

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

- Visit capincrouse.com/ransomware-update 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.



Ransomware Update

Allison Ward, Partner
3.22.2023



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

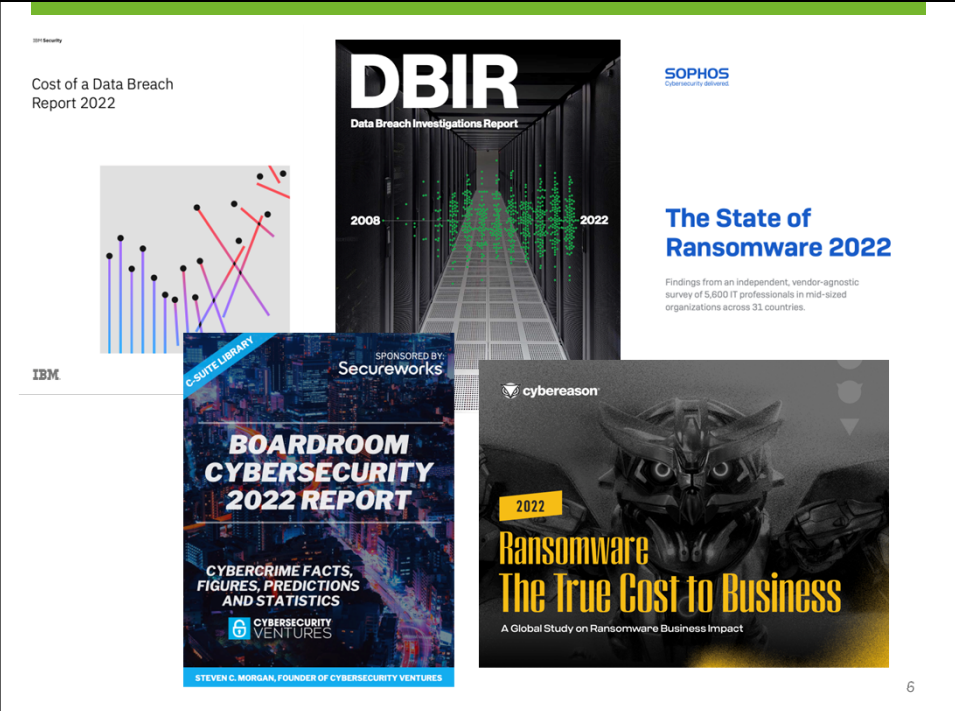
Polling Question 1

Do you want CPE credit?

4

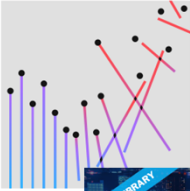


Ransomware Landscape




IBM Security

Cost of a Data Breach Report 2022




IBM



DBIR
Data Breach Investigations Report


2008 2022



SOPHOS
Cybersecurity delivered

The State of Ransomware 2022


Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries.



