
TECHIMPACT®

TECHIMPACT®

CYBER SECURITY BASICS

TECHIMPACT®

CYBER SECURITY BASICS

TECHIMPACT®

CYBER SECURITY BASICS

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

Cyber Security Overview

What Is Cyber Security?

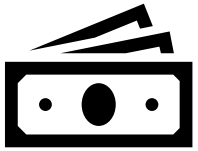
Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked.

This environment includes users, networks, devices, software, processes, information (in storage or transit), applications, services, and systems that can be connected directly or indirectly to networks.

TARGETS

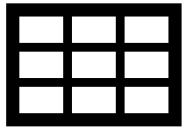
Systems

Criminals want *access* to computers and servers in order to launch scams and attacks on other organizations



Money

Nothing shocking here – looking for quick cash transfers



Data

Standard information like medical records, credit numbers have commodity pricing information on the black market. $x/record

Information

Criminals might want damaging information or internal communications to use against your mission

THREATS

Criminals

Staff

Adversaries

Systems

Most Common Threats

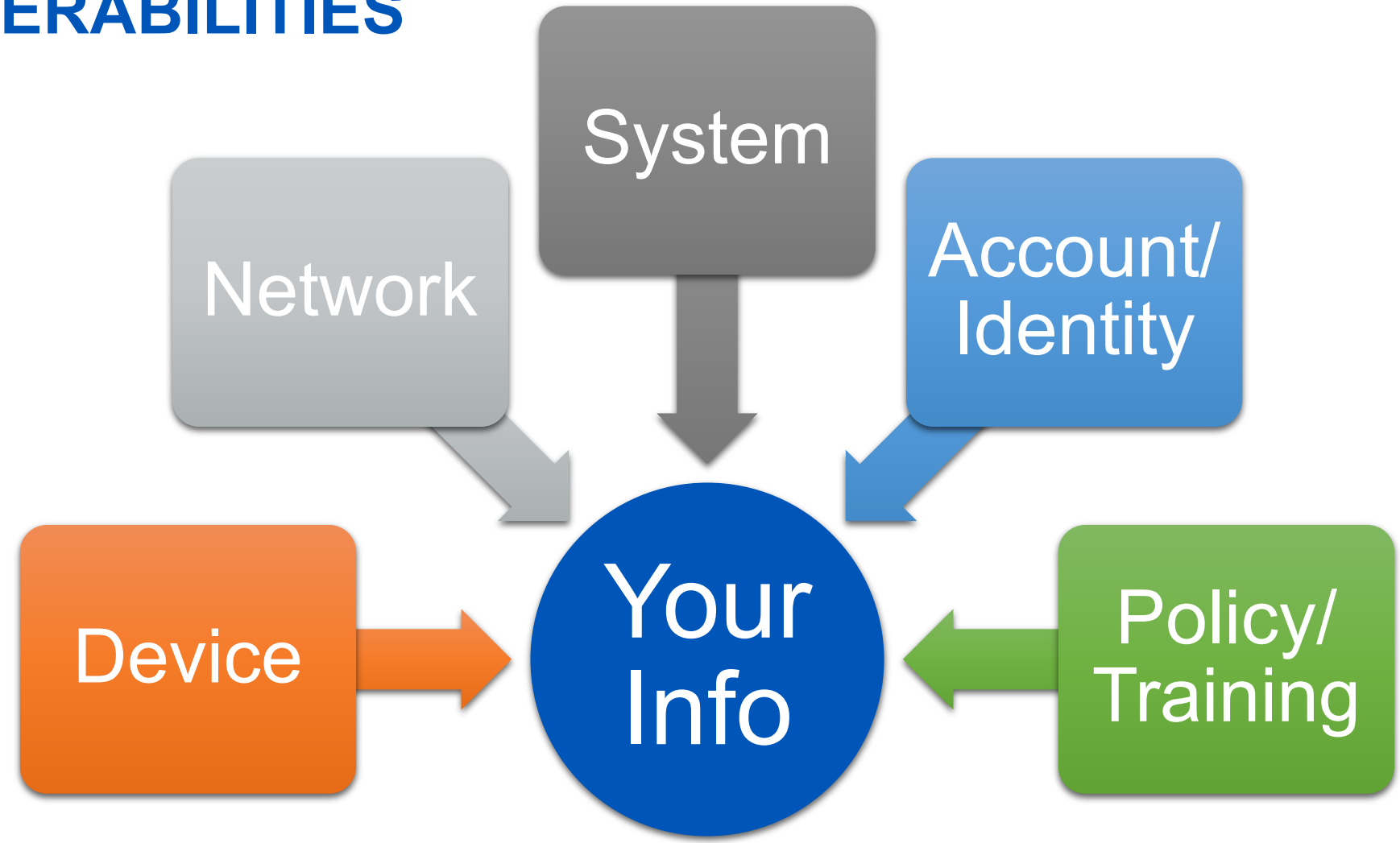
- Phishing to make money
- Stealing account credentials
- Device/Network compromise

