



# Five tactics you need to know for an effective cybersecurity strategy

Cybersecurity Summit

September 28, 2022



# Five tactics you need to know for an effective cybersecurity strategy



## **Rex Johnson**

Executive Director, CAI Cybersecurity

- Over 30 years senior level management experience encompassing IT, cybersecurity, privacy, digital forensics and analysis, and enterprise risk management.
- Frequent speaker on cybersecurity addressing national and international audiences with Gartner, Secure World, and the Information Systems Audit and Control Association.
- Retired Lieutenant Colonel from the US Army and holds CISSP, CISA, CIPT, PMP, and PCIP certifications.

# Agenda

- Objectives
- Current Cyber Landscape
- What Can I Do?
- Summary
- Questions and Answers





# Objectives

## Learning Objective #1

Understand the importance of business and operational activities which have an impact on the data security and privacy of the organization.

## Learning Objective #2

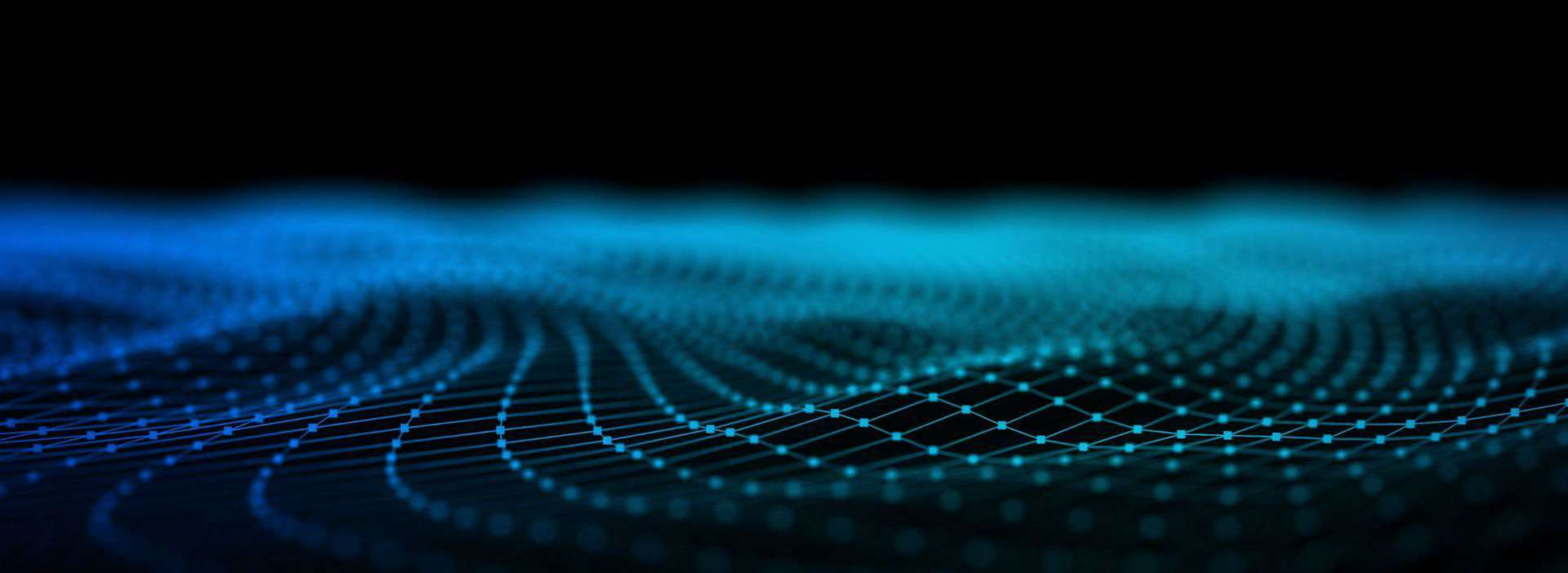
Identify risks that exist due to advanced privilege of users allowing for access to critical information and executable processes.

## Learning Objective #3

Be able to understand the critical elements of the incident response plan.

## Learning Objective #4

Learn how security awareness plays a role.



# Cybersecurity Landscape Overview

# Data Breach Statistics



**\$4.35M**

Average total cost



**277 days**

Average time to  
identify & contain



**\$4.54M**

Average cost of  
ransomware



**10x**

Recovery cost over  
the ransom payment



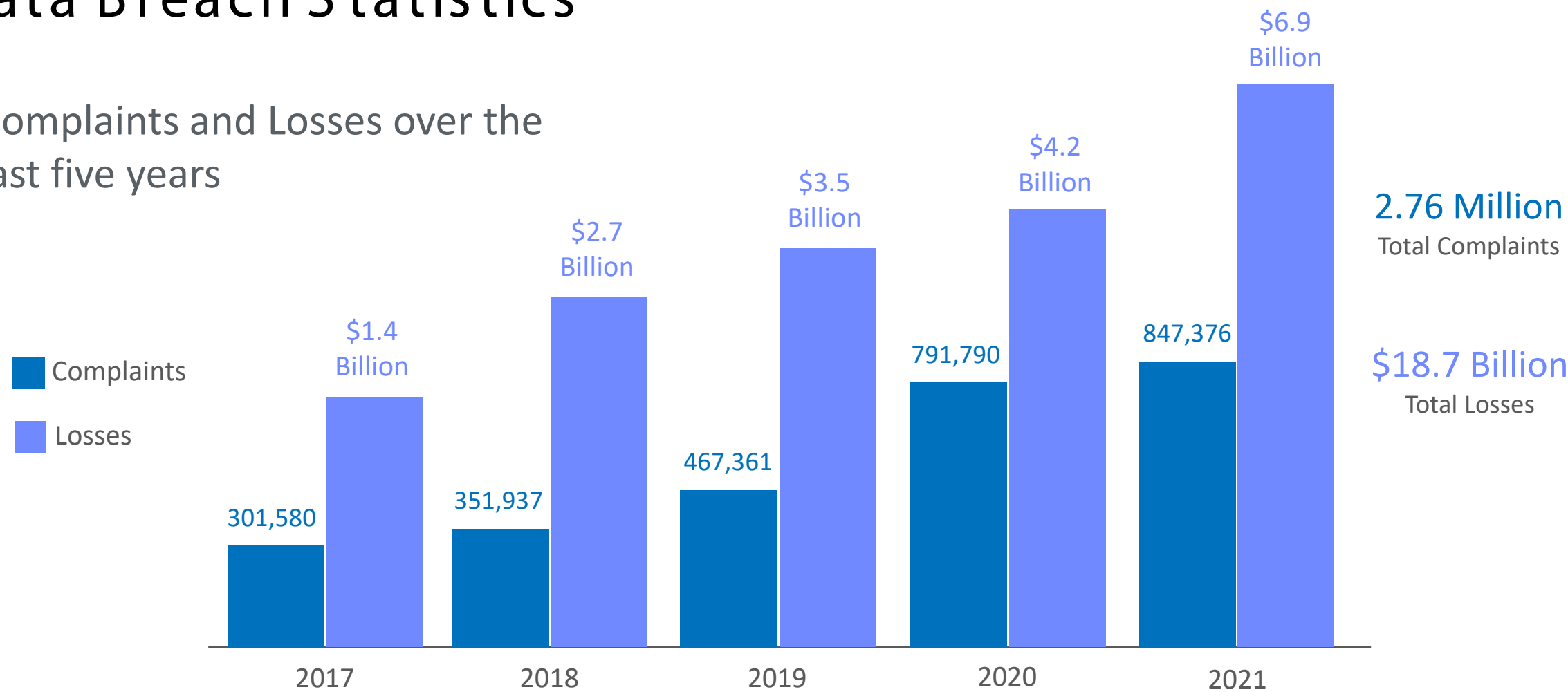
**4%**

Of those who paid  
received all their data  
back

Sources: IBM 2022 Cost of Data Breach Study  
Sophos, The State of Ransomware 2022

# Data Breach Statistics

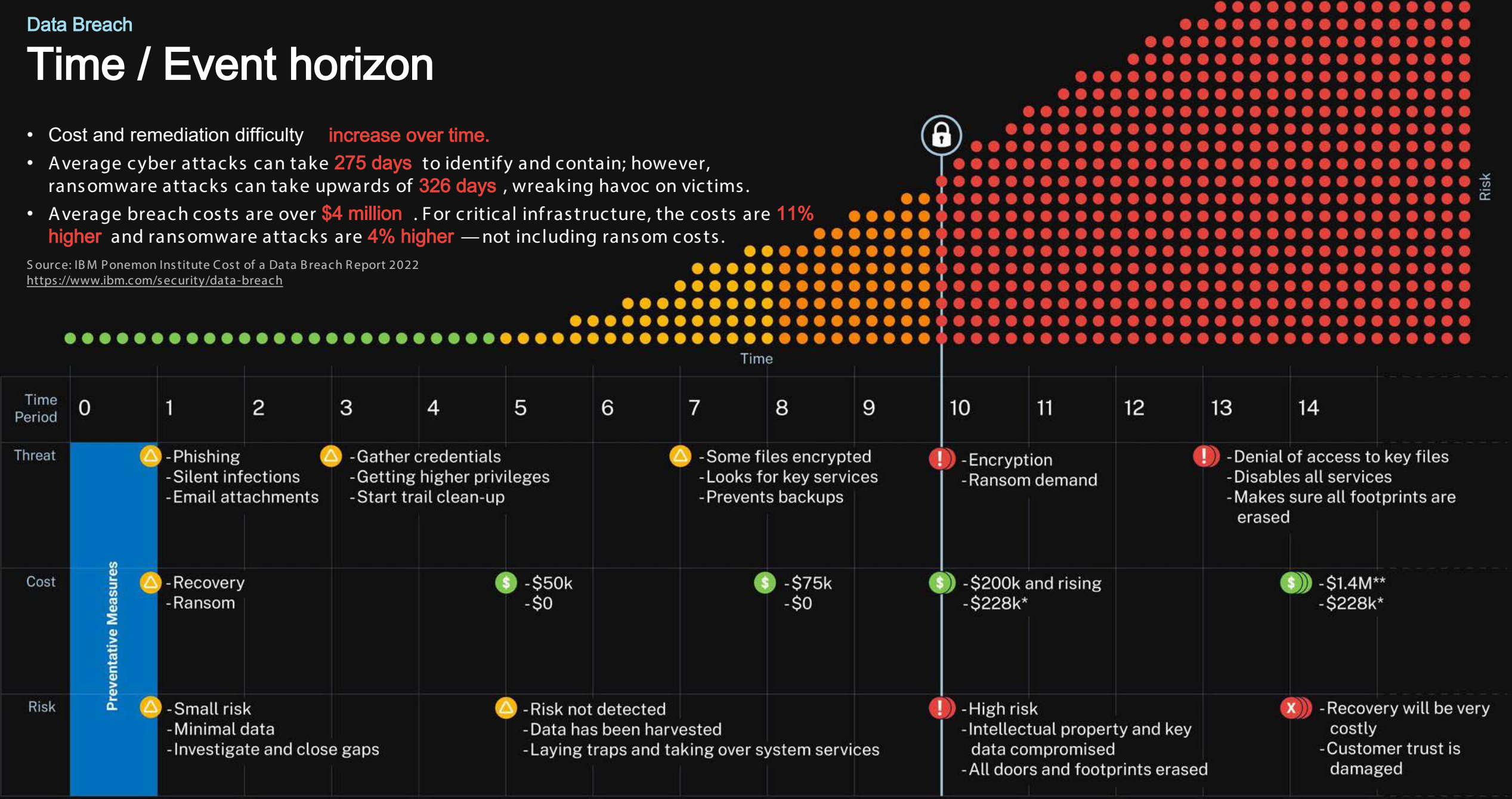
Complaints and Losses over the last five years



# Time / Event horizon

- Cost and remediation difficulty **increase over time.**
- Average cyber attacks can take **275 days** to identify and contain; however, ransomware attacks can take upwards of **326 days** , wreaking havoc on victims.
- Average breach costs are over **\$4 million** . For critical infrastructure, the costs are **11% higher** and ransomware attacks are **4% higher** — not including ransom costs.

Source: IBM Ponemon Institute Cost of a Data Breach Report 2022  
<https://www.ibm.com/security/data-breach>





# What About Cybersecurity Insurance?

## 2017 – “We just want to be in the cyber market”

- Inexpensive add -on by agents with no cyber -knowledge, no security questions

## 2021

- \$20B market
- But a very poor “loss ratio”
- Lloyd’s: “no more silent cyber”

## 2022

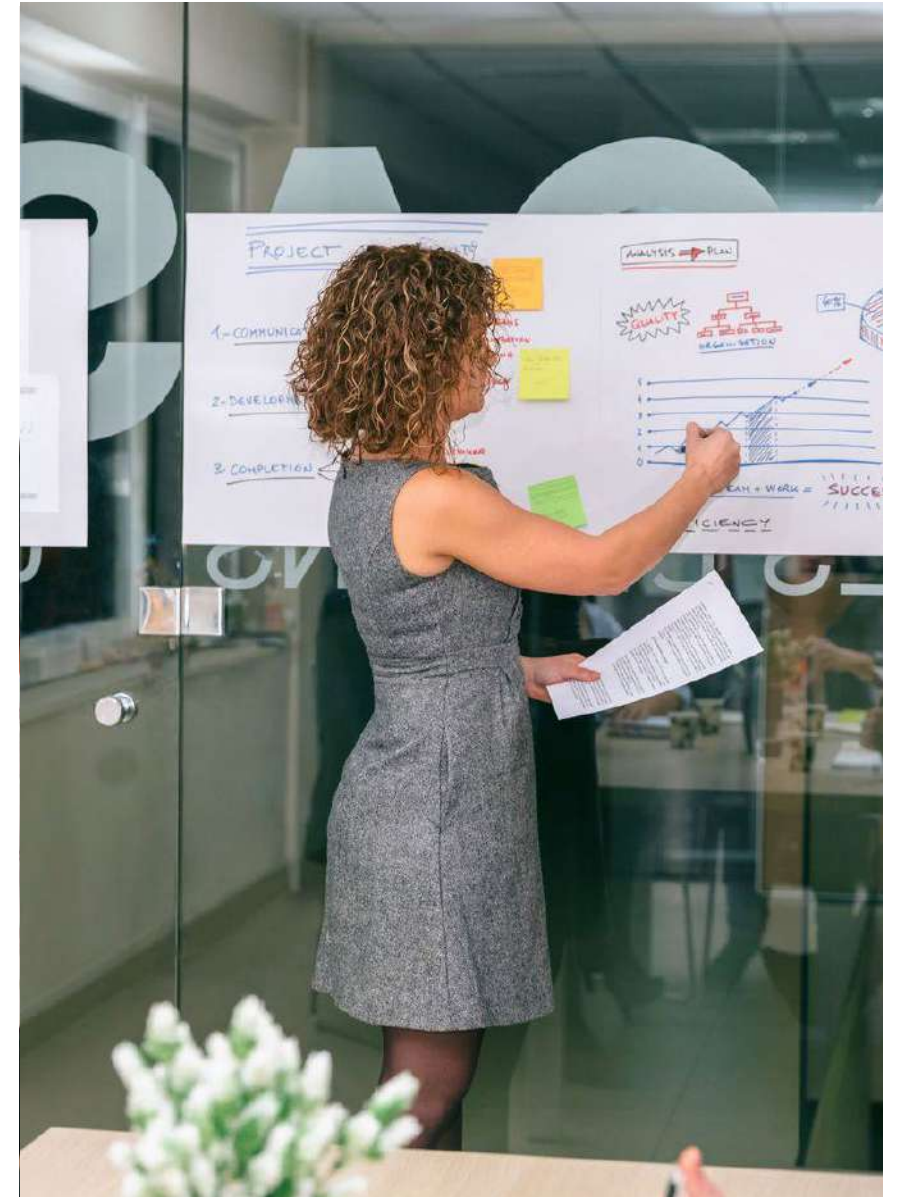
- Costs have risen and there are more requirements to qualify
- Sub-limits come into play (“up to \$100K for X expense”)
- Increased rates are coming
- No reliable actuarial tables

Source: “State of the Industry, Challenges, Estimating Risk”  
Cynthia James, Microsoft (RSA 2022)

# Polling Question 1

How many of you have cybersecurity insurance?

- A. Yes
- B. No
- C. Not Sure



# Some Facts on Insurance

- 95% of claims were paid
- 70% of the time insurance providers paid business recovery costs
- But now...
  - May not pay for losses due to outdated or unsupported systems
  - MFA
  - Phish-test users
  - Disaster Recovery / Incident Response
  - MDR/XDR
  - Encryption
  - Enforce Data Loss Prevention
- Premiums will rise

Source: "State of the Industry, Challenges, Estimating Risk"  
Cynthia James, Microsoft (RSA 2022)

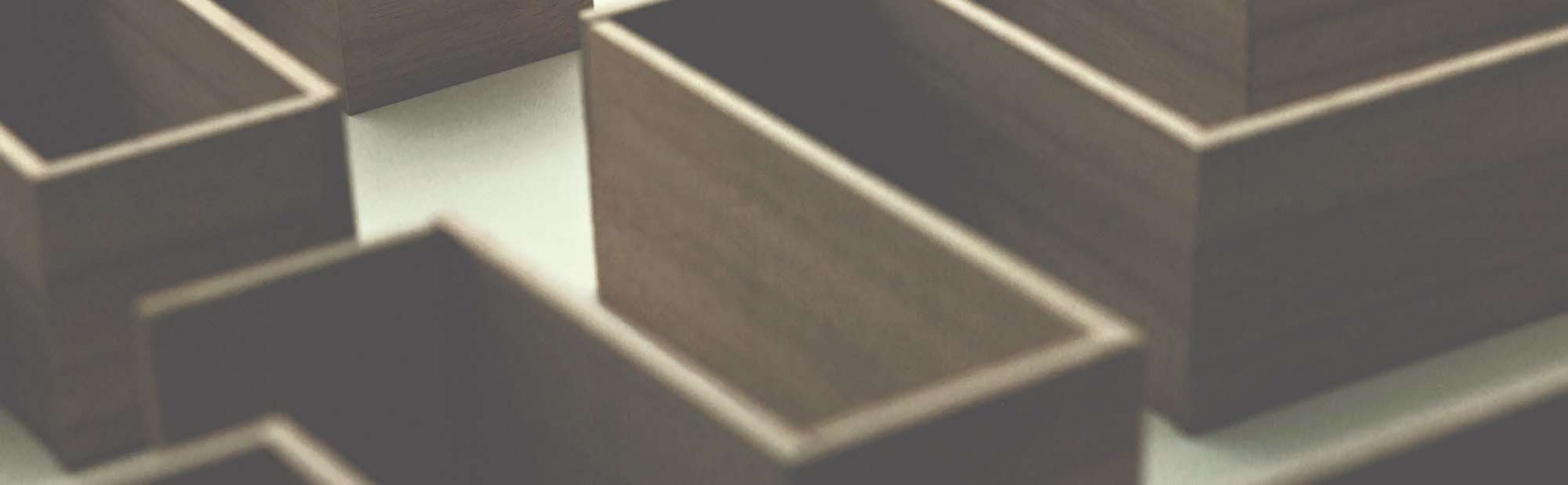
# What Can I Do?



# Five Tactics for An Effective Cybersecurity Strategy

1. Understand Your Environment
2. Develop and Test Incident Response
3. Build a Culture of Security Awareness
4. Choose a Trusted Partner
5. Conduct Periodic Checks



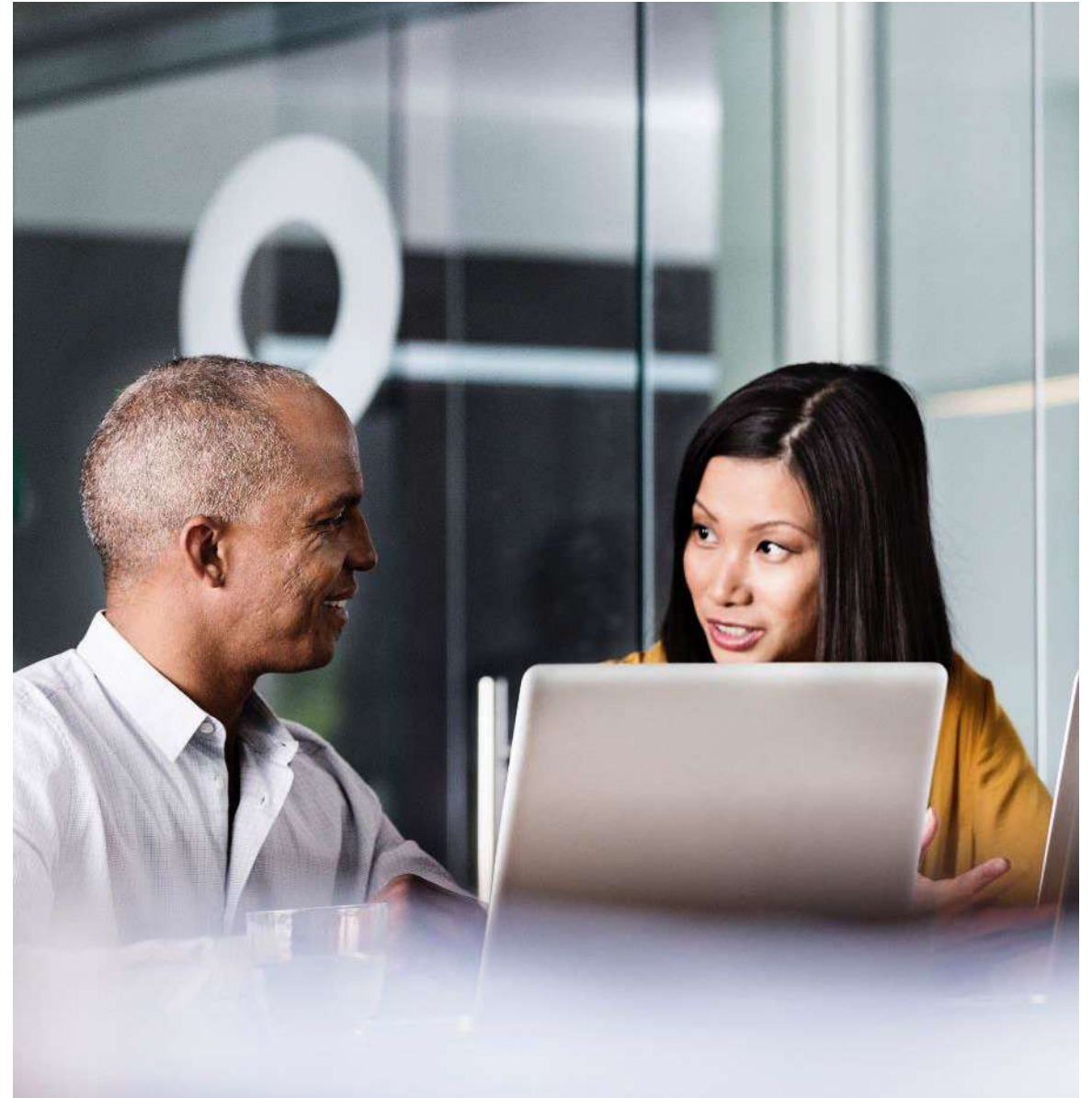


Cybersecurity

# 1. Understand Your Environment

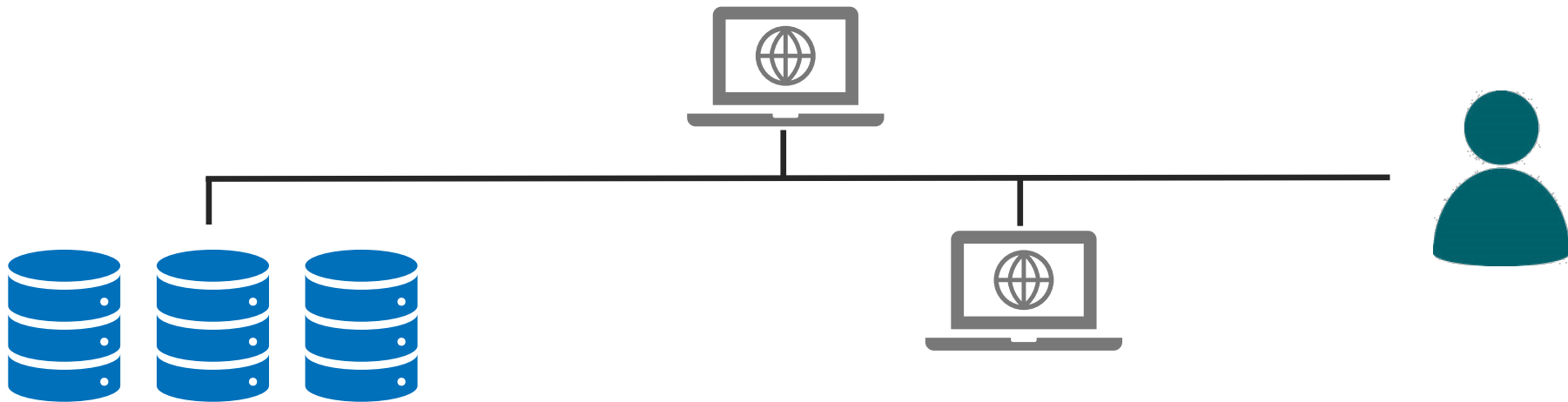
# Data Classification

- *Do this before anything else*
- Not all information is created equal:
  - Public Data:** information this is available and freely accessible.
  - Private Data:** prudent to restrict public access to protect the integrity of the data and access to other information.
  - Internal Data:** information available to employees or contractors of an organization but should not be shared externally.
  - Confidential Data:** sensitive information that a limited group of individuals or parties should have access.
  - Restricted/Classified Data** : highly sensitive information exempt from public disclosure requirements under law or regulations.



# Where is My Data?

- Where is data at rest?
- How does that data move throughout the organization?
- What applications/system does this data touch?
- Who can access that data?





# Access

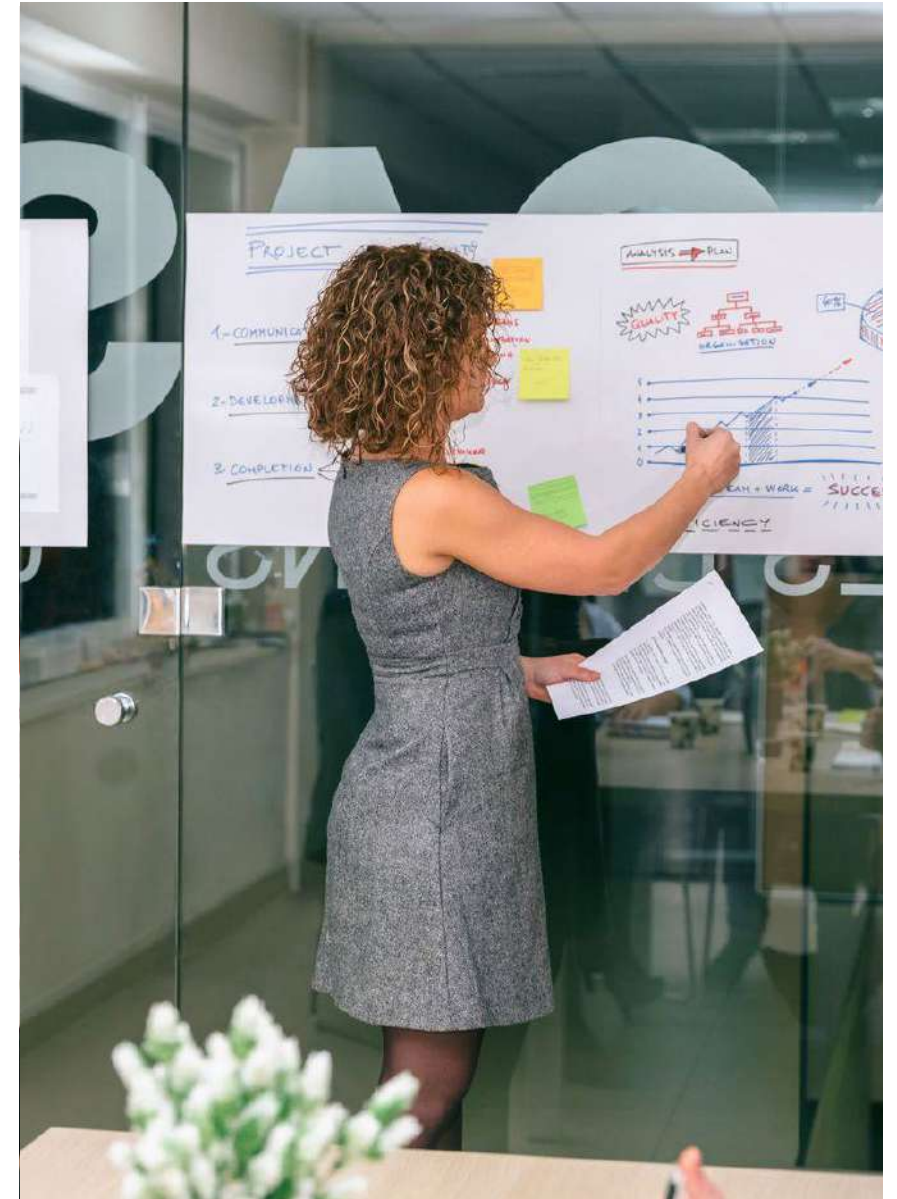
- Multi -Factor Authentication (MFA)
- Review Privileged Accounts
- Zero-Trust
  - Continuous verification
  - Endpoint security
  - Geo-Location
  - All access requests are vetted prior to granting access



## Polling Question 2

What is the first thing to do in order to secure your environment?

- A. Data Classification
- B. MFA
- C. Zero Trust
- D. The Users





Cybersecurity

## 2. Develop and Test Incident Response

# What is an Incident?

## US Department of Homeland Security

- An incident is the act of violating an explicit or implied security policy according to NIST Special Publication 800 -61 (rev. 2)

## Cybersecurity Incident and Vulnerability Response Playbooks

- An occurrence that — (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

*Of course, this definition relies on the existence of a security policy that, while generally understood, varies among organizations.*

### Sources:

United States Computer Emergency Readiness Team (US -CERT), <https://www.us-cert.gov/government-users/compliance-and-reporting/incident-definition>  
Cybersecurity Incident & Vulnerability Response Playbooks, Publication November 2021,  
[https://www.cisa.gov/sites/default/files/publications/Federal\\_Government\\_Cybersecurity\\_Incident\\_and\\_Vulnerability\\_Response\\_Playbooks\\_508C.pdf](https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf)



# These include but are not limited to:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- The unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Analytics or hunt teams that identify potentially malicious or otherwise unauthorized activity



# Building the Plan



- What are the things that could interrupt your core business?
- Consider the worse things that could happen
- Loss or Theft of Data
- What are the impacts if your operations are shut down for a day or more?
- Identify:
  - What are the most critical assets?
  - Levels of severity for bad things to happen
  - Actions to be taken if these bad things happen
  - Members of the organization that play a role
- A cyber incident response team (CIRT) would include members who play a role

# Assign Plan Ownership

- A single person, with designated alternates, is in charge of the plan.
- This may be an executive or a team manager, authorizing one or more deputies in their absence.
- It is important that the person that owns this plan has the authority to execute the plan
- Would designate an Incident Commander when something happens



Source: NIST 800-61 r2

# Communicate the Plan

- A plan is only as effective when it is known.
- CIRT should know who they are and the roles they will play.
- Assign team members task they are required during an actual incident.





# Testing the Plan

- An IR tabletop is one of the most effective ways to test an IR plan
- Involves the key stakeholders
- Walks through a scenario
  - What actions does each stakeholder take
  - These actions impact what happens next
- Refines the procedures and steps to be taken for an actual incident
- Results in changes to the plan



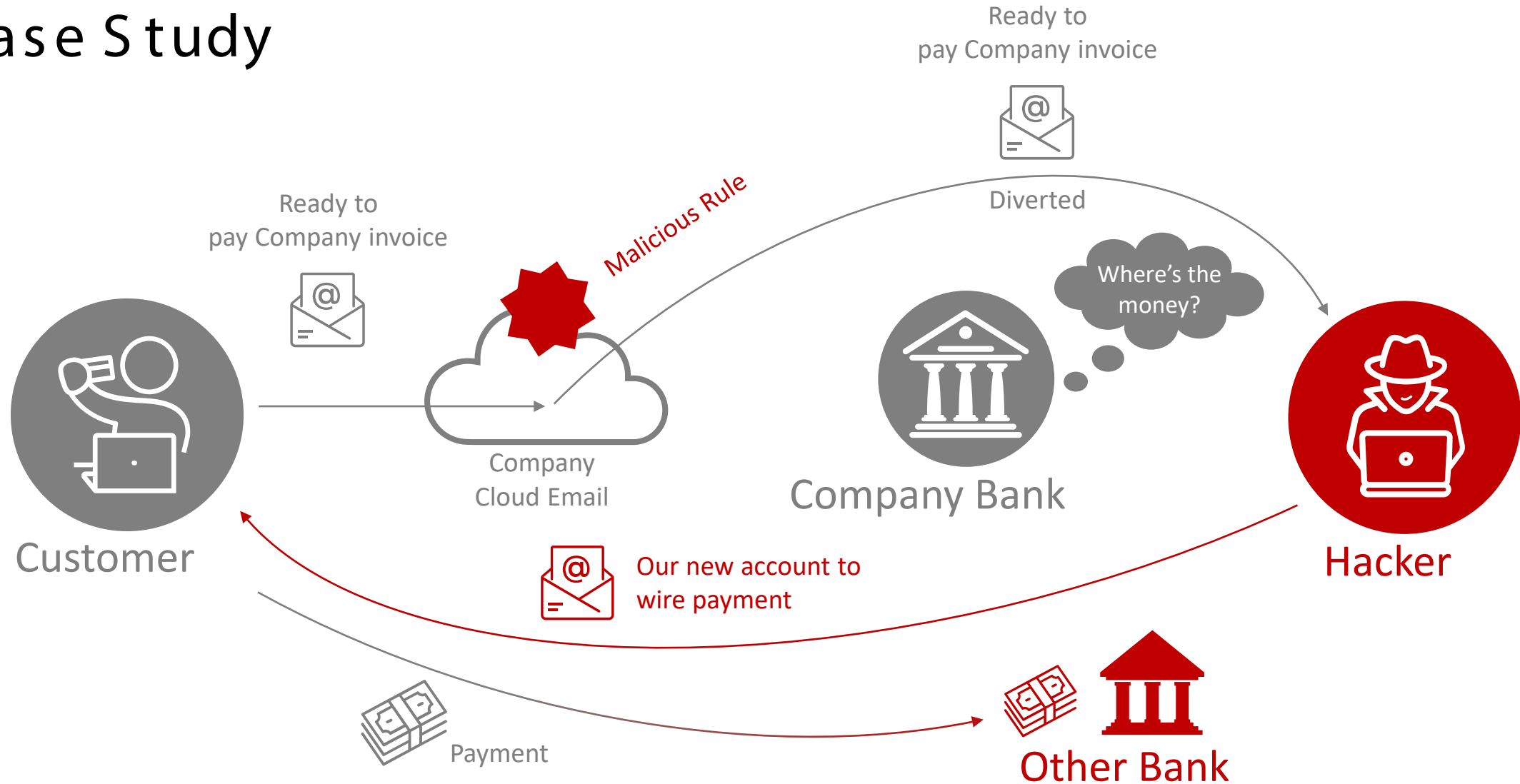
## Polling Question 3

Which of the following is true about an incident response plan?

- A. It should be current and tested
- B. It is the same as a disaster recovery plan
- C. It will rarely change once written
- D. It should only be shared by a few individuals



# Case Study

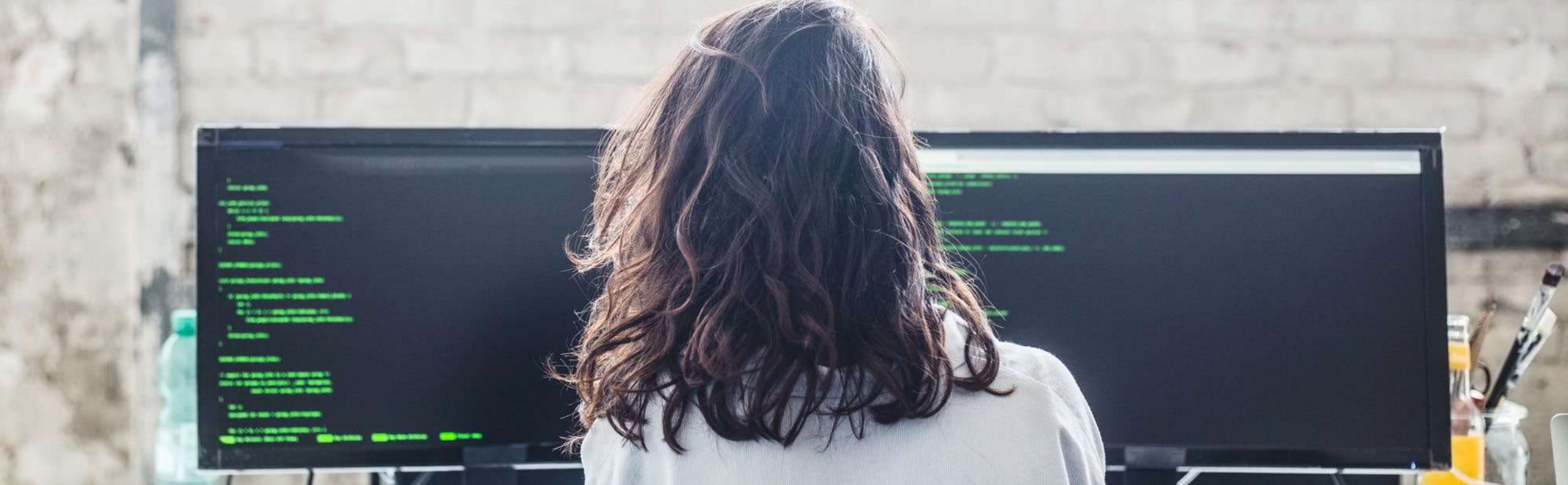


# Case Study: How It Happened

- Company provides commercial building services
- Hacker used social media to learn about the company
- Set up email rules in Office 365 to divert emails with “Invoice” or “Payment Information” in subject line to a Gmail account:
  - Mails were redirected, never arrived to Accounts Receivable
  - Provided hacker with client information & payer's email accounts
- With a different email that resembled the contractor's, hacker sent the client the account information & wiring instructions
- Clients paid the invoices to the fraudulent account
- Company did not find out until they called their clients

new





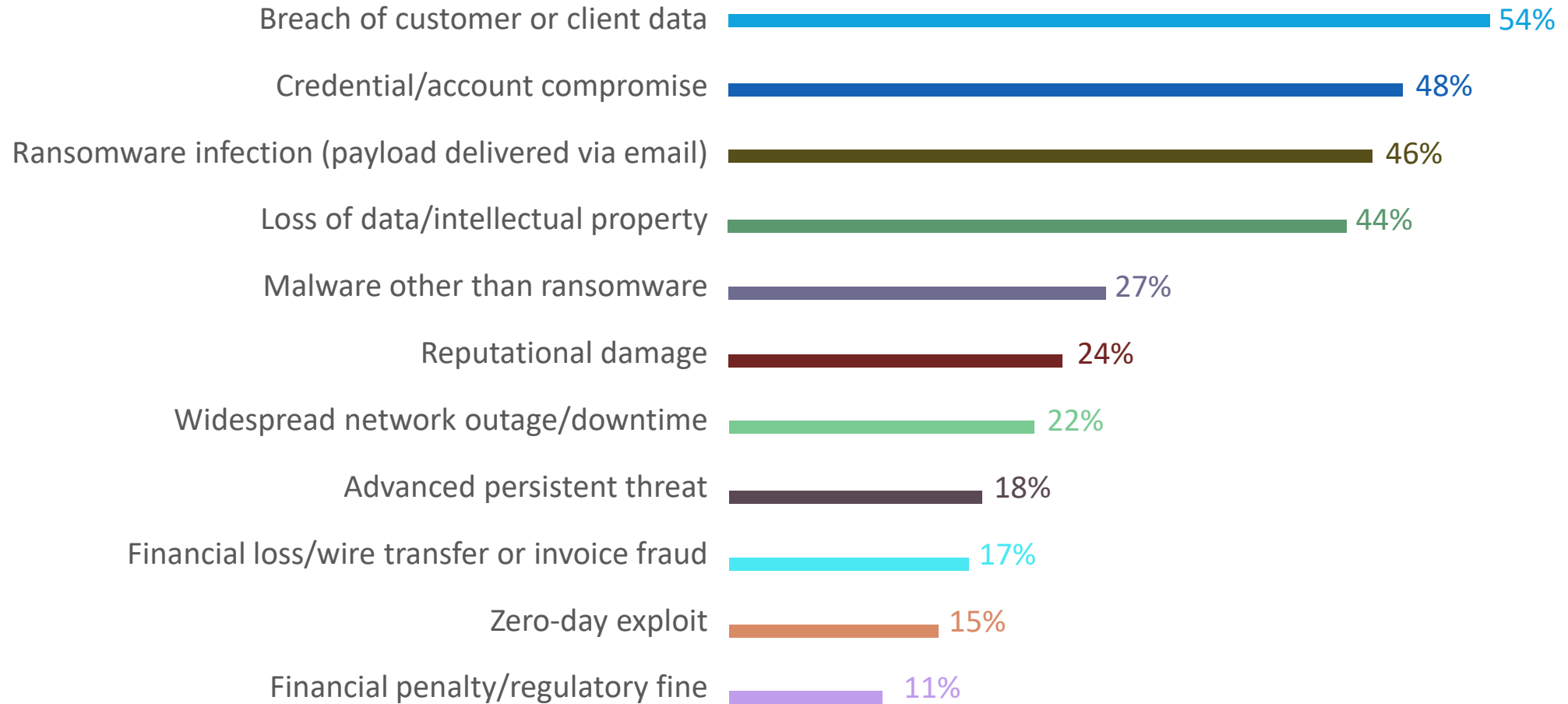
### 3. Build a Culture of Security Awareness



# Security Awareness

- Because people are still the weakest link
- Develop a program that reminds everyone of their responsibility to protect information
- Annual training
- Phishing exercises
- Should include everyone, including managers and executives
- May be required for insurance

# Results of Successful Phishing



Source: ProofPoint 2022 State of the Phish

# Passwords vs Passphrases

- According to the Verizon Data Breach Investigations report in 2020
  - 81% of all data breaches are caused by so -called 'weak' passwords
  - Out of 1,800 surveyed businesses:
    - 40% didn't offer password training for their staff
    - 61% did not require password complexity
    - 25% used multi -factor authentication (MFA)
- Passphrases offer a better solution
  - Easy to remember
  - Hard to crack
  - You can even randomize symbols or letters, or not...



# Passphrases

*“My favorite color is Hawaii”*

Password

My favorite color is Hawaii

☐

Hide password

Complexity

Very Strong

Score

Legend

**Exceptional** Exceeds minimum standards. Additional bonuses are applied.

**Sufficient** Meets minimum standards. Additional bonuses are applied.

**Warning** Advisory against employing bad practices. Overall score is reduced.

**Failure** Does not meet the minimum standards. Overall score is reduced.

Additional points are given for increased character variety. Final score is a cumulative result of all bonuses minus deductions. Final score is capped with a minimum of 0 and a maximum of 100. Score and Complexity ratings are not conditional on meeting minimum requirements.

Additions	Type	Rate	Count	Bonus
Number of characters	Flat	$+(n^4)$	27	+ 108
Uppercase letters	Cond/Incr	$+(len-n)^2$	2	+ 50
Lowercase Letters	Cond/Incr	$+(len-n)^2$	21	+ 12
Numbers	Cond	$+(n^4)$	0	0
Symbols	Flat	$+(n^6)$	0	0
Middle numbers or symbols	Flat	$+(n^2)$	0	0
Requirements	Flat	$+(n^2)$	3	0



## Polling Question 4

What is the main reason for Security Awareness?

- A. Not required so long as I have good tools and detection
- B. It is a requirement for insurance
- C. Users are the weakest link
- D. It makes technology more robust

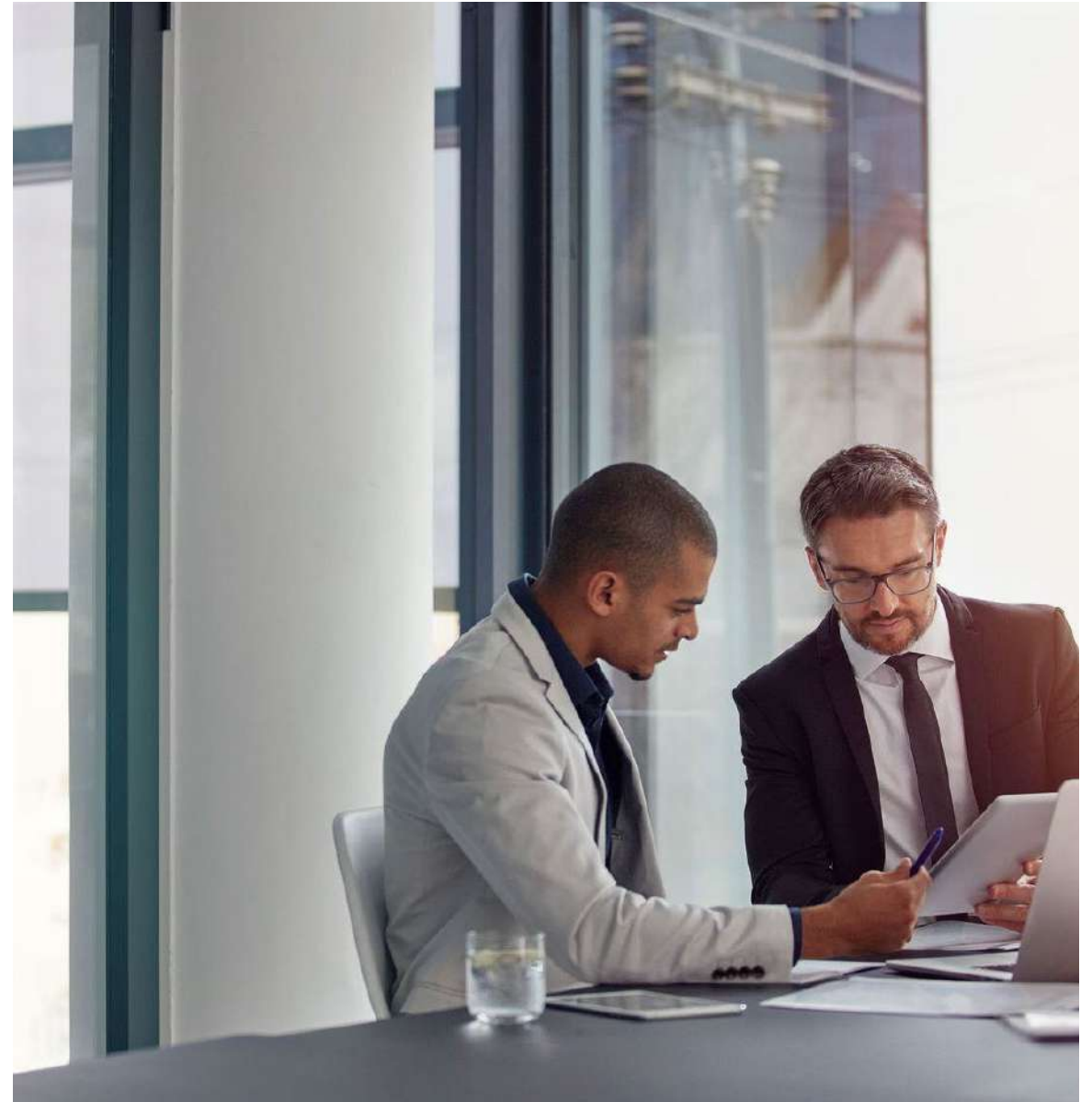




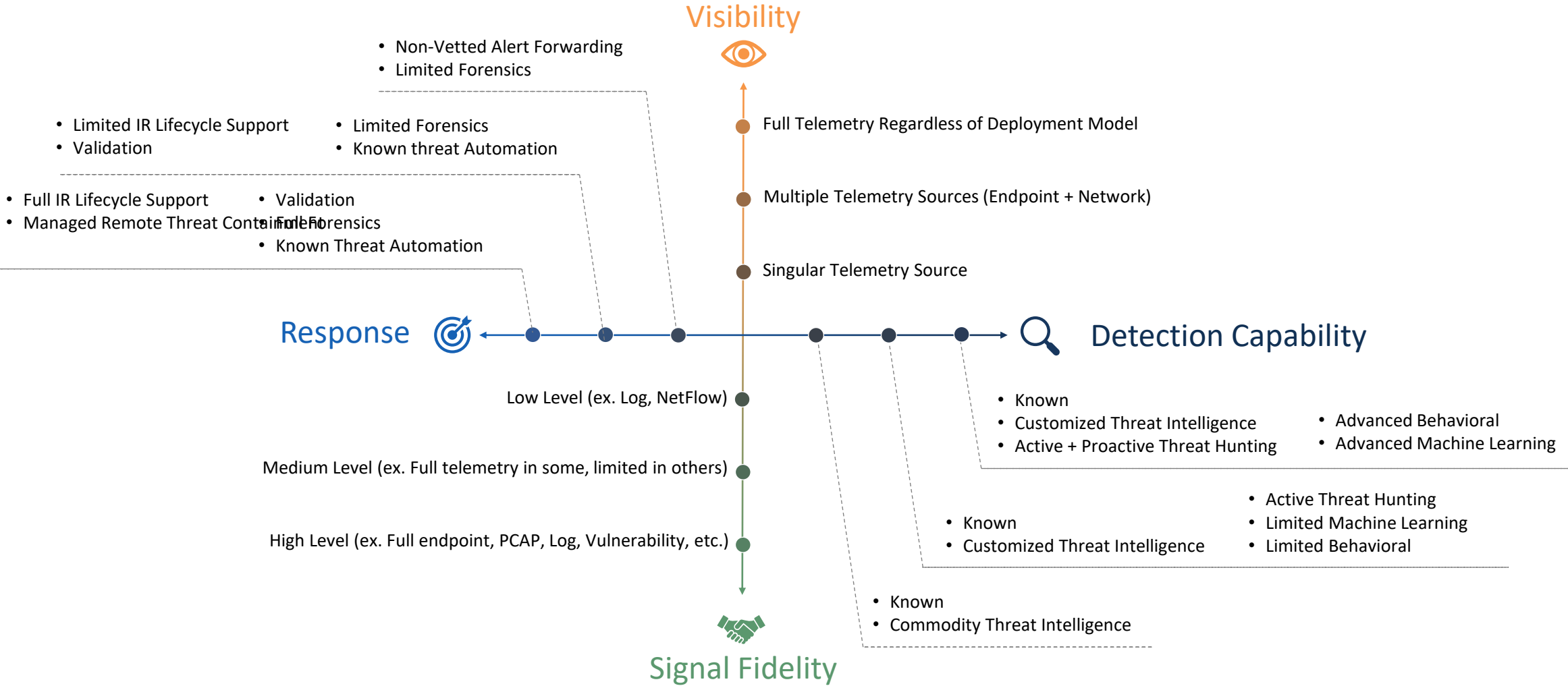
## 4. Choose A Trusted Partner

# The right partner

- Cybersecurity Trusted Advisor
  - Assists with determining cyber strategy and initiatives
  - Part time, only when needed
  - Has connections to solution providers
  - Unbiased
- Managed Detection and Response (MDR) or Extended Detection & Response (XDR)

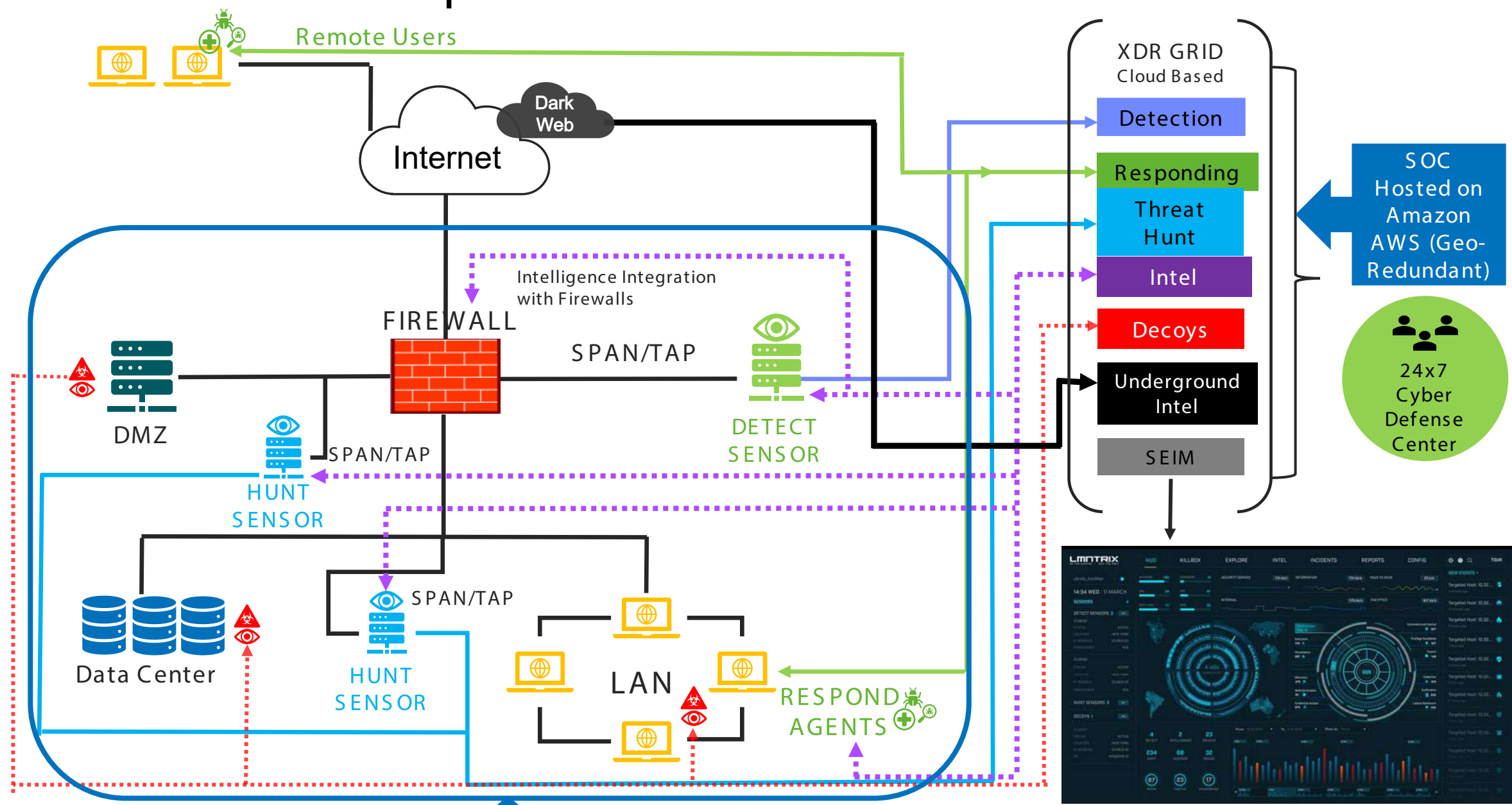


# What to look for MDR /XDR





# How this Would Operate



All data remains on client network sensors and endpoint agents.

Online XDR PORTAL

## Polling Question 5

What Are Key Elements of XDR / MDR Solutions?

- A. Active Monitoring
- B. Threat Containment & Remediation
- C. Incident Forensics
- D. Full IR Lifecycle (or All of the Above)

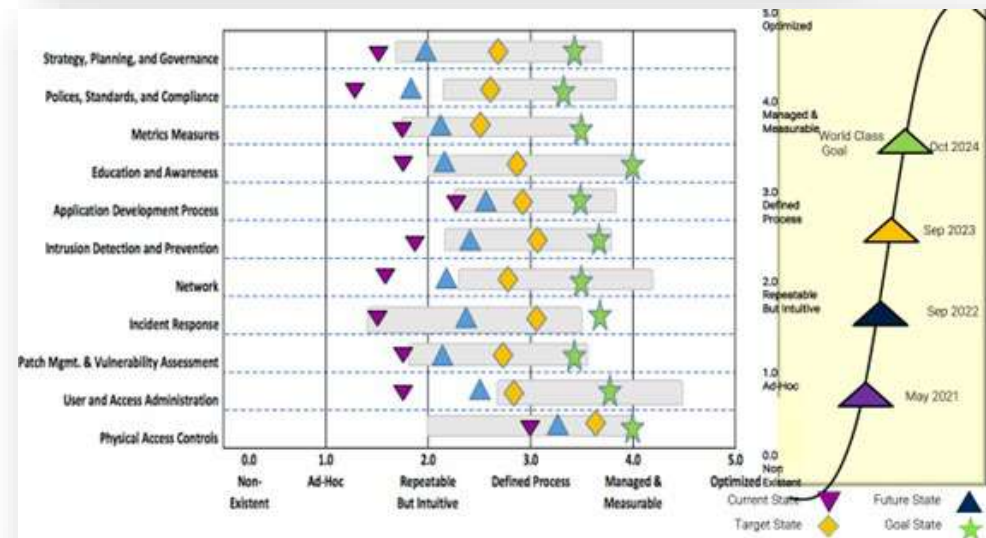




## 5. Conduct Periodic Checks

# Conduct Periodic Checks

- What is required?
  - Regulatory or Legal
  - Insurance
- Measure progress
- Remember the cybersecurity trusted partner





# How to Secure A Network



Take an inventory of  
all assets



Unplug  
everything



Move to a farm and  
forget that the  
internet exists



A woman with long dark hair, wearing a grey cardigan over a white top, is seated at a desk. She is looking at two computer monitors displaying a video conference with multiple participants. Her hands are raised in a gesture, palm up, as if she is speaking or explaining something. The desk is dark, and a keyboard is visible in front of her. The background is a blurred office environment.

Summary

# Challenges with Cybersecurity; and How to Be Proactive

## Challenges

- Cyberthreats continue, Insurance is changing, Options costly
- No or outdated incident response plan
- Users lack the skills to prevent attacks and are often the cause
- Monitoring can be a full-time job and false positives
- Can be overwhelming

## Resolutions

- Trusted partner to help advise and work with solutions and carriers
- Rehearse plans, tabletop exercises
- Basic awareness can reduce success rate and mitigate impact of successful ones
- Look for a partner for MDR / XDR that provides the necessary services
- Find a trusted cybersecurity partner



# Questions?



**Rex Johnson**

Executive Director

CAI Cybersecurity

[rex.johnson@cai.io](mailto:rex.johnson@cai.io)

+1 (913) 579-6716






Thank You!

 [www.cai.io](http://www.cai.io)

 [@CAI](https://www.linkedin.com/company/cai)

 [inquire@cai.io](mailto:inquire@cai.io)

 [@CAI\\_Insights](https://twitter.com/CAI_Insights)

 +1 (888) 824 – 8111

