TECHIMPACT®

Managing Cyber Risk

OCTOBER 17 2023

WE’RE A NONPROFIT ON A MISSION TO LEVERAGE TECHNOLOGY TO ADVANCE SOCIAL IMPACT.

TECHIMPACT®

We do this by delivering tech services, education, and training that help nonprofits and communities thrive.

NONPROFIT TECH SERVICES:

- Impartial advice
- Well-aligned solutions
- Adopt technology that fulfills missions

NONPROFIT EDUCATION & TRAINING:

- Unbiased research
- Easy-to-understand
- One-to-many approach

WORKFORCE DEVELOPMENT:

- Hands-on experience
- Launching careers
- Improved quality of life

FRANCIS JOHNSON

Managing Director of Technology Services

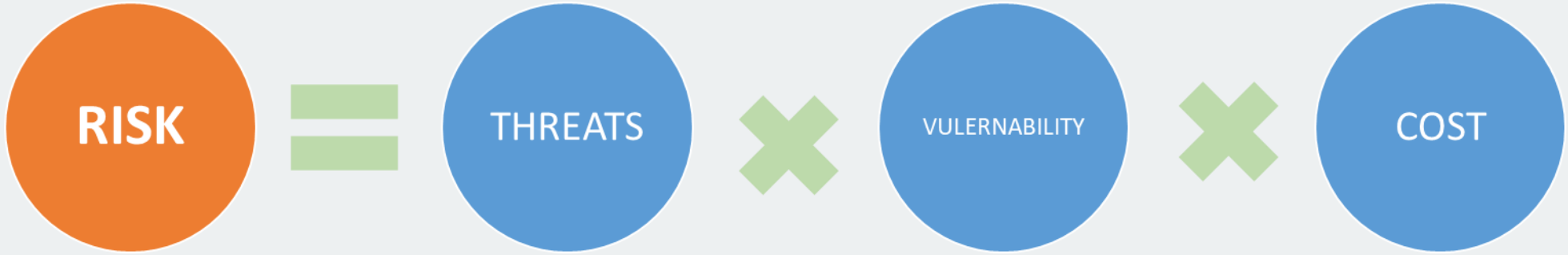
I manage all aspects of technology services including our Managed IT Support and Cybersecurity services, and technical projects. Our team works with nonprofits across the country to implement on-premises and cloud infrastructure, improve security and provide mobile working opportunities.

francis@techimpact.org

TECHIMPACT®

ORGANIZATIONAL RISK

CYBER RISK EXPLAINED



Cyber criminal	Weak policies	Ransom
Network failure	Outdated systems	Fund transfer
Device loss	Unsecure device	System recovery

Cyber risk is based on the probability of a bad event happening to your information systems, leading to the loss of data, integrity, and/or money.

DATA BREACH STATISTICS

Data breach costs averaged **$4.45 million**

Data breach costs for the healthcare industry averaged **$10.93 million**, by far the costliest industry

82% of breaches involved data stored in the cloud

Only **33%** of breaches were detected by internal teams and tools

Initial Attack Vectors:

- Phishing **(16%)**
- Stolen or compromised credentials **(15%)**
- Cloud misconfiguration **(11%)**

Source: Ponemon Institute 2023 Cost of Data Breach Study

TECHIMPACT®

COST OF A DATA BREACH: ACTUAL COSTS

- System recovery
- Data restoration
- Legal guidance
- Crisis management
- Regulatory fines
- Breach notification
- Forensics
- Credit monitoring

Source: Ponemon Institute 2023 Cost of Data Breach Study

Managing Cyber RISK

TECHIMPACT®

What is NIST?

