Post COVID-19: What's next for information security

Pennsylvania Coalition of Affiliated Healthcare & Living Communities

April 20, 2022

bakertilly
now, for tomorrow

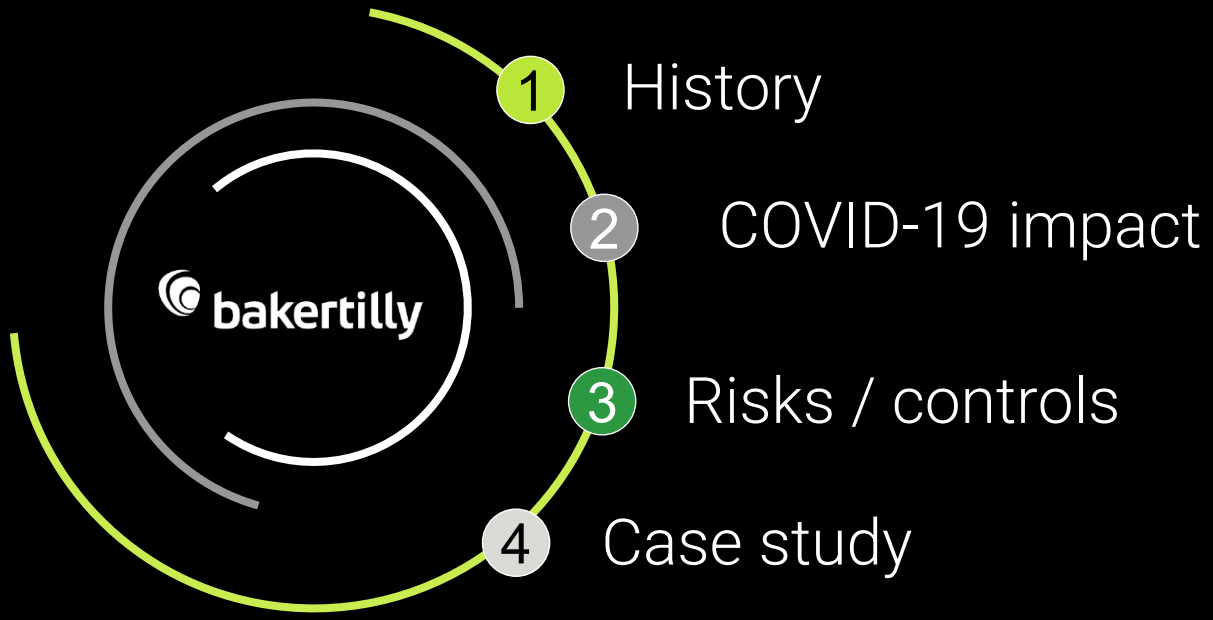
Presenter

Chris Joseph, CPA, CISA, CRISC, CITP

Director, Baker Tilly

- IT auditing
- IT security
- Risk assessment
- Certified Public Accountant
- Certified Information Systems Auditor
- Certified in Risk and Information Systems Control
- Certified Information Technology Professional

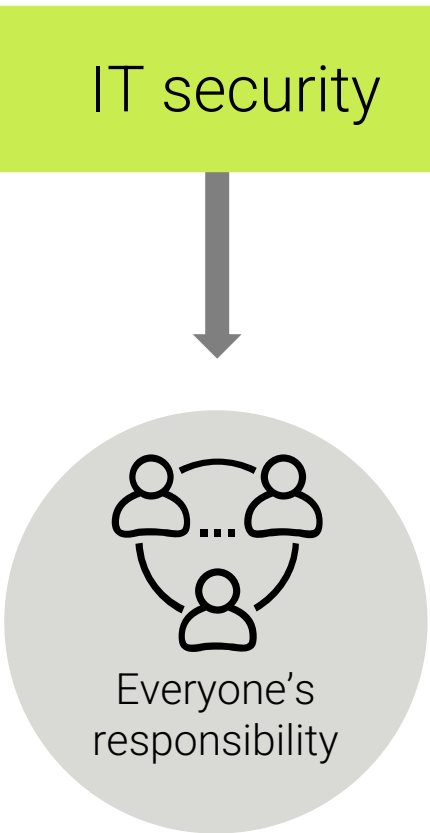
Objectives


bakertilly
1
History
2
COVID-19 impact
3
Risks / controls
4
Case study

HISTORY

Who’s responsible

IT security



HISTORY

Pre COVID-19 work model

Various studies

- Most worked in the office
- Trend
  - Increasing number working remotely

HISTORY

Pre COVID-19 work model

Various studies

- Gallup survey released February 2017
  - 2016 – 43% spend some time working remotely
    - 4% increase from 2012
  - Working remotely more often (four to five days)
    - Increased from 24% to 31% (from 2012 to 2016)
  - A day or less
    - Decreased from 34% to 25% (from 2012 to 2016)

HISTORY

Pre COVID-19 work model

Why the increase?

Rise in freelance workers

50% of millennials were freelancers
(Forbes, October 2017; survey released by Freelancers Union)

HISTORY

Pre COVID-19 work model

Why the increase?

