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

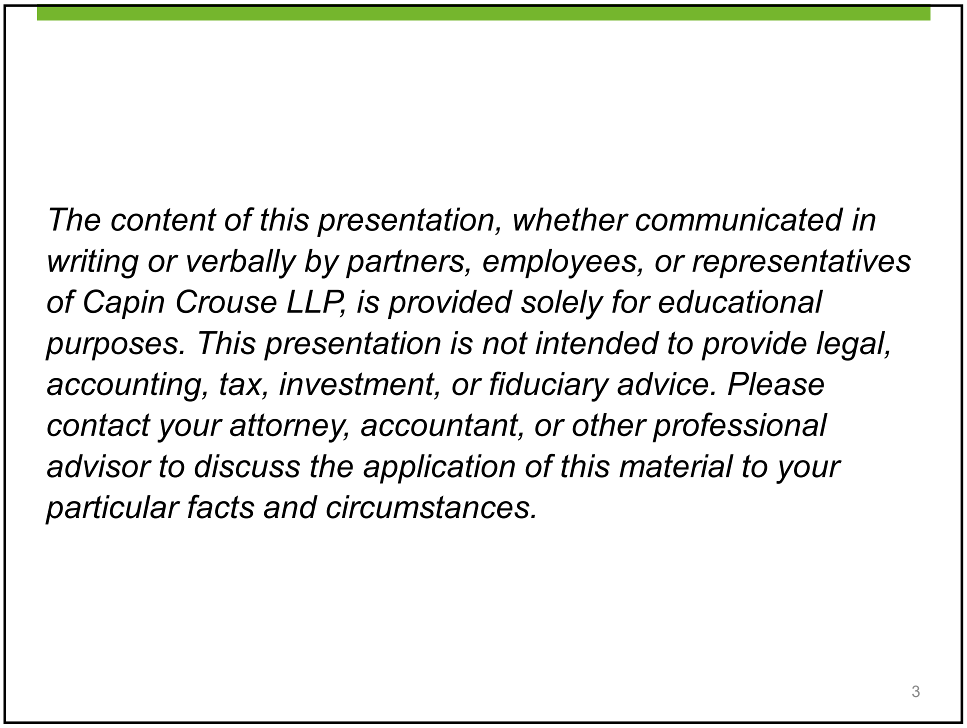
- Visit capincrouse.com/incident-management to access these resources from today's webcast:
  - Handout
  - Recording
- To receive CPE credit, you must respond to the polling questions.
- If you qualify for CPE credit, a certificate will be emailed to you within the next few weeks.

Incident Management:

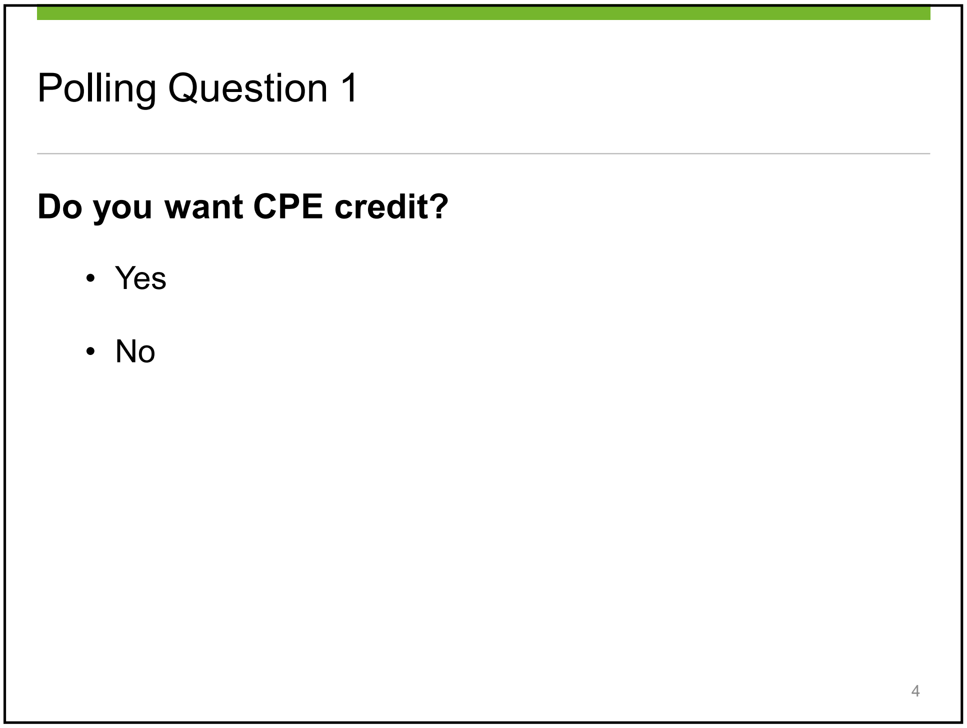
An Effective Response Starts Now

Allison Ward, Partner
Katie Herbert, Senior Manager
7.17.24

CAPINTECH



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, tax, 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?

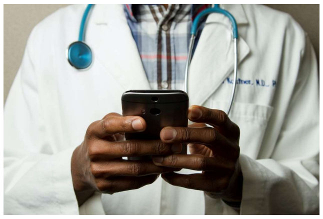
- Yes
- No

What are you up against?

CAPINTECH

You have a lot to plan for.

Who is being targeted?



Polling Question 2

Has your organization experienced an incident?

- Yes, but we were able to stop it.
- Yes, and unfortunately it resulted in a breach.
- No! Knock on wood.
- Unknown at this time.

What types of attacks are we seeing?

