Compromise Is Not an Option:

Beat Criminals at Their Own Game Through People, Process, and Technology!

Zoran Jovic – Manager, Cybersecurity Services Group

CLA (*CliftonLarsonAllen LLP)*

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Disclaimer

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Learning Objectives

Recognize	• Recognize the top threats and risks with respect to cybersecurity
Identify	• Identify the current state of cybersecurity maturity at your organization
Understand	• Understand the importance of proactive cybersecurity endeavors

Data Breaches and Cybercrime

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Cybercrime and Black-Market Economies

- Black market economy to support cyber fraud
  - Business models and specialization
  - Underground Marketplace (The Dark Web)

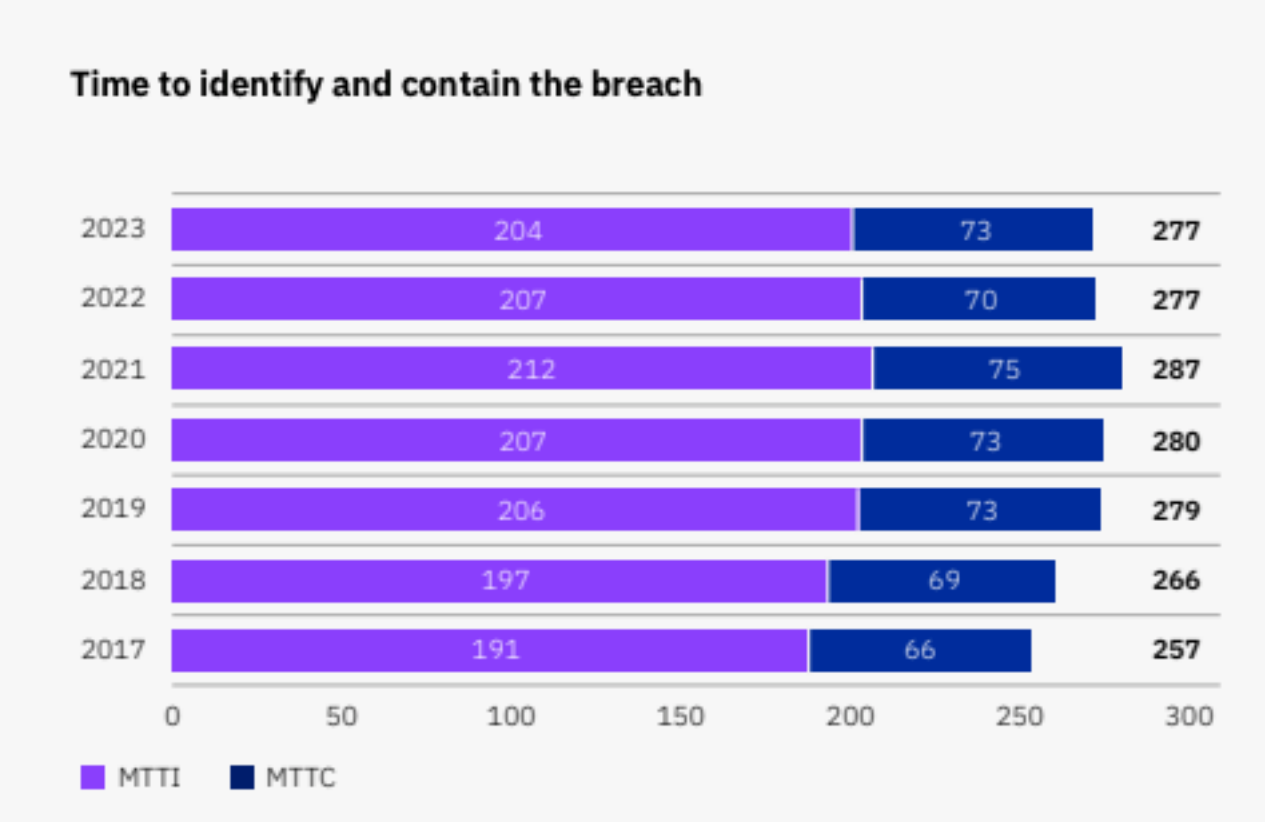
- Most common cyber fraud scenarios we see affecting our clients
  - Theft of information
    - Log-in Credentials
    - ePHI, PII, PFI, account profiles, etc.
    - Credit card information
  - Ransomware and interference w/ operations

➢ To the Hackers, we all look the same…

They will hit you with any or all of the following:

1. Email Spear Phishing Attacks
2. Password Guessing and Business Email Account Takeovers
3. Payment and Funds Disbursement Transfer Fraud
4. Ransomware
5. Extortion to avoid breach disclosure

