Cybersecurity Year-End Review

Allison Ward, Partner
Katie Herbert, Senior Manager
12.4.24

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.

4

Polling Question 1

Do you want CPE credit?

- Yes

- No

Answer in the Conferences i/o app on your device.

What are you up against?

CAPINTECH

We are up against a lot.

More money, more problems.

Global average total cost of a data breach

3.86 3.92 3.86 4.24 4.35 4.45 4.88
2018 2019 2020 2021 2022 2023 2024
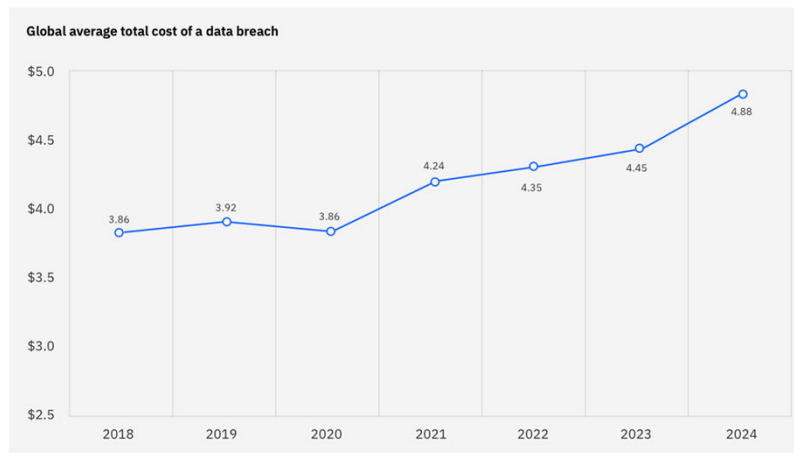
Figure 1. Measured in USD millions

IBM Cost of a Data Breach Report, 2024

Average cost of a data breach in 4 components
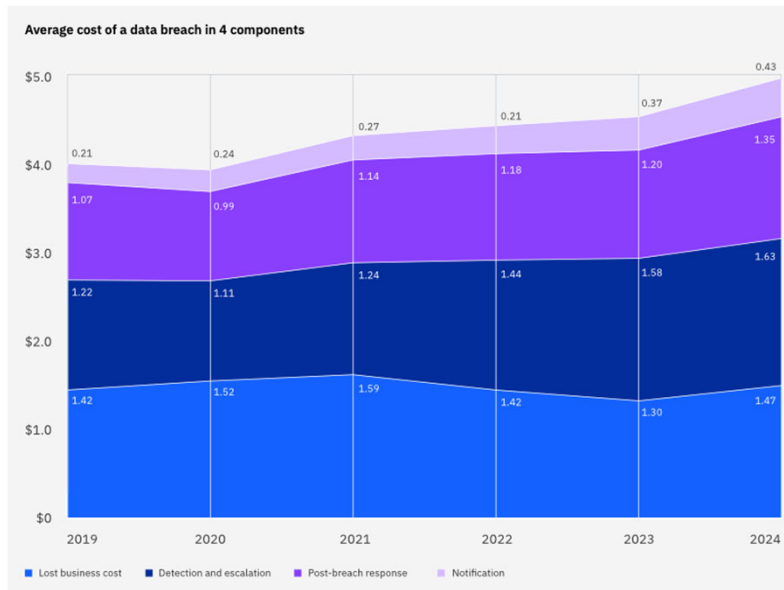
Figure 5. Measured in USD millions

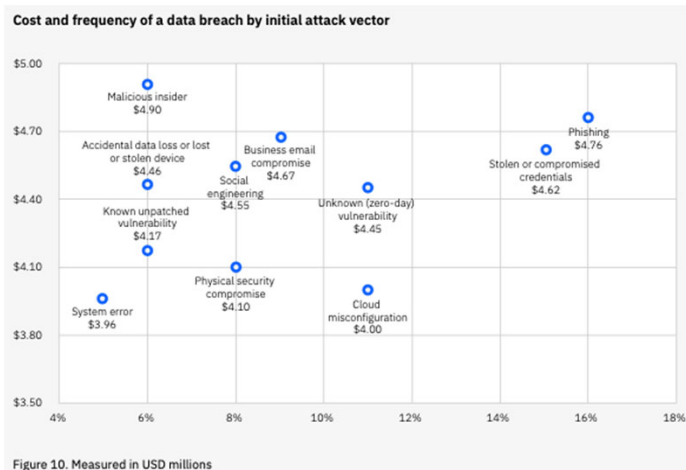*IBM Cost of a Data Breach Report, 2024*

Same threats, different day.

Cost and frequency of a data breach by initial attack vector

Figure 10. Measured in USD millions

IBM Cost of a Data Breach Report, 2023

Cost and frequency of a data breach by initial attack vector

$5.2	
$5.0	Business email compromise, 4.88 — Malicious insider, 4.99 — Phishing, 4.88
$4.8	Social engineering, 4.77 — Stolen or compromised credentials, 4.81
$4.6	Unknown zero-day vulnerability, 4.46
$4.4	Known unpatched vulnerability, 4.33
$4.2	Accidental data loss and lost or stolen device, 4.28 — Physical security compromise, 4.19
$4.0	System error, 4.07 — Cloud misconfiguration, 3.98
$3.8	

4%   6%   8%   10%   12%   14%   16%   18%

Figure 7. Measured in USD millions; percentage of all breaches

IBM Cost of a Data Breach Report, 2024

11

Factors that increased the average breach cost

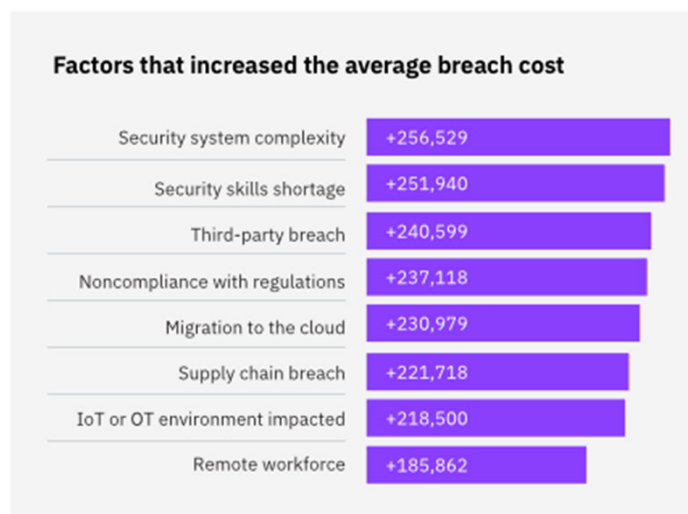|	
Security system complexity	+256,529
Security skills shortage	+251,940
Third-party breach	+240,599
Noncompliance with regulations	+237,118
Migration to the cloud	+230,979
Supply chain breach	+221,718
IoT or OT environment impacted	+218,500
Remote workforce	+185,862

Figure 26. Cost difference from USD 4.88M breach average; measured in USD

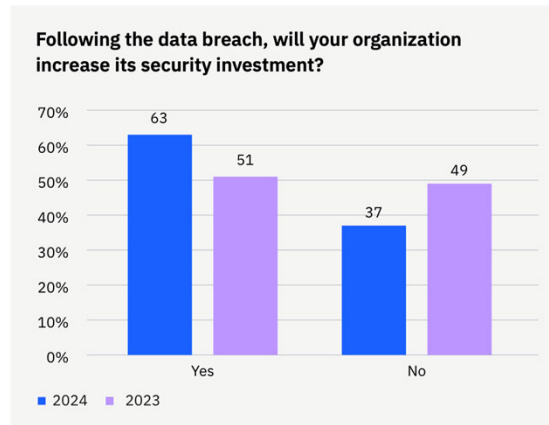*IBM Cost of a Data Breach Report, 2024*

12

6

Breaches led to more investments.

Following the data breach, will your organization increase its security investment?

Figure 44. Percentage of all organizations

IBM Cost of a Data Breach Report, 2024

13

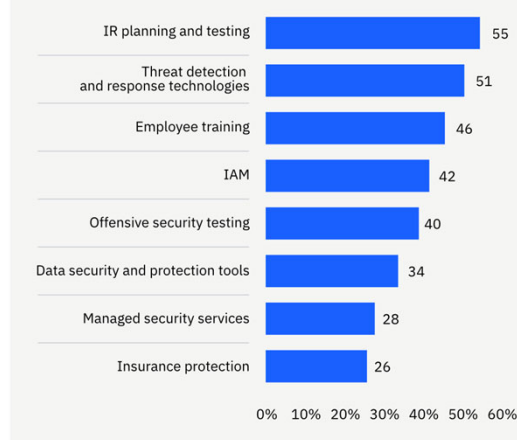**Most common investment types among those increasing security investments after a data breach**

Investment type	%
IR planning and testing	55
Threat detection and response technologies	51
Employee training	46
IAM	42
Offensive security testing	40
Data security and protection tools	34
Managed security services	28
Insurance protection	26

Figure 45. Share among organizations that are increasing security investment; more than 1 response permitted

IBM Cost of a Data Breach Report, 2024

14

Factors that reduced the average breach cost

−258,629	Employee training
−258,538	AI, machine learning driven insights
−255,932	Security information and event management (SIEM)
−248,072	Incident response (IR) planning
−243,914	Encryption
−243,090	Threat intelligence
−240,499	DevSecOps approach
−225,634	IR team
−222,883	Identity and access management (IAM)

−219,074	Proactive threat hunting
−214,603	Security orchestration, automation and response (SOAR)
−206,344	Insurance protection
−200,050	Offensive security testing
−186,463	ASM
−185,533	Endpoint detection and response tools
−167,430	Gen AI security tool
−166,600	Data security and protection software
−152,256	Board-level oversight
−144,365	CISO appointed
−92,734	Managed security service provider (MSSP)

IBM Cost of a Data Breach Report, 2024

15

But investments aren't always easy.

- Insurers are getting "tougher"

- Controls you invest in don't always evolve with threats

- Extensive skills gaps exist in cybersecurity

  - … or are the expectations too high?

- Culture can impact the success of implementations

- Regulation continues to evolve

16

Polling Question 2

What is your biggest roadblock to security?

- Continued evolution of threats

- Budgetary and resource constraints

- Skills gaps in cyber area

- Lack of management support

- Staff culture

Answer in the Conferences i/o app on your device.

17

What can we do?

CAPINTECH

Brainstorm: How are they getting our data?

- Social engineering

- System compromise

- Misdelivery, lost devices, misconfigurations

- Vulnerability exploitation

- Vendor issues

- Extraneous access

Brainstorm: Where are the gaps in vulnerability management?

- Identification of assets

- Identification of new vulnerabilities

- Reliance on third parties

- Resource limitations

20

Brainstorm: How are they defeating MFA?

- Social engineering

- SIM swapping

- Device theft

- Malware

- Push fatigue

Example: HK and Deepfakes

Images generated from thispersondoesnotexist.com

AI + Social Engineering

- Democratization via fraud-as-a-service

- Enhanced toolkits with generative AI and deepfakes

23
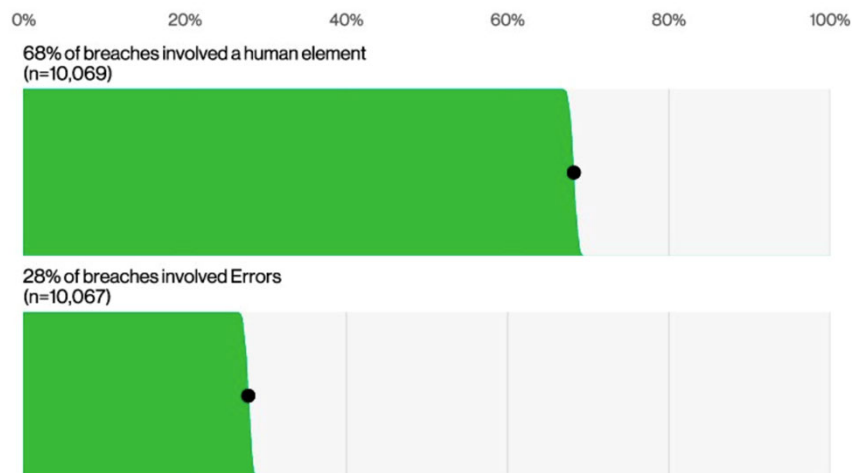
Verizon Data Breach Investigations Report, 2024

24
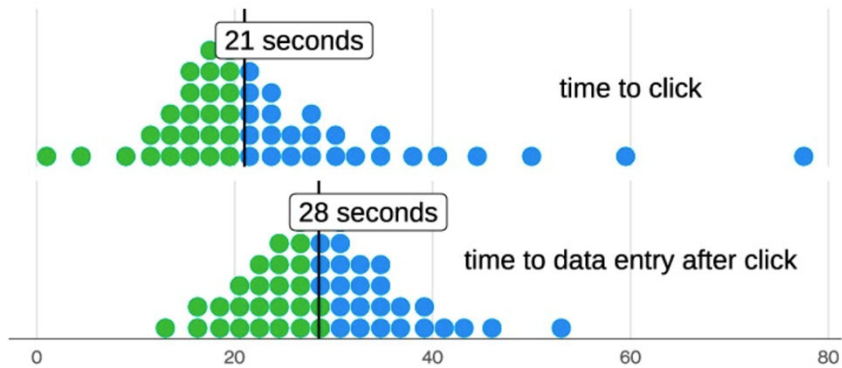
Figure 39. Time between email clicked and data entered

Verizon Data Breach Investigations Report, 2024

25
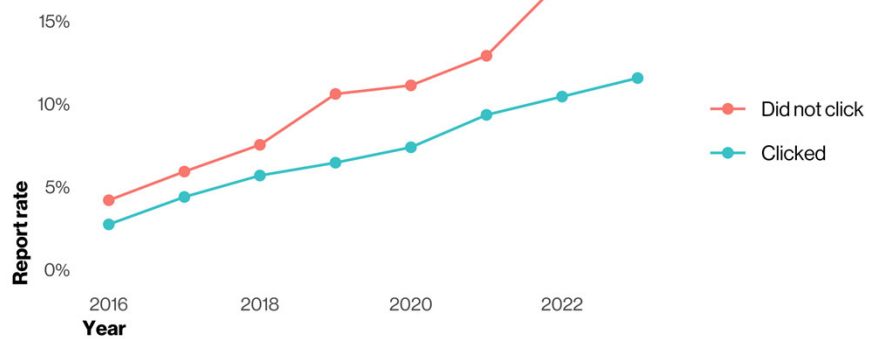
Figure 4. Phishing email report rate by click status

Verizon Data Breach Investigations Report, 2024

26

13

Polling Question 3

What control helps you the most in fighting phishing?

- Employee training

- Email filtering

- Phishing simulations

- External email disclaimers

- Other – chat it!
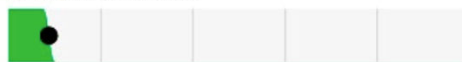
Answer in the Conferences i/o app on your device.

27
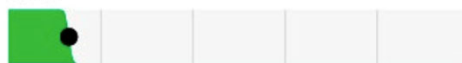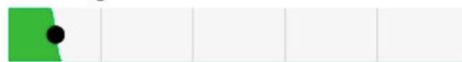
Verizon Data Breach Investigations Report, 2024

28

New Term: Shadow Data

Time to identify and contain a data breach including shadow data

	MTTI	MTTC	Total
Included shadow data	220	71	291
Did not include shadow data	169	58	227

■ MTTI ■ MTTC
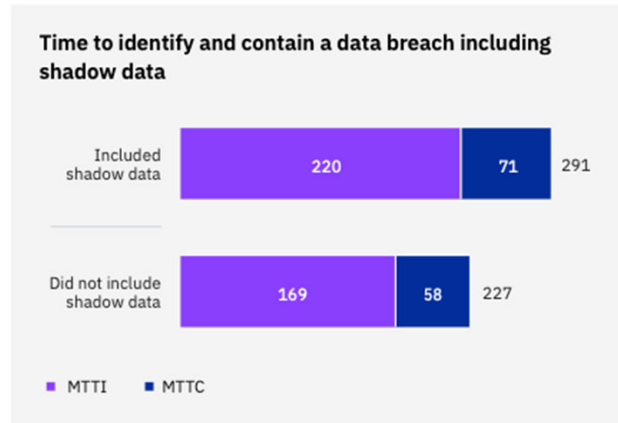
Figure 41. Measured in days

IBM Cost of a Data Breach Report, 2024

29

New Term: Shadow Data

Where was the shadow data included in the breach stored?

	Percentage
Across multiple types of environments	35
On premises	25
Public cloud	23
Private cloud	17
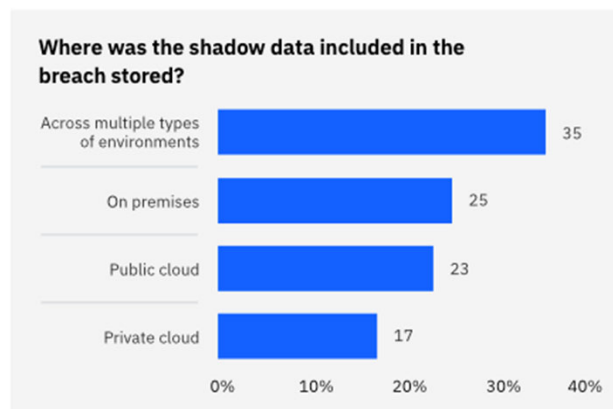
Figure 42. Percentage of breaches involving shadow data; 1 response permitted

IBM Cost of a Data Breach Report, 2024

30

15

How do you identify threats?

- Vendor alerts

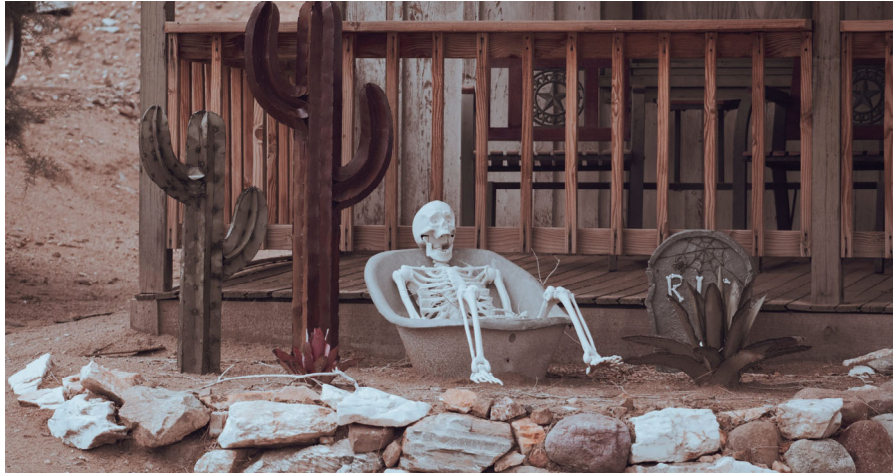- Threat-sharing groups

- Vulnerability scanning

31

How do you manage configurations?

- Baselines

- Standardization

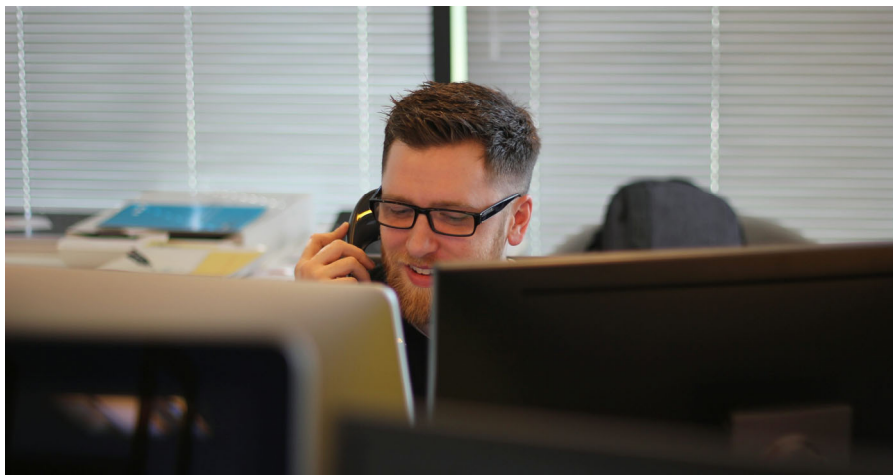- Change management

- Monitoring and review

32

16

Monitoring for End-of-Life

How do you manage your vendors?

Are there gaps with ancillary endpoints?

Zero-Day Vulnerabilities

Think about resiliency.

