TECHIMPACT®

Understanding Cyber Security Insurance Requirements

WE’RE A NONPROFIT ON A MISSION TO USE TECHNOLOGY TO BETTER SERVE THE WORLD.

TECHIMPACT®

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

NONPROFIT TECH SERVICES:

- Managed IT Support
- Cloud Migration
- Cyber Security & Compliance
- Data Systems Support
- Strategic Consulting & Planning
- Machine Learning & AI

NONPROFIT EDUCATION & TRAINING:

- Nonprofit Technology Reports
- Consumer Guides to software
- Technology Assessments
- Workbooks & Articles
- Online Training Courses
- Free Webinars

WORKFORCE DEVELOPMENT:

ITWorks & CXWorks:
Free IT and Customer Experience training programs

PunchCode:
12-week immersive programming bootcamp

TECHIMPACT®

LINDA WIDDOP

Chief Customer Officer

Over the past two decades, I have worked with thousands of nonprofits across the country and the world to help them understand, implement, and support the ever-changing technologies that help them meet their mission. I speak at conferences and events presenting relatable and timely topics include the importance of technology planning, cybersecurity, data visualization and more.

I am an obsessed birder who loves to travel and engage in citizen science projects that help inform environmental protection actions.

linda@techimpact.org

TECHIMPACT®

FRANCIS JOHNSON

Chief Technology Officer

I manage all aspects of technology services including our Managed IT Support services and technical projects. Our team works with nonprofits across the country to support and improve their infrastructure and systems.

francis@techimpact.org

TECHIMPACT®

INTRODUCTION TO CYBER SECURITY RISK

WHAT IS CYBER SECURITY?

Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked which can lead to financial loss, damaged reputation and even cause your organization to close.

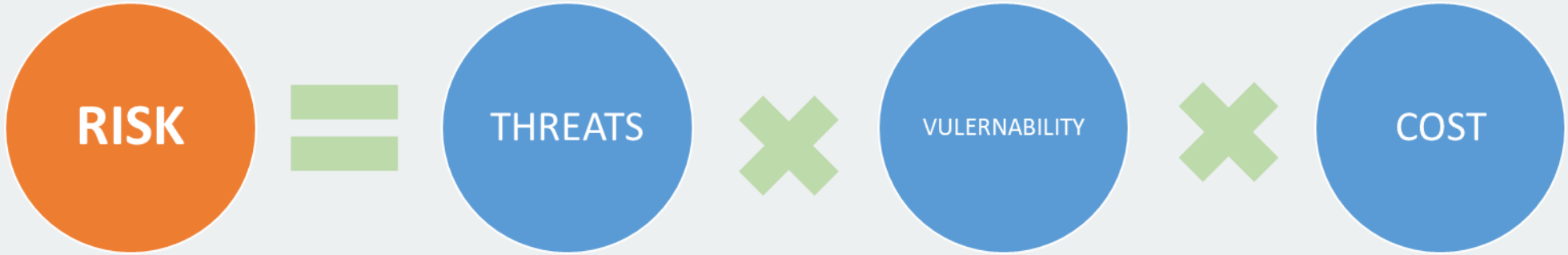
Protecting against cyber crime and/or data leakage involves lowering your organization’s risk of such events.

WHAT IS CYBER SECURITY?

Cybersecurity refers to **preventative methods** used to protect information from being stolen, compromised or attacked which can lead to financial loss, damaged reputation and even cause your organization to close.

Protecting against cyber crime and/or data leakage involves **lowering risk** of such events.

CYBER RISK EXPLAINED



THREATS	VULERNABILITY	COST
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.

COST OF A DATA BREACH: ACTUAL COSTS

- System recovery
- Data restoration
- Legal guidance
- Breach notification
- Forensics
- Credit monitoring

Source: Ponemon Institute 2020 Cost of Data Breach Study

WHAT ELSE IS AT RISK?

Your Reputation

Financial Performance

Regulatory Environment

COST OF A DATA BREACH: INTANGIBLE COSTS

The lost trust that nonprofits experience from donors, volunteers and the community can affect

- fundraising activities
- volunteer engagement
- partnerships with other organizations

Source: Ponemon Institute 2018 Cost of Data Breach Study

IT'S NOT "IF", IT'S "WHEN"

Security Breaches are going to happen even if your organization has taken steps to secure the environment and train users.