Average Days to Identify and Contain a Data Breach

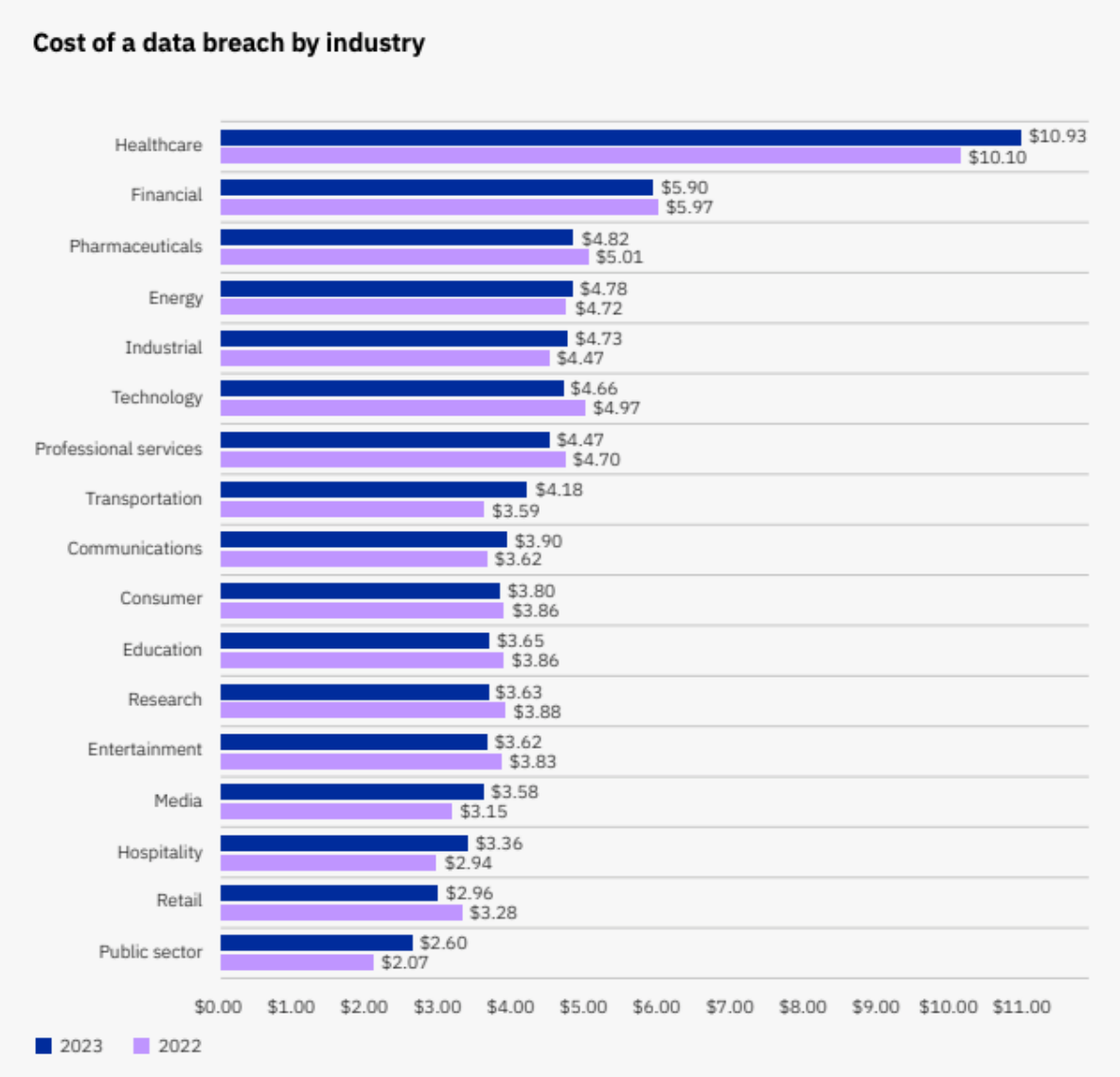


Average is 277 days

- 204 days to identify a breach
- 73 days to contain the attack

Source: IBM Security Cost of a Data Breach Report 2023

Average Cost of a Data Breach

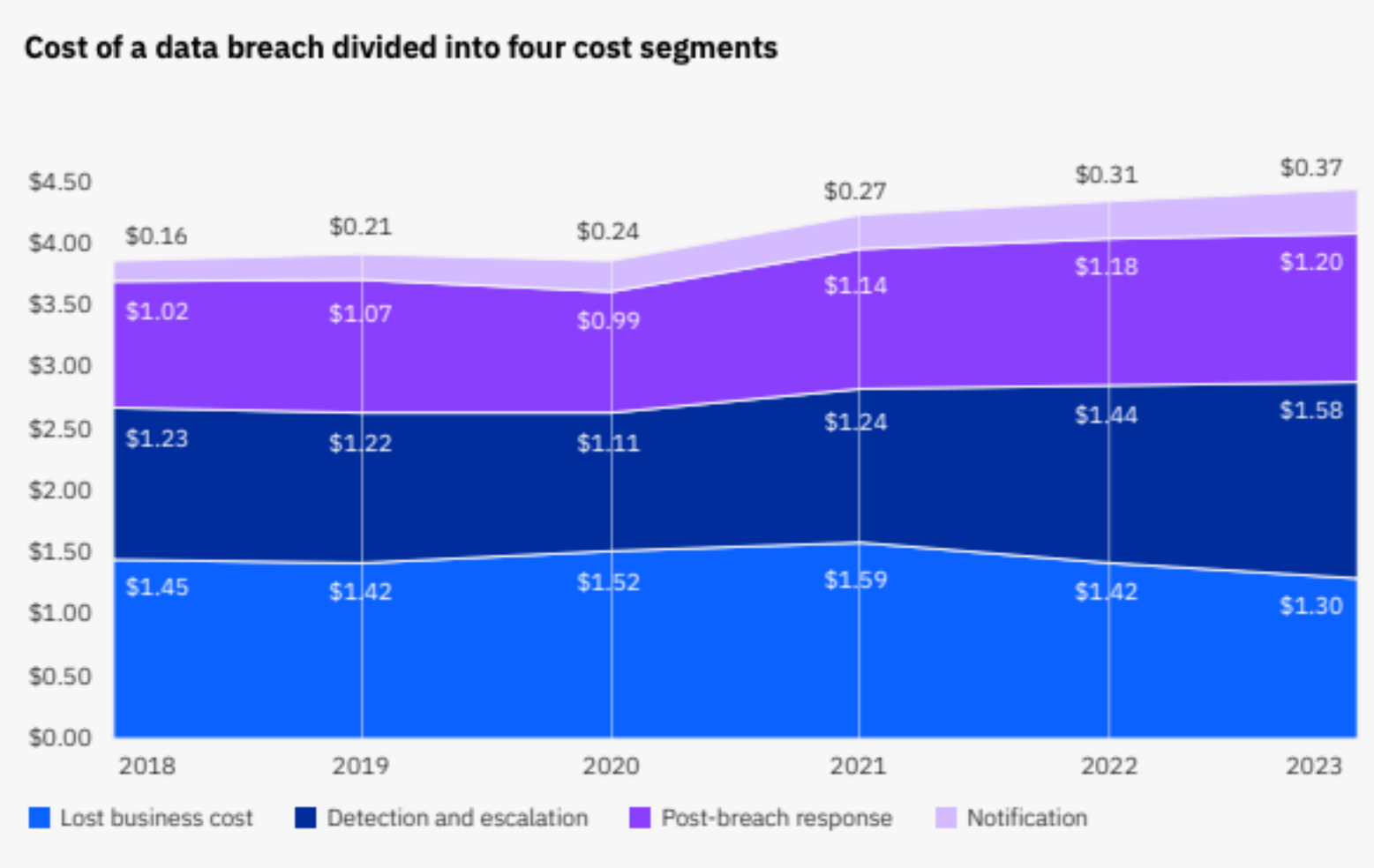