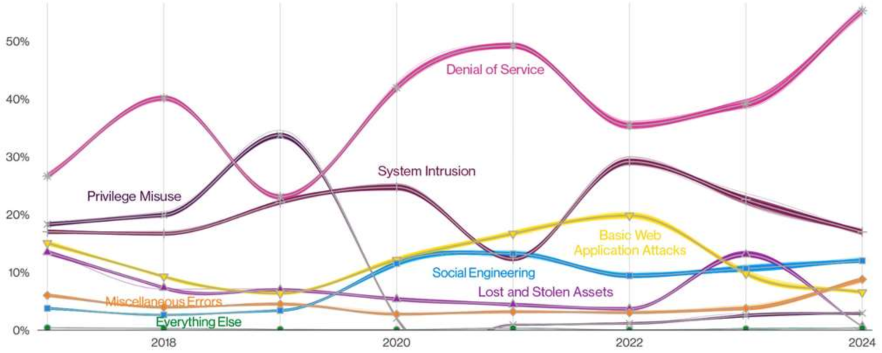


Figure 26. Patterns over time in incidents

Source: Verizon Data Breach Investigations Report, 2024

What types of attacks are we seeing?

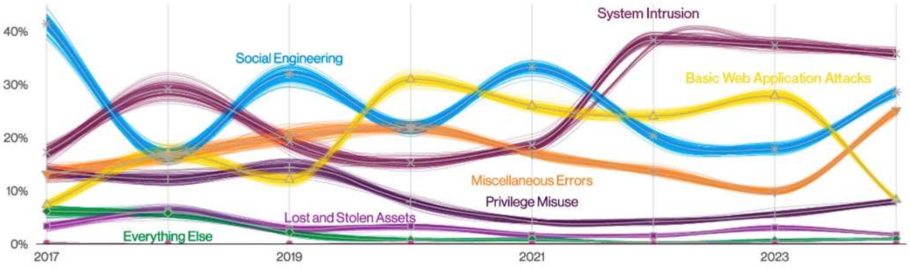


Figure 27. Patterns over time in breaches

Source: Verizon Data Breach Investigations Report, 2024

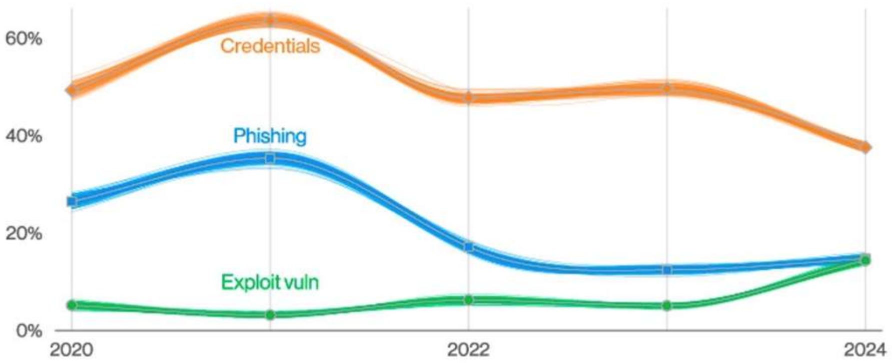


Figure 6. Select ways-in enumerations in non-Error, non-Misuse breaches over time