National Institute of Standards and Technology
Their mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

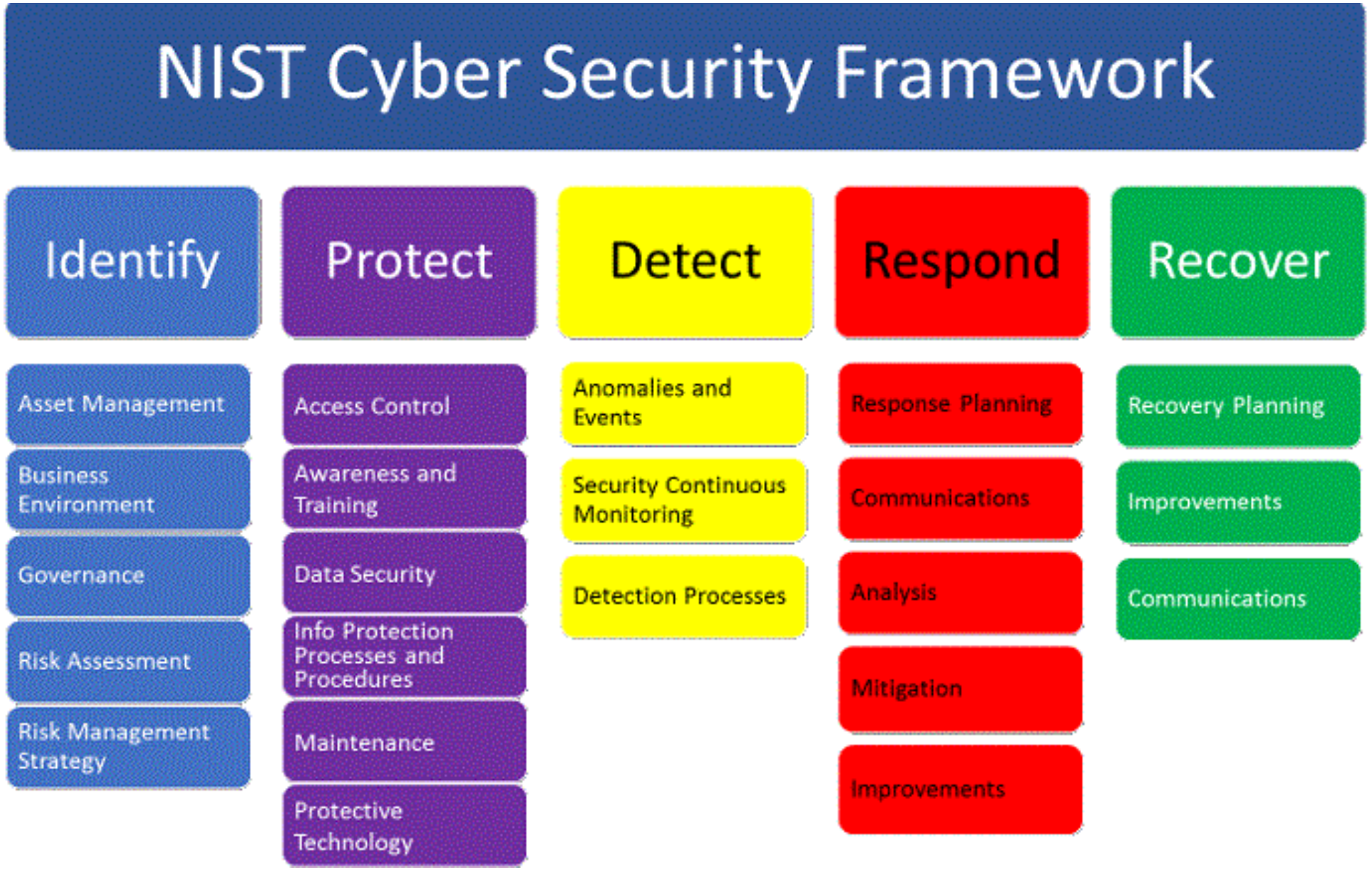
What is NIST CSF?

Cyber Security Framework
The CSF provides high-level guidance, including a common language and a systematic methodology for managing cybersecurity risk across sectors and aiding communication between technical and nontechnical staff.