Factors

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

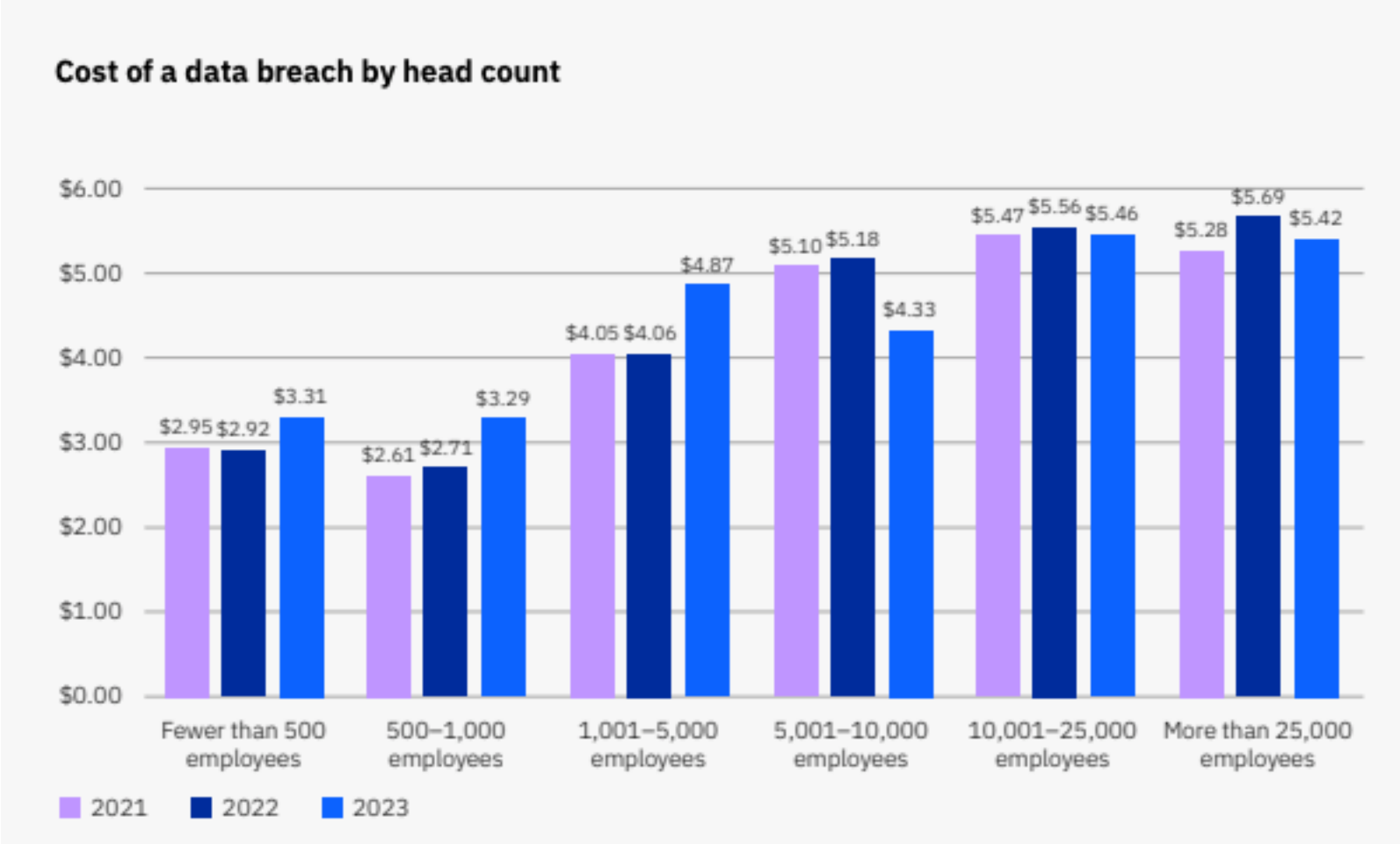
Source: IBM Security Cost of a Data Breach Report 2023

Cost by Factor



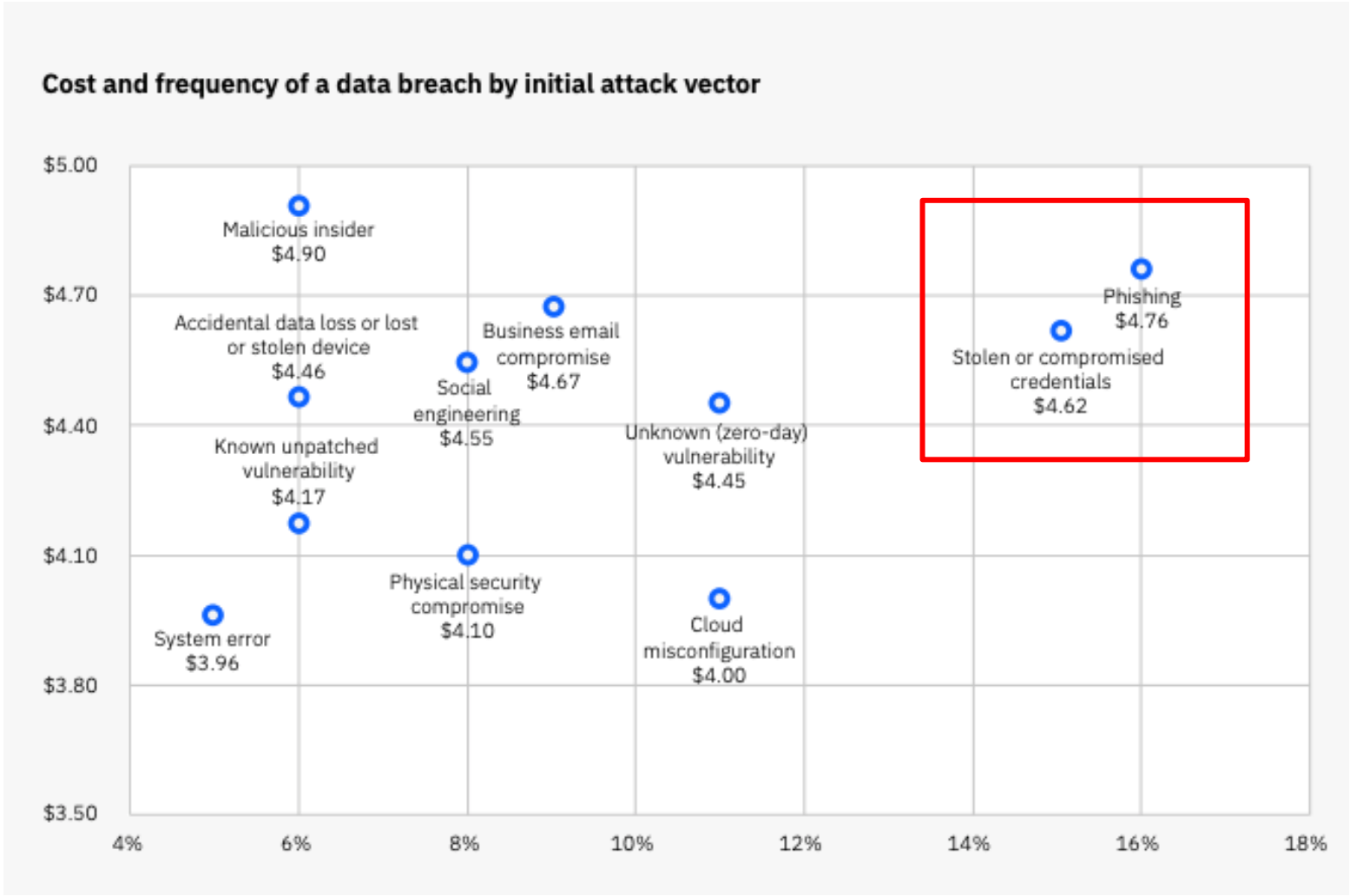
Source: IBM Security Cost of a Data Breach Report 2023

