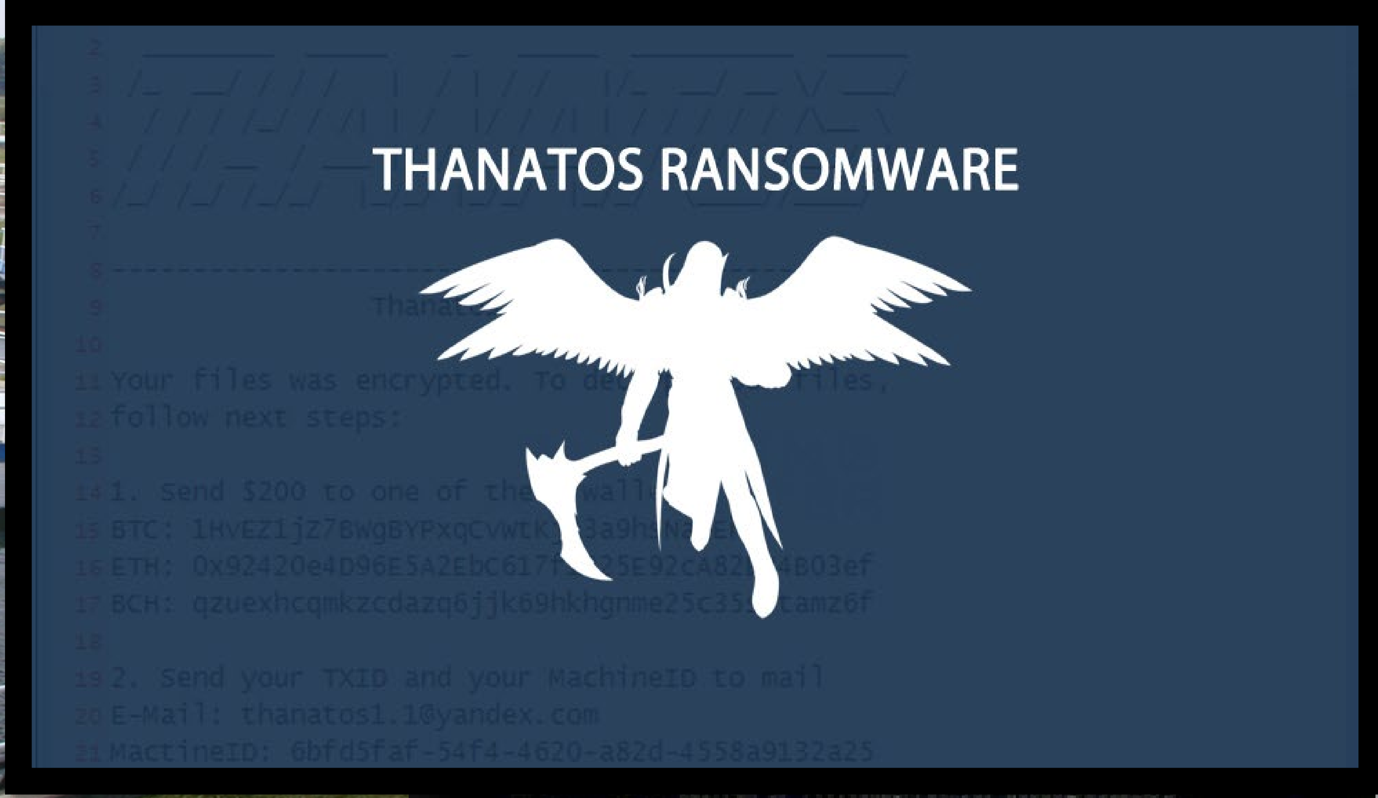
Cyber

CONNER
STRONG &
BUCKELEW

Trico JIF 2023 Retreat

July 2023

How Did We Get Here?

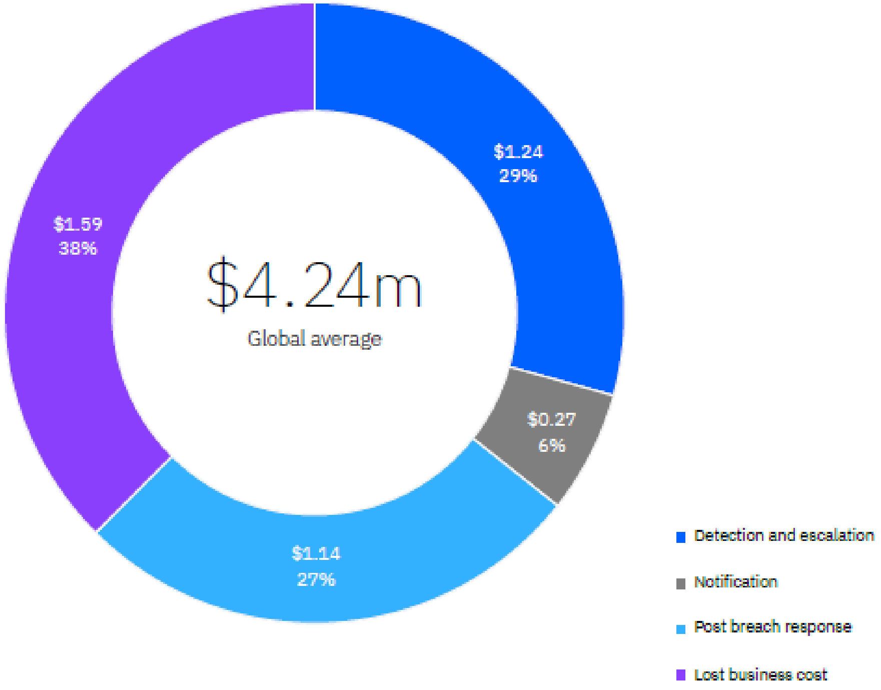


```
Thana

Your files was encrypted. To de        files,
follow next steps:

1. Send $200 to one of the   wall
BTC: 1HVEZ1jZ7BWgBYPxqCVWtK  3a9h
ETH: 0x92420e4D96E5A2EbC617F  25E92cA82  4B03ef
BCH: qzuexhcqmkzcdazq6jjk69hkhgnme25c35  tamz6f

2. Send your TXID and your MachineID to mail
E-Mail: thanatos1.1@yandex.com
MactineID: 6bfd5faf-54f4-4620-a82d-4558a9132a25
```

