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

- Visit capincrouse.com/security-controls-2 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.

18 Critical Security Controls, Part 2

Allison Ward, Partner
Katie Kane, Senior Manager
8.30.23

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.

3

Polling Question 1

Do you want CPE credit?

4

Quick Recap of Part 1

CAPINTECH

What is the CIS and why use its framework?

“Making the Connected World a Safer Place”

Source: cisecurity.org

6

Tell me about Implementation Group (IG) 1.

- Minimum standards
  - 56 foundational safeguards
- Limited IT and security expertise
- Limited tolerance for downtime
- Sensitivity of data is low
- General, non-targeted attacks

7

Moving on up to IG2 (+74 safeguards).

- Help security teams cope with increased complexity
- Store and process sensitive client or enterprise data
- Loss of public confidence expected with a breach

8

And then there was IG3 (+23 safeguards).

- Requires expert support
- Subject to regulatory and compliance oversight
- Concerned with availability, confidentiality, and integrity
- Attack could cause significant harm to public
- Goal is to thwart complex attacks

9

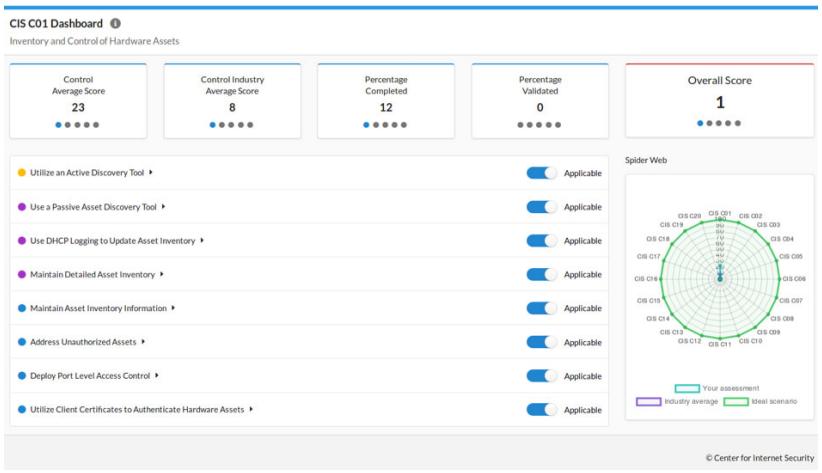
Navigator Tool

Sub	Title	Asset Type	Implementation Group:	IG1	IG2	IG3	HIPAA	NISTCSF
CIS Control 1 - Inventory and Control of Enterprise Assets Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.								
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Devices		●	●	●	●	●
1.2	Address Unauthorized Assets	Devices		●	●	●		
1.3	Utilize an Active Discovery Tool	Devices			●	●		●
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Devices			●	●		●
1.5	Use a Passive Asset Discovery Tool	Devices				●		●

Source: cisecurity.org/controls/cis-controls-navigator

10

CIS Controls Self-Assessment Tool (CSAT)

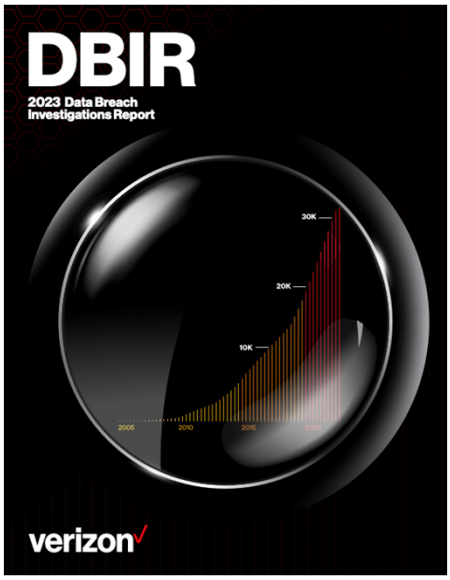


Source: cisecurity.org/insights/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls

11

A Tale of Two Studies

CAPINTECH



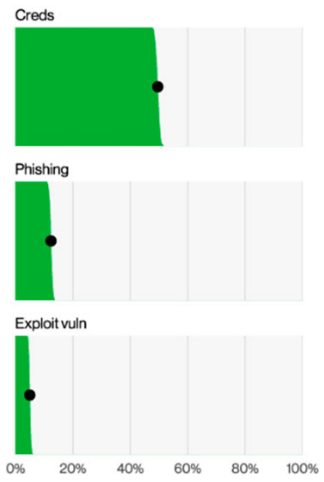
IBM Security

Cost of a Data Breach Report 2023

IBM

13

Select Enumerations for Non-Error, Non-Misuse



Source: Verizon Data Breach Investigations Report, 2023

14

This looks familiar…

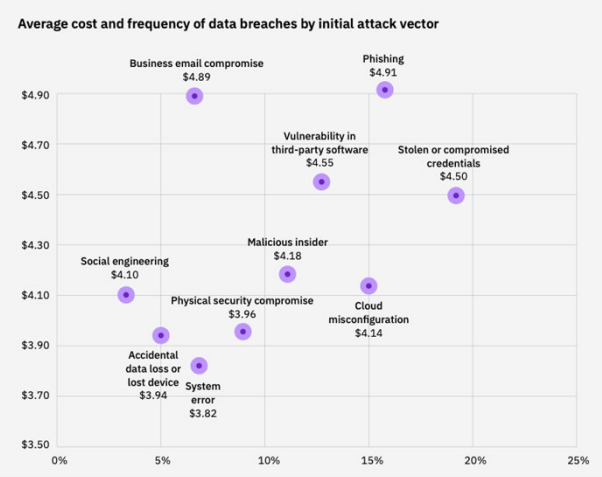


Figure 11: Measured in USD millions

Source: IBM Cost of Data Breach Report, 2022

15

Are you getting déjà vu?

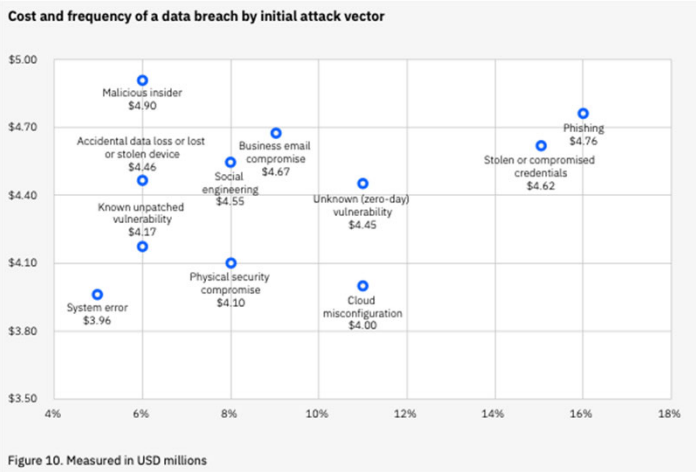
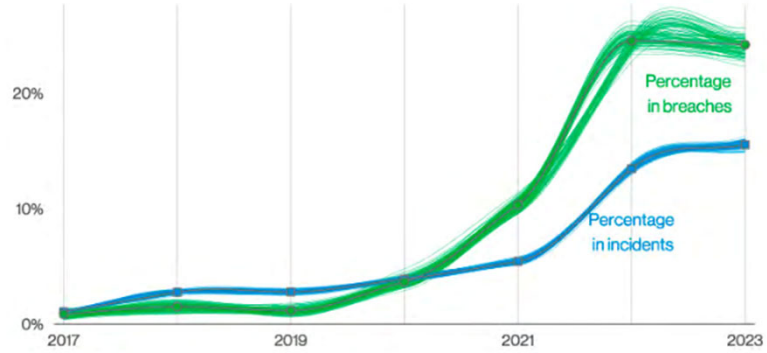


Figure 10. Measured in USD millions

Source: IBM Cost of a Data Breach Report, 2023

16

Ransomware's not a problem… just kidding!



