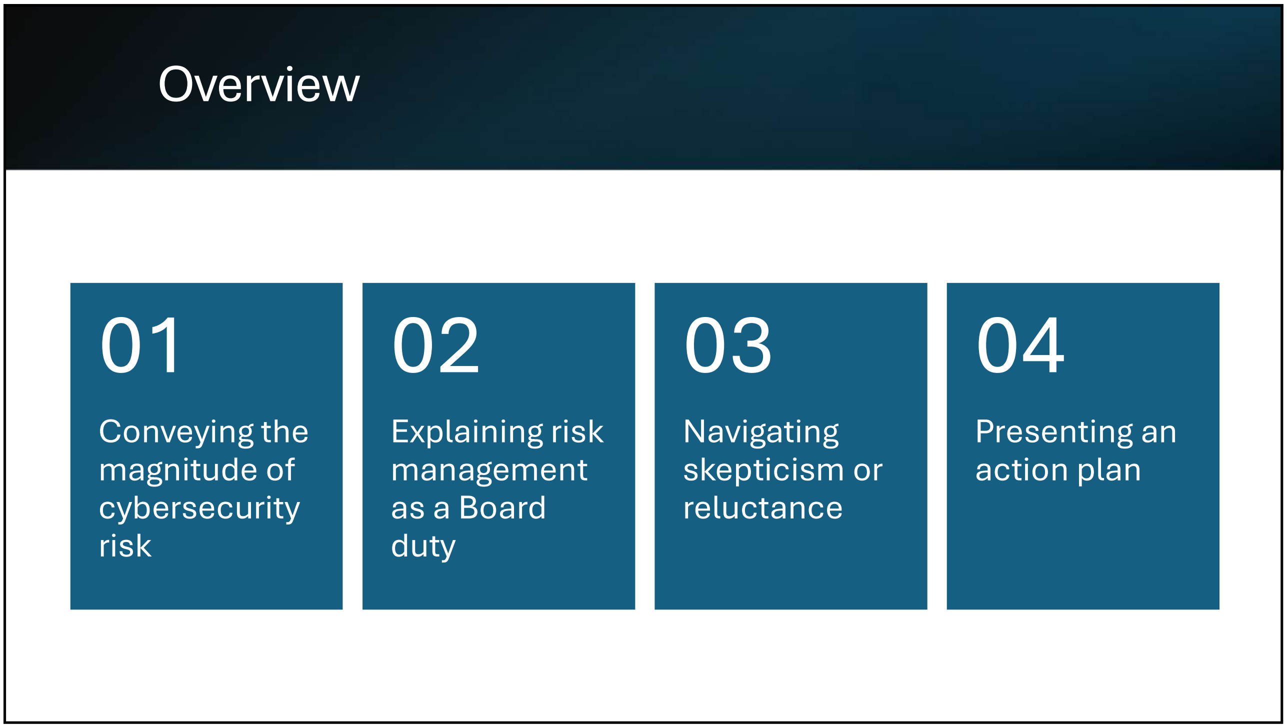
Building Board Support for a Cybersecurity Program

Frank Bulk, Premier Communications
Joshua Seidemann, NTCA-The Rural Broadband Association