FRAMEWORK: NIST CSF

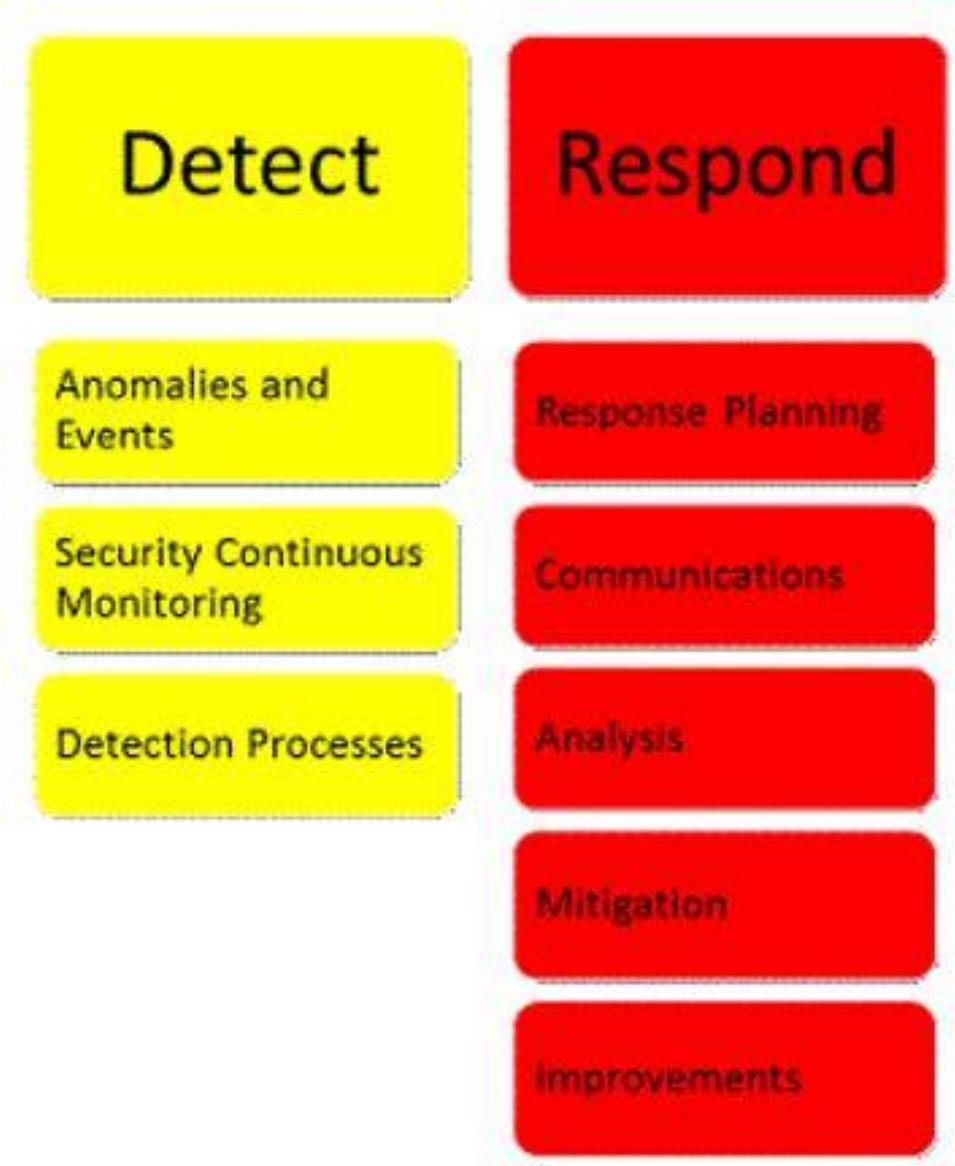
Source: N.Hanacek/NIST

FRAMEWORK: NIST



TECHIMPACT®

FOCUS:



TECHIMPACT®

Only **33%** of breaches were detected by internal teams and tools

Source: Ponemon Institute 2023 Cost of Data Breach Study

TECHIMPACT®


THAT'S TURRIBLE
quickmeme.com

Only **33%** of breaches were detected by internal teams and tools

Source: Ponemon Institute 2023 Cost of Data Breach Study

TECHIMPACT®

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

- ❑People
- ❑Processes
- ❑Tools

SIEM
Security Information & Event Management

What is SIEM?

Security Information and Event Management, is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.

SIEM, pronounced “sim,” combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action.

