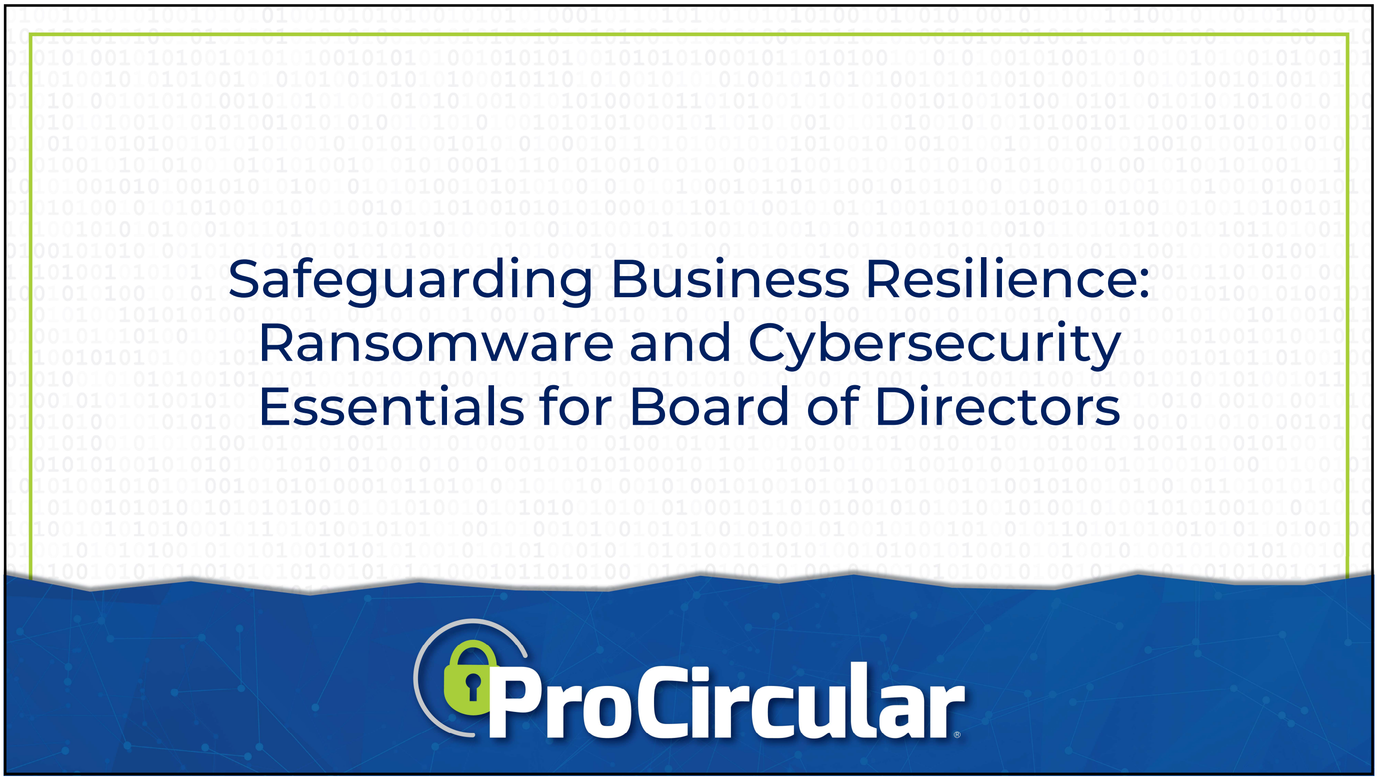
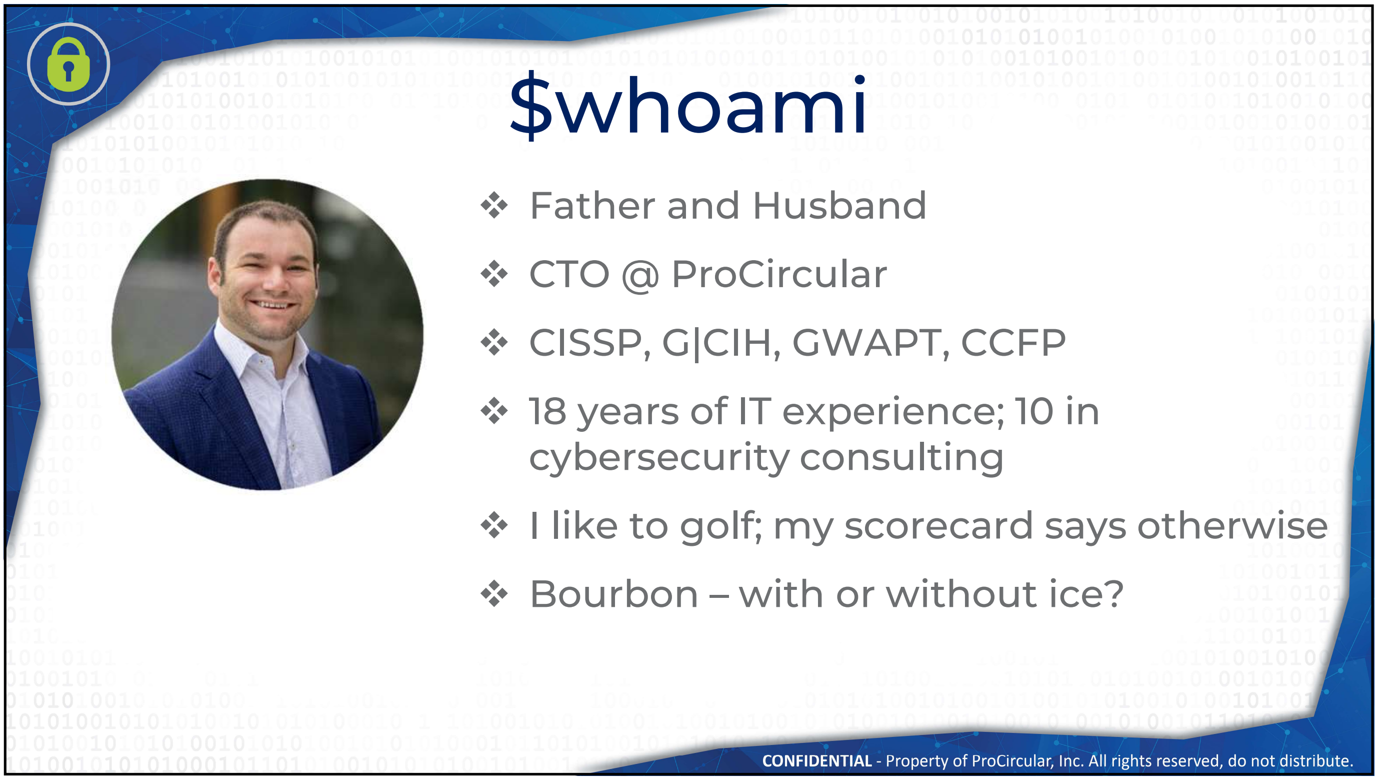


Safeguarding Business Resilience: Ransomware and Cybersecurity Essentials for Board of Directors