Larger employee pool
- Less geographical restrictions

Desired less commuting

Technology
- Increased reliance
- Increased capabilities

HISTORY

Pre COVID-19 work model

We are not in Kansas anymore!

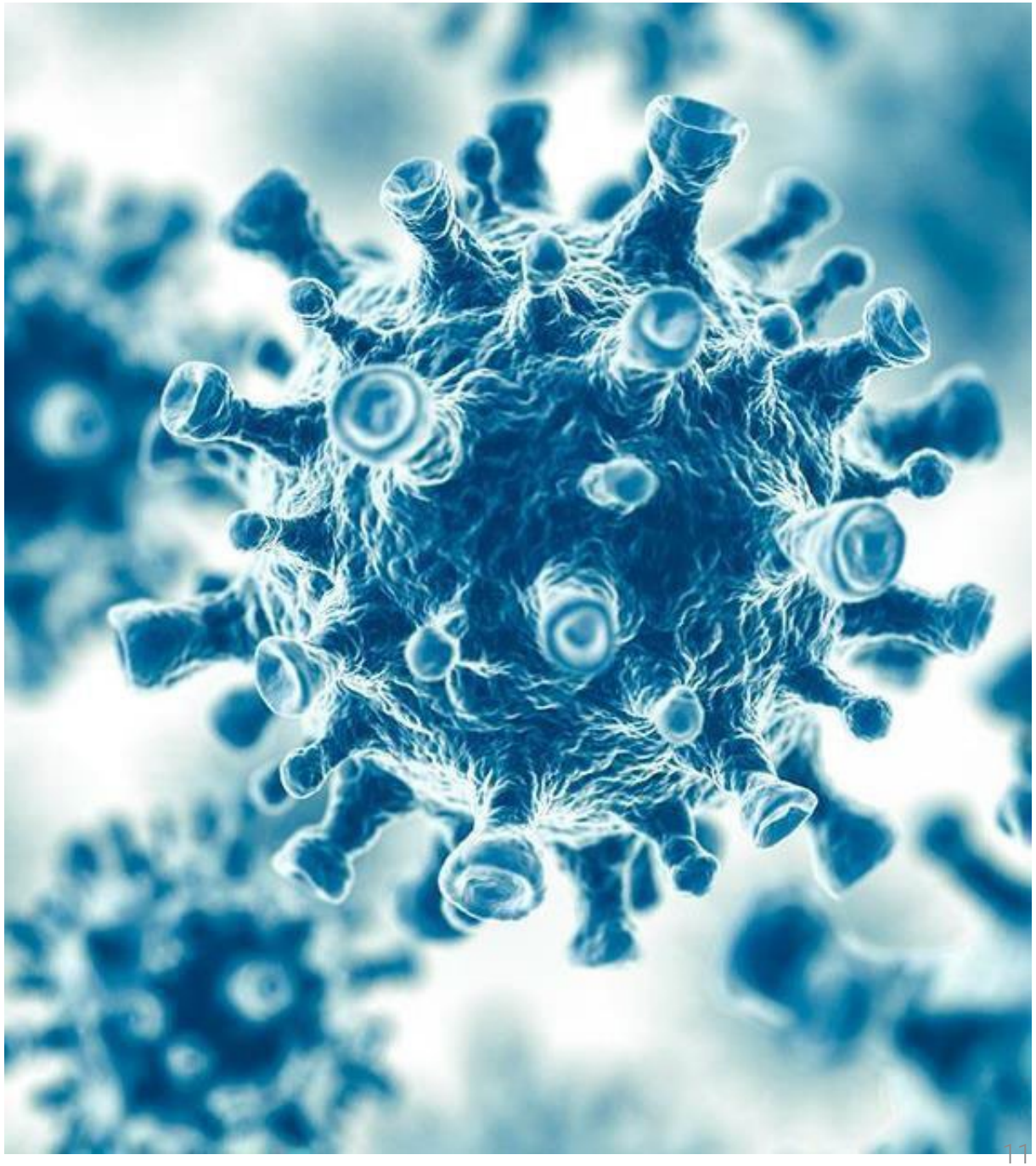
COVID-19 impact:
What did COVID-19 really do?

bakertilly
now, for tomorrow

COVID-19 IMPACT

Working remotely

- Became a necessity, not an option for most
- What were the organization’s choices?



COVID-19 IMPACT

Statistics (initially)

43% of small businesses shut down

(Bartik et al. 2020a)

45% of small businesses had employees working from home at least two days a week

(National Association for Business Economics (NABE)

Suggests?