C-SUITE LIBRARY
SPONSORED BY:
Secureworks


BOARDROOM CYBERSECURITY 2022 REPORT

CYBERCRIME FACTS,
FIGURES, PREDICTIONS
AND STATISTICS



CYBERSECURITY
VENTURES

STEVEN C. MORGAN, FOUNDER OF CYBERSECURITY VENTURES



cybereason

2022

Ransomware The True Cost to Business

A Global Study on Ransomware Business Impact

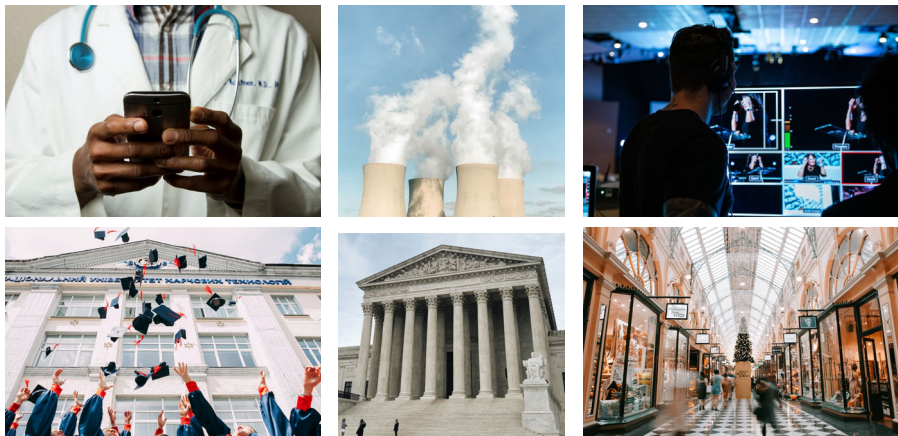
6

First, why is ransomware so impactful?

- Three-fold impact:
 - Confidentiality, integrity, and availability (CIA triad)
- Attackers don't have to find data with a specific value
 - Can interrupt operations
 - Makes any organization a perfect target
- No-win situation when attacked

7

Who is being targeted?



8

They Want More Than Our Credit Card Data

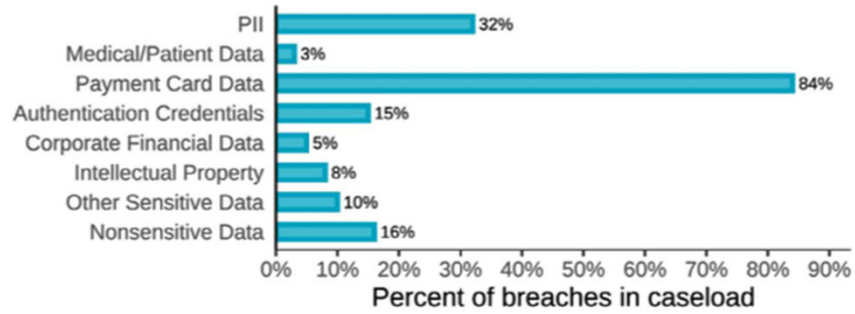


Figure 26. Compromised Data Types (2008 DBIR Figure 20)

Verizon Data Breach Investigations Report, 2022

Top Compromised Data Sets In 2021

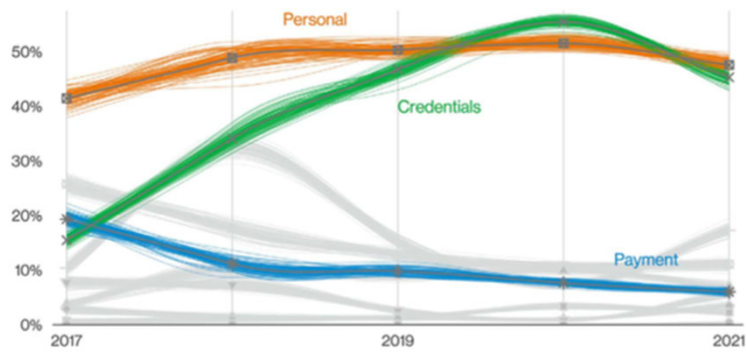
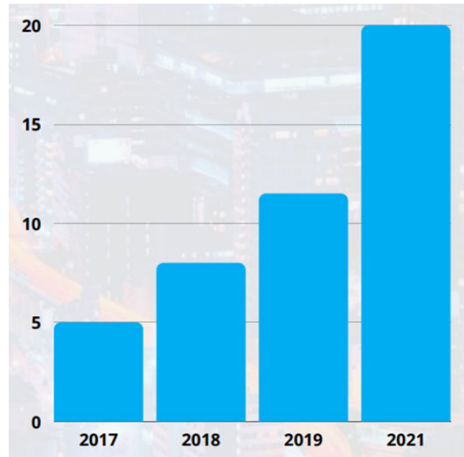


Figure 27. Top Confidentiality data varieties over time in breaches

Verizon Data Breach Investigations Report, 2022

Same threats, different day... but worse!