Microsoft Security: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

Microsoft 365

Google Workspace

WEBROOT

cisco Meraki

SONICWALL

SOPHOS

aws

SIEM PLATFORM

TECHIMPACT®

ROCKETCYBER

148 Devices Online

96 Devices Offline

0 Devices Isolated

4,812 Office365 Mailboxes

21 Network Devices

Advanced Breach Detection

445 Events

Review

Configure

Crypto Mining Detection

0 Events

Review

Configure

Cyber Terrorist Network Connections

2,875 Events

Review

Configure

Datto EDR Monitor

0 Events

Review

Configure

Datto Ransomware Detection

0 Events

Review

Configure

Defender for Business

12 Events

Review

Configure

Defender Manager

143 Events

Review

Configure

Endpoint Event Log Monitor

30,070 Events

Review

Configure

What questions do have?

TECHIMPACT®

LIVE DEMO……

RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

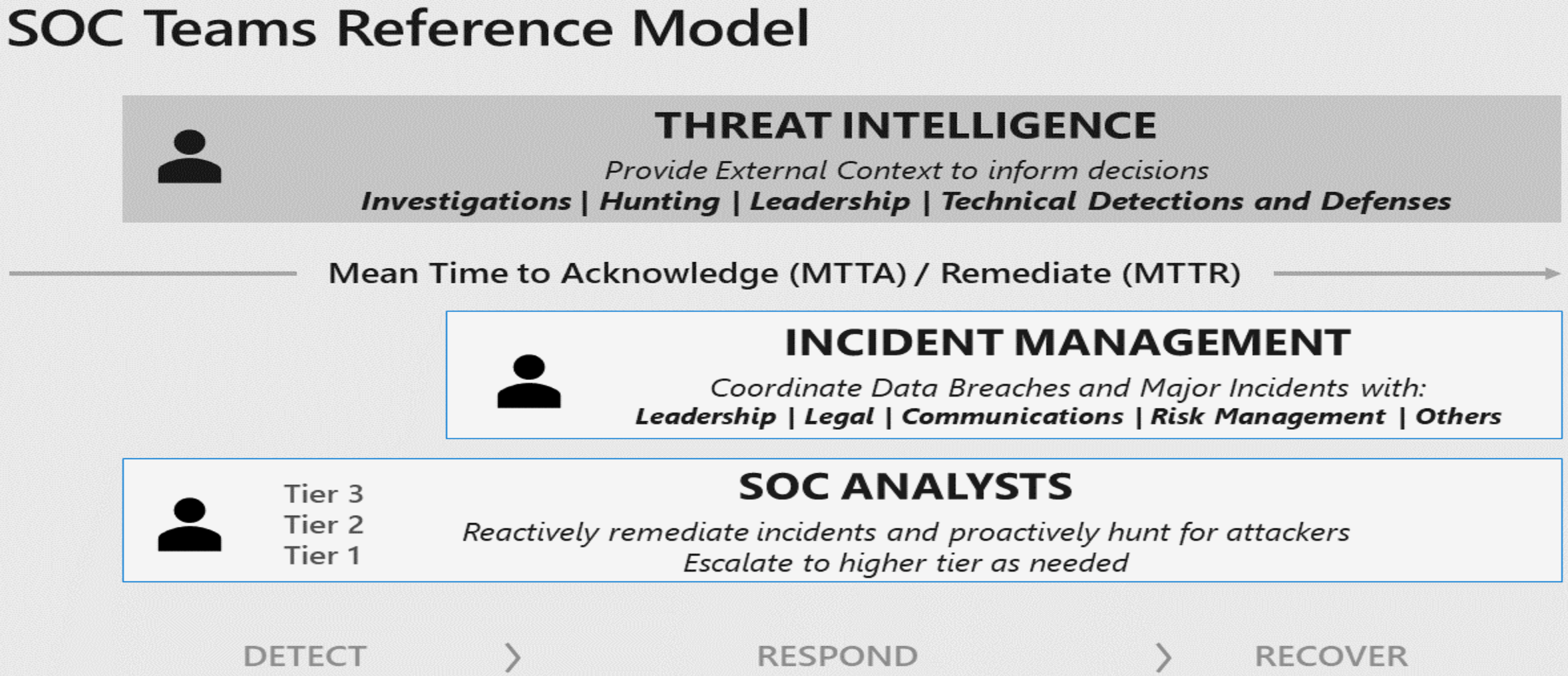
- ❑People
- ❑Processes
- ❑Tools

SOC
Security Operations Center

What is SOC?

