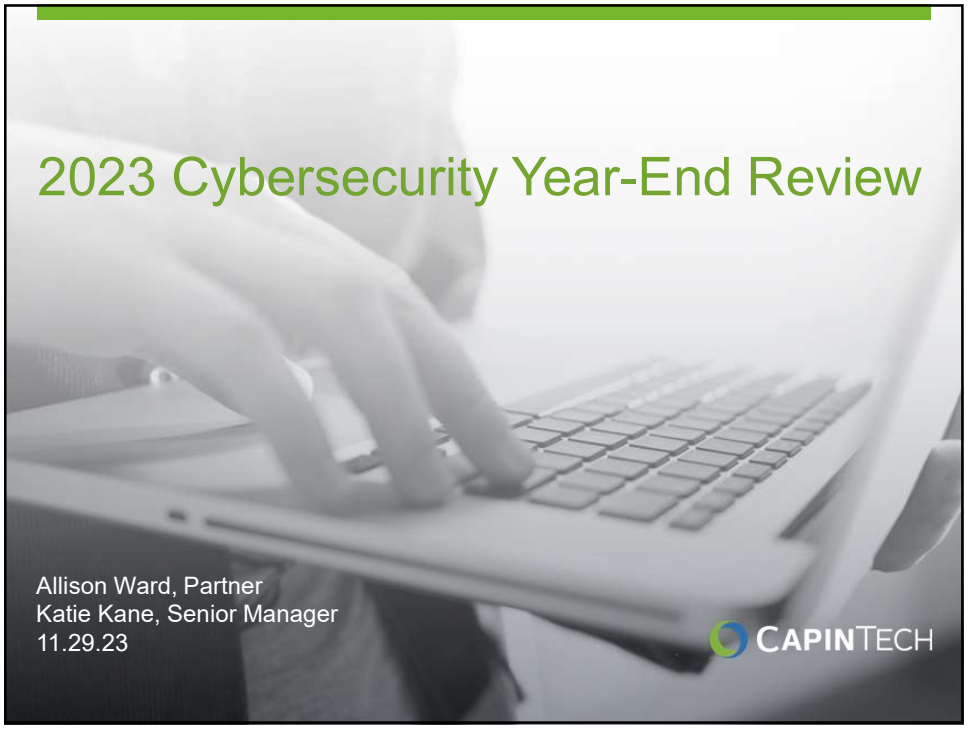
The webcast will start at 1:00 p.m. Eastern

- Visit capincrouse.com/2023-cyber to access these resources from today's webcast:
  - Handout
  - Recording
- To receive CPE credit, you must respond to the polling questions, which are not available on mobile devices. To receive CPE credit, you must log in on a computer.
- CPE certificates will be emailed to you within the next few weeks.



The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of Capin Crouse LLP, is provided solely for educational purposes. This presentation is not intended to provide legal, accounting, investment, or fiduciary advice. Please contact your attorney, accountant, or other professional advisor to discuss the application of this material to your particular facts and circumstances.

Polling Question 1

Do you want CPE credit?

- Yes
- No

The State of Cybersecurity

CAPINTECH

Here to Stay: Cyberattacks on Nonprofits

Ransomware gang steals 6.8TB of data from Save The Children

The charity has had financial, medical and health data stolen in the cyber attack

Cyber Security Hub, September 2023

Nonprofit ransomware task force finds 'steady' rise in ransomware attacks impacting education sector

Inside Cybersecurity, November 2023

Cybercrime groups find a new target: religious institutions

Two well-established hacking groups claimed attacks on religious organizations over the weekend, a foray into a new arena for gangs that typically focus their attention on corporations and government agencies.

The Record, May 2023

Hacking a Church Is About Exploiting Its Weakest Link

As generative AI improves communications, church hackers are refining their tactics.