ProCircular

1

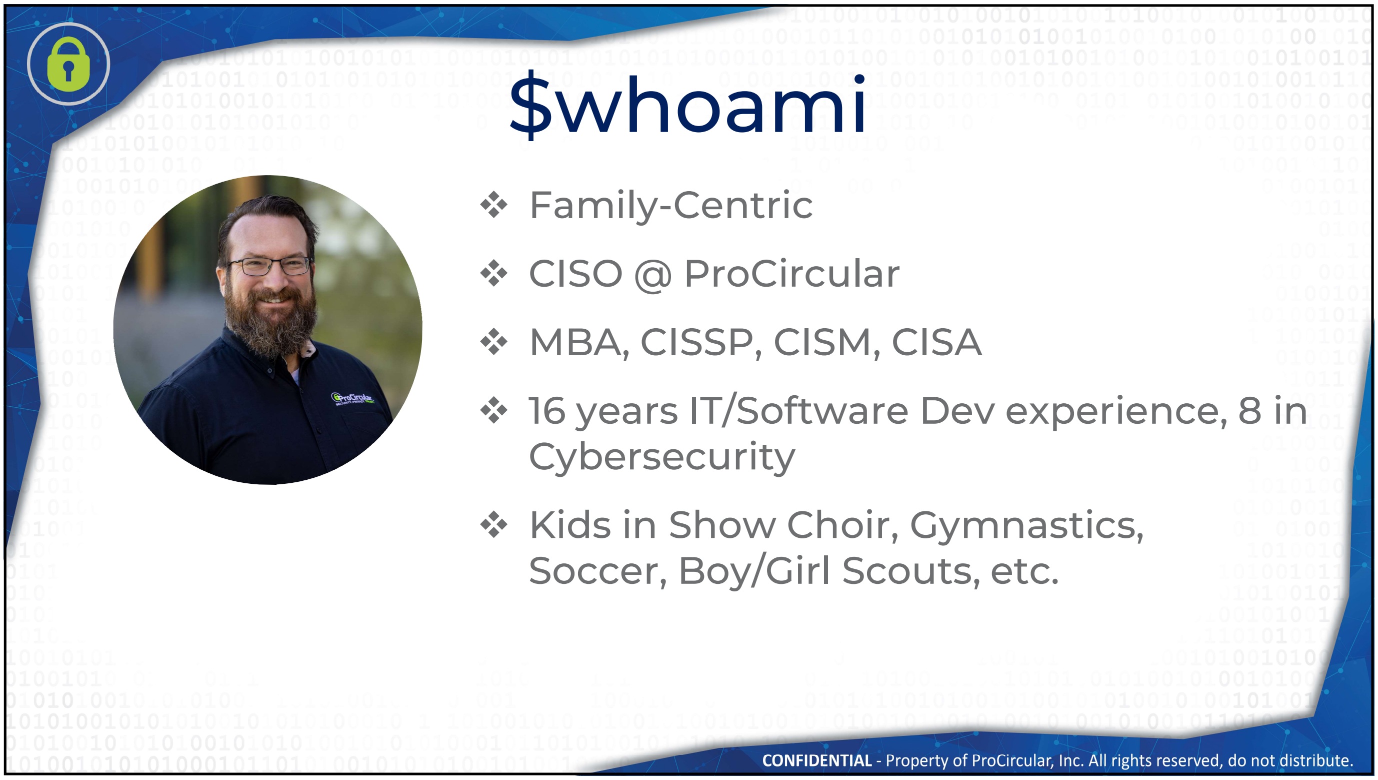


$whoami

- ❖ Father and Husband
- ❖ CTO @ ProCircular
- ❖ CISSP, G|CIH, GWAPT, CCFP
- ❖ 18 years of IT experience; 10 in cybersecurity consulting
- ❖ I like to golf; my scorecard says otherwise
- ❖ Bourbon – with or without ice?

CONFIDENTIAL - Property of ProCircular, Inc. All rights reserved, do not distribute.

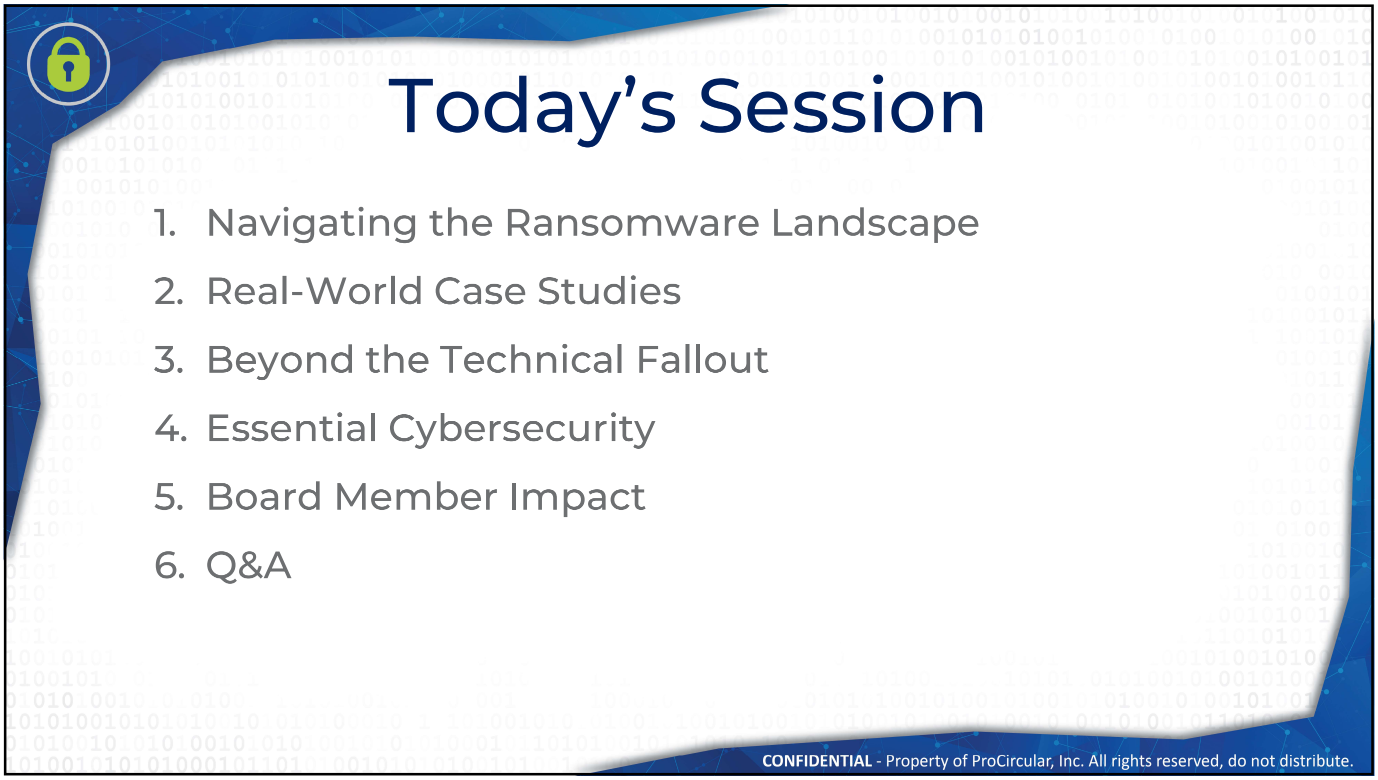
2



$whoami

- Family-Centric
- CISO @ ProCircular
- MBA, CISSP, CISM, CISA
- 16 years IT/Software Dev experience, 8 in Cybersecurity
- Kids in Show Choir, Gymnastics, Soccer, Boy/Girl Scouts, etc.