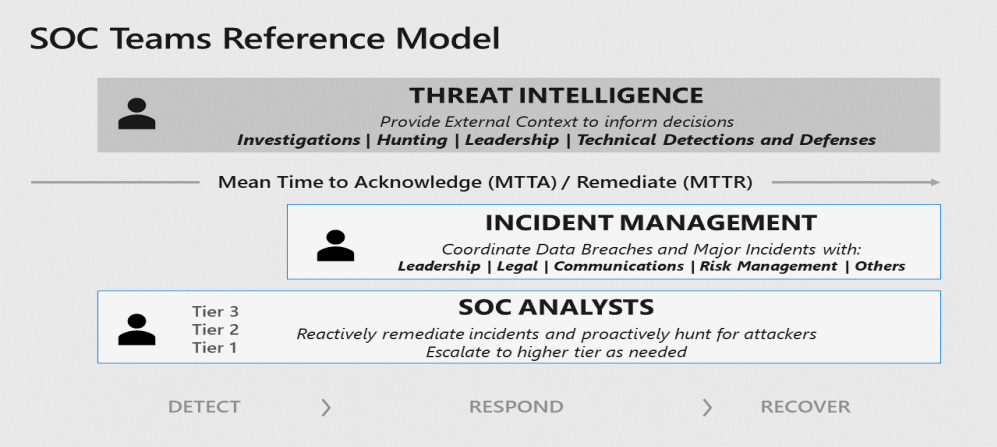
Security Operations Center, is the team responsible for protecting an organization against cyber threats. SOC analysts perform round-the-clock monitoring of an organization's network and investigate any potential security incidents. If a cyberattack is detected, the SOC analysts are responsible for taking any steps necessary to remediate it.

Example of a SOC Team



Microsoft SOC Teams Reference Model https://www.microsoft.com/en-us/security/blog/2019/04/23/lessons-learned-microsoft-soc-part-2-organizing-people/

Managed SOC



External SOC Team

SIEM Monitoring
Alert Configuration
Initial Remediation
Incident Management
Incident Reporting
Escalation to Internal Team

Internal IT Team

Remediation
Escalation
Incident Management
Security Control Implementation

TECHIMPACT®

What questions do have?

