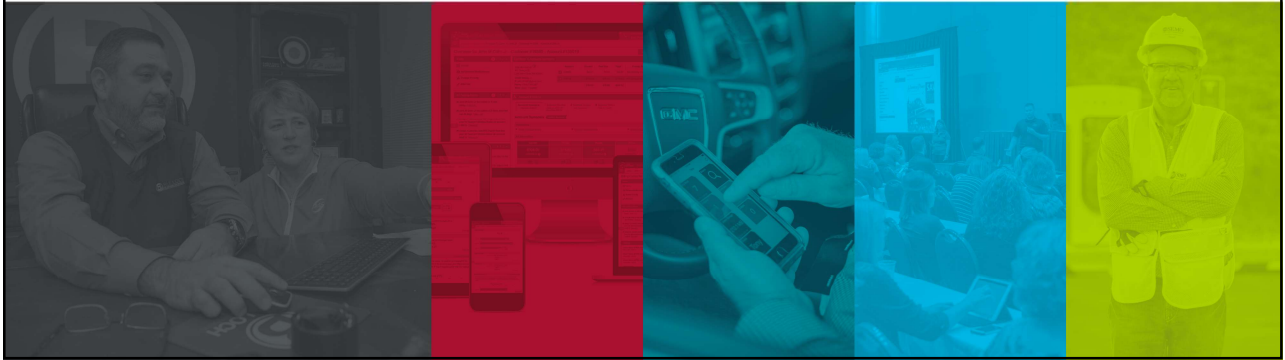


IOWA COMMUNICATION ALLIANCE ANNUAL MEETING
SURVIVING THE GREAT TRANSITION
WHAT'S NEXT?