CYBERCON IX – May 16, 2024
Des Moines, IA

1



Overview

01 Conveying the magnitude of cybersecurity risk

02 Explaining risk management as a Board duty

03 Navigating skepticism or reluctance

04 Presenting an action plan

2

Current industry environment

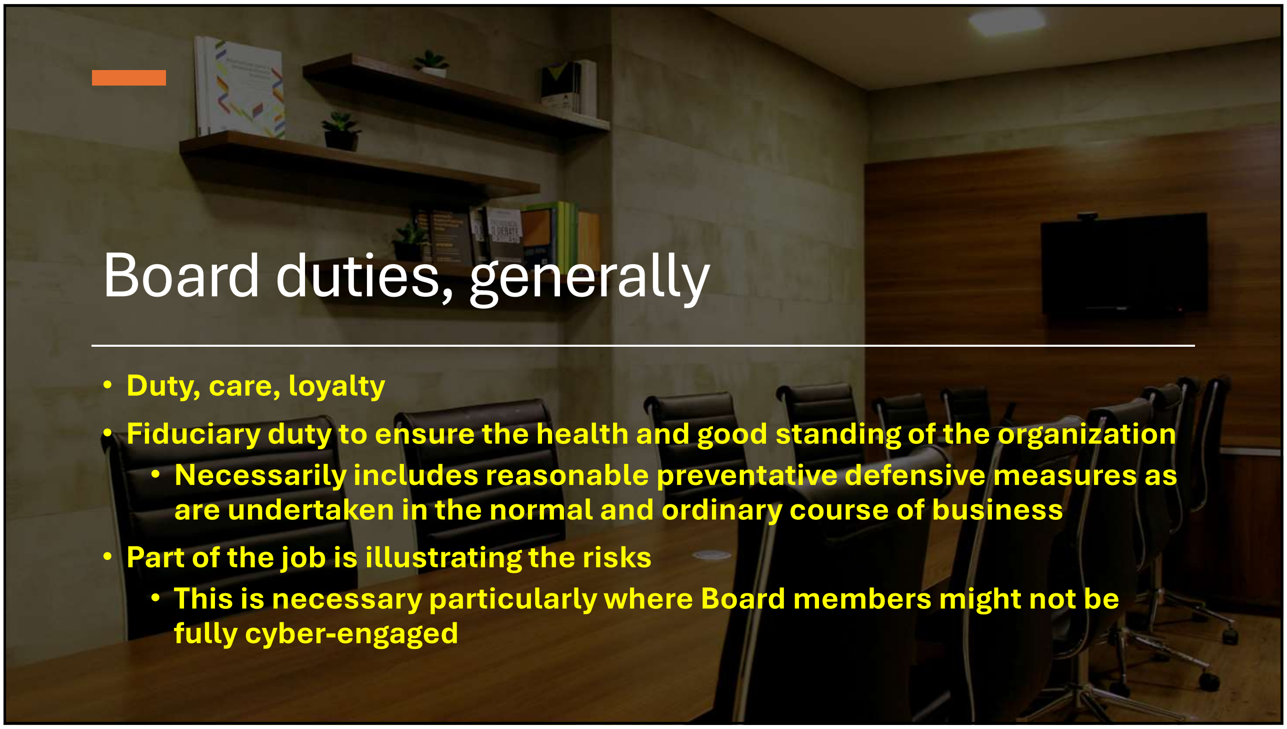
- Cybersecurity risks threaten numerous industry sectors
- No sector is immune from intentional adversarial attack; even “mischief makers” can cause significant harm
- Average impact of data breach for a small business (fewer than 500 employees) is $3.31 million
  - Data breaches can be unintentional, the result of employee carelessness or error

3

Current regulatory environment

- **Even if business does not respond, government is imposing standards**
- **Coordination among Federal agencies**
  - **NIST CSF: Minimum practices – Identify, Protect, Detect, Respond, Recover**
  - **CISA: Target discovery; vulnerability scanning; recommendations**
  - **ICT SCRM Task Force**
- **Will the FCC “get in the game”?**

