Webinar

Cyber Liability Insurance Simplified

January 20, 2022

Newfront

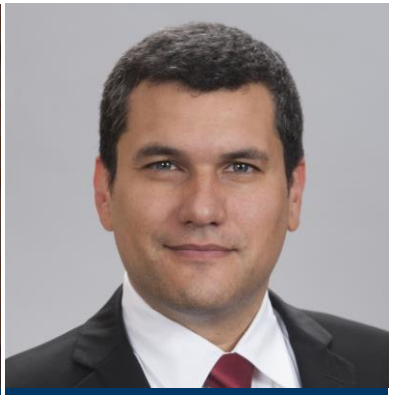
Today’s Topics

- Cyber security trends
- Cyber liability insurance
- Preparedness and response plans
- Litigation best practices
- Insurance Recovery

Speakers

Casie Collignon
Cybersecurity and Privacy, Partner
Baker & Hostetler LLP

Tyler Gerking
Insurance Recovery, Partner
Farella Braun + Martel LLP



M. Scott Koller
Privacy and Data Security, Partner
Baker & Hostetler LLP

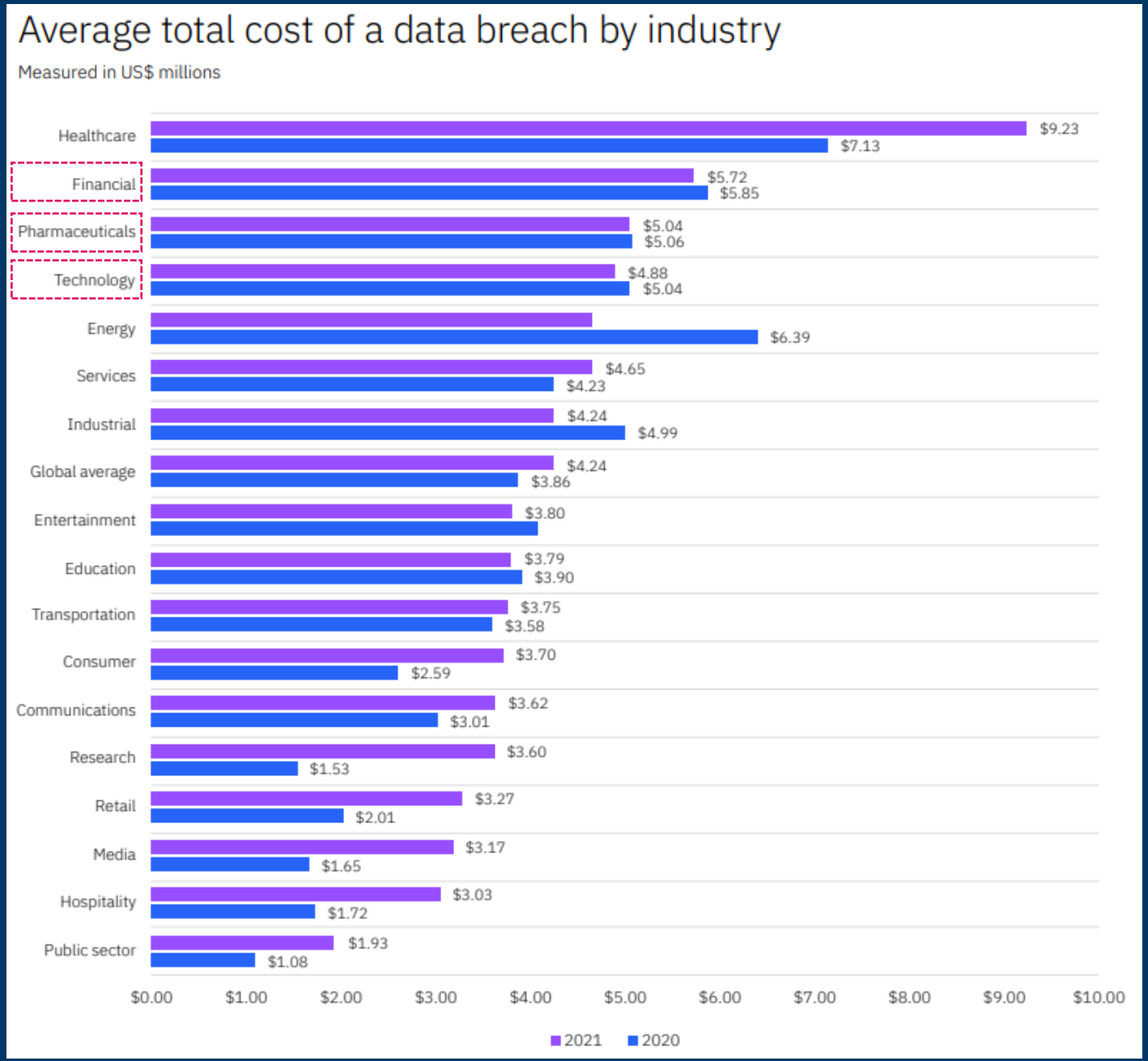
By the Numbers

Newfront

7.8%	ransomware was a factor in the breach
$4.6m	average total cost of a ransomware breach
1.0%	increase in average total cost of a breach from ‘20 to ‘21
$4.24m	average total cost of a data breach
287	average number of days to identify and contain a data breach
$1.07m	difference where remote work was a factor in causing the breach

Setting the Stage

Many of you joining today are in the top industries in average total cost



Source: IBM Cost of a Data Breach Report 2021

Setting the Stage

Audience Poll:

When data breaches started to become an insurable risk, the majority of concern was on notification costs… please select the one elements that makes up the largest category for the average data breach:

- Detection and escalation
- Notification
- Post breach response
- Lost business cost

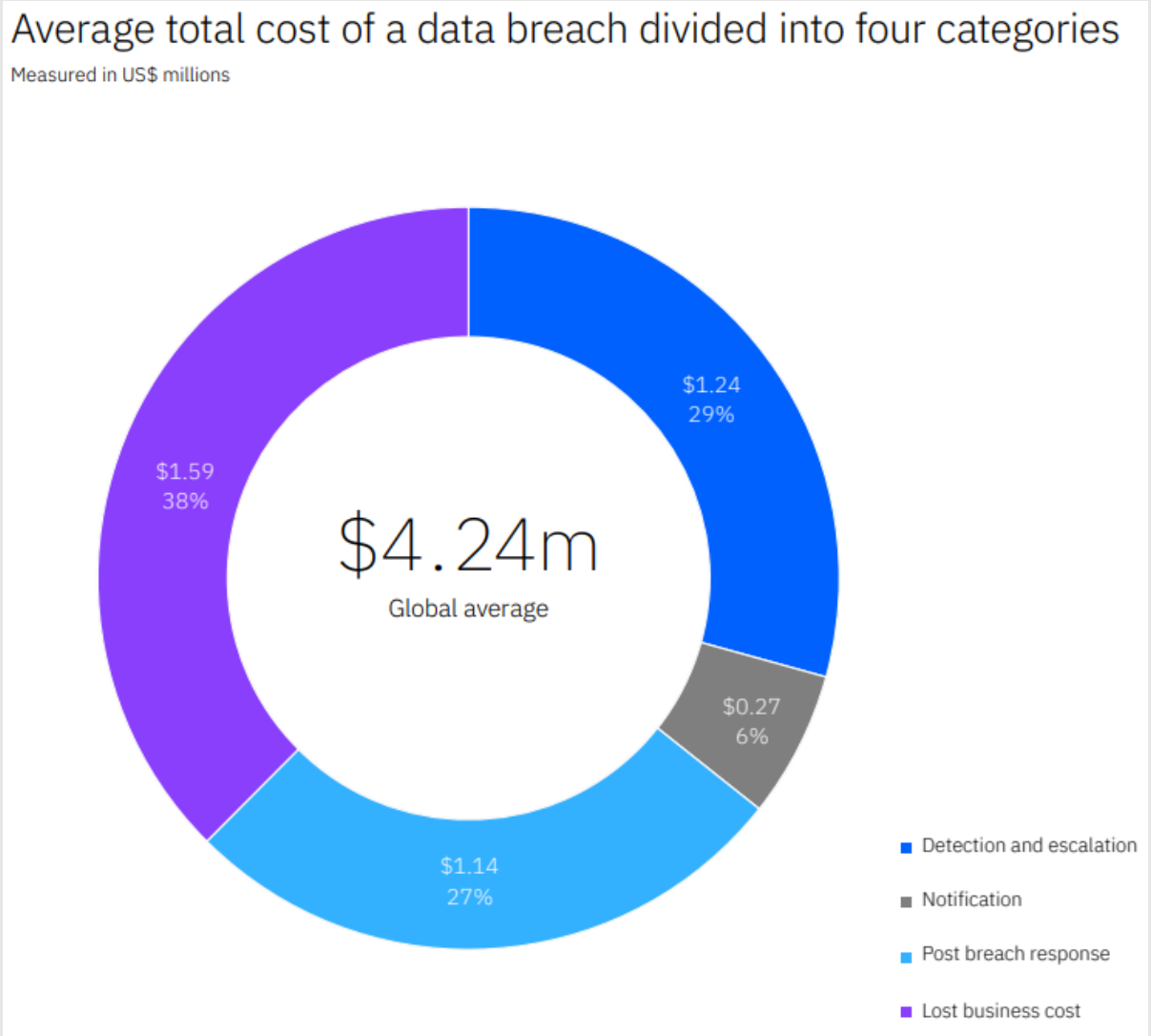
Source: IBM Cost of a Data Breach Report 2021

Setting the Stage

Audience Poll:

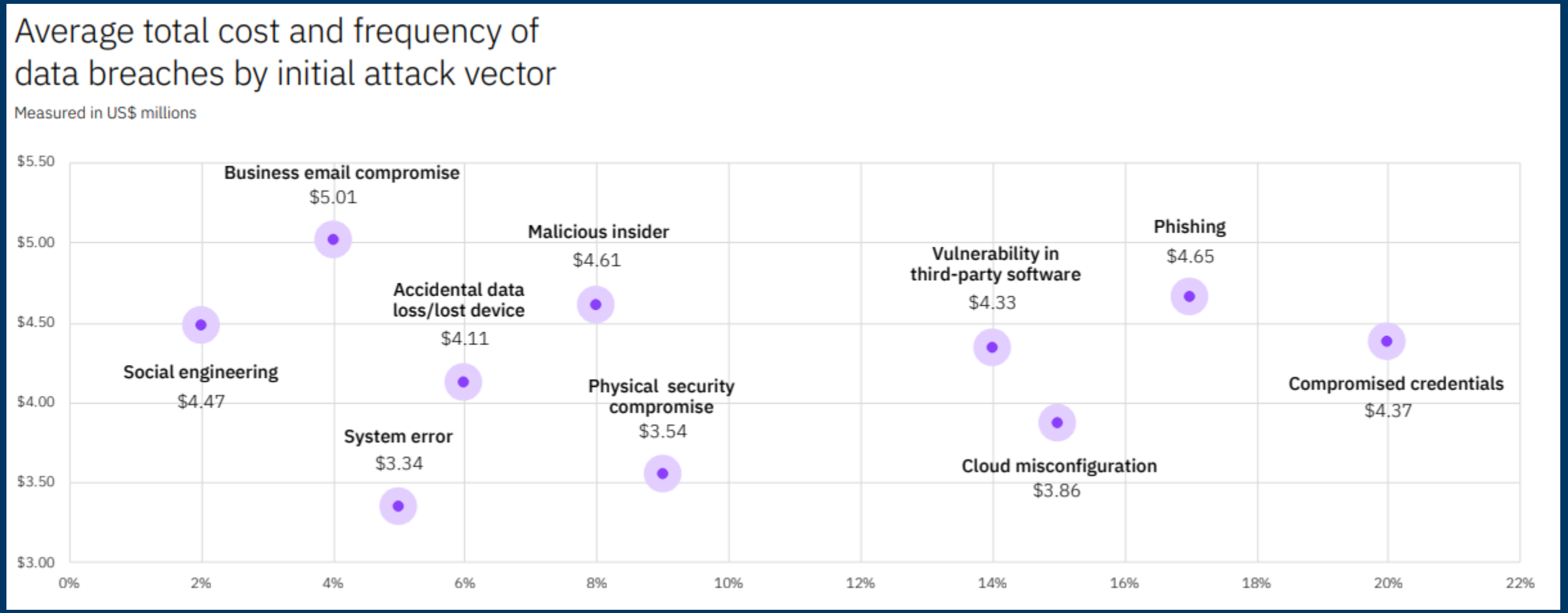
When data breaches started to become an insurable risk, the majority of concern was on notification costs… please select the one elements that makes up the largest category for the average data breach:

- Detection and escalation
- Notification
- Post breach response
- Lost business cost



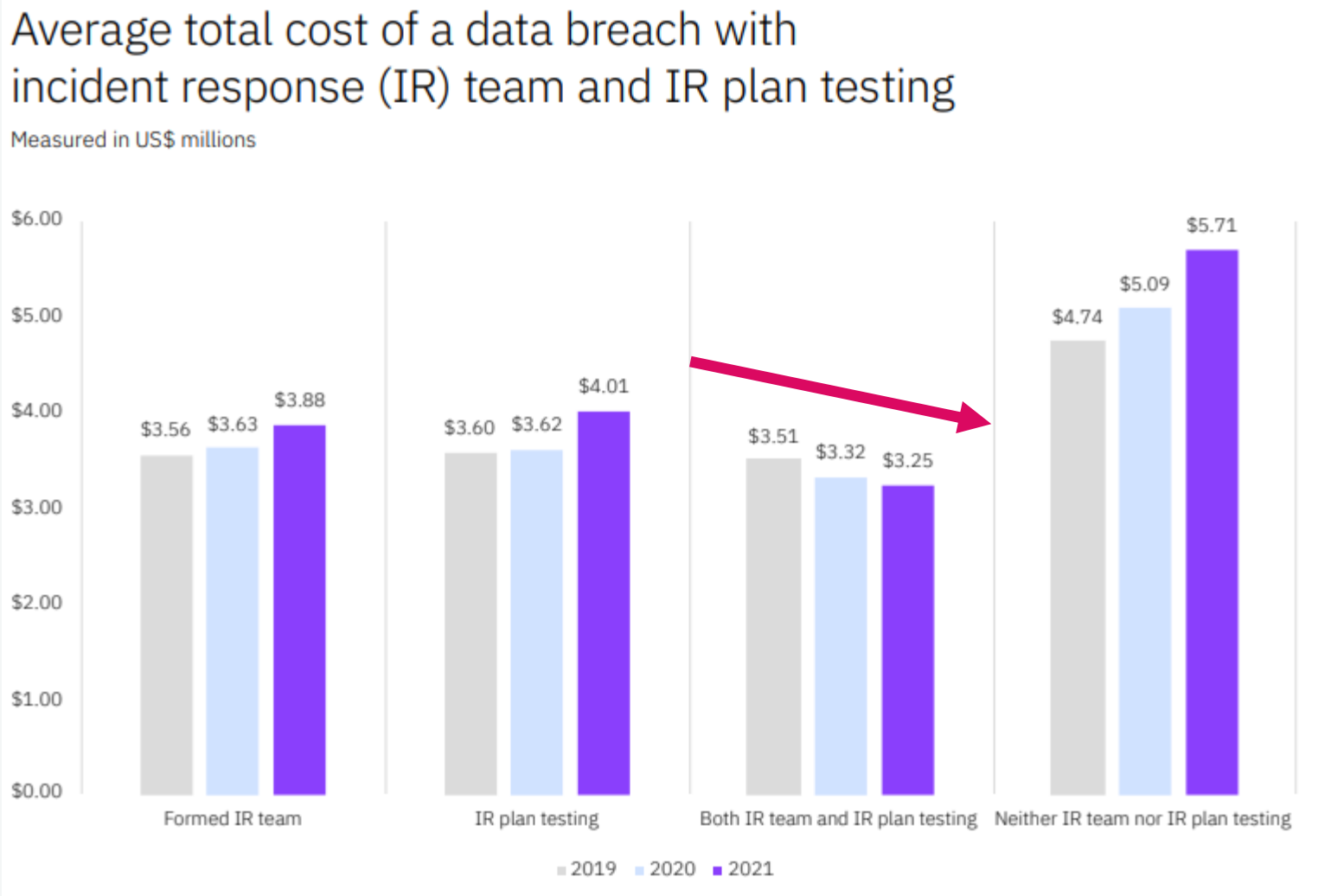
Source: IBM Cost of a Data Breach Report 2021