Source: Verizon Data Breach Investigations Report, 2024

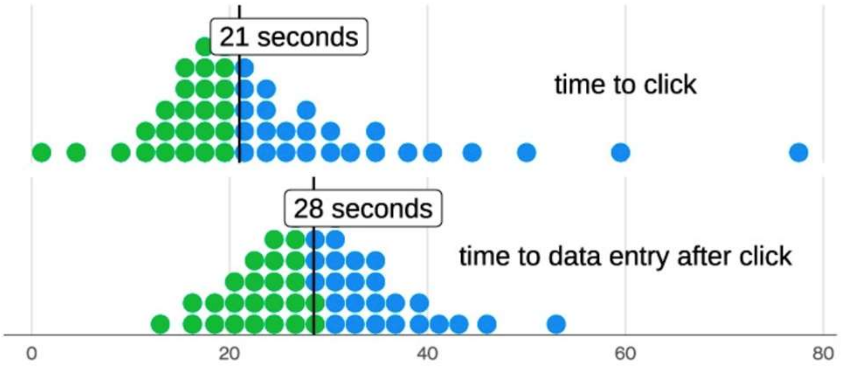


Figure 39. Time between email clicked and data entered

Source: Verizon Data Breach Investigations Report, 2024

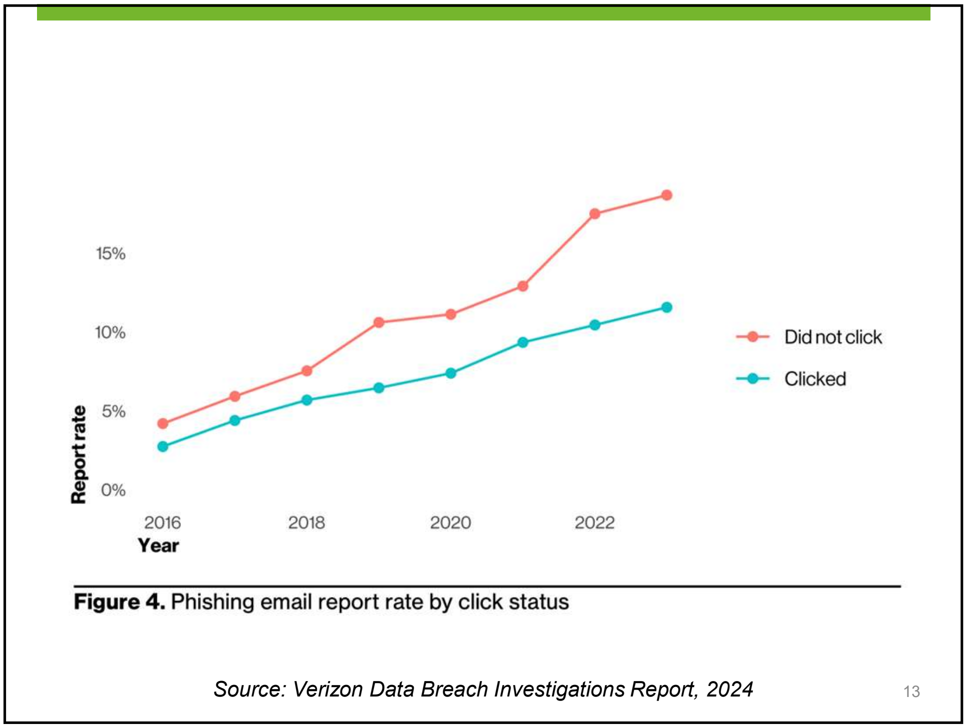


Figure 4. Phishing email report rate by click status

Source: Verizon Data Breach Investigations Report, 2024

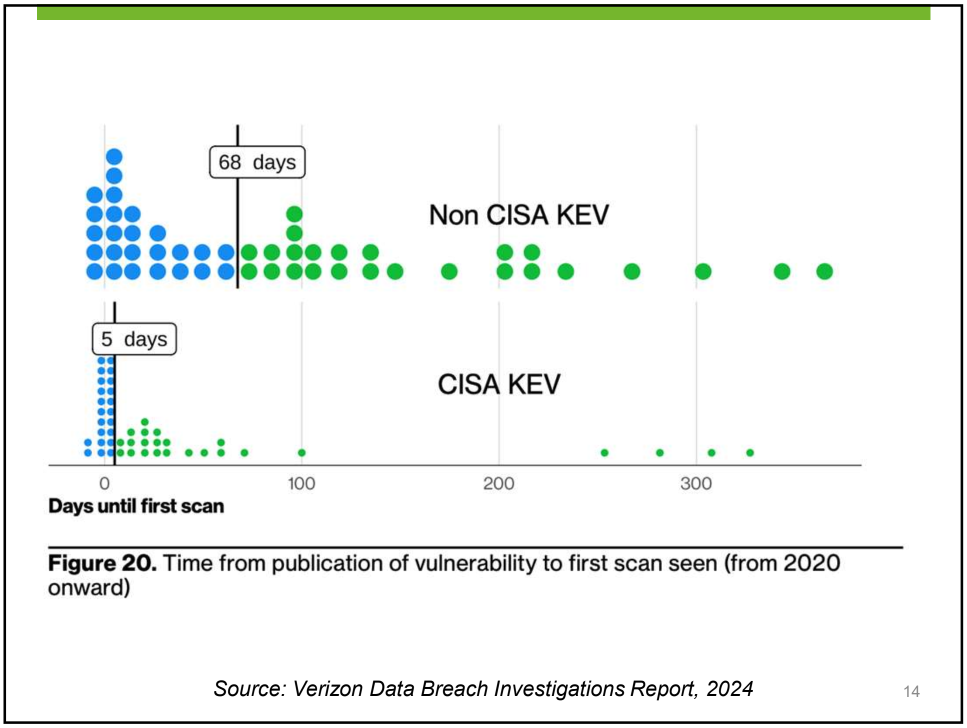


Figure 20. Time from publication of vulnerability to first scan seen (from 2020 onward)

Source: Verizon Data Breach Investigations Report, 2024

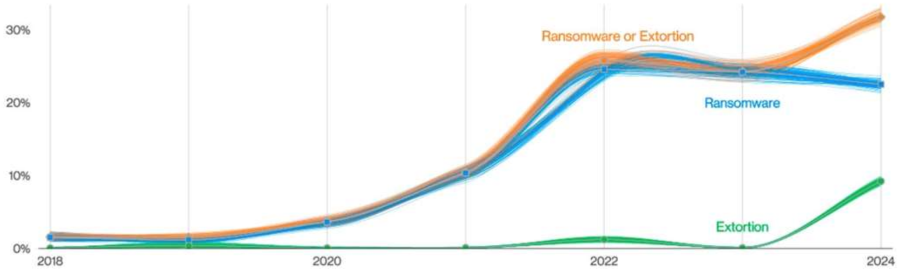


Figure 2. Ransomware and Extortion breaches over time

Source: Verizon Data Breach Investigations Report, 2024

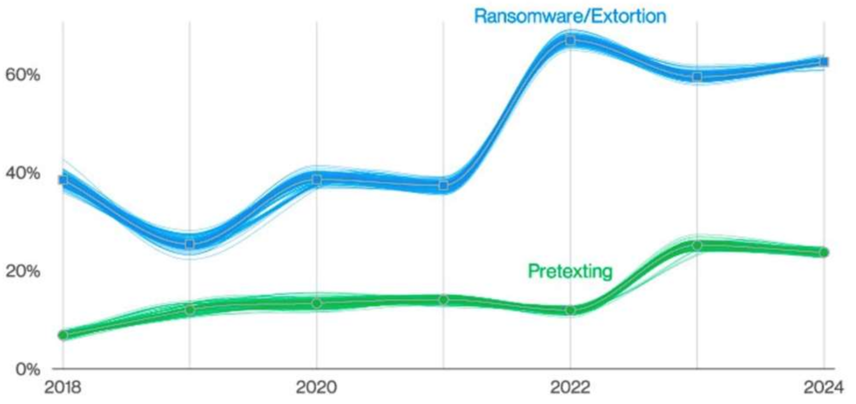


Figure 5. Select action varieties in Financial motive over time

Source: Verizon Data Breach Investigations Report, 2024

Supply Chain Disruptions

- How are you impacted?
- How are your service providers impacted?
- How are your service provider’s service providers impacted?
- And on and on…

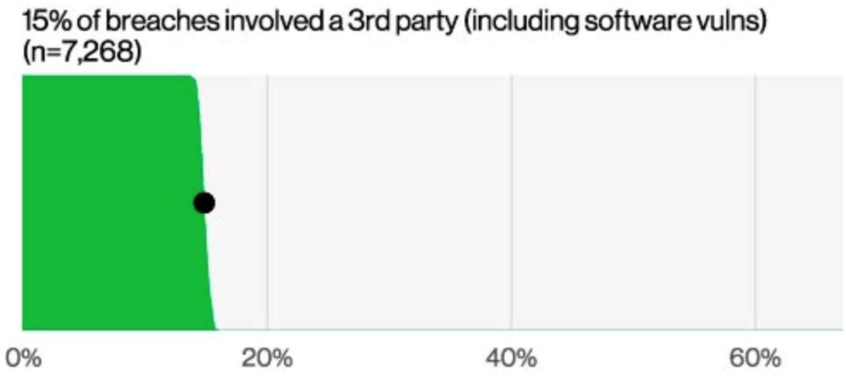

15% of breaches involved a 3rd party (including software vulns) (n=7,268)

