



Global Cyber Trends

What is going on?

16th October 2024



Agenda

Cyber Market Cycle and Trends

- What has happened over time

Ransomware

- Why it became an Epidemic, where has it gone?
- Florida's No Ransomware Payments Legislation

Supply-Chain

- A Cyber hurricane
- Crowdstrike, ChangeHealth, MSPs

Social Engineering

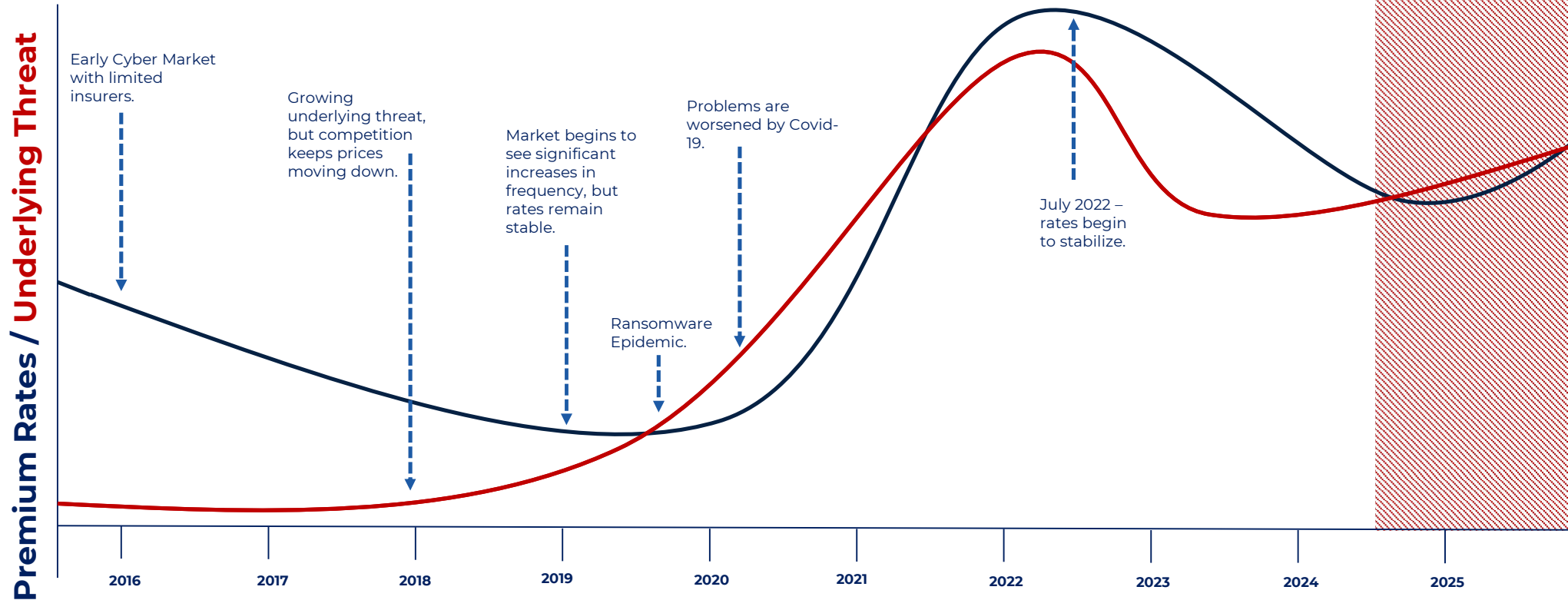
- Can happen to anyone (even the underwriters!)
- Call-back Procedures / Crime-Market

Claims

- Hear about the weirdest, wonderful and awful claims out there!

Market Cycles

Cyber Market



Ransomware

“There are a lot of parallels, there’s a lot of importance, and a lot of focus by us on disruption and prevention.

There’s a shared responsibility, not just across government agencies but across the private sector and even the average American”

Christopher Wray – FBI Director

2021

On comparing the ransomware epidemic to 9/11

Ransomware

What is it?

Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.

11

Ransomware attacks
a second

3m

Attacks a year



Attacks



Demands



Data Leaks

57x

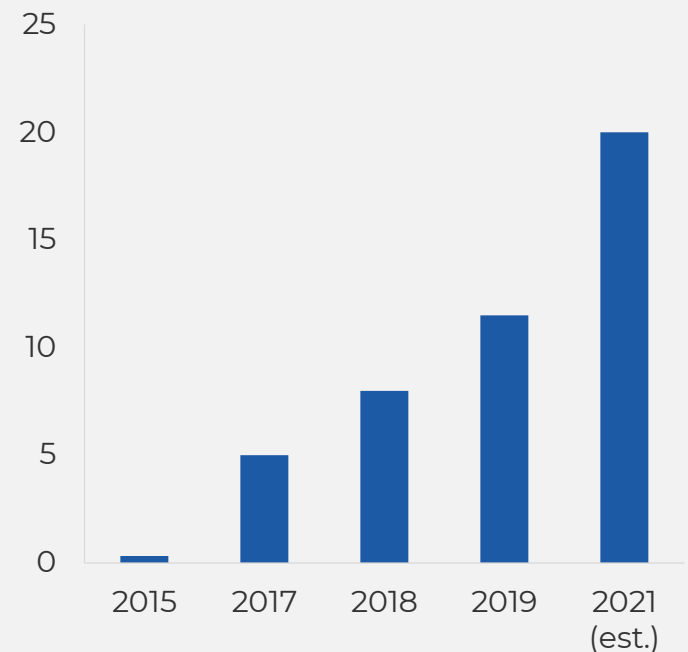
Higher Global losses in
2021 compared to 2015

37x

Higher demands in 2021
compared to 2018

<https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>
<https://www.cloudwards.net/ransomware-statistics/>