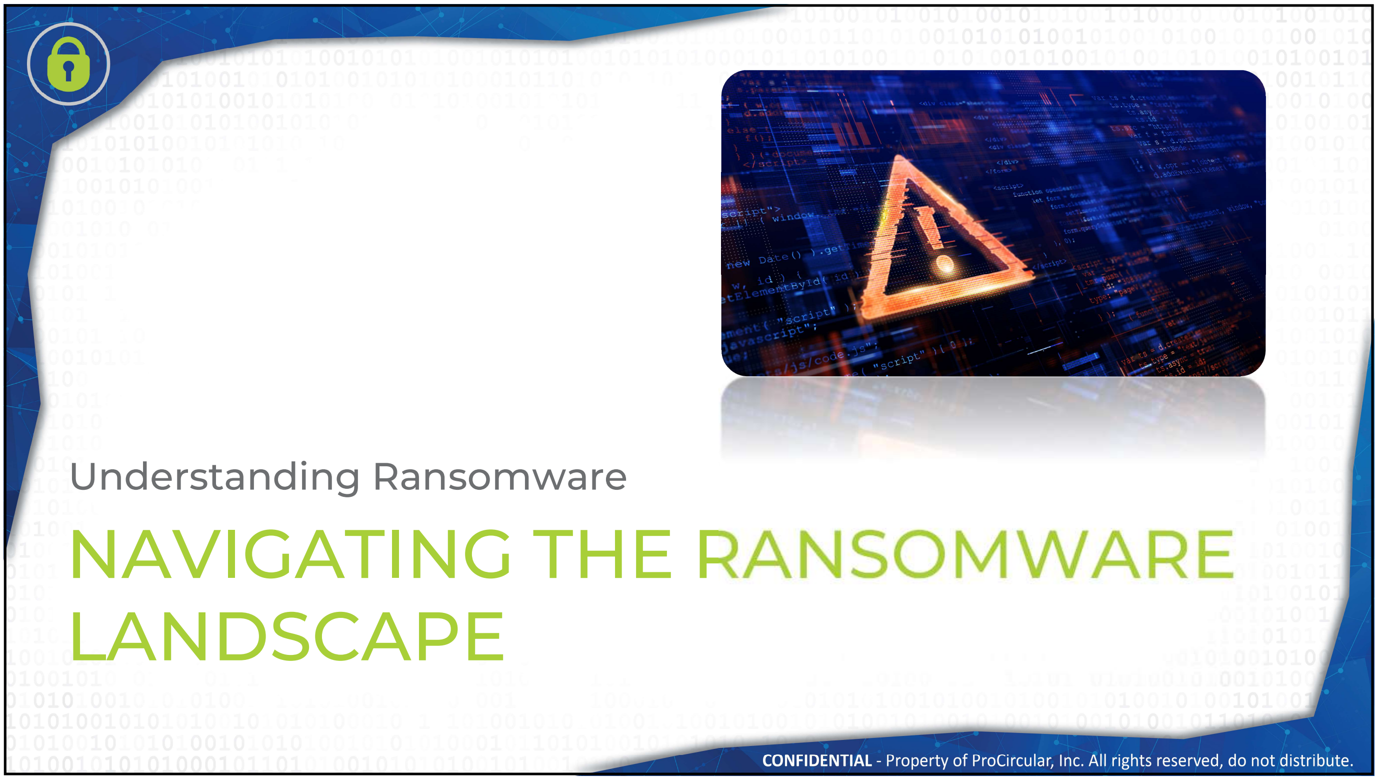
3



Today’s Session

1. Navigating the Ransomware Landscape
2. Real-World Case Studies
3. Beyond the Technical Fallout
4. Essential Cybersecurity
5. Board Member Impact
6. Q&A

