Anatomy of a Breach

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Arnett Carbis Toothman llp
CPAs & Advisors

April 13, 2021

Anatomy of a Breach

Everyone’s Responsibility

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

- **Current Information Security (IS) Environment**
  - Current state of affairs
  - Statistics including health care industry
  - Cyber events
  - Cybersecurity
  - COVID-19 impact
- **Risks & Controls**
- **Information Security Impact**
- **Case Study**

Current State of Affairs

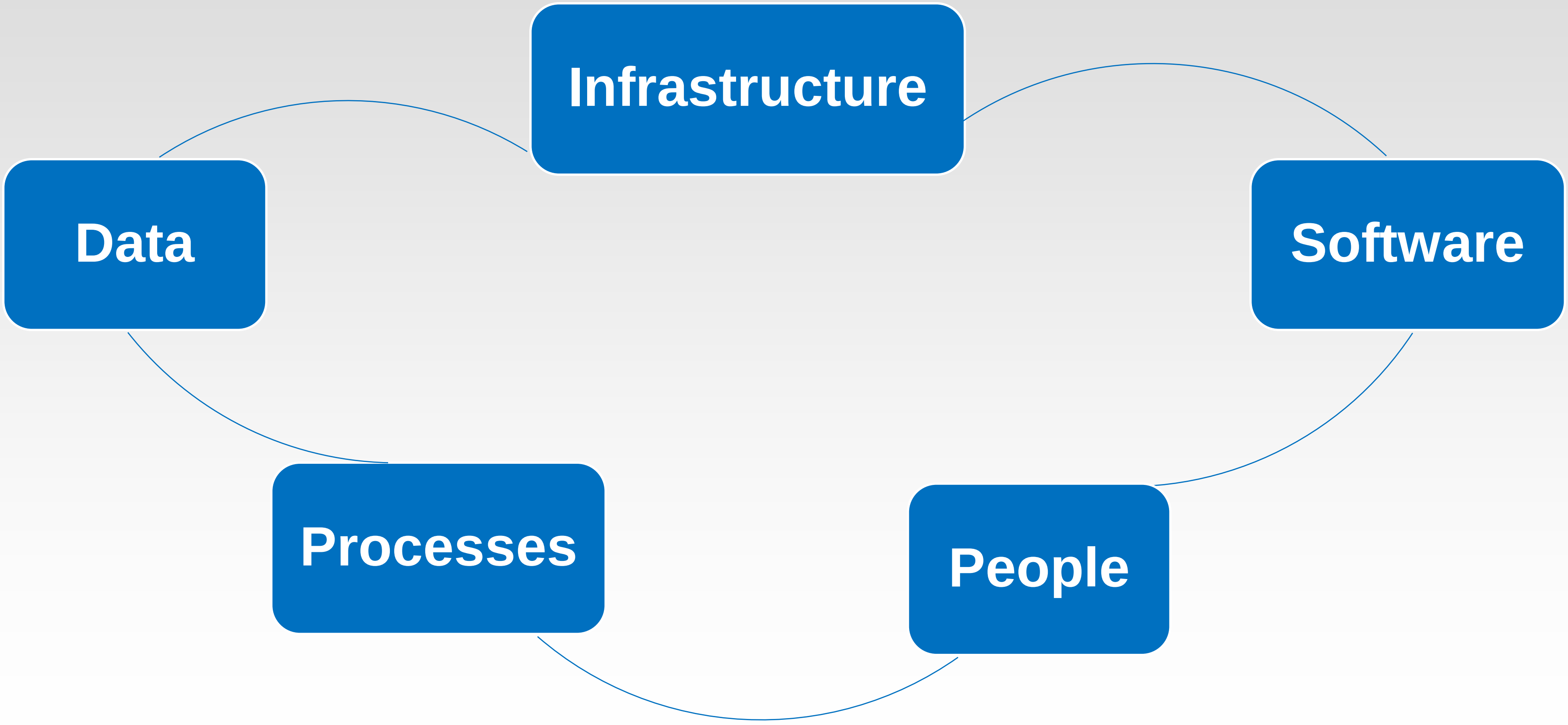
Crazy Times!!!