Church Law & Tax, October 2023

Nearly a million dollars stolen from a North Carolina church

WFMY News 2, January 2023

BianLian ransomware gang holds Save the Children hostage

The dangerous and prolific BianLian ransomware gang claims to have stolen almost 7TB of data from NGO Save the Children, but thankfully the charity's vital work on the ground appears to be unaffected

ComputerWeekly.com, September 2023

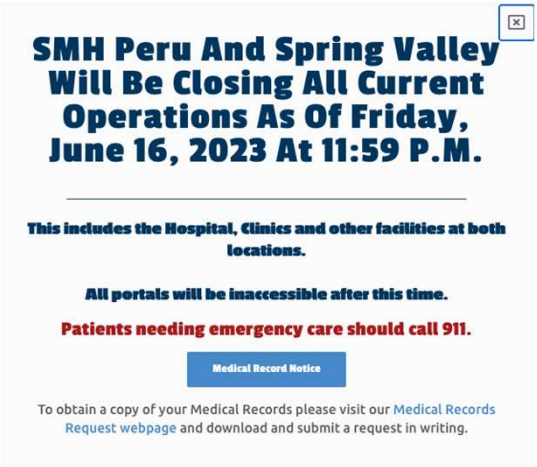
CommonSpirit Health Increases Ransomware Attack Cost Estimate to $160 Million

The HIPAA Journal, September 2023

Nonprofits and Cyberattacks: Key Stats That Boards Need to Know

BoardEffect, June 2023

Here to Stay: Ransomware + Long-Term Impacts



Source: aboutsmh.org

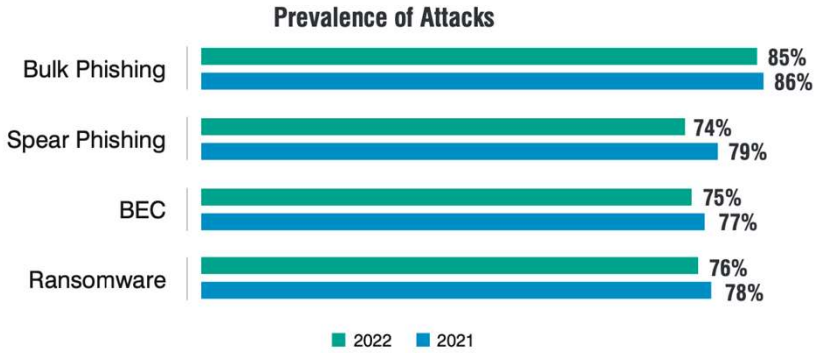
Here to Evolve: Encryption-Less Attacks

Here to Stay: Employee Involvement

74% of breaches involved a human element (n=4,482)

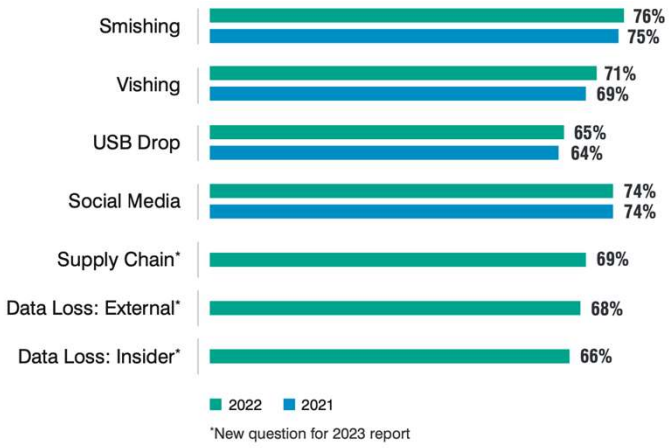
Source: Verizon Data Breach Investigations Report, 2023

Here to Stay: Social Engineering



Source: Proofpoint State of the Phish, 2023

Here to Evolve: Social Engineering Tactics



Source: Proofpoint State of the Phish, 2023

MGM Resorts September 2023

- Passwords likely included in database breach
- Same passwords reused across systems
- Information gathered from LinkedIn profile
- Social engineering attack launched on helpdesk

Here to Stay: You Have Many Assets

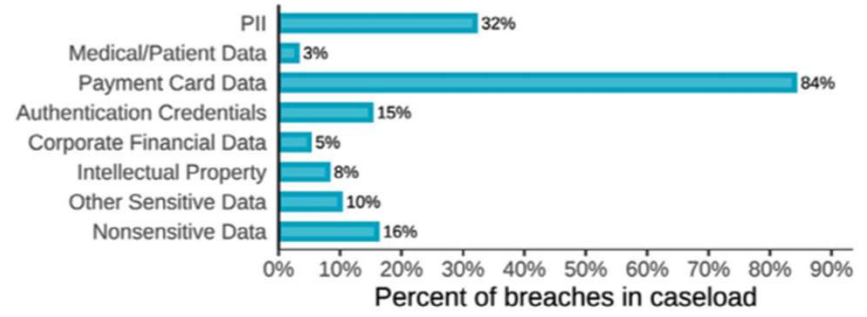


Figure 26. Compromised Data Types (2008 DBIR Figure 20)