Cost by Factor



Source: IBM Security Cost of a Data Breach Report 2023

Cost by Attack Vector



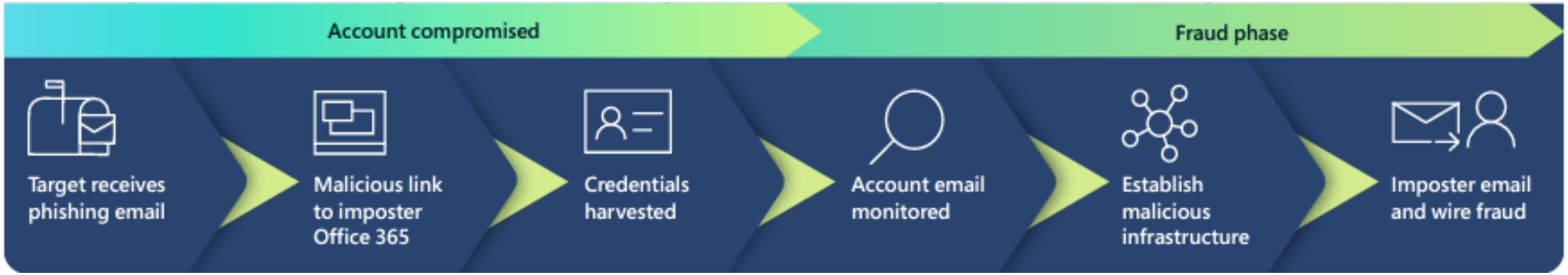
Source: IBM Security Cost of a Data Breach Report 2023

Email Phishing & Business Email Compromise

We'll get you there.