Figure 3. Select key enumerations in breaches

Source: Verizon Data Breach Investigations Report, 2024

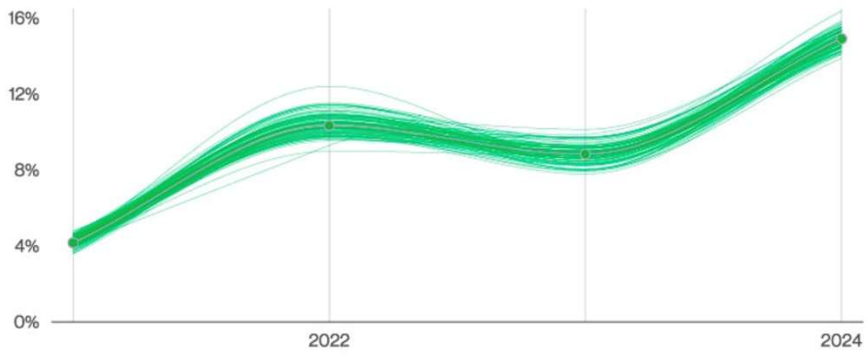


Figure 9. Supply chain interconnection in breaches over time

Source: Verizon Data Breach Investigations Report, 2024

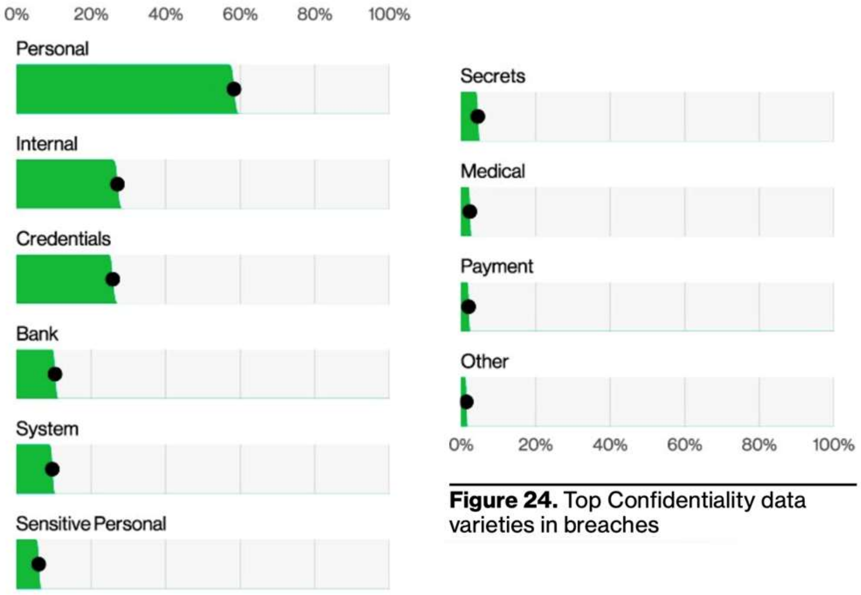
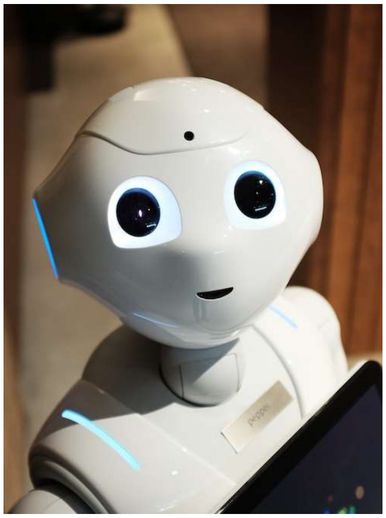


Figure 24. Top Confidentiality data varieties in breaches

Source: Verizon Data Breach Investigations Report, 2024

What are the challenges?

Growing Challenges



- Balancing regulatory requirements and usability
- Expanding technologies
- System integrations
- Mergers and acquisitions
- Vendor supply chain
- More to plan for

To address challenges, your plan must be…

- Fluid and adaptable
- Straightforward and useable
- Comprehensive enough to:
  - Support continuity of operations
  - Minimize impact
  - Enable timely recovery

Where do you start?

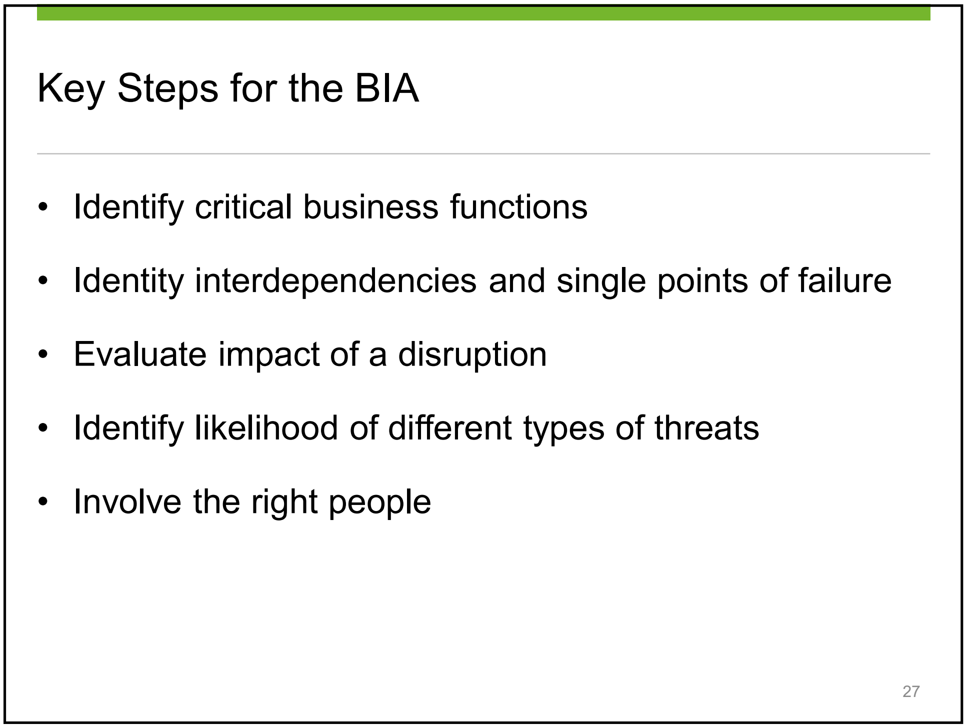
CAPINTECH

Polling Question 3

Do you have an incident response plan?