Protecting against these is a matter of making it harder for the attacker to get in. They often go after someone else

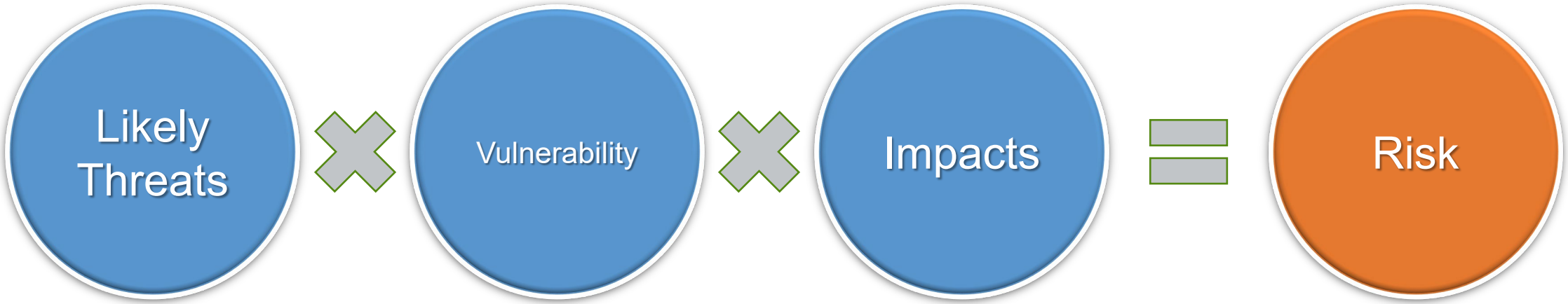
Targeted Threats

- Espionage and/or damaging reputation.
- Reducing risk is difficult requiring more protections, monitoring and expense
- Protecting against government actors is even harder because you often can’t use cloud-based services.

VULNERABILITIES



RISK



WHO?
HOW?
WHY?

PEOPLE
SYSTEMS
PROCESSES

Data Loss
Financial Loss
Reputation Loss
Business Interuption

Cybersecurity risks relate to the **loss of confidentiality, integrity, or availability of information, data, or information (or control) systems** and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. Cyber insurance companies calculate this with numeric values.

BUSINES IMPACT ANALYSIS

Threat	Probability	Impact	Action
Network penetration	LOW	HIGH	Invest in firewall/VPN
Donor record breach	LOW	HIGH	Review SF permissions
User credentials stolen	MED	HIGH	User training, policy, MFA, system credential review
Weather event	MED	LOW	Services delivered remotely