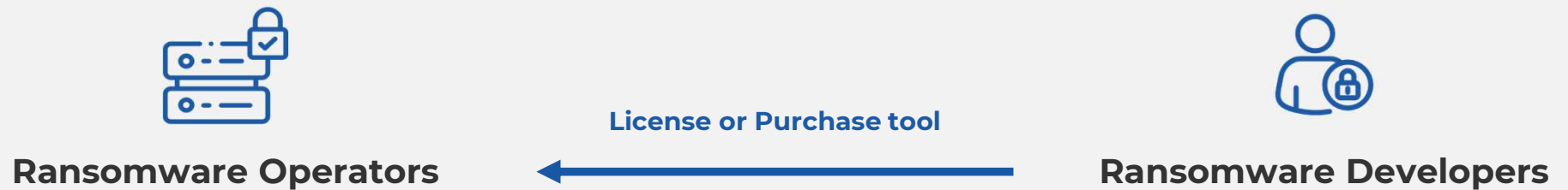
Ransomware Costs Globally



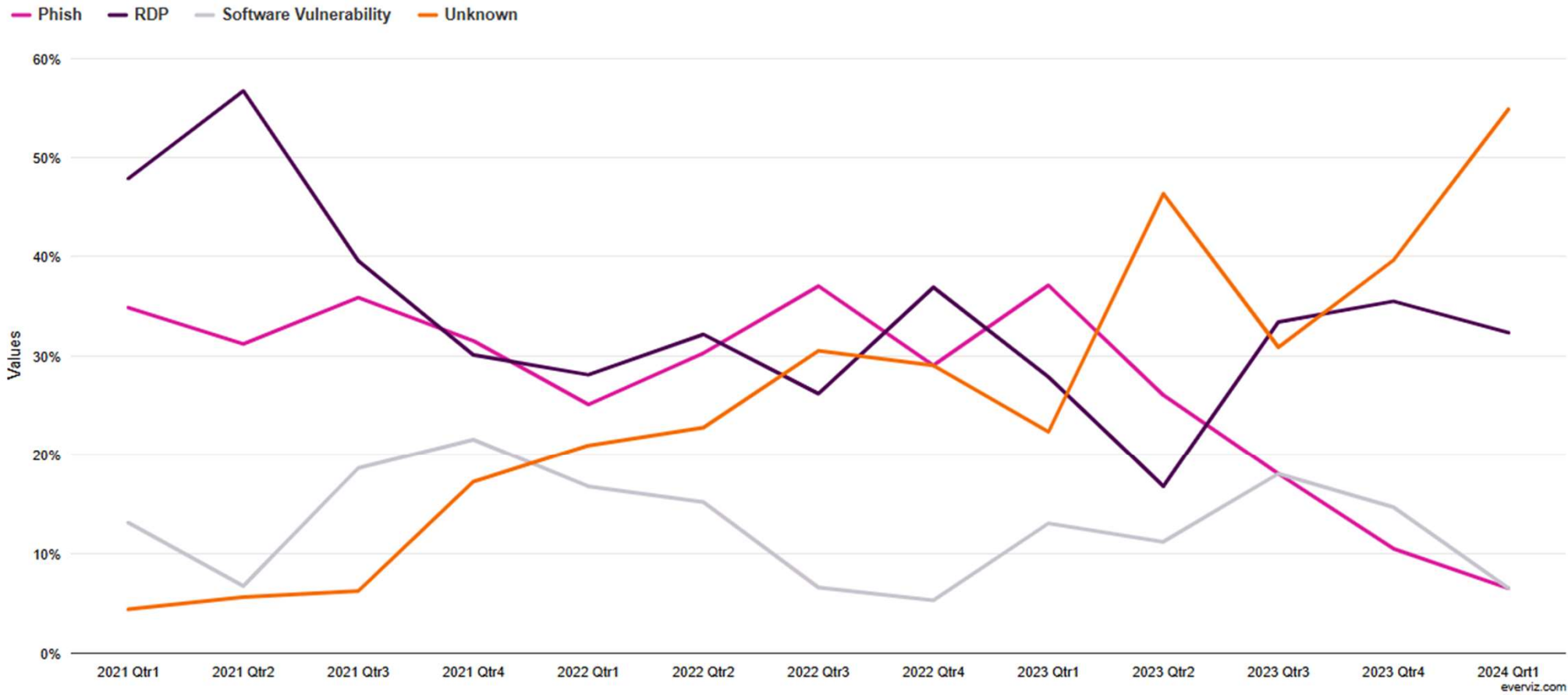
Frequency

Ransomware-as-a-Service

Develop Ransomware & Deploy as widely as possible



Ransomware Vectors



Ransomware

2020-2022

Colonial hack: How did cyber-attackers shut off pipeline

By Joe Tidy
Cyber reporter

10 May 2021

Insurance giant AON hit by a cyberattack over the weekend

By Lawrence Abrams

28 February 2022

10:39 AM

Meat giant JBS pays \$11m in ransom to resolve cyber-attack

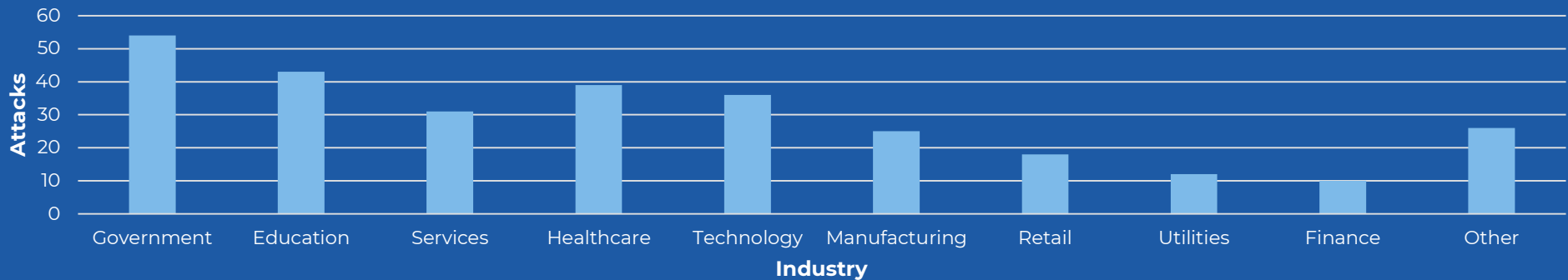
10 May 2021

Kaseya ransomware attack sets off race to hack service providers-researchers

By Joseph Menn

CNA Financial Paid \$40 Million in Ransom After March Cyberattack

- Payment bigger than previously disclosed ransoms, experts say
- Malware tied to Russian cybergang sanctioned by U.S in 2019



<https://www.blackfog.com/the-state-of-ransomware-in-2021/>

What is being done

Ransomware



Government Intervention

- Law Enforcement Action



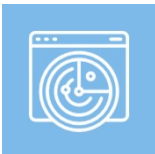
Arms Race

- New better detection and response tools



Not Paying Demands

- State by State, Country by Country bans on Ransom payments



Insurer's Minimum Standards of Security....