TECHIMPACT®

BRINGING IT ALL TOGETHER…

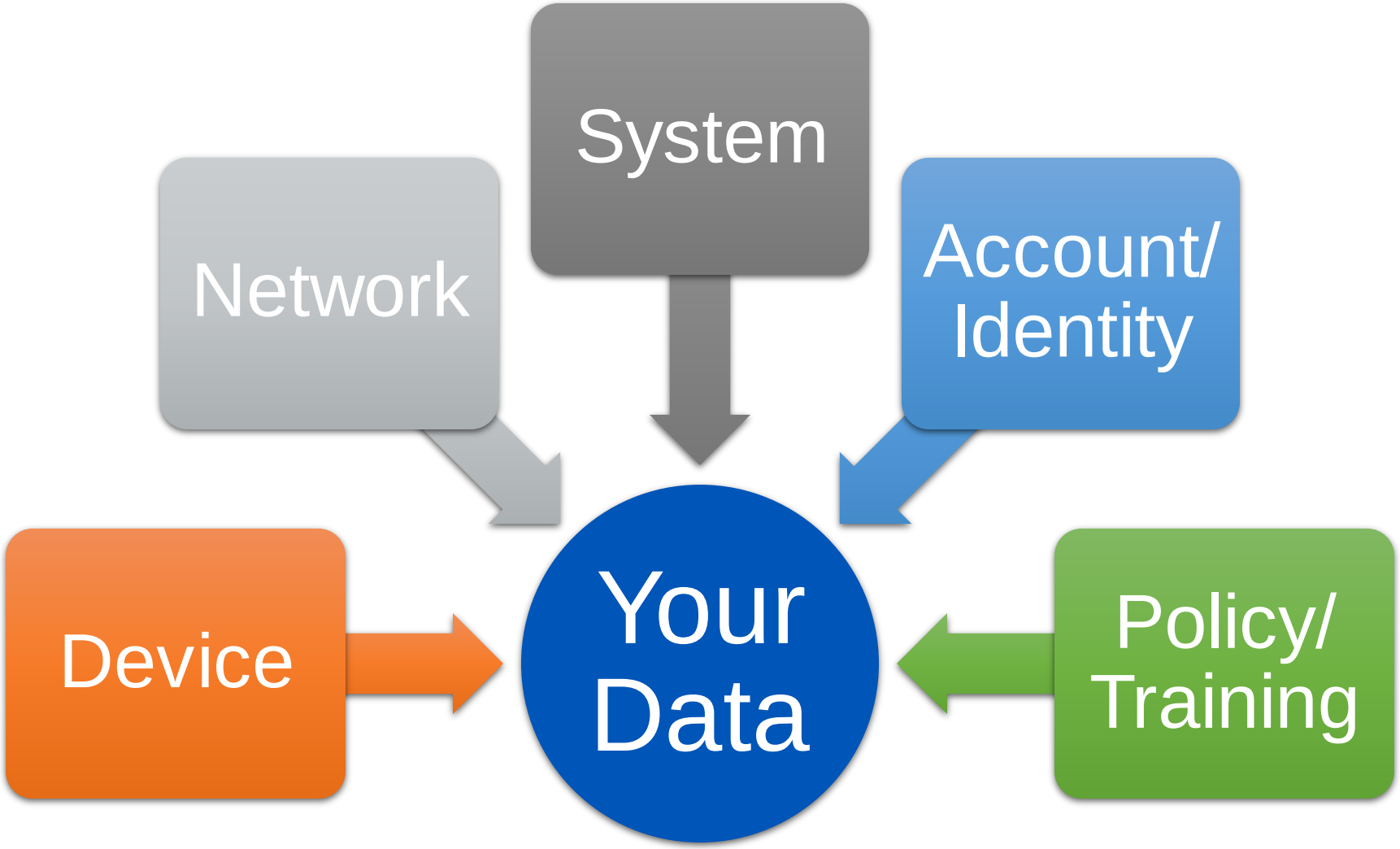

RECOVER
IDENTIFY
CYBERSECURITY
FRAMEWORK
VERSION 1.1
PROTECT
RESPOND
DETECT

Identify EVERYTHING

- Cloud Discovery
- On-Premise Discovery
- Compliance Discovery
- Data Discovery
- Device Discovery