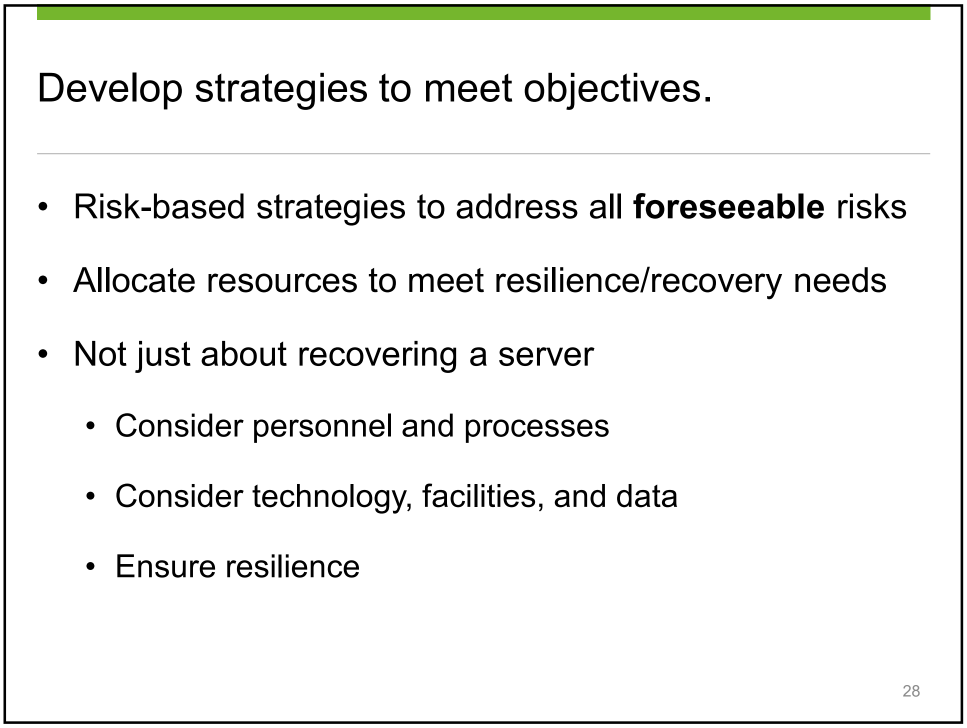
- No, why do you think I’m here?
- Yes, but it’s not formalized.
- Yes, signed, sealed, and delivered!
- Other (chat it)

Conduct a business impact assessment (BIA).



Key Steps for the BIA

- Identify critical business functions
- Identity interdependencies and single points of failure
- Evaluate impact of a disruption
- Identify likelihood of different types of threats
- Involve the right people



Develop strategies to meet objectives.

- Risk-based strategies to address all **foreseeable** risks
- Allocate resources to meet resilience/recovery needs
- Not just about recovering a server
  - Consider personnel and processes
  - Consider technology, facilities, and data
  - Ensure resilience

An effective response starts now.

Planning: Who is your team?

- Define team member roles and responsibilities
- Include wide range of backgrounds and expertise from different areas within the organization
- Who is on your team?

Planning: What are your goals?

- How do you balance confidentiality, integrity, and availability?
  - Drives containment
  - Legal and liability considerations
- Are you focused on security of data or operations?
  - What can be disconnected?
  - What needs to remain online?

Planning: Would you pay the ransom?

Planning: Scope and Escalation

- What constitutes an incident?
- What warrants escalation of the plan?
- Who makes the call to enact the plan?
- Do front-line staff know how to identify an issue?

Planning: Identification

- Do you have visibility?
  - Network perimeter
  - Internal traffic
  - Within applications
  - Within endpoints
- Where are the gaps?
- What can't you see?

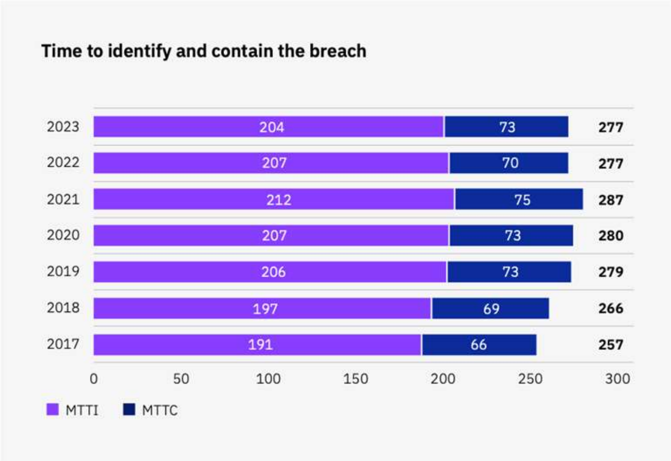
Is AI the future of incident response?

With all the practice, the response must be good!