- Act Quickly – contact your IT professional at the first hint of trouble. Train staff to notify IT without fear of Repercussion
- Have a Plan and Follow It – know what to do, how to communicate
- Recover Losses – invoke your insurance plan

TECHIMPACT®

QUESTION:
WHAT IS THE AVERAGE NUMBER OF DAYS A RANSOM INCIDENT LASTS?

QUESTION:
WHAT IS THE AVERAGE COST OF A RANSOMWARE ATTACK?

LET'S ANSWER SOME QUESTIONS!

TECHIMPACT®

Cyber Insurance Explained

TECHIMPACT®

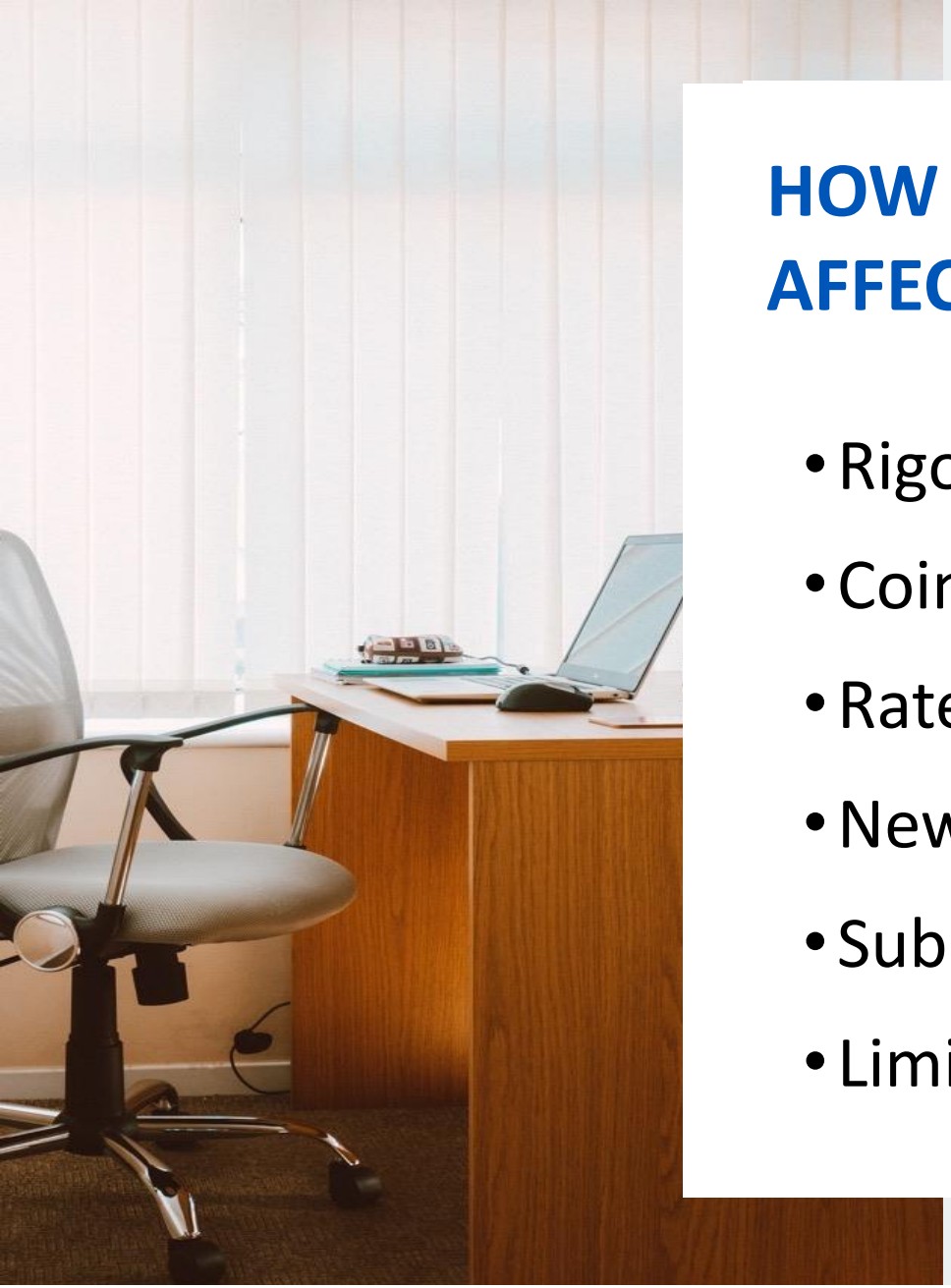
CYBER LIABILITY INSURANCE

FIRST PARTY

Losses/ expenses
incurred by insured

THIRD PARTY

Economic damages
suffered by others



HOW HAVE INCREASED CYBER THREATS AFFECTED THE CYBER INSURANCE MARKET?