Dmitry Smiljanets
@ddd1ms

DarkSide [#ransomware](#) Leaks Press Center:

About the latest news.

10.05.2021

We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined government and look for other our motives.
Our goal is to make money, and not creating problems for society.
From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.

6:05 AM · May 10, 2021 · Twitter Web App

Russian OSINT

DarkSide CLOSED

Servers were seized (country not named), money of advertisers and founders was transferred to an unknown account. Ransom topics will be removed from the forums.

REvil's comment from the exp: In connection with the recent events in the USA, sorry for being straightforward, DarkSide Ransomware, a quote from the previously named PP:

Since the first version, we promised to speak honestly and openly about the problems. A few hours ago, we lost access to the public part of our infrastructure, namely: the

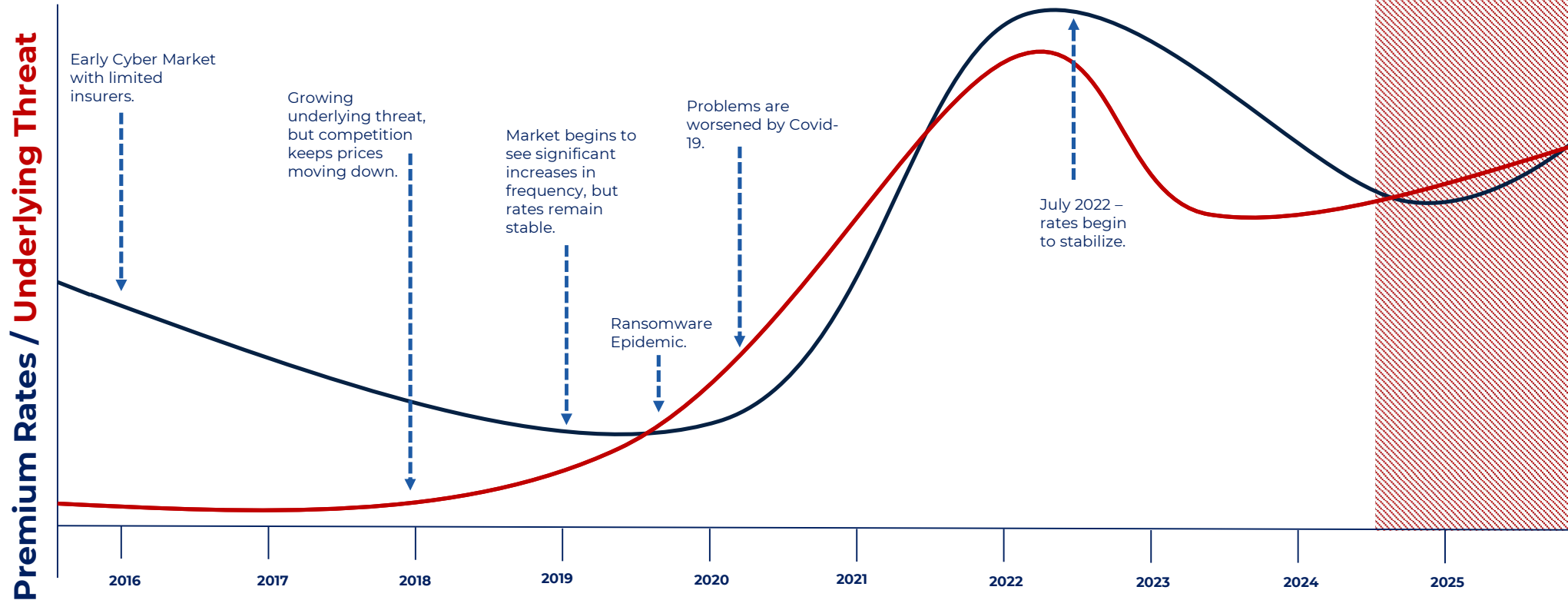
*Blog.
Payment server.
DOS servers.*

Now these servers are unavailable via SSH, the hosting panels are blocked. Hosting support, apart from information "at the request of law enforcement agencies", does not provide any other information.

Also, a few hours after the withdrawal, funds from the payment server (ours and clients') were withdrawn to an unknown address.

Market Cycles

Cyber Market



Supply Chain Events

“Software supply chain infiltration is one of the key threats that organizations need to pay attention to, particularly how software vulnerabilities are exploited. The impacts to proprietary data, trade secrets, and national security are profound ”

William Evanina – NCSC Director
2018

Supply Chain Risk

What is it

CHANGE
HEALTHCARE



CROWDSTRIKE

Kaseya®

solarwinds 

UKG



Progress® MOVEit®

Cyber Court

Make your case



Ellie Kemp
KC, of his majesty's
royal cyber insurer's
committee

Supply Chain Attacks pose the biggest threat to Cyber insurers and the cyber-economy.

- M&As and Interconnectivity
- Single Point of Failure – Change Healthcare / CDK
- Security companies are also causing losses - CrowdStrike



Simon Meech
KC, of his majesty's
royal cyber
defense panel

While a major threat, the severity of supply chain attacks are overstated and should be viewed in the context of speedy recovery.

