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

- Visit capincrouse.com/glba-updates-2 to access these materials from today's webcast:
  - Handouts
  - Recording
- To receive CPE credit, you must respond to the polling questions, which are not available on mobile devices. Please log in on a computer if you would like to receive CPE credit.
- CPE certificates will be emailed to you within the next few weeks.

CAPINCROUSE LLP

Important GLBA Updates, Part 2

Allison Ward, Partner, CapinTech
Patricia Willhite, Senior Manager, CapinCrouse
9.13.23

CAPINCROUSE LLP

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.

3

Polling Question 1

Do you want CPE credit?

- Yes
- No

4

Quick Recap of Part 1

CAPINCROUSE LLP

What is the Safeguards Rule?

6

Common Issues We're Seeing

- Enabling multi-factor authentication
- Encrypting data in transit and at rest
- Establishing data retention and purging when met

7

What happens if you don't comply?

8

Expect follow up discussions!

9

But we are REALLY small…

- Exceptions exist if you maintain data on fewer than 5,000 customers
  - 314.4(b)(1) – written risk assessment
  - 314.4(d)(2) – continuous monitoring
  - 314.4(h) – written incident response plan
  - 314.4(i) – annual report to the board
- Should still be considered

10

What are we covering today?

- Testing and monitoring of your program
- Training procedures
- Oversight of service providers
- Incident response planning

11

Testing and Monitoring of Your Program

CAPINCROUSE

§ 314.4(d) – Test and Monitor

- Test and monitor effectiveness of key controls, systems, and procedures
- For information systems:
  - Continuous monitoring
  - Vulnerability scanning
  - Penetration testing

13

Polling Question 2

How are you meeting this requirement?

- We are not compliant yet
- Vulnerability scanning + penetration testing
- Continuous monitoring systems
- A combination

14

What constitutes continuous monitoring?

15

Alphabet Soup: EDR vs. NDR vs. MDR vs. XDR

- Same ‘why’
  - *Detection and response*
- Similar ‘how’
  - *Behavioral analysis, machine learning, AI*
  - *Human element required to be fully effective*
- Difference in the ‘what’

16

Why Continuous Monitoring Is Important

- Attackers were in the organization's network for extended times before being detected:
  - 63% – up to 6 months
  - 21% – 7 to 12 months
  - 16% – one year or more

Source: Cybereason Ransomware: The True Cost to Business Report, 2022

17

So continuous monitoring is easy breezy, right?

18

What should we do?

- Assess current capabilities.
- Identify the gaps.
- Develop action plans.
- Document!

19

Training Procedures

CAPINCROUSE LLP

What's the problem here?

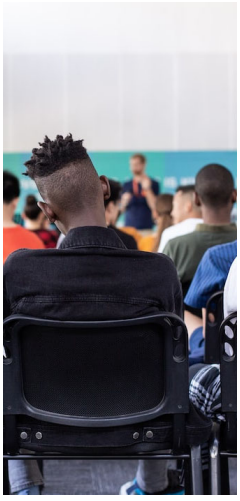
Source: Verizon Data Breach Investigations Report, 2023

21

§ 314.4(e) – Empower Your Employees

- Perform security awareness training
- Use qualified staff for the information security function
- Provide information security staff with a means to expand their knowledge

Invest in your people.



22

What makes for a good training program?

- The method
- The frequency
- The content
- Your culture

23

Invest in Technical Staff

24

Oversight of Service Providers

CAPINCROUSE

§ 314.4(f) – Oversee Your Service Providers

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

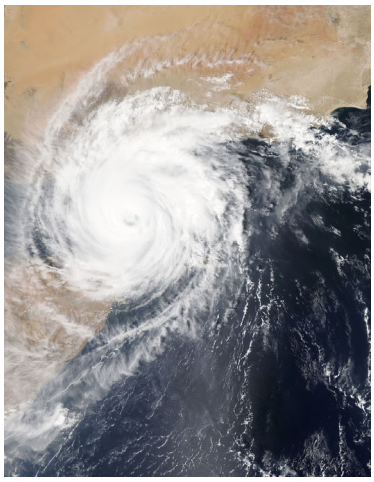
Relying on reputation alone is not sufficient due diligence for compliance.

What to Consider

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

27

What to Consider



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

28

What to Consider

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

Polling Question 3

What is your biggest struggle with vendor management?

- Understanding what to do
- Finding the time to do it
- Getting our vendors to release information
- The expertise to assess the documents received
- Other (pop it in the chat!)

30

Incident Response Planning

CAPINCROUSE

§ 314.4(h) – Develop Your Plan

(h) Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address the following areas:

(1) The goals of the incident response plan;

(2) The internal processes for responding to a security event;

(3) The definition of clear roles, responsibilities, and levels of decision-making authority;

(4) External and internal communications and information sharing;

(5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(6) Documentation and reporting regarding security events and related incident response activities; and

(7) The evaluation and revision as necessary of the incident response plan following a security event.

Source: 16 CFR 314.4(h)

32

An effective response starts now.

33

Who are you going to call?

34

Containment Strategies

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

35

Notification Requirements

36

Exercise your response muscle.

37

Polling Question 4

Do you feel ready to continue tackling compliance?

- Yes!
- No!
- (I'm crying softly to myself)

38

So how does this all tie together?

39

§ 314.4(i) – Regularly Report to Your Board

- Overall status
- Risk assessment, risk management, and control decisions
- Service providers
- Results of testing
- Security events/violations
- Suggestions for changes

40

More GLBA Resources

Access articles, recorded webcasts, and other helpful GLBA resources!

Scan the QR code or visit capincrouse.com/glba-compliance.

41

Thanks!

Allison Ward, Partner
CapinTech, a CapinCrouse Company

award@capincrouse.com
505.50.CAPIN ext. 2008

Patricia Willhite, Senior Manager
CapinCrouse LLP

pwillhite@capincrouse.com
505.50.CAPIN ext. 2030

CAPINCROUSE LLP