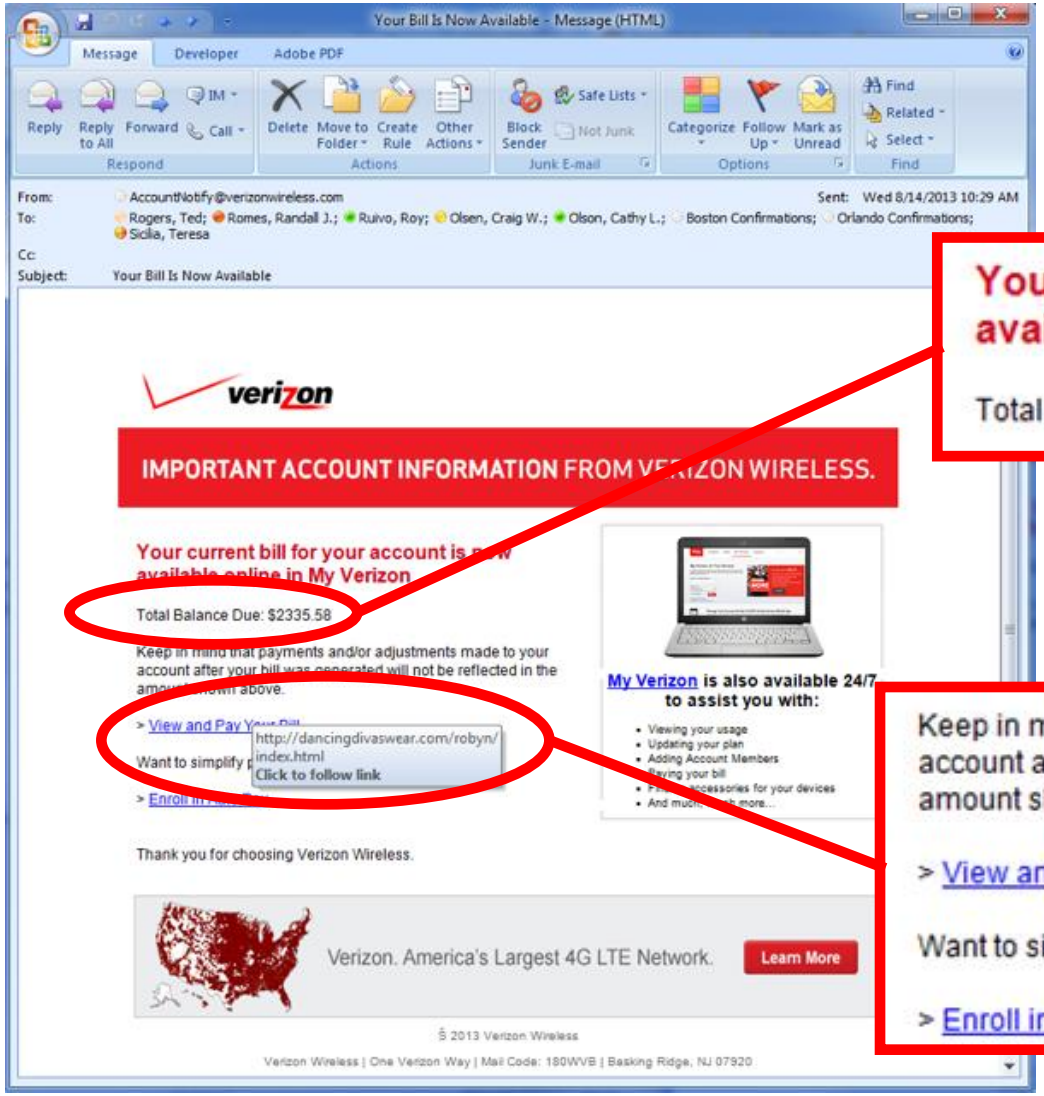
CPAs | CONSULTANTS | WEALTH ADVISORS

Email Compromise Timeline

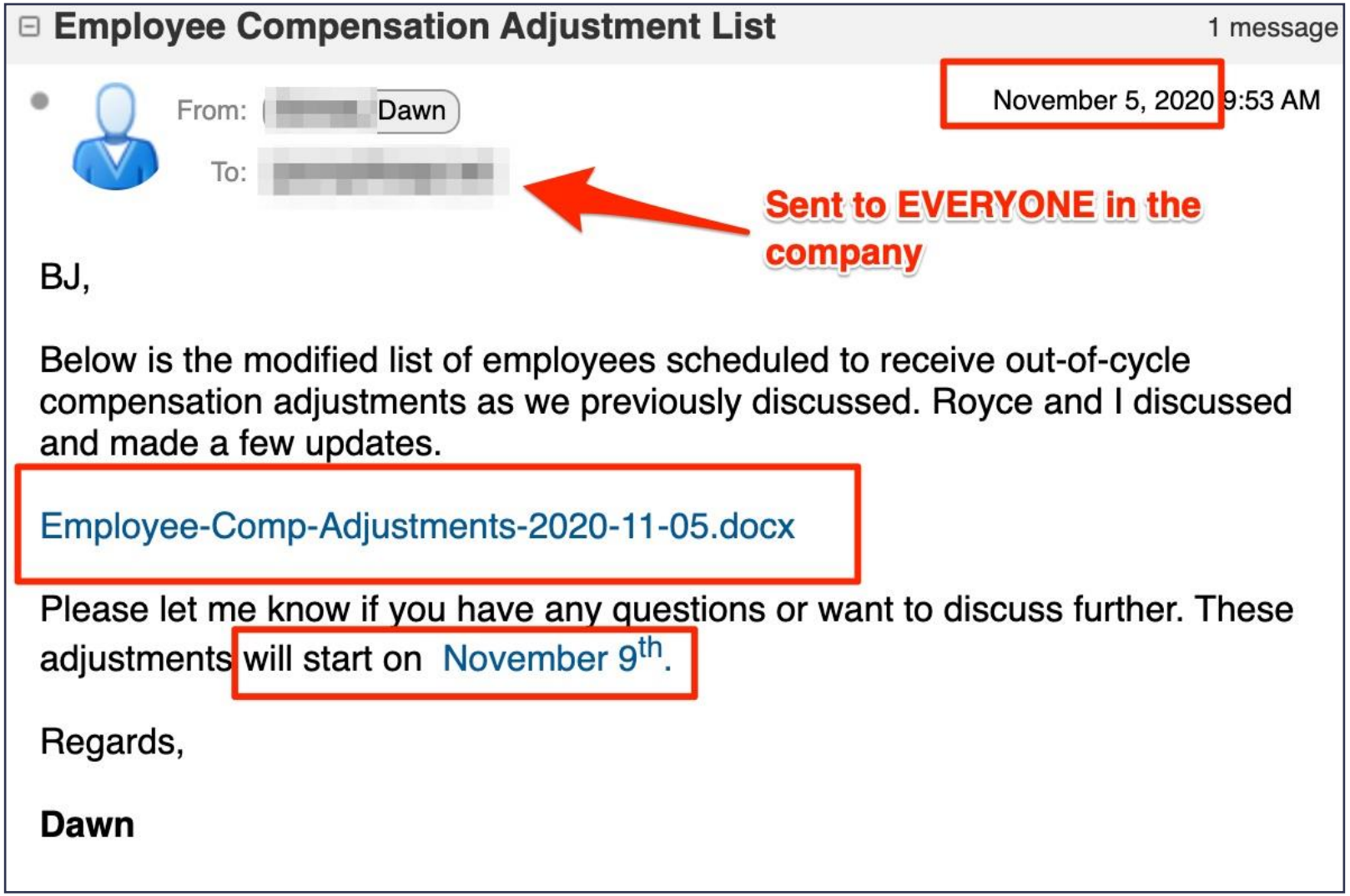


- Credentials = Access
- Gathering user credentials is generally the goal
- The credentials are then sold or traded on the dark web

Emotional Response Required!



”Accidental” Email Example



Employee Compensation Adjustment List 1 message

From: [redacted] Dawn

To: [redacted]

November 5, 2020 9:53 AM

Sent to EVERYONE in the company

BJ,

Below is the modified list of employees scheduled to receive out-of-cycle compensation adjustments as we previously discussed. Royce and I discussed and made a few updates.

Employee-Comp-Adjustments-2020-11-05.docx

Please let me know if you have any questions or want to discuss further. These adjustments will start on November 9th.

Regards,

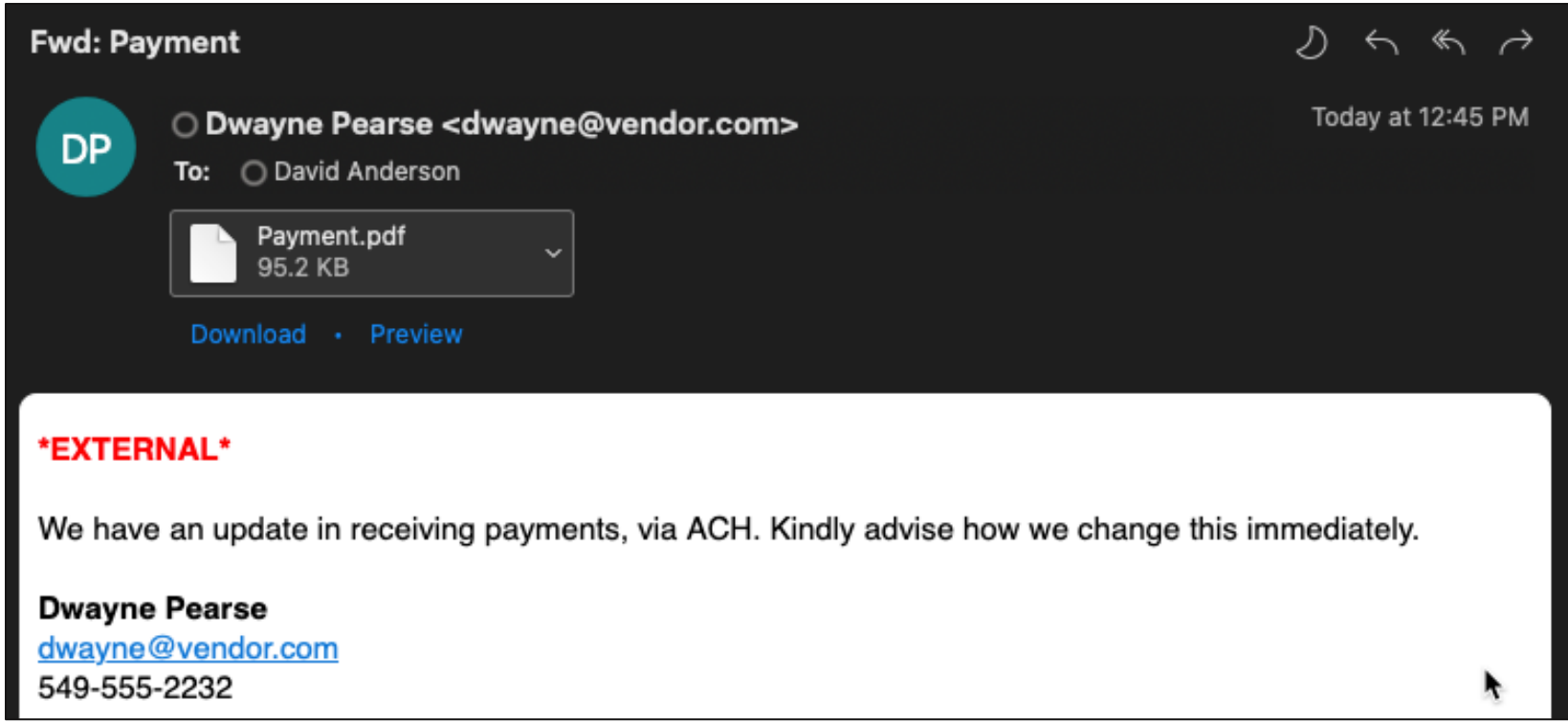
Dawn

Business Email Compromise

- Fraudsters impersonate employees, service providers, or vendors via email in an attempt to…