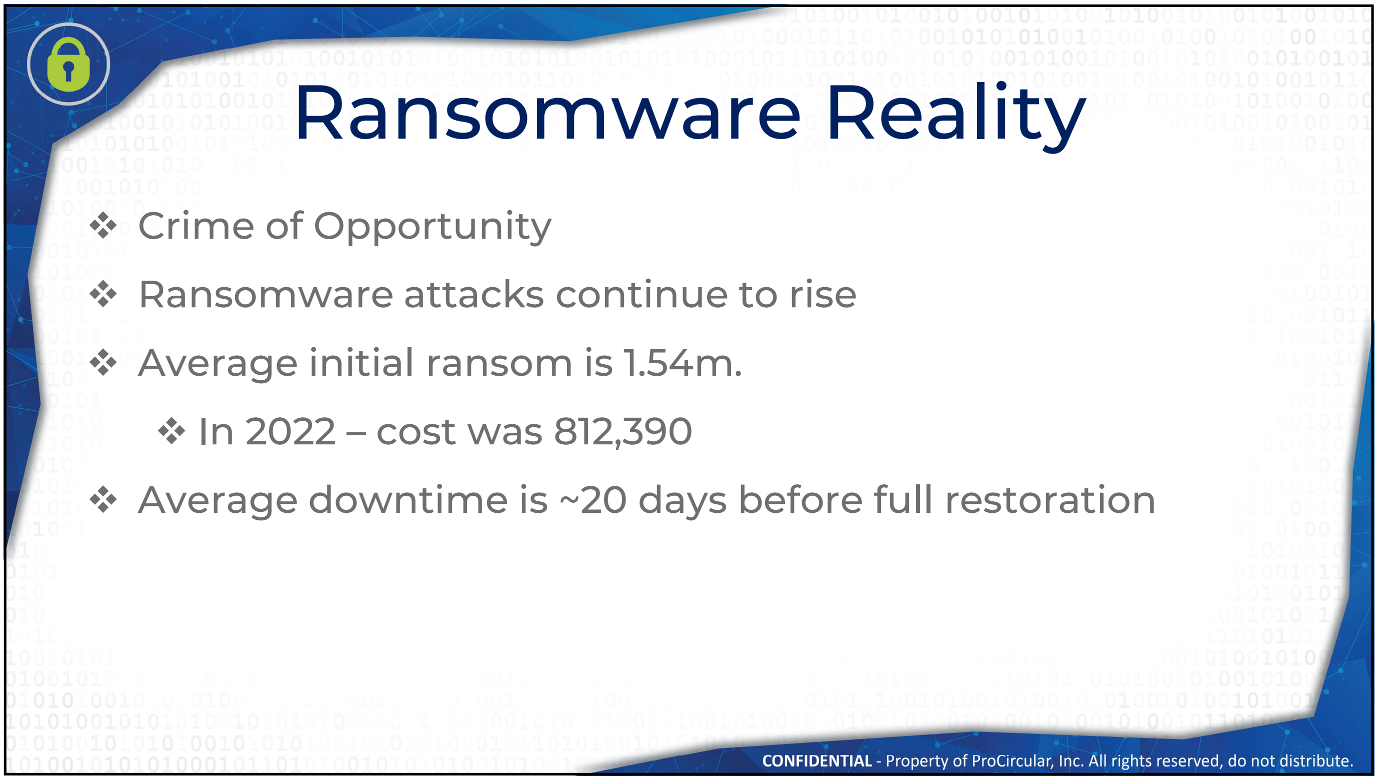
4



Understanding Ransomware

NAVIGATING THE RANSOMWARE LANDSCAPE

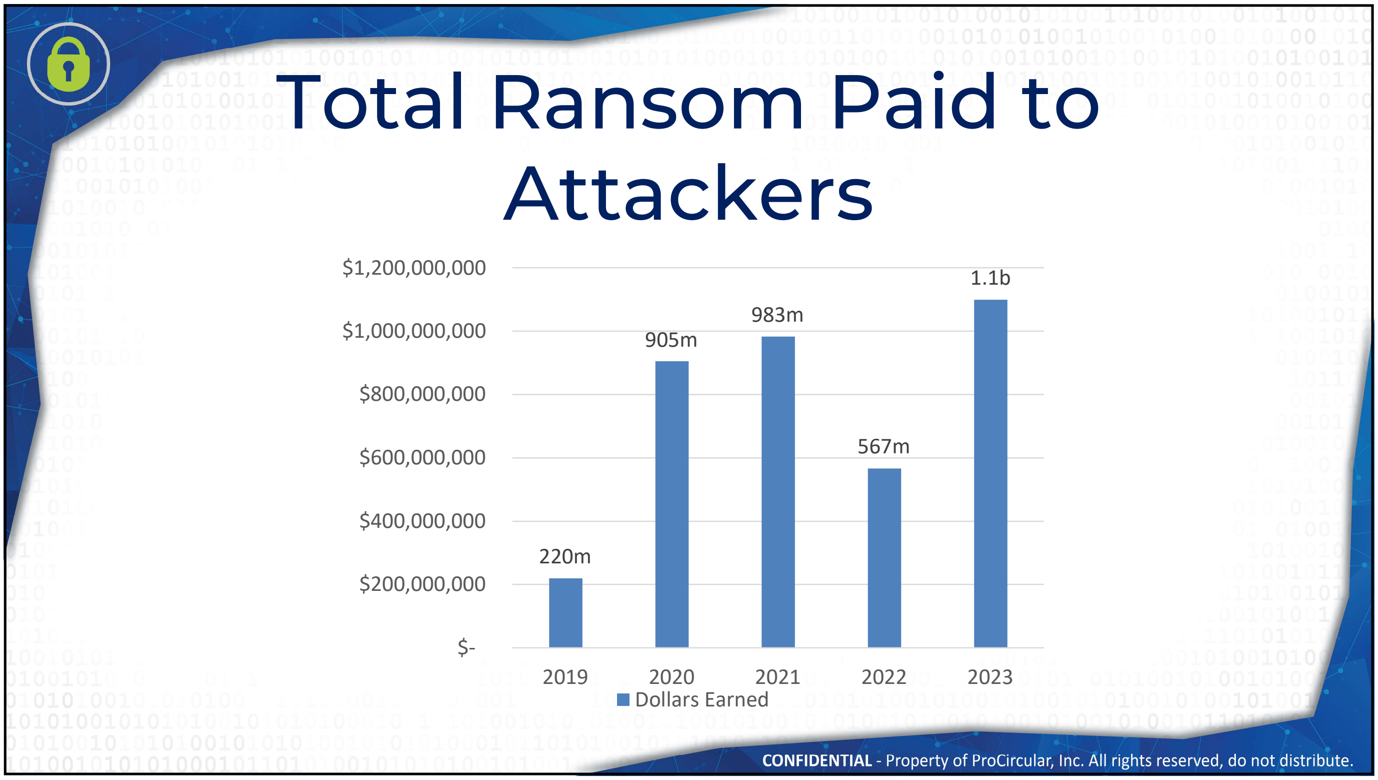
5



Ransomware Reality

- ❖ Crime of Opportunity
- ❖ Ransomware attacks continue to rise
- ❖ Average initial ransom is 1.54m.
  - ❖ In 2022 – cost was 812,390
- ❖ Average downtime is ~20 days before full restoration

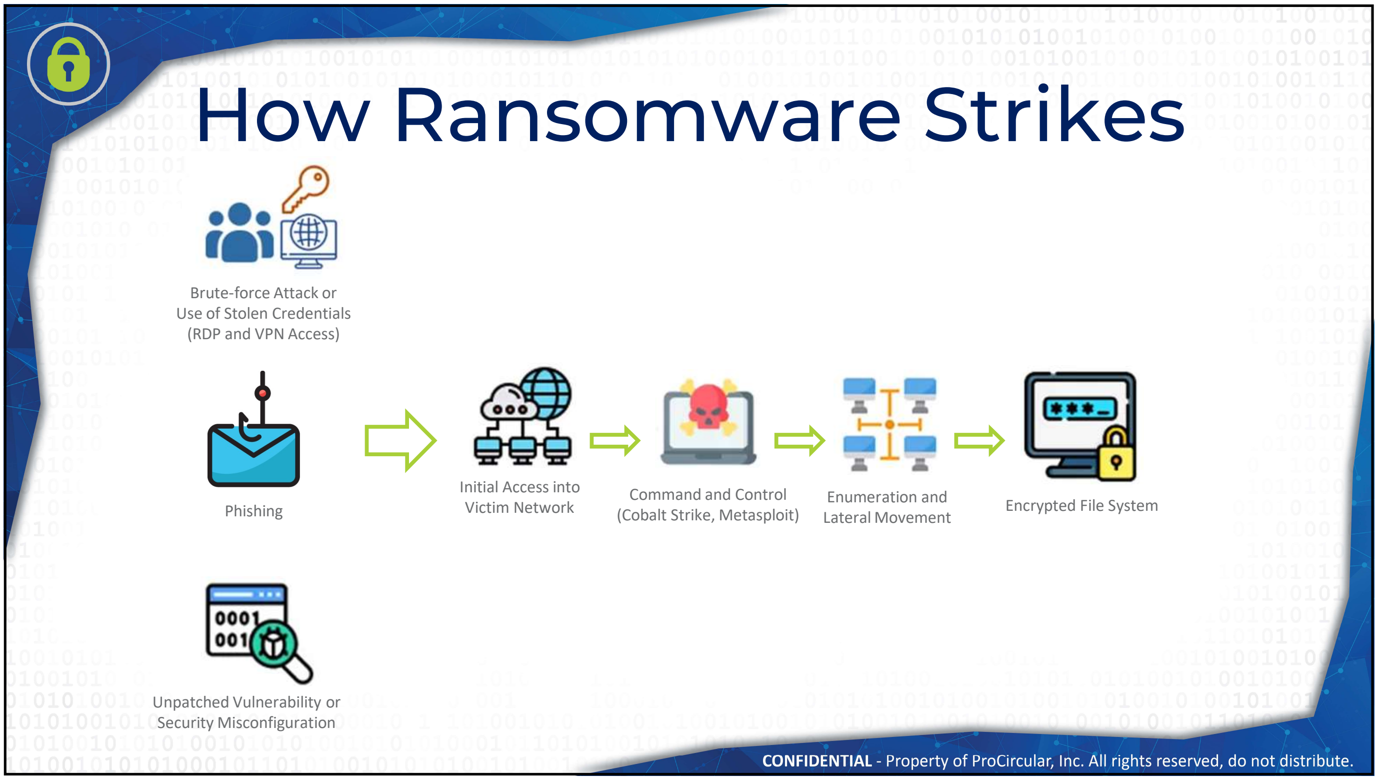
6



Total Ransom Paid to Attackers

CONFIDENTIAL - Property of ProCircular, Inc. All rights reserved, do not distribute.

7



How Ransomware Strikes

Brute-force Attack or Use of Stolen Credentials (RDP and VPN Access)

Phishing

Unpatched Vulnerability or Security Misconfiguration

Initial Access into Victim Network

Command and Control (Cobalt Strike, Metasploit)

Enumeration and Lateral Movement

Encrypted File System

CONFIDENTIAL - Property of ProCircular, Inc. All rights reserved, do not distribute.