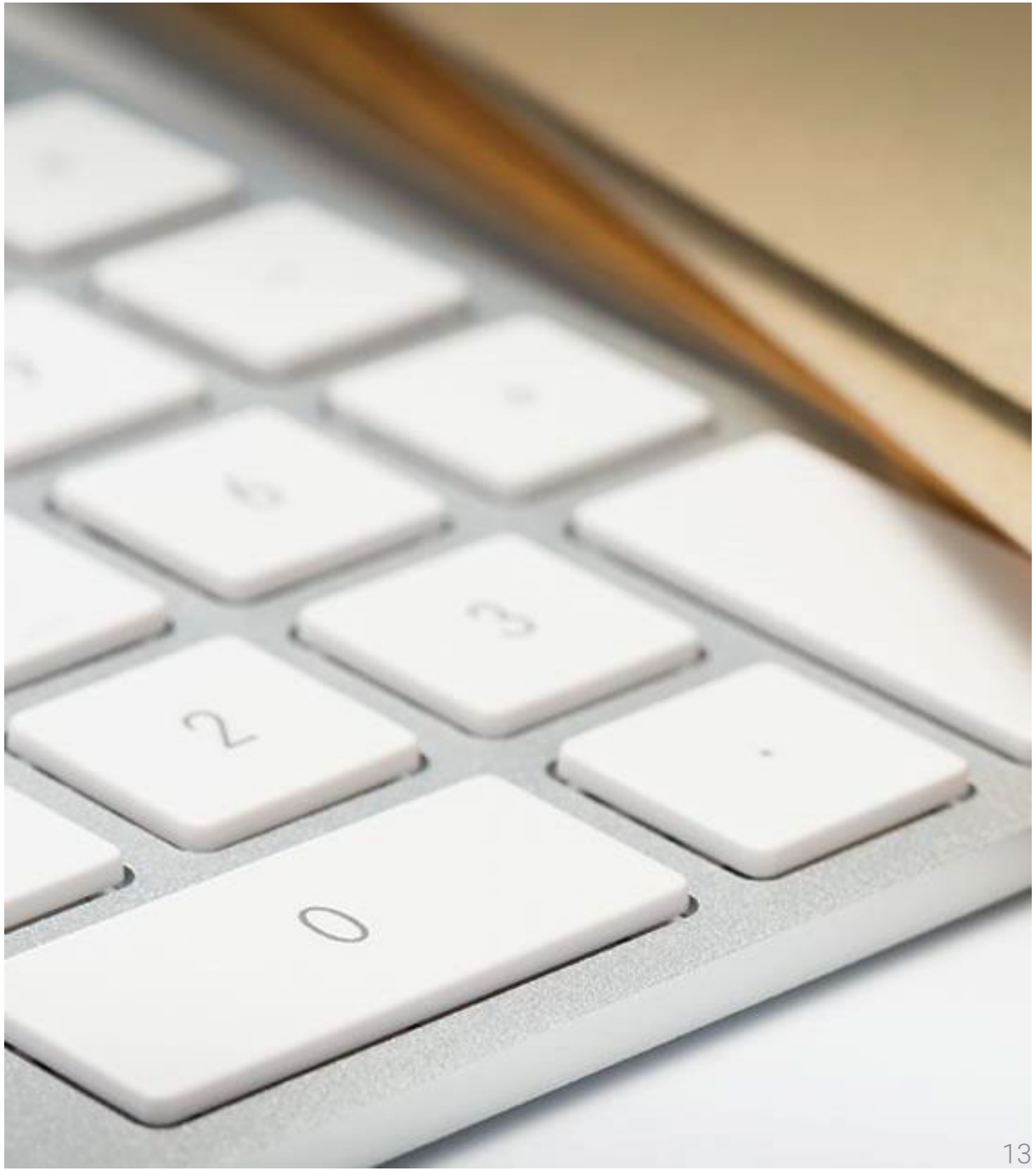
From an article titled “How the COVID-19 Crisis is Reshaping Remote Working,” authored by Alex Bartik, Zoe Culen, Edward Glaeser, Michael Luca, Christopher Stanton – July 19, 2020

COVID-19 IMPACT

Benefits of working remotely

Employer and employee

- Reduce the chance of spreading the virus
  - Throughout the organization
- Expand the geographic footprint for potential employees



COVID-19 IMPACT

Benefits of working remotely

Employer

- Hiring talent
- Staying competitive
  - Gallup – 35% would change jobs for full-time working remotely
- Possibly saving business costs
- Lower real estate
- Productivity
- Increased engagement
- Talent retention
- Profitability

COVID-19 IMPACT

Benefits of working remotely

Employee

- Increased flexibility and autonomy
- Better work-life balance
- Eliminating the long commute
- More freedom (flexibility)
- Productivity(?)
- Reduced stress
- Better health
- More time to exercise
- Less interruptions from co-workers

Risks/Controls

What is one of the biggest reasons for increased risks?

What happened to your organization’s footprint?

Risks/Controls

Large increase in the attack service area

- Multiple new access points for the bad actors
  - In what way?

What additional risks does that introduce?