Cyber Events

- Increasing
- Alarming (but not surprising) rate

Current State of Affairs

System Components



Infrastructure

Software

People

Processes

Data

Current State of Affairs

Which System Component is the Weakest Link?

1. Infrastructure
2. Software
3. People
4. Procedures
5. Data

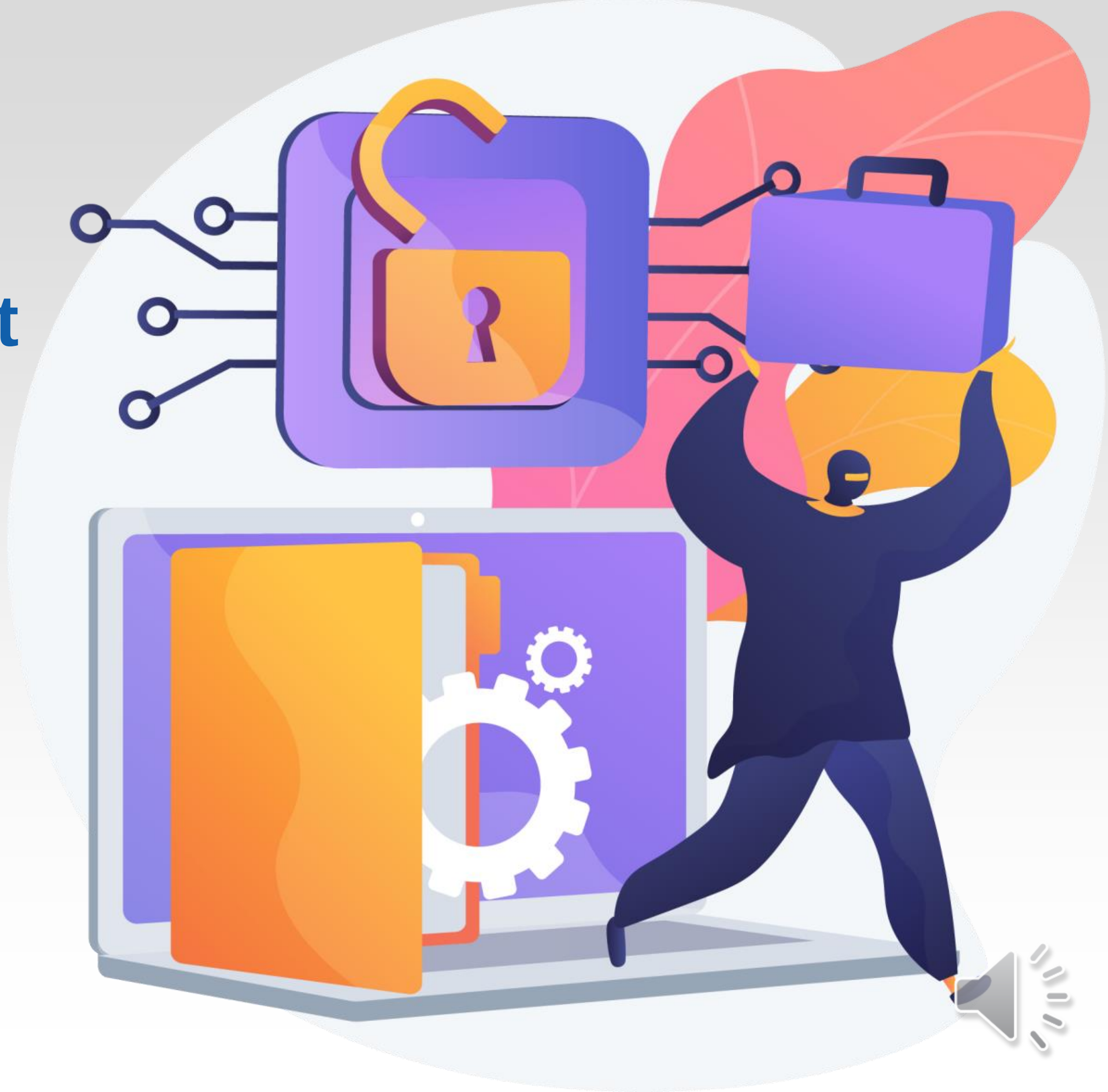
Current State of Affairs

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

Current State of Affairs

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

Current State of Affairs

Most Common Threats

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

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Current State of Affairs

Most Common Threats

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

Statistics

Who are the Threat Actors in Healthcare?

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

Statistics

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

Statistics

LeadingAge Whitepaper (2018)

- Second year in a row
  - Criminal attacks leading cause of data breaches
- In the past 24 months, 89% of health care organizations
  - At least one data breach of loss or theft of patient data
  - 45% - more than five breaches
- Average number of days to detect the breach
  - 201 days

Statistics

LeadingAge Whitepaper (2018)

- Cost of a breach
  - Notification
  - Forensics
  - Legal fees
  - Fines
- Amount?

Statistics

Department of Health and Human Services

- HIPAA Breach Reporting Website (July 9, 2020)
  - 2020 to-date
    - Added 250 breaches affecting 5.4 million individuals
    - 10 largest breaches
      - Impacted 2.8 million individuals
      - 52% individuals (2020 to-date)
  - Since tracking in 2009
    - Breaches impacting 500 or more individuals

Statistics

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 healthcare data breaches of 500 or more records
    - 268,189,693 healthcare records

Statistics