- More complex, “low-and-slow” attacks
- Goal of compromising as much of network as possible to get the largest possible payout
- 56% didn’t detect a breach for **3 – 12 months**

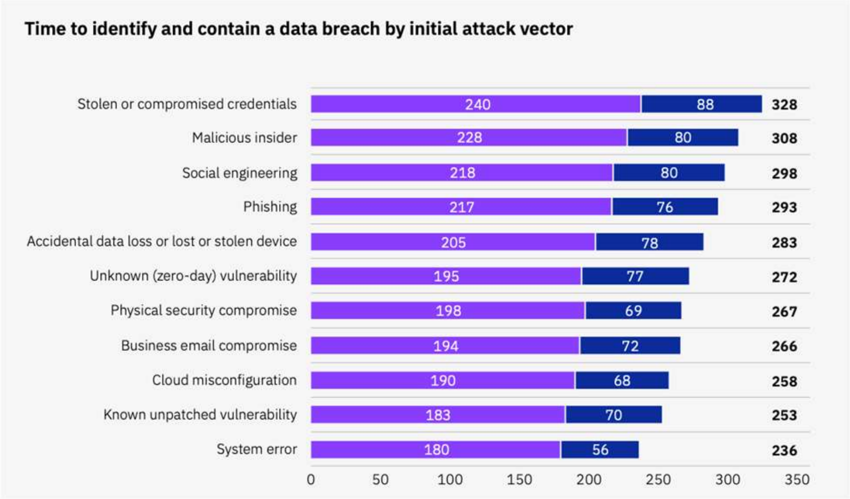
Source: Cybereason Ransomware: The True Cost to Business Report, 2024

With all the practice, the response must be good!



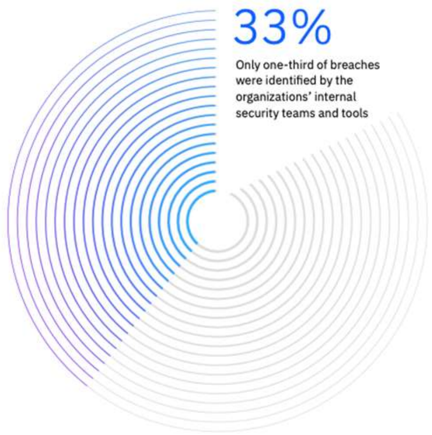
Source: IBM Cost of a Data Breach Report, 2023

With all the practice, the response must be good!



Source: IBM Cost of a Data Breach Report, 2023

With all the practice, the response must be good!



33%

Only one-third of breaches were identified by the organizations' internal security teams and tools

Source: IBM Cost of a Data Breach Report, 2023

With all the practice, the response must be good!

How was the breach identified?

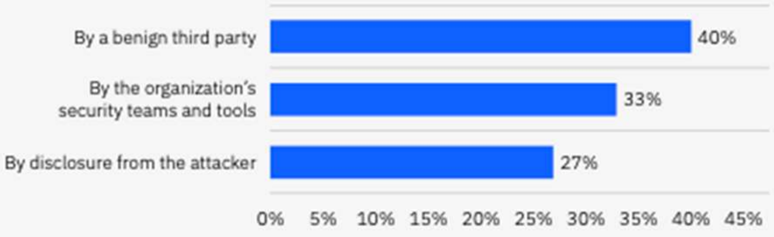


Figure 12. Only one response permitted

Source: IBM Cost of a Data Breach Report, 2023

With all the practice, the response must be good!

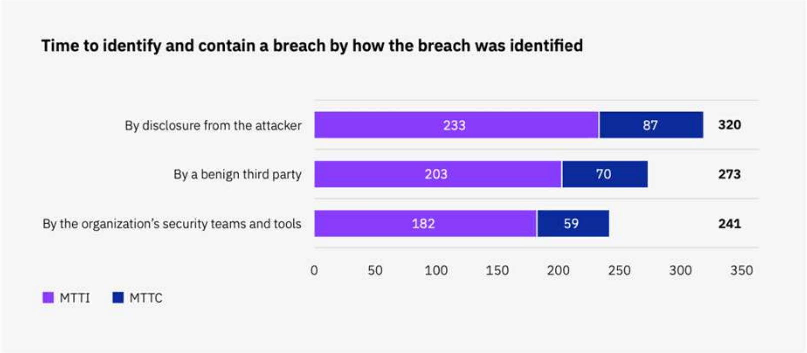


Figure 14. Measured in days

Source: IBM Cost of a Data Breach Report, 2023

41

Planning: Notification

- Who do you need to notify internally upon enacting the plan?
- How do you notify?
  - Unique considerations with cyber incidents.
  - Do you have alternate contact mechanisms?

42

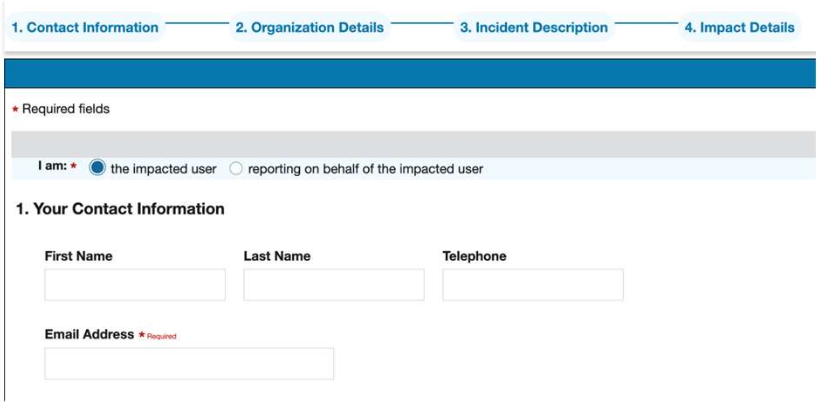
Planning: Notification

- Who are you going to notify to aid in mitigations?
  - Insurance
  - Law enforcement
  - Ransomware specialists
  - Forensics
  - Legal

Planning: Notification

- What external parties do you need to notify? When?
  - Regulators
  - Information-sharing organizations
  - Key vendor relationships