RISKS / CONTROLS

Perimeter security - firewalls

Risks

Controls

Risks

- Lack of firewalls
- Outdated
- Not updated

RISKS / CONTROLS

Perimeter security - firewalls

Risks

Controls

Controls

- Obtain and/or update firewalls
- Keep the firmware updated
- Enhance configuration at the organization

RISKS / CONTROLS

Perimeter security - routers

Risks

Controls

Risks

- Lack of routers
- Cable modem only
- Outdated models

RISKS / CONTROLS

Perimeter security - routers

Risks

Controls

Controls

- Obtain and/or update routers
- Keep updated

RISKS / CONTROLS

Patch management - risks

Risks

Controls

Huge issue

- Unpatched systems
- Major cause of security breaches

Employee-owned devices

- Systems patched?
- Should these be allowed?
- Routers

RISKS / CONTROLS

Patch management - controls

Effective patch management solution

- Operating system
- Regular updates
- Critical, high and security risks
- Third party products
- Employee-owned devices

RISKS / CONTROLS

Physical security - risks

Risks

Controls

Home life vs. work life

- Access
- Accidental damage
- Children
- Pets
- Others
- Unattended computers

RISKS / CONTROLS

Physical security - controls

Risks

Controls

- Lock down unattended computers
- Physically secure computers
- Do not allow anyone else access to the computer
- Encryption
- What about printers?

Employee-owned devices

Is it a good idea?

RISKS / CONTROLS

Employee-owned devices - risks

Risks

Controls

Desktop/Laptops

- Outside users
- Used for more than work
  - Online gambling
  - Fantasy football
  - Shopping
  - Social media (Facebook, etc.)

RISKS / CONTROLS

Employee-owned devices - risks

Risks

Controls

Patch management, revisited

- Solution used
- Frequency
- Third-party applications
- Exception processing

RISKS / CONTROLS

Employee-owned devices - risks

Risks

Controls

Virus protection

- Solution utilized
- Frequency
- Zero-day attacks
- Exception processing
- Traditional AV solution only

RISKS / CONTROLS

Employee-owned devices - risks

Risks

Controls

Others

- Firewalls/Routers
- Printers

RISKS / CONTROLS

Employee-owned devices - controls

Risks

Controls

- Limit the use
- Require patch management
- Require antivirus
- Require a robust router or firewall
  - Cable modems are NOT enough

RISKS / CONTROLS

Employee-owned devices - controls

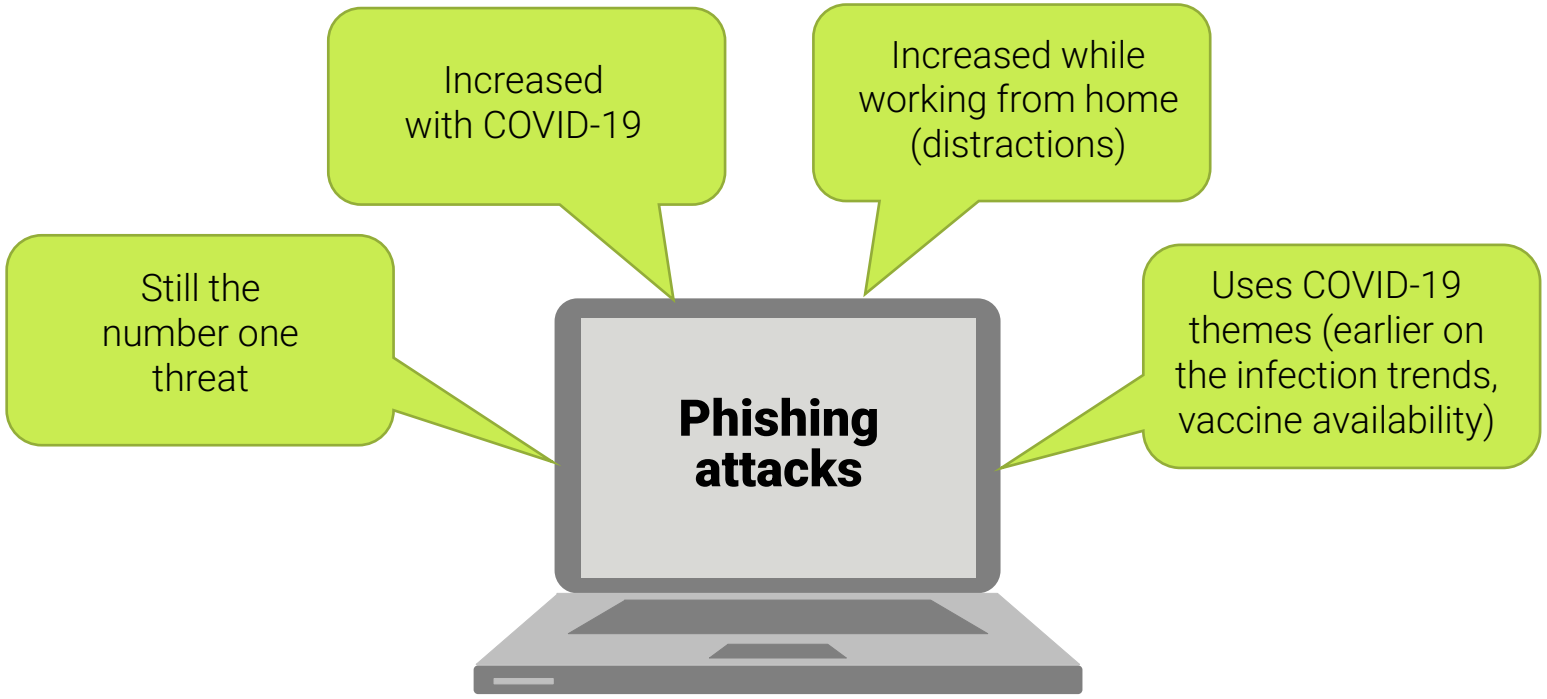
Risks

Controls

- Limit what others can do on the device
  - Is that going to be easy?
- Limit who has privilege access
  - Is that going to be easy?
- Properly shred printouts