Source: Verizon Data Breach Investigations Report, 2023

17

Top Ransomware Routes

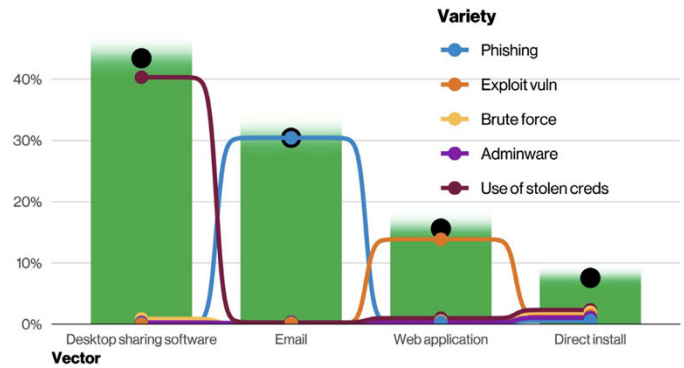
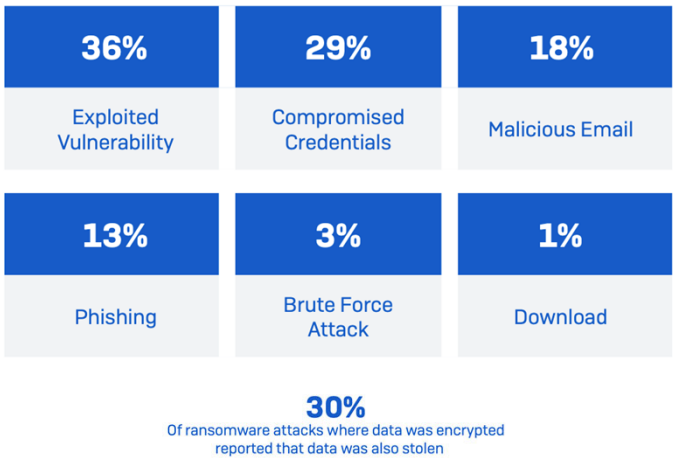


Figure 39. Select action varieties within vectors in System Intrusion Ransomware incidents (n=1,032)

Source: Verizon Data Breach Investigations Report, 2022

18

Okay, one more study.



Source: Sophos The State of Ransomware 2023

19

Bad actors don't just want our credit card data.

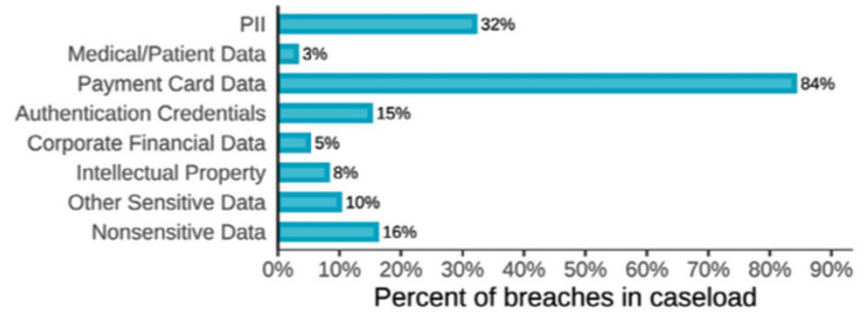


Figure 26. Compromised Data Types (2008 DBIR Figure 20)

Source: Verizon Data Breach Investigations Report, 2022

20

Top Compromised Data Sets In 2021

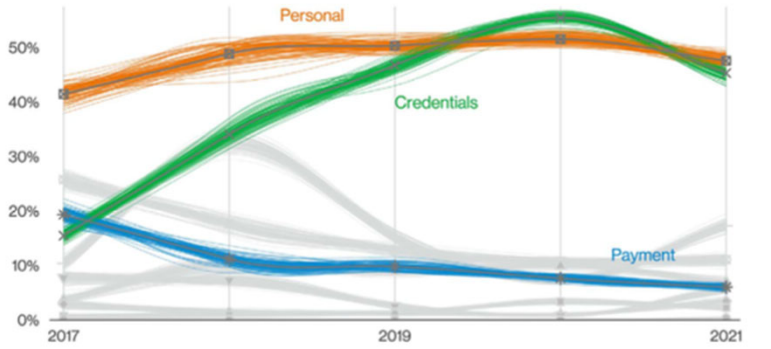


Figure 27. Top Confidentiality data varieties over time in breaches

Source: Verizon Data Breach Investigations Report, 2022

21

And it looks like nothing has changed.

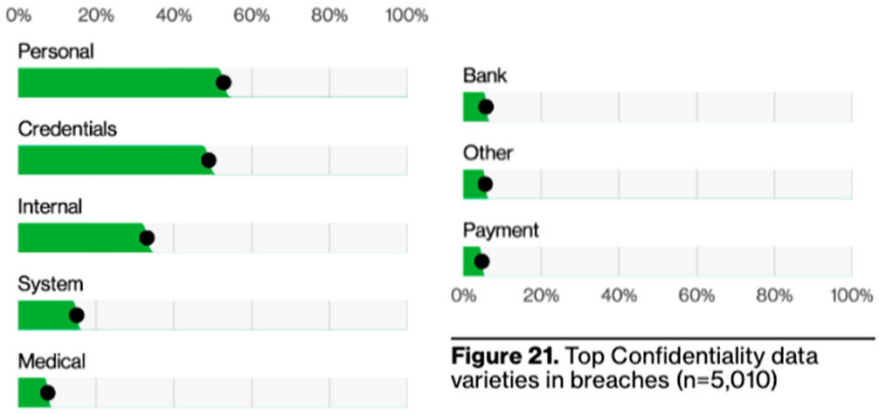
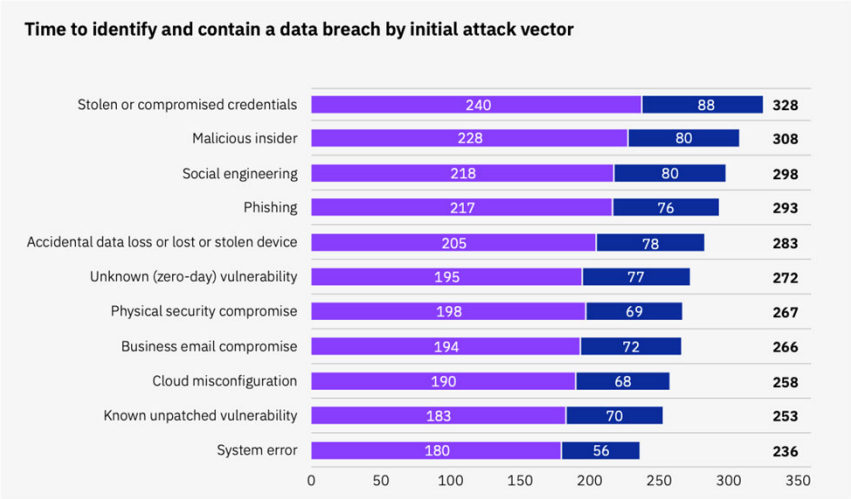


Figure 21. Top Confidentiality data varieties in breaches (n=5,010)

Source: Verizon Data Breach Investigations Report, 2023

22

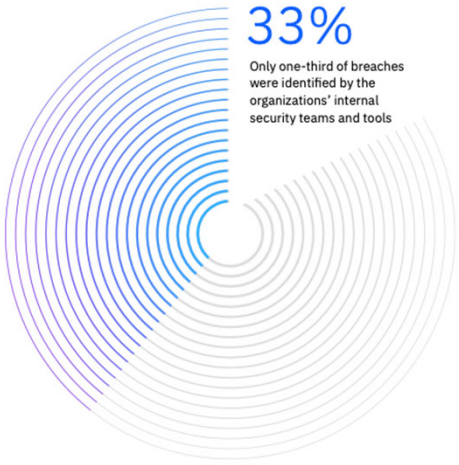
With all the practice, our response must be good.



Source: IBM Cost of a Data Breach Report, 2023

23

With all the practice, our response must be good.



Source: IBM Cost of a Data Breach Report, 2023

24

What decreased the cost and impact of a breach?

- Usage of automation and artificial intelligence
  - *$1.76 million cost savings*
  - *Identification and containment 108 days faster*
- Incident response teams and testing
  - *$1.49 million cost savings*
  - *Identification and containment 54 days faster*

Source: IBM Cost of Data Breach Report, 2023

25

Other Factors that Decrease the Cost

- Employee training
- Encryption
- Centralized reporting
- Threat hunting
- Identity and access management (IAM)
- Endpoint detection and response
- Data security and protection software
- Board-level oversight and appointed CISO

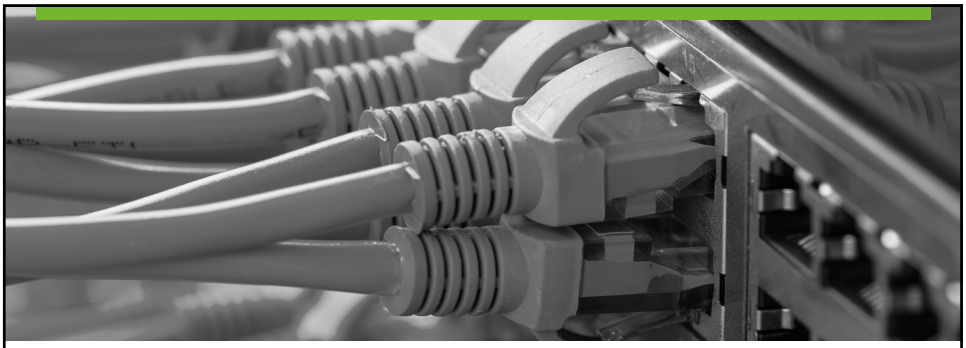
Source: IBM Cost of Data Breach Report, 2023

26

Polling Question 2

What area concerns you most about your control framework?

27



Asset Control

CAPINTECH

Hardware Management

- Maintain a network diagram
- Utilize active and passive discovery tools
- Uninstall and disable unnecessary services

29

Control Mobile Devices

- Lockout configurations
- Remote wipe capabilities
- Containerization

30

Software Management

- Utilize automated software inventory tools
- Implement software allow lists
- Implement web filtering

Data Management

- Classify data
- Document flow
- Encrypt in transit and at rest
- Deploy data loss prevention

32

Authentication and Access

CAPINTECH

Authentication and Access

- Inventory service accounts
- Centralize
- Utilize role-based access

Traditional Management or IAM: What to Do?

35

Polling Question 3

Are you using an identity access management (IAM) solution?

36

Network Infrastructure

- Consider segmentation and least privilege
- Implement secure remote authentication

37

What is zero trust architecture?

“Never trust. Always verify.”

- John Kindervag, then at Forrester Research

38

Vulnerability Management and Response

CAPINTECH

Continuous Vulnerability Management

- Automate scanning of internal and external assets
- Perform penetration testing
- Remedy identified issues

40

Risk-Based Vulnerability Management

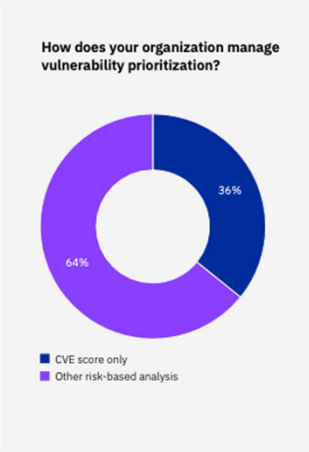


Figure 45. Percentage of all organizations

Figure 46. Measured in USD millions

Source: IBM Cost of a Data Breach Report, 2023

41

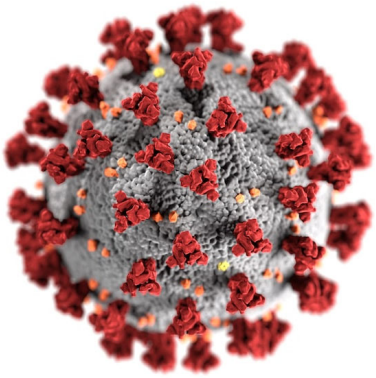
Risk-Based Vulnerability Management

- Prioritize risks by patch type, system, and endpoint
- Help security teams triage
- Allows more proactive management vs. reactive

42

Malware Defenses

- Auto-scan removable media
- Centralize management
- Use behavior-based
  - Next generation anti-virus (“NGAV”)
- Application allow listing



43

Network Monitoring and Defense

- Centralize alerting
- Deploy intrusion detection and prevention systems
  - Host-based
  - Network
- Monitor internal traffic

44

Enhance Web and Email Controls

- Blocking unnecessary file types
- Scanning attachments for viruses
- Sandboxing
- Web filtering

Alphabet Soup: Detection/Response Solutions

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

46

Audit Log Management

- Collect
- Centralize
- Review

47

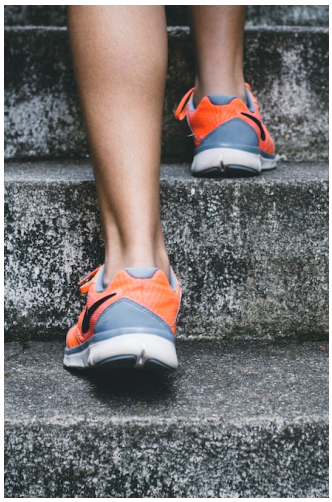
Incident Response

- Establish a process
  - Define incident vs. event
  - Key roles and responsibilities
  - Communication
  - Post-incident reviews

48

Practice makes ~~perfect~~ better.

- Conduct exercises
- Test your backups!



49

Polling Question 4

Based on what you've heard in this webcast and Part 1, are you interested in using the CIS Top 18 controls framework?

50

Other

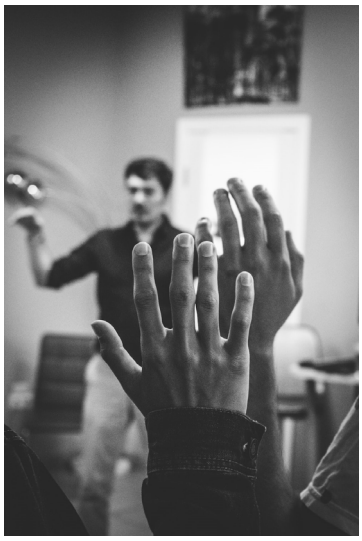
CAPINTECH

Security Awareness and Skills Training

- Train based on role and skill needs

Note: 8 of the 9 controls in the Security Awareness and Skills Training section are considered baseline.

Employee awareness is an essential protection.



Service Provider Management

- Formalize a policy
- Classify vendors
- Hold them responsible by contract
- Assess and monitor
- Decommission securely

53

You Could Win a Free CapinTech Cyber Checkup or Phishing Test!

- Receive one entry for each 2023 CapinTech Cyber Series webcast you:
  - Attend live, or
  - Watch the recording of within one week of the webcast date
- Winner selected after the final webcast of the 2023 series

54

Questions?

Thanks!

Allison Ward
Partner, CapinTech

award@capincrouse.com
505.50.CAPIN ext. 2008

Katie Kane
Senior Manager, CapinTech

kkane@capincrouse.com
505.50.CAPIN ext. 2007

CAPINTECH