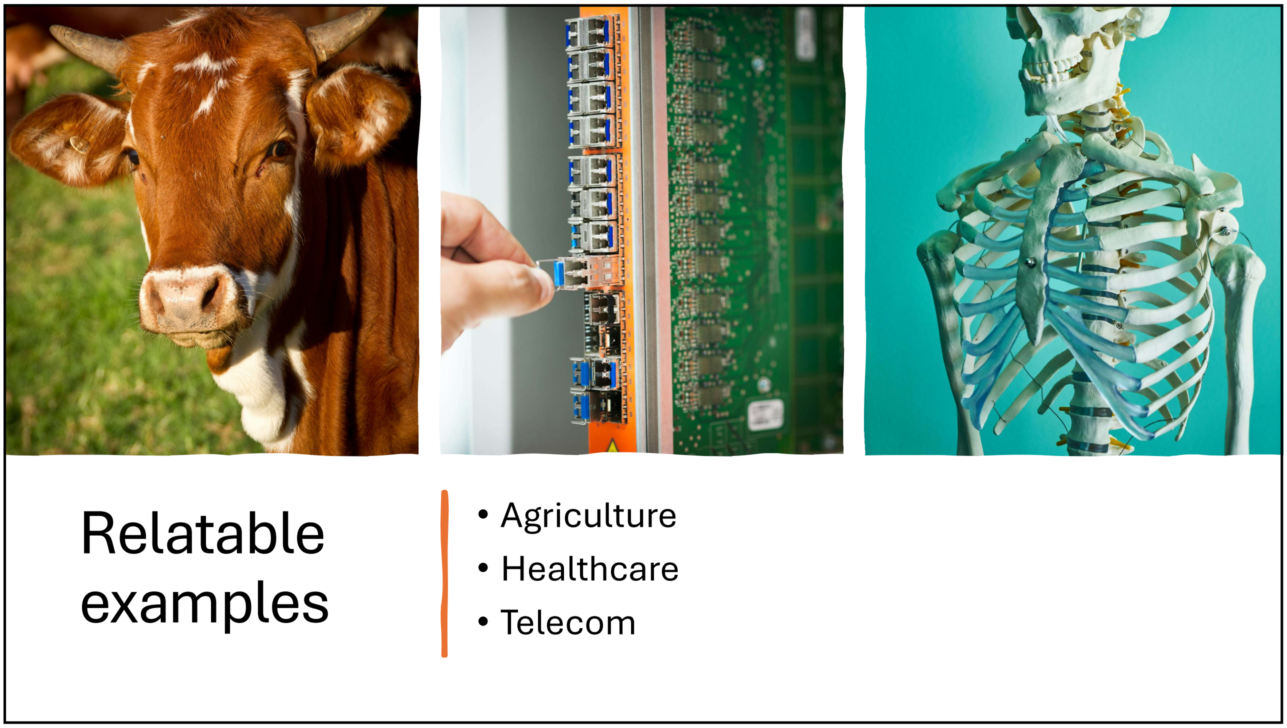
4



Board duties, generally

- Duty, care, loyalty
- Fiduciary duty to ensure the health and good standing of the organization
  - Necessarily includes reasonable preventative defensive measures as are undertaken in the normal and ordinary course of business
- Part of the job is illustrating the risks
  - This is necessary particularly where Board members might not be fully cyber-engaged

5



Relatable examples

- Agriculture
- Healthcare
- Telecom

6

Costs, and cost avoidance

- Businesses may consider that a breach is not a question of “if,” but “when” - and to what extent
- Globally, 48% of small and mid-sized businesses have suffered a cyberattack in the past years
- 73% of small U.S. businesses have reported an attack
    - Even a successfully defended attack is an attack

7

Cybersecurity and business objectives

- First: Protect the fort
- Second: Help others
    - Revenue stream?
    - Community engagement/ goodwill

8

CISA vulnerability scanning (not difficult, but detailed)

- Asset inventory
  - Networks
  - Systems
  - Hosts
- Vulnerability identification
  - Potential vulnerabilities
  - Configuration weaknesses
- Recommendations for enhancement