Source: Verizon Data Breach Investigations Report, 2022

Here to Evolve: Passwords as an Asset

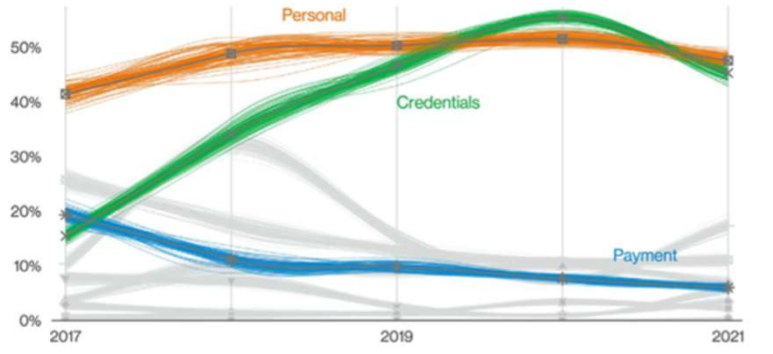


Figure 27. Top Confidentiality data varieties over time in breaches

Source: Verizon Data Breach Investigations Report, 2022

Here to Evolve: Passwords as an Asset

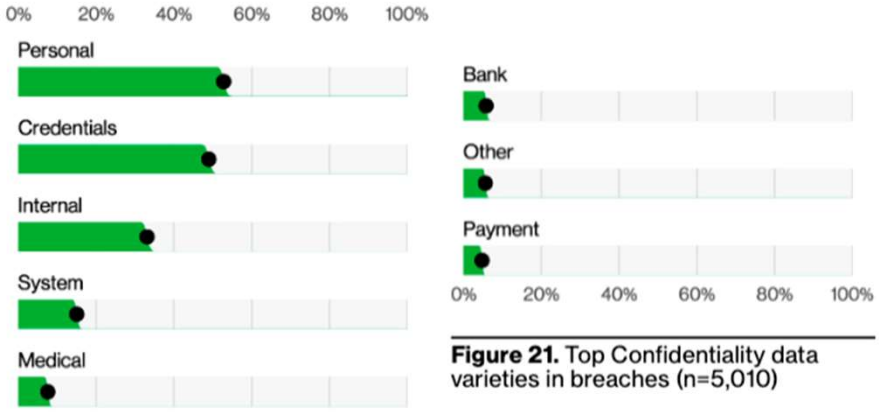


Figure 21. Top Confidentiality data varieties in breaches (n=5,010)

Source: Verizon Data Breach Investigations Report, 2023

Here to Stay: Passwords Being Comprised

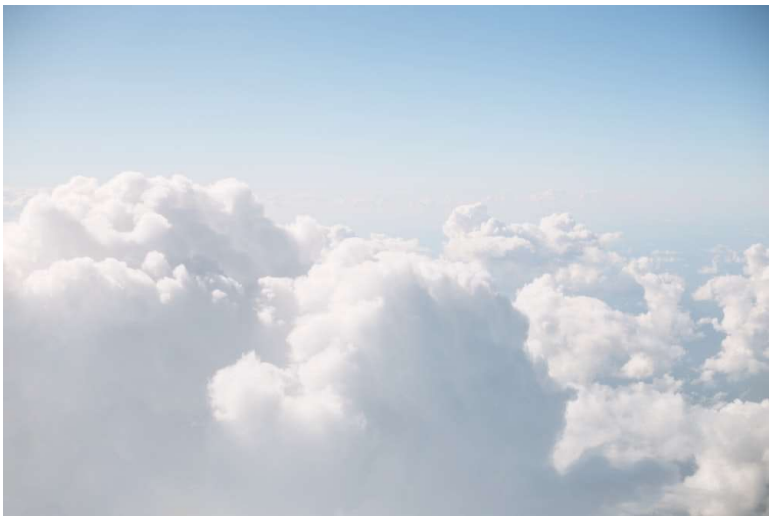
TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS › Learn how we made this table at hivesystems.io/password