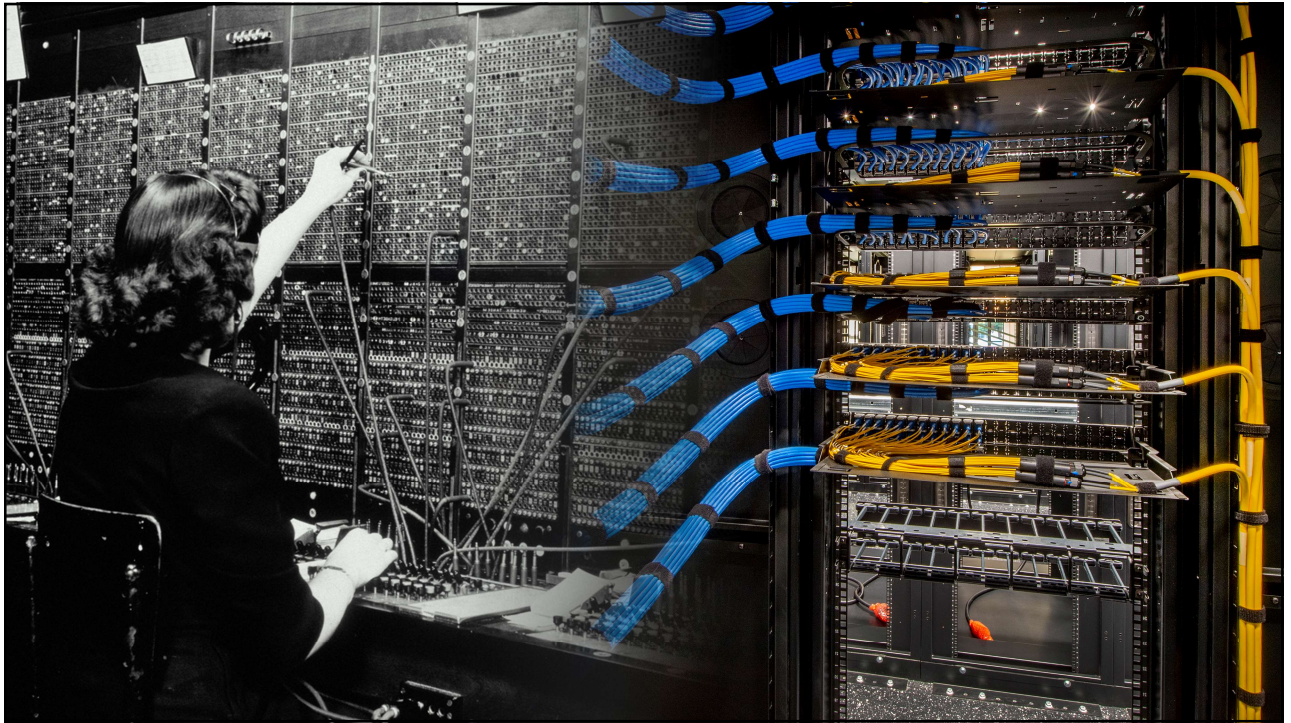


1



ED WOLFF
Chief Member Officer

2

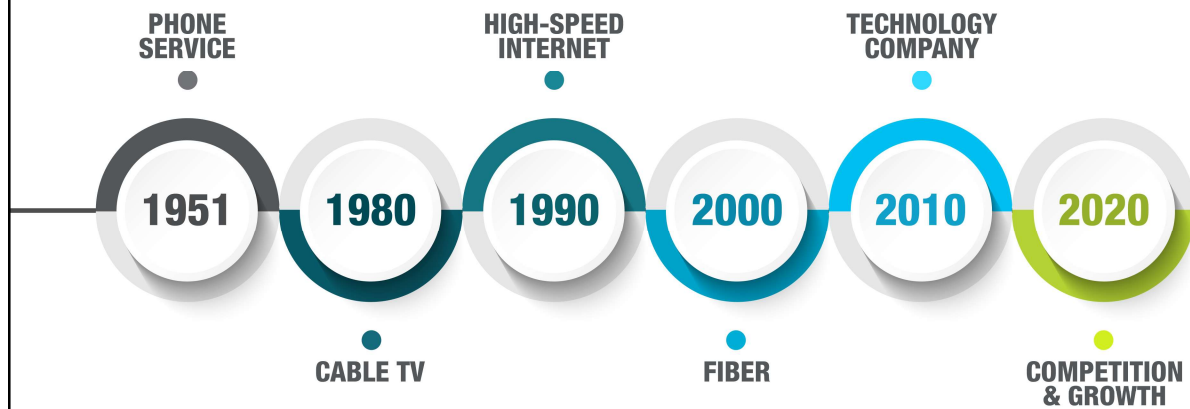


3



4

THE GREAT TRANSITION



5



CULTURE

**CONTINUOUS
IMPROVEMENT**

CYBER AWARENESS

6



7



8



9



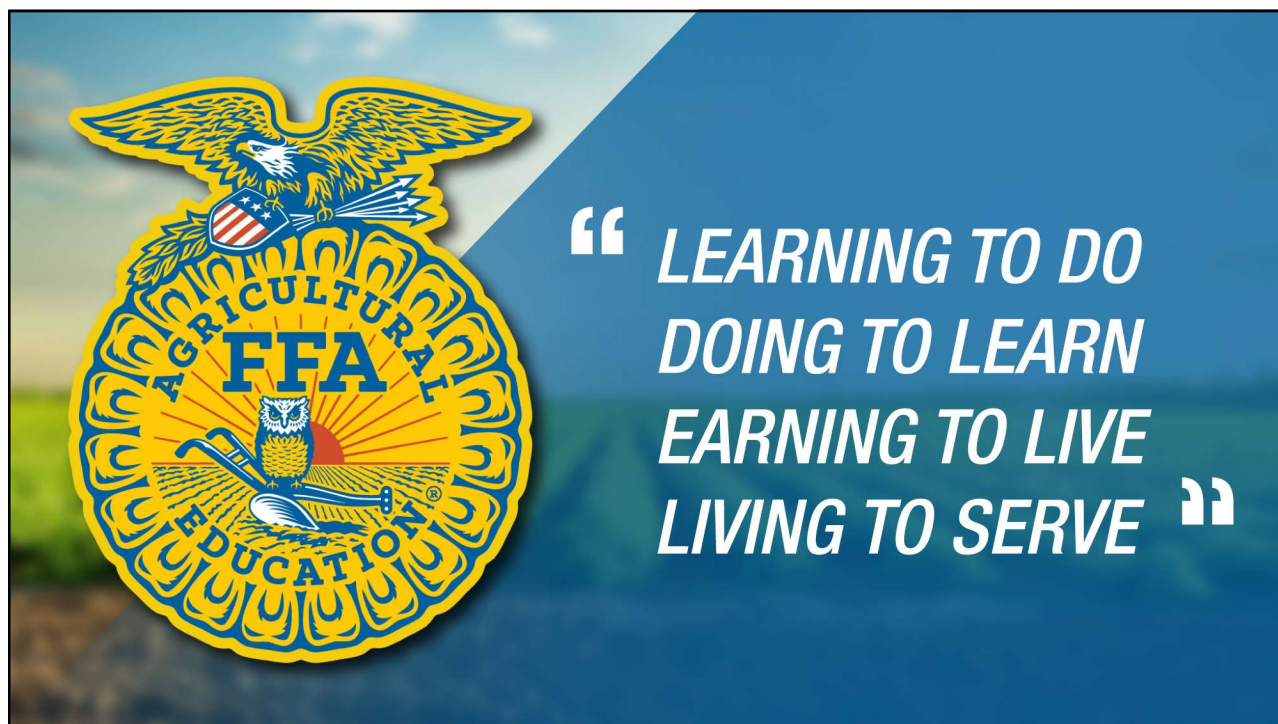
10



11



12



**“ LEARNING TO DO
DOING TO LEARN
EARNING TO LIVE
LIVING TO SERVE ”**

13



THEODORE ROOSEVELT
ROUGH RIDER AWARD:

SISTER THOMAS WELDER

14

“ In a servant leadership culture we learn by choice or example that if we want to be great, we have to serve others respectfully. ”