- Bigger, usually means better. SMBs don't have security resources.
- Better competition regulation needed – but not inherently a cyber risk.
- But Security Companies/Tech companies fix losses very quickly

Social Engineering

“More than a third of all cybercrime losses can be attributed to BEC scams, causing about \$2.4 billion in losses to U.S. businesses last year.”

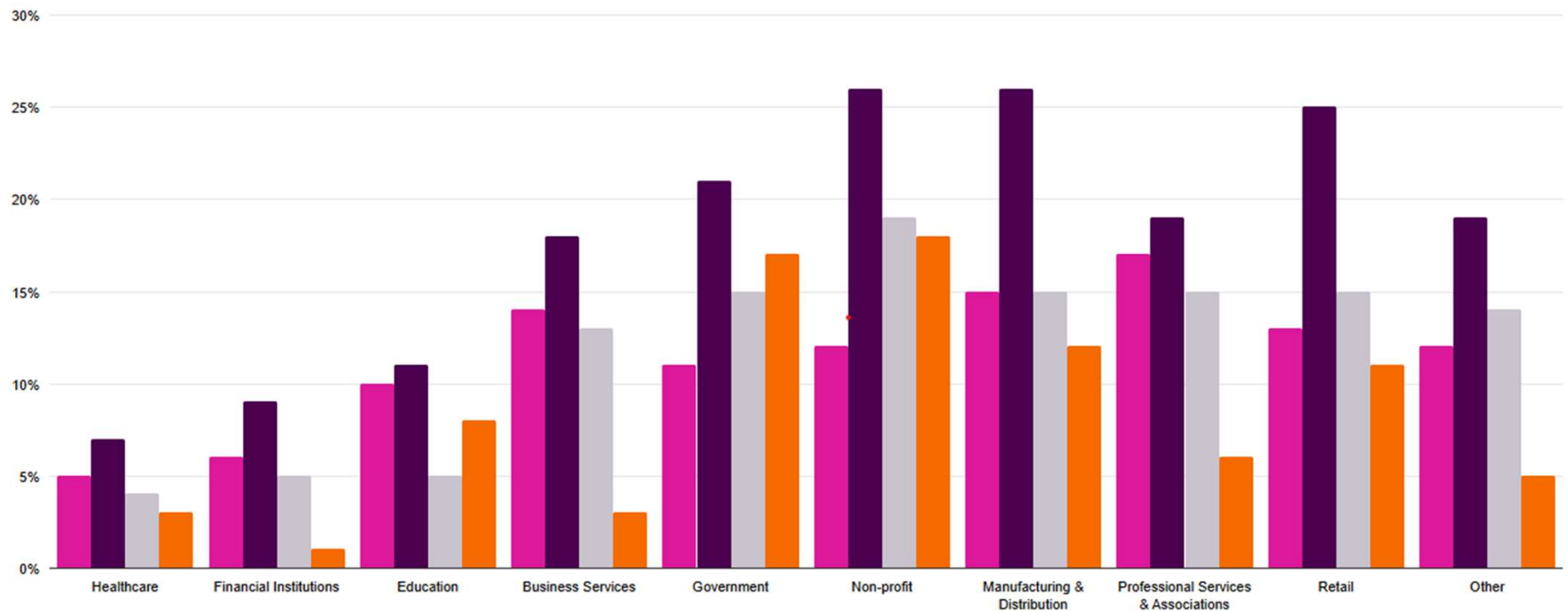
Forbes
2022

Fraudulent Instruction

Fraudulent instruction as a cause of loss

Percentages by industry

■ 2021 ■ 2022 ■ 2023 ■ 2024 Q1



Cyber vs Cyber Crime – CIA Rule

CIA Rule:

*If it relates to **Confidentiality, Integrity or Availability** = Cyber*

*If it relates to **Money** = Computer/Cyber Crime*

Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access.

Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct.

Availability means that authorized users have access to the systems and the resources they need.

Money



Cyber Crime

Call Back Conditions

Fraudulent Instruction means the transfer, payment or delivery of **Money** or **Securities** by an **Insured** as a result of fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions provided by a third party, that is intended to mislead an **Insured** through the misrepresentation of a material fact which is relied upon in good faith by such **Insured**.

Fraudulent Instruction will not include loss arising out of:

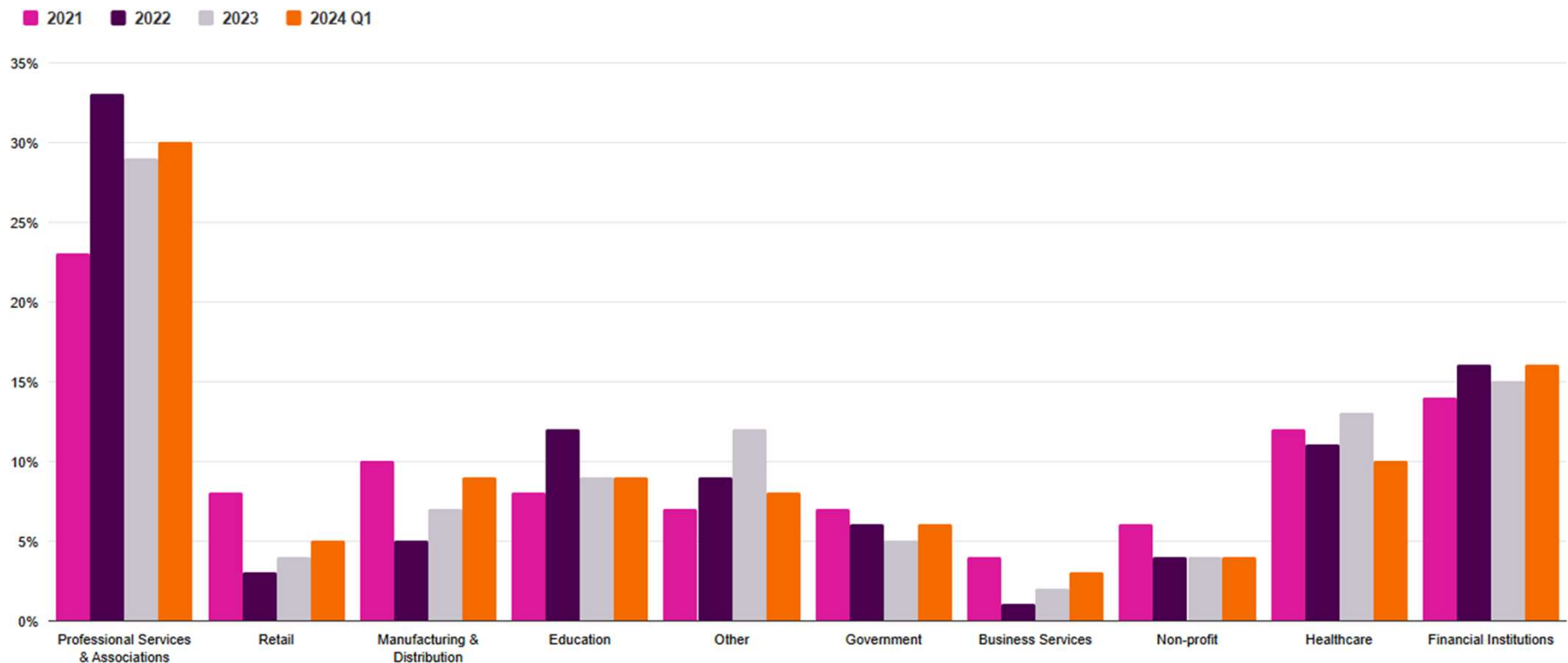
1. fraudulent instructions received by the **Insured** which are not first authenticated via a method other than the original means of request to verify the authenticity or validity of the request;
2. any actual or alleged use of credit, debit, charge, access, convenience, customer identification or other cards;
3. any transfer involving a third party who is not a natural person **Insured**, but had authorized access to the **Insured's** authentication mechanism;
4. the processing of, or the failure to process, credit, check, debit, personal identification number debit, electronic benefit transfers or mobile payments for merchant accounts;
5. accounting or arithmetical errors or omissions, or the failure, malfunction, inadequacy or illegitimacy of any product or service;
6. any liability to any third party, or any indirect or consequential loss of any kind;
7. any legal costs or legal expenses; or
8. proving or establishing the existence of **Fraudulent Instruction**.

Business Email Compromise

Business email compromise (BEC) continues to increase, up 35% quarter over quarter, with increases across all industries, except for Healthcare. Professional Services continues to experience the highest number of BEC incidents overall!

Business email compromise

Percentages by industry



Social Engineering

Phishing - can you spot it?

Would
you trust
this email?



YES



NO

EMAIL



From: Tim Frost <Timm.Frost@abclifting.com>

Sent: 28 September 2022 1:32 PM

To: James Harvey

Subject: URGENT - Dunnder Mifflin Invoice

Hi James,

Great to have you join the team! Welcome to the business.

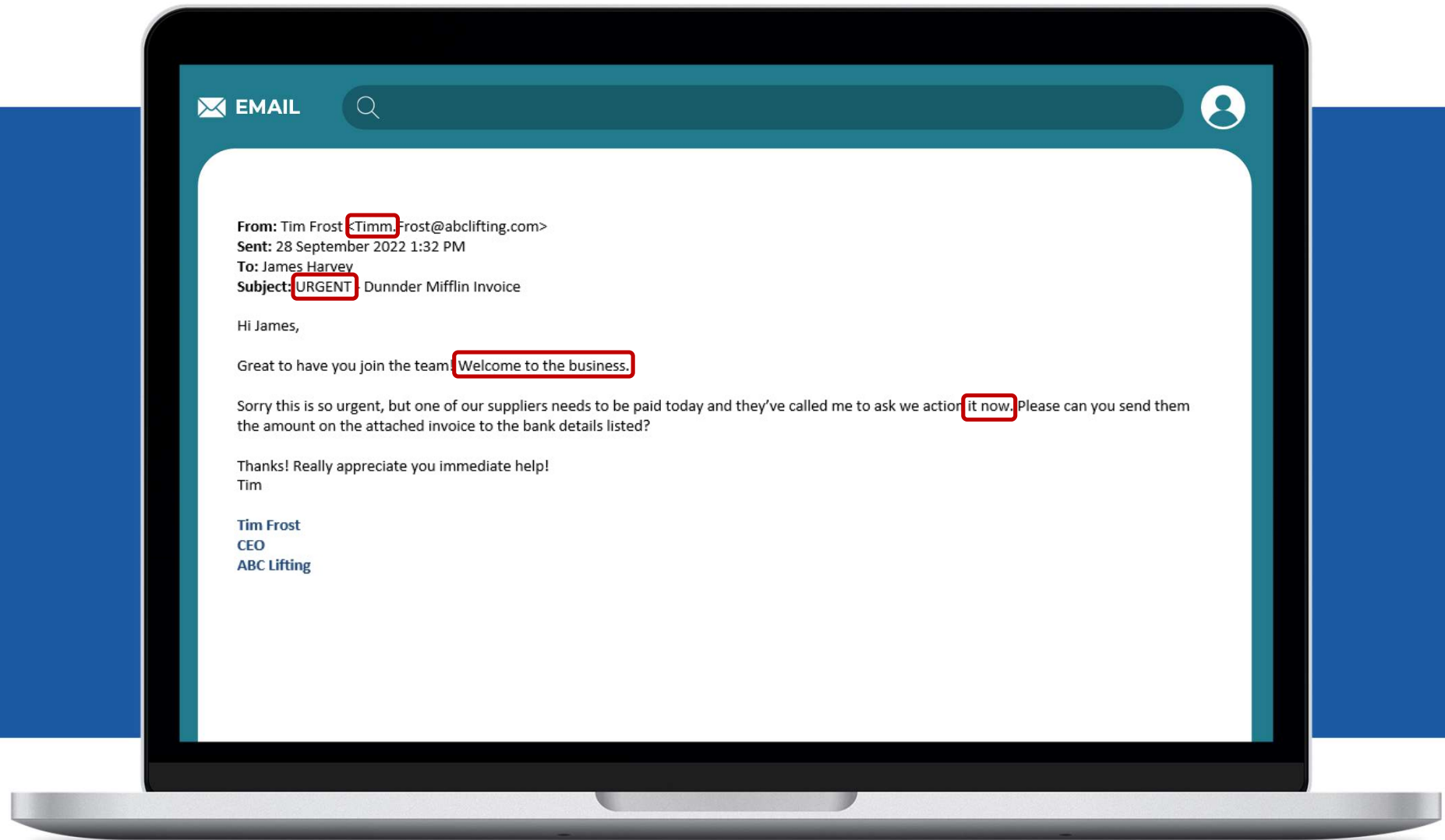
Sorry this is so urgent, but one of our suppliers needs to be paid today and they've called me to ask we action it now. Please can you send them the amount on the attached invoice to the bank details listed?