RISKS / CONTROLS

Phishing attacks



RISKS / CONTROLS

Phishing attacks

Cybersecurity & Infrastructure Security Agency (CISA)

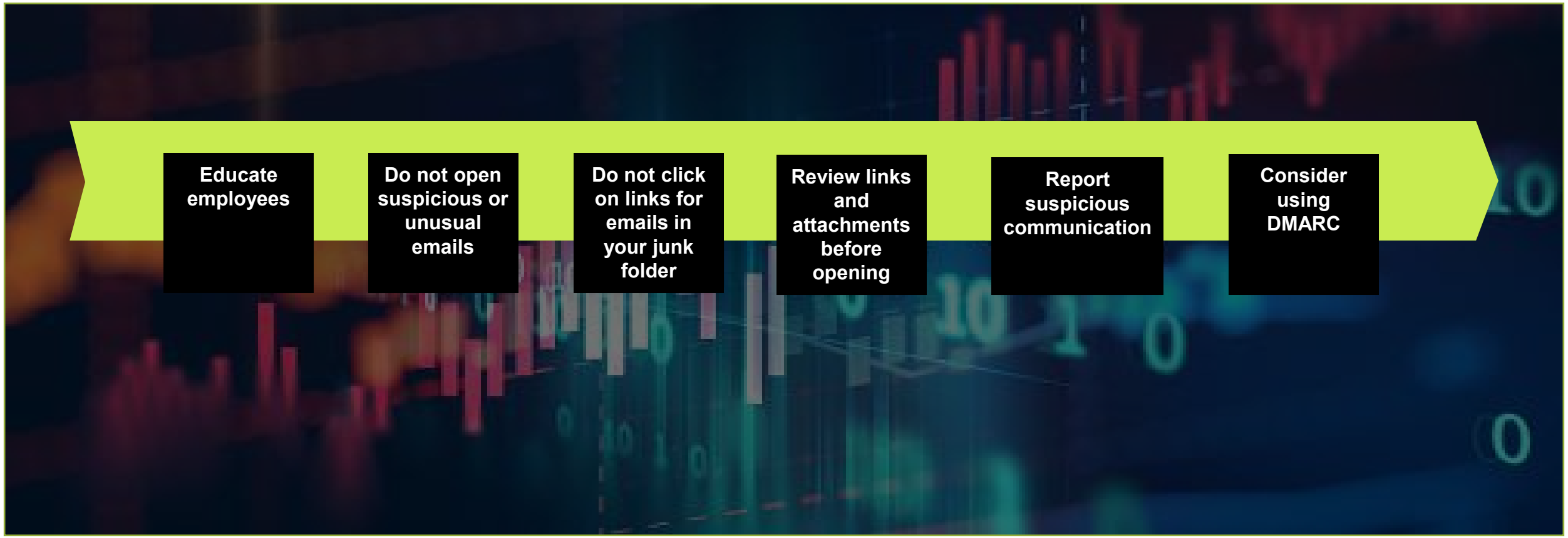
32% of breaches involve phishing attacks

78% of cyber-espionage incidents enabled by phishing

(Sept. 10, 2020)

RISKS / CONTROLS

Phishing attacks – what can you do?



RISKS / CONTROLS

Phishing attacks

What is DMARC?

Why should the health care industry consider DMARC?
(phishing, spear phishing)

Credential stuffing

bakertilly
now, for tomorrow

What is it?

RISKS / CONTROLS

Credential stuffing

- Not a breach on the target organization
- Previously leaked username-passwords
- Launched against other websites
  - Automated fashion

Risk/Controls

What can you do to combat credential stuffing?