Setting the Stage



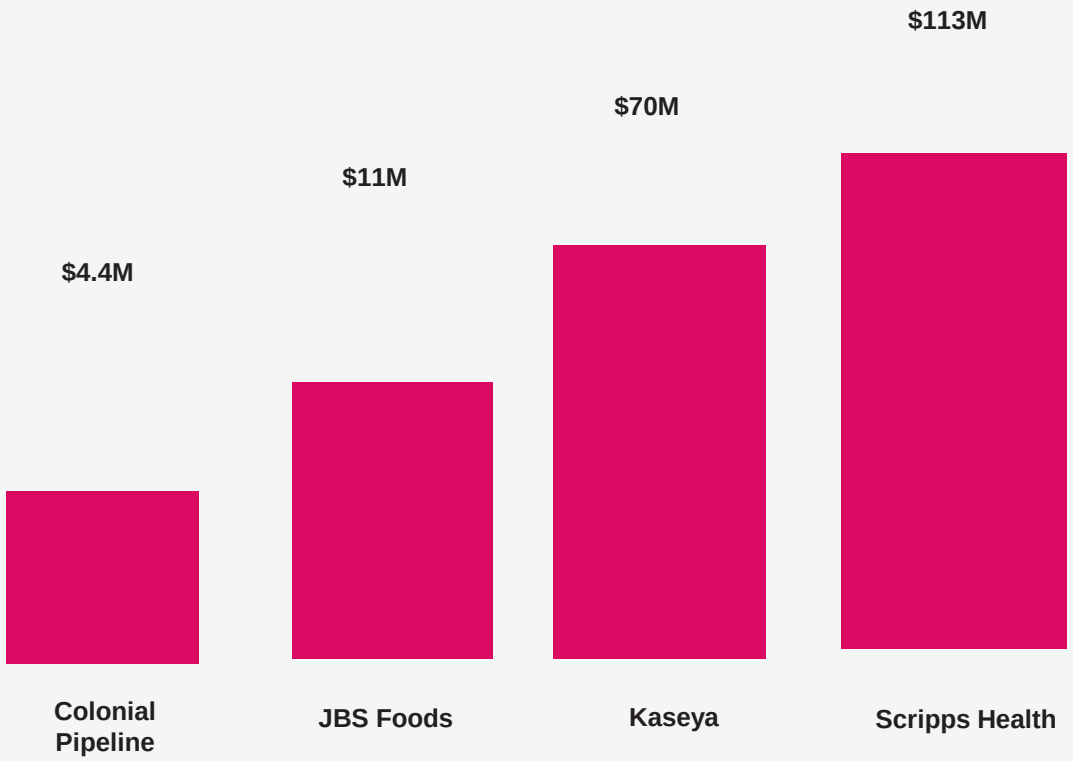
Source: IBM Cost of a Data Breach Report 2021

Setting the Stage



Source: IBM Cost of a Data Breach Report 2021

Ransom Demands In 2021



Ransom demands of $1M or more are now more common.

For example, the demand on the recent attack on Kaseya is reported at $70M. JBS meat supplier paid an $11M demand. Colonial Pipeline paid a $4.4M demand, yet the Department of Justice recovered approximately $2.3M of it.

Losses sustained by Scripps Health is expected to exceed $113M.

What is “Cyber” Insurance?

“Cyber” Insurance protects companies against losses and claims arising from data security breaches and many other risks

- First-party losses due to data security breaches
- Third-party liability claims arising from data security breaches and many other risks

Until Recently, the cyber insurance market was very competitive.

- Many new coverages were added
- Policies include a lot of the same types of coverages but are not standard.

In the past one to two years, the cyber insurance market has become much harder in light of numerous large losses and events:

- Higher premiums
- New coverage limitations
- Coverage terms less negotiable

Potentially Covered Losses and Liabilities

First Party Losses

Security event or privacy event

- PII or corporate confidential information

Cyber extortion / Ransomware

- Response expenses
- Ransom payments

Response expenses

- Crisis management/PR
- Forensic investigation
- Legal advice regarding notification requirements and liability exposures
- Breach notification
- Credit monitoring
- Call center
- Data restoration

- **Bricking (property damage to computer hardware)**
- **Crime / Social engineering**
- **Lost trade secrets?**
- **Notice to insurer and consent to lawyers and vendors**

Potentially Covered Losses and Liabilities

First Party Losses (cont.)