Cybersecurity & Infrastructure Security Agency



1. Contact Information — 2. Organization Details — 3. Incident Description — 4. Impact Details

* Required fields

I am: * ● the impacted user ○ reporting on behalf of the impacted user

1. Your Contact Information

First Name

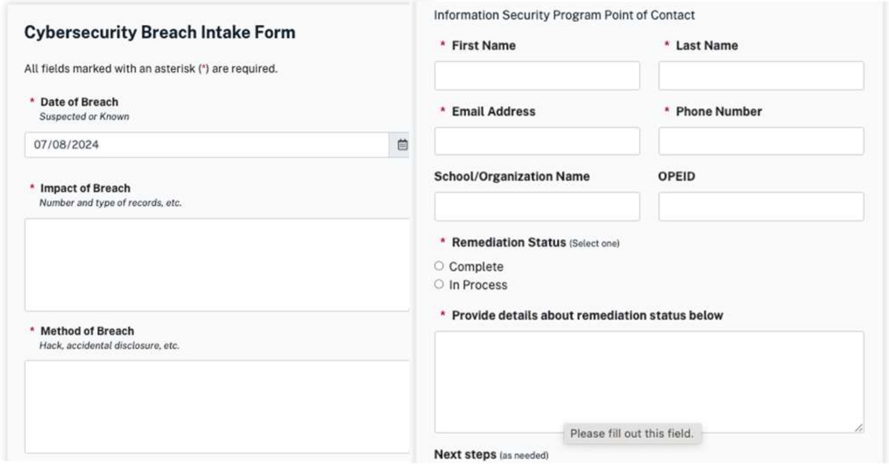
Last Name

Telephone

Email Address * Required

Source: Cybersecurity & Infrastructure Security Agency (CISA) Incident Reporting System

Federal Student Aid Breach Intake Form



Cybersecurity Breach Intake Form

All fields marked with an asterisk (*) are required.

* Date of Breach
Suspected or Known

07/08/2024

* Impact of Breach
Number and type of records, etc.

* Method of Breach
Hack, accidental disclosure, etc.

Information Security Program Point of Contact

* First Name

* Last Name

* Email Address

* Phone Number

School/Organization Name

OPEID

* Remediation Status (Select one)

○ Complete

○ In Process

* Provide details about remediation status below

Please fill out this field.

Next steps (as needed)

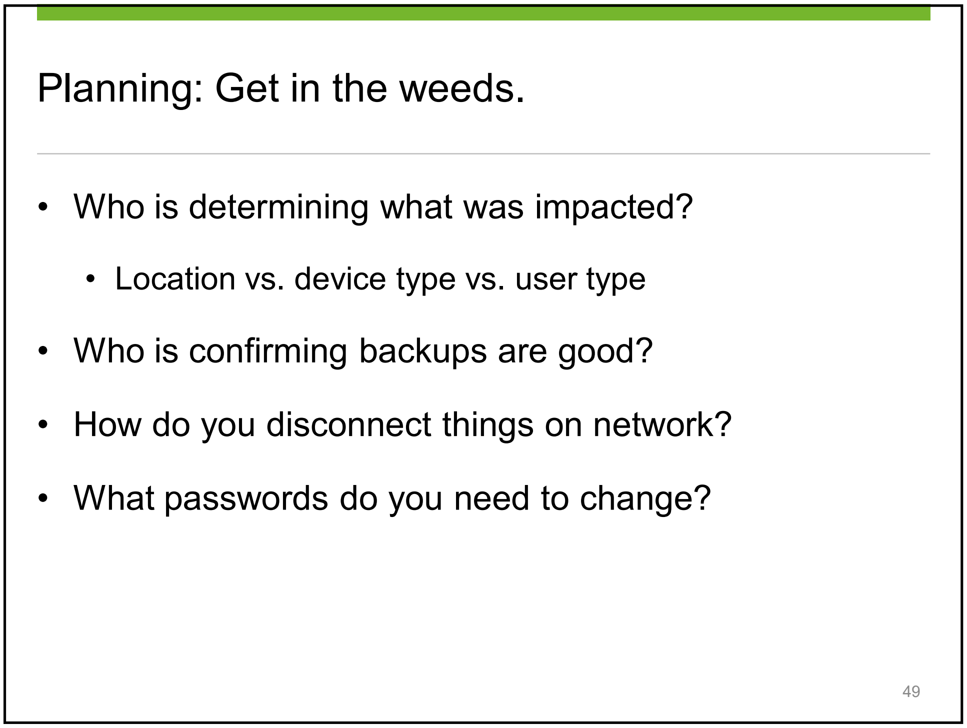
Source: Federal Student Aid website, Cybersecurity page

Planning: Containment

- What "categories" do you plan for?
  - External attacks
  - Vendor-initiated events
  - Customer-initiated events
  - Employee-initiated issues (e.g., phishing)
- Any separate processes for specific events?

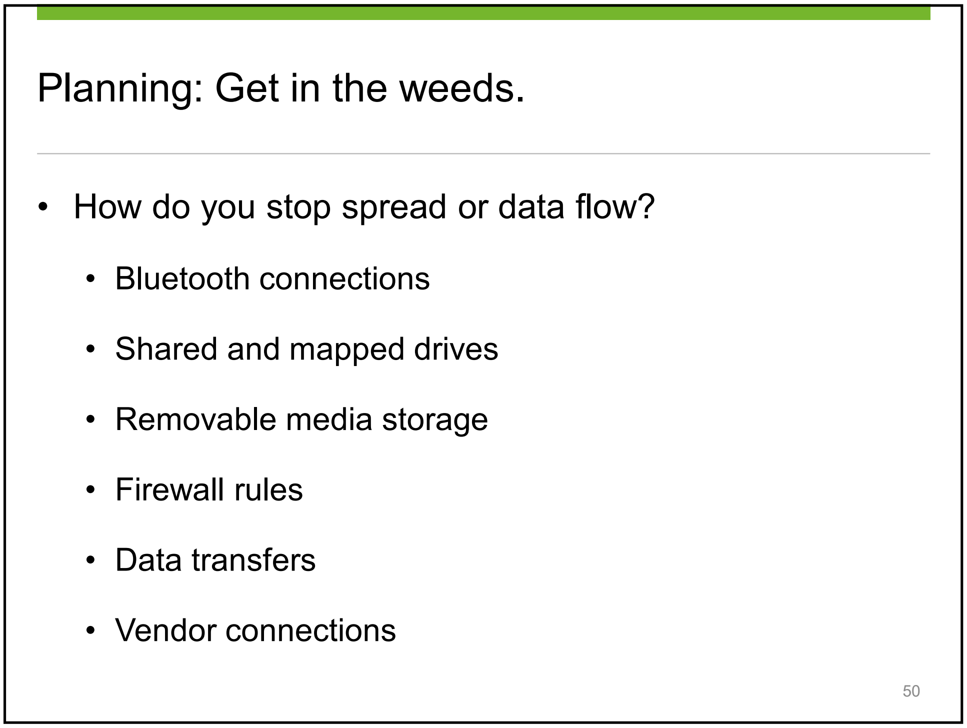
Planning: Containment

- How do you contain?
  - Isolation of compromised systems
  - Additional monitoring of intruder activities
  - Searching for additional compromised systems



Planning: Get in the weeds.