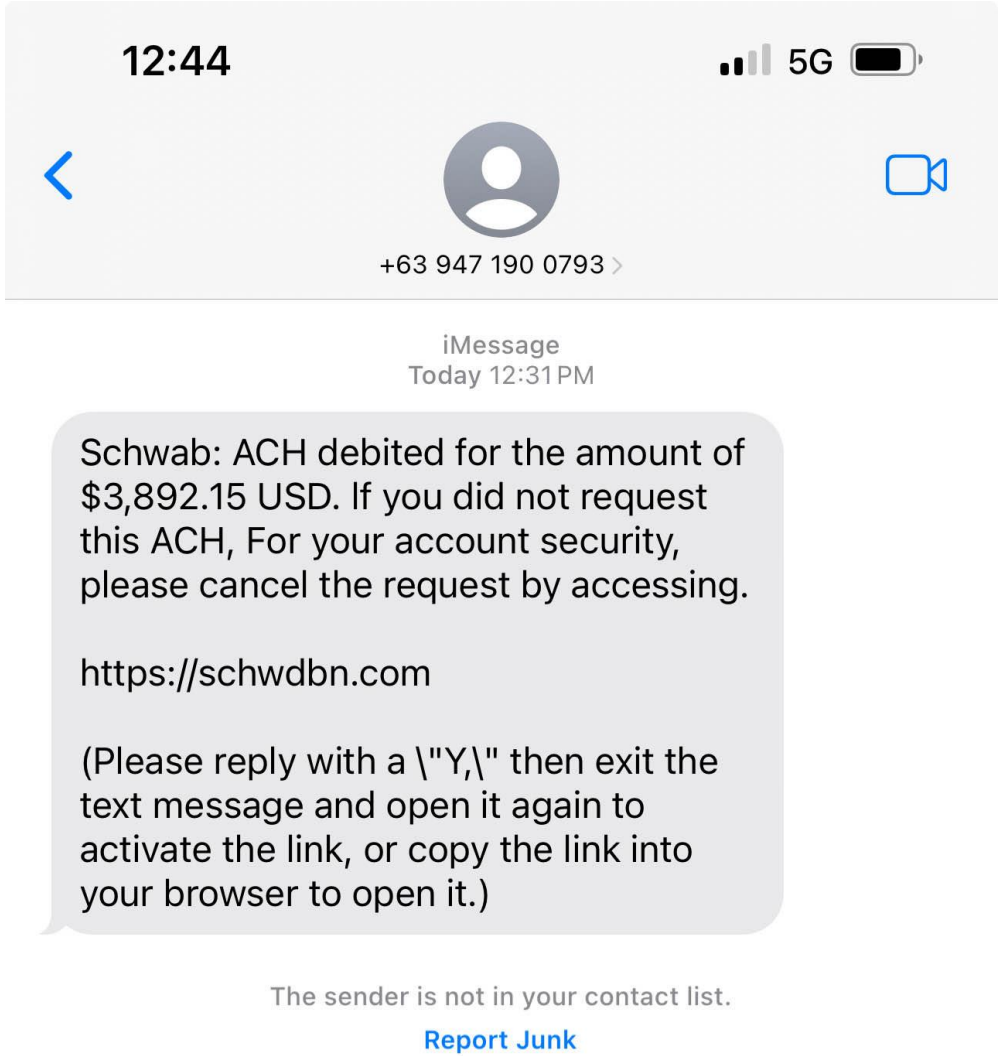
EXAMPLES

- Vendor payments
- Direct deposit changes
- Login to cloud application
- Etc.



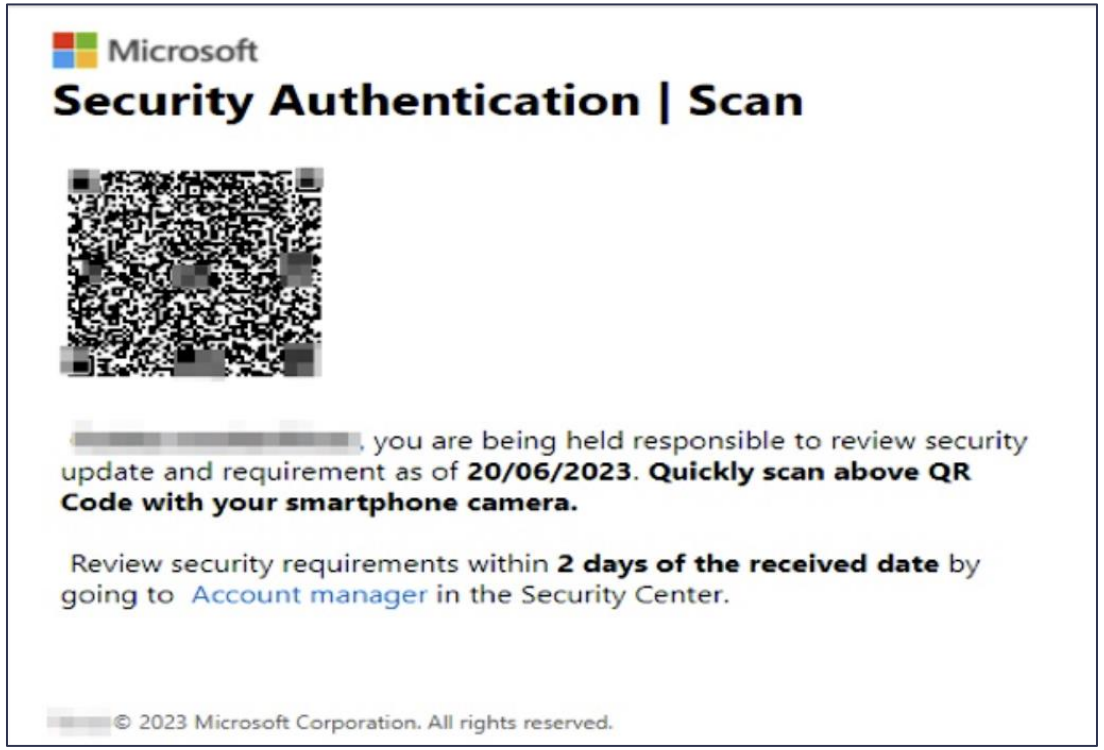
SMS Phishing

- If it looks/feels suspicious…



QR Phishing

- Emails contain a PDF or image of a QR code
- QR emails are much harder to detect and block



Identify Suspicious Emails

- Generic greetings
- Spelling or grammatical errors
- Suspicious email addresses or domains
- Requests for personal information
- Be cautious of email attachments and links
- Avoid clicking links or downloading files!