Business Interruption

Four types	Key Issues

• Security events
  • Insured's own system
  • Third-party system (dependent business)
• System Failure
  • Insured's own system
  • Third-party system (dependent business
	• Total shutdown vs. partial slowdown
	• Waiting period
	• Period of restoration
	• Consequential losses / contractual losses

Potentially Covered Losses and Liabilities

Newfront

Third-party claims

Types of claims

- Defense costs and liability in third-party actions (e.g., consumers class actions, corporate customer claims)
- Regulatory scrutiny / investigation / fines and penalties (OCR, HHS, FTC, state AG, SEC)
- PCI-DSS Assessments

Defense cost issues

- Duty to defend vs. duty to reimburse
- Defense counsel selection
- Defense cost allocation between covered and non-covered claims

Other coverages often combined with cyber

- Tech E&O
- Media Liability
- Bodily injury

BakerHostetler

2021 DATA SECURITY INCIDENT RESPONSE REPORT

Digital Assets and Data Management – Disruption and Transformation

1,250+

Incidents in 2020

U.S. Breach Notification Law Interactive Map

bakerlaw.com/BreachNotificationLawMap

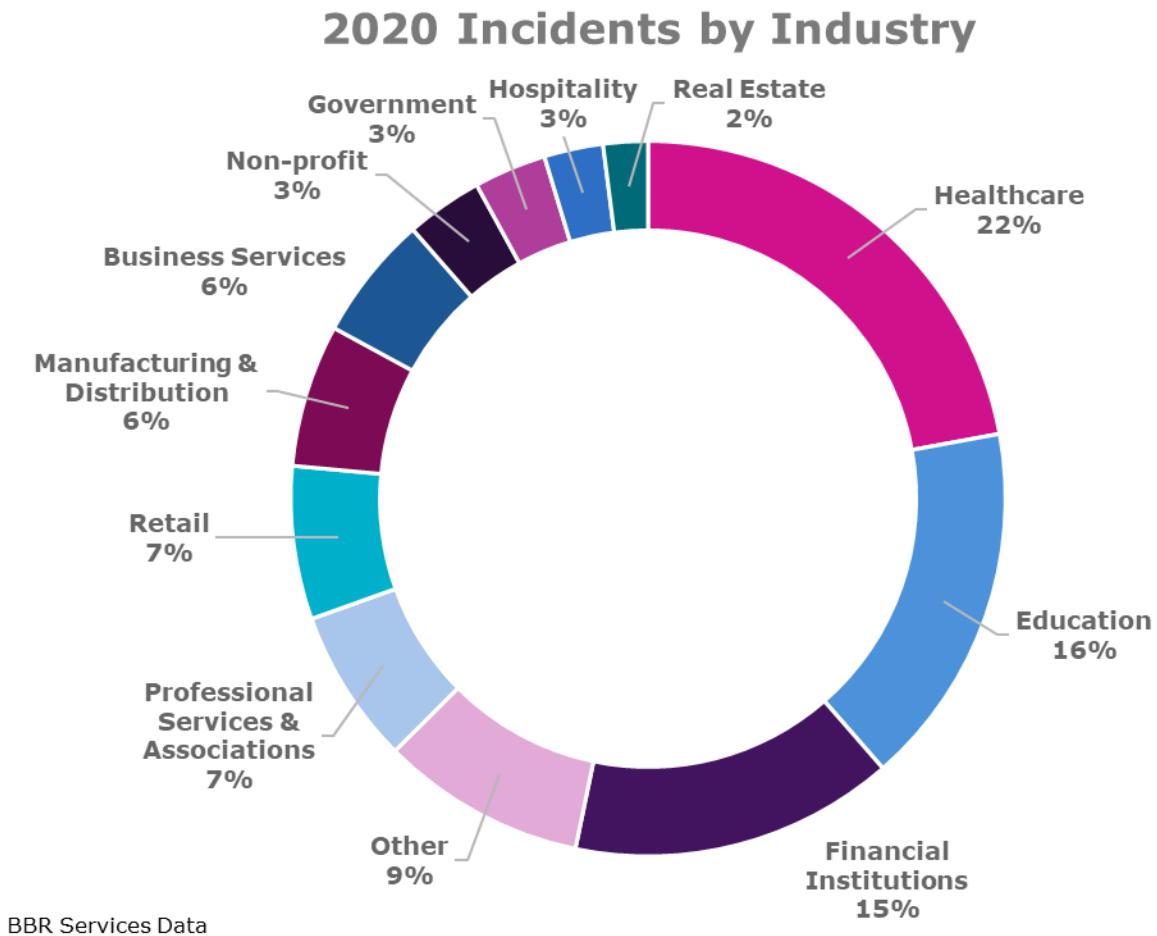
EU GDPR Data Breach Notification Resource Map