- Rigorous underwriting process
- Coinsurance up to 50%
- Rate increases from 30% to 100%, but stabilizing.
- New Exclusions
- Sublimiting cyber extortion, etc.
- Limiting dependent business interruption

CYBER SECURITY INSURANCE CHECKLIST

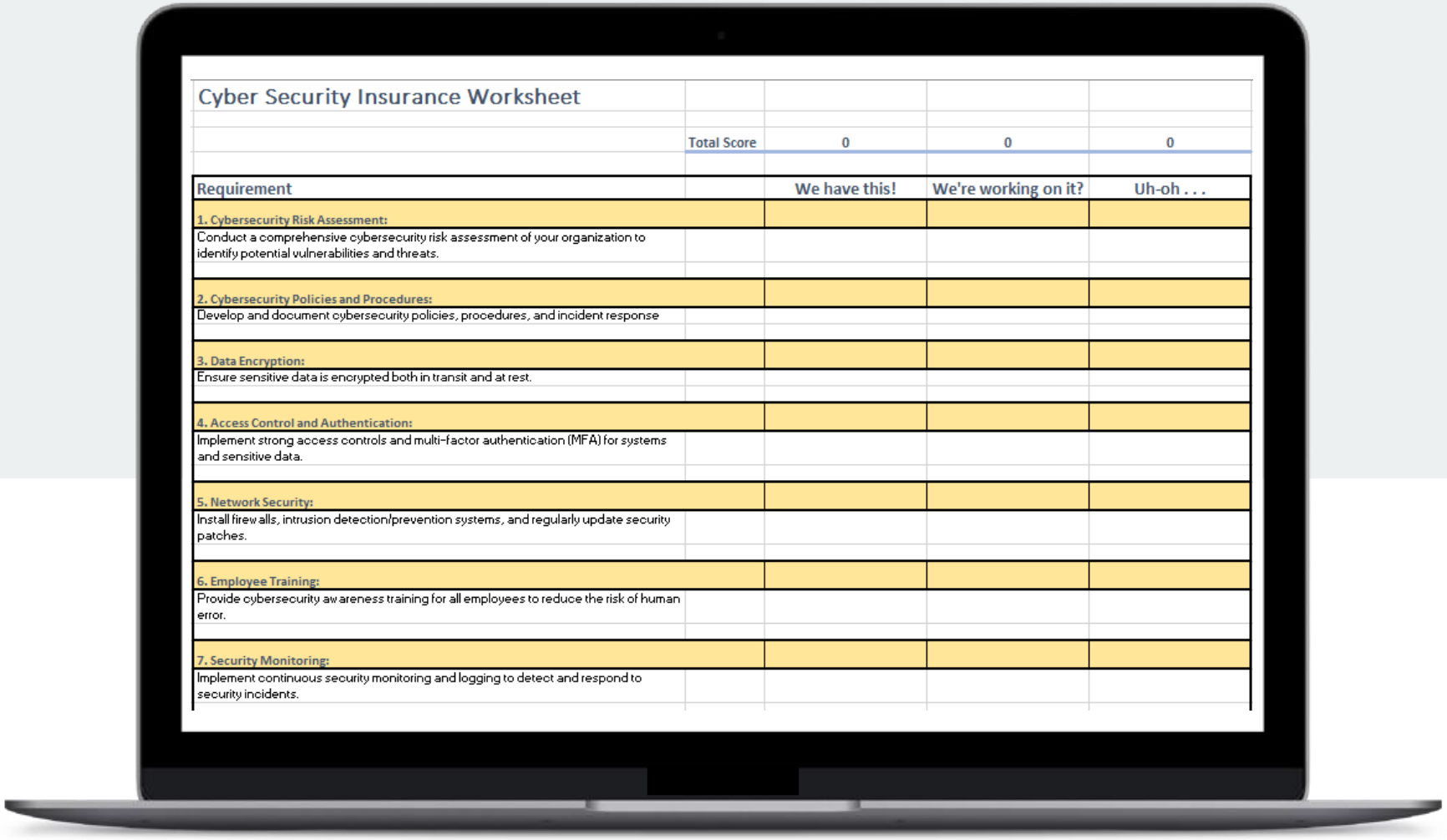
https://offers.techimpact.org/reports/cyberinsurance_checklist