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

Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Statistics

Are We At War?

Answer: Yes

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Statistics

We are Not in Kansas Anymore!!!

What is a Cyber Event?

Cyber Event

Cyber Event Defined:

Any occurrence in an information system or network that has or may potentially result in:

- Unauthorized access, processing, corruption, modification, transfer or disclosure of data and/or confidential information

OR

- Disclosure of data and/or confidential information or a violation of an explicit or implemented company security policy

Cyberattack

Anatomy of a Cyberattack

- Information Gathering
- Intrusion and Infiltration
- Malware Deployment
- Data Extraction
- Cleanup

Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Top Ten Threats

Top Ten Threats:

1. Phishing Attacks
2. Negligent Insiders
3. Malicious Insiders
4. Advanced Persistent Threats
5. Cyberattacks

Cybersecurity White Paper: LeadingAge

Top Ten Threats

Top Ten Threats (cont.)

6. Zero Day Attacks
7. Known Software Vulnerabilities
8. Social Engineering
9. Denial of Service Attacks
10. Brute Force Attacks

Cybersecurity White Paper: LeadingAge

What is Cybersecurity?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Cybersecurity

What is Cybersecurity

- Part of information security
- Protect information from malicious threats
  - Confidentiality
  - Integrity
  - Availability

Cybersecurity

What is Cybersecurity

- Confidentiality
  - Sensitive information
  - Limit access to authorized personnel, vendors, etc.
  - Example threats
    - Stolen or lost laptops
    - User accounts hacked
    - Unencrypted transmissions
    - Social engineering

Cybersecurity

What is Cybersecurity

- Integrity
  - Authentic
  - Accurate
  - No unauthorized alteration
  - Example threats
    - Intentional modification
    - Accidental modification