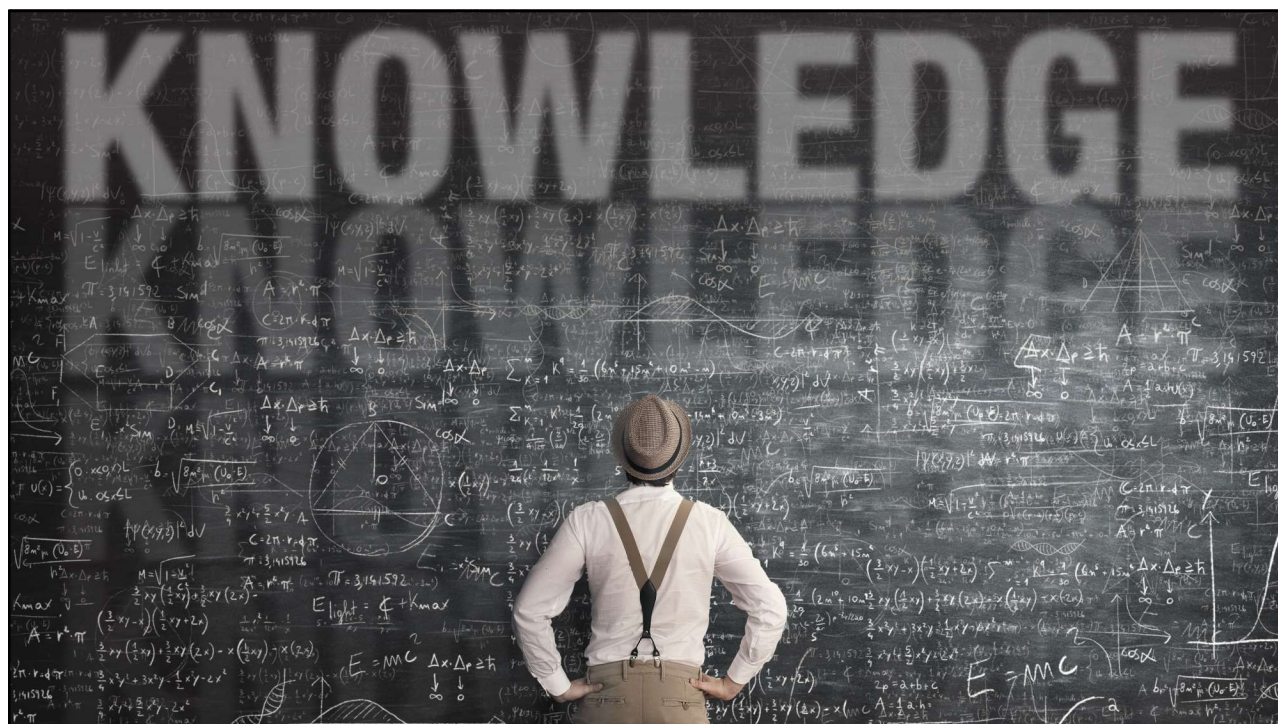
- Vern Dosch, Wired Differently



15



16



17



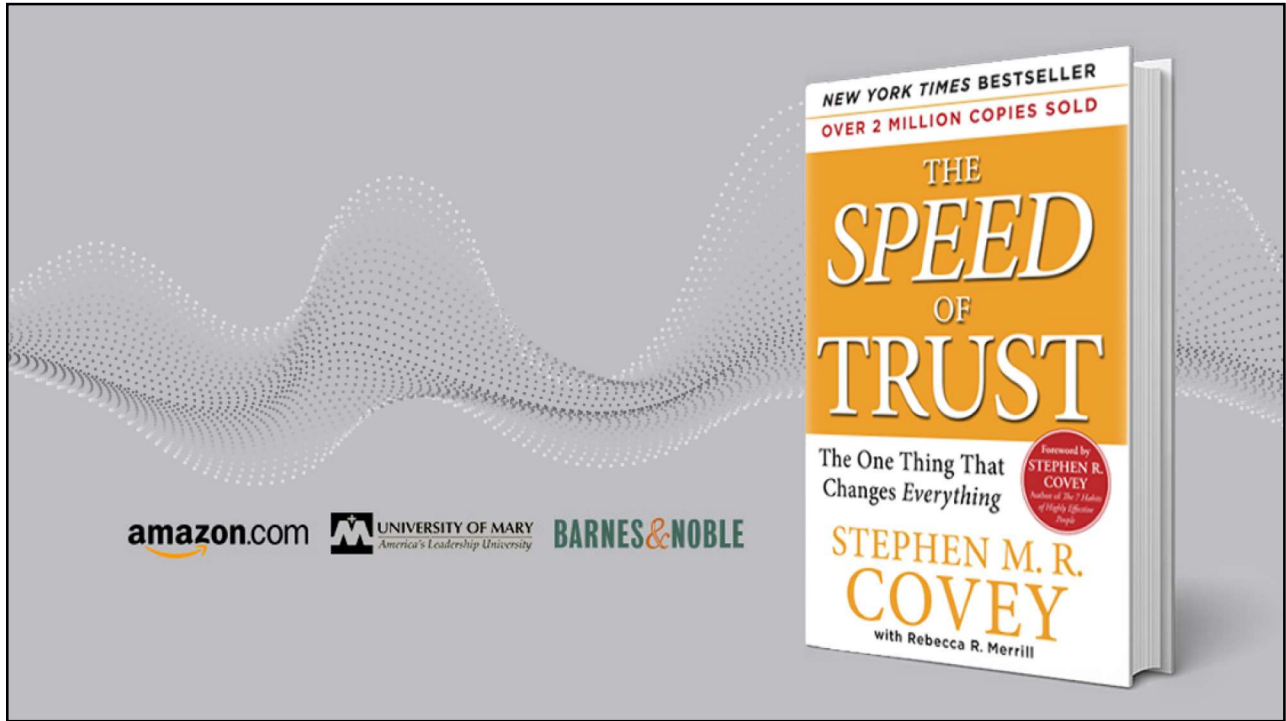
18



19



20



21



22



23



24



25



26



27



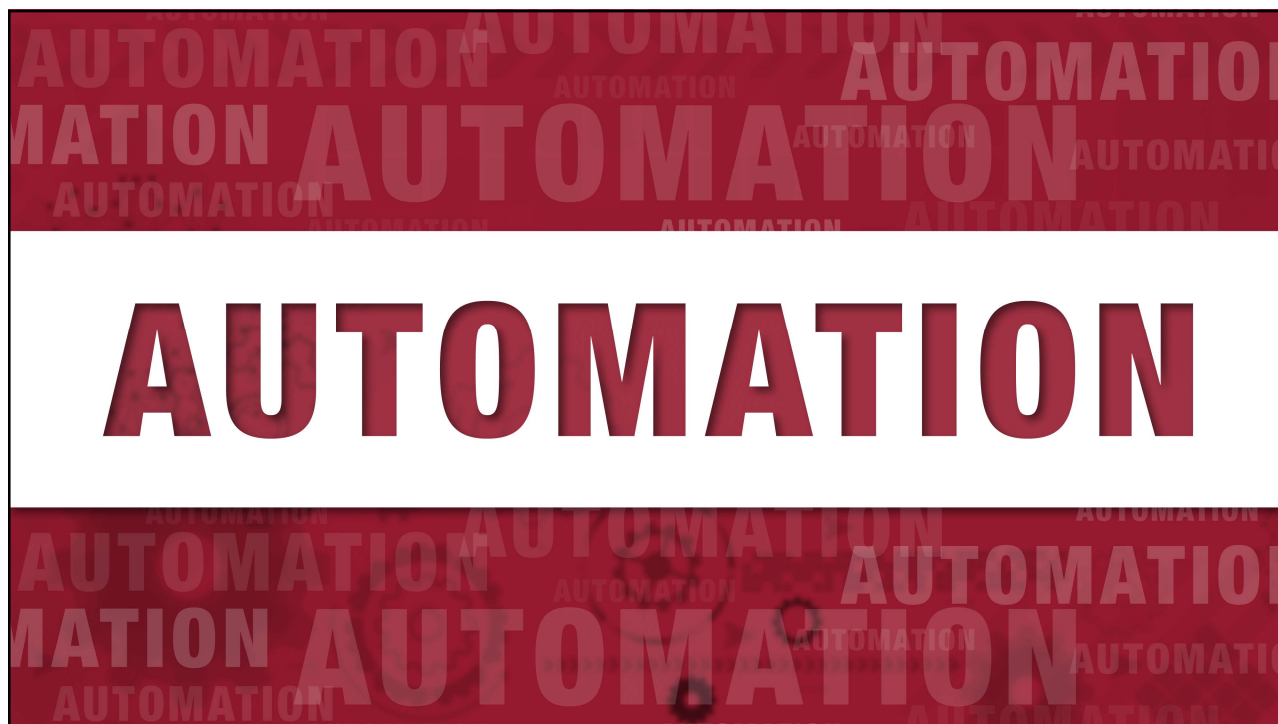