CAPINTECH
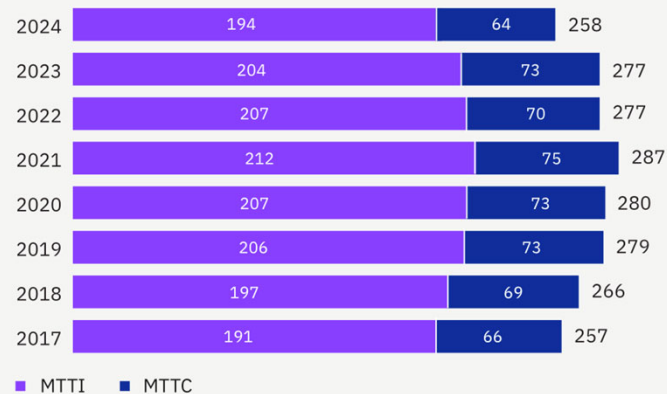

Time to identify and contain a data breach

Year	MTTI	MTTC	Total
2024	194	64	258
2023	204	73	277
2022	207	70	277
2021	212	75	287
2020	207	73	280
2019	206	73	279
2018	197	69	266
2017	191	66	257

■ MTTI   ■ MTTC

Figure 4. Measured in days

IBM Cost of a Data Breach Report, 2024

38

19

Potential Gap: Succession Planning

Potential Gap: Over-Reliance on Third Parties

Potential Gap: Inadequate Visibility

- Scope not comprehensive

- Lack of resources

- Inadequate frequency

41

Potential Gap: Plans Are Too General

- Plans have not evolved

- No tabletop discussions to flesh out procedures

- Leads to slower and less effective response

42

Potential Gap: Don't Know What Insurance Offers

43

Potential Gap: Backup Process Issues

- Lacking scope
  - Missing servers
  - Incorporation of cloud environments
- Encryption
- Retention
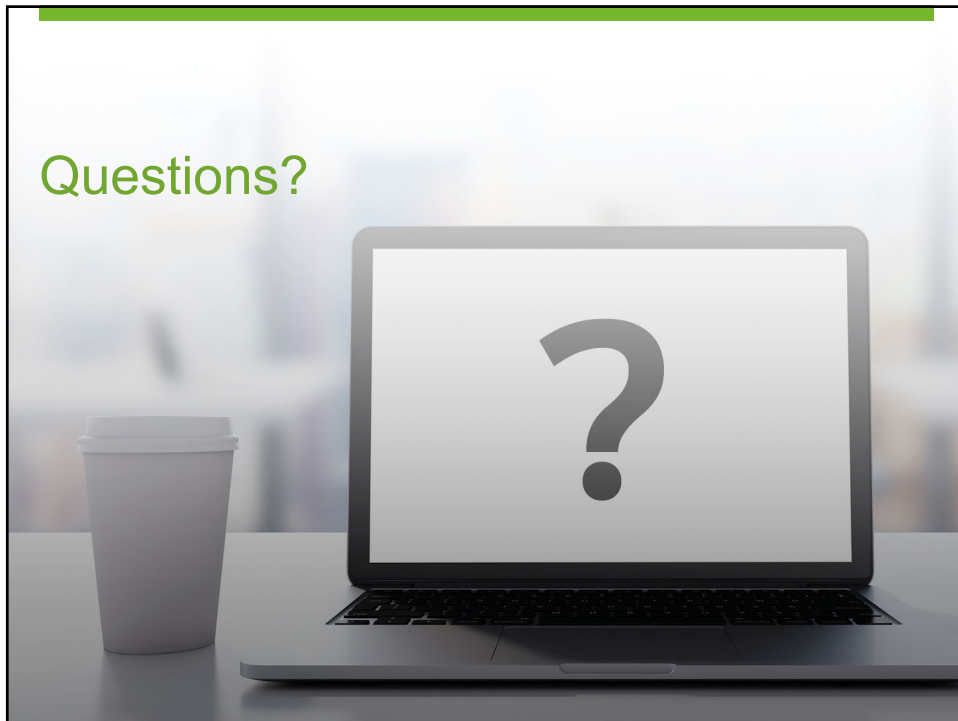- Ransomware protections

44

Polling Question 4

When it comes to cyber, how do you feel about the coming year?

- Shaking in my boots

- Preparing and feeling optimistic
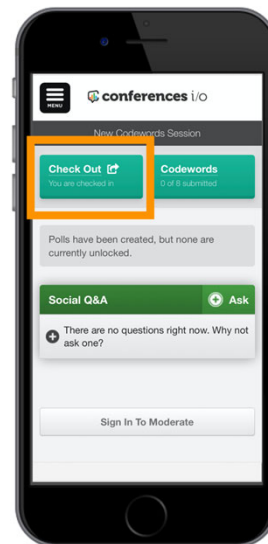
- Aiming for continual improvement

Answer in the Conferences i/o app on your device.

45

Questions?

Don't forget to check out of Conferences i/o before you leave!

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