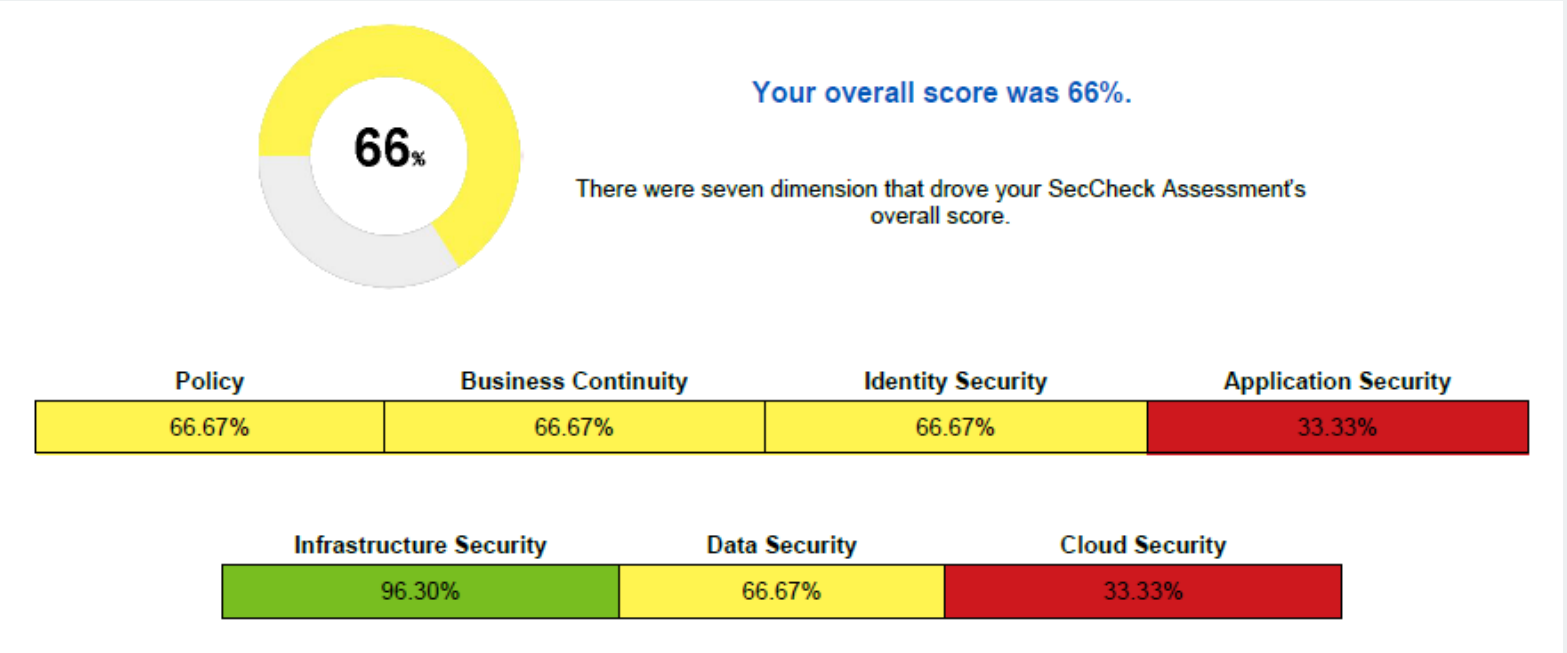
Example: local office has server with client files shared to office workers and remote workers. Email is in Google or Microsoft 365. Donor information is in Salesforce

LET'S ANSWER SOME QUESTIONS!

TECHIMPACT®

Reducing Risk

ASSESSING RISK



- Full Cyber Security Risk Assessment – using NIST guidelines
- Targeted Assessment – focused on common threat vectors and vulnerabilities
- Penetration Testing – network and website
- Testing Users – through simulated phishing campaigns

TECHIMPACT®

Close Vulnerability Gaps

Devices	• Updated & Patched Operating Systems • Antivirus/Antimalware • Mobile Device Management (MDM)
Network	• Updated Firewall including home network • Secure Wireless
Systems	• Cloud System BAA • On-premise systems secured • Data Loss Prevention (DLP)
Account/Identity	• Individual accounts • Strong password policy • Multifactor Authentication (MFA)
Policy/Training	• Computer Use Policy • Cyber awareness training/testing

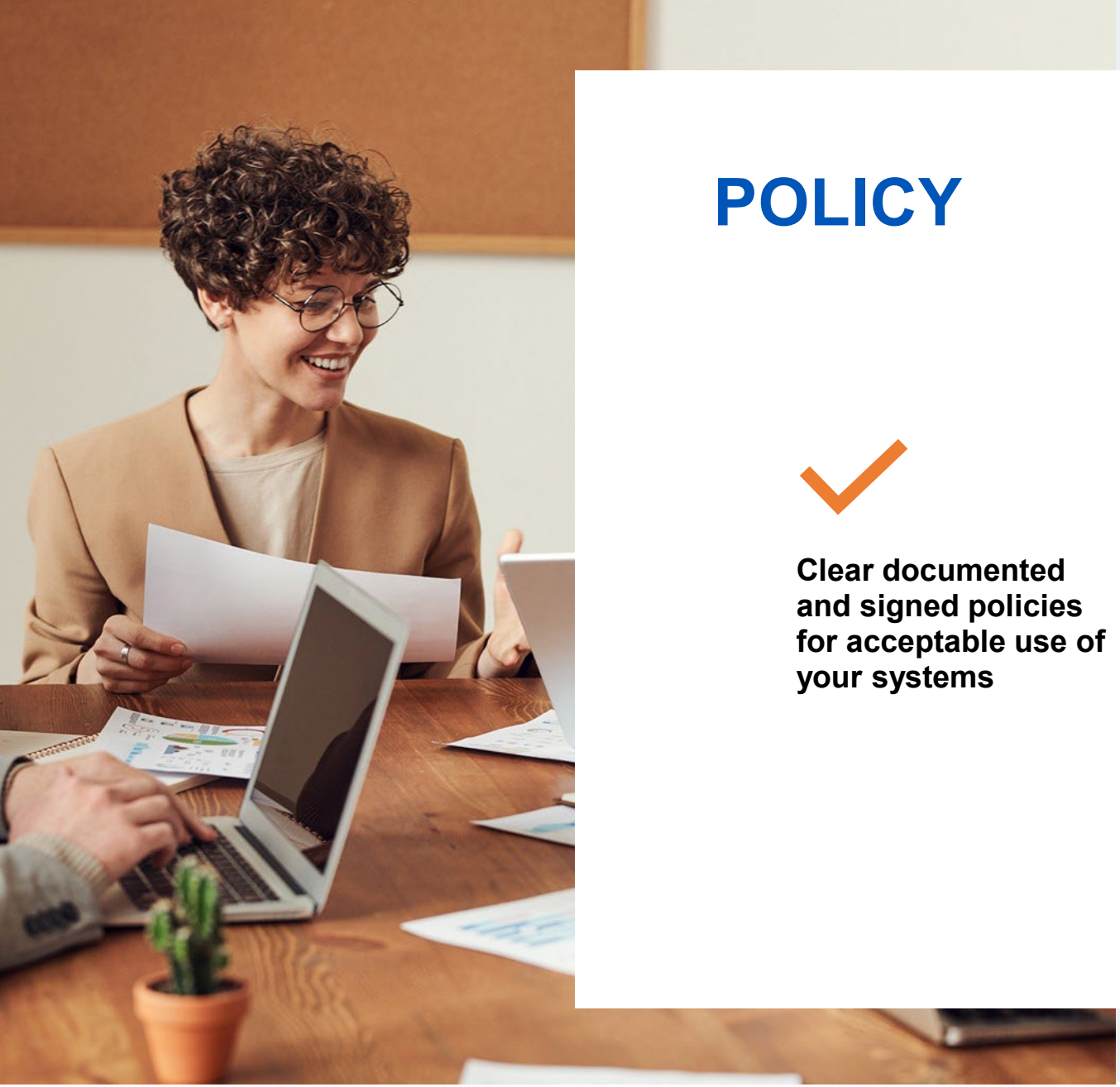
TECHIMPACT®

RISK vs PROTECTION

- Perfect security isn’t possible
- Maximum security keeps more bad actors out but makes it harder for users to work efficiently

Key Recommendations

1	“Quick wins” Do these first Fast Enablement Minimum user impact and cost	1. Create/Update Computer Policy 2. Provide user training/testing 3. Update software, and keep it updated 4. Block access to known-dangerous sites
2	Do these next Base protections Moderate user impact and cost	1. Protect all accounts with MFA 2. Use a password manager 3. Encrypt devices 4. Fully manage your devices
3	Do these last Best protections Additional investments required	1. Know who is doing what in your systems 2. Monitor and proactively prevent data loss 3. Protect network traffic



POLICY

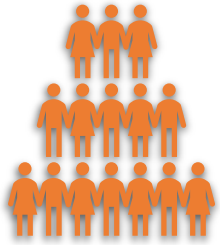
Clear documented and signed policies for acceptable use of your systems

Clearly documented and communicated methods for storing, sharing, and taking home information

Educate your staff about how they are *supposed* to work

Protect yourself in case of dispute

AWARENESS



The *culture* of security in your organization

Are people likely to think about security before taking action?

Know there are **consequences** to poor security practices

Trust that you care more about them **getting work done** than fear mongering

Have **usable** tools to be secure

USER EDUCATION

- Regular security briefs and educational content – threats are always changing
- Educate – use KnowBe4 to simulate phishing attacks and provide education. Will protect organization but extra benefit to protect employee personal information.
- Accountability – keep users accountable

TECHIMPACT®

SOFTWARE UPDATE & ANTIVIRUS

- Use a centralized tool to check for and apply software updates to all of your PCs
- Use a centralized tool to check for and enforce the presence of up-to-date antivirus tooling on all PCs
- Have policies requiring staff to apply updates / restart PCs when prompted

Examples of RMM tools include Kaseya, Solar Windows, Comodo, AutoTask

Windows Defender

WEBROOT SecureAnywhere®

Symantec™ Endpoint Protection

PASSWORD PRACTICES

01

Make passwords as long as possible: 20+ characters

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

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

TECHNOLOGY MITIGATIONS

Helpful where policy is difficult to apply and/or follow (protecting against technical external attacks)

Enforces policy and culture and provides feedback about what is working and what isn't

Gives staff tools to **enable** then to do what is right (send data securely, store safely, etc)

Not a panacea, but a *safety net*

MOBILE DEVICE MANAGEMENT

- Enrolled devices have configuration policies applied
- View compliance with your policies using Compliance policies
- Remote wipe
- Device geolocation
- Allow users to enroll personal devices, preferably at the application level

LET'S ANSWER SOME QUESTIONS!

TECHIMPACT®

Recovering After Event

Bad News – 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
- Follow the Plan – know what to do, how to communicate
- Recover Losses – invoke your insurance plan

TECHIMPACT®

Basic Costs of a Data Breach:

Stopping and recovering from a breach starts with basic tech services which can add up to thousands of dollars:

- Investigation
- Workstation recovery
- Network recovery
- Server recovery
- User credential recovery
- Data recovery and restore

Source: Tech Impact

Additional Costs of a Data Breach:

In addition to IT recovery costs, the average per lost record cost is estimated at $221. Costs may include:

- legal guidance
- breach notification
- forensics
- credit monitoring

*Source: Ponemon Institute 2018 Cost of Data Breach Study (*www.ibm.com/downloads/cas/861MNWN2**)**

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 (*www.ibm.com/downloads/cas/861MNWN2**)**

Data Backup & Recovery

Scheduled and Automated

Offsite

Tested

Data Events are going to happen
Make sure that you can recover!

Different Levels of Cyber Insurance Coverage

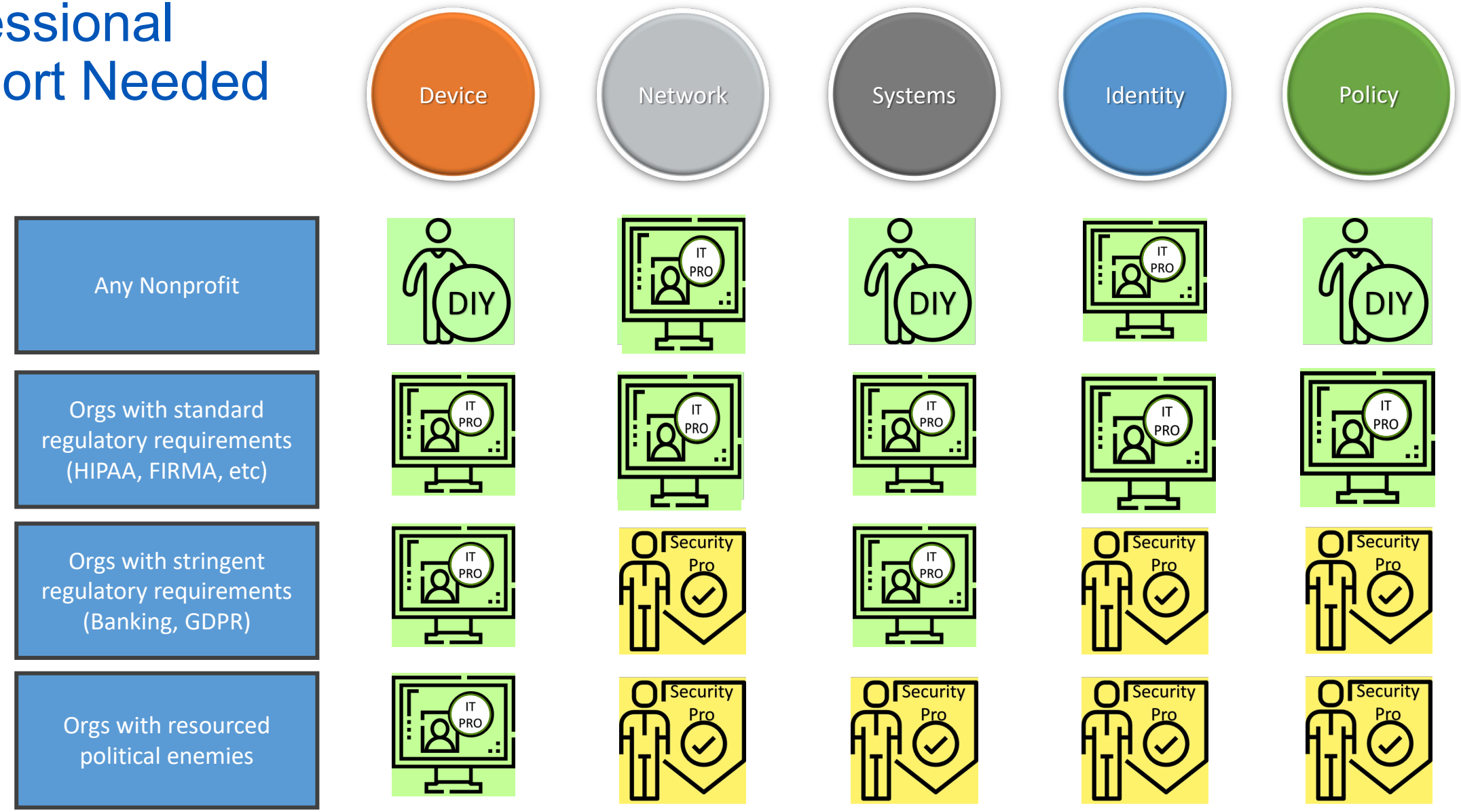
First-party data breach insurance provisions include:

- Data breach investigation costs
- Hardware and software damage costs
- Fines incurred by lost data
- Lost revenue

Third-party data breach insurance provisions include:

- Lawsuits from individuals due to data loss
- Fees incurred for aiding individuals in the event of data loss

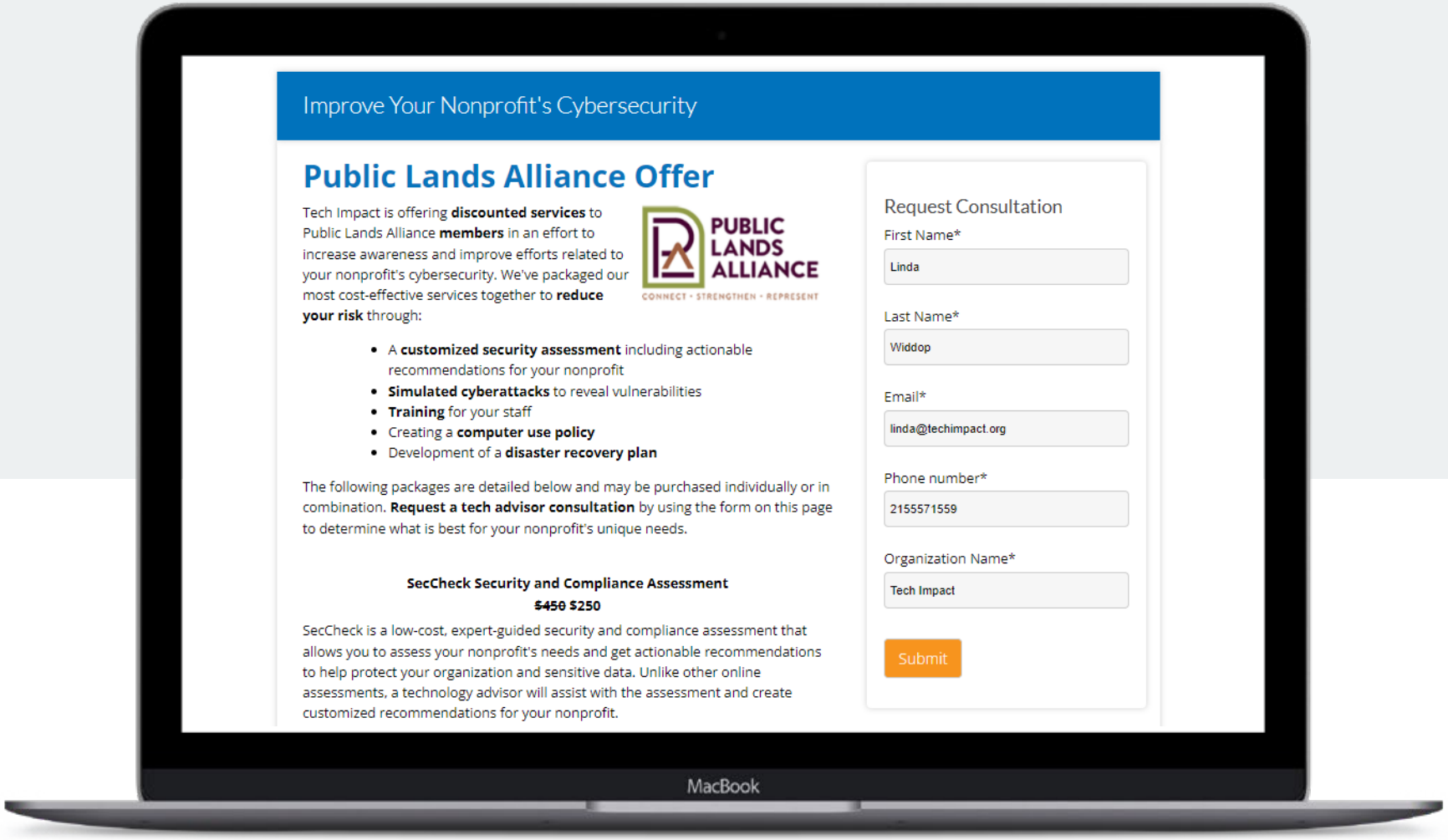
Levels of Professional Support Needed



Cyber Security Services

Special Offers for Public Lands Alliance Members

[Public Lands Alliance Member Request for Cybersecurity Consult (techimpact.org)]



TECHIMPACT®

SPECIAL OFFER SERVICES

Assessment $500	• SecCheck® assessment • Network Scan
Policy $250	• PolicyBuilder® • Disaster Recovery Plan
Awareness $2/license	• KnowBe4 Training

TECHIMPACT®

LET'S ANSWER SOME QUESTIONS!

TECHIMPACT®

THANK YOU

Let’s keep the criminals out and the data safe!

TECHIMPACT®

LINDA WIDDOP

Managing Director of Client Solutions

I manage all aspects of client relations for Tech Impact including educating nonprofits about technology solutions. I work with local, regional and national partners to provide the nonprofit community with increased knowledge of technology through speaking engagements.

Contact: linda@techimpact.org