- Brute force attacks
- Keylogger malware
- Database breaches
- Phishing

Here to Stay: Outsourcing



Here to Evolve: Outsourcing Risks

- Availability and reliability
- Supply chain compromises
- Zero-day vulnerabilities
- Tenancy issues
- Privacy concerns

Here to Stay: Basic Cyber Hygiene

- Authentication controls
- User access management
- Patch management and malware protections
- Employee training
- Backup procedures

Here to Evolve: Increased Scrutiny

- External audits
- Breach laws and privacy regulations
- Insurance
- Information security standards

Polling Question 2

What concerns you the most about the evolution?

- People still making mistakes
- Inability to keep up with the bad guys
- Reliance on vendors
- Lack of resources to invest
- Other (chat it!)

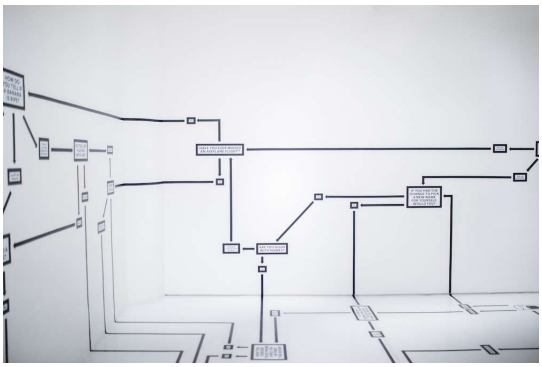
What can you do?

First Step: Acceptance

Budget for cybersecurity.

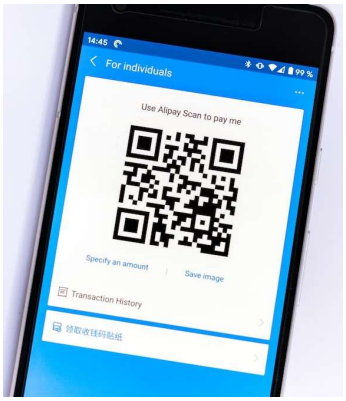
Identify your assets.

- Hardware
- Software
- Data sets
- People/users
- Connections
- Data flows



Train ***your*** people.

- Include employees, volunteers, and other relevant constituents
- Update your content
  - How to identify threats
  - Evolution of social engineering (vishing, smishing, quishing)
  - Authentication risks and controls (e.g., MFA)



Shift focus to layered authentication.

- Aim for **“password diversity”**
- Configure lockout settings
- Use multi-factor authentication
- Do not forgo previous controls if you do not have sufficient mitigating layers to mitigate risks

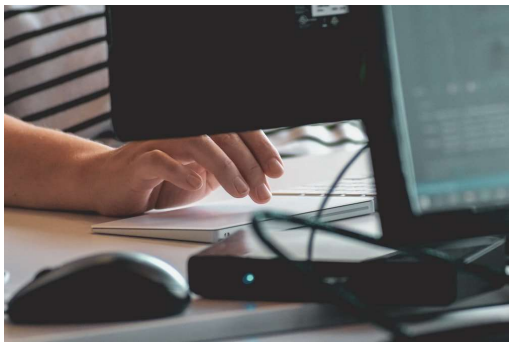
Polling Question 3

What is the biggest challenge with authentication?

- Too many passwords to remember
- Employees don’t see the risk
- We can’t keep up with the bad guys
- Resources to implement multi-factor authentication
- Other (chat it!)

Administer access well to support job function.

- Types of access
  - Employees
  - Volunteers
  - Contractors
  - Services
  - Vendors
- Unique identifiers (vs. shared accounts)



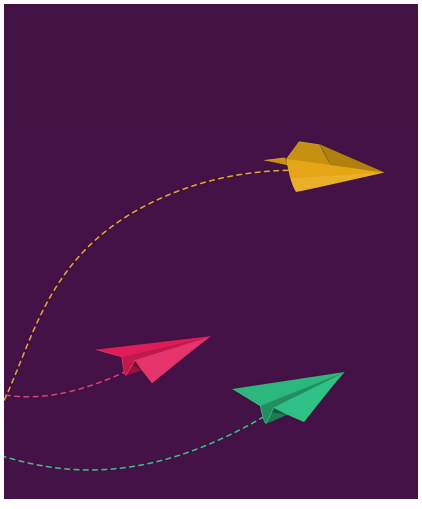
Is it time for better authentication solutions?

