Cybersecurity Essentials for Ops

Cybersecurity: 201

CommunityIT Innovators®
where technology meets mission

Hartford Foundation
FOR PUBLIC GIVING

About Community IT

100% Employee Owned

Advancing mission through the effective use of technology.

Channel Futures.
Leading Channel Partners Forward
MSP 501
2021 WINNER

PRESENTER

Matthew Eshleman
CTO

Poll – Org Size

How many staff to do you have

- 1-10
- 11-29
- 30-50
- 50+

Poll – Role with IT

What is your role at the organization?

- End User
- I am the IT person
- I manage our IT function

Agenda

- Cybersecurity Landscape
- Cybersecurity Playbook
- Putting it into Action

IC3 Complaint Statistics

Last Five Years

2,211,396 TOTAL COMPLAINTS

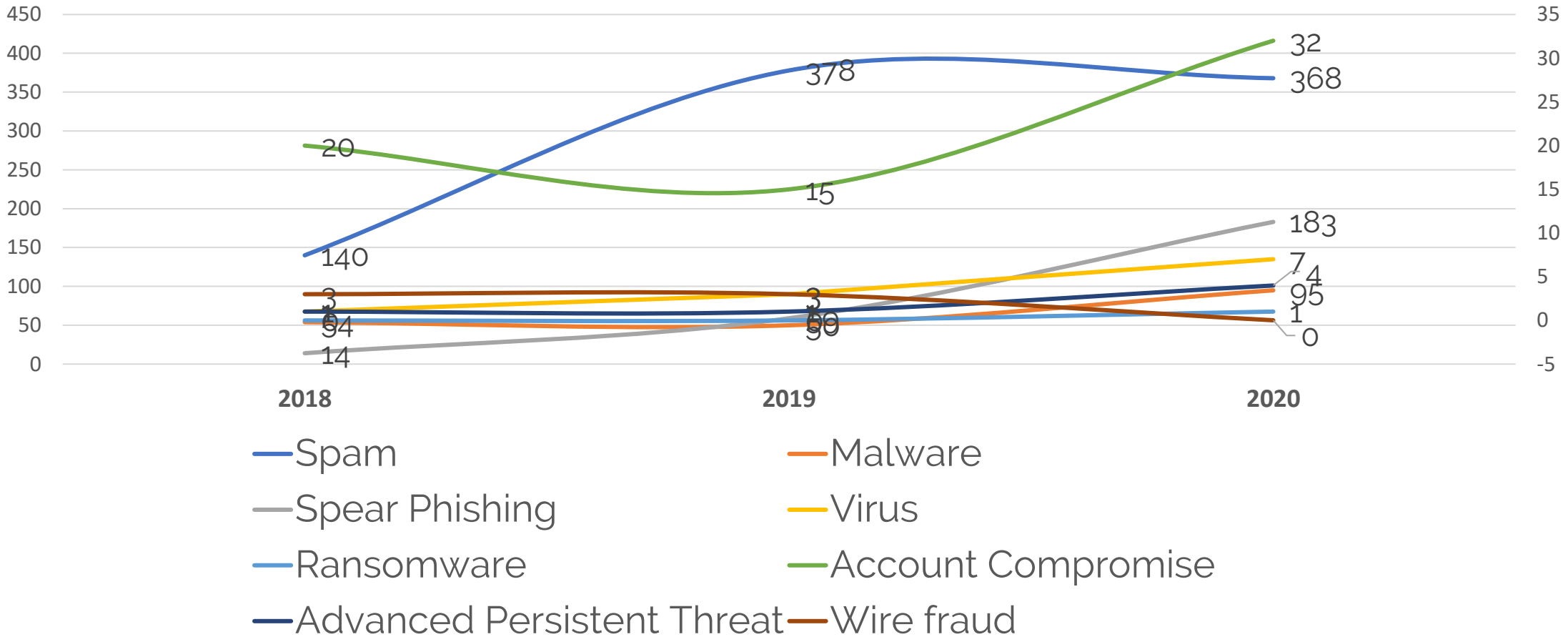
*$13.3 Billion TOTAL LOSSES**

(Rounded to the nearest million)

State of Nonprofit Cybersecurity

- 60 percent of organizations either did not know or don't have a policy in place that would identify how they would handle risk, equipment usage and data privacy.
- 74 percent of organizations have not implemented Multi-Factor Authentication.
- 46 percent reported that they used unsecured wireless and Bluetooth devices.
- 92 percent reported that staff could access org email, files and information systems from personal devices.

Nonprofit Cybersecurity Incidents



Cybersecurity - Adversaries

HOW MUCH IS BUSINESS DATA WORTH TO BAD ACTORS?

6 BILLION DIGITAL RECORDS EXPOSED IN 2018

43% OF ALL BREACHES INVOLVED SMB VICTIMS

CREDIT CARD INFO
$2-$5 (per record)

CUSTOMER PII
$20-$450 (per record)

EMPLOYEE PII
$20-$450 (per record)

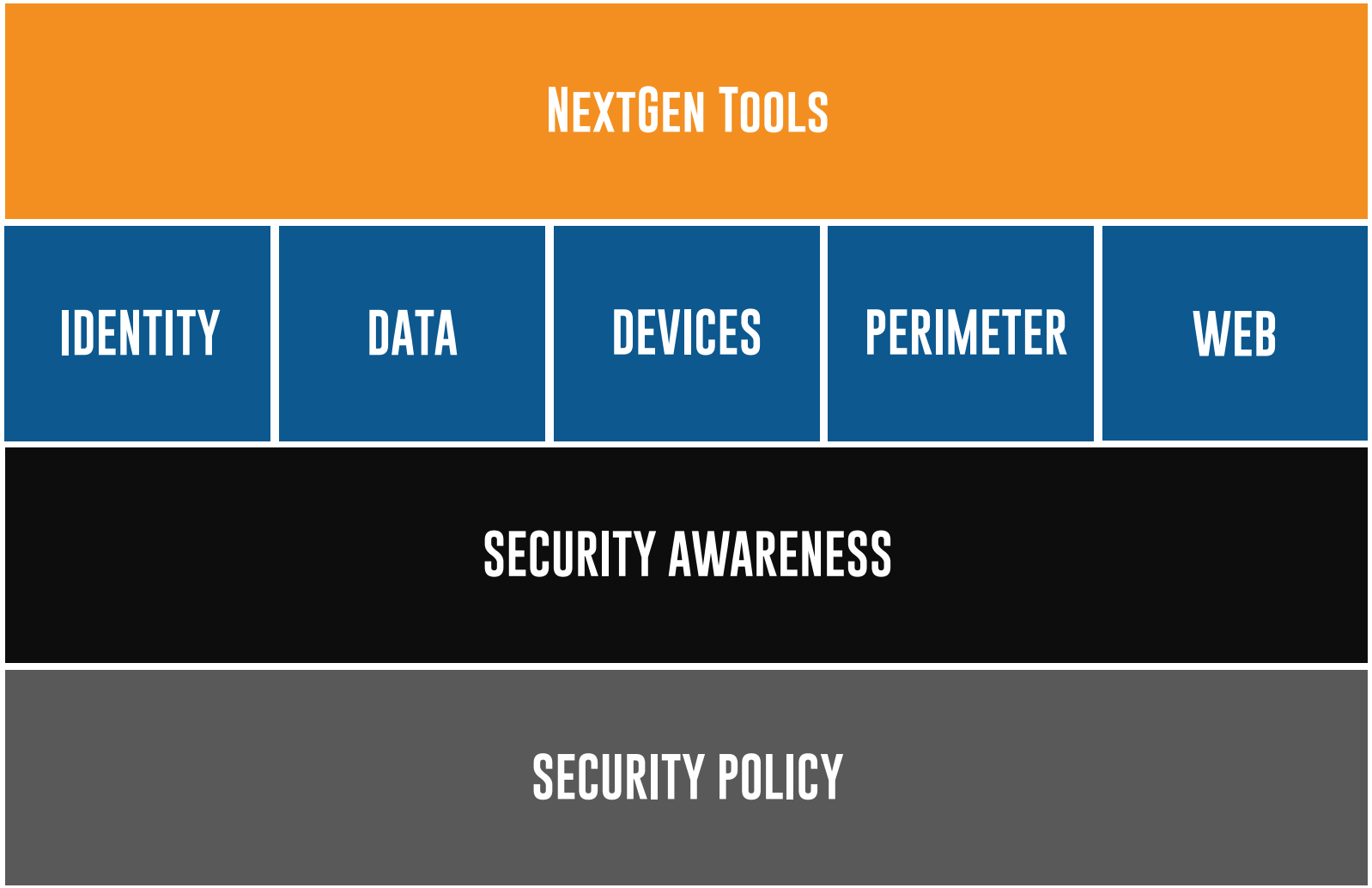
MEDICAL RECORDS
$20-$50 (per record)

SALES/FINANCIAL INFO
Competitive Value

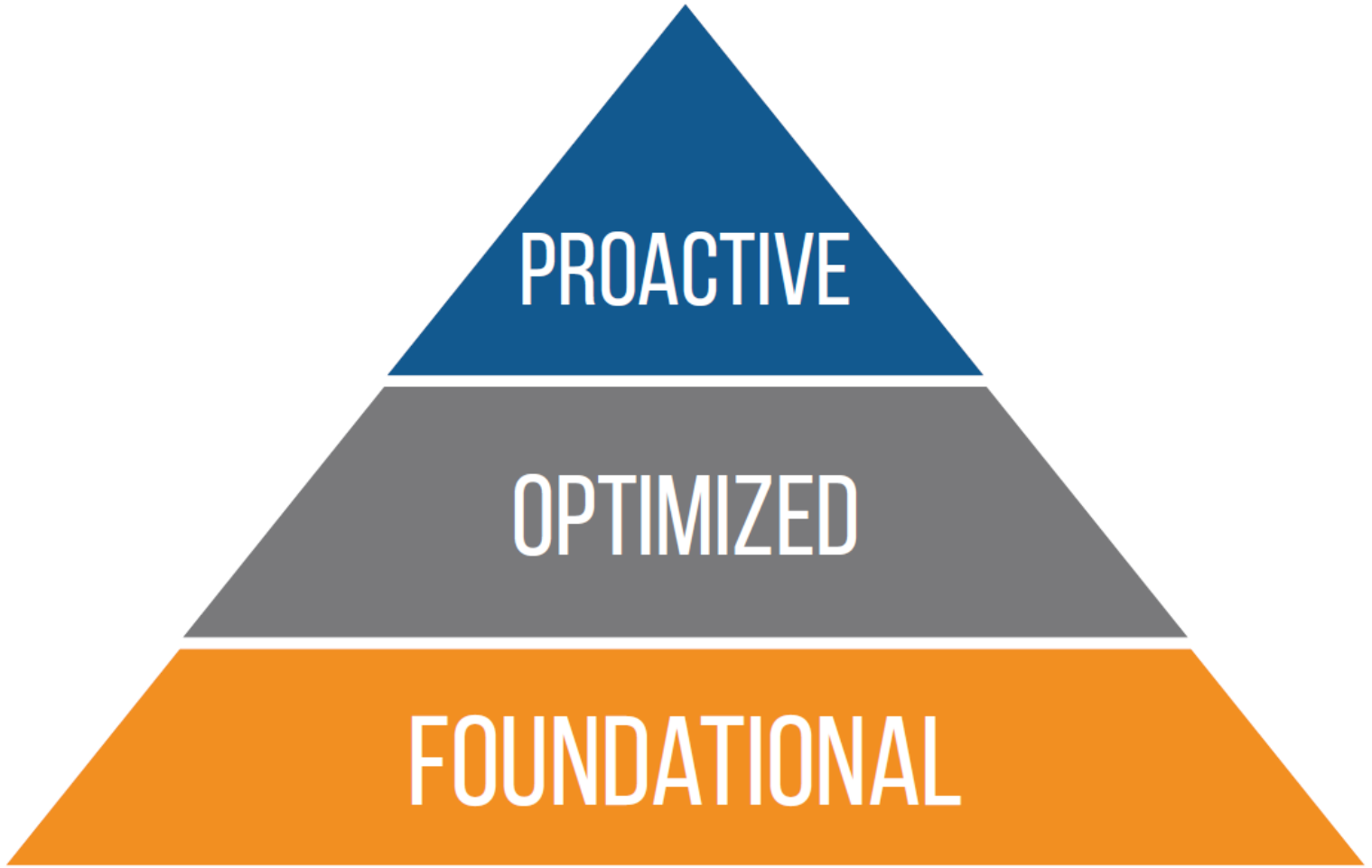
PROPRIETARY INFO
Competitive Value

Per the Verizon Data Breach Investigation Report
Estimated data values from Sociable

OUR APPROACH TO CYBERSECURITY



Cybersecurity Controls



CommunityIT Innovators®

QUESTION

- Does your organization have a formal budget for IT and Cybersecurity
  - Ad Hoc Budgeting
  - We budget for IT only
  - We budget for IT and cybersecurity
  - Holistic and strategic multi-year budgeting

Budget

- To help provide some context to these recommendations we've assigned a scale from $-$$$$.
- These costs for what a 25-person organization would incur over the course of a year.

$	$0-$2,000
$$	$2,000-$8,000
$$$	$8,000-$15,000
$$$$	$15,000+

Foundational

Policy

- IT Acceptable Use
- Data Privacy
- Incident Response
- Insurance Review

Security Awareness

- Free or ad hoc Staff training

IT Acceptable Use

- Includes overview of technology use at the Organization
- Incorporates a list of information systems
- Establishes basics of password and access
- Defines some data retention guidelines

Free IT Training Resources

- Stop Think Connect
  - www.stopthinkconnect.org
- Community IT
  - www.communityit.com/resources
  - www.youtube.com/CommunityIT

Foundational

Technology Controls

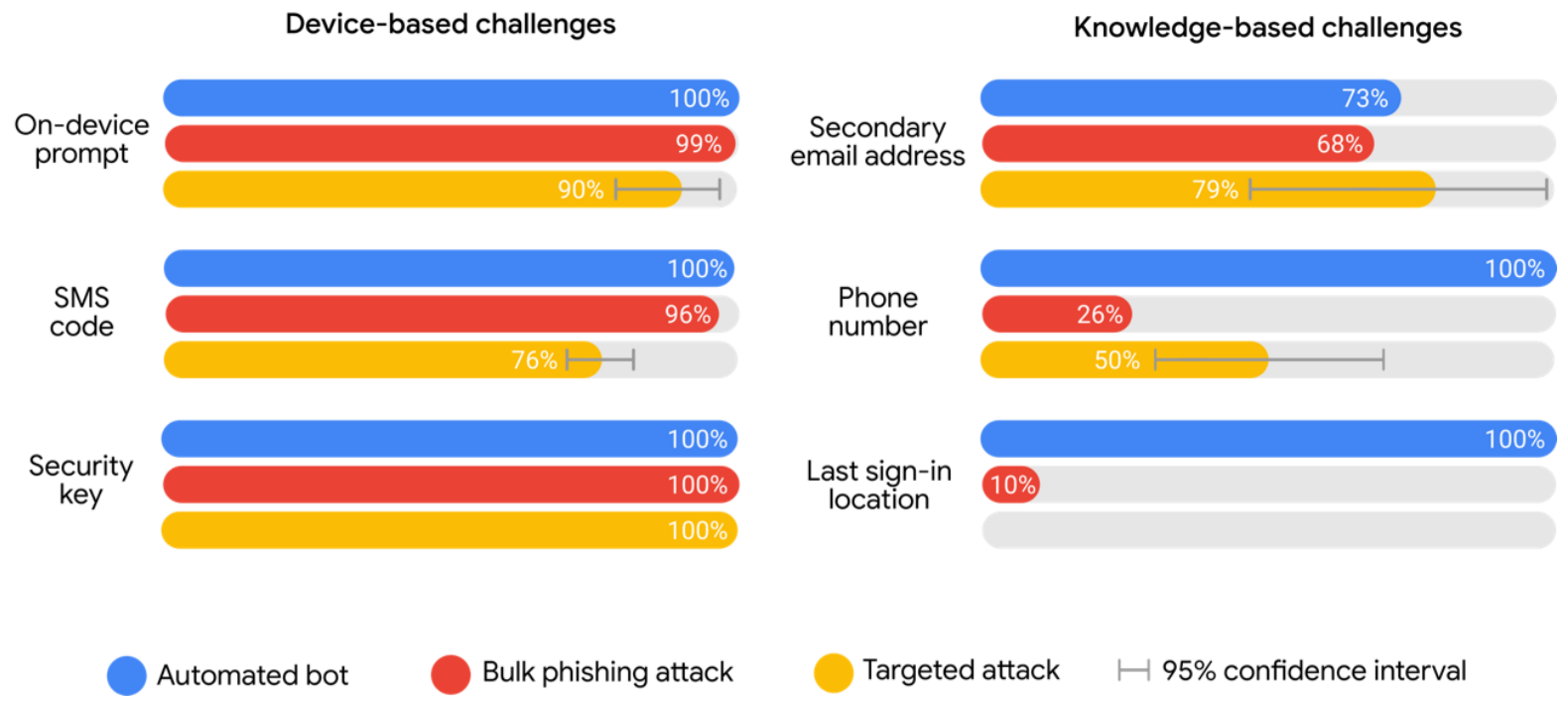
- Multi Factor Authentication
- Password Manager
- Backups
- OS and Third-Party Updates
- Antivirus
- Spam Filtering
- Business Email Compromise Protection
- Website protection

Poll – Foundational IT Controls

- We've implemented the following controls at our org:
  - Multi Factor Authentication
  - Password Manager
  - Backups
  - OS and Third-Party Updates
  - Antivirus
  - Spam Filtering
  - Business Email Compromise Protection
  - Website protection

MFA is Effective

Account takeover prevention rates, by challenge type



Business Email Compromise

Proactive

Policy

- Risk Assessment
- Cyber liability insurance
- BYOD Policy

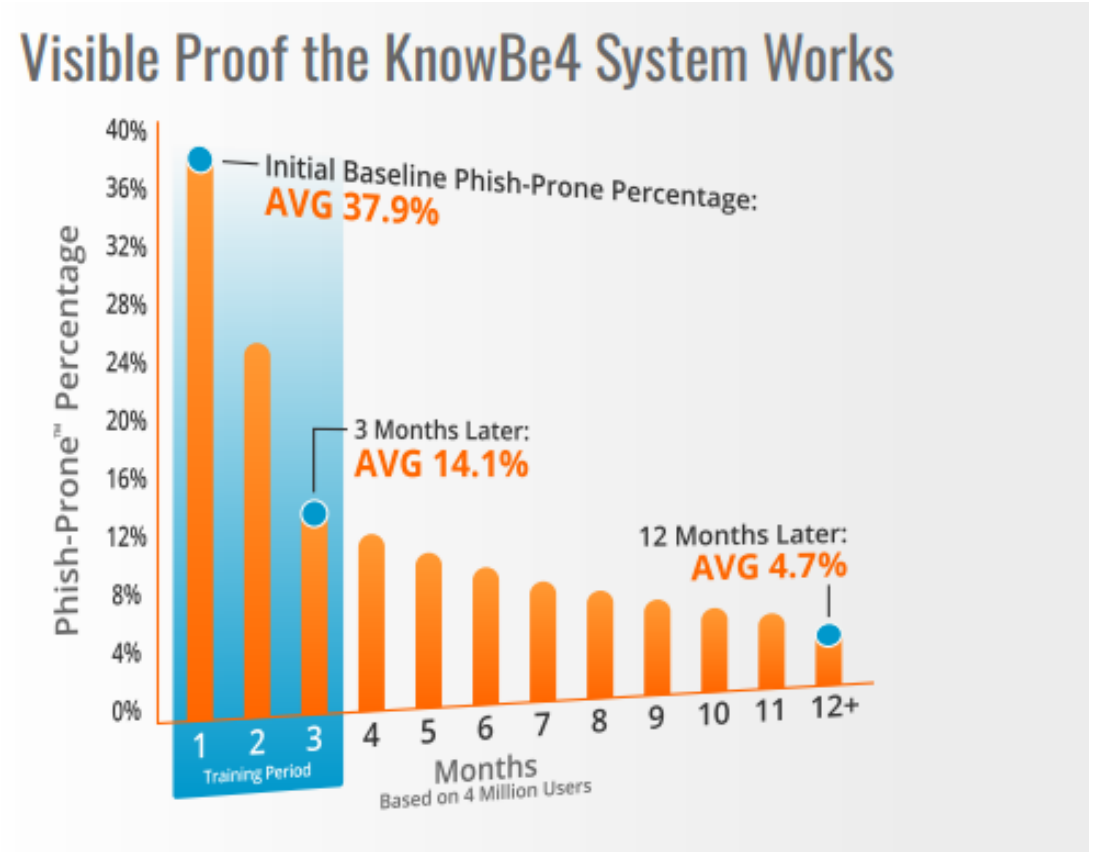
Security Awareness

- Formal LMS system

Cybersecurity Awareness

SMB Nonprofits (1-249 employees)

- Phase 1 (Initial baseline results) – **39.4%**
- Phase 2 (90 days after initial training) – **14.9%**
- Phase 3 (1 year into training program) – **4.8%**



NIST 800-53

- NIST is one cybersecurity framework
- Developed for Federal Agencies & Contractors
- 1683 line spreadsheet of controls

IDENTIFY

- ASSET MANAGEMENT
- BUSINESS ENVIRONMENT
- GOVERNANCE
- RISK ASSESSMENT
- RISK MANAGEMENT STRATEGY

PROTECT

- ACCESS CONTROL
- AWARENESS & TRAINING
- DATA SECURITY
- INFO PROTECTION PROCESS & PROCEDURES
- MAINTENANCE
- PROTECTIVE TECHNOLOGY

DETECT

- ANOMALIES & EVENTS
- SECURITY CONTINUOUS MONITORING
- DETECTION PROCESSES

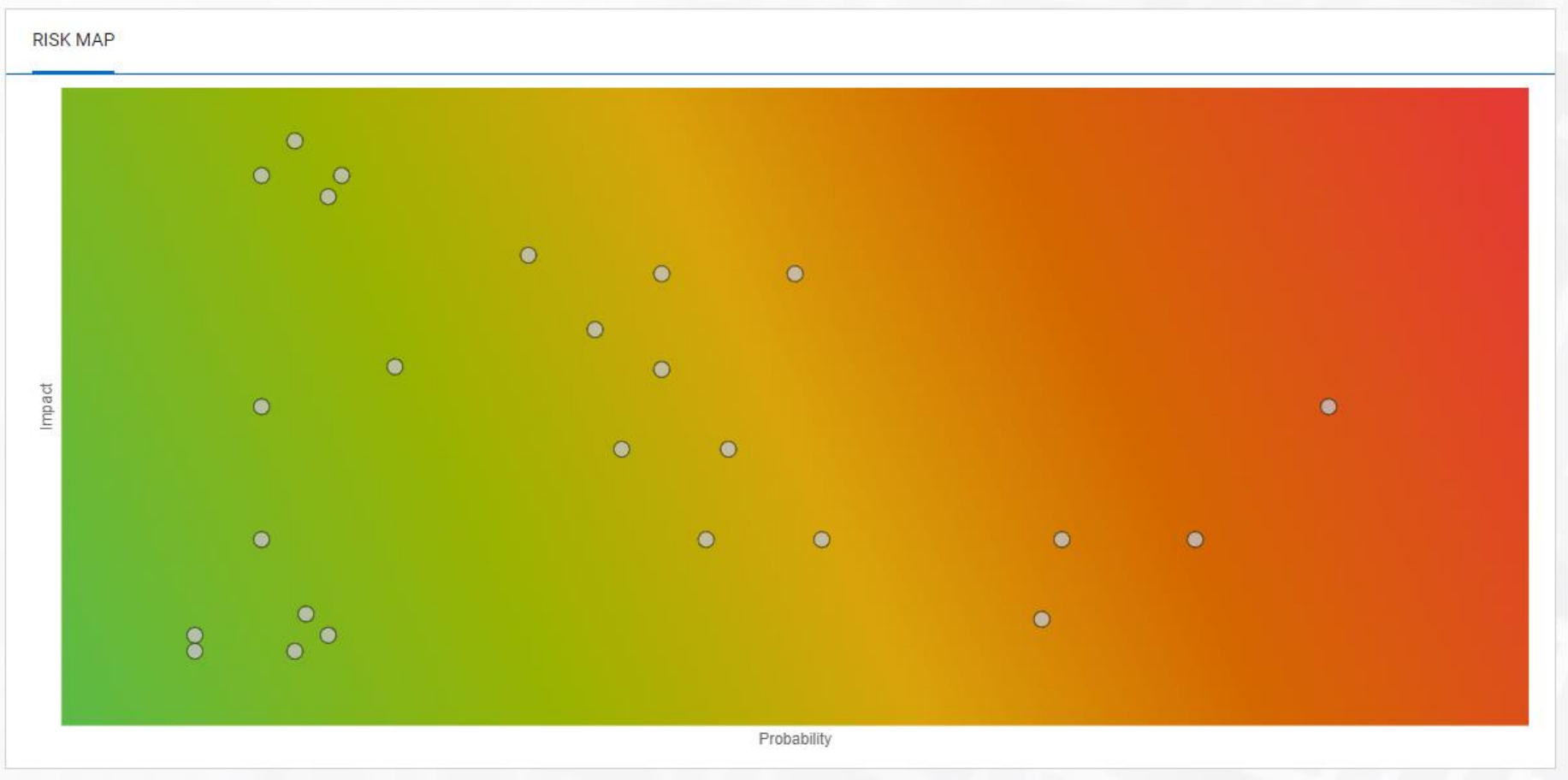
RESPOND

- RESPONSE PLANNING
- COMMUNICATIONS
- ANALYSIS
- MITIGATION
- IMPROVEMENTS

RECOVER

- RECOVERY PLANNING
- IMPROVEMENTS
- COMMUNICATIONS

RISK MAP



Prioritized Recommendations

TOP RISK AREAS

PR.AT-1: All users are informed and trained	Critical
ID.RA-3: Threats, both internal and external, are identified ...	Critical
ID.RA-1: Asset vulnerabilities are identified and documented	High
DE.CM-3: Personnel activity is monitored to detect potential ...	High
ID.RA-2: Threat and vulnerability information is received fro...	High

POLL – Cybersecurity Insurance

- Does your organization have Cyberliablity Insurance?
  - No, doesn't apply to us
  - Not yet, working on our application now
  - Yes, for a year
  - Yes, have had it in place for several years

Cyberliablity Insurance

- Distinct from existing insurance policies
- Many controls are now required
  - MFA for everything
  - Managed security
  - Encrypted data
  - Vulnerability scanning

Proactive

Technology Controls

- Single Sign on
- Data Management (DLP)
- BIOS / Driver Updates
- BYOD Control
- Device Encryption
- Endpoint Detection and Response
- Web filtering

Poll – Proactive Controls

- We've implemented the following controls (multiple choice)
  - Single Sign On
  - DLP
  - BIOS & Driver updates
  - BYOD Management
  - Device Encryption
  - Endpoint Detection and Response
  - Web filtering
  - None

Optimized

Policy

- Business Continuity

Security Awareness

- Cybersecurity Assessment

Optimized

Technology Controls

- Device Trust / Zero Trust
- CASB / SASE
- Vulnerability Scanning
- Penetration Testing
- SOC / SIEM

Getting Started

There's no one right way

- Bottom up: IT takes ownership and leads the process
- Top down: Executive leadership or the Board mandates changes

Action Steps

- Review your existing controls
- Develop risk profile
- Incorporate cybersecurity into budget planning

Questions?