IBM Security Report

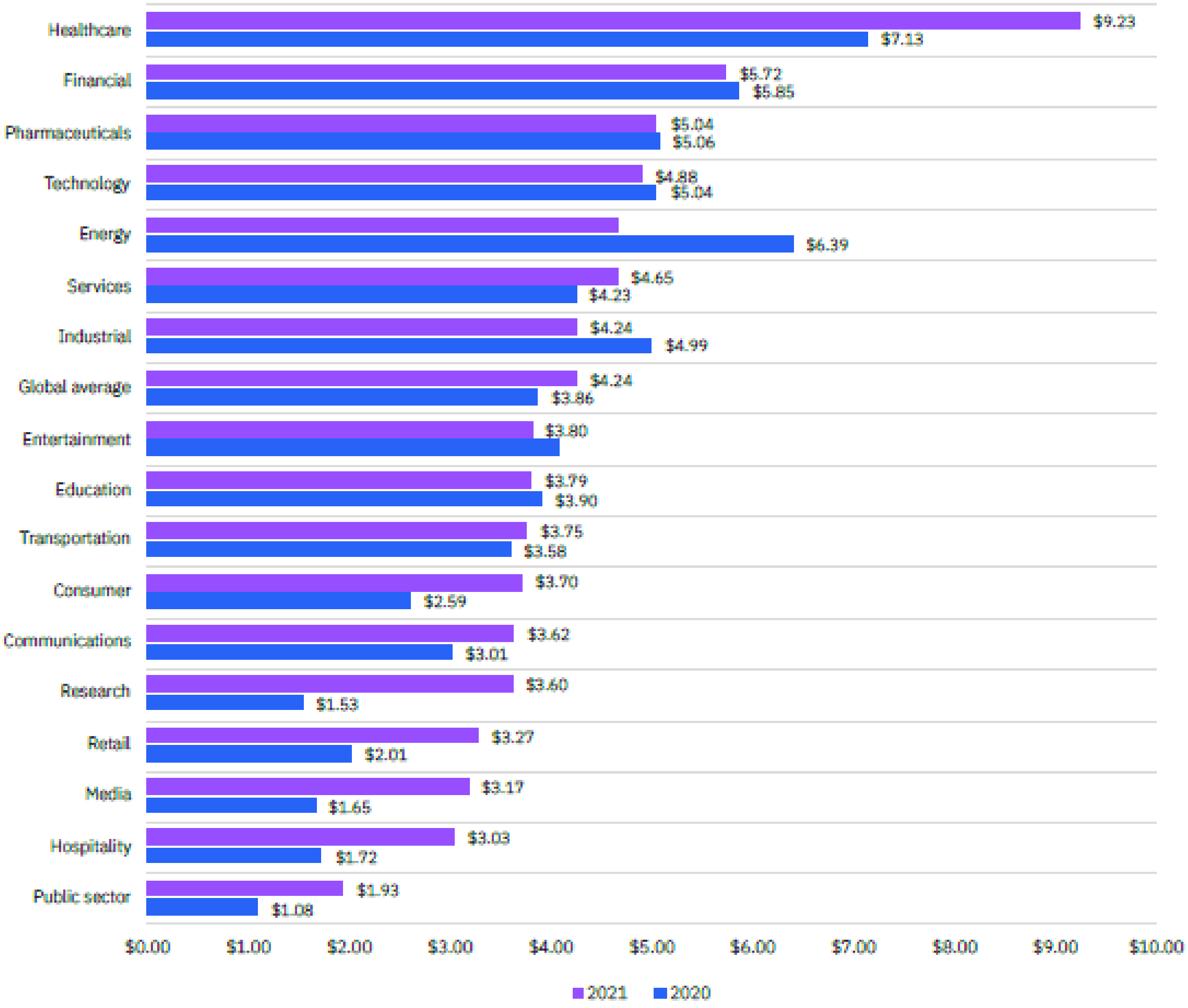
Average total cost of a data breach divided into four categories