- Who is determining what was impacted?
  - Location vs. device type vs. user type
- Who is confirming backups are good?
- How do you disconnect things on network?
- What passwords do you need to change?



Planning: Get in the weeds.

- How do you stop spread or data flow?
  - Bluetooth connections
  - Shared and mapped drives
  - Removable media storage
  - Firewall rules
  - Data transfers
  - Vendor connections

Planning: Do you kill the Internet completely?

51

Planning: Containment

- Identify critical processes for unique events
  - Comprised emails and creation of auto-forwarding rules
  - Ransomware vs. wiperware

52

Planning: Maintaining Evidence

- What activity logs do you have?
  - Sufficient storage time
  - Off-loaded from associated device
  - Backed up and retained
- Remember: many issues aren’t identified right away
- Other concerns: custody, integrity, preservation, etc.

53

Planning: Restoration

- Ties heavily to Disaster Recovery Plan but more than having backups to restore from
- Ensure backups cannot be impacted by ransomware
  - Make immutable
  - Create physical offline copies
  - Utilize logical air gapping
- How do you ensure backups are “clean”?

54

Planning: Post-Incident Notification

- Who are you going to notify? And when and how?
  - Constituents
  - Donors
  - Vendors
  - Organizations in the industry
  - Public or media
- Do you have contact details readily available?

What are you going to say?

Planning: Understanding Legal Requirements

57

Planning: Lessons Learned

- What worked in your plan?
- What didn’t work?
- Where did you struggle?
- What wasn’t documented?

58

Cyber insurance: where does it fit in?

Check with your vendors.

- What are they doing to protect your hosted data?
- If your vendor has a ransomware incident, you could potentially lose your data.
  - It may be their fault, but it's still *your* problem.
  - What does that mean for you?

Practice makes ~~perfect~~ better.

- Conduct exercises
- Incorporate key stakeholders
- Evaluate effectiveness of your training program
- Identify gaps in plans before disaster or incident happens

Takeaways from Tabletop Discussions

- Where are the maybes?
- Where do you not have visibility?
- Where do you need training?
- Where do you need authorization?
- What do you need to document?
- Is this attack plausible in your environment?
- What is the ONE thing you need to do?

Report to Management regularly.

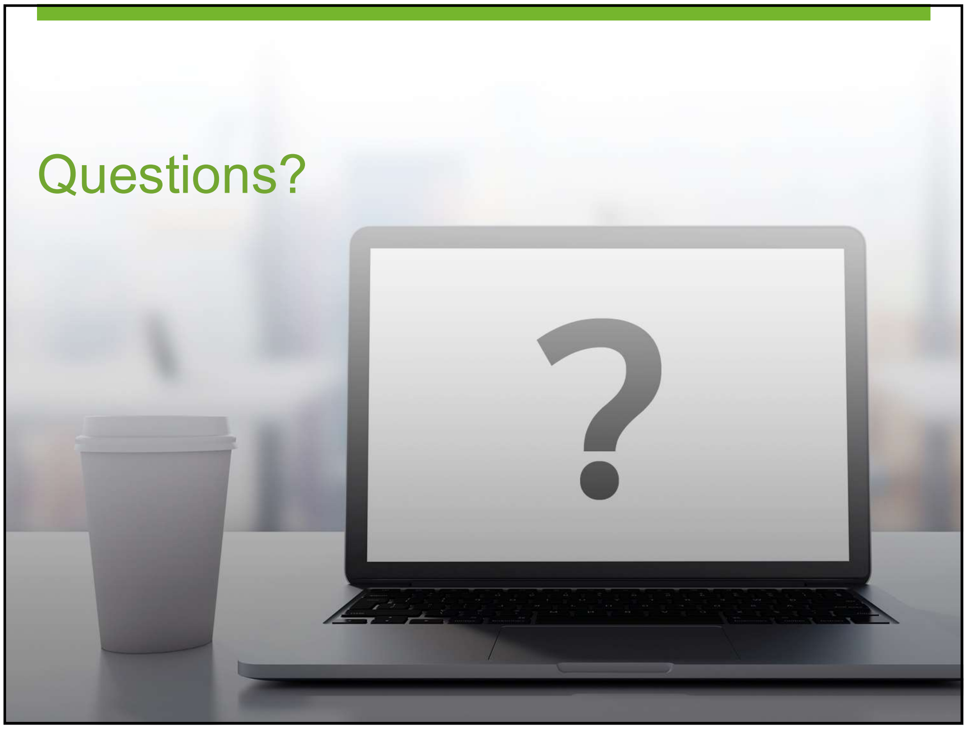
- Results of your BIA and risk assessment
  - *Advocate for your needs*
- Major changes to plans
- Results of training
- Results of testing

Polling Question 4

Do you feel more prepared?

- No! I’m making a motion to get rid of the Internet.
- A little, but it’s overwhelming.
- Yes, I feel like we can do this!

Questions?



Thanks!

Allison Ward, CISSP, CISA, CISM
Partner, CapinTech

✉ award@capincrouse.com
☎ 505.50.CAPIN ext. 2008

Katie Herbert, CISSP, CISA, CISM
Senior Manager, CapinTech

✉ kherbert@capincrouse.com
☎ 505.50.CAPIN ext. 2007

CAPINTECH