RISKS / CONTROLS

Do not:

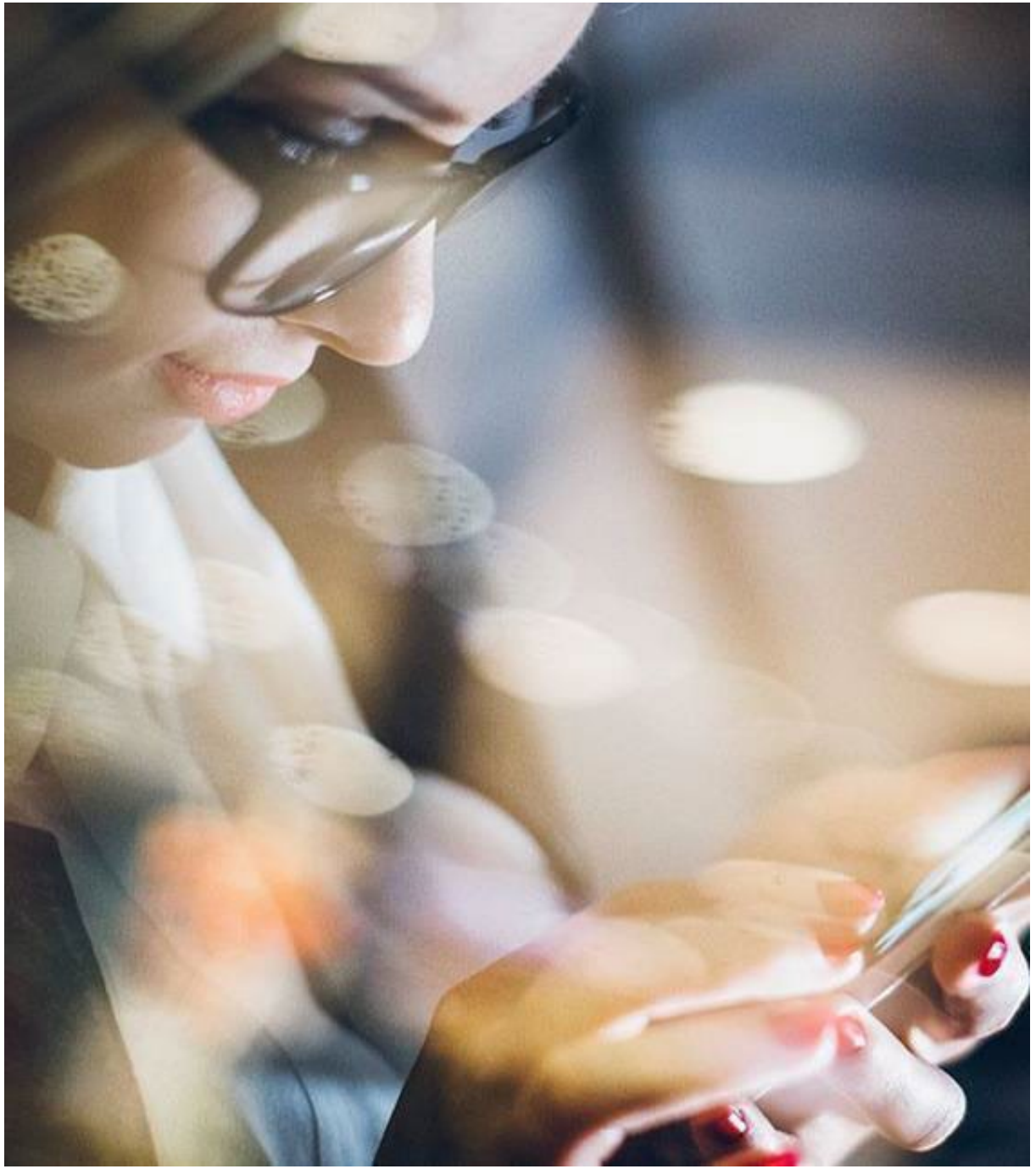
- Use the same username-password
- Across different websites/systems

How do you remember these usernames-passwords?

RISKS / CONTROLS

Use of public Wi-Fi

- For business
  - Not a good idea
  - Not secure
  - Bad actors
    - Obtain user code and passwords
    - Data at risk
    - Sensitive information at risk



RISKS / CONTROLS

Personal email account

- Using for business
- What are the risks?