Measured in US$ millions

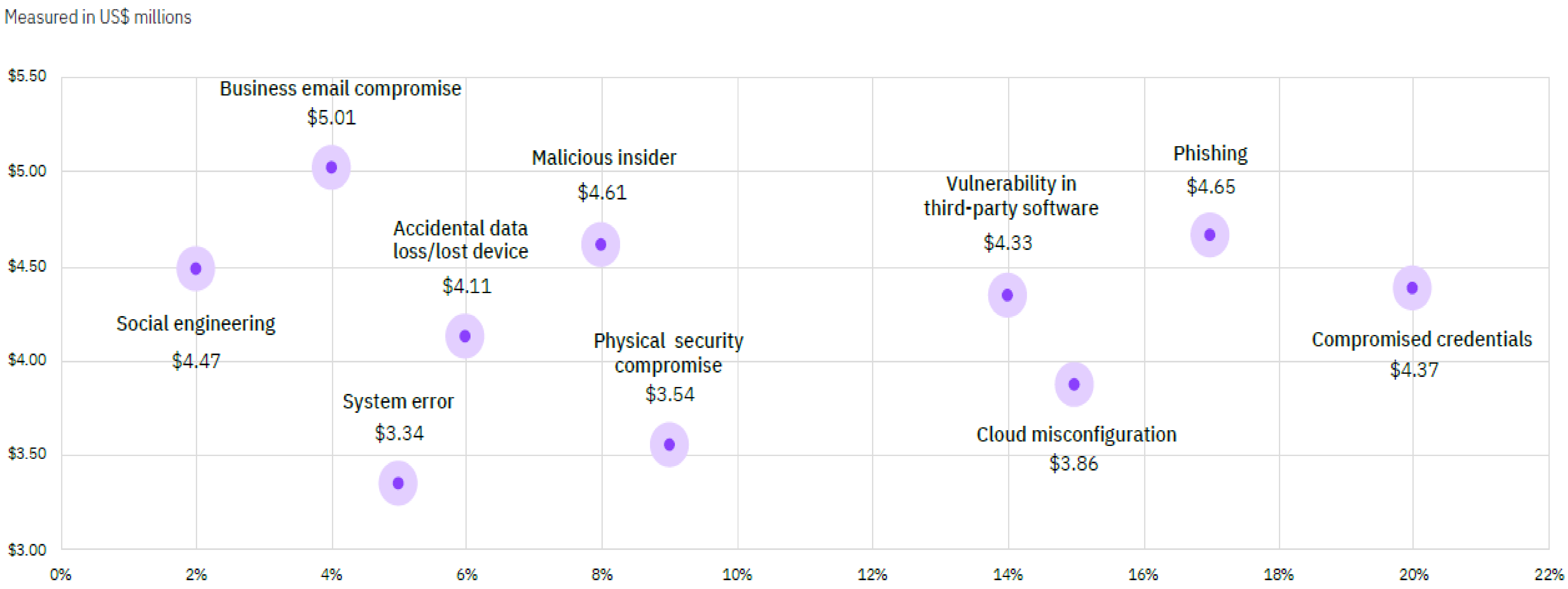


Average total cost of a data breach by industry

Measured in US$ millions



IBM Security Report



Verizon Data Breach Investigations Report

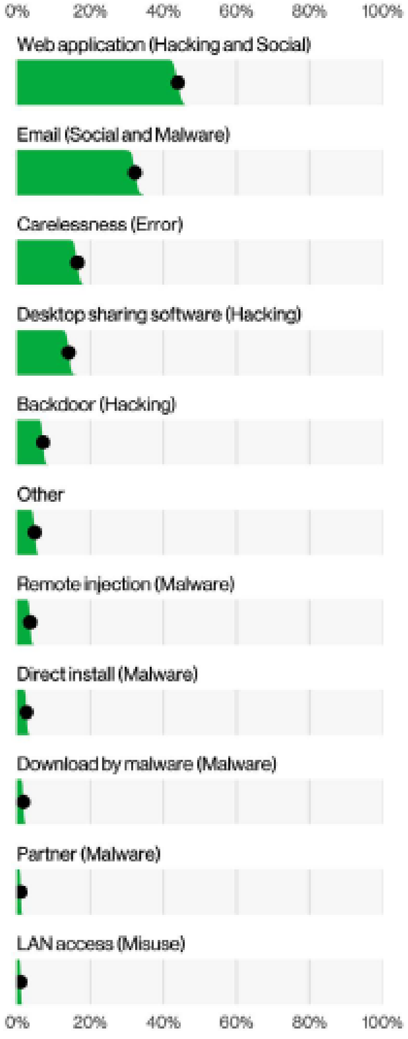


Figure 18. Top Action vectors in breaches (n=3,279)

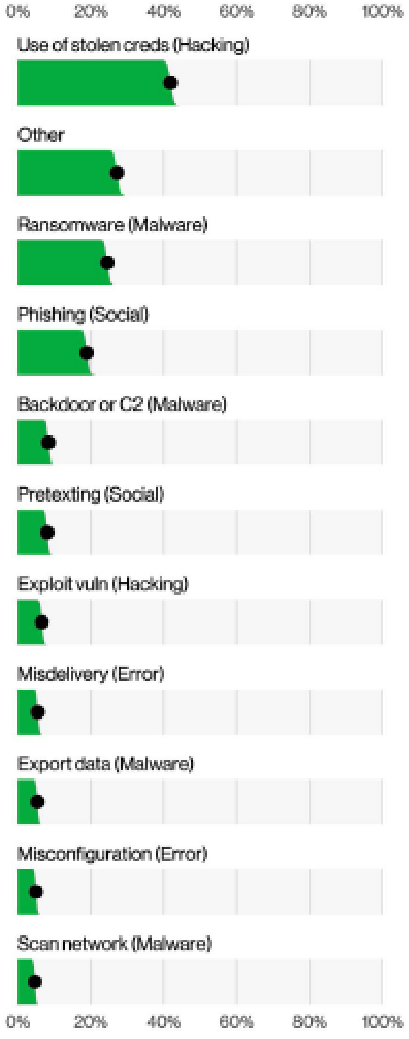
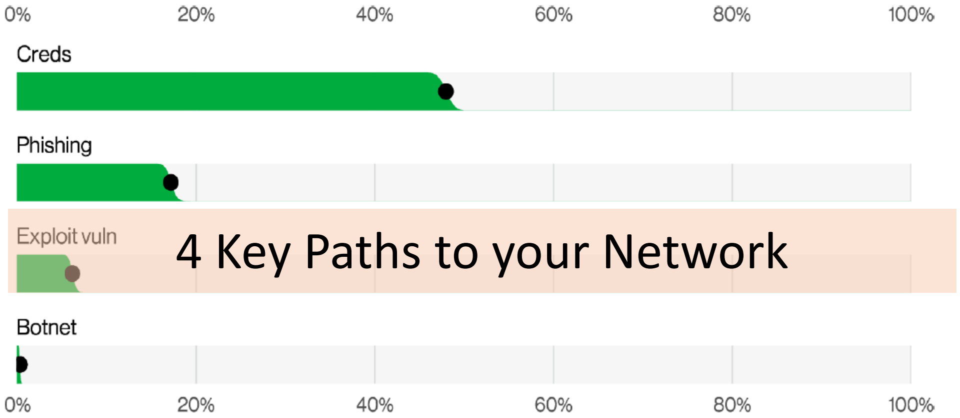
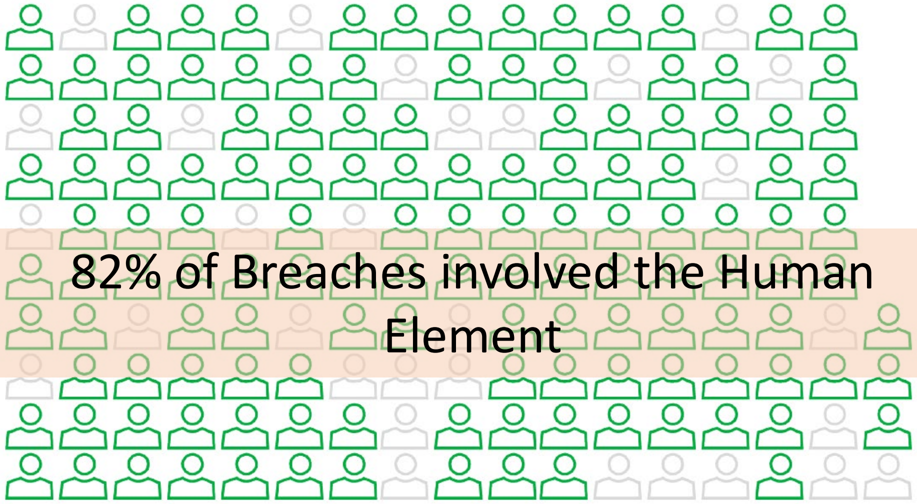