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Cybersecurity

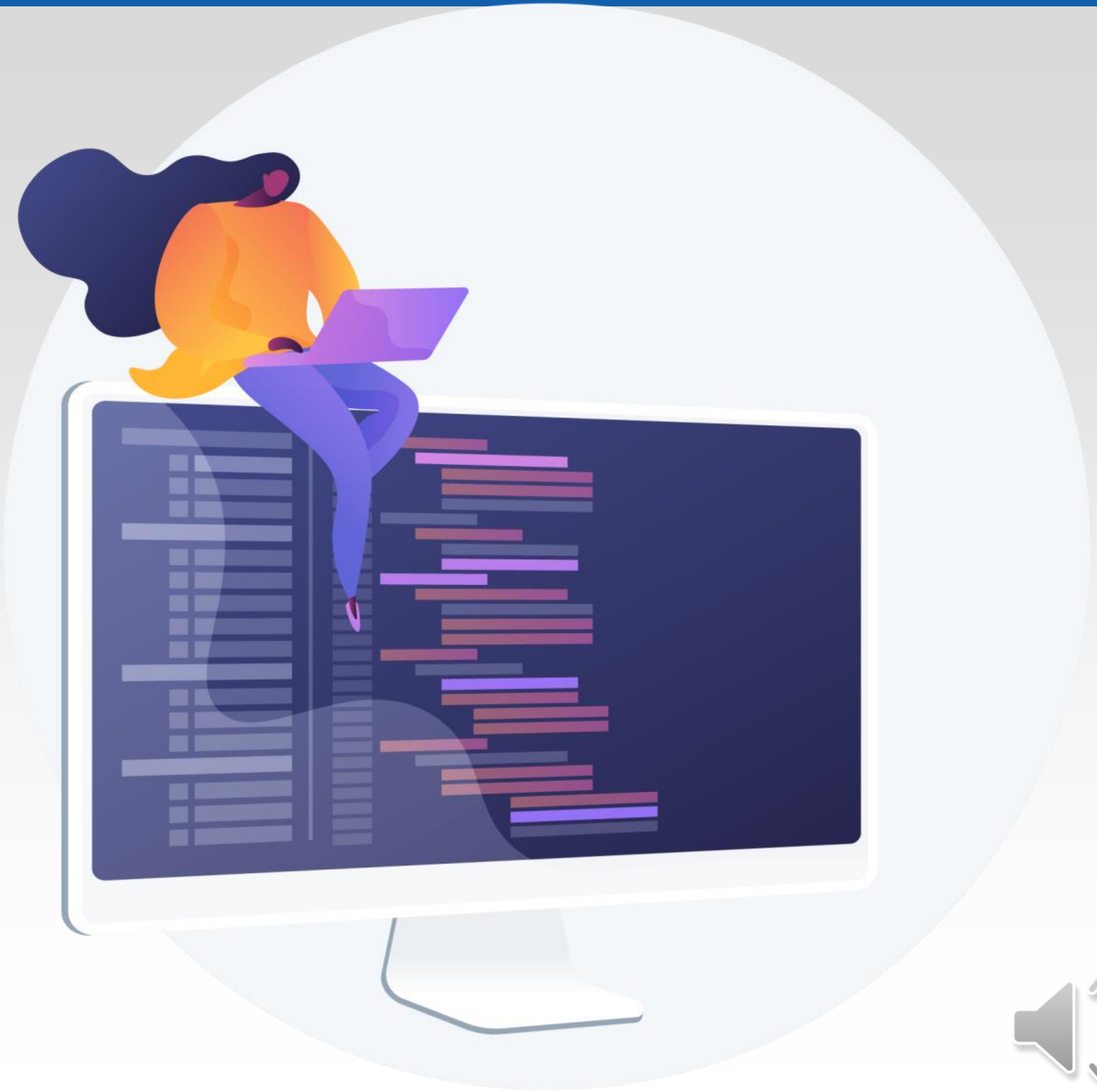
What is Cybersecurity

- Availability
  - Information accessible
  - Authorized users
  - Example threats
    - Downed servers
    - Natural disasters
    - Internet access interruptions
    - Cloud access
    - Network access interruptions

Cybersecurity

What is Cybersecurity

- Other threats
  - Confidentiality
    - Stealing personal or health information
    - Employee acts (downloading and selling information)
    - Inappropriate employee access
    - Losing an unencrypted flash/ thumb drive