Thanks! Really appreciate you immediate help!
Tim

Tim Frost
CEO
ABC Lifting

Social Engineering

Phishing - can you spot it?



Social Engineering

Phishing - can you spot it?

Would
you trust
this email?



YES



NO

EMAIL



From: Tim Frost <Tim.Frost@abclifting.com>

Sent: 28 September 2022 1:32 PM

To: James Harvey

Subject: Dunder Mifflin Invoice

Hi James,

Hope you're keeping well.

One of our suppliers needs to be paid today so I was hoping you could organise it soon? Please can you send them the amount on the attached invoice to the bank details listed?

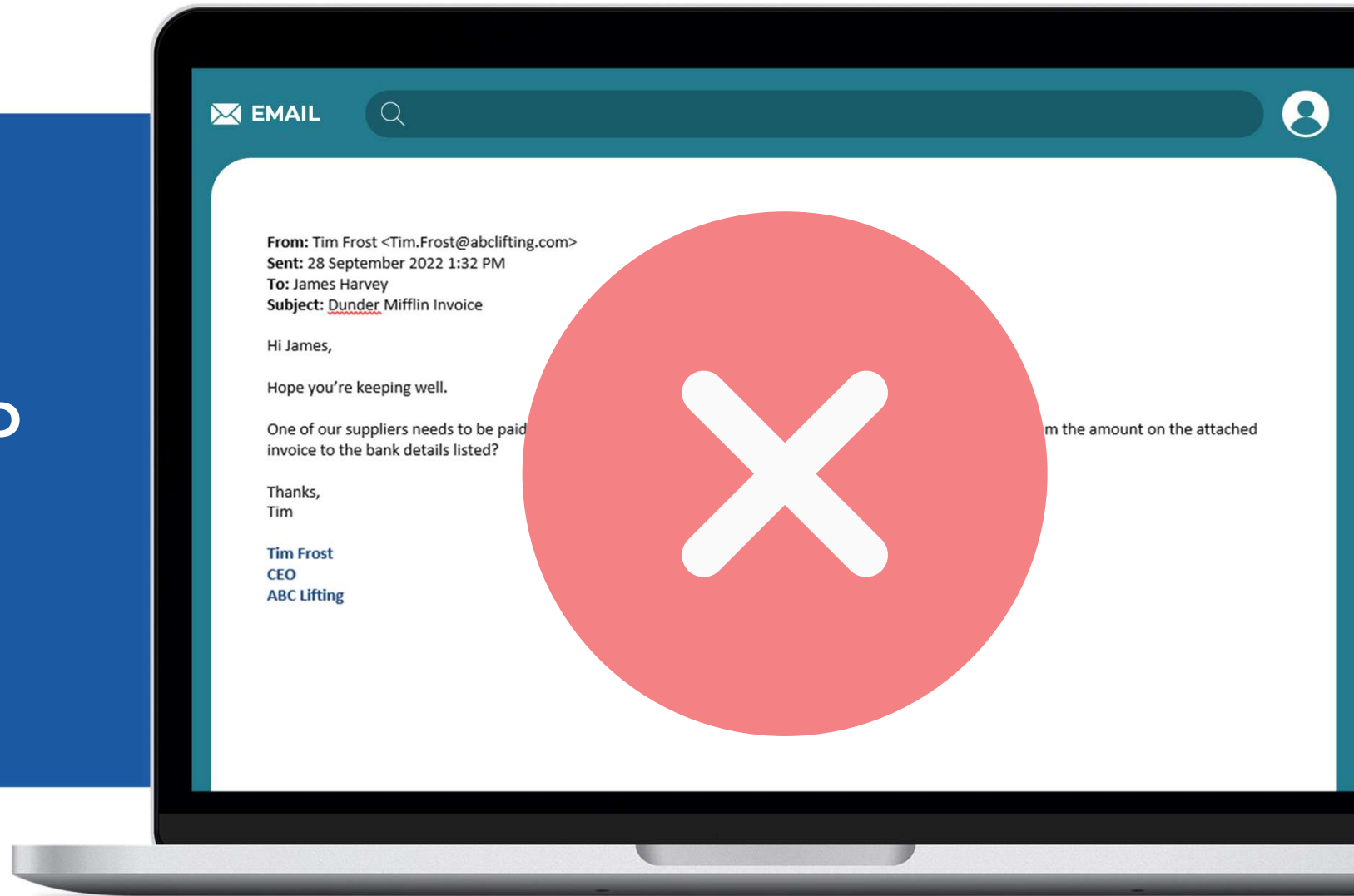
Thanks,
Tim

Tim Frost
CEO
ABC Lifting

Social Engineering

Phishing - can you spot it?

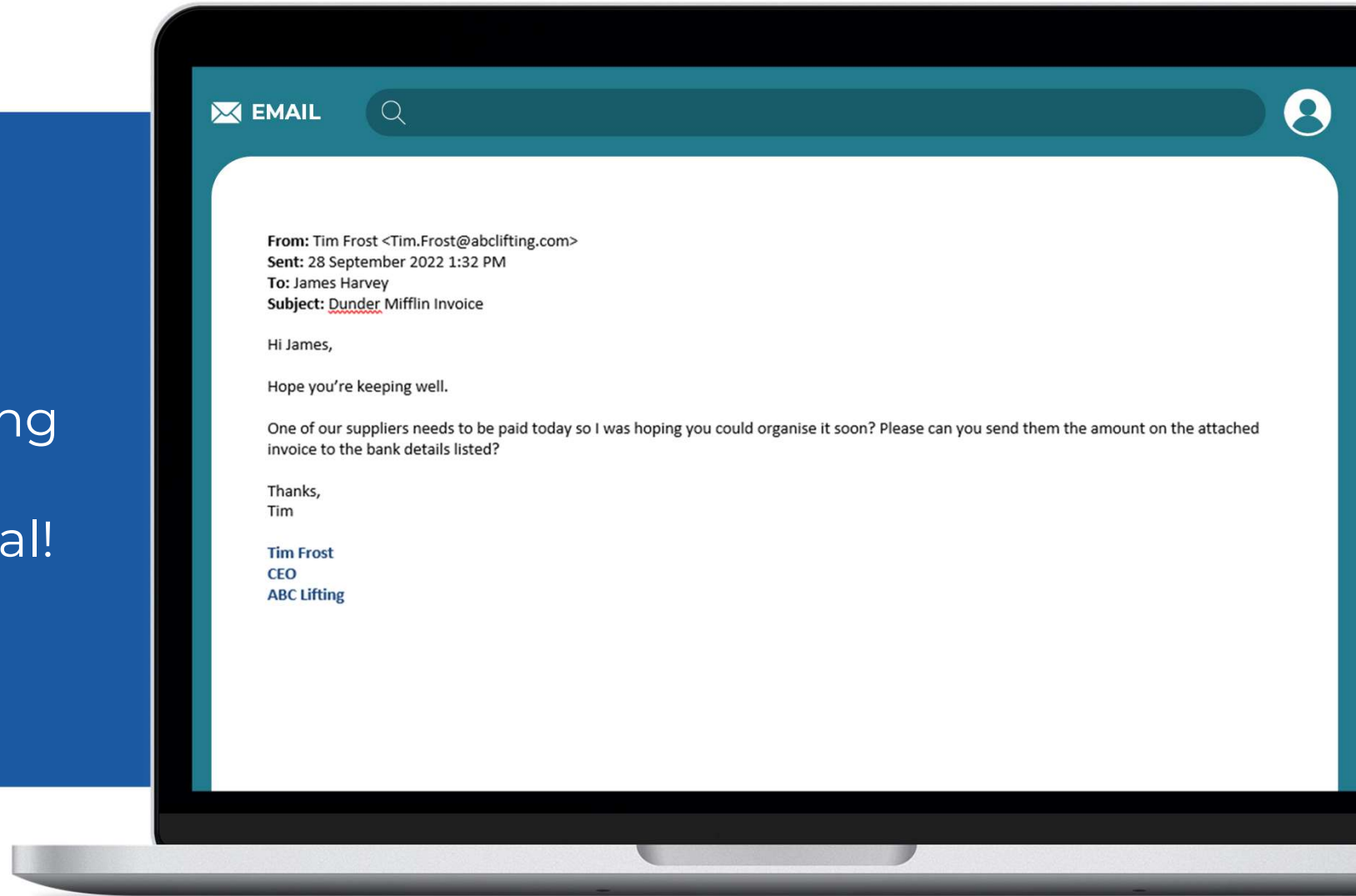
ALSO A BAD
EMAIL!...



Social Engineering

Phishing - can you spot it?

Not all Phishing
Training is
created equal!



Social Engineering

The BMS Test

10 Cyber Underwriters sent an email with 'malicious' link.

Email content was customized based on publicly available information (and some simple ego tricks)



9
Failed



1
Passed

Because he didn't receive the email.