Figure 19. Top Action varieties in breaches (n=3,875)



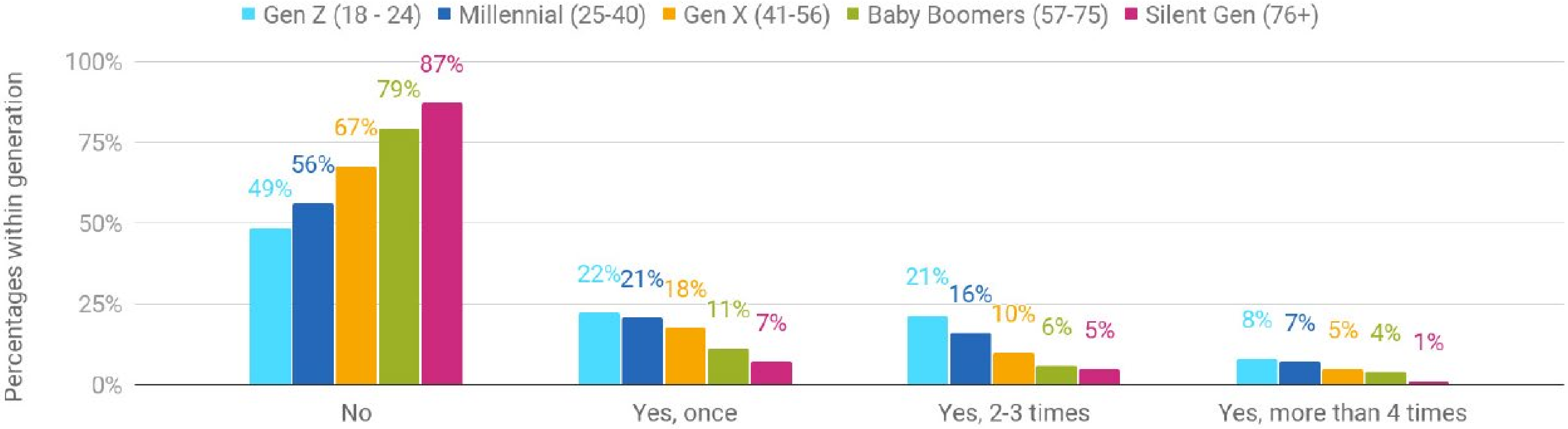
4 Key Paths to your Network



82% of Breaches involved the Human Element

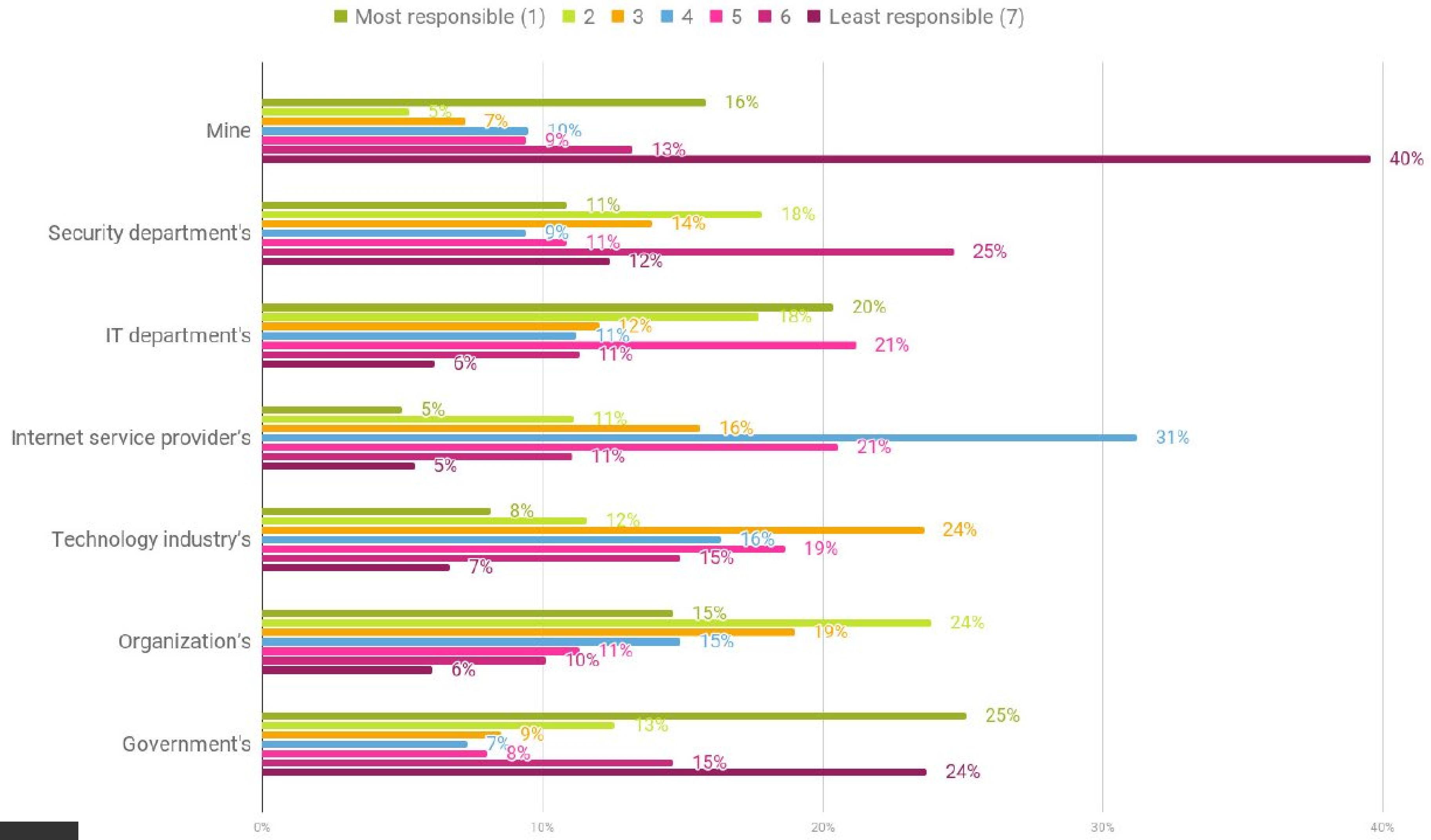
Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

Victims of Cybercrime by Age Group



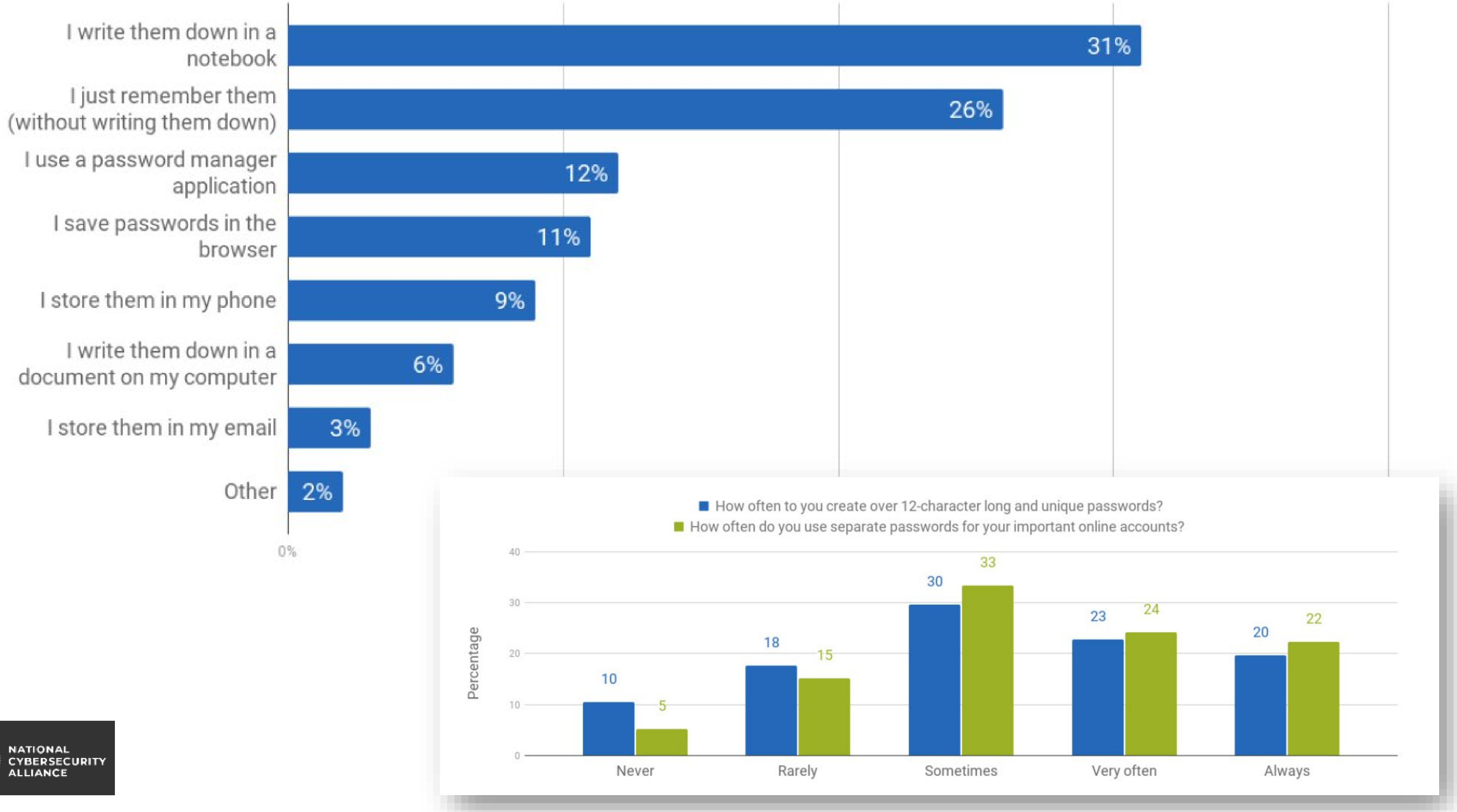
NATIONAL CYBERSECURITY ALLIANCE

Whose Responsibility is Cybersecurity?