TECHIMPACT®

Worksheet Time

CYBER SECURITY INSURANCE WORKSHEET

Let’s work on the paper copy today. Digital copy will be emailed.



Cyber Security Insurance Worksheet

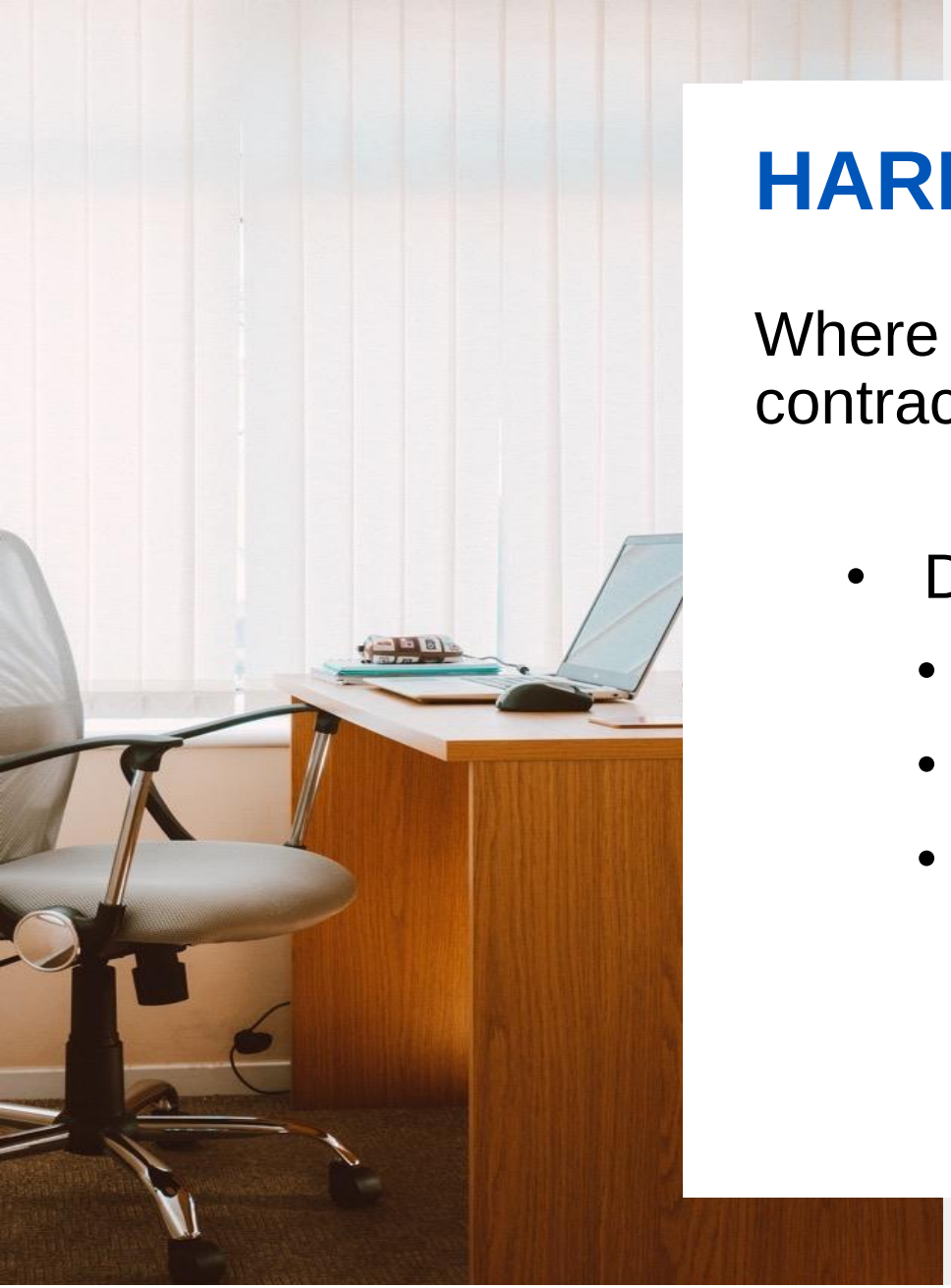
	Total Score	0	0	0
Requirement		**We have this!**	**We're working on it?**	**Uh-oh . . .**
1. Cybersecurity Risk Assessment:				
Conduct a comprehensive cybersecurity risk assessment of your organization to identify potential vulnerabilities and threats.				
2. Cybersecurity Policies and Procedures:				
Develop and document cybersecurity policies, procedures, and incident response				
3. Data Encryption:				
Ensure sensitive data is encrypted both in transit and at rest.				
4. Access Control and Authentication:				
Implement strong access controls and multi-factor authentication (MFA) for systems and sensitive data.				
5. Network Security:				
Install firewalls, intrusion detection/prevention systems, and regularly update security patches.				
6. Employee Training:				
Provide cybersecurity awareness training for all employees to reduce the risk of human error.				
7. Security Monitoring:				
Implement continuous security monitoring and logging to detect and respond to security incidents.				

