# Cybersecurity in the Public Sector: 5 Key Steps For Protecting Your Organization

Rehmann

EMPOWER YOUR PURPOSE®

# Presenter

**Paul Kennedy**

Senior Manager | CISSP | CISA | vCISO
616.301.6318 | paul.kennedy@rehmann.com

- Virtual Chief Information Security Officer (vCISO)
- Advises clients in a variety of industries to implement, monitor and improve their security controls
- Helps lead Rehmann's Information Security Assessment team
- Leads cyber security consulting engagements such as:
    - Security strategy development
    - Vulnerability and penetration testing
    - Social engineering testing
    - Information security training
- Certified Information Systems Security Professional (CISSP)

# Today’s Agenda

Cybersecurity Primer

Moving Security Forward

1. Strategy
2. Identify
3. Protect
4. Build
5. Policies

# Cybersecurity Primer

# Have you seen the headlines?

***"Curry County computer system 'starting from scratch' after ransomware attack"***
- opb.org

***"King County Sheriff's Office struggling after 'security incident'"***
– 770KTTH

***"For weeks, the healthcare providers' … systems were down. It meant everything had to be done by hand, from scheduling appointments to handling medical records."***
– WeAreGreenBay.Com

***"Hillsborough County Public Schools alert parents to cyberattack, data breach."***
– WTSP 10 Tampa Bay

# Suffolk County, NY

**The County with 1.5 million constituents shut down on Sept. 8th due to a ransomware attack.**

County 911 services operated in an emergency model delegating dispatching to other counties for 2 weeks.

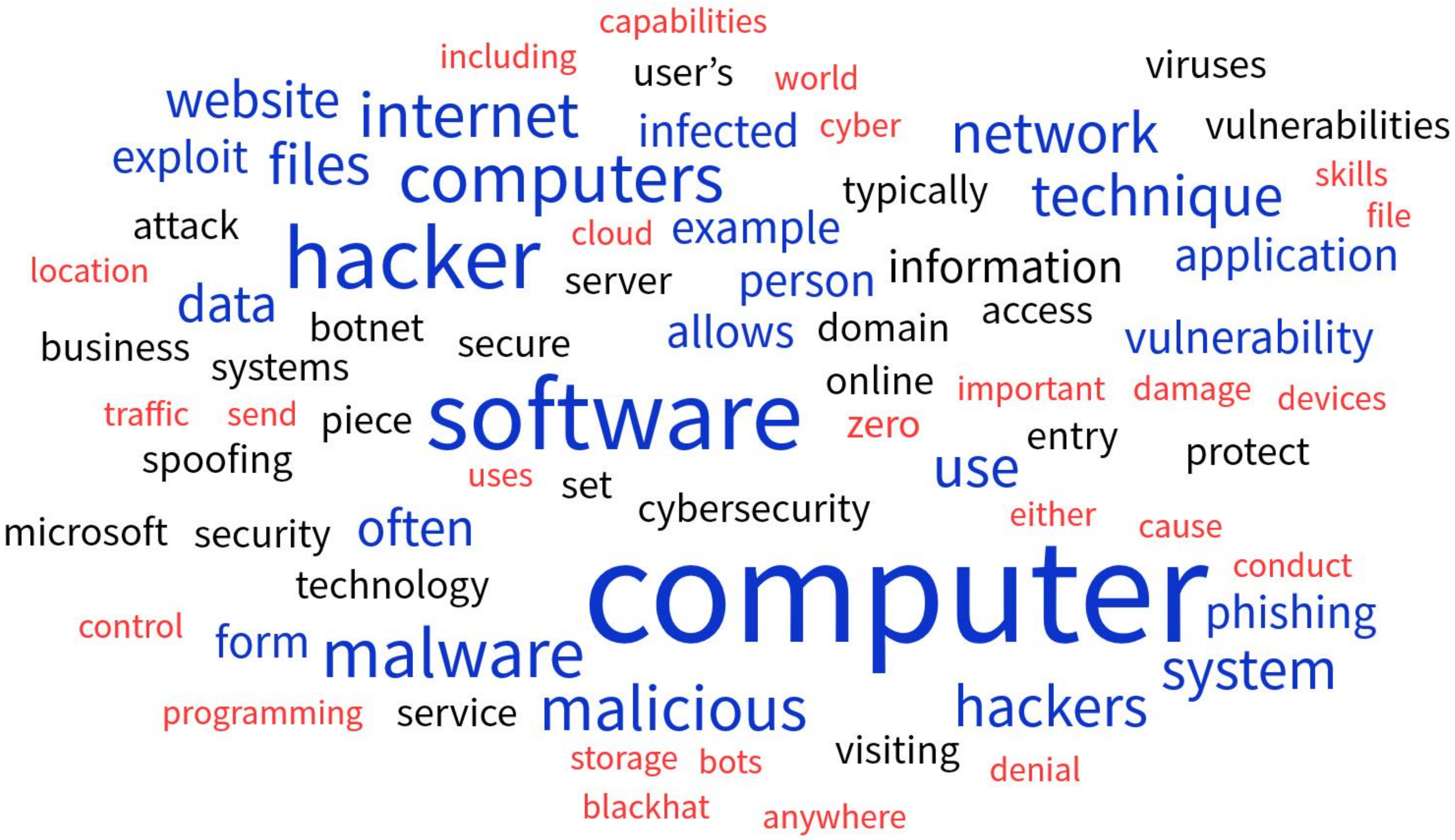
The attack impacted the ability of Sheriff Deputies to write tickets and enter traffic stops into county systems.

Title search services were unavailable for 4 weeks.

As of mid-October, the county had missed over $140 Million in vendor payments and still was manually signing all payment checks.

**Cybersecurity is formally defined in a dictionary as:**

*"Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."*


capabilities
including
user’s
world
viruses
website
internet
infected
cyber
network
vulnerabilities
exploit
files
computers
typically
technique
skills
file
attack
hacker
cloud
example
location
server
person
information
application
data
botnet
access
business
secure
allows
domain
vulnerability
systems
online
important
damage
devices
traffic
send
piece
software
zero
entry
spoofing
protect
uses
set
use
cybersecurity
either
microsoft
security
often
cause
conduct
technology
computer
control
form
malware
phishing
system
programming
service
malicious
hackers
visiting
storage
bots
denial
blackhat
anywhere

# Redefine Cybersecurity based on what to protect:

## Confidentiality

**Protecting information from unauthorized access and disclosure.**

For example, what would happen to your organization if donor information such as usernames, passwords, or credit card information was stolen?

## Integrity

**Protecting information from unauthorized modification.**

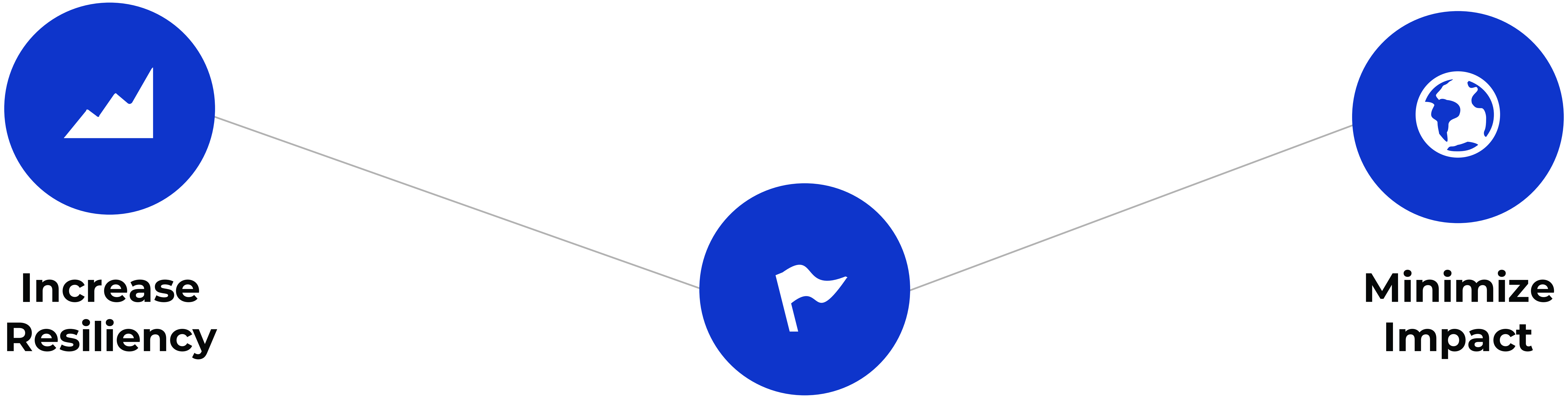
For example, what if your payroll information or a proposed product design was changed?

## Availability

**Protecting disruption in how you access your information.**

For example, what if you couldn’t log in to your bank account or access your donor’s information, or your supporters couldn’t access you?

# Cybersecurity Goals



**Increase Resiliency**

**Reduce Attack Frequency**

**Minimize Impact**

# Common Types of Attacks

## Ransomware

Ransomware is a form of malicious software designed to encrypt a victim's files or lock their computer system, rendering it inaccessible until a ransom is paid. It typically spreads through malicious email attachments, compromised websites, or other methods. Once infected, the victim is presented with a ransom demand, usually in the form of cryptocurrency, in exchange for the decryption key to restore access to their files or system.

## Social Engineering

Social engineering is a method used by malicious individuals to manipulate and deceive people into divulging sensitive information or performing actions that can lead to security breaches. It exploits human psychology, trust, and vulnerabilities rather than relying solely on technical exploits.

# Common Types of Attacks

## Distributed Denial of Service (DDoS)

In a DDoS attack, attackers flood a target system or network with a massive volume of traffic, overwhelming its resources and rendering it inaccessible to legitimate users. The goal of a DDoS attack is to disrupt the targeted system's normal functioning, causing service interruptions, downtime, or loss of business continuity for your organization.

## Business Email Compromise

Malicious actors gain unauthorized access to a legitimate email account within your organization and use it to deceive or defraud individuals or other organizations. This often involves impersonating a trusted entity, such as an executive or vendor, to trick victims into performing fraudulent actions, such as transferring funds or sharing sensitive information.

# CPE Prompt 1 of 5

You might be wondering,
“What do dams have to do with
cybersecurity?"

Cybersecurity serves the same purpose as a dam – To protect and control important systems and data by building a robust defense layer.

# Ponemon Institute: 2023 Cost of a Breach

## Global Averages

Average total cost of a data breach

**$4.45M**

Average total cost of a ransomware attack

**$4.54M**

Highest country average cost ($9.48 million)

**United States**

Time to identify and contain a breach

**277 days**

Highest industry average cost ($10.93 million)

**Healthcare**

## Long-term Impact

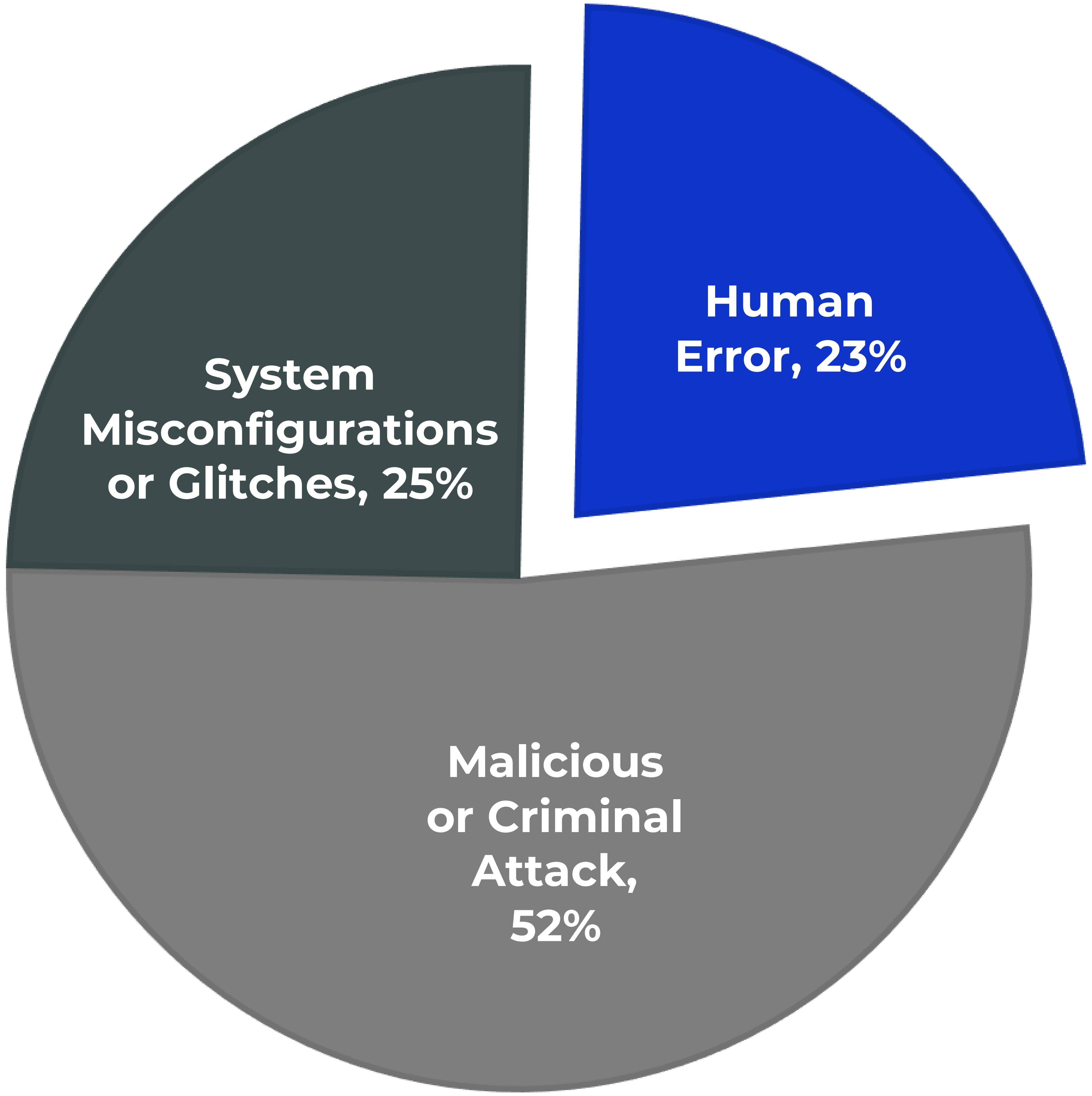
On average, only 53 percent of breach costs came in the first year, 31 percent accrued in the second year after a breach, and 16 percent of costs occurred more than two years after a breach.

# Data Breach Root Causes

**SMB Cost Disadvantage**

It was observed that significant variation in total data breach costs by organizational size exist as smaller organizations have higher costs relative to their size than larger organizations, which can hamper their ability to recover financially from the incident.

*Ponemon, Cost of a Data Breach 2022*



# CPE Prompt 2 of 5

# 5 Steps for Protecting Your Organization

1 STRATEGY

2 IDENTIFY

3 PROTECT

4 BUILD

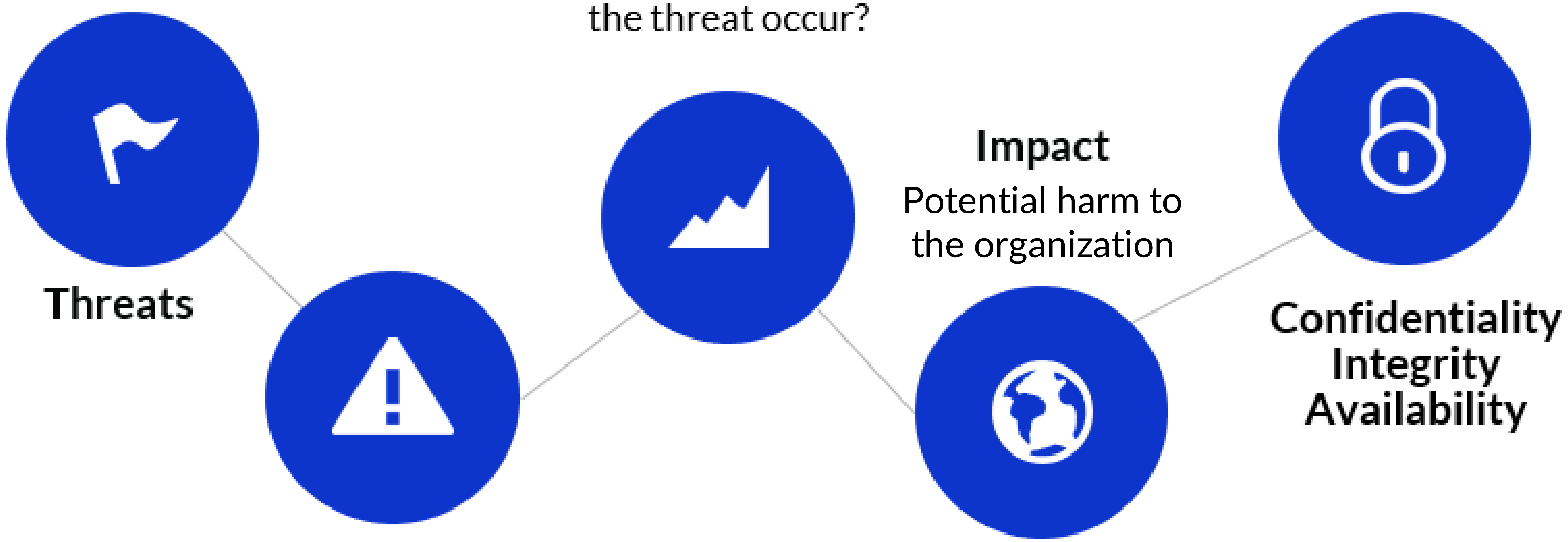
5 POLICY

Build the right team with the right information to guide cybersecurity within the organization.

Educate the team on their roles and the basics of cybersecurity.

# Cybersecurity is Risk Management

The world of cybersecurity is filled with technical terms and lots of acronyms. However, information security is fundamentally a risk that comes with using technology.



**Threats**

**Vulnerabilities**

Weaknesses in security protections

**Likelihood**

How often will the threat occur?

**Impact**

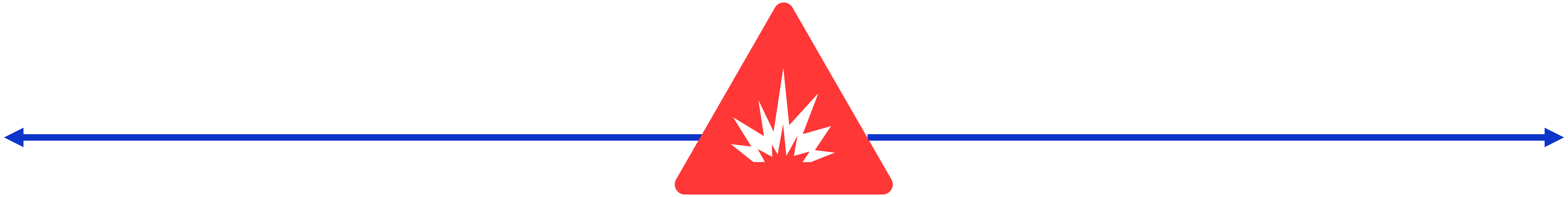
Potential harm to the organization

**Confidentiality**
**Integrity**
**Availability**

# Risk Management is proactive decision making

The goal of Risk Management is to identify the right information to be able to make proactive decisions about whether to invest time and budgets before or after a potential event.

***Cybersecurity Incident***



**Spend time and budget here** *OR* **Spend time and budget here**

# Typical Ransomware Timeline

**T + 2 days…**

Third party IR team engaged and investigating

**T + 9 days…**

“You will finally feel like you have your feet underneath and a plan to get out of the mess.”

**T + 21 days…**

*Average* ransomware incident has been resolved.

**T + 35 days…**

Are we back to normal yet?

# Management Cybersecurity Motivations?

| *Deprioritize Cybersecurity* | | *Prioritize Cybersecurity* |
|---|---|---|
| ⬇ | **Resiliency** | ⇧ |
| ⬇ | **Incident Impact** | ⇩ |
| ⬇ | **Incident Frequency** | ⇩ |
| ⇩ | **Cybersecurity Budget Spend** | ⬆ |
| ⇩ | **Leadership Focus Outside of Core Services** | ⬆ |
| ⇧ | **Operational Efficiency** | ⬇ |

*Long term  hard to measure payback…*

*Short term visible return on investment…*

## Who is on the Info. Sec. Team?

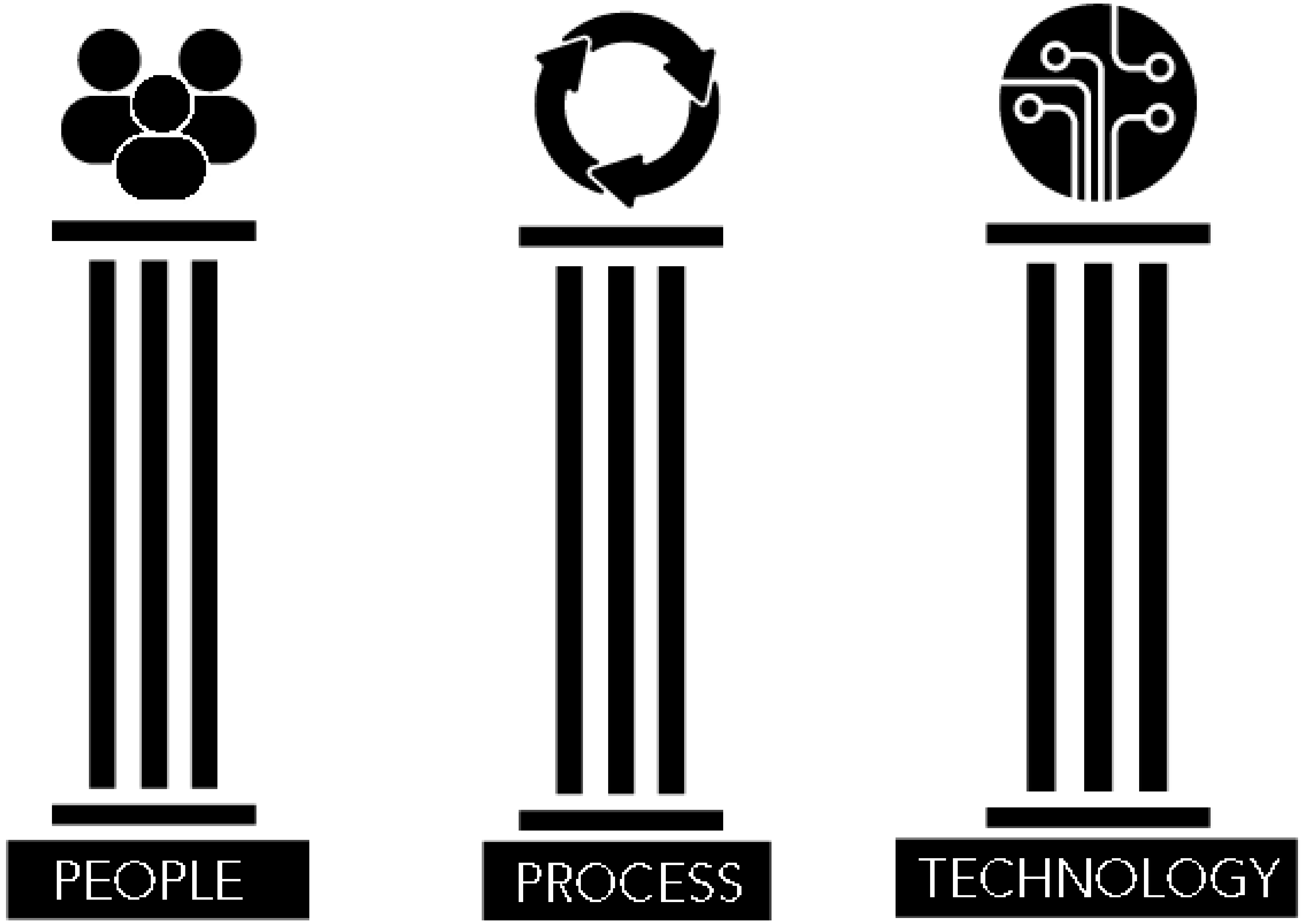
Your organization needs to have the right roles represented within your information security function.

Many of the solutions are technical, but the risks are operational.

Information Security needs to be guided by the operational departments.

# Cybersecurity Must Be Collaborative

To be effective, cybersecurity must be an effort led by leaders representing Information Security, IT, Operations, and Financial departments.



# The Right Players at the Table

## The Board of Directors (or Governance function)

- Whether Directors, Commissioners, or others are charged with governance, the Board must be engaged with understanding the status of the Cybersecurity program.

## Executive Management / Department Heads

- Management across all departments must be responsible for securing the mission and reputation of the organization. Cybersecurity responsibilities must sit with both the IT and operational departments

## Information Security Officer (ISO)

- Ensure day to day execution of policies, procedures, and practices are carried out by business and IT departments.
- Oversees key physical and personnel security functions.

## IT Officer and Department

- Executive authority over the IT department responsible for ensuring IT systems and functions are aligned with operational strategy and needs.
- Oversees the installation and maintenance of information systems, ensuring that they run smoothly.

# 5 Steps for Protecting Your Organization

1 STRATEGY

2 IDENTIFY

3 PROTECT

4 BUILD

5 POLICY

Determine the assets (people, systems, data, etc.) that needs to be protected.

Gather the right information about each asset to make an informed risk assessment to guide your information security process.

# Assess Your Risk

## Conduct a Business Impact Analysis (BIA) for your organization

- Management should have a process to identify what functions the organization needs to deliver services to constituents.
  - What processes must happen daily, weekly, monthly, etc.?
    - How critical is each of those processes?
    - How long can the organization go without the process functioning?
  - What are the IT systems and data assets that each function relies on?
    - ERP System
    - Payroll Processing
    - Banking Systems
    - Communication Systems
  - What non-public data is collected?

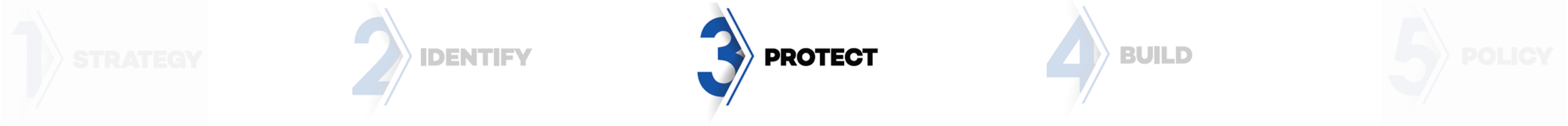
# Assess Your Risk

## Information System Risk Assessment

- Appropriate leaders should review the inventory of systems and data assets identified in the BIA to identify criticality and prioritization for securing each.
  - Identify the team responsible:
    - Who is responsible for making decisions about the information system?
    - Who is responsible for maintaining and securing it?
  - Gather high level security requirements:
    - What security is in place for the system?
    - What should be?
  - Identify key backup metrics:
    - How long can the organization go without it?
    - If the system fails, how much of recent transaction history can the organization afford to lose and/or recreate?
  - Perform a risk assessment:
    - What threats and vulnerabilities (risks) are each asset vulnerable too?
    - What is the likelihood that these risks will be realized?
    - What is the impact on Confidentiality, Integrity, and Availability of the assets if the risks are realized?

# CPE Prompt 3 of 5

# 5 Steps for Protecting Your Organization



**Pick the right information security controls to protect your organization.**

**Every organization’s risks and systems are different, make sure your strategy is your own.**

# Protecting Your Environment

## Design a Control Strategy Specific to Your Risk

- The organization should review the results of the risk assessment and determine what information security controls are already in place.
- Based on this review, leadership needs to determine if additional information security controls should be put in place to leave the level of risk in place (residual risk) that the Board is comfortable with.
- Leadership should be working with the Board to make sure that level of risk is acceptable.

## Third Party Control Frameworks

- While every organization's risk and therefore the appropriate level of control is different, there are best practices available in third party frameworks.
- Leadership should use third party frameworks to help make sure controls that should have been considered are not missed.

# Use a Cybersecurity Framework

All people, including our team members have blind spots in our experiences. Security frameworks help address that by providing a solid foundation to build your security program and customize it specific to your environment.

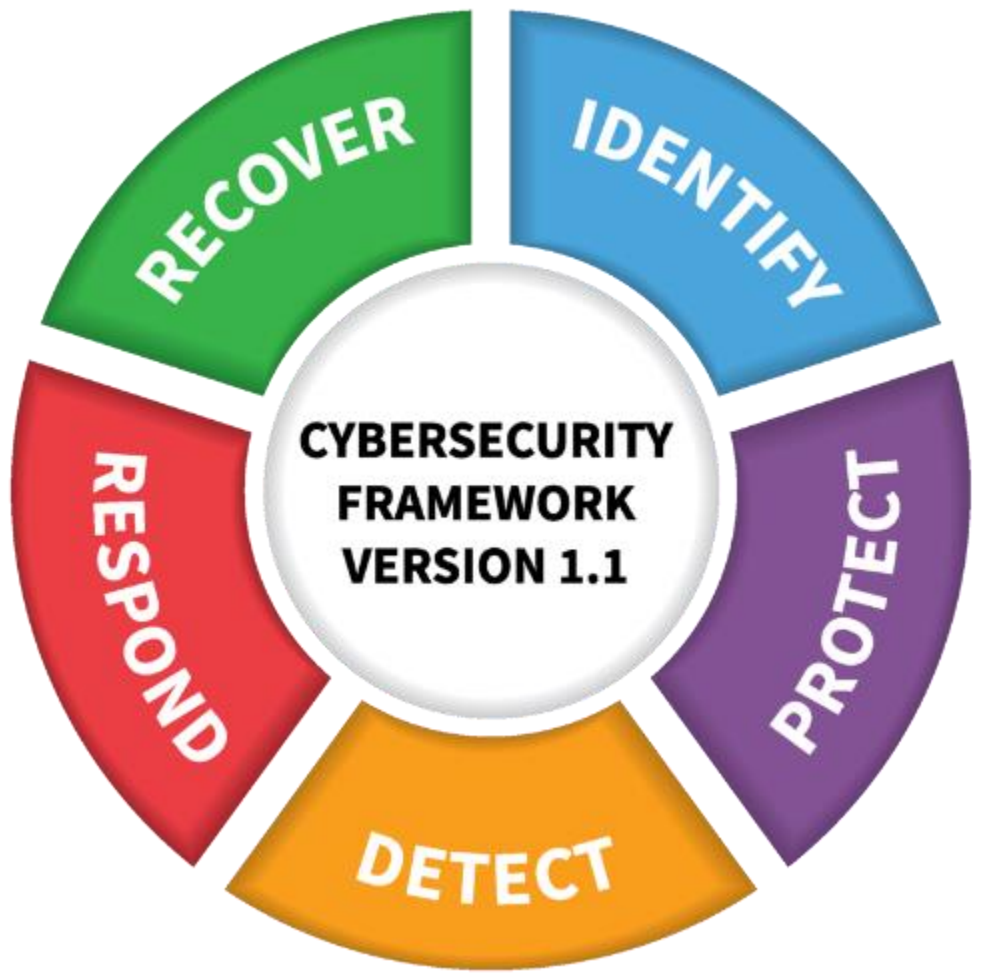
The leading cybersecurity frameworks such as the NIST Cybersecurity Framework (CSF) have been built by thousands of collaborators who have collectively worked to identify what is a “complete” program.

# Commonly Referenced Cybersecurity Frameworks

Applying a cybersecurity framework can assist you in demonstrating that your organization has applied Due Care and Due Diligence.

NIST

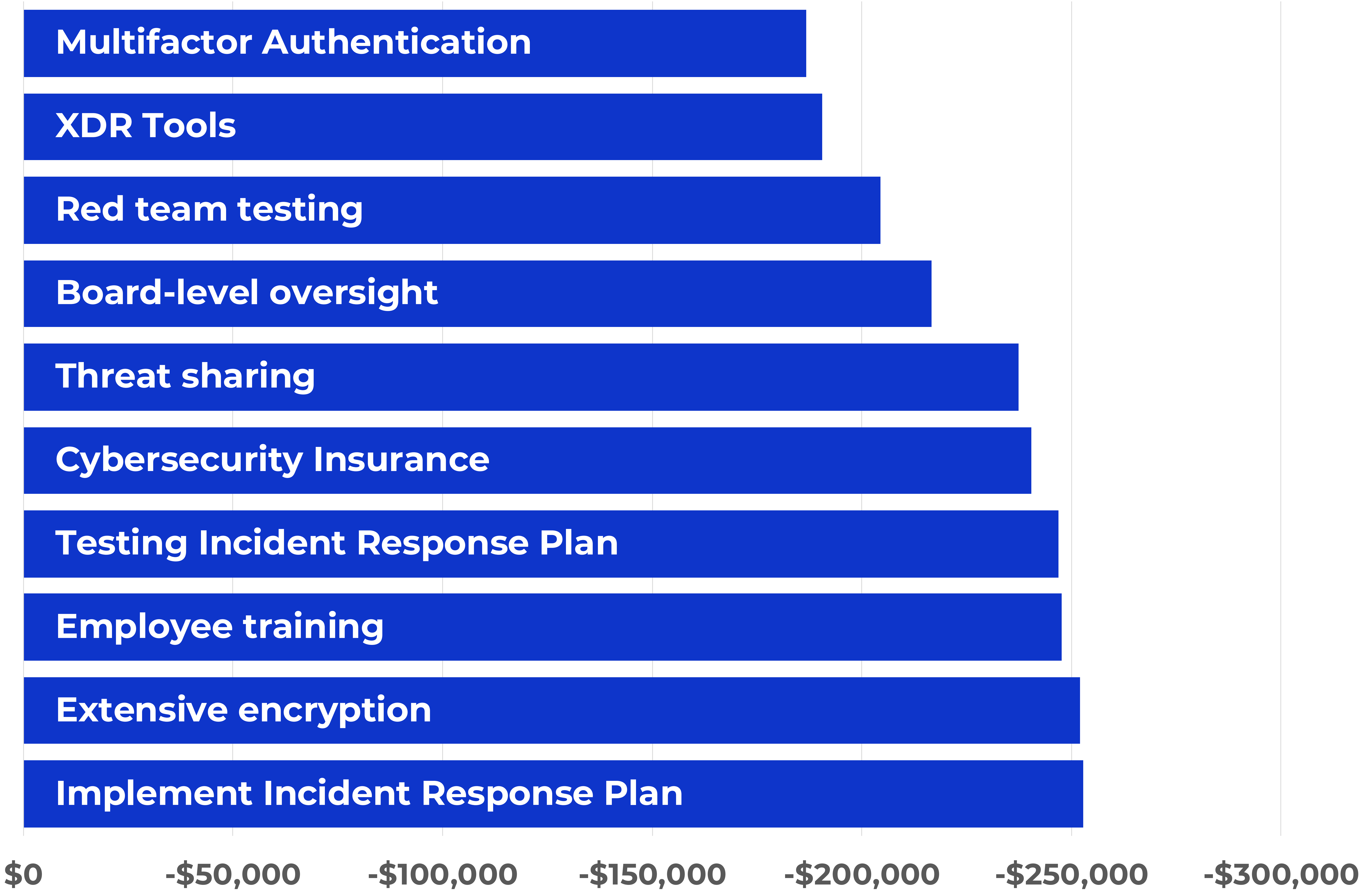
National Institute of Standards and Technology



CIS® Center for Internet Security®

Critical Security Controls

# What can you do to reduce the cost of an incident?

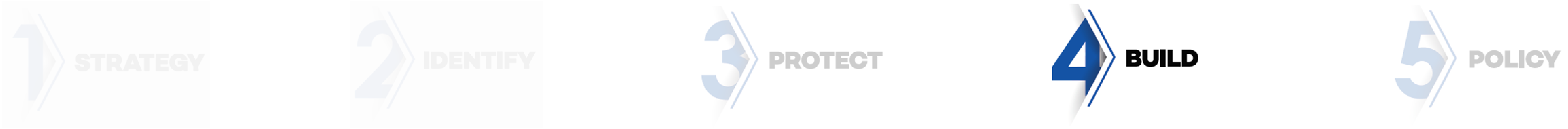


Average total cost of a data breach

**$4.35M**

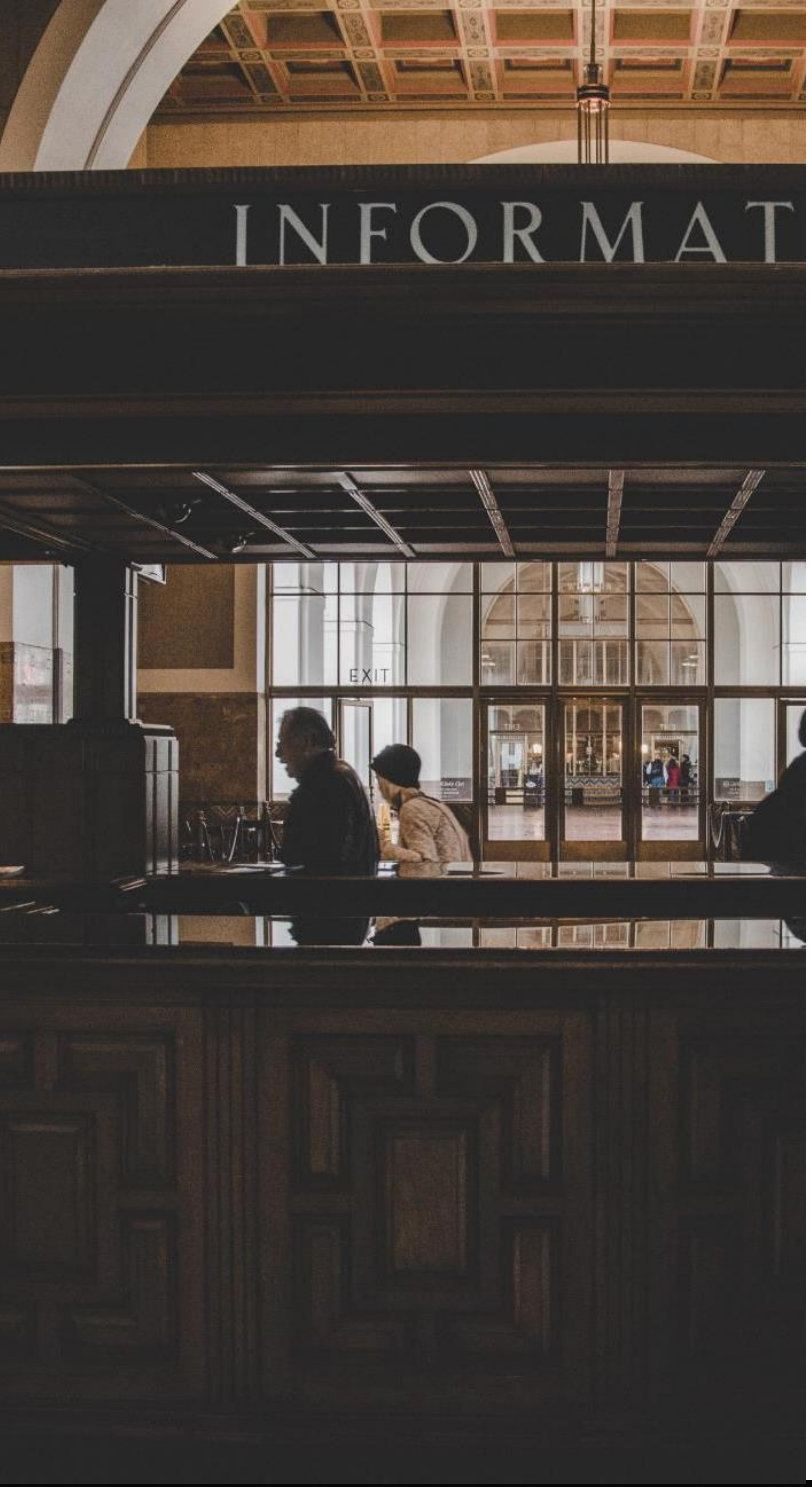
*Cost of a Data Breach Report 2022*

# 5 Steps for Protecting Your Organization



Implement information security controls according to your strategy.

Make sure the controls are consistently and completely executed.



# Cybersecurity Training

Your employees are likely your greatest risk when it comes to cybersecurity. However, they can also be one of your greatest assets when trained appropriately.

A German study of 30,000 people found that the application of cybersecurity best practices was significantly reduced after 4 months.

- End Users (all employees) need to be trained at least quarterly on the basics of information security so they can watch out for things like social engineering attacks.
- Individuals with Information Security roles need specialized training related to those roles so that they can keep up with current best practices.
- The Board and leadership team need training to assist them in overseeing the information security program.

# Which is a better password?

**OPTION A: i^vs6vFa**

**OPTION B: lance goes stagnant gentle**

**Password strength calculated by security.org.*

# Securing User Accounts

## i^vs6vFa

*8 hours to crack**

## lance goes stagnant gentle

*7 septillion years**

### Use Passphrases with MFA instead of Passwords

Long phrases made up of randomly selected words are far easier for a human to remember. If long enough, they are also harder for a computer to guess.

### Use Password Vaults

For many years, cybersecurity has been saying “Never write down your password!” However, human behavior has shown that not writing down your password and using long, random, and complex passwords leads to poor security. Instead, we should shift to leveraging security tools like password vaults that secure the passwords for us so we do not need to remember them.

**Password strength calculated by security.org.*

# Executives are Attractive Targets

## Significant Return on Investment

Executives simply have more influence and access. This makes it more likely that an attacker is going to get a significant return on their time investment.

## Publicly Available Information

Executives often have significant public presences either through a company or through community engagement.

## Expansive Networks

Executives often are connected individuals whose relationships can be leveraged to compromise other executives or high value targets.

## Attackers Prey on Relationships

Attackers will try to convey a sense of urgency which is all that much easier to do when the target has other individuals working for them.

# Data Backups

## 3-2-1 Backups

The concept of 3-2-1 backups is a data backup strategy that involves creating three copies of your data, storing them in two different storage media, and keeping one copy air-gapped and offsite.

This approach ensures redundancy, protection against hardware failures, and mitigates the risk of data loss due to disasters like fire, theft, or natural calamities.

## Immutable Backups

A backup approach where the backed-up data is made unchangeable and cannot be altered, modified, or deleted during a specific retention period. This ensures that the backup data remains intact and protected from accidental or intentional modifications, ransomware attacks, or other forms of data tampering.

# Internal Protections

## Network Segmentation

Network segmentation is the practice of dividing a computer network into isolated segments to enhance security and control access to specific areas. It involves implementing separate security controls, permissions, and monitoring for each segment. The goal is to protect sensitive information and limit the impact of potential breaches or unauthorized access.

## Firewalls

A firewall is a network security device that acts as a barrier between internal and external networks. It monitors and filters network traffic based on predetermined rules, allowing authorized traffic to pass through while blocking unauthorized or potentially malicious communication.

## Intrusion Detection and Prevention Systems

Intrusion Detection and Prevention Systems (IDPS) are security solutions that monitor network traffic and system activities to detect and prevent unauthorized or malicious activities. They analyze network packets, log files, and behavior patterns to identify potential intrusions or security breaches. IDPS can provide real-time alerts, block suspicious traffic, and take proactive measures to defend against threats.

# Internal Protections

## Encryption – At Rest and In Transit

Encryption algorithms use advanced mathematical concepts to make data impossible to read. These algorithms can either be reversible (i.e. you can unlock the data if you know the secret) or one-directional so the original data cannot be read.

## SIEM (Security Information and Event Management)

A SIEM is used to collect, analyze, and correlate security event data from various sources, allowing for real-time threat detection, incident response, and compliance reporting. It provides a centralized view of security events, enables proactive monitoring, and helps organizations identify and respond to potential security threats more effectively.

## Endpoint Detection and Response (EDR)

An EDR focuses on detecting and responding to threats by monitoring activity on individual workstations and servers. It monitors endpoint activities in real-time, collecting and analyzing data to identify and investigate suspicious or malicious behavior. EDR solutions provide visibility into endpoint activities, enable rapid incident response, and help organizations detect and mitigate advanced threats that may bypass traditional security defenses.

# CPE Prompt 4 of 5

# Cyber Insurance
## *Transferring Risk*

The reality is no organization can implement enough controls to completely address the related cybersecurity risks.

Insurance carriers provide cyber insurance policies which allow your organization to transfer the related risks.

Insurance carriers are implementing strict requirements to qualify for cybersecurity policies.

# Cybersecurity Insurance

## Obtaining a Policy

Given your attendance here, your organization likely has coverage through the Michigan Municipal Risk Management Authority. However, it is still important to understand how the process works.

Cybersecurity insurance carriers have incurred significant losses over the last ~5 years on cyber insurance policies. As a result, many carriers have started implementing strict requirements to qualify for coverage, reducing coverage amounts, and increasing carve out exclusions.

## Cyber Attestation Form

Many insurance carriers have started requiring 5-10 page detailed cyber attestation forms when applying for coverage. These forms contain many questions that must be answered accurately though many can be interpreted in multiple ways leading to confusion. Incorrectly answering the form could lead to a claim being denied and the policy rescinded.

# Cybersecurity Insurance

## Ongoing Maintenance Requirements

Cyber insurance policies often include requirements that must be proactively implemented such as identifying and remediating critical vulnerabilities within a certain number of days. It is critical to know requirements must be met to keep your organization’s policy in effect.

## Notifying Your Carrier

One such requirement is usually to notify your carrier in the event of a potential cybersecurity incident even if it would not result in the filing of a claim. Your organization should build into your incident response plan what level of incidents require notification to your insurance carrier.

# Responding to Incidents

## Incident Response Providers

During a significant cybersecurity incident, your organization likely will need to pull in key incident response specialists to investigate and resolve the incident. Your cybersecurity insurance carrier likely will drive who you engage with – either selecting the firms for you or providing you a “panel” of providers to choose from.

*Cybersecurity Legal Experts*

Your insurance carrier will likely engage external counsel from a firm that specializes in handling cybersecurity incidents. The other specialists will be engaged through counsel so that the work is performed under attorney client privilege.

*Digital Forensics and Incident Response (DFIR) team*

Specialists who are trained and have the tools to full investigate root cause of the incident. The DFIR will generally assist you with removing the attacker from your environment and identifying how to stop them from returning.

*Negotiation Experts*

Should the incident involve extortion, a team of negotiators is often brought in even when there is no intent to pay the extortion. These negotiators can be used to gather information about the attackers, stall for additional time, and reduce the payment amount (if necessary.)

# How do we know our controls are working?

Once the cybersecurity program is designed and implemented, it is critical to test whether it is working as intended.

The threats in the world of cybersecurity are constantly evolving so we must continue to measure whether the cybersecurity program needs to be improved.

# Assessing Cybersecurity

### Internal Assessments

Given cybersecurity threats constantly evolve, your organization needs to continuously review the implementation of your security controls to ensure they are operating effectively.

On an ongoing basis, the team should use information from alerts and reports (such as phishing emails that reach employees) to re-evaluate control implementation. At least annually, the organization should do a formal review of the implemented controls.

### Third Party Assessments

Consider having a third party perform independent assessments of your governance and technical control environment against best practices. An independent assessor brings the value of exposure to best practices in many environments.

### Tabletop Exercises of Contingency Plans

A tabletop test of contingency plans facilitated by an external consultant can provide perspective on whether your response teams are trained well to be able to contain an incident and minimize impact.

# Vulnerability Assessments and Penetration Tests

### Vulnerability Assessment

Vulnerability Assessments use a tool to detect known vulnerabilities in the environment. This provides insights of technical flaws with minimal effort but can be incomplete.

### Penetration Test

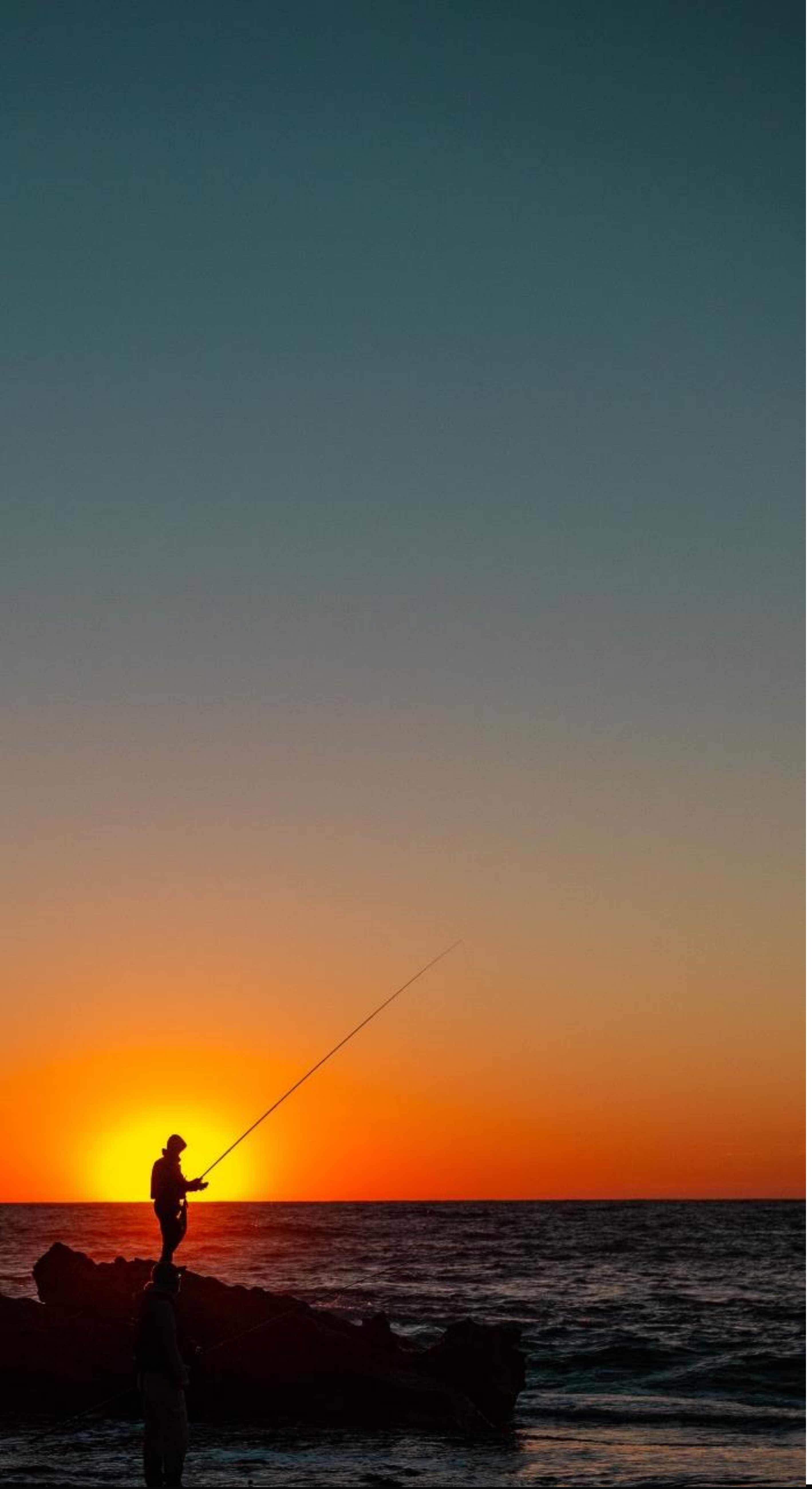
A Penetration Test uses the skills of someone who is trained to use an attacker's toolset to determine where the significant gaps are in the external and/or internal security of the organization. They essentially act as an attacker would, without breaking your environment.

### Test Scope

The assessments should cover both the external perimeter and internal network.

### Test Frequency

Vulnerability assessments should be performed quarterly. A penetration test by an external independent third party should be performed at least once a year.



# Validating Employee Training

### Information Security Awareness Training

The platform and/or process used to train employees on cybersecurity best practices should include checks to make sure that users are understanding and applying the material.

### Phishing / Social Engineering Tests

Additionally, consider performing simulated phishing or other social engineering attacks against the users monthly or quarterly. A well-trained organization will average 3-5% of users failing a phishing test. However, the focus should be on making sure users reported the phishing attempts to the cybersecurity team.

### Tabletop Exercises of Contingency Plans

A tabletop test of contingency plans facilitated by an external consultant can provide perspective on whether your response teams are trained well to be able to contain an incident and minimize impact.

# CPE Prompt 5 of 5

# 5 Steps for Protecting Your Organization

1 STRATEGY

2 IDENTIFY

3 PROTECT

4 BUILD

5 POLICY

Capture your decisions in well documented policy and procedures.

Pick the right policies and procedures for your needs.

# Information Security Program

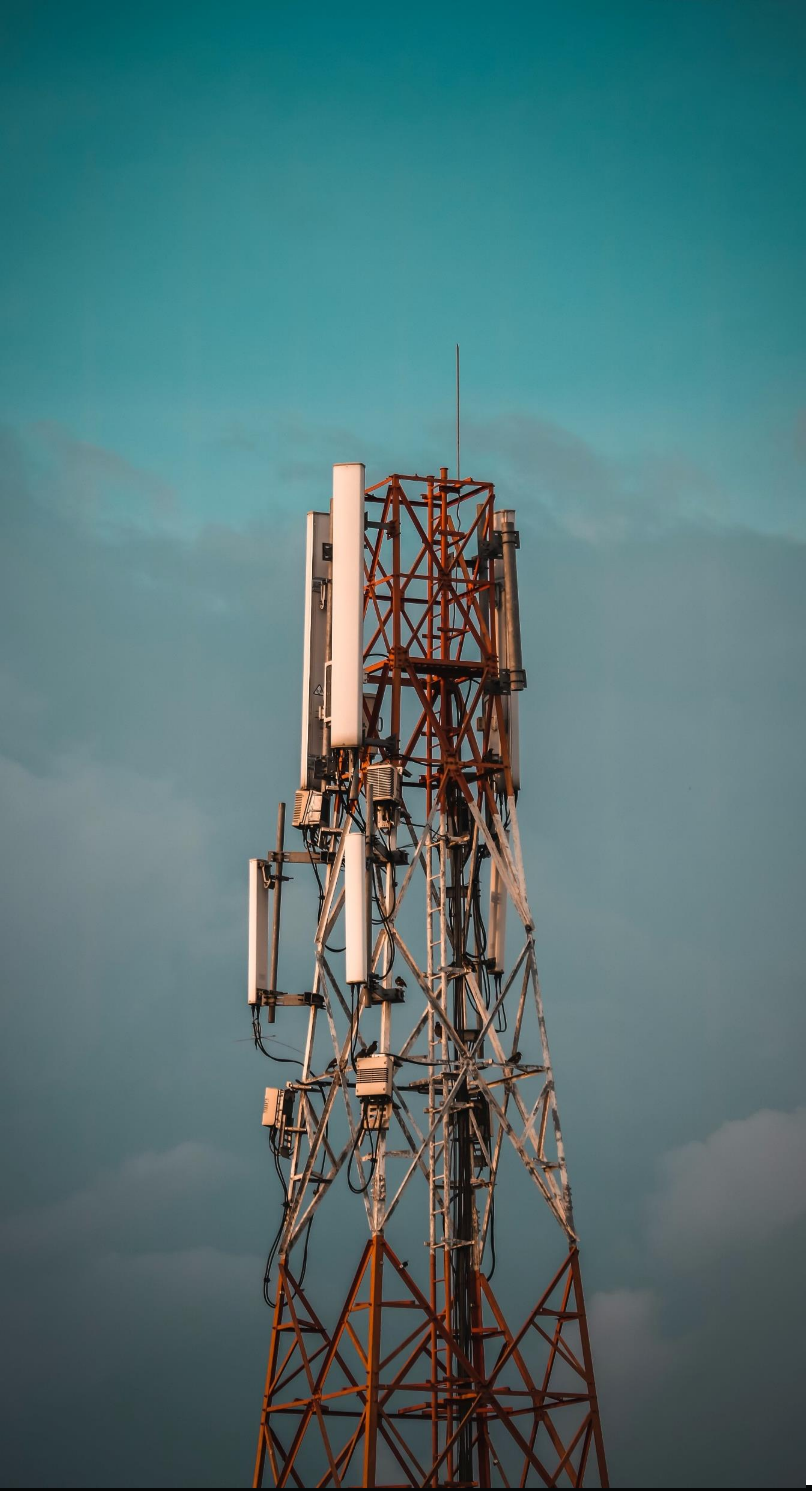
Captures the comprehensive framework and strategy determined by the organization for safeguarding an organization's data and information assets.

- Establishes a process for identifying and assessing security risks.
- Documents a series of policies, procedures, and technical measures to mitigate risks.
- Creates a process for continuously managing and monitoring security measures to protect sensitive information.

# Employee Acceptable Use Policy

Defined set of guidelines for employees regarding the appropriate use of organization's technology resources.

- Identifies permissible and prohibited actions and behaviors when utilizing the organization's assets and systems.
- Implements rules and restrictions to ensure the responsible and secure usage of these resources.
- Sets expectations for employees to uphold organizational security requirements.



# Third Party Risk Management Program

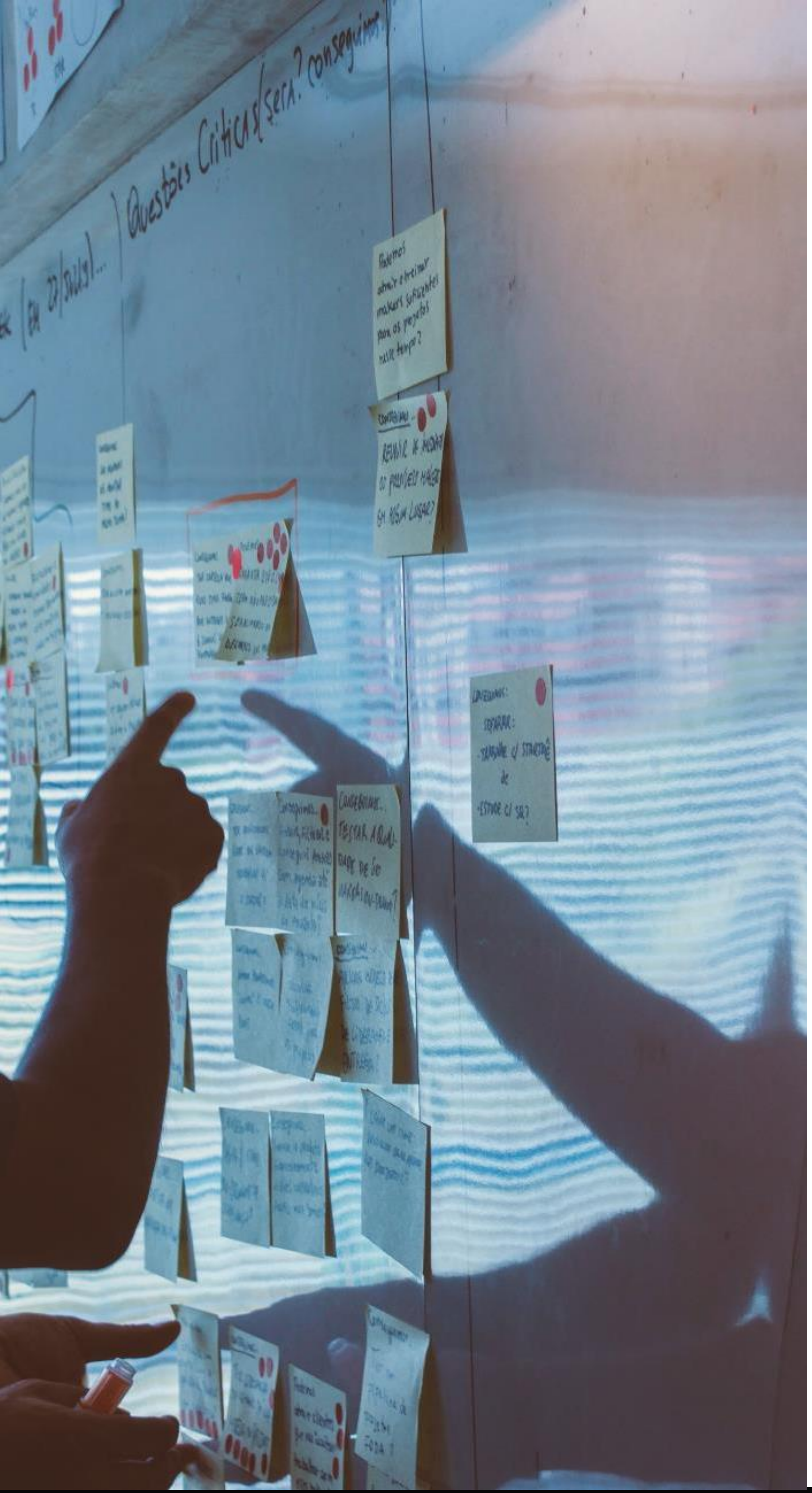
A structured approach to understanding and mitigating potential risks associated with external vendors, constituents, and other third parties.

- Identifies and assesses risks posed by third-party relationships.
- Creates and implements risk mitigation strategies and controls.
- Continuously monitors and manages risks of the third parties to safeguard your organization’s interests and operations.

# Business Continuity Plan (BCP)

Crisis management plan which establishes approaches to maintain critical operations and constituent services during a disaster scenario.

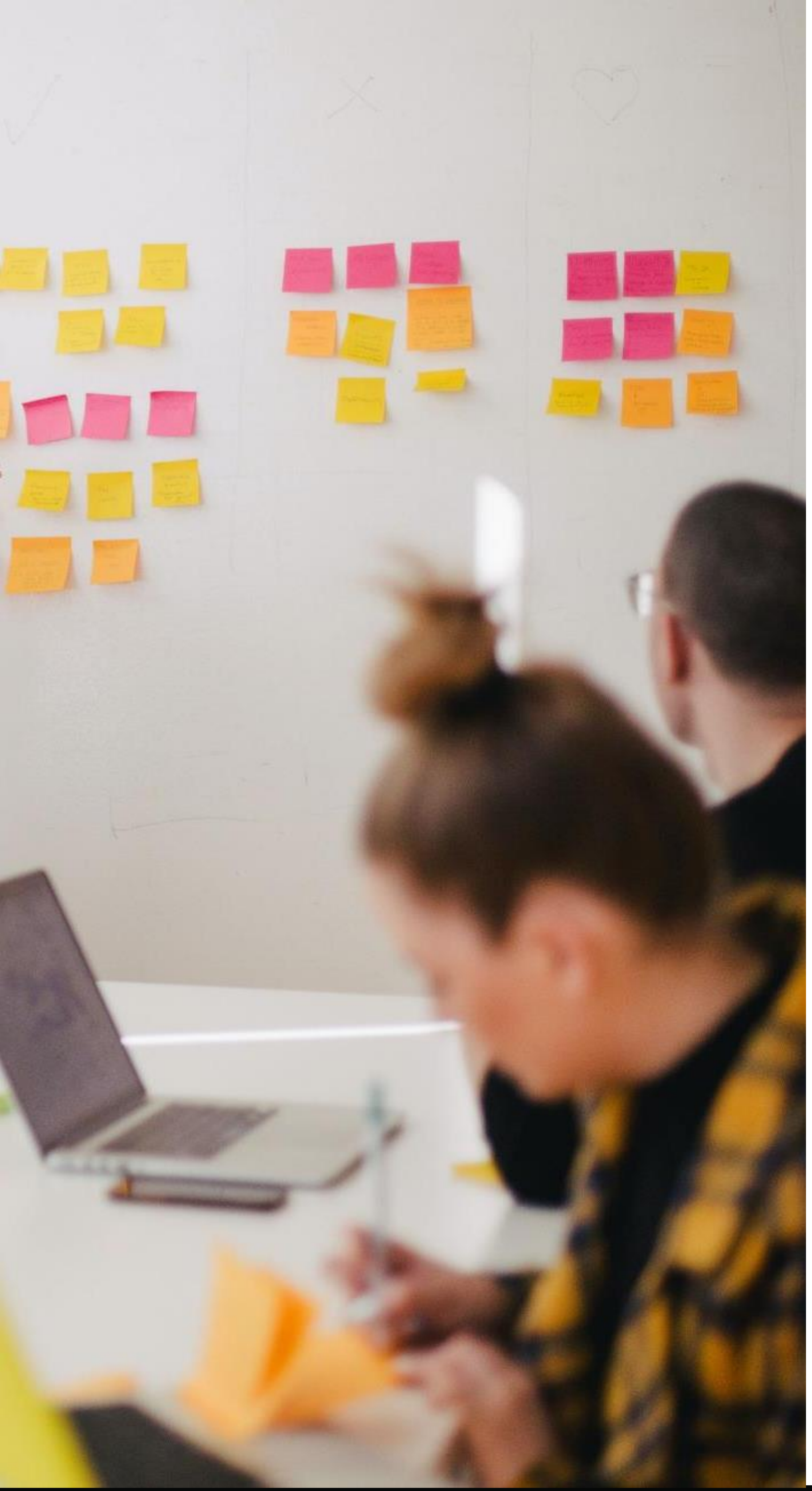
- Identifies critical services that must continue even during a widespread disaster.
- Determines the people, processes, and technology that each critical service is dependent on.
- Builds alternative processes to continue to deliver the critical services when one or more of a critical service’s dependencies  are unavailable.



# Disaster Recovery Plan (DRP)

Information Technology focused plan which supplements the BCP and documents the processes to restore the technology environment back to normal after a disaster.

- Systems are restored to temporary and then normal operating processes.
- The prioritization of the systems being restored and the time objectives for doing so should be driven by operational needs identified in the BCP.



# Incident Response Plan (IRP)

Information Technology focused plan which supplements the BCP and documents the processes to restore the technology environment back to normal after a disaster.

- Systems are restored to temporary and then normal operating processes.
- The prioritization of the systems being restored and the time objectives for doing so should be driven by operational needs identified in the BCP.

# Thank you for joining us!

Rehmann

EMPOWER YOUR PURPOSE®

Stay up-to-date on helpful resources for your organization at www.rehmann.com.

**Questions?**

Please contact us at:
publicsector@rehmann.com