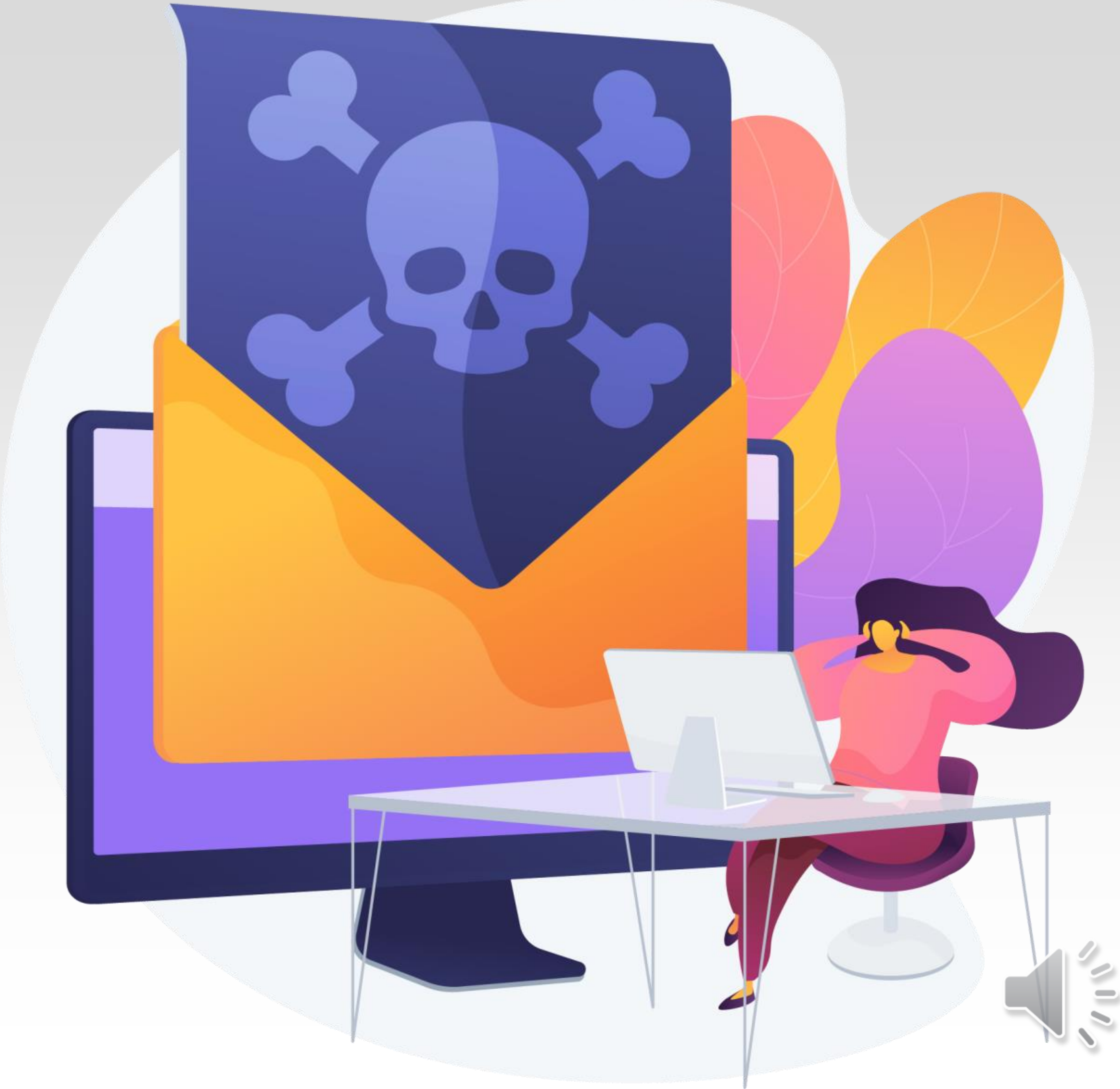
PACAH

Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Cybersecurity

What is Cybersecurity

- Other threats
  - Integrity
    - Modifying information
    - Creating information (unauthorized)
    - Deleting information



Cybersecurity

What is Cybersecurity

- Other threats
  - Availability
    - Ransomware
    - Denial of service
    - Server failure
      - Organization level
      - Vendor or service provider

How Are We Working?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

COVID-19 Impact

Increase in Working Remotely

- Primarily from home
- What are the potential issues?