- Examples
  - Identity and access management (IAM) solutions
  - Password managers
- Evaluate pros vs. cons
- Can be excellent controls but not without risk

Considerations for Authentication

- Oversight and management
- Single point of failure
- Integration challenges
- Privilege escalation

Evaluate data loss controls.



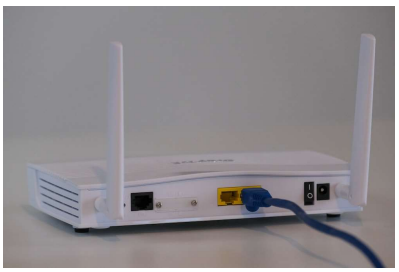
- Email solutions
- File-sharing services
- Removable media
- Vendor connections
- Firewall configurations

Purge your data when no longer required.

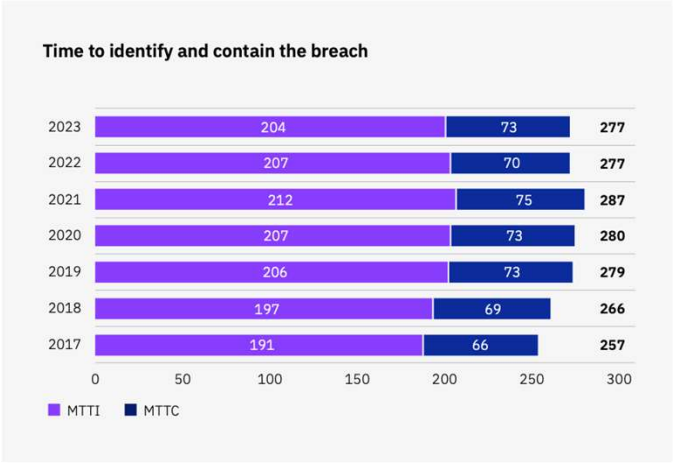
Anti-Malware and Patch Management

- Automated for all servers, desktops, and laptops
  - Operating systems and applications
  - Apple products are not immune to viruses!
- How does remote work impact this?

What do these have in common?

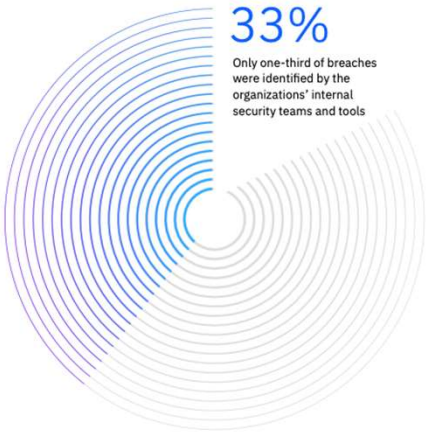


With all the practice, our response must be good.



IBM Cost of a Data Breach Report, 2023

With all the practice, our response must be good!



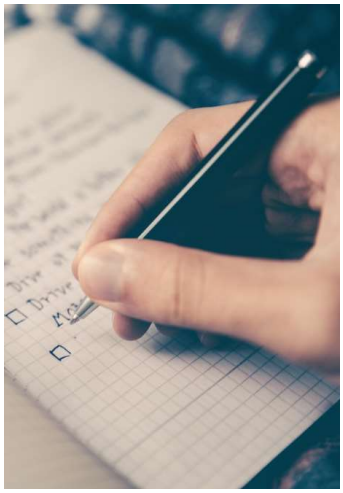
IBM Cost of a Data Breach Report, 2023

Future of Cybersecurity: Fighting AI with AI

- Tools to identify, correlate, and respond to activity
- More involvement of third parties
- Risk-based approach to threat management
- More comprehensive and holistic

What do you do in the interim?

- Identify key activities
- Enable logging
- Manually review activity
- Establish process to correlate
- Identify gaps in visibility



Plan your response.

- Make connections
- Discuss process with insurance provider
- Walk through your plan
- Understand potential impact and legal and regulatory requirements

Polling Question 4

Do you have an incident response plan?