Anyone can be fooled by Phishing emails – they are not easy to spot anymore

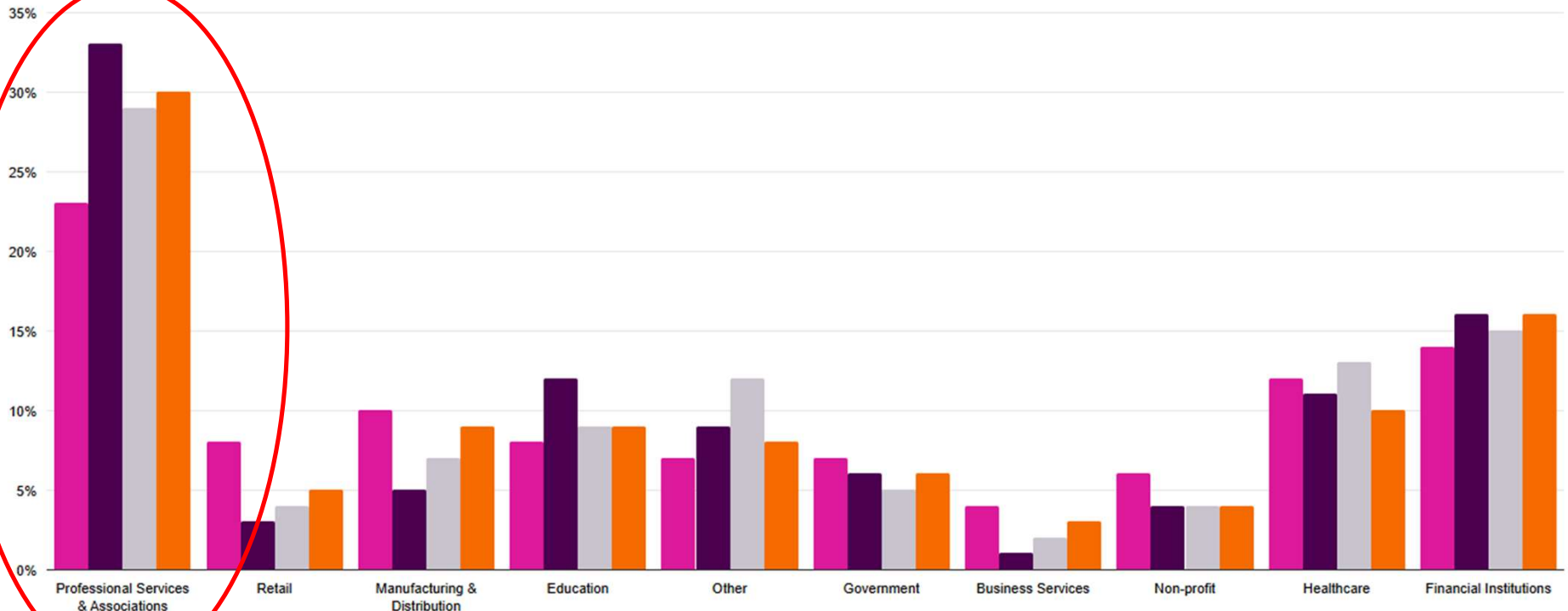
Business Email Compromise

Business email compromise (BEC) continues to increase, up 35% quarter over quarter, with increases across all industries, except for Healthcare. Professional Services continues to experience the highest number of BEC incidents overall!

Business email compromise

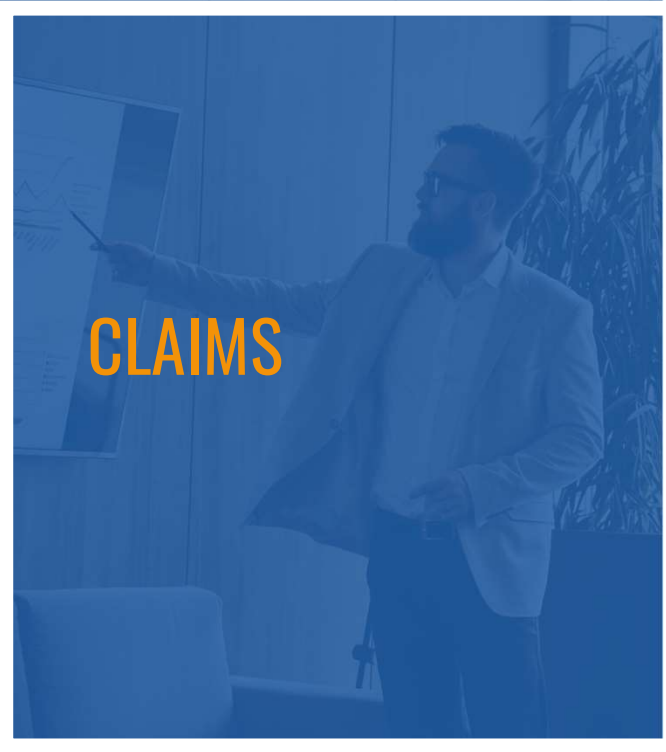
Percentages by industry

2021 2022 2023 2024 Q1



What do you want to hear about?

Choose your own adventure!

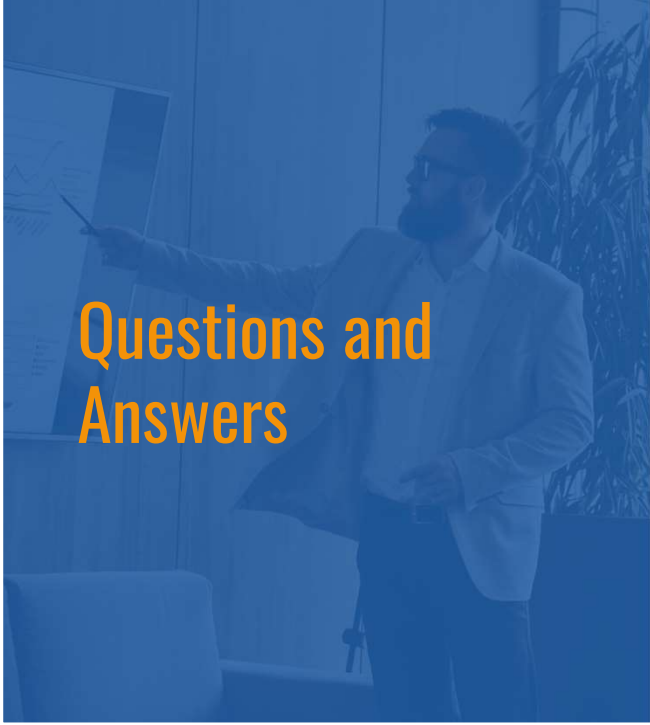


CLAIMS

1. Public School – testing Sovereign Immunity Rules
2. City not paying ransom demand
3. “Chinese” Tracking of Military Bases
4. Threat Actors Using inventive ways to extort
5. Deepfake - \$25m loss transferred!
6. Largest “Russian” Attack in History
7. How not to handle your response
8. Protein Shakes revenge – vicarious liability of data!
9. ChangeHealth – learn more about their double extortion
10. Don’t ignore the ransomware gang, kids!

Ask us anything

Within reason!



Questions and Answers

Some suggested questions:

- ☐ War Exclusions – how do they function when attacks appear to be coming from State Governments
- ☐ Property Damage – is it covered?
- ☐ How quickly will Artificial Intelligence change things?
- ☐ Should it be illegal to pay ransomware claims?

Appendix

Data Privacy

Oregon Consumer Privacy Act

Forbes
2022

Oregon Consumer Privacy Act

OCPA

L

List – all entities data has been sold to

O

Opt-out – of data being sold or being used for advertising

C

Copy – request a copy of data held on you

K

Know – what information the business collects about you

E

Edit – you can demand inaccuracies are amended

D

Delete – you can demand your data is deleted

Does not apply to government organizations

But has already had an affect on a court case!



Almost none of
these questions
existed before
**2018 on cyber
application forms**

Insurance

Minimum Standards



Multifactor Authentication



Offline / Disconnected Backups



Privileged Access Management



Endpoint Detection and Response



Regular Patching



Log and Monitor Abnormalities



Anti-Spoofing controls – DMARC, SPF, DKIM



Sandboxing suspicious emails



Authenticate communications before changing bank details