Example of a Self Assessment Worksheet

Protect EVERYTHING



PASSWORD PRACTICES

01

Make passwords as long as possible: 20+ characters or use pass phrase

02

Don’t reuse passwords – ever

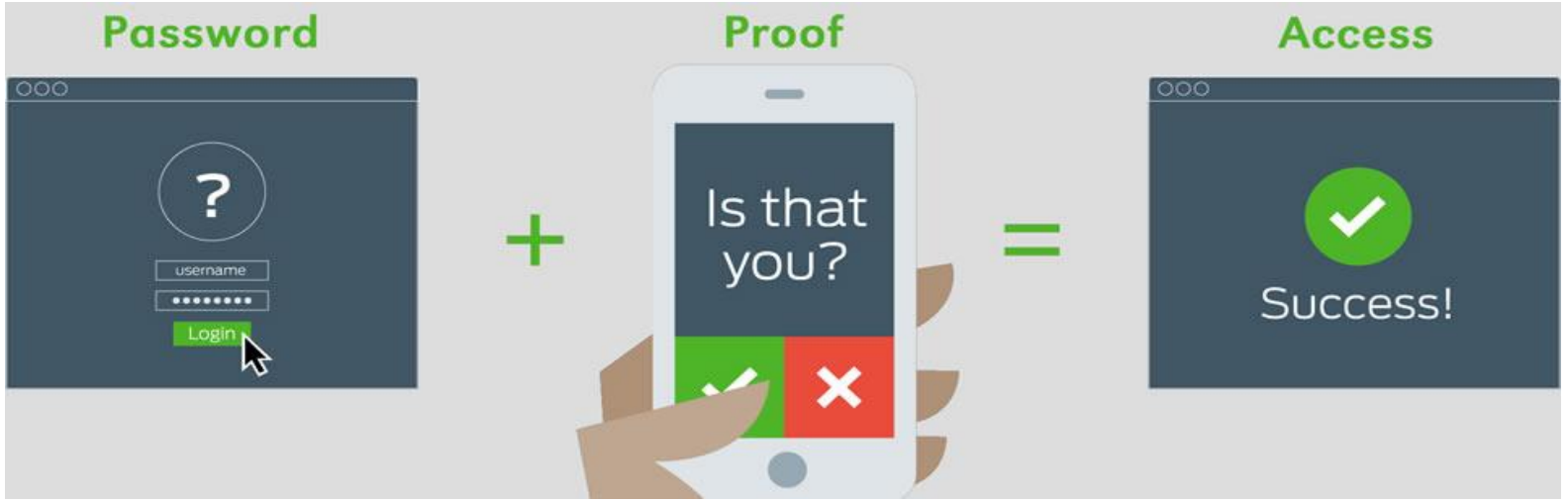
03

Don’t share passwords unless you absolutely have to. Use a password manager

04

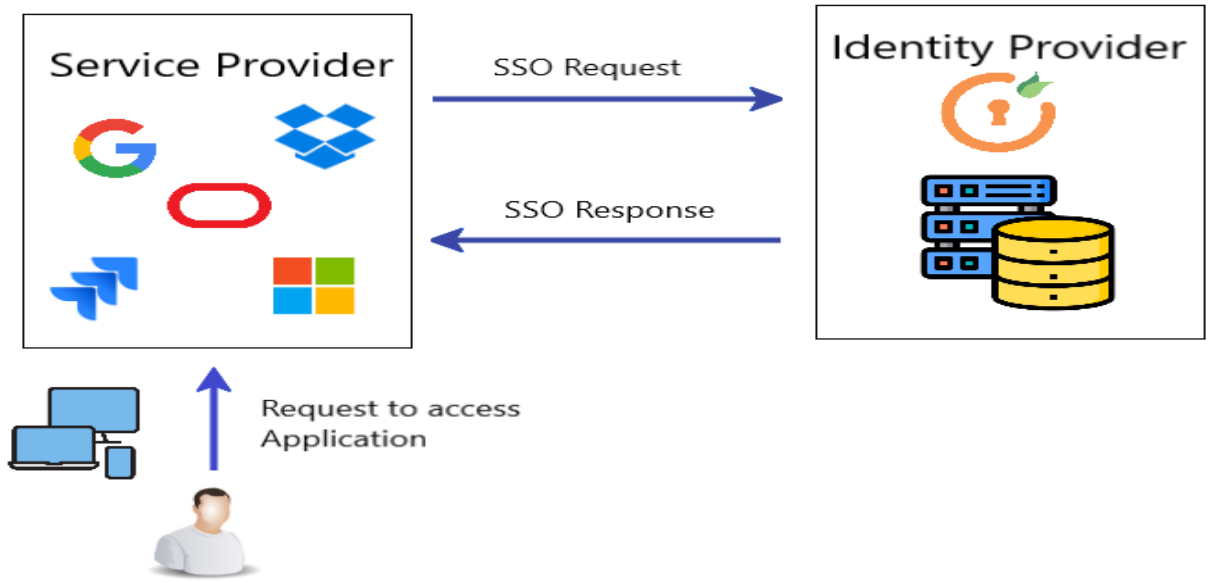
Use multi-factor authentication

MULTI-FACTOR AUTHENTICATION



- Use one centralized system as an identity / MFA provider
  - Users are prompted on phone using mobile app
  - Users receive phone call or text message verifying identity
- “Remember” devices for configurable period of time to prevent the need for entering two-factor during that time

SINGLE SIGN ON



- Use one identity provider to provide secure access to multiple applications and services
  - ❑ Allows for efficient and secure user account management
  - ❑ Significantly reduces user password fatigue and frustration
  - ❑ Improves user logon experience

PASSWORD MANAGERS

- Improves security by organizing credentials and passwords, allows users to have strong passwords that they do not have to remember
- Some, like Keeper allow centralized administration

RECOVER

Your mission and business relies on access to computers systems and data to operate. Having a plan and practices in place to continue to work in the event of outage or system breach allows your work to go on as you recover.