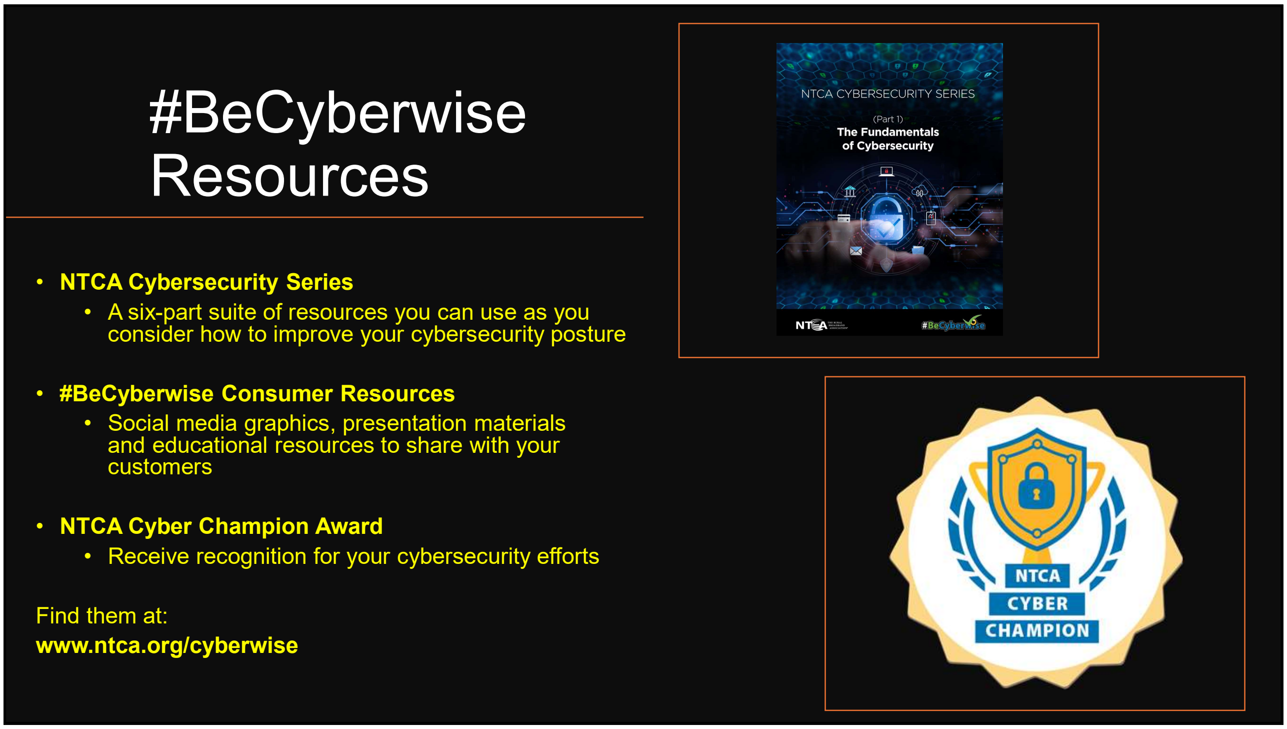
9

CyberShare

The small broadband provider ISAC

- **What:** Cyber threat information sharing forum tailored to small broadband providers
- **Why:** Small providers lack dedicated cyber resources
- **Who:** Small providers
- Includes:
  - Daily report of threat indictors with analysis
  - Weekly technical report
  - Two scheduled calls per month that cover a variety of topics.
  - Secure information portal in which providers may share actionable threat intelligence with other participants and access secure documents.

10



NTCA CYBERSECURITY SERIES
(Part 1)
The Fundamentals of Cybersecurity
NTCA
#BeCyberwise
NTCA
CYBER
CHAMPION

#BeCyberwise Resources

- **NTCA Cybersecurity Series**
  - A six-part suite of resources you can use as you consider how to improve your cybersecurity posture
- **#BeCyberwise Consumer Resources**
  - Social media graphics, presentation materials and educational resources to share with your customers
- **NTCA Cyber Champion Award**
  - Receive recognition for your cybersecurity efforts

Find them at:
www.ntca.org/cyberwise

11

Thank you

12