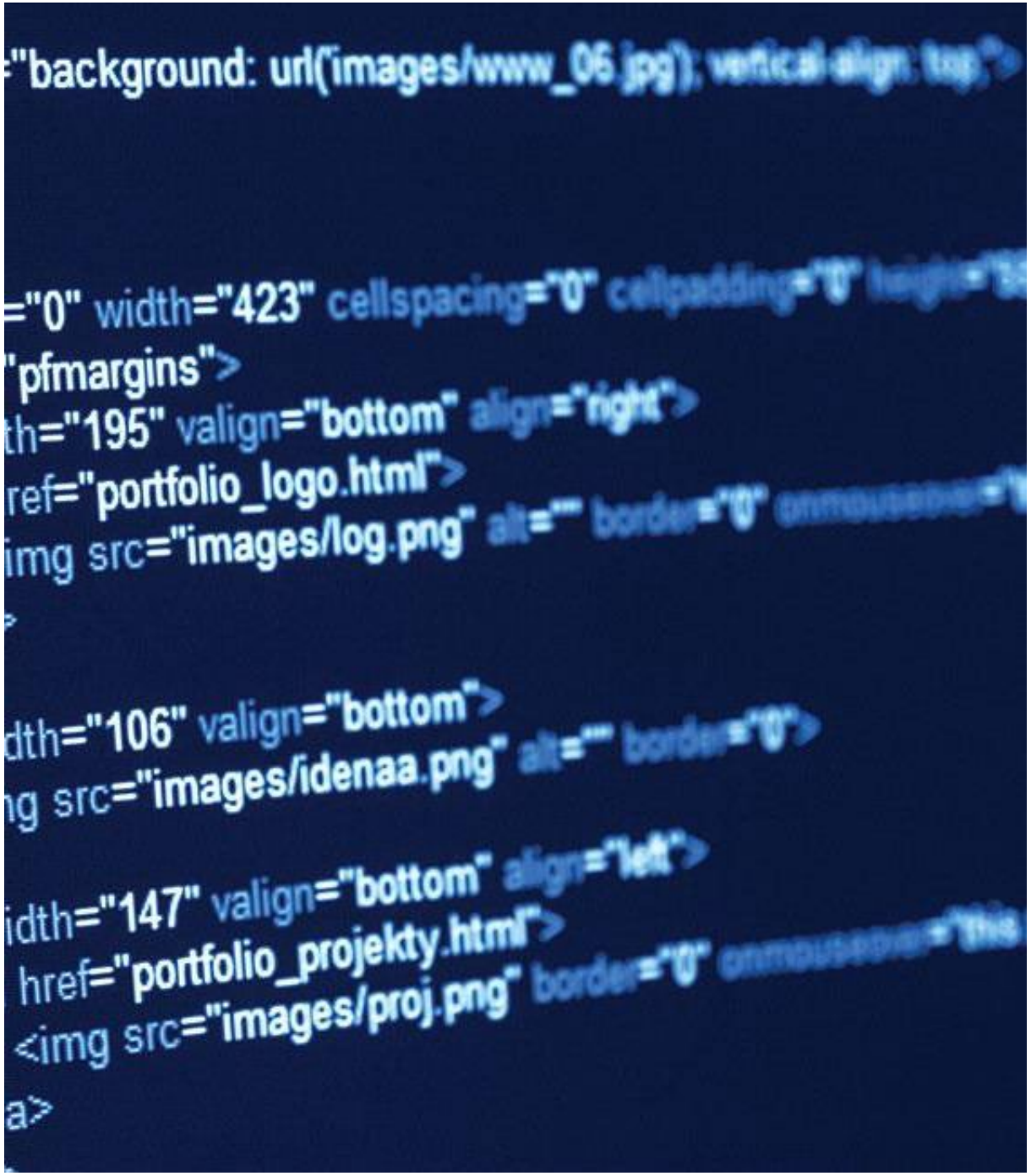
RISKS / CONTROLS

Personal email account

Risks

- Not using the organization's security infrastructure
- Privacy information at risk
- Confidential data at risk

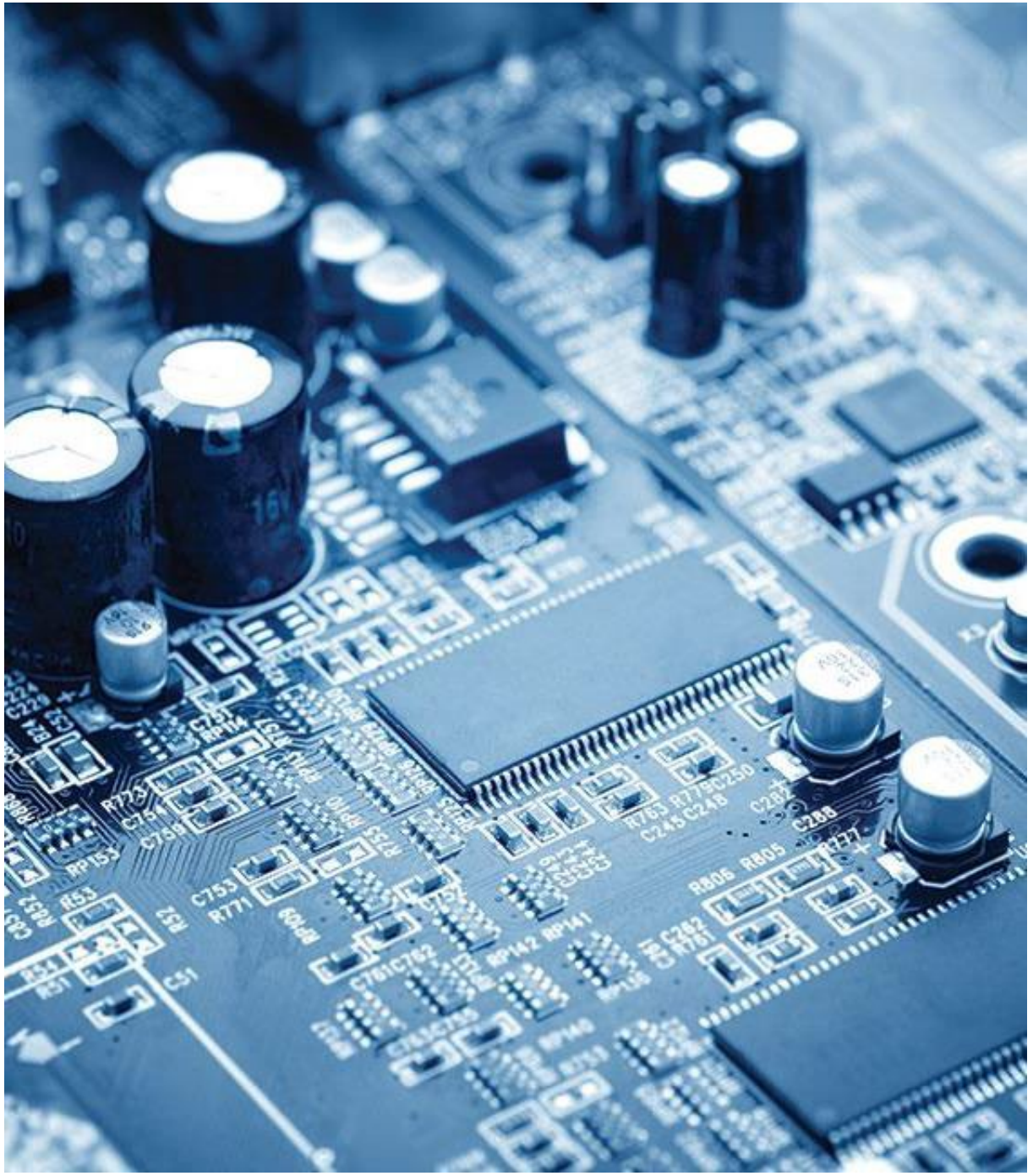
What can you do?