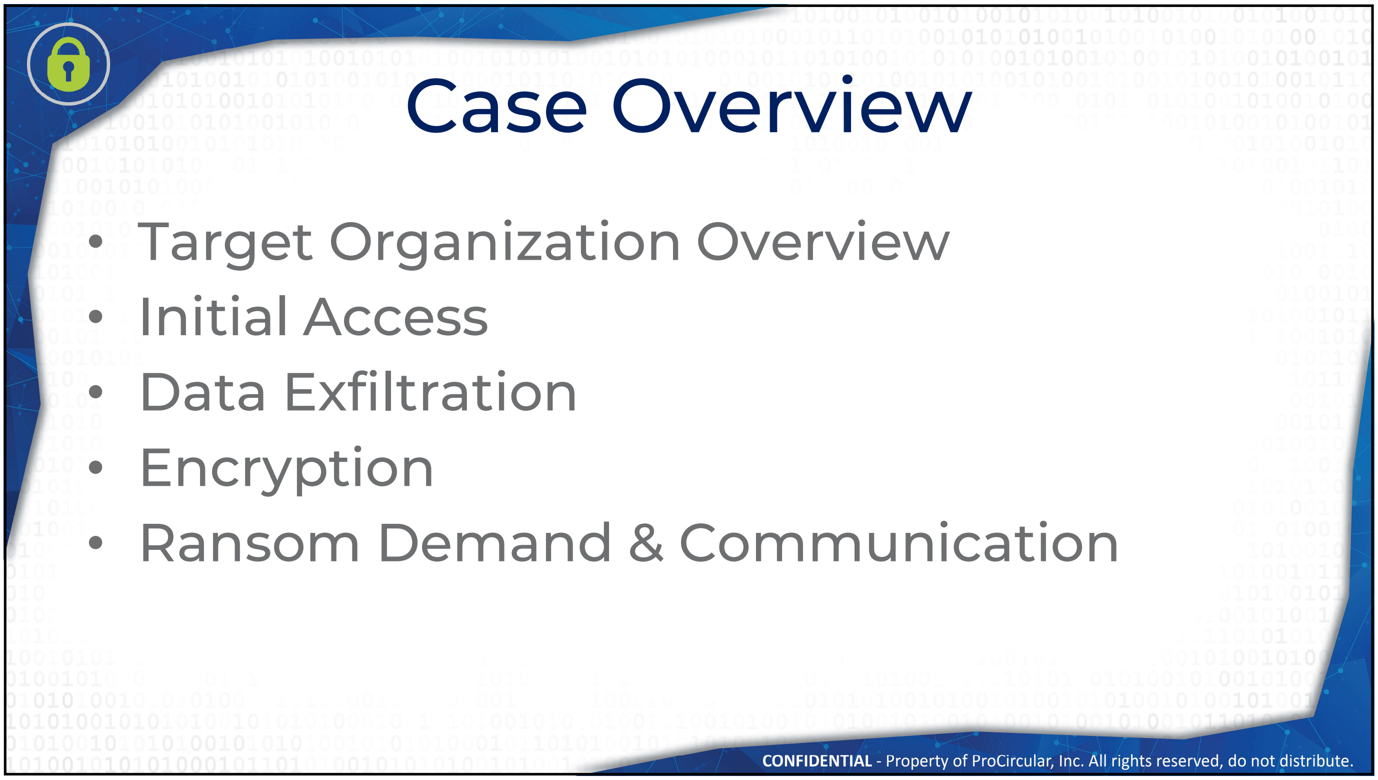
8

Case Study # 1

LOCKBIT 3.0

CONFIDENTIAL - Property of ProCircular, Inc. All rights reserved, do not distribute.

9



Case Overview

- Target Organization Overview
- Initial Access
- Data Exfiltration
- Encryption
- Ransom Demand & Communication

CONFIDENTIAL - Property of ProCircular, Inc. All rights reserved, do not distribute.

10

Case Study # 2

BLACKCAT / ALPHV

11

Case Overview

- Target Organization Overview
- Initial Access
- Data Exfiltration
- Encryption
- Ransom Demand & Communication

12

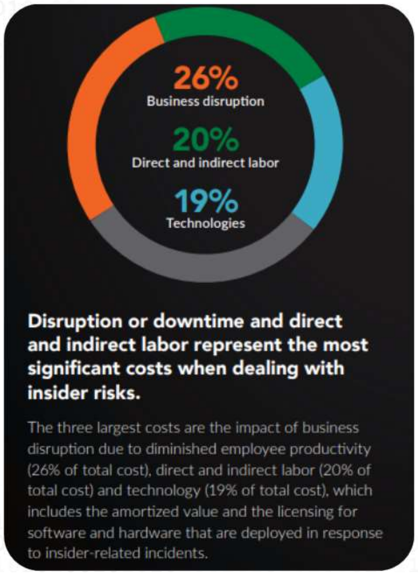
Hidden Risks....

BEYOND THE TECHNICAL FALLOUT

Hidden Risks of Ransomware

- Downtime Costs
- Data Exposure
- Lost business and reputation damage
- Legal and non-compliance penalties
- Customer trust (harder to gain than to lose)
- Additional Expenditures
  - New tech
  - New security spend
  - Increased Premiums

Cost Components

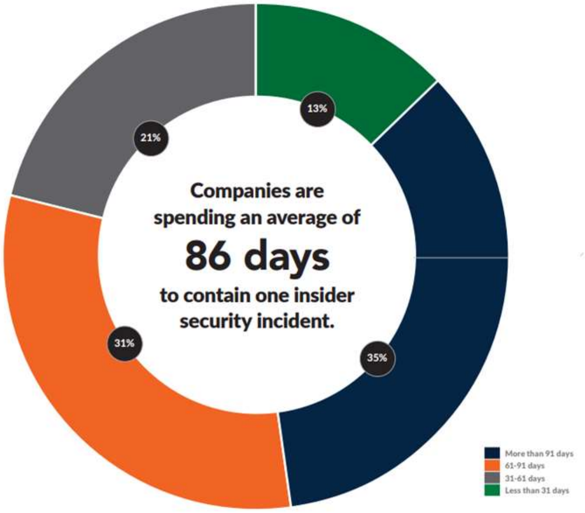


Disruption or downtime and direct and indirect labor represent the most significant costs when dealing with insider risks.

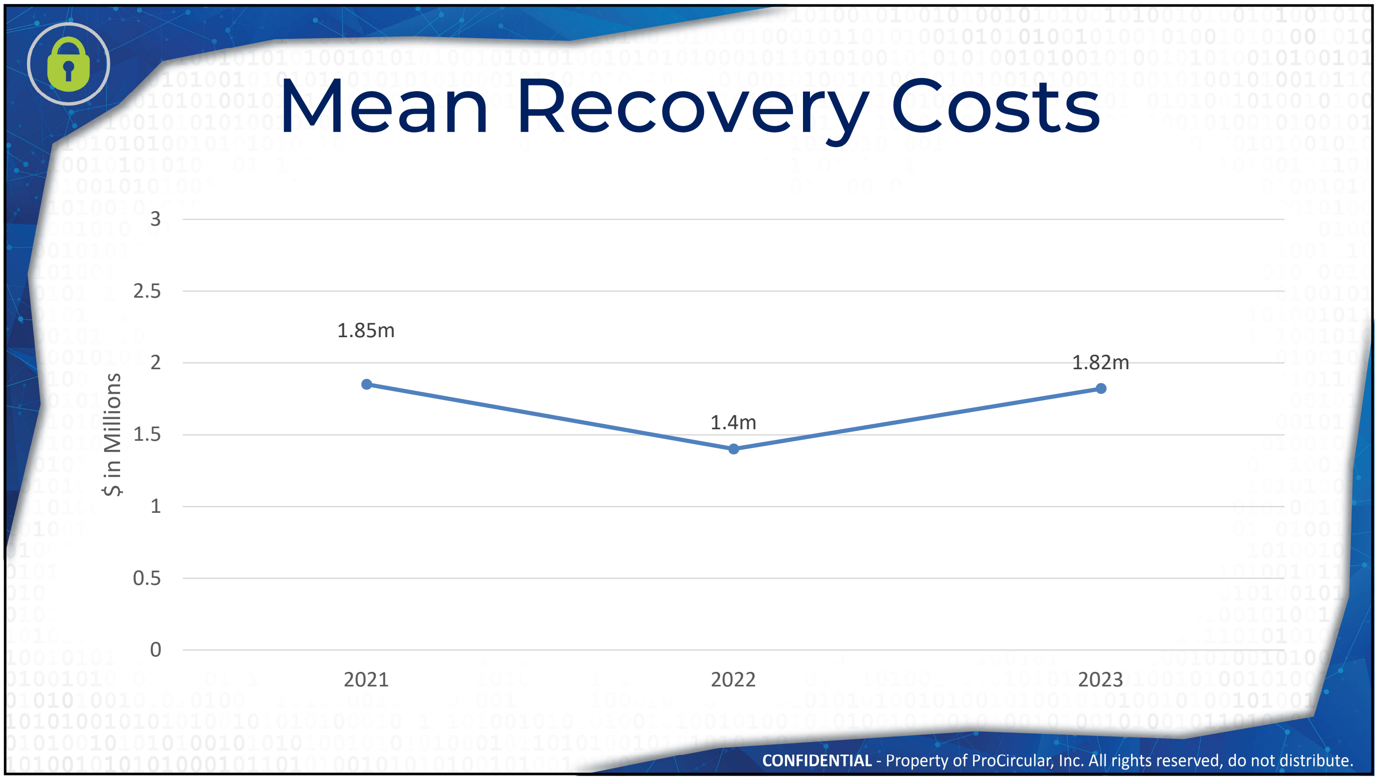
The three largest costs are the impact of business disruption due to diminished employee productivity (26% of total cost), direct and indirect labor (20% of total cost) and technology (19% of total cost), which includes the amortized value and the licensing for software and hardware that are deployed in response to insider-related incidents.