28



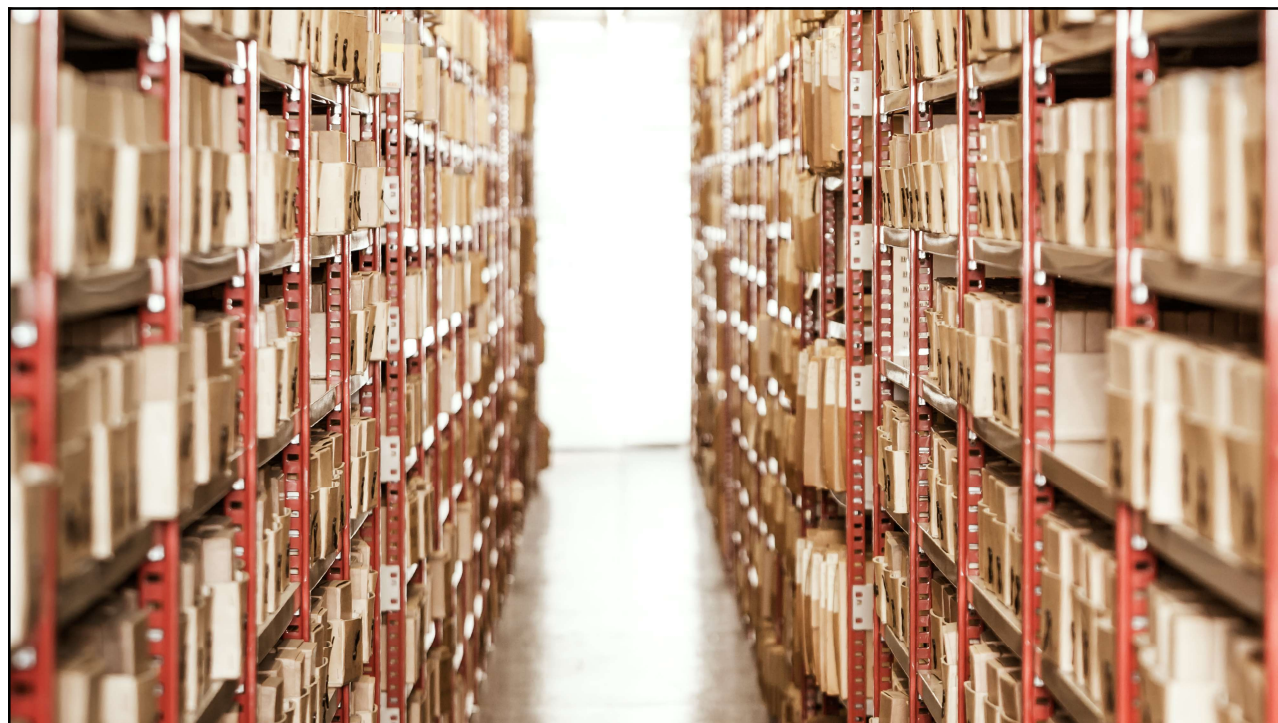
29



30

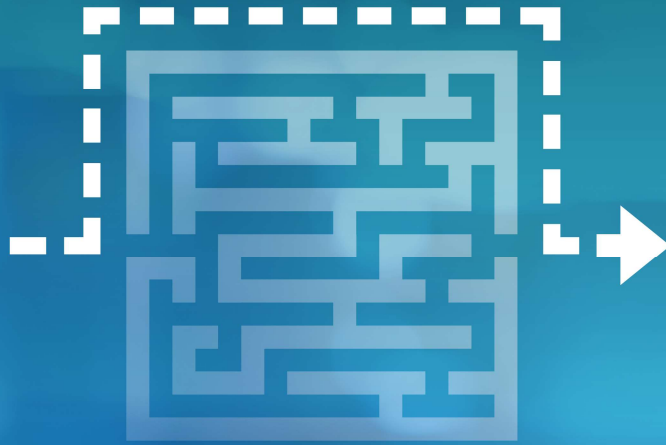


31



32

THINK DIFFERENTLY



33



CYBER AWARENESS

34



RANSOMWARE

WE ARE ALL TARGETS.
COMPANY SIZE IS NOT A FACTOR


RANSOMWARE AS A SERVICE

- CONTI
- LORENZ
- BLACKBYTE

CRITICAL INFRASTRUCTURE

35

CYBER THREATS: RECENT EVENTS



100+ CYBER EVENTS AFFECTING NISC MEMBERS IN THE LAST 6 MONTHS
- All requiring some sort of remediation