TECHIMPACT®

WHAT'S WITH THE SCORES?

- **We Have This!** – is obviously a good thing. Your cyber insurance premiums should be reasonable, the carrier is likely to underwrite the policy and you've actually *lowered the risk* of a data loss event
- **We're Working On It?** – is still a good thing. Your carrier should consider your efforts as "*good faith*" when writing the policy
- **UH-OH …** - is obviously going to *limit* your ability to get a policy or make the premium *more expensive*. You'll need to take action.

It’sNot on the Checklist,BUT …



HARDEN DEVICE SECURITY

Where possible, limit the use of personal devices by staff, contractors and volunteers

- Devices are centrally managed by the IT Pro
  - Pro version of operating system, desktop apps
  - Automated updates, AV/AM
  - User authentication managed by AD/AzureAD or other

MDM

Mobile Device Management

Control Of Full Device

- Best suited for organizational owned devices
- Can set security parameters:
  - Requiring PIN or Multi-Factor Authentication
  - Remote Wipe & Password Reset

BRING YOUR OWN DEVICE (BYOD) POLICIES

Personal devices present risk to the organization:

- Outdated, Home version of OS and applications
- Lack of / outdated AV/AM
- Updates require user involvement
- No user authentication / weak passwords
- Shared among family members

MAM

Mobile Application Management

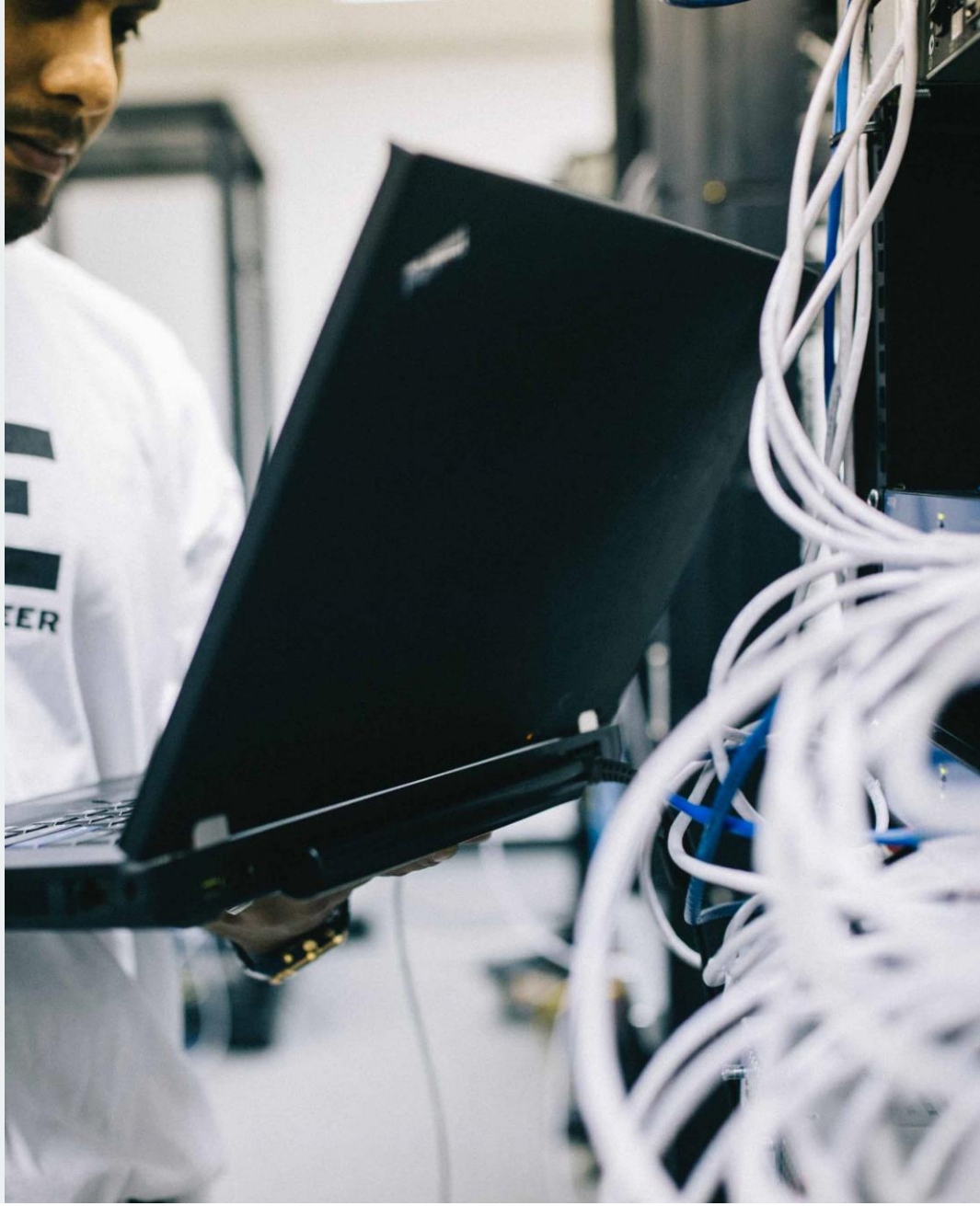
Control Of Applications

- Best suited for personally owned devices
- Can apply security settings to applications:
  - Restrict actions
  - Set authentication policies
  - Selective wiping of organizational data

REDUCE PENETRATION TARGET

Where possible, eliminate public facing servers, applications, and network devices managed by your organization.

- Move to cloud
  - Cloud provider handles perimeter, server and platform security
- Streamline networks
  - Remove excess devices
  - Take out unused VPNs or WAN connections
- Stay up to date
  - Upgrade outdated equipment
  - Keep current on service subscriptions



VPNS AND REMOTE DESKTOP PROTOCOLS

VPNs and Remote Desktop Protocols create a “tunnel” for your data to travel through securely on its way from the cloud host to your computer.

CLOUD SECURITY

With so many cloud applications in use, accounts and licensing can go unmanaged and become a risk. Websites should be audited to reduce risk of hijacking and data breach. Implementing access controls such as multifactor authentication and single sign-on help reduce risk

- Audit and manage all cloud platform accounts
- Audit website platform security and admin access
- Implement Multi-factor Authentication, Single Sign-On