- ❖ Business Resiliency is King
- ❖ Costs are Long Lasting

Time to Contain Incident



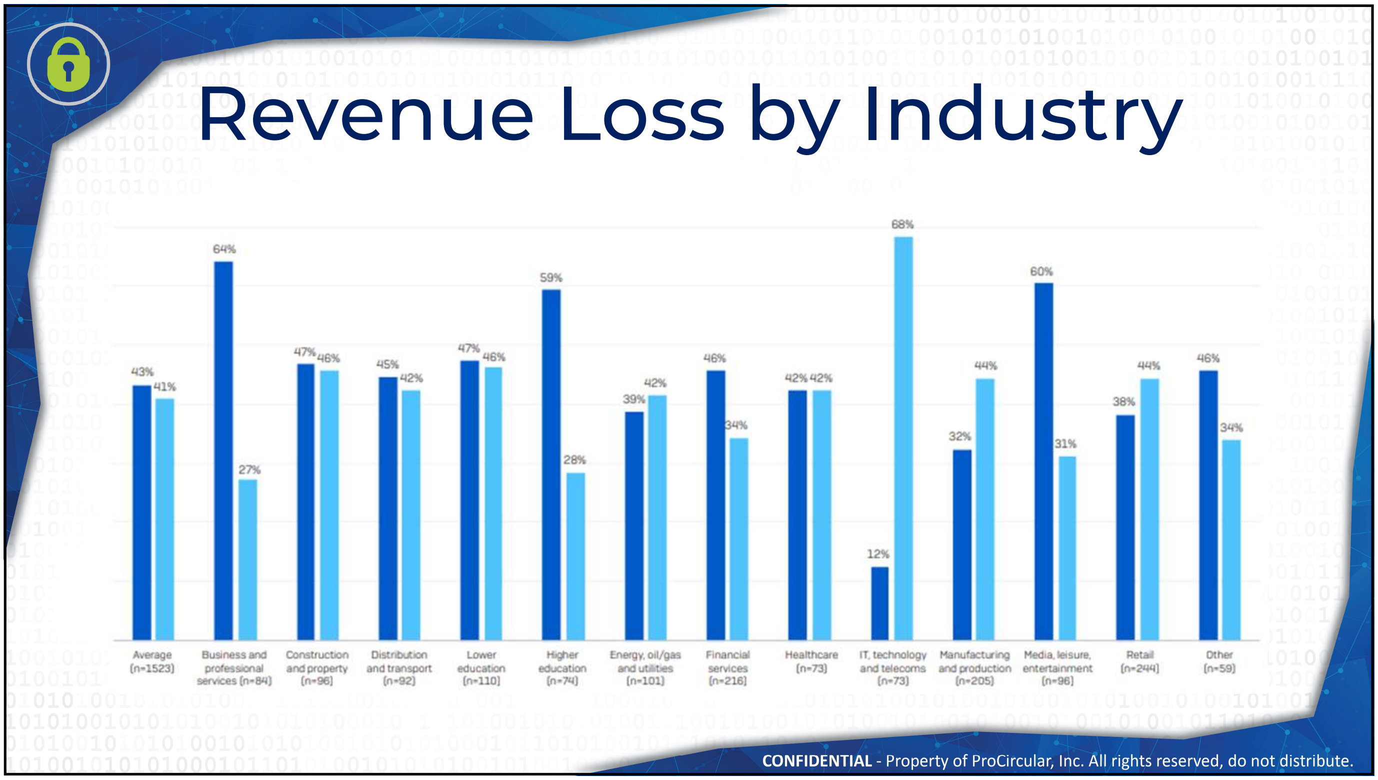
Companies are spending an average of **86 days** to contain one insider security incident.



Mean Recovery Costs

CONFIDENTIAL - Property of ProCircular, Inc. All rights reserved, do not distribute.

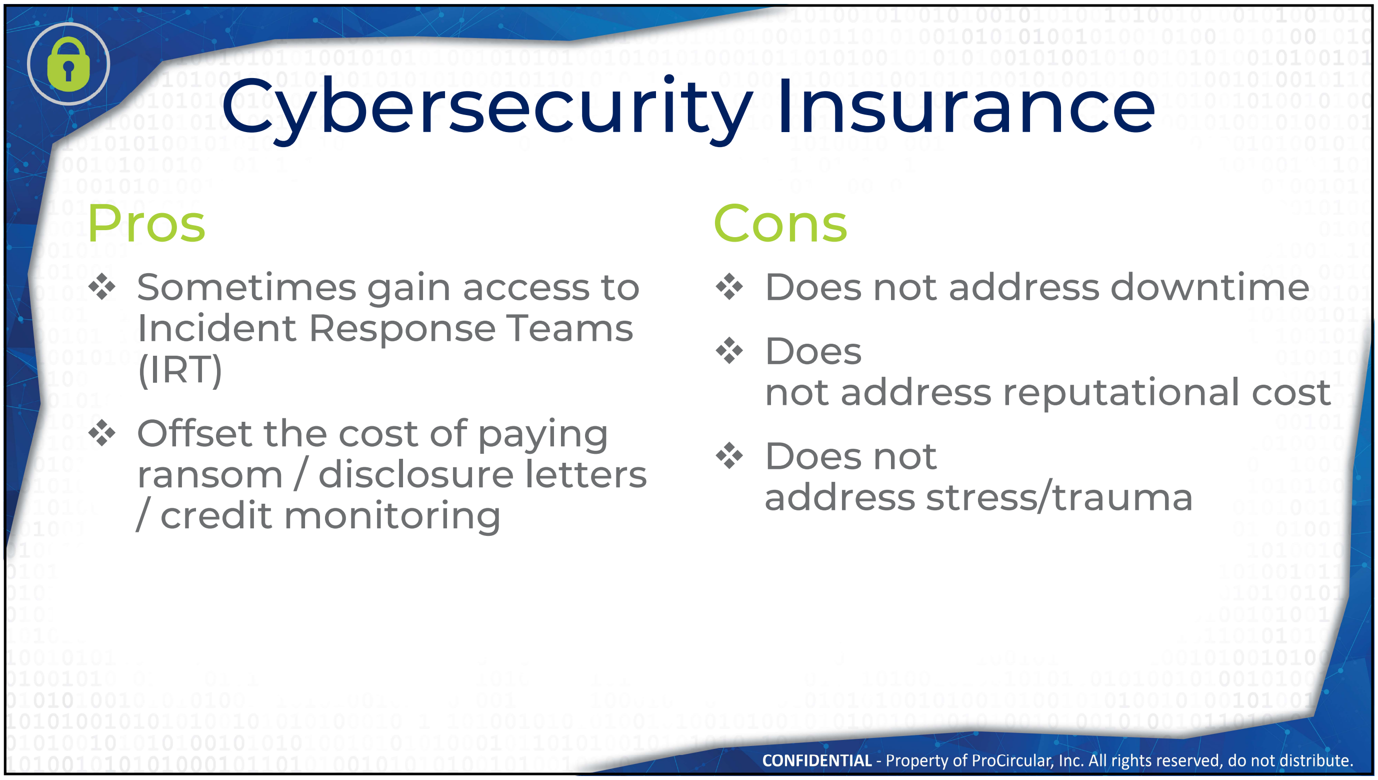
17



Revenue Loss by Industry

CONFIDENTIAL - Property of ProCircular, Inc. All rights reserved, do not distribute.

18



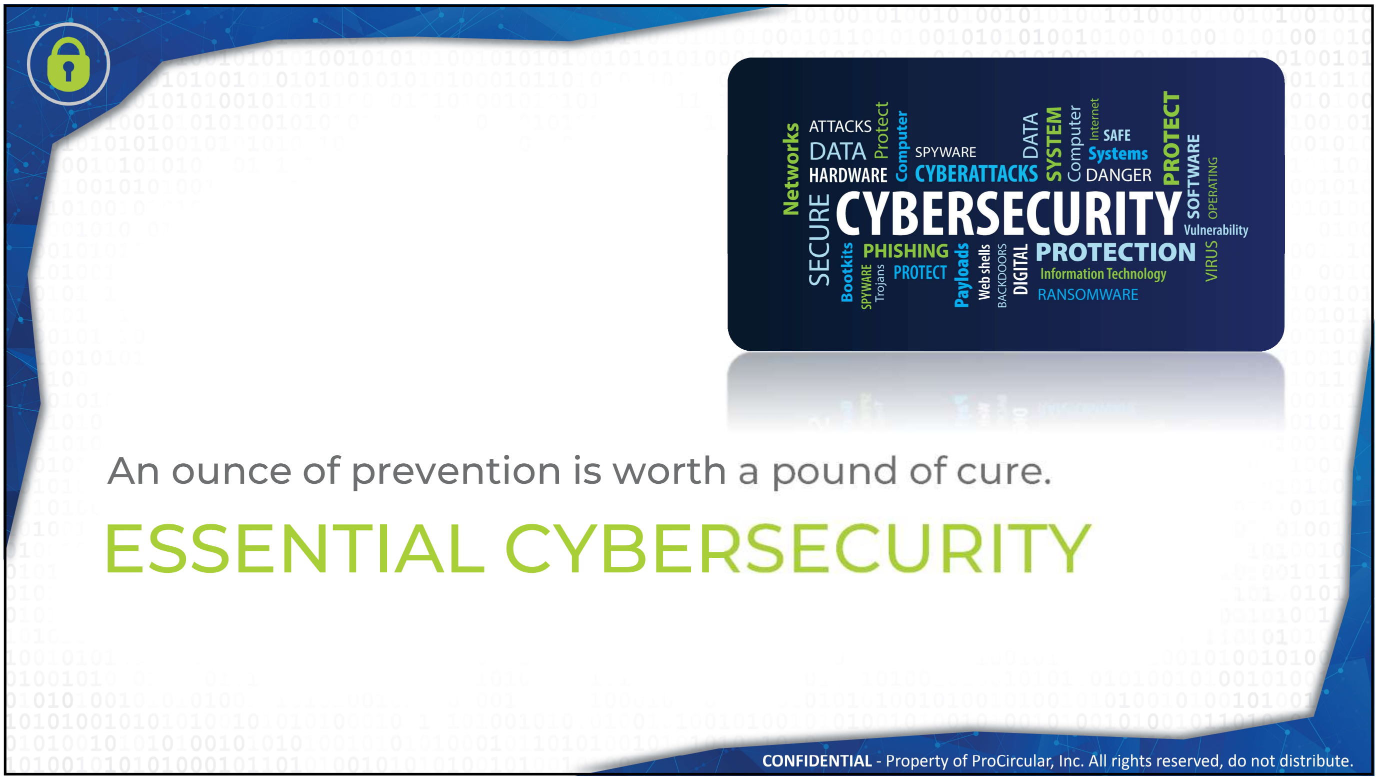
Cybersecurity Insurance

Pros

- Sometimes gain access to Incident Response Teams (IRT)
- Offset the cost of paying ransom / disclosure letters / credit monitoring

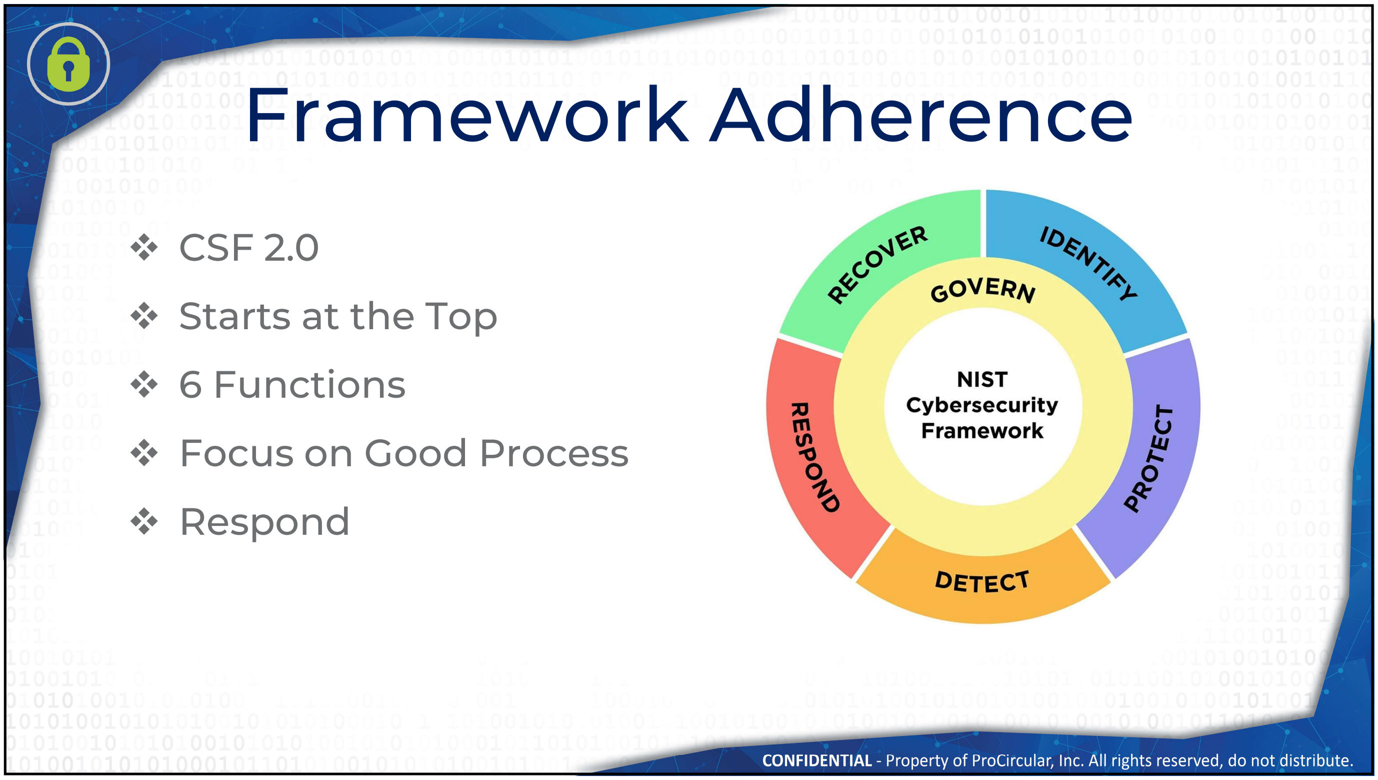
Cons

- Does not address downtime
- Does not address reputational cost
- Does not address stress/trauma


Networks
SECURE
ATTACKS
DATA
HARDWARE
Protect
Computer
SPYWARE
CYBERATTACKS
DATA
SYSTEM
Computer
Internet
SAFE
Systems
DANGER
PROTECT
SOFTWARE
OPERATING
CYBERSECURITY
Vulnerability
Bootkits
SPYWARE
Trojans
PHISHING
PROTECT
Payloads
Web shells
BACKDOORS
DIGITAL
PROTECTION
Information Technology
RANSOMWARE
VIRUS

An ounce of prevention is worth a pound of cure.