- Business Continuity Plan
- System Recovery
- Data Backup

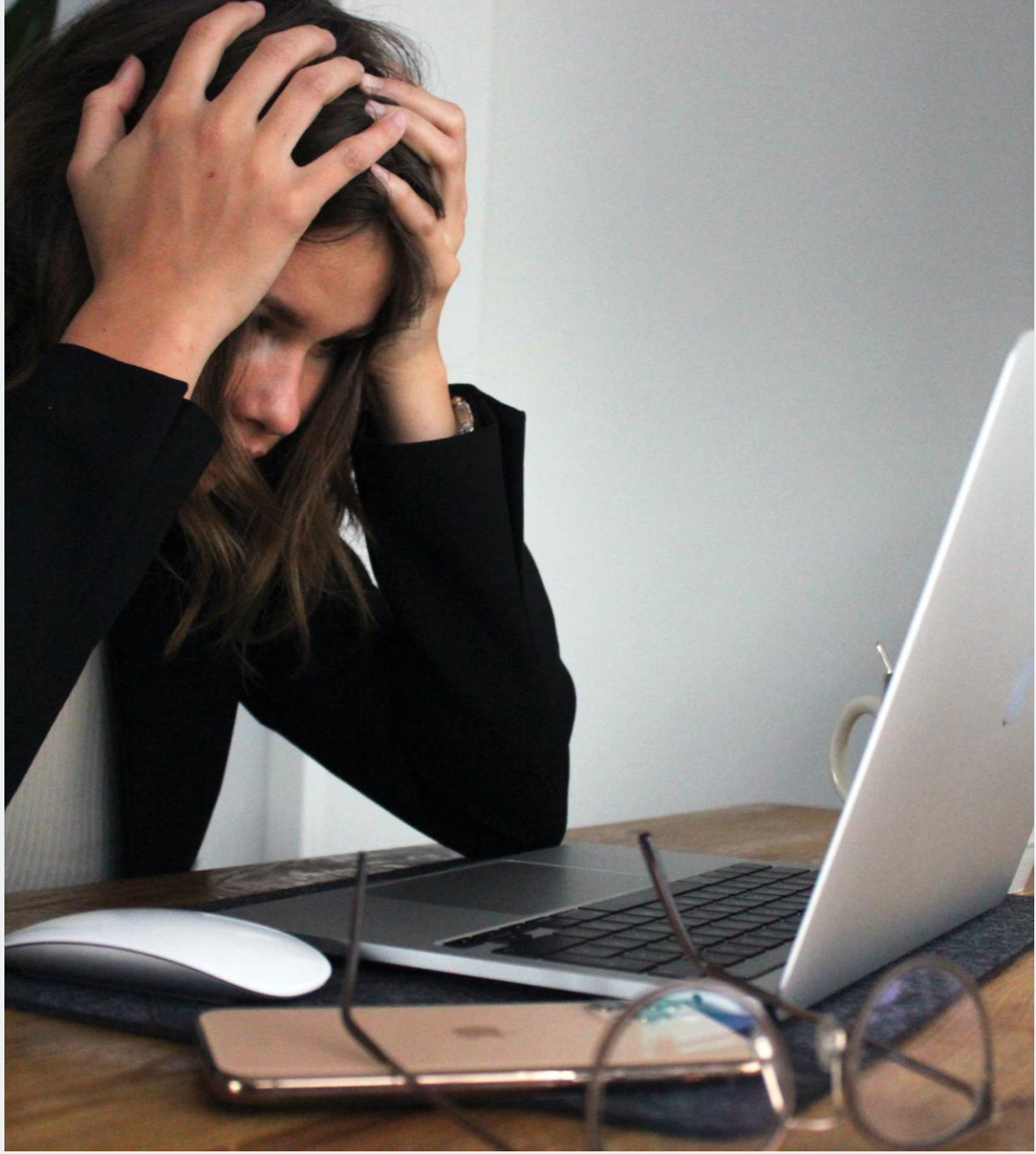
Example of a Disaster Recovery Plan

Managing CYBER RISK Is...

- ✓ Difficult
- ✓ Time Consuming
- ✓ Frustrating
- ✓ Confusing
- ✓ Costly

And yet...

TOTALLY WORTH IT!



TECHIMPACT®

INTO THE Q&A:
What questions do have?

TECHIMPACT®

THANK YOU

Francis Johnson: francis@techimpact.org