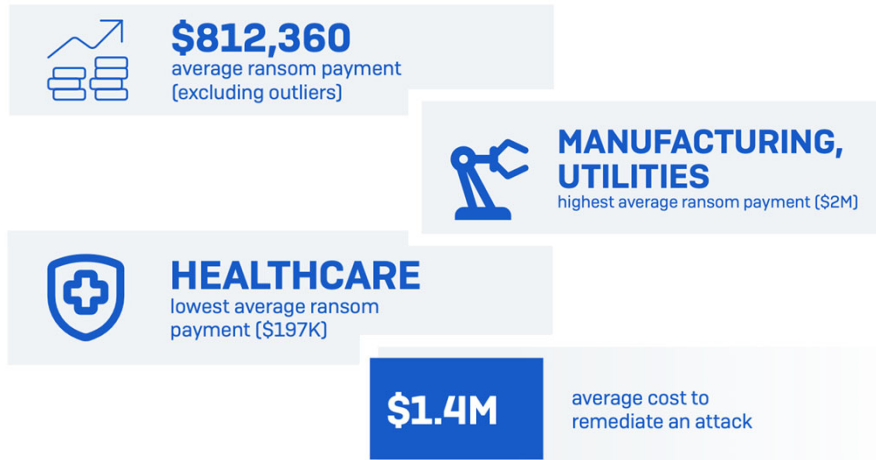


Global ransomware costs are predicted to grow from \$325 million (2015) to \$265 billion (2031).

Cybersecurity Ventures Boardroom Cybersecurity Report, 2022

11

Same threats, different day... but worse!



Sophos The State of Ransomware Report, 2022

12

Same threats, different day... but worse!

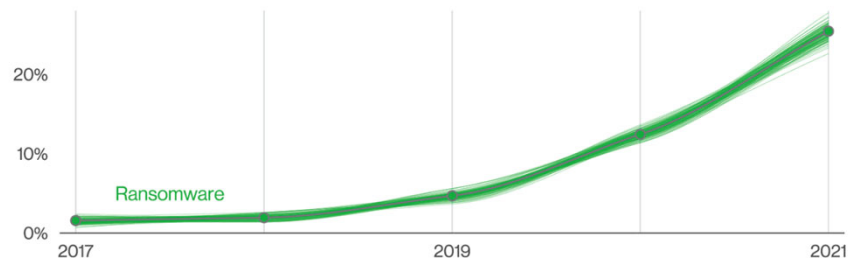


Figure 6. Ransomware over time in breaches

Verizon Data Breach Investigations Report, 2022

13

Sophos and Cybereason Echoed the Sentiment

- 66% of organizations hit in 2021
 - *Up from 37% in 2020*
- 65% of attacks successfully encrypted data in 2021
 - *Up from 54% in 2020*
- 73% of organizations targeted by at least one attack
 - *33% increase year-over-year*

14

Polling Question 2

What is your experience with ransomware?

15

It Doesn't Pay to Pay...

- ... but we still do:
 - 49% to avoid loss of revenue
 - 41% to expedite recovery
 - 34% because they were too short-staffed to respond effectively
 - 28% to avoid downtime that could result in human harm
 - 27% hadn't backed up their data

Cybereason Ransomware: The True Cost to Business Report, 2022

16

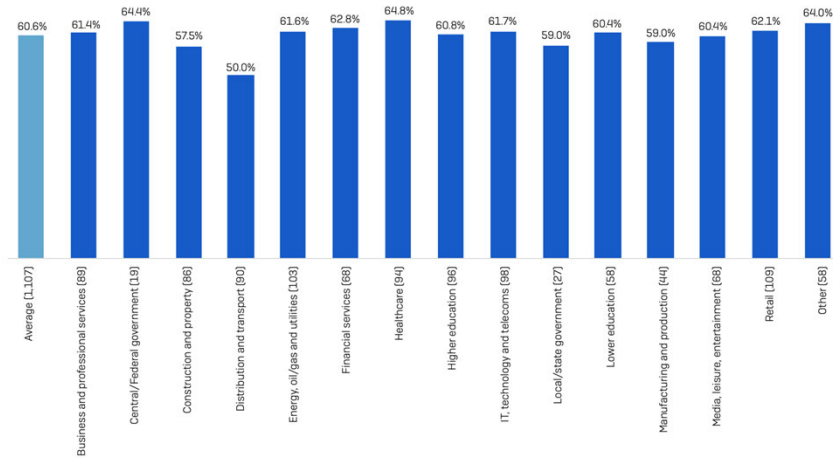
It Doesn't Pay to Pay...

- Of those who paid:
 - 80% were victims of a second attack
 - 68% were hit again less than a month later for a higher ransom
 - 54% reported system issues or corrupted data after decryption
 - 42% were able to restore all systems and data (*down from 51% in prior report*)

Cybereason Ransomware: The True Cost to Business Report, 2022

17

Percentage of Data Restored After Paying Ransom



Sophos The State of Ransomware Report, 2022

18

Double Extortion Increasingly Popular

- As of Q1 2021, 77% of attacks included this tactic
- Top data sets pursued:
 - 54% - account credentials, sensitive customer data
 - 34% - personally identifiable information (PII)
 - 30% - intellectual property
 - 27% - protected health information (PHI)

Cybereason Ransomware: The True Cost to Business Report, 2022

19

Resolution Can Be Long and Arduous

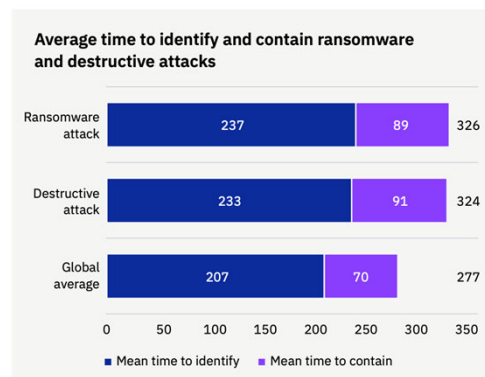


Figure 31: Measured in days

49 days

Ransomware breaches took 49 days longer than average to identify and contain.

IBM Cost of Data Breach Report, 2022

20

Resolution Can Be Long and Arduous

- 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

Cybereason Ransomware: The True Cost to Business Report, 2022

21

Poor Response Can Lead to Significant Impacts

- Cost of the ransom
- Disruption of operations, leading to lost revenue
- Reputational damages and loss of support
- Loss of key executives and employee layoffs
- Loss of customers and strategic partners
- Viability of the business

22

“Overall, the cost of preventing a ransomware attack from being successful is lower than the combined cost of paying the ransom and all the associated costs of recovery”.

Cybereason Ransomware: The True Cost to Business Report, 2022

23



What Do We Do?

Ransomware Prevention

“Ransomware is not the real problem. It’s how ransomware got in.
It’s how ransomware got admin.”

– Roger A. Grimes, Data-Driven Security Evangelist, KnowBe4

25

Ransomware Routes

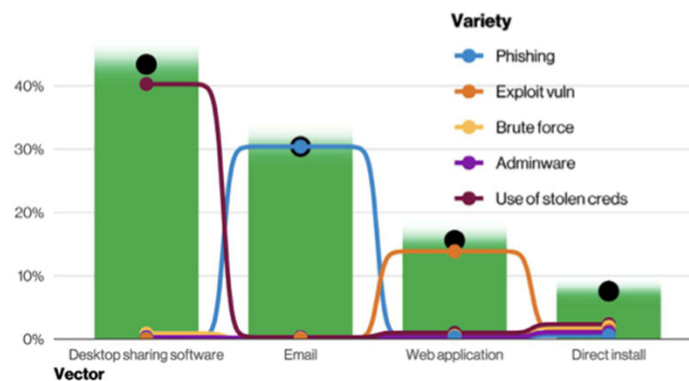


Figure 39. Select action varieties within vectors in System Intrusion Ransomware incidents (n=1,032)

Verizon Data Breach Investigations Report, 2022

26

“Had we known that what was true nine years ago would still be true today, we could have saved some time by just copying and pasting some text. Oh well...”

Verizon Data Breach Investigations Report, 2022

27

Polling Question 3

**What is the most probable
“route” for ransomware in your
environment?**

28

How do we protect ourselves?

- Restricting common pathways for ransomware
- Limiting administrative capabilities where we can
- Layered controls to increase steps in the event chain
 - *Basic hygiene practices*
- Empower our people with knowledge
- Plan for the inevitable attack

29

The Breach Event Chain

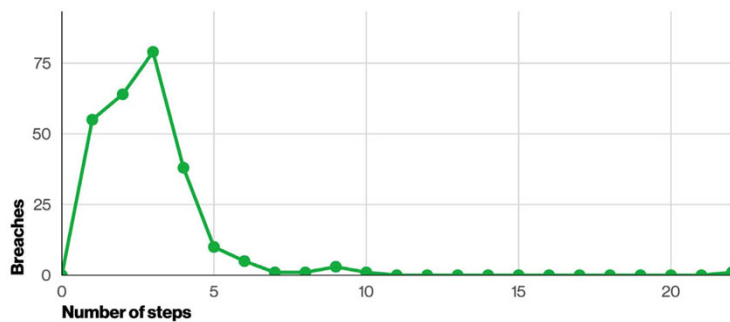


Figure 30. Number of steps per breach in non-Error breaches (n=258)

Verizon Data Breach Investigations Report, 2022

30

Email: A Common Pathway

- Establish controls surrounding incoming emails
 - Establish strong filtering of malicious email
 - Block executables from running
 - Prepend external emails with a disclaimer (awareness)
 - Strip links from emails
- Consider enhanced filtering



31

Do you recognize your staff as a control?

- 81% know attachments can be malicious
- 77% know emails can be spoofed

But only...

- 52% know familiar contacts aren't automatically safe
- 36% know that internal emails could be dangerous
- 37% know that cloud files can be malicious

Proofpoint State of the Phish Report, 2022

32

You must combat social engineering!

- Providing frequent training
- Recognizing indicators of social engineering
- Spotting fake URLs
- Understanding evolving tactics (e.g., push fatigue)



33

Vulnerability Exploitation: A Common Pathway

- Inventory your assets
- Install anti-malware protection where you can
- Apply security updates religiously
- Monitor for industry or vendor alerts

34

Patching and Security Updates

- Limit software on servers and workstations.
 - Less software = less patching
- Limit access rights – don't let people install software without IT's knowledge!
- Implement centralization and reporting, as feasible:
 - Application whitelisting
 - Automated reports of installed software
 - Centralized tools for pushing out patches

35

Anti-malware Protections

- Something is better than nothing
- macOS is not immune
- Look for “behavioral-based” solutions (next-gen anti-virus, aka NGAV)
- Centralize where possible
- Monitor – don't set and forget

36

Implement Strong Authentication

- Strong passwords
 - Not reused
 - Not easy to guess
- Lockout settings
- Multi-factor authentication
 - *Reconsider challenge questions*



37

Polling Question 4

Are you using multi-factor authentication on your systems?

38

Implement Strong Authentication

- Inventory where people can login
- Restrict administrative and other elevated rights
 - Consider locking accounts during holidays or weekends
- Monitor activity with alerts or logs

39

Remote Access: A Common Pathway

- Discontinue use of unsecured Remote Desktop Protocol (RDP) for access.
- Use strong authentication – MFA is non-negotiable!
- Monitor activity and enable alerts.
- Don't make exceptions for vendors.
- Understand how people connect.

64%
ransomware came
from third-party
supply chain

Cybereason Ransomware: The True Cost to Business Report, 2022

40

Detection: do you have sufficient visibility?



41

Backups: It's More Than Just Having Them

- Ensure backups cannot be impacted by ransomware
 - Make immutable
 - Create physical offline copies
 - Utilize logical air gapping
- Test the ability to restore critical data from backups

42

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?

43

Cyber insurance: do you need it?