ESSENTIAL CYBERSECURITY



Framework Adherence

- CSF 2.0
- Starts at the Top
- 6 Functions
- Focus on Good Process
- Respond

NIST Cybersecurity Framework

GOVERN

IDENTIFY

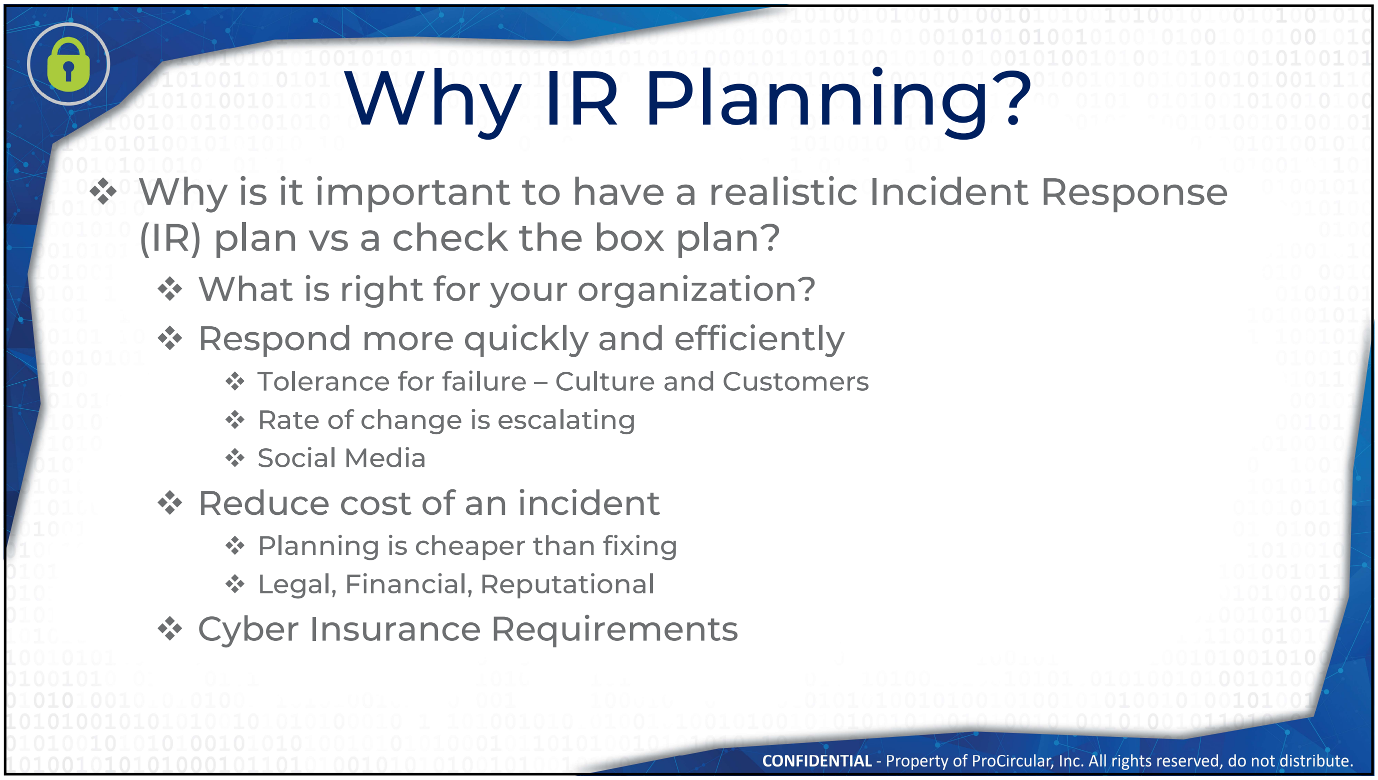
PROTECT

DETECT

RESPOND

RECOVER

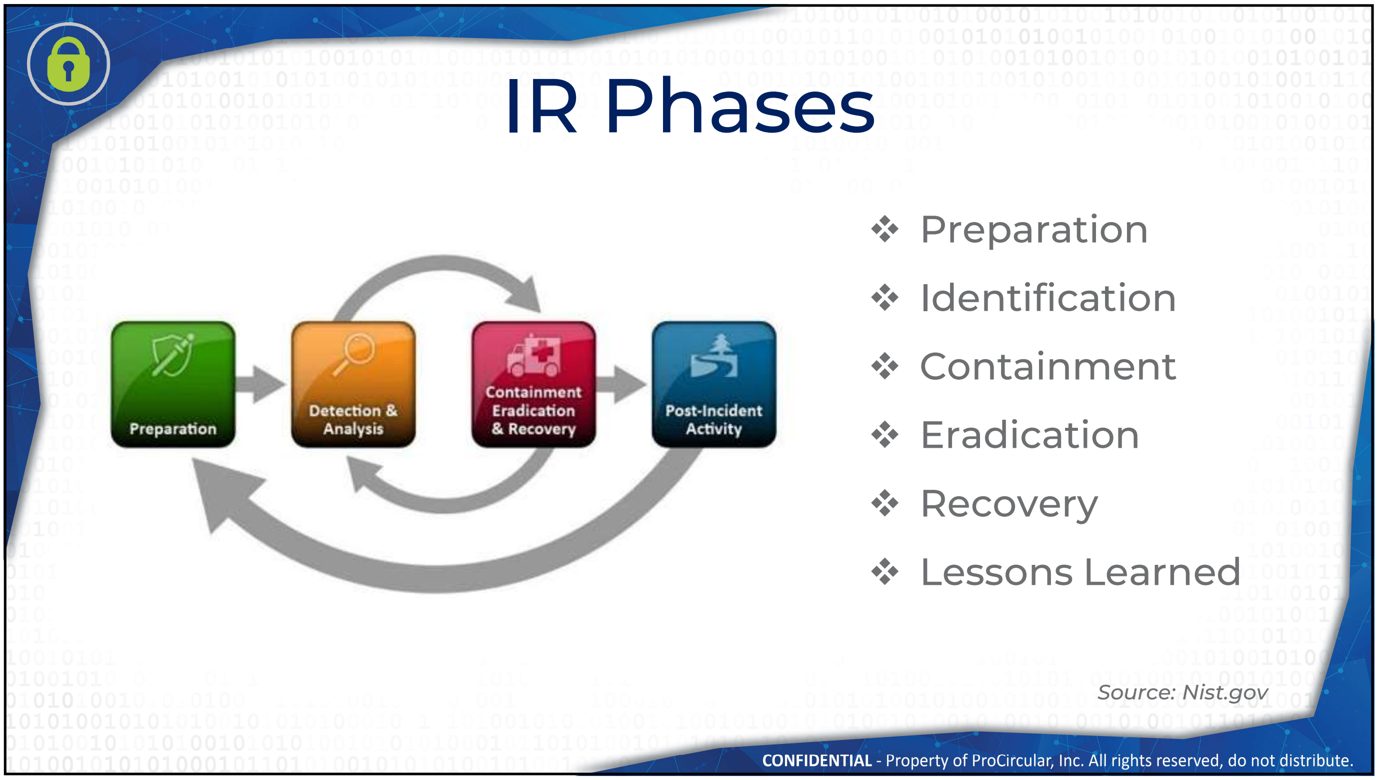
21



Why IR Planning?

- Why is