Avoiding Social Engineering

- Be skeptical and question requests
- Independently verify the legitimacy of any requests
- Be wary of urgency and high-pressure tactics
- Be cautious about sharing sensitive information
- Hover over links (without clicking) to inspect the actual destination address

Credential Compromise

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

“Keys to the kingdom”

- Microsoft 365 credentials remain one of the most highly sought after account types for attackers
- Once compromised attackers can log in to corporate-tied computer systems

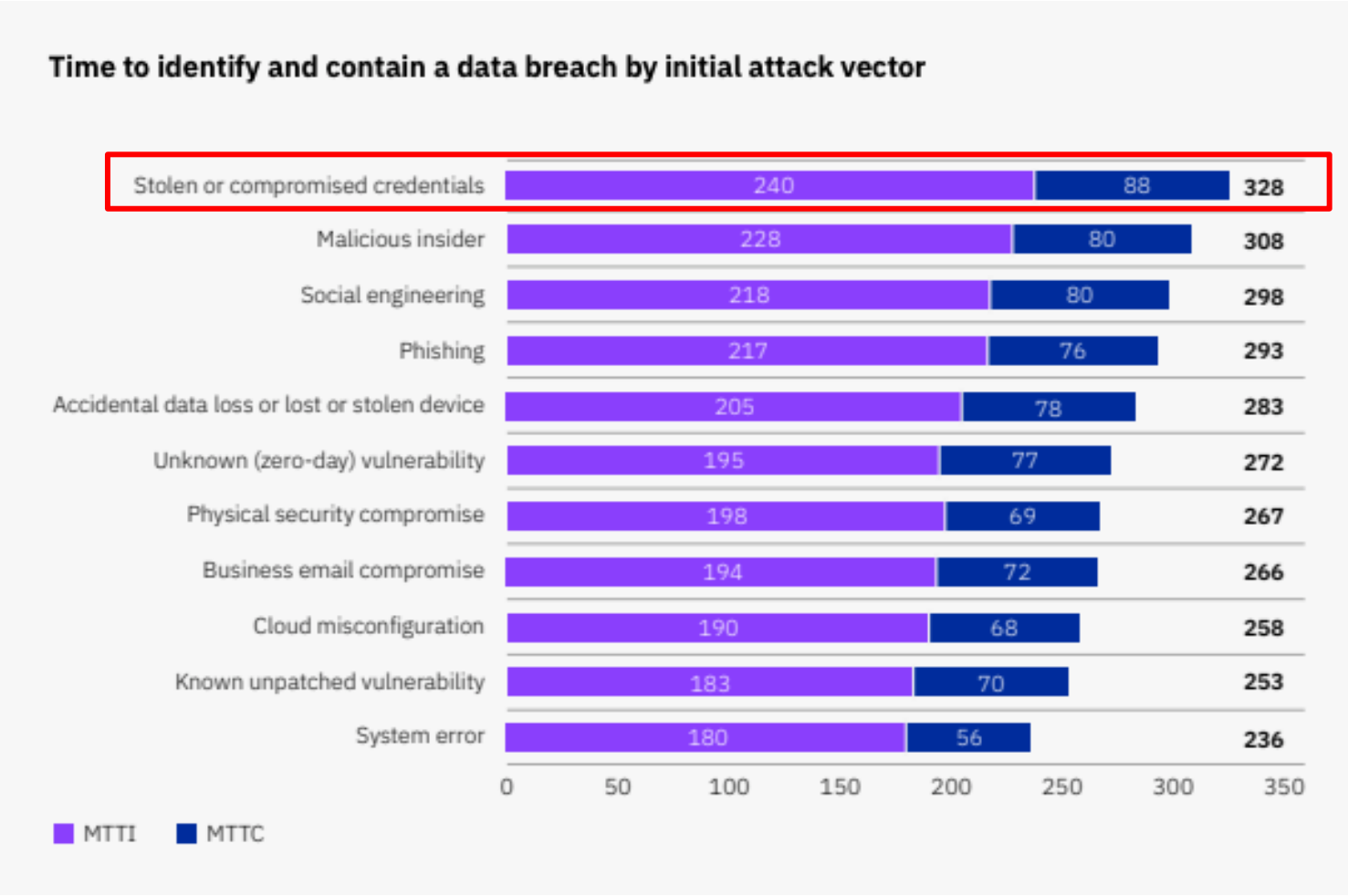
1hr 12 m

The median time is takes for an attacker to access your private data if you fall victim to a phishing email

1hr 42 m

The median time for an attacker to begin moving laterally within your corporate network once a device is compromised

Passwords



- Attackers use tools to steal and guess credentials

Source: IBM Security Cost of a Data Breach Report 2023

Password Strategies:

- **Pass Phrases – Looooooong natural language**

  Password23 <---------- ***Unforgiveable!***

  Summer23 <---------- *Terrible*

  *N*78fm/12f* <---------- *Painful*

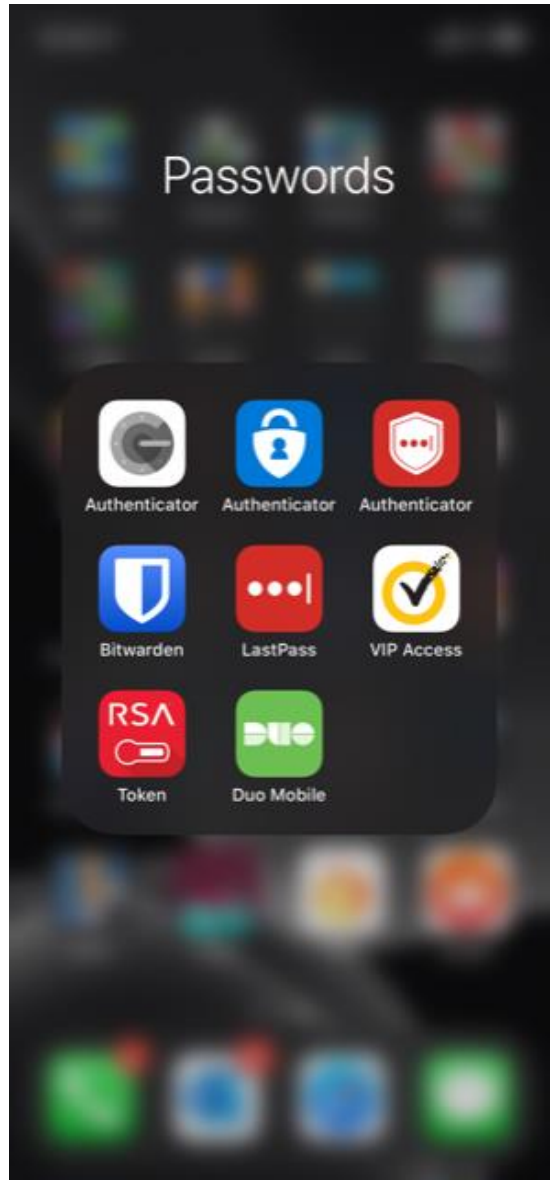
  Wallet Painting lamp <-- Good

  I bought the Chevy in 1992 from Jack Smith! <-- **Best**

- Password tools: **Password Managers** are needed

Multi-Factor Authentication (MFA)

- All remote systems/applications should require MFA
  - Email, VPN, Remote Desktop, Banking, etc.
- Not all MFA is created equal
  - Number matching, push notifications, phone calls, SMS text, soft token (6 digit code), etc.