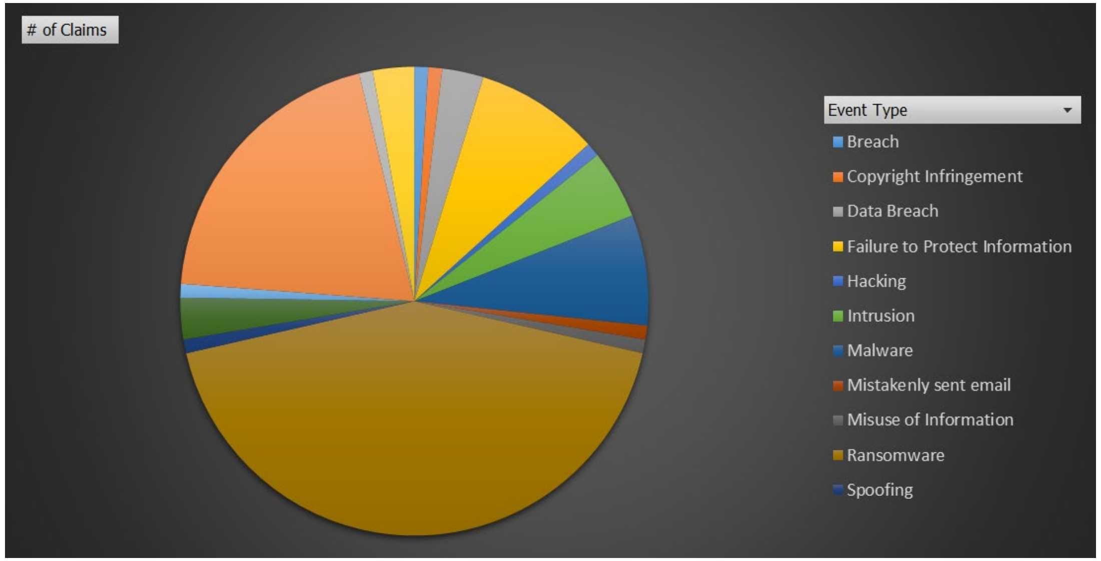
NATIONAL CYBERSECURITY ALLIANCE

Passwords



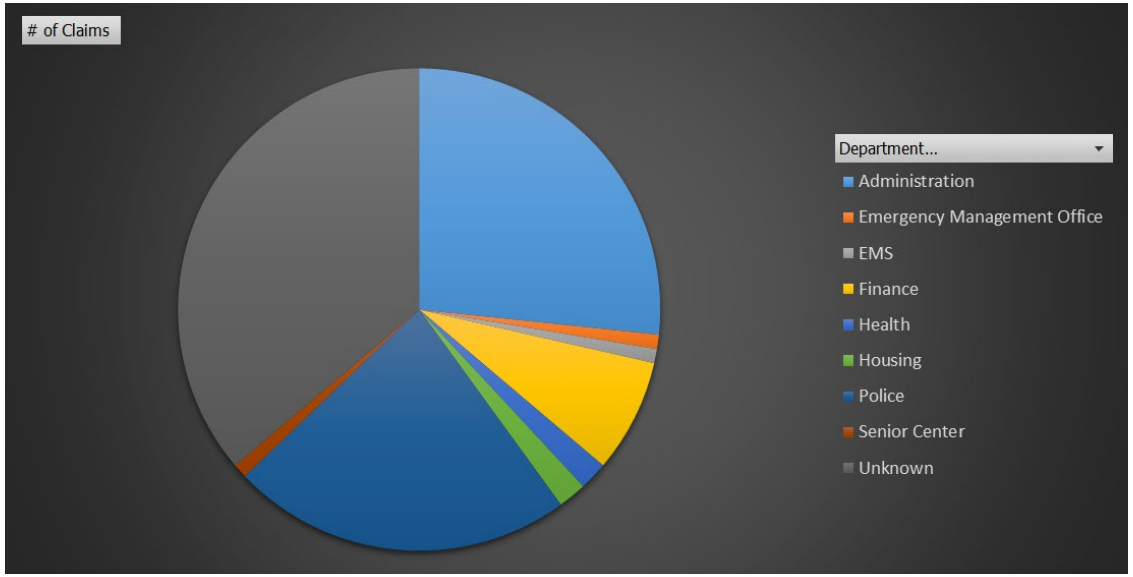
NATIONAL CYBERSECURITY ALLIANCE

Overview of NJ Public Entity Events



By Department

By Event Type



Our Neighbors’ Experiences

Phishing

Social Engineering

Hacktivist

Credential Stuffing

Accidental Release

Unpatched

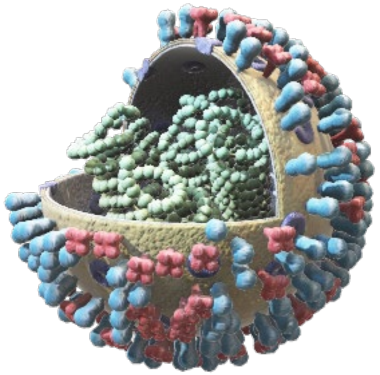
Zero Day

IoT Device

Case #1

Employee receives password reset request from IT

Computer is locked


Ransomware virus spreads

Attacker demands $5m to unencrypt and give back stolen data

Do You Pay?

Don’t Pay?

Case #2

Personal login credentials for social media are breached

Attacker finds person’s work email address

Attacker tries social media password on work account

Attacker has full access to person’s work network

What were the security failures?