COVID-19 Impact

Dynamic Workforce (more statistics)

- All from RSA Security LLC – per Dell survey
- 45% admitted to one of the following
  - Used public Wi-Fi for business
  - Shared confidential data – personal email
  - Lose devices (laptops, phones)
    - Containing company information

COVID-19 Impact

Dynamic Workforce (more statistics)

- All from RSA Security LLC – per Dell survey
- 1 in 4 engage in risky behavior
  - To get the job done
  - Many unaware of the risky behavior
  - Examples?
  - What can you do?

COVID-19 Impact

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?

COVID-19 Impact

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

COVID-19 Impact

Types of Ransomware

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

Pennsylvania Coalition of Affiliated Healthcare & Living Communities

COVID-19 Impact

Types of Ransomware

- Encrypting ransomware
  - Nasty stuff
  - Obtains the files and encrypts them
  - Demands payment to decrypt
- Should you pay?

FBI Does NOT Recommend Paying

Why Not?

COVID-19 Impact

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?

COVID-19 Impact

Significant Ransomware Increase

- 900% increase
- Why?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

COVID-19 Impact

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?**

Risks & Controls

Recap of Risks

- Primarily the organization’s data
- Very valuable to fraudsters
- High risk
  - Financial
  - Legal
  - Reputation

Risks & Controls

Controls

- Back to basics
  - Effective patch management
  - Next gen anti-virus
  - Next gen firewalls
  - Education programs
    - BOD
    - Senior Management
    - Employees
  - Encryption

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Risks & Controls

Controls

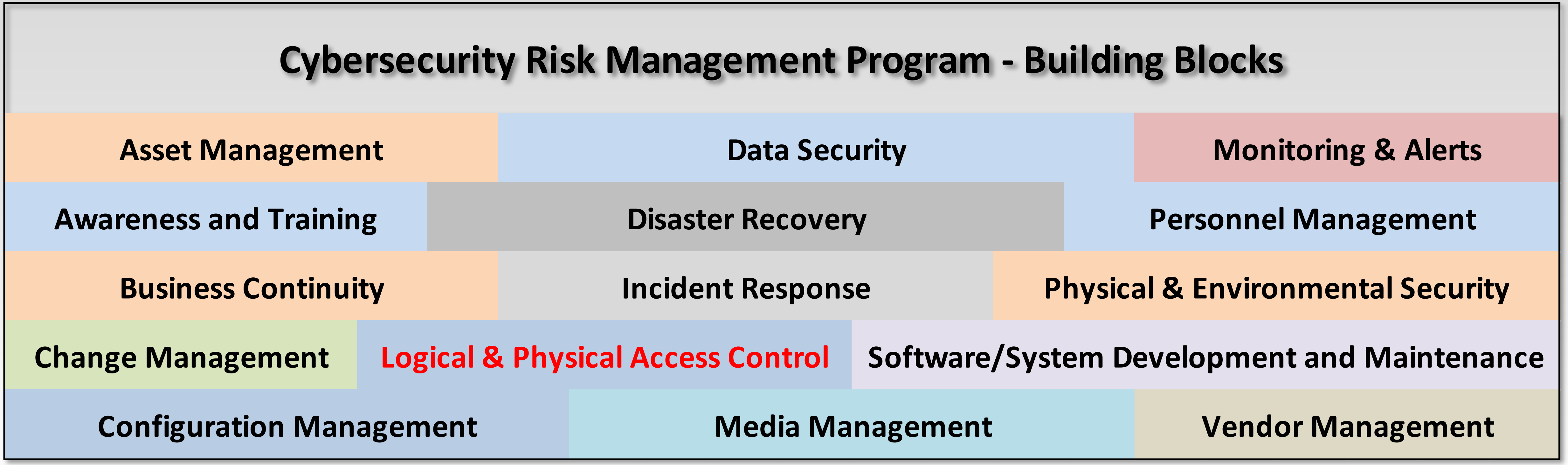
- Back to basics
  - Incident response program
  - Backup solutions
    - Ensure there is an offline component
  - Disaster Recovery/ Business Continuity Planning
    - Remember to consider cybersecurity
  - Intrusion detection systems
  - Intrusion prevention systems