RISKS / CONTROLS

Ransomware

- Continues to rise
- Obtains files
- Encrypts them
- Demands payment to decrypt
- Should you pay?
- Double extortion?
- Triple extortion?



RISKS / CONTROLS

Ransomware

- Controls
  - Educate employees
  - Offline backup
    - Why offline
  - Patch management
  - Next gen antivirus
  - Next gen firewall
  - Vendor management
  - Multi-factor authentication
  - Segment networks
  - End to end encryption

RISKS / CONTROLS

Virtual meetings

Provide many benefits

Critical to remain in contact and stay connected

Security flaws discovered and addressed

Like whack-a-mole

RISKS / CONTROLS

Other controls

- Strong password practices
  - Long passwords
  - Different passwords for all accounts
  - Do not share passwords
  - Use password managers
  - DO NOT use default passwords

RISKS / CONTROLS

Other controls

- Multi-factor authentication
  - Bad actors are increasingly harvesting passwords
  - More difficult for a bad actor to gain access
  - Requires two of three
    - Something you know
    - Something you have
    - Something you are

RISKS / CONTROLS

Other controls

- Incident response policy and team
- Business continuity plan
- Vendor management program

CASE STUDY

An actual event

- Broward Health
- Impacted 1,357,879
- Occurred on Oct. 15, 2021
- Discovered on Oct. 19, 2021
- Reported on Jan. 4, 2022
  - Why the delay?

CASE STUDY

An actual event

- Gained access through
  - Third-party medical provider
- Included
  - Social security numbers
  - Phone numbers
  - Birth dates
  - Addresses
  - Email addresses

CASE STUDY

An actual event

- Medical information
  - Medical history
  - Conditions
  - Treatment
  - Diagnosis information
- Exfiltrated data

CASE STUDY

An actual event

- Notified FBI and DOJ
- Engaged cybersecurity firm
- Employee password reset
- Data review specialist
- Implemented multi-factor authentication

CASE STUDY

An actual event

- Minimum security
  - Devices not managed by Broward Health IT
- Employees and patients
  - Two years free identify theft protection
- Went into effect January 2022

An actual event

What did Broward Health do well during the security event?

An actual event

What could Broward Health have done to reduce the risk of the security event occurring?

CASE STUDY

An 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

CASE STUDY

An actual event

- November 17, 2019
  - Ransomware attack at 1:30 a.m.
  - Encrypted all data VCPI hosts
    - Serve 110 nursing homes (45 states)
    - 2,400 nursing homes
    - Approximately 80,000 computers
    - Clients could not access
      - Data
      - Software solutions

CASE STUDY

An actual event

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

CASE STUDY

An actual event

- VCPI could not afford the ransom
- Highest priority
  - Clients up and running
- VCPI employees
  - Wondering about getting paid
- What saved them?

CASE STUDY

An actual event

- VCPI discussed with Krebbs on Security
- Open with Krebbs provided he did a follow-up interview
  - Krebbs received an email from the bad actors
  - Indicated that the reduced ransomware demand still on the table
- What did that tell Krebbs?

An actual event

What did VCPI do well during the security event?

An actual event

What could VCPI have done to reduce the risk of the security event occurring?

Thank you!

Chris Joseph, CPA, CISA, CRISC, CITP

Director, Baker Tilly

- IT auditing
- IT security
- Risk assessment
- Certified Public Accountant
- Certified Information Systems Auditor
- Certified in Risk and Information Systems Control
- Certified Information Technology Professional

Disclosure

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.