Cyber Risk Management

EMAIL DOs & DON'Ts

EMAIL ADDRESSES

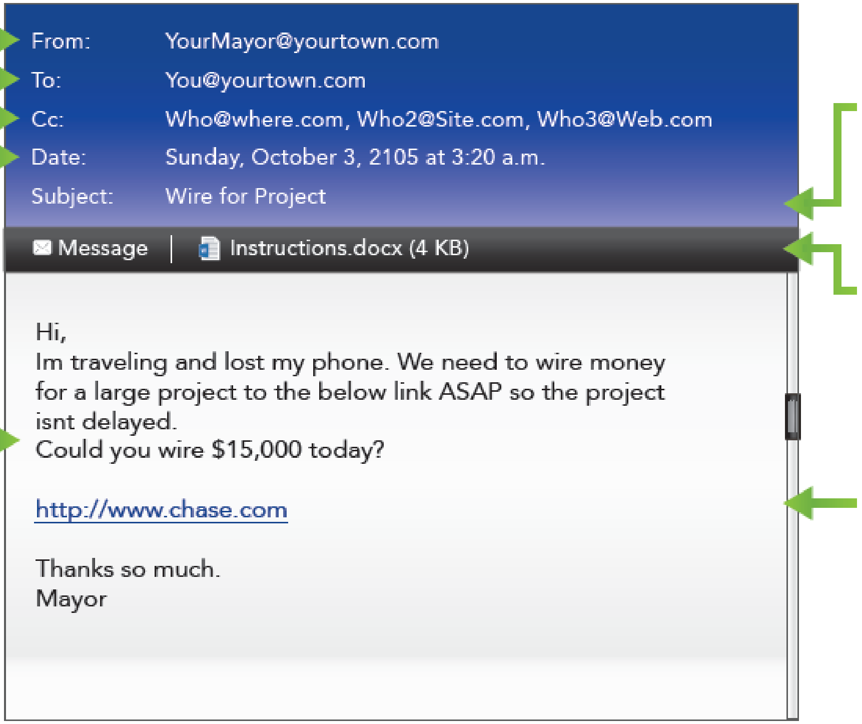
- Do you recognize the sender and the CCs?
- Is the sender's email spelled correctly? (i.e. "YourMayor" vs. "YourMay0r")

DATE & TIME

- Was the email sent on a typical day and at a typical time?

EMAIL CONTENT

- Are the format and grammar in the email typical for the sender?
- Does the content seem atypical?
- Did the sender seem overly urgent?
- Does the email ask for person info/login info?



From: YourMayor@yourtown.com

To: You@yourtown.com

Cc: Who@where.com, Who2@Site.com, Who3@Web.com

Date: Sunday, October 3, 2105 at 3:20 a.m.

Subject: Wire for Project

Hi,
Im traveling and lost my phone. We need to wire money for a large project to the below link ASAP so the project isnt delayed.
Could you wire $15,000 today?

http://www.chase.com

Thanks so much.
Mayor

SUBJECT

- Is the subject a typical style for the sender?
- Does the subject match the email content?

ATTACHMENT

- Is an attachment needed for the email content?
- Were you expecting the attachment?
- Is it a ".txt" file?

LINKS

- Does the link look appropriate?
- Does the web address match the hyperlink shown (scroll over the hyperlink)?

DON'T GET PHISHED!

. . . but if you do, remember to

1. Report to Claim Administrator
2. Call XL Catlin 24/7 Breach Hotline at **(855) 566-4724** and they will triage your incident.

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND • MEL •

Cybersecurity Framework

- Asset Management – *Inventory of your physical technology ecosystem*
- Data Management – *Inventory of your digital technology ecosystem*
- Account Management – *User account inventory and access security, including MFA*
- Vulnerability Management – *Vulnerability scans and patching cadence*
- Logging – *Logging practices*
- Defensive Tools & Strategies – *Antivirus, firewalls, rules and settings*
- Cyber Hygiene – *Employee training and testing*
- 3rd Party Risk Management – *Cybersecurity assessments of the organizations you do business with*
- Policies & Procedures – *Documentation of all security practices, Incident Response Plan and Business Continuity*
- Penetration Testing – *Network penetration testing*

Q & A

Q & A

- Closing Ports – Virtual or physical?
- Training – What if training is not 100%? Part-time, per diem, on leave?
- Penetration Testing – What if Pen testing is not done yet?
- Monitoring Third Parties – Risk assessment tool? Monitoring tool?
- Email Breach Monitoring Tool – Deep web monitoring?

Where do I Go for Help?

Various Organizations

GMIS: https://www.njgmis.org/

CIS / MS-ISAC: https://www.cisecurity.org/

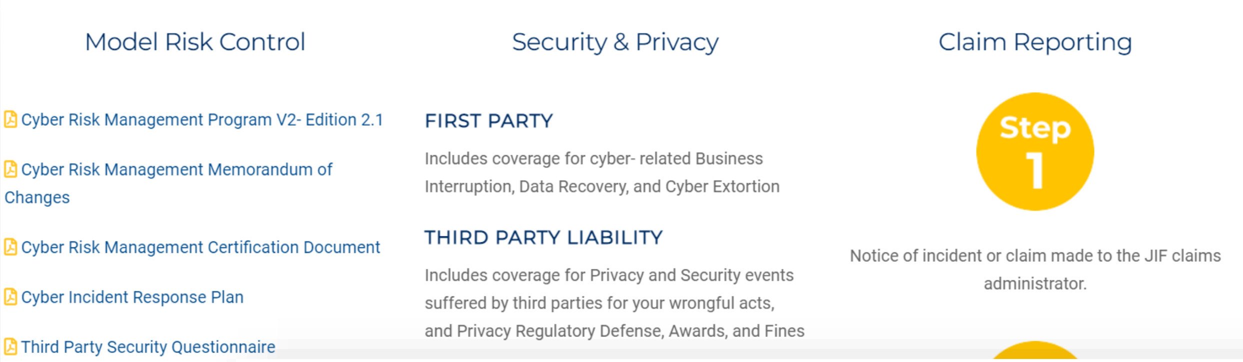
CISA: https://www.cisa.gov/

NJCCIC: https://www.cyber.nj.gov/

US-CERT: https://www.us-cert.gov/

Your insurance company

Cyber JIF Website: https://cyberjif.org/



Model Risk Control

- Cyber Risk Management Program V2- Edition 2.1
- Cyber Risk Management Memorandum of Changes
- Cyber Risk Management Certification Document
- Cyber Incident Response Plan
- Third Party Security Questionnaire

Security & Privacy

FIRST PARTY

Includes coverage for cyber- related Business Interruption, Data Recovery, and Cyber Extortion

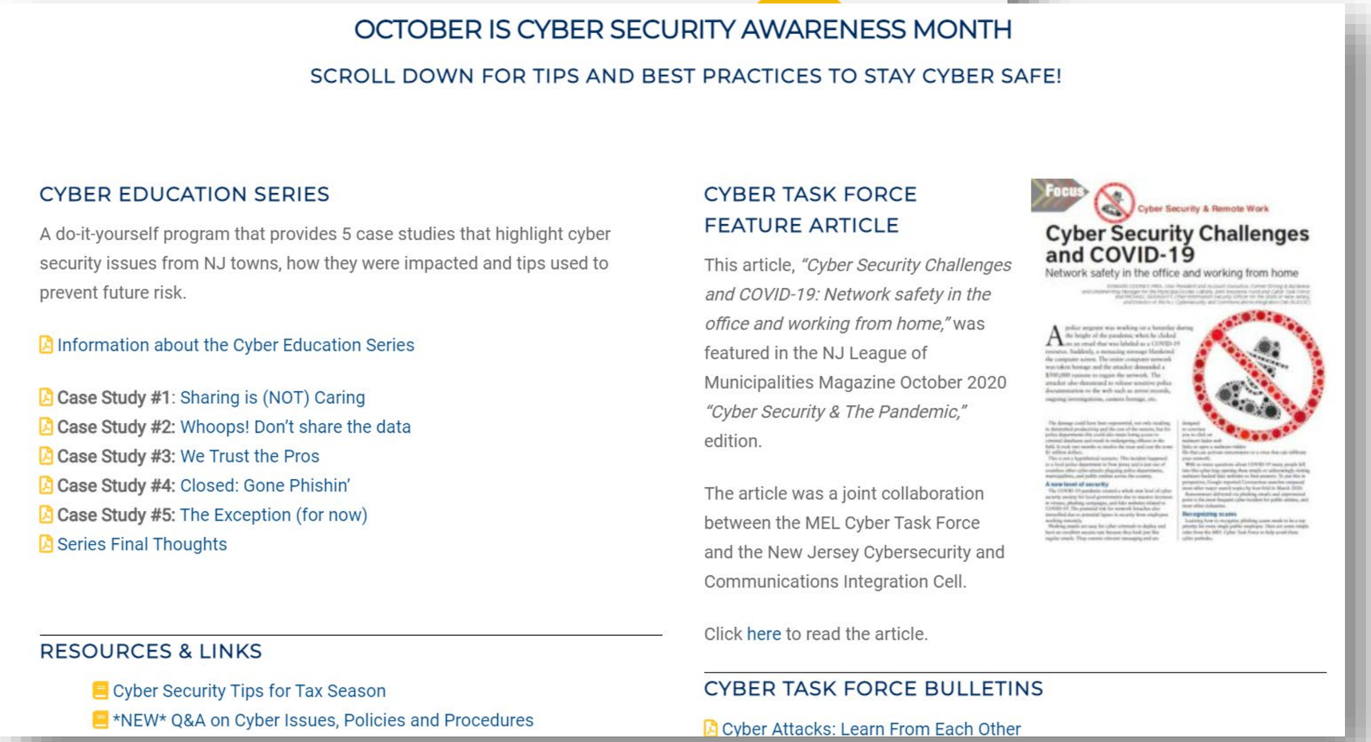
THIRD PARTY LIABILITY

Includes coverage for Privacy and Security events suffered by third parties for your wrongful acts, and Privacy Regulatory Defense, Awards, and Fines

Claim Reporting

Step 1

Notice of incident or claim made to the JIF claims administrator.



OCTOBER IS CYBER SECURITY AWARENESS MONTH

SCROLL DOWN FOR TIPS AND BEST PRACTICES TO STAY CYBER SAFE!

CYBER EDUCATION SERIES

A do-it-yourself program that provides 5 case studies that highlight cyber security issues from NJ towns, how they were impacted and tips used to prevent future risk.

- Information about the Cyber Education Series

- Case Study #1: Sharing is (NOT) Caring
- Case Study #2: Whoops! Don't share the data
- Case Study #3: We Trust the Pros
- Case Study #4: Closed: Gone Phishin'
- Case Study #5: The Exception (for now)
- Series Final Thoughts

RESOURCES & LINKS

- Cyber Security Tips for Tax Season
- *NEW* Q&A on Cyber Issues, Policies and Procedures

CYBER TASK FORCE FEATURE ARTICLE

This article, *"Cyber Security Challenges and COVID-19: Network safety in the office and working from home,"* was featured in the NJ League of Municipalities Magazine October 2020 *"Cyber Security & The Pandemic,"* edition.

The article was a joint collaboration between the MEL Cyber Task Force and the New Jersey Cybersecurity and Communications Integration Cell.

Click here to read the article.

Focus

Cyber Security & Remote Work

Cyber Security Challenges and COVID-19

Network safety in the office and working from home

CYBER TASK FORCE BULLETINS

- Cyber Attacks: Learn From Each Other