Risks & 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

Risks & Controls



Cybersecurity Risk Management Program - Building Blocks

Asset Management | Data Security | Monitoring & Alerts

Awareness and Training | Disaster Recovery | Personnel Management

Business Continuity | Incident Response | Physical & Environmental Security

Change Management | Logical & Physical Access Control | Software/System Development and Maintenance

Configuration Management | Media Management | Vendor Management

Risks & Controls

Controls

- Independent security testing
  - Vulnerability assessment
  - Penetration test
  - Social engineering
  - IT audits
- **S**ystem and **O**rganization **C**ontrols (**SOC**)

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Case Study

First Case

- Based on an actual event
- A hospital updated their IT systems
  - Core provider solution
  - IT infrastructure
  - Most workstations
- New network support vendor
- Challenges with full data conversion

Case Study

First Case

- Kept prior system for history
  - Legacy system
  - No longer receiving regular updates
  - Limited access to legacy system
    - Personnel who required access
    - Trusted vendors upon approval
  - Legacy system not compatible
    - Network O/S after Windows 2008
    - Workstation O/S after Windows 7

Case Study

First Case

- Organization considered legacy system as decommissioned
- Decommissioned systems
  - Not considered a priority
  - Not included in security risk management programs
- No cybersecurity monitoring services
- Good backup / recovery system

Case Study

First Case - Issue

- Was hit with ransomware in April
  - Launched ransomware 1 week after gaining access
- Prevented the organization from accessing records in the legacy system
  - Proprietary software used to view the files was infected
- Could not access records the last five years of the legacy system
- No evidence files were exported or viewed
  - i.e. no unauthorized access known
- Some electronic records not available

Case Study

First Case - Issue

1. What was wrong with controls of the organization?
2. What control in place could work in the organization’s favor during recovery?
3. What was a big risk between the security incident and the recovery of the files?
4. What is another potential risk for the organization?

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Case Study

Second Case

- Based on an actual event
- Maryland-based nursing home
- Lorien Health Services
- Victim to a ransomware attack
  - Occurred on June 6
- 47,754 resident personal information exposed

Case Study

Second Case

- Hired a team of security experts
  - Determined the bad actors also breached PII
    - Social security numbers
    - Dates of birth
    - Addresses
    - Treatments and health diagnosis

Case Study

Second Case

- Attributed to the Netwalker ransomware gang
  - Lorien refused to pay the ransom
  - Exfiltrated information
  - 147 MB password-protected archive
    - Available for download
    - More than likely, represents only a small batch of the data

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Case Study

Second Case

- Lorien reported to the FBI
- Notified potentially impacted residents – June 16
- Offering complimentary credit monitoring and identity protection

Case Study

Second Case

1. What potential impact could the Lorien Health Services breach have on its victims?
2. Should Lorien pay the ransom?
3. In addition, to current steps being taken, what else should Lorien Health Services consider doing?

Case Study

Third Case

- Actual event
- 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

Case Study

Third Case

- 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

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Case Study

Third Case

- 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

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Case Study

Third Case

- 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

PACAH
Pennsylvania Coalition of Affiliated Healthcare & Living Communities

Case Study

Third Case

1. What are some of the risks that VCPI clients faced?
2. What control assisted VCPI to mitigate the impact?
3. What else should organizations consider implementing as it relates to user authentication to access systems?

Conclusion

Health Care industry is a prime target for cyber attacks, specifically in long-term care

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

Certain basic controls need to be followed including offsite / offline backups

Employees need to be aware of the risks: EDUCATE, EDUCATE, EDUCATE

Information security/cybersecurity plan must be an active live program

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