- No, we do not.
- Yes, but it's not formalized.
- Yes, it's formally documented.
- Yes, it's formally documented and we test it, too!

Establish a strong backup strategy.

- Frequency and retention
- Encryption and security
- Air gapping
- Location from source data
- Vendor considerations

Oversee your service providers.

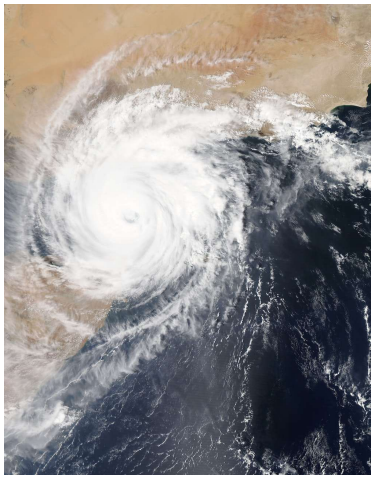
- Establish procedures for selection and monitoring
- Implement contractual requirements for security
- Remember the “why” behind outsourcing

Relying on reputation alone does not support adequate due diligence.

What to Consider

- Financial viability
  - *How does this tie in?*
- Security controls
  - Policy overview
  - Security audit reports, vulnerability scans, penetration testing
  - Location of data

What to Consider

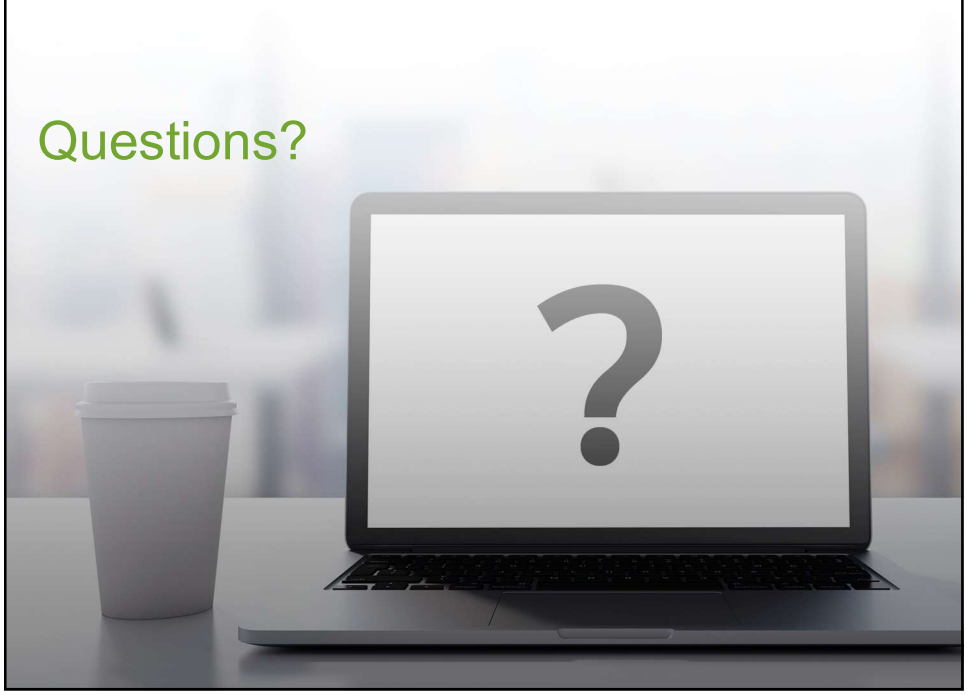


- Incident management
  - Business continuity plans
  - Incident response plans
  - Testing of plans
  - Insurance coverage
  - Capacity constraints

What to Consider

- Vendor management
  - Policies and procedures
  - Subcontractor usage (supply chain)
- Compliance considerations
- Ransomware controls
  - It may be their fault, but it's still *your* problem

Questions?



Thanks!

Allison Ward, Partner
CapinTech, a CapinCrouse Company

award@capincrouse.com
505.50.CAPIN ext. 2008

Katie Kane, Senior Manager
CapinTech, a CapinCrouse Company

kkane@capincrouse.com
505.50.CAPIN ext. 2007

CAPINTECH