44

Create and Walk Through Your Plan... Now

- Know what to do *before* it happens.
- Would you pay the ransom?
- Who would you contact?
 - Insurance and legal
 - Ransomware specialists
 - Regulatory bodies
 - Law enforcement



45

Create and Walk Through Your Plan... Now

- Do you have alternate contact mechanisms?
 - Email likely down
 - Voice-over-IP systems likely down
- How do you determine what the issue is?
- Who is responsible for what?

46

Create and Walk Through Your Plan... Now

- Where do you need to disconnect things on network?
- What passwords do you need to change?
- Are you repairing or rebuilding?
- What legal impacts are there related to the breach?
- How are you retaining documentation?

47

Conduct Tabletop Discussions



48

Join Us On May 24 to Learn About Critical Security Controls

Free Cyber Series Webcast

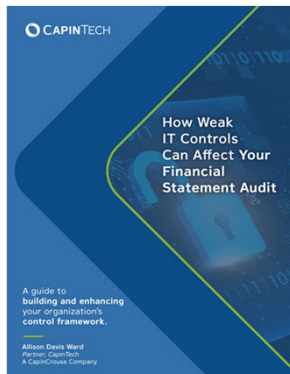
18 Critical Security Controls – Part 1

Wednesday, May 24
1:00 – 2:00 p.m. EDT

Scan the QR code or visit
capincrouse.com/events to register!



New E-book Now Available!



Download your free copy!
Scan this QR code or visit
capincrouse.com/it-controls

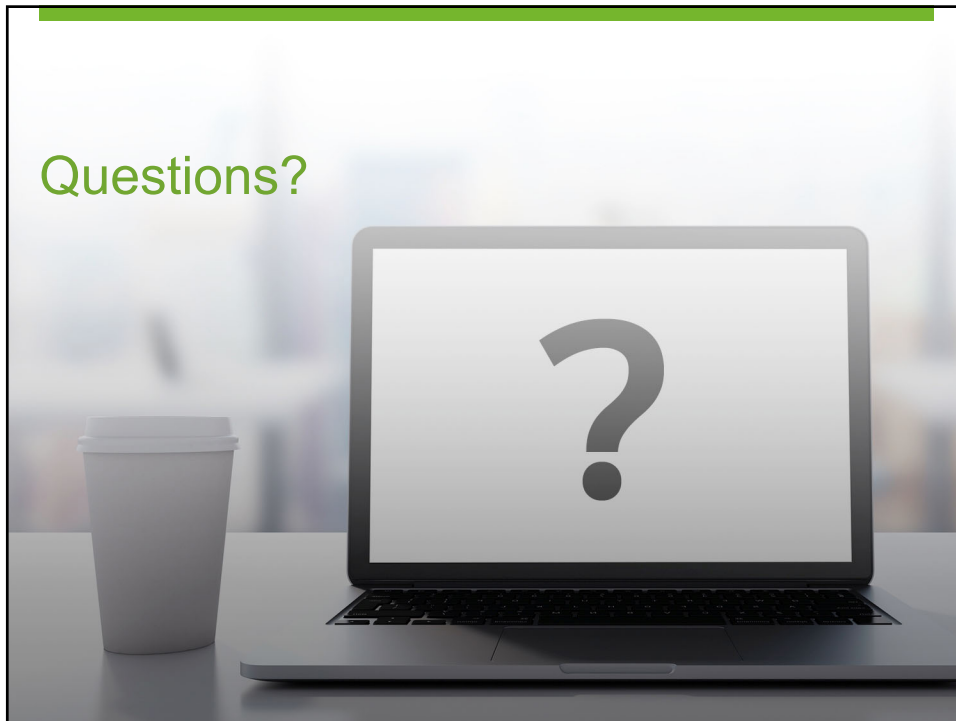
You Could Win a Free CapinTech Cyber Checkup!

- 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



51

Questions?





Thanks!

Allison Ward, Partner
CapinTech

✉ award@capincrouse.com

📱 505.50.CAPIN ext. 2008

© 2023 Capin Technology LLC