Protect your credentials!

Use looong passwords/passphrases

Do not reuse passwords

Use multi factor authentication and password managers

Geo-Restrict and System-restrict access to email if possible

Most importantly: Don’t use obvious passwords!!!

Are You Ready For The Upcoming Cyberattack?

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Are We Ready?

What are we doing to prevent cyber attacks?

What will we do if we are attacked?

Have we been attacked/compromised in recent history?

Did this result in data loss?

10 Questions You Need To Answer

1. Do we have a Formal Information Security Program in Place?
2. What Data is Important to our Organization?
3. How are Vulnerabilities Managed at the Organization?
4. When was our Risk Assessment or Security Audit performed?
5. Are Employees Receiving Security Awareness Training?
6. Are we Ready for a Cyber Attack?
7. What Could an Attacker do in our Environment?
8. Do we have an Incident Response Plan in Place?
9. How do we Assess Third-Party Risks?
10. Do we have a Business Continuity and Disaster Recover Plan in Place?

Develop Policies, Standards, and Procedures

Network and System Policies

- Logging and monitoring of security events
- Remote access
- Wireless networking
- Patch management
- Firewall management
- Antivirus management
- Intrusion Detection/Prevention

The Board should review (annually)

- Information Security Program and Status
- IT and Information Security Policies
- Security Breaches or Attempted Breaches
- IT Strategic Plan
- Information Security Risk Assessment
- Business Continuity Plan and Testing Results
- Incident Response Plan
- Results from Vendor Management Reviews
- Insurance Coverage for Cybersecurity

Proactively Manage and Test Vulnerabilities

Do you have an inventory of assets and vulnerabilities?

Within how many days are critical and high vulnerabilities addressed for:

- Operating Systems?
- Network Devices?
- Applications?

Are there any end-of-life systems in the environment?

- What is the goal with these systems?

Is Penetration Testing performed?

- Done at least annually?

Test People, Processes, and Technology!

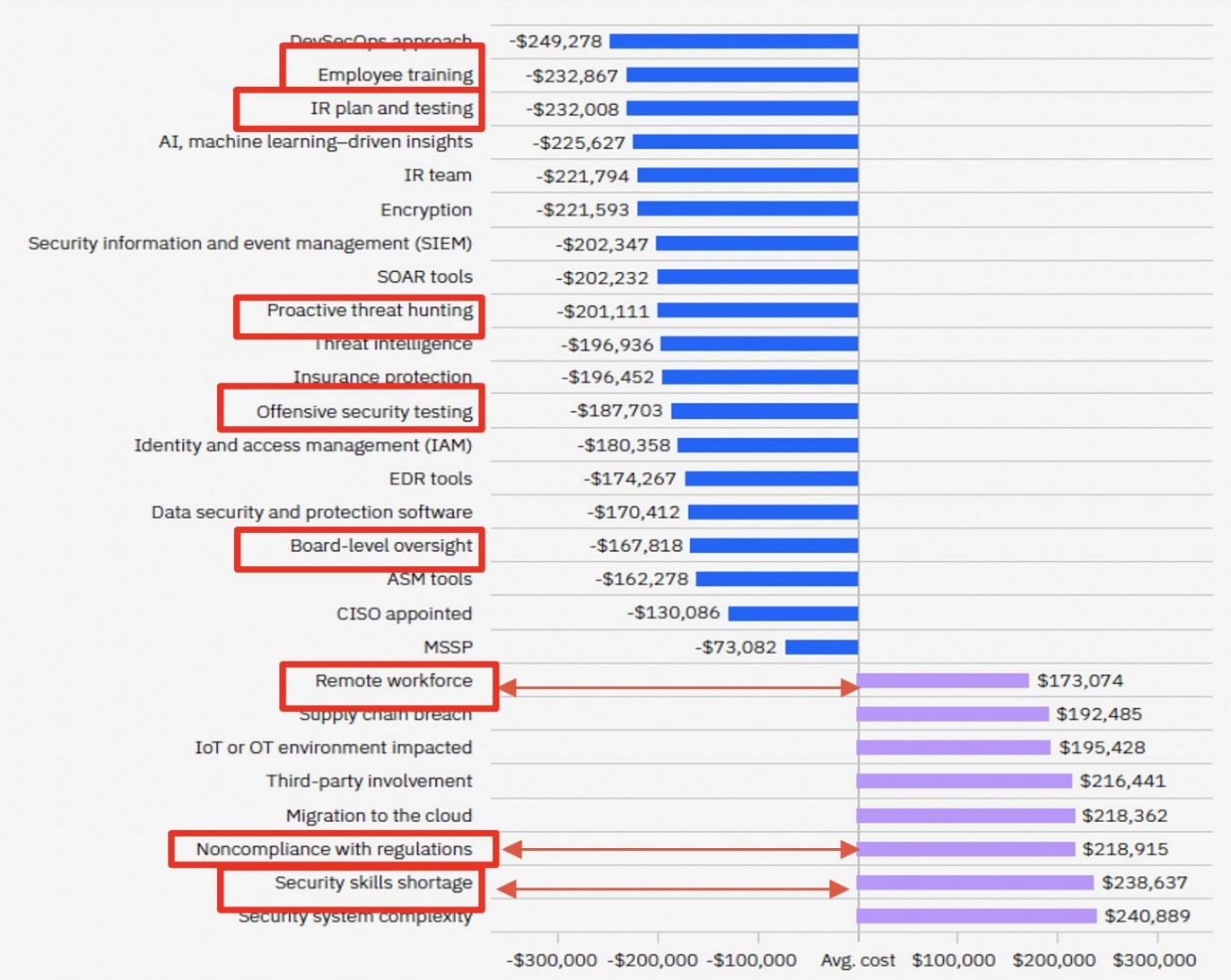
Prepare For An Incident

- Develop a “Business Continuity – Disaster Recovery” plan
- Create incident response policies
- Develop roles and responsibilities
- Establish communication procedures
- Ensure we have the correct people, process, and tools/technologies in place

Practice

- Like all emergency procedures, they need to be practiced
- Penetration testing validates/exploits vulnerabilities as an attacker would
- Table-top exercises help participants walk through the incident and response procedures
- Both should be conducted annually

Incident Response Preparedness- Cost Savings



Source: IBM Security Cost of a Data Breach Report 2023

Thank You!

Zoran Jovic
Manager, Cybersecurity
813-947-9656
Zoran.Jovic@CLAconnect.com

We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS