just businesses/organizations
  - Core infrastructure

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Why Cyberterrorism

Purpose of Terrorism

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Why Cyberterrorism

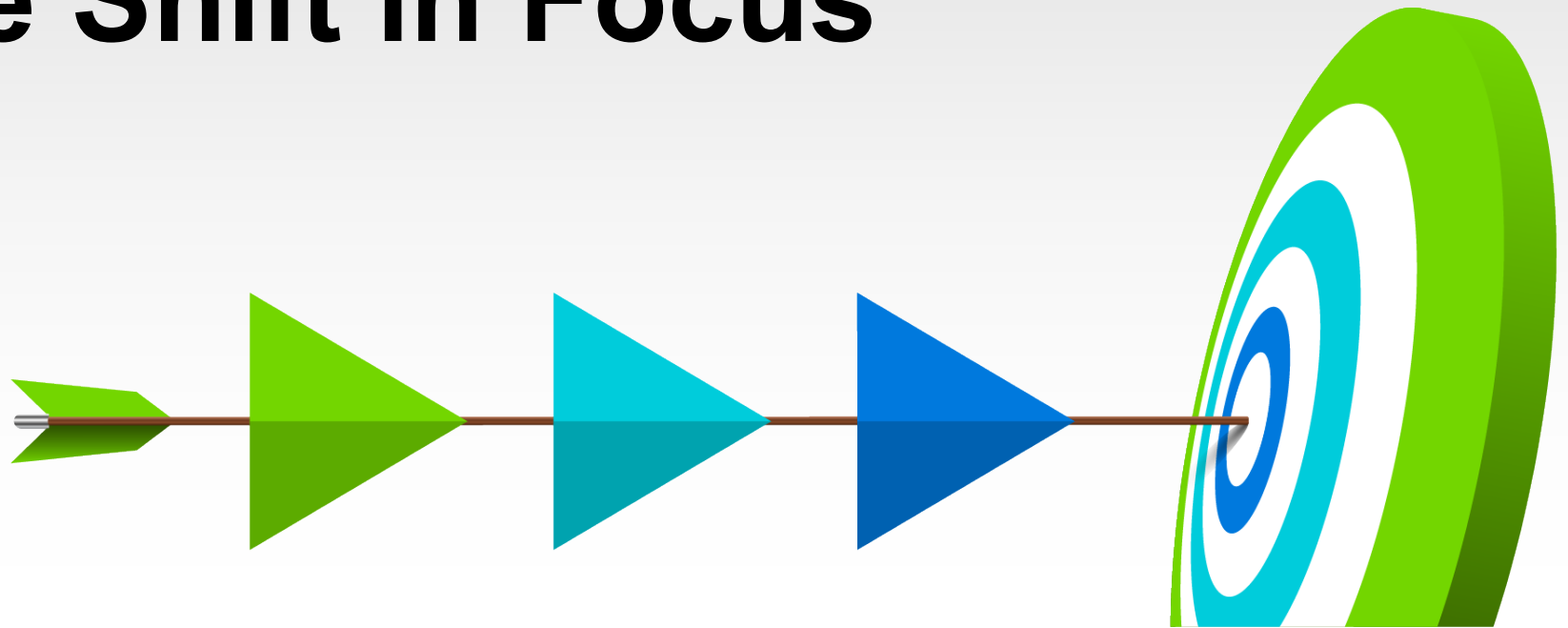
Cyberterrorism defined

- **Cyberattack**
  - Creates an impact that draws public attention
  - Creates fear in the public
  - Concern that our government organizations
    - Are not strong
    - Cannot protect us
  - In some cases, provides political value to the bad actors

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Why Cyberterrorism

The Shift in Focus



PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Why Cyberterrorism

- **Recent attacks used various forms of ransomware**
- **Historically used**
  - Encrypt data
  - Demanded ransom for decryption key
  - Upon payment, provided decryption key

There has been a change

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Why Cyberterrorism

- Now employ double extortion
- Does anyone know what the double extortion?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Why Cyberterrorism

- Hit people where they live
- Another shift
- Attacking the core infrastructure
  - Utilities
  - Water
  - Supply chain
    - Huge change in the trend
  - Others?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Targets

As indicated previously, potential, and real targets:

- Power grids
- Utility companies
- Water
- Supply chain
- Other traditional targets
  - Financial services industry
  - Health care industry

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

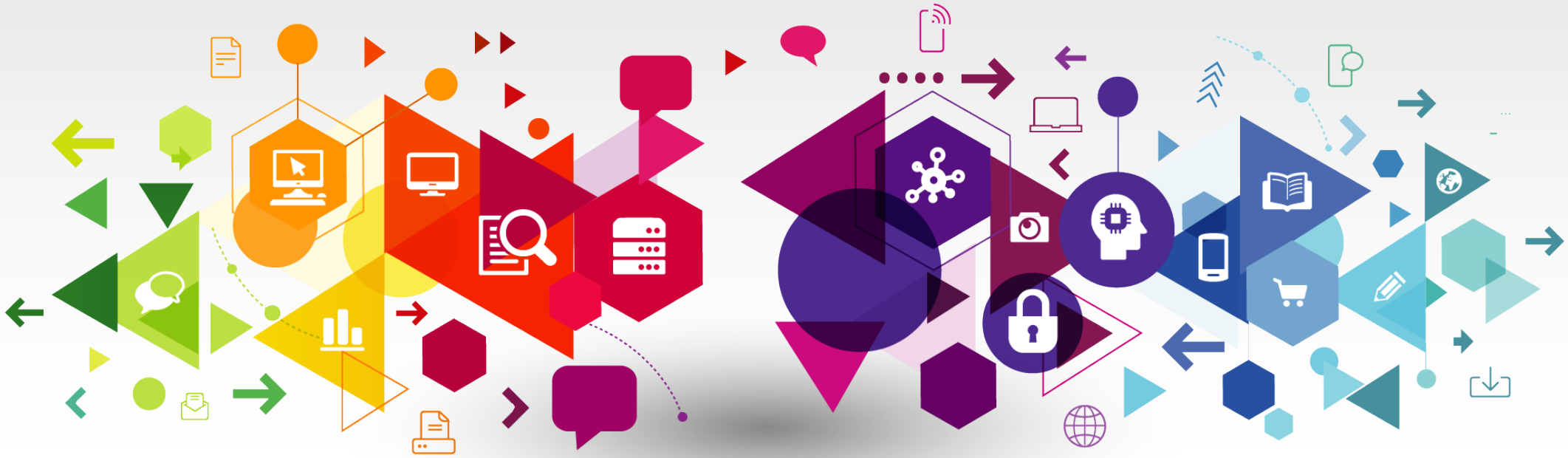
Targets

What allows the attack on the core infrastructure?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Targets

Information Technology vs Operational Technology



PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Targets

Information Technology

- Controls data
- Securing
  - Confidentiality
  - Integrity
  - Availability

Systems and data

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Targets

Operational Technology Defined

- Is it hardware?
- Is it software?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Targets

Operational Technology

- Use of hardware and software
- Monitor and control
  - Physical processes
  - Devices
  - Infrastructure

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Targets

Operational Technology

- Used in multiple industries
  - Manufacturing
  - Oil and gas
  - Electrical generation and distribution
  - Aviation
  - Maritime
  - Rail
  - Utilities
  - Others?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Targets

Operational Technology

Gartner Defines:

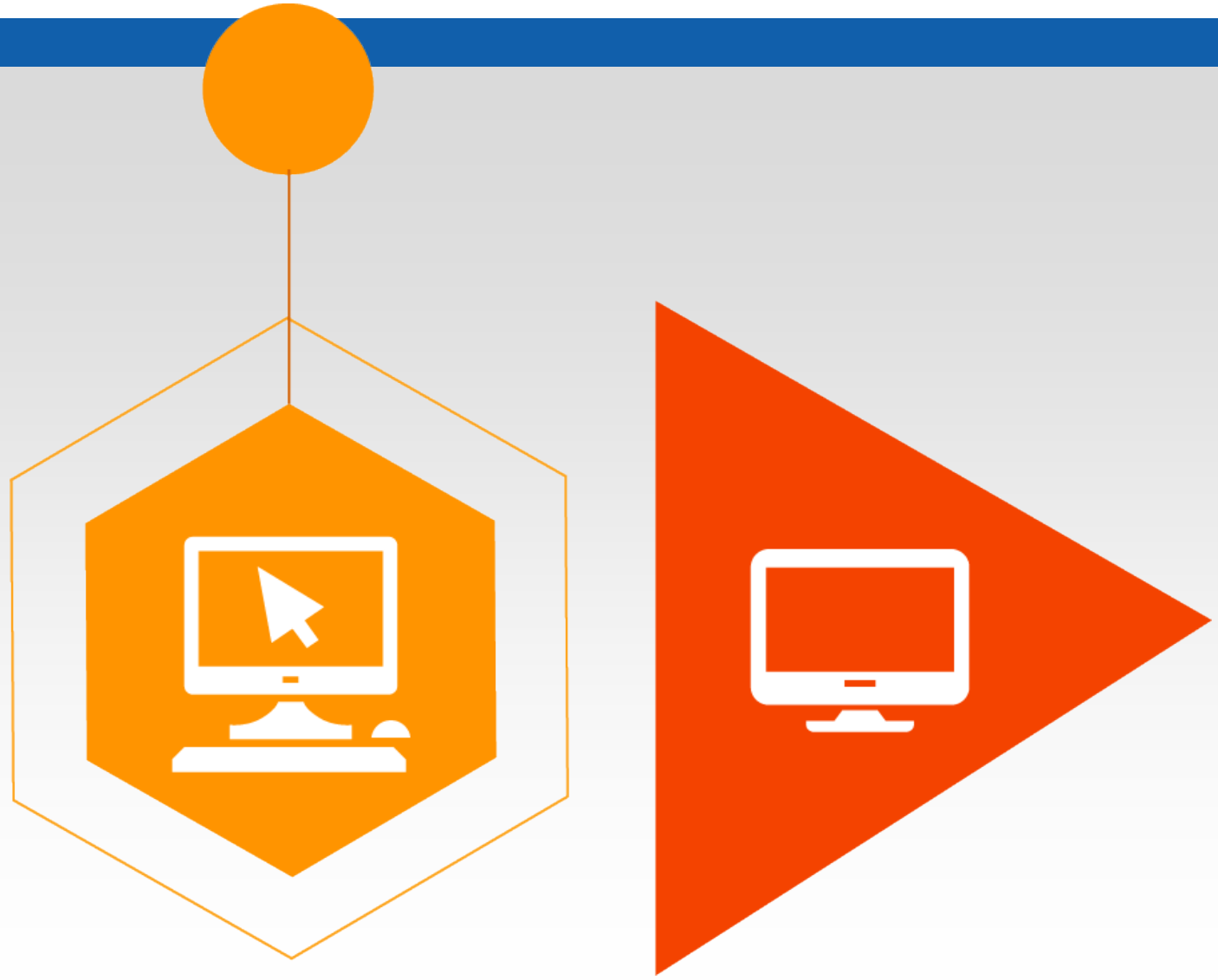
- Protect people, assets, and information
- Monitor and/or control physical devices, processes and events
- Initiate state changes to enterprise OT systems

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Targets

Operational Technology

- Initially not a target
- Why the change?

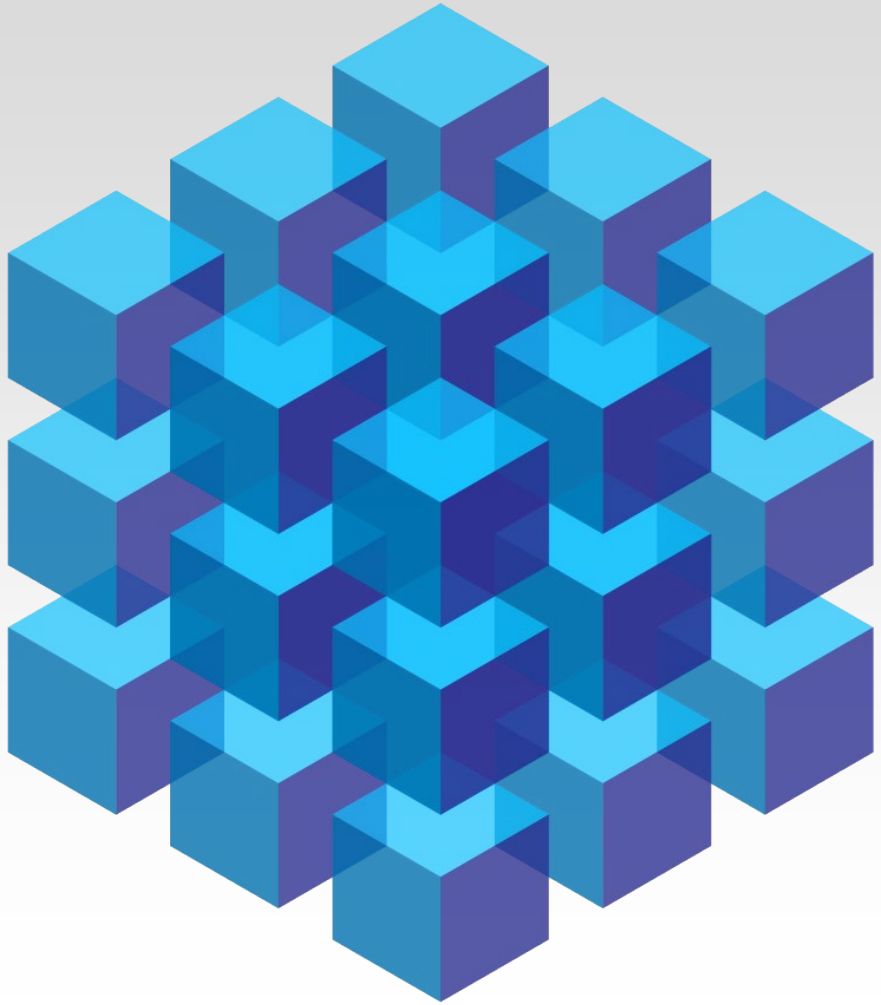


PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Targets

Operational Technology

- Separate IT and OT networks
  - Duplicating security efforts
  - Lack of transparency
- During an attack
  - Difficult to track what is happening
  - Typically different leaders
    - OT report to Chief Operations Officer
    - IT report to Chief Information Officer
- Difficult to identify the boundaries



PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

Various type of attacks/threats:

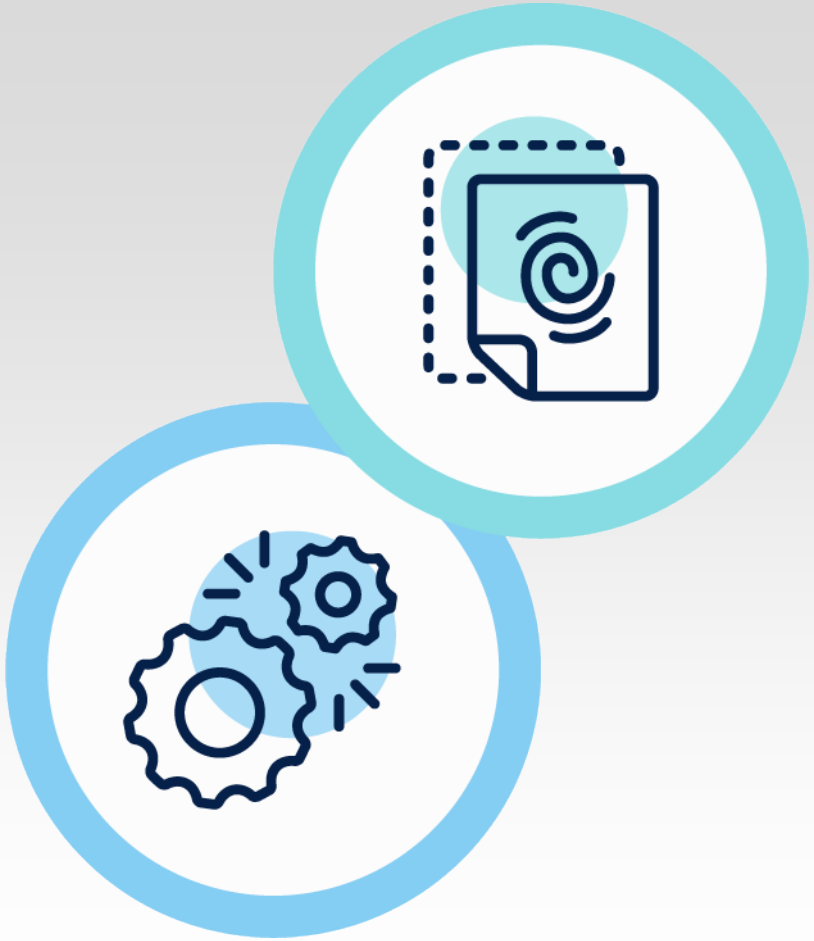
- **Phishing attacks**
- Negligent and malicious insiders
- Advanced persistent threats
- Cyberattacks
- Zero day attacks

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

Various type of attacks/threats:

- Known software vulnerabilities
- **Social engineering**
- Denial of service attacks
- Brute force attacks
- **Ransomware**



PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

- Phishing attacks have historically and remain number one

- Huge increase in ransomware
  - Various ways to engage
  - Phishing attacks one of the ways

Going to focus on ransomware today

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

First 5 months of 2020

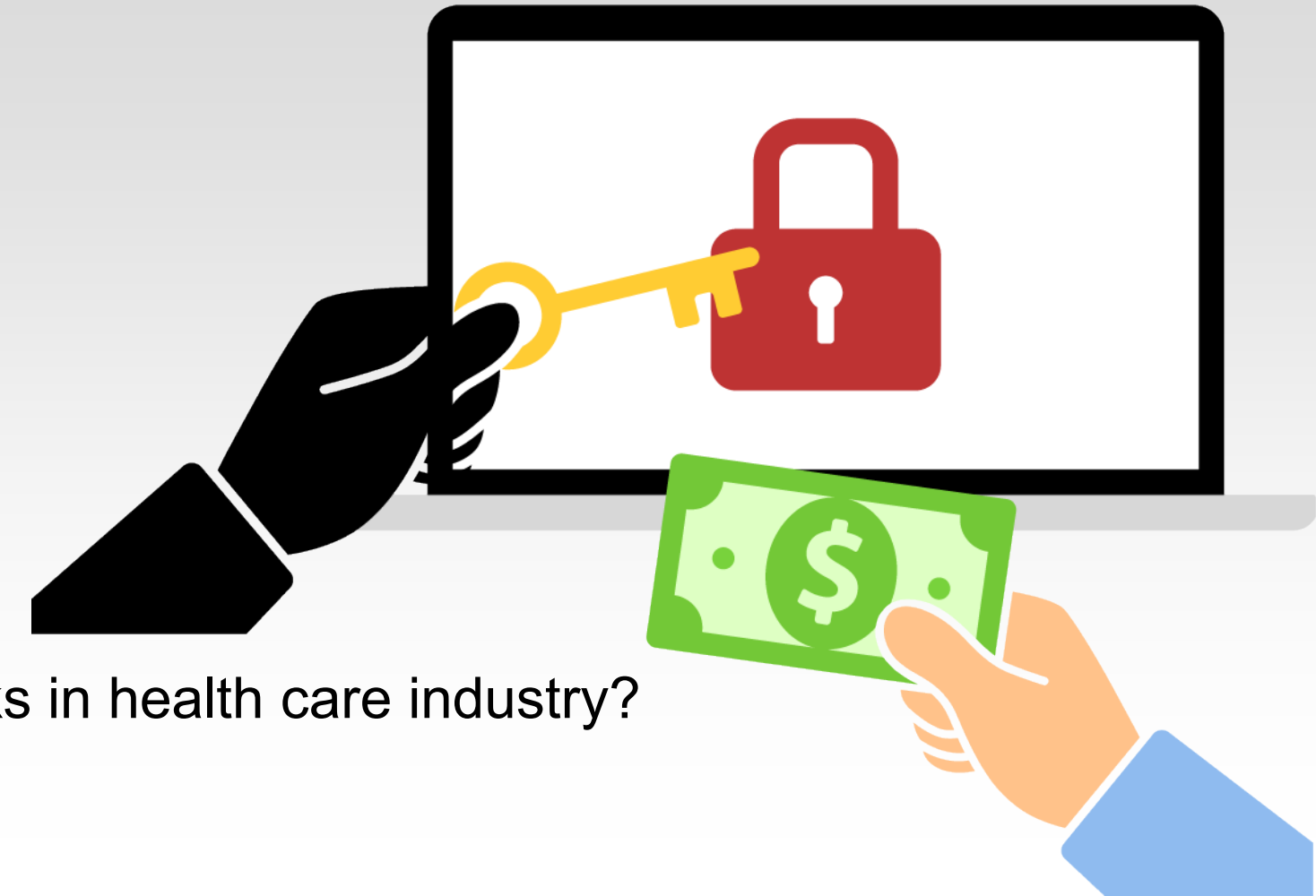
- 900% increase in Ransomware
- 64% increase in wire transfer fraud
- 33% of the time
  - Island Hopping occurs
- 25% experience escalation responses
  - Destructive attacks

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

In 2020

- 2,354 ransomware attacks
- Industries attacked
  - U.S. Government
  - Health care
  - Schools
  - Others
- Industry with most successful attacks?
- Number of successful attacks in health care industry?



PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

Ransomware

- Prevents users from accessing
  - Their system
  - Personal files
- Demands ransom payment to regain access
- First variants back in the 1980s
  - Payment through the mail
  - How is payment handled today?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

Types of Ransomware

- Scareware
  - More of a nuisance
  - Receive popups claiming malware
  - Claims payments to get rid of it
  - No threats to files, just popups

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

Types of Ransomware

- Screen lockers
  - Locks the screen
  - Claims illegal activity from the FBI, etc.
  - Wants payment to unlock

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

Types of Ransomware

- Encrypting ransomware
  - Nasty stuff
  - Obtains the files and encrypts them
  - Demands payment to decrypt

- Should you pay?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

FBI Does NOT Recommend Paying

Why Not?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

Payment

- Initially, small amounts of money
  - $100 to a few thousand
- Now, amounts increased dramatically
  - Can reach into 6 figures
    - Sometimes greater
- Why the change?

Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

Significant Ransomware Increase

- 900% increase
- Why?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Types of Attacks/Threats

Ransomware-as-a-Service

- Yes there is such a thing – increasing
  - Do not have to have advanced technical skills
- What's the source
  - Cyber gangs
  - A new model has develop
- Used to demand a significant subscription fee
  - **Anyone have an idea how it is packaged now?**

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure

SolarWinds

- The game changer
- Termed the worst nightmare by some

Why?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure

SolarWinds

- Compromised the routine software update process
  - A popup window announces its arrival
  - Plug everything in before bed
  - Next morning, software is updated
- In a way, we have an implied trust with the updates

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure

SolarWinds

- What happened
- Orion product
  - Popular network management system
  - Keeps a watchful eye on all the various components in a company's network
- "Routine" update was posted

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure

SolarWinds

- Bad actors slipped malicious code into the Orion software
  - Through the routine update
- Became a vehicle
  - Massive cyberattack against various organizations
  - At one time, 18,000 organizations was the best guess impacted
    - Per SolarWinds
    - Feels the actual number impacted was lower

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure

SolarWinds

- Two conditions
  - Download the tainted update and deploy it
  - Compromised networks needed to be connected to the internet
    - Allowed the bad actors to communicate with the servers
- Organizations known to be impacted
  - Treasury
  - Department of Justice
  - Energy departments
  - Microsoft, Intel, Cisco among others

Pennsylvania Coalition of Affiliated Healthcare & Living Communities

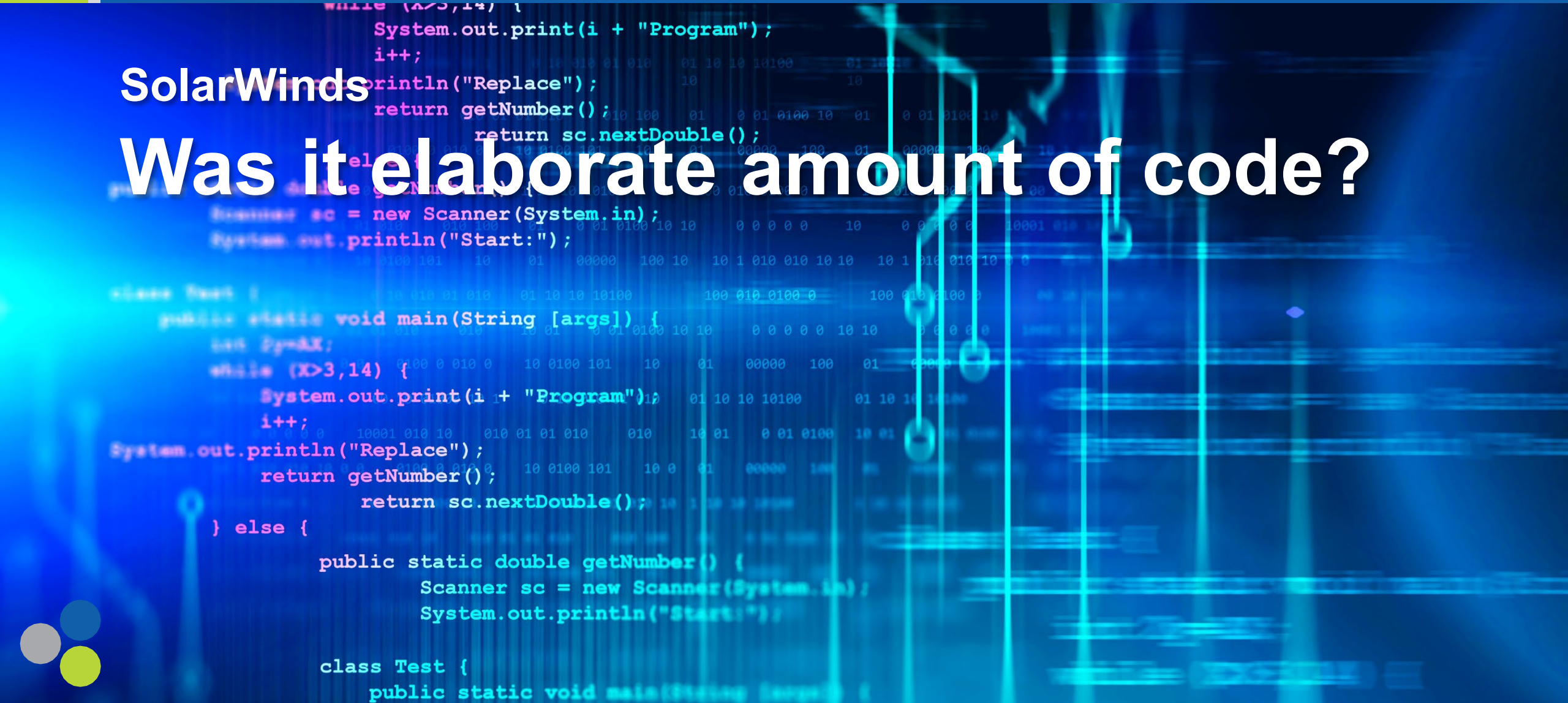
Attacks on the Core Infrastructure

SolarWinds

- Monitoring software touches the entire network
- Potential to do a great deal of harm
- Cybersecurity firm FireEye discovered it
  - FireEye's CEO – used to be in the U.S. Air Force Office of Special Investigations
  - An employee appeared to have two phones registered on the network
  - Follow-up indicated phone not registered by the employee

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure



PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure

Oldsmar, Florida Water Supply

- Bad actor remotely accessed the water supply system
- Changed the setting for the amount of sodium hydroxide
  - Known as lye
  - Typically small amounts are used to control acidity
  - Large amounts can lead to major issues
- Increased it more than a 100 fold
  - 100 parts to 11,100 parts

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure

Oldsmar, Florida Water Supply

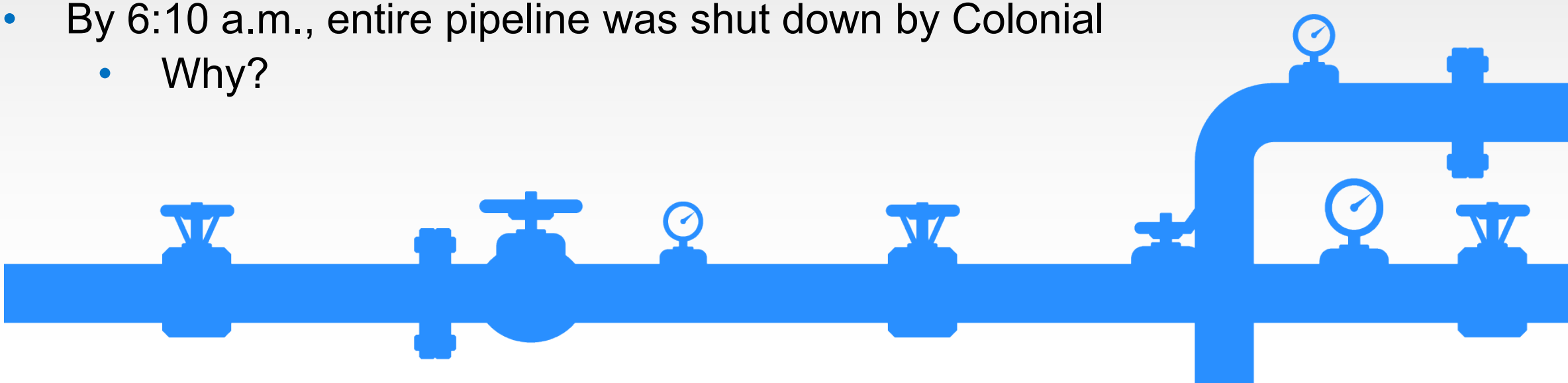
- Results could have been
  - Sickened residents
  - Corroded pipes
- How discovered
  - Plant operator / supervisor
  - Noticed mouse move around on his computer screen
  - Noted the bad actor changed the sodium hydroxide levels

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure

Colonial Pipeline

- Bad actors gained entry into the networks on April 29
  - Anyone know how?
- May 7, Colonial received the ransom note / message
  - Notified just before 5:00 a.m.
- By 6:10 a.m., entire pipeline was shut down by Colonial
  - Why?



PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure

Colonial Pipeline

- First time shutdown in 57 year history
- 5,500 miles of pipeline
- From Texas to New Jersey
- 2.5 million barrels a day of gasoline
- Approximately half of the East coasts gasoline
- Resumed service on May 12

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

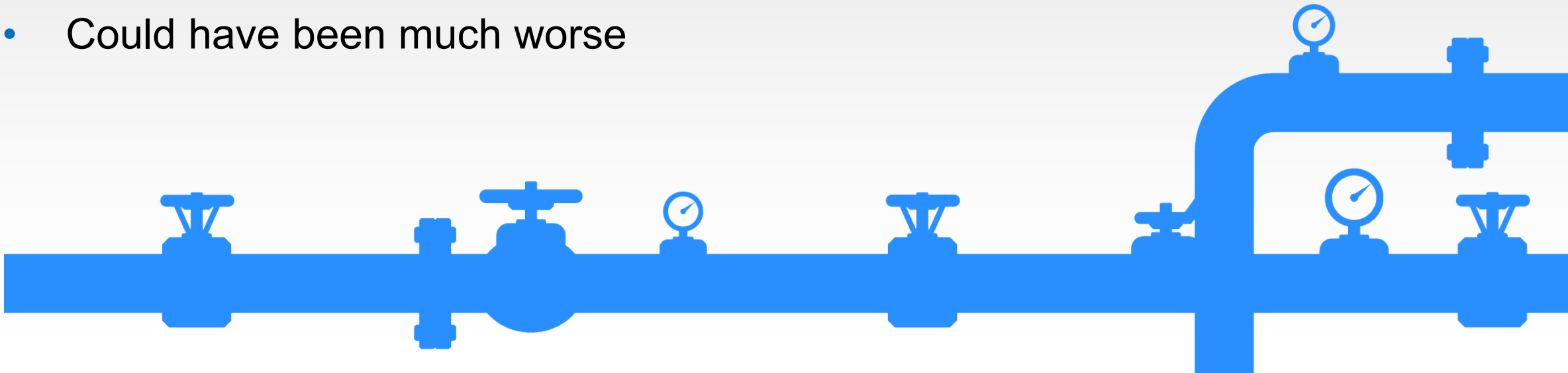
Attacks on the Core Infrastructure

Colonial Pipeline

- Colonial paid the bad actors' ransom ($4.4 million in bitcoin)
- Worked with the FBI to recover part of the ransom
- Does anyone know what else the bad actors did?

Did not compromise the overall Operational Technology

- Could have been much worse

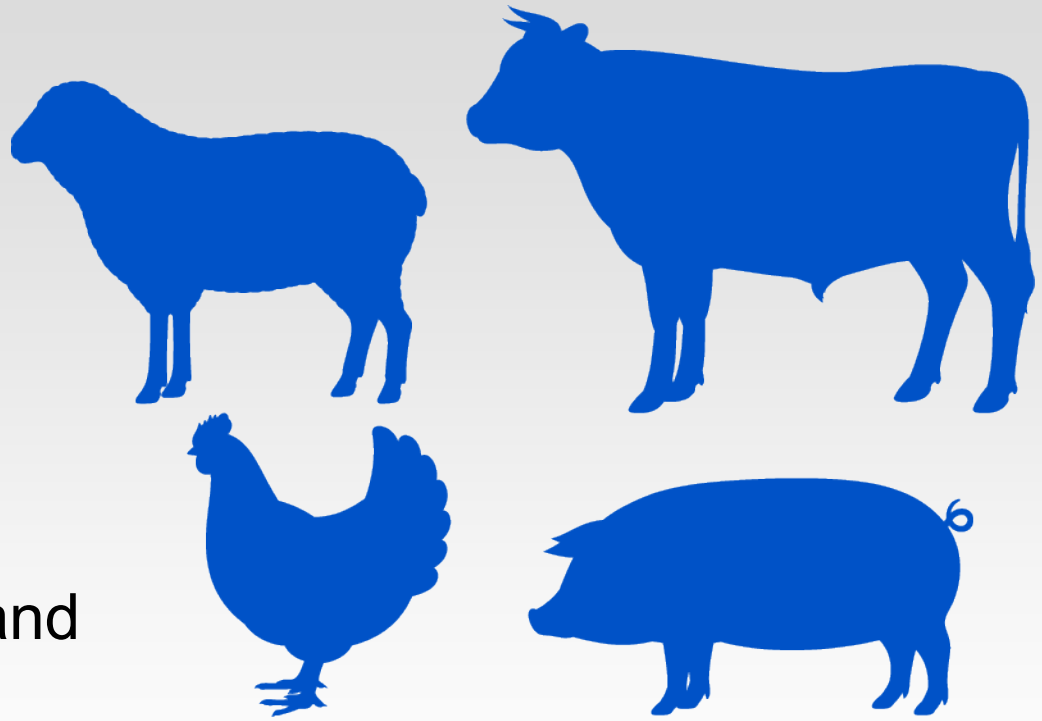


PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure

JBS

- World's largest meat supplier
  - 150+ plants
  - 15 countries
  - 150,000+ employees
- Customers include supermarkets, McDonalds, etc.
- Supplies close to one-fourth of the beef and one-fifth of pork to the United States

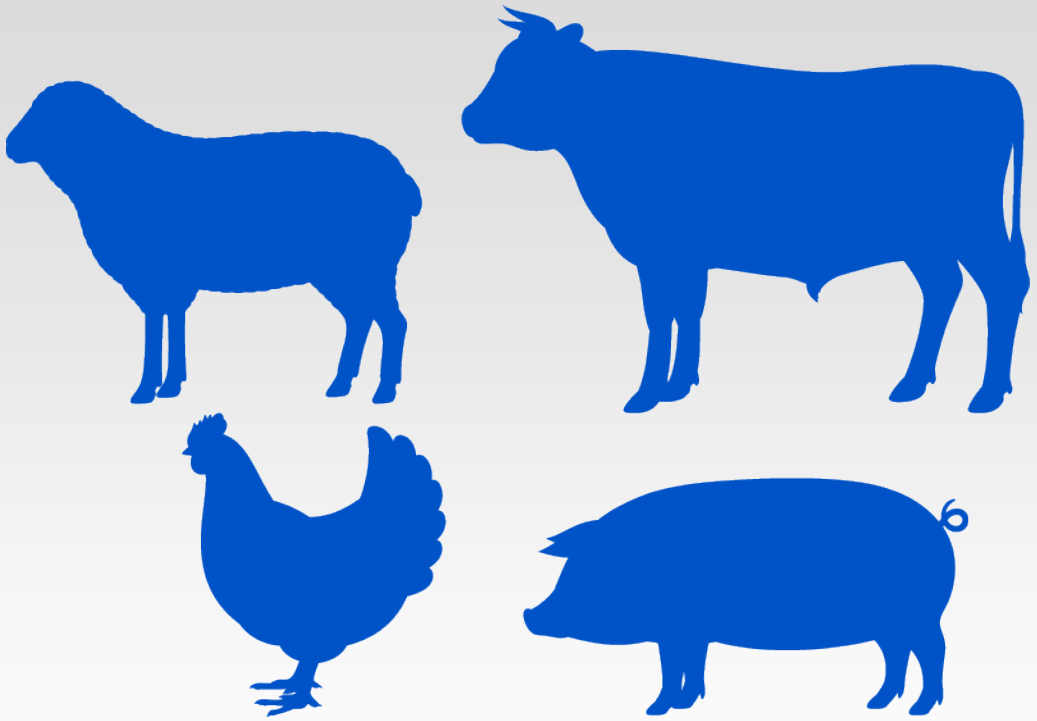


PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks on the Core Infrastructure

JBS

- Ransomware attack in May
  - REvil ransomware gang
  - Shut down operations
    - Australia
    - Canada
    - United States
  - Shut down for at least a day
  - Paid $11 million ransom
    - Concerned about exfiltration of data



Attacks – Health Care Industry

In 2014

- FBI – Health care industry under attack

Health Care Industry a Prime Target

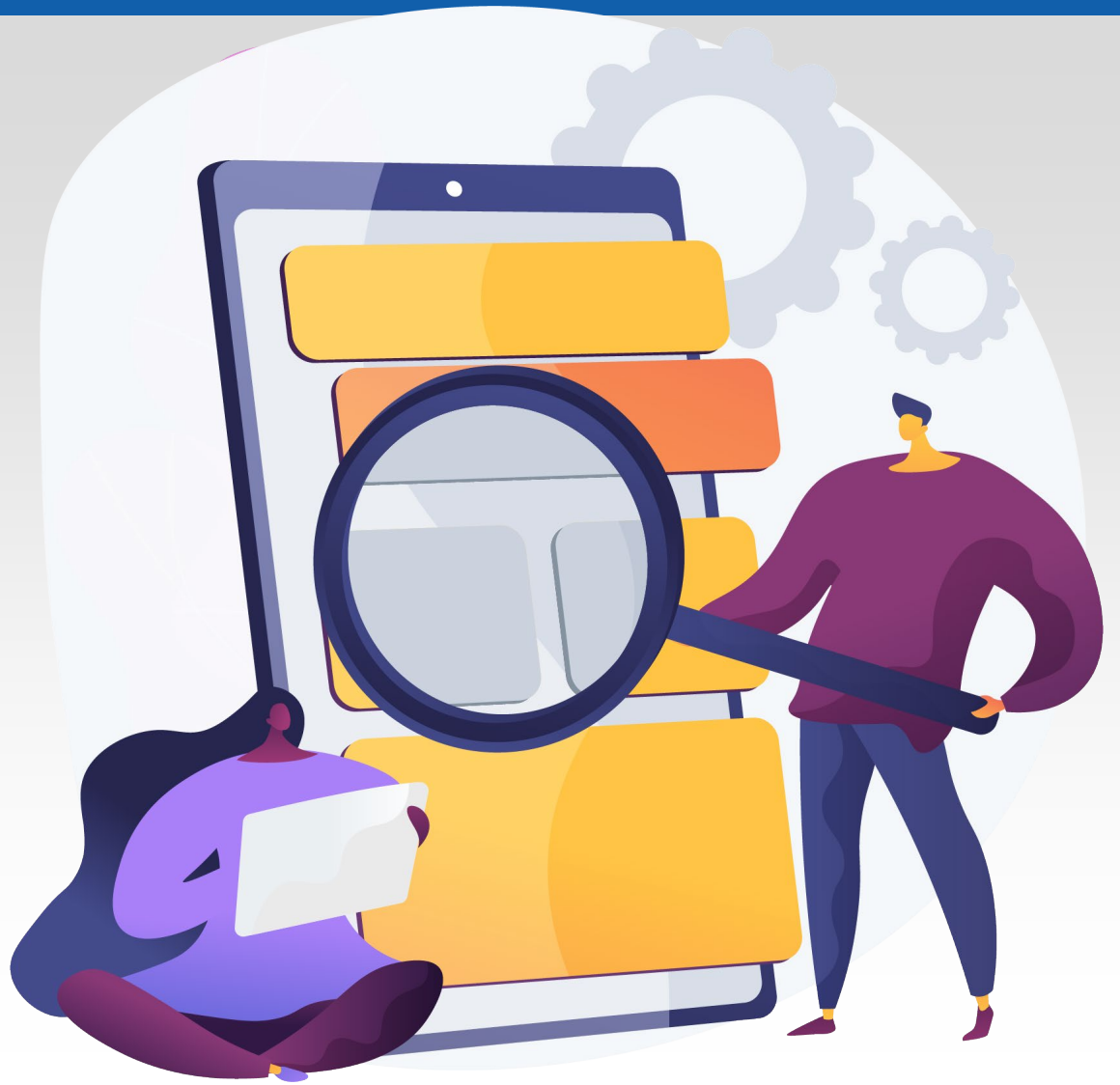
- Data stored
  - PHI
  - ePHI
  - PII
  - Financial
- Black market value?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks – Health Care Industry

Health Care Industry Under Attack

- IT security challenges
  - Legacy systems
  - Budgetary restraints
  - Availability of information security personnel
  - Different type of users



Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks – Health Care Industry

Who are the Threat Actors in Health Care?

External

- Hackers
- Nation States
- Organized Crimes

51%

Internal

- Careless Employee
- Malicious Employee
- Disgruntled Employee

48%

Partners

- Vendors
- Business Partners
- Commonly Controlled

2%

Source of % is Verizon's 2020 Data Breach Investigation Report

Attacks – Health Care Industry

HIPAA Journal

- Include data breaches of 500 or more records
- Upward trend over the past 10 years
  - 2020 more data breaches since records published
- Between 2009 and 2020
  - 3,705 health care data breaches of 500 or more records
  - 268,189,693 health care records

Attacks – Health Care Industry

HIPAA Journal

- Hacking is now the leading cause of data breaches
  - Detection has taken months and even years before detected
- Insider breaches
- Loss/theft of PHI and unencrypted ePHI
- Improper disposal of PHI/ePHI

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks – Health Care Industry

Virtual Care Provider Inc. (VCPI)

- Milwaukee, WI based IT company
- Provides multiple services to nursing homes and acute-care facilities
  - IT consulting
  - Internet access
  - Data storage
  - Security services

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks – Health Care Industry

Virtual Care Provider Inc. (VCPI)

- November 17, 2019, launched ransomware at 1:30 a.m.
  - Ryuk
- Encrypted all data the VCPI hosts for their clients
  - Serve 110 clients in 45 states
  - 2,400 nursing homes
  - Approximately 80,000 computers and file servers
  - Clients could not access their data or software solutions

Attacks – Health Care Industry

Virtual Care Provider Inc. (VCPI)

- Demanded a ransom of $14 million
- VCPI CEO and Owner noted the attack impacted
  - Virtually all their core offerings
  - Internet services
  - Email
  - Access to patient records
  - Client billings
  - Phone systems
  - VCPI’s payroll operations

Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks – Health Care Industry

Virtual Care Provider Inc. (VCPI)

- VCPI – cannot afford the ransom
- Highest priority – getting clients up and running
- VCPI employees – wondering when they were going to get paid
- VCPI implemented an offsite / offline backup solution 6 months before the attack

Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Attacks – Health Care Industry

Memorial Health System

- Cyberattack, suspected ransomware
- Forced to shut down IT systems
- Switched to paper charts
- Forced to divert emergency care patients
  - All urgent surgical appointments and radiology examinations canceled the day after the attack

Attacks – Health Care Industry

Memorial Health System

- Was unsure as of August 17, if data was stolen
- Investigation ongoing
- Beeping Computer reported
  - Hive ransomware threat group responsible
  - Known for stealing data
  - Evidence obtained a database containing PHI stolen
    - 200,000 patients
    - Names, dates of birth, social security numbers

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Controls

Controls

- Back to basics
  - Identify assets
    - Classify and prioritize
  - Effective patch management
  - Next gen anti-virus
  - Next gen firewalls
  - Education programs
  - Encryption

Controls

Controls

- Back to basics
  - Incident response program
  - Backup solutions
    - Ensure there is an offline component
  - Disaster Recovery/ Business Continuity Planning
    - Remember to consider cybersecurity
  - Intrusion detection systems
  - Intrusion prevention systems

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Controls

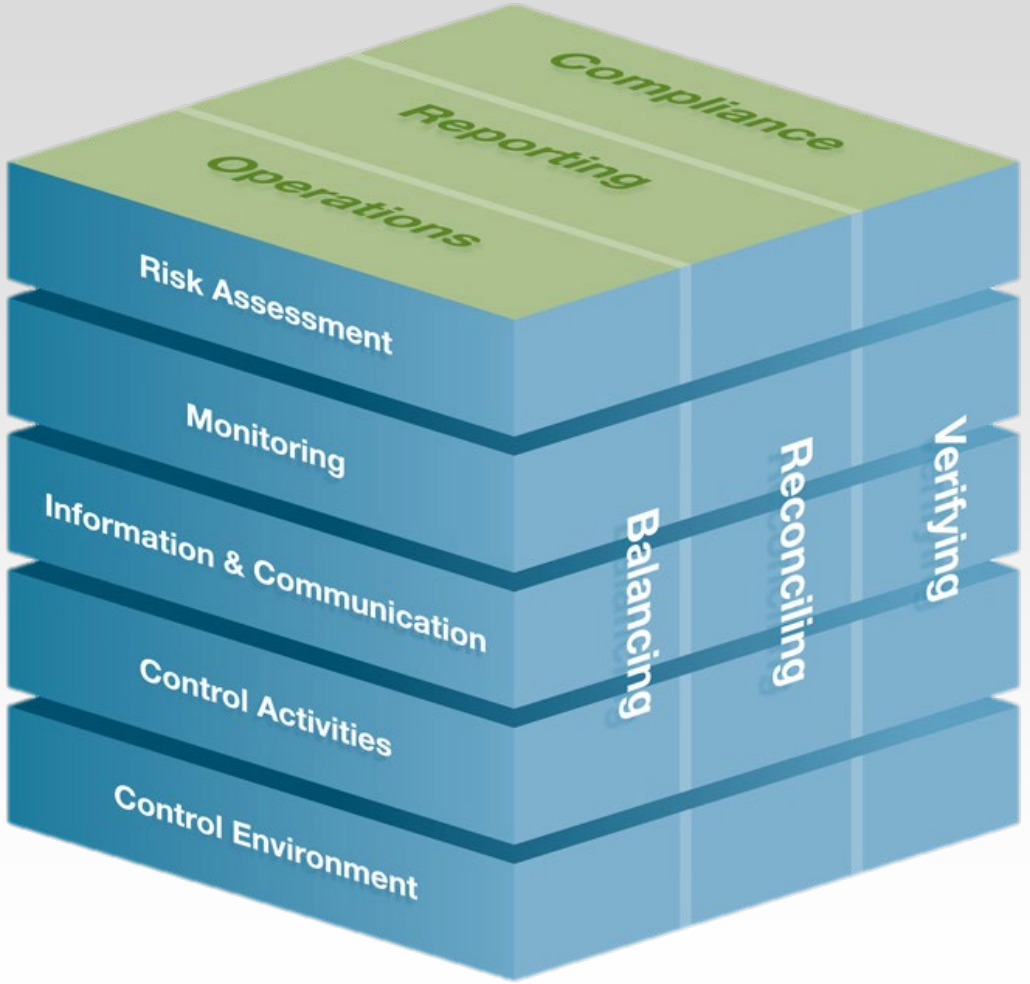
Controls

- Back to basics
  - Consider cyber with all new products/services
    - Part of the evaluation process
    - Do not forget about DR/BCP
  - Educate all users
    - How?
  - Vendor management program
  - Multi-factor authentication

Controls

Controls

- Independent security testing
  - Vulnerability assessment
  - Penetration test
  - Social engineering
  - IT audits
- System and Organization Controls (SOC)



Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Conclusion

Cyberattacks have expanded to the core infrastructure

The Health Care Industry continues to be a prime target of the Bad Actors AND is part or the core infrastructure

Ransomware is increasing at an alarming rate and can lock down an Organization

Certain controls need to be followed including offsite / offline backups

EDUCATE, EDUCATE, EDUCATE

Information security/cybersecurity plan must evolve and change to address the new risks

Questions

Thank You for Joining Us

Name	Email Address	Phone Number
Chris Joseph	chris.joseph@actcpas.com	304.346.0441

Arnett Carbis Toothman llp
CPAs & Advisors