21 NISC MEMBERS AFFECTED BY RANSOMWARE ATTACKS
- Downtime ranging from hours to weeks

NISC HAS SEEN A 20% INCREASE IN MALICIOUS PHISHING EMAILS IN THE LAST TWO MONTHS

36

COMMON ATTACK METHODS

- PHISHING
- REMOTE ACCESS
- UNPATCHED SYSTEMS

37

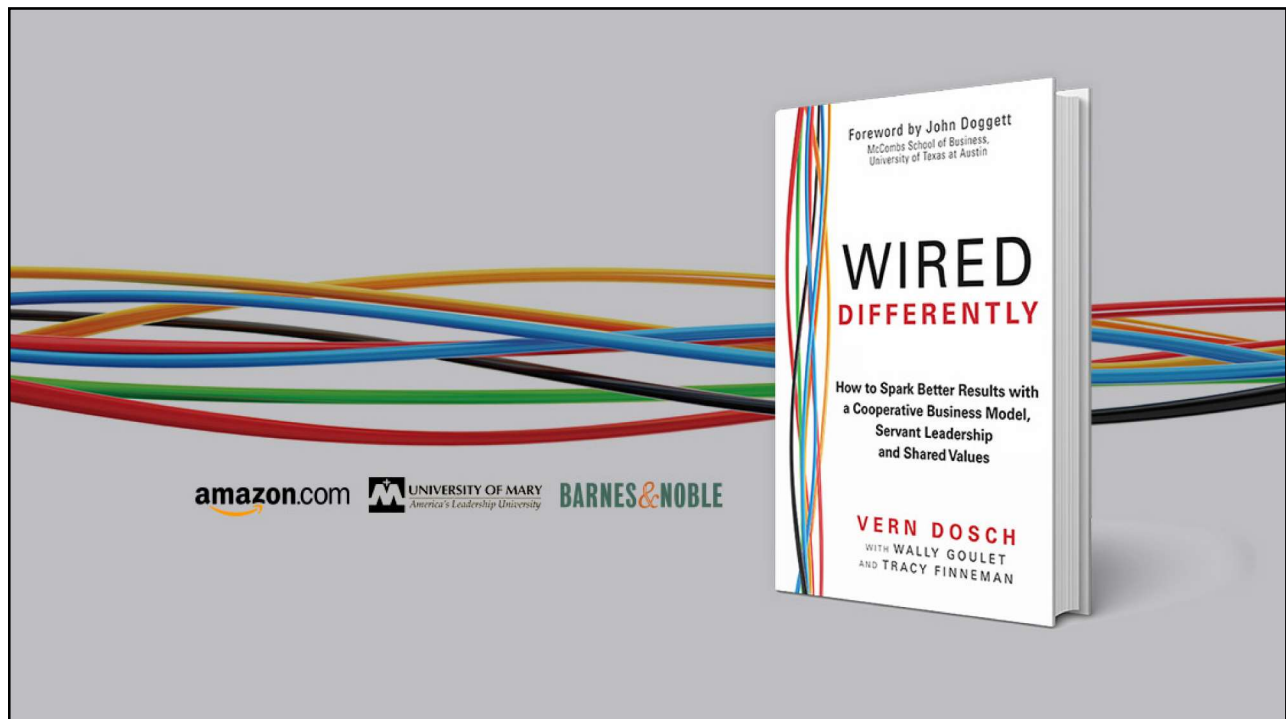
CYBERSECURITY QUESTIONS:

1. Do we have a program in place to train our employees on Cybersecurity Awareness?
2. Do we know everything we have, all hardware and software, that is on our network, and if so, are we regularly scanning those assets for vulnerabilities?
3. Do we have a program in place to regularly update or patch our systems for known vulnerabilities, and if so, how often?
4. How are we protecting our network from personal devices such as smart phones, tablets or even laptops that are not owned by our organization?
5. What is our strategy around password security and enabling multi-factor authentication for web applications?

38

6. Can you walk me through the defenses we have and what each would do in the event of a ransomware attack?
7. What do we have in place to find unauthorized access and notify us in a reasonable amount of time?
8. What disaster recovery and business continuity plans do we have in place for a cyberattack and which systems specifically are backed up and how?
9. Do we know which parts of security we are responsible for and which parts our vendors are responsible for?
10. Do we have an incident response plan?

39



40