IDENTITY SECURITY

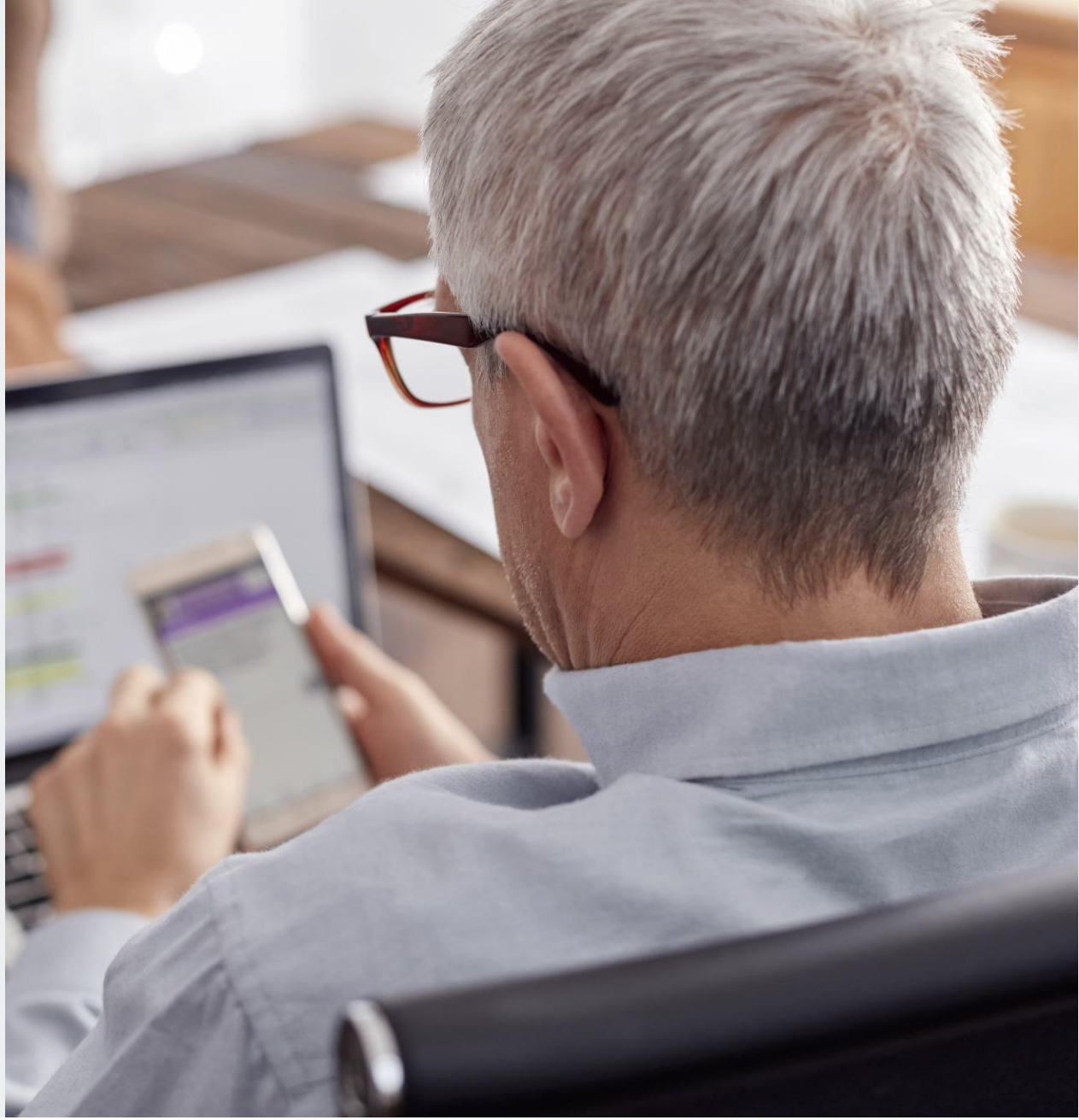
80% of cyber breaches start with user credentials being compromised. Cyber awareness training for all users is a great start to reduce this risk. Strong password management practices make credential stealing more difficult.

- Implement cyber awareness training for all users
- Require and manage strong passwords
- Audit administrator access to all systems

SINGLE SIGN-ON

Single Sign-On (SSO) allows access to cloud systems with one password that is managed by the organization.

- HR easy onboard/offboard
- IT sets strong credentials
- USER only needs to remember one login



DATA SECURITY

Data systems allow you to track critical aspects of your business including donors, volunteers, cases, and finance. Understanding and auditing access and storage of this data can lower risk of breach by eliminating records that are not in use.

(Each record lost in a breach costs your org $164 in recovery costs)

- Understand your data retention requirements
- Limit access
- Properly dispose of unnecessary data

RESILIANCE & CONTINUITY

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

I THINK WE'VE HAD A BREACH…

- Notify your insurance company
- Refrain from using business email
- Preserve data
- Disconnect all devices from network
- Understand how your cyber policy works

LET'S ANSWER SOME QUESTIONS!

TECHIMPACT®

THANK YOU!

Connect with us:

Linda Widdop at linda@techimpact.org
Francis Johnson at francis@techimpact.org

TECHIMPACT®