bakerlaw.com/EUGDPRResourceMap

For the latest, visit our blog

bakerdatacounsel.com

2020 Incidents by Industry



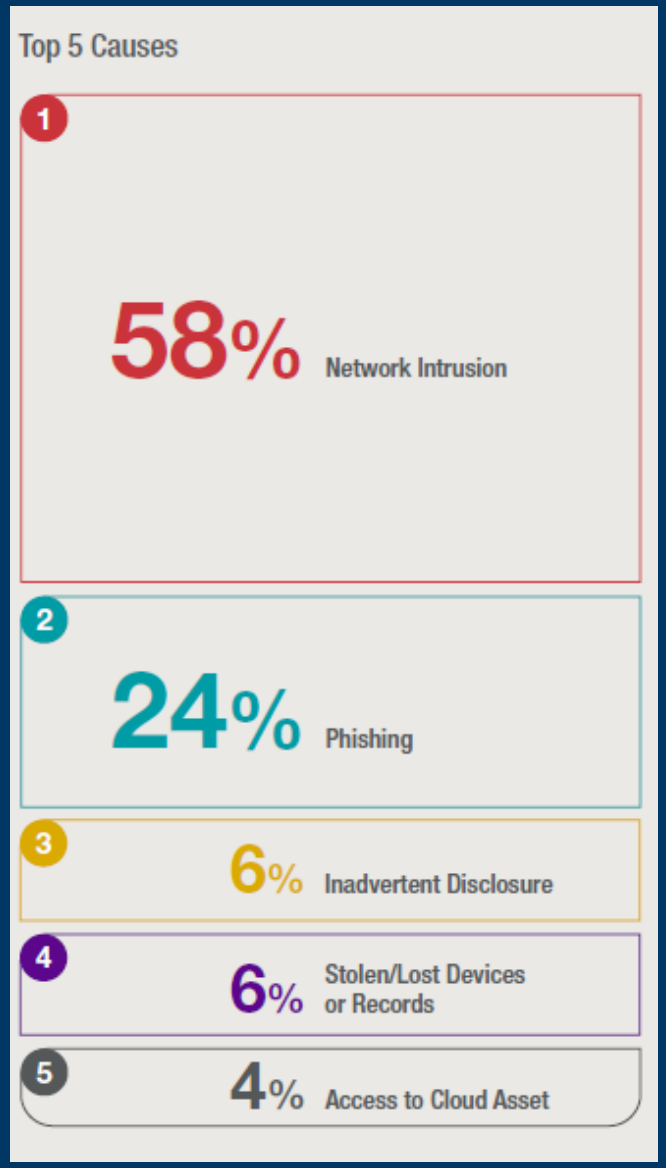
BBR Services Data

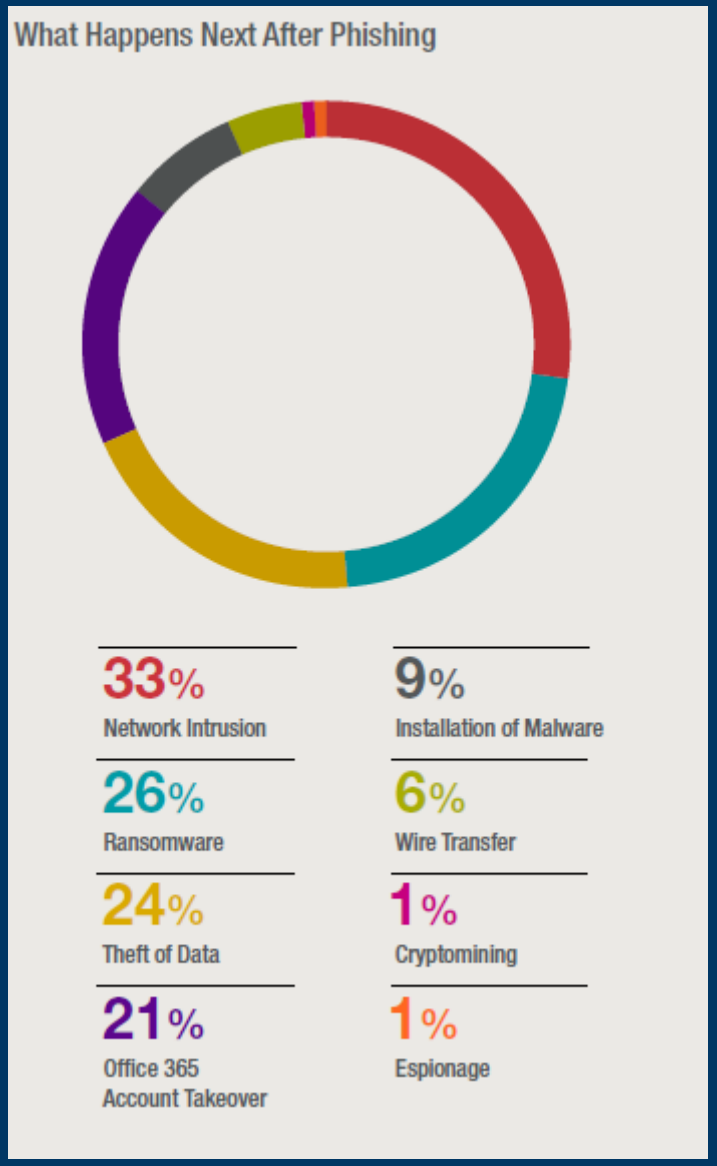
Other industries include but are not limited to:
Construction
E-commerce
Entertainment & Media
Technology
Telecommunications
Utilities

Incident Trends

Top Cause in 2019: Phishing – 38%

Top Cause in 2020: Network Intrusion – 58%





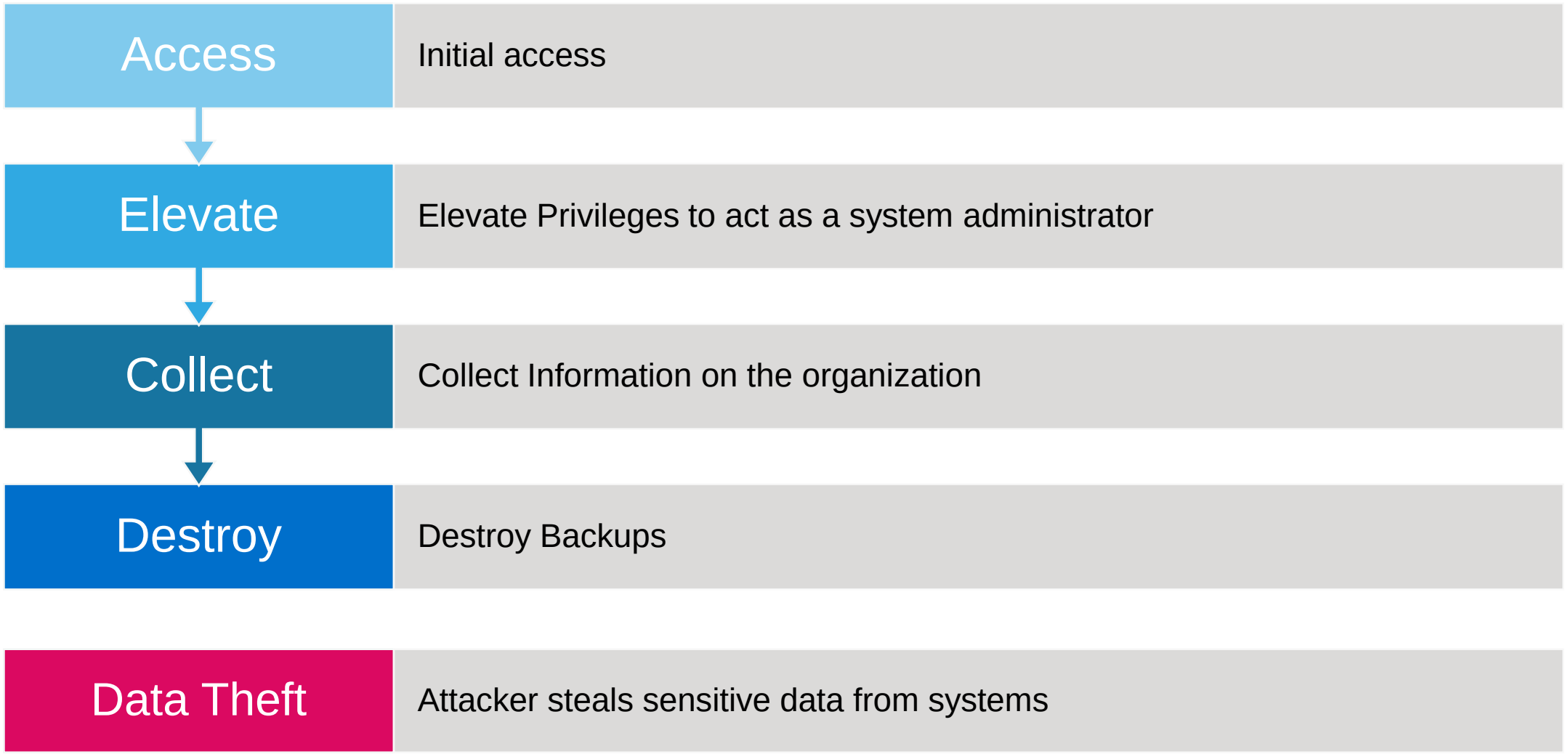
Source: BakerHostetler 2021 Data Security Incident Response Report

Ransomware Primer

How these attackers operate and evolve

Anatomy of an Attack – Phase 1

Newfront



Anatomy of an Attack – Phase 2

Newfront

Attacker deploys ransomware

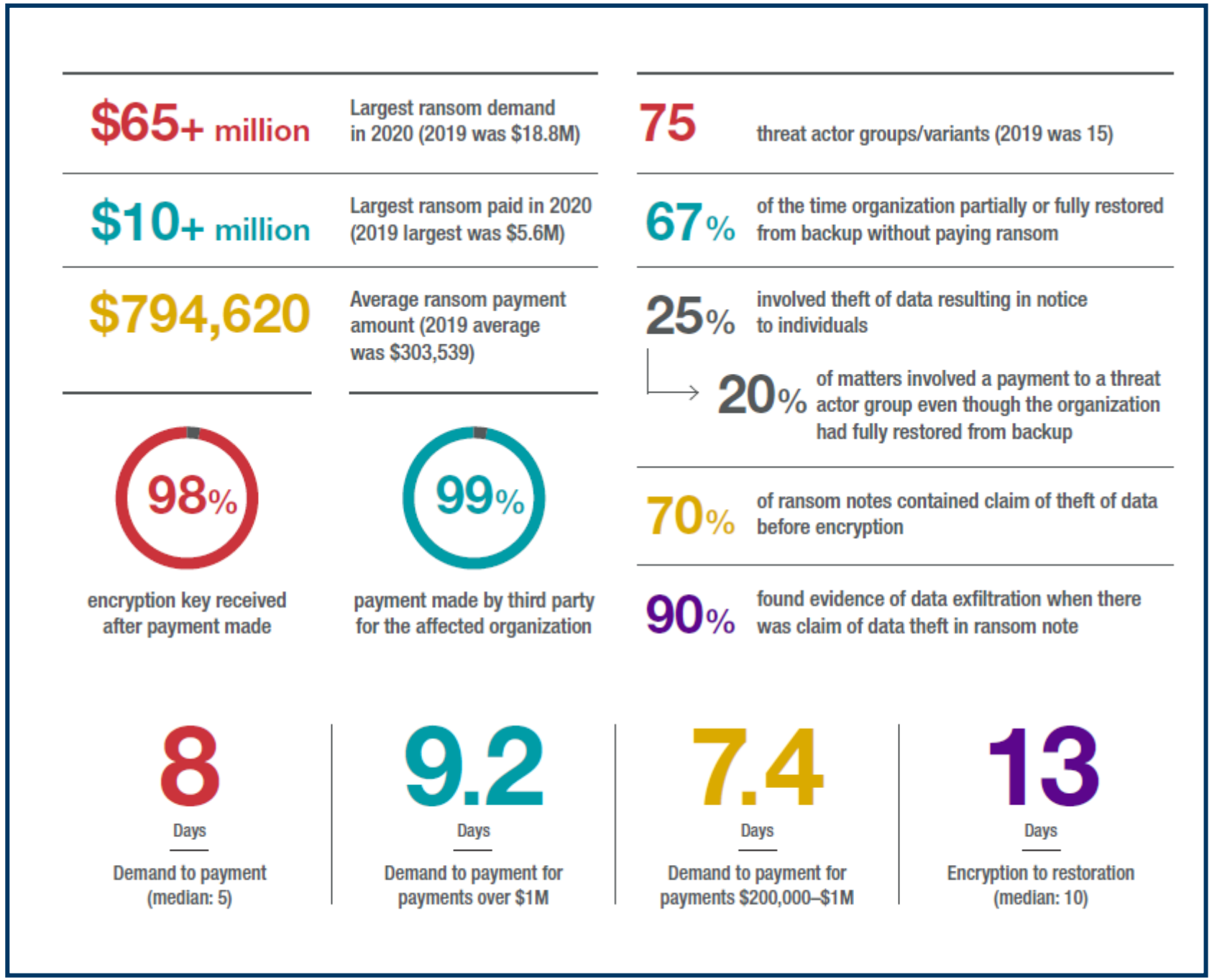
Waits for contact

Negotiates payment

Day One Ransomware Key Considerations

- **Impact assessment** – determine what is not operational, who will notice, and what consequences will likely follow. Identify any potential “downstream” impacts to franchisees or vendors.
- **Vendor engagement** – identify the external legal counsel, forensics firm, negotiation and payment, workforce augmentation/restoration, forensic accountant to document expense and income loss, and communications firms to consider engaging.
- **Threat actor intelligence** – find the ransom note and make preliminary attribution based on file extension and note content to start analysis of: (1) is this a threat actor known to only encrypt or steal/encrypt; and (2) is this a threat actor who may be on a sanctions list.
- **Ransom negotiation strategy** – directly or through negotiation, make initial contact with the threat actor to obtain initial demand and then begin to develop negotiation strategy. Identify threat actor’s history of payment default, decryptor efficacy, and tor site data posting strategy. Consider payment logistics (e.g., timing of wiring funds to negotiation vendor before wire close/weekend).
- **Restoration planning** – determine viability of backups and what alternate restoration options exist.
- **Containment** – identify how access occurred and how ransomware was deployed, are there systems that should be taken offline to prevent further spread and build plan for eliminating current access so you can restore to a secure environment (or build segmented VLAN to restore in until containment occurs).
- **Preservation** – account for preservation needs before wiping and reimaging devices during restoration.
- **Communications** – determine stakeholder communication needs and prepare drafts of reactive holding statement for media, associates, franchisees
- **“Response Plan” execution** – align response to key response considerations based on incident, business continuity, and crisis response plans
- **Notice analysis** – develop preliminary assessment of potential notification obligations.
- **Documentation** – identify what insurance carrier(s) (e.g., cyber, kidnap/ransom) will require to give consent to ransom payment and to reimburse (e.g., “business case” for payment, OFAC clearance report).

Ransomware Epidemic



Does Ransomware Automatically Lead to Litigation?

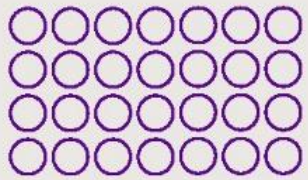
20 lawsuits filed related to incidents disclosed in 2020 (compared with 14 in 2019)

- 3 lawsuits arose from incidents that started with unauthorized access to Office 365 inboxes
- 2 lawsuits involved payment card data
- 9 lawsuits involved SSNs
- 9 lawsuits involved medical/health information
- 7 lawsuits involved ransomware
- 3 lawsuits were vendor related

Number of Lawsuits by Individuals Notified

2	6	4
over 2 million	under 1,000	under 10,000

Notifications vs. Lawsuits Filed



Regulatory Inquiries Following Notification

Does Ransomware Automatically Lead to Litigation?

Is there a correlation between payment of the ransom and litigation?

What are the biggest factors that indicate that there will be litigation?

- Number of people notified/impacted
- Type of data impacted
- High profile nature of entity (potential defendant)

How should you work with your carrier on paying/negotiating ransom payment?

Does Ransomware Automatically Lead to Litigation?

Newfront

1. **What kind of damage theories are Plaintiffs suing for after a Ransomware Attack?**
   - Lost Time
   - Increased Risk of Future Harm
   - Out of pocket expenses associated with the purchase of credit monitoring
   - Emotional distress
   - Statutory Penalties

1. **What are my chances on winning a ransomware attack class action?**
   - *Blahous v. Sarrell Reg'l Dental Ctr. for Pub. Health, Inc.*, 2020 WL 4016246, at *1 (M.D. Ala. July 16, 2020) (“The Plaintiffs’ claim that they suffered money damages because they paid for services at Sarrell but would not have done so had they known that Sarrell would get hacked [in a ransomware attack] later on, is pure applesauce.”)

Key Issues Relating To Cyber Policies

Insurer notice and consent

- Policies vary on consent for first-party costs:
  - Some strictly require prior insurer consent before incurring costs
  - Some allow the use of panel or pre-approved consultants for defined periods or up to certain amounts
- Counsel and vendor billing rates
  - Approved counsel (“panel counsel” and “panel vendors”)
  - Specified rate caps

Specific Ransomware Provisions

- Some policies require insurer’s prior written consent before a ransom payment is made
- Some policies require that the insured first confirm OFAC compliance and make the ransom payment, then seek coverage after-the-fact
- Some policies go so far as to say that the insurer will not comment on OFAC compliance and coverage before the insured actually makes the ransom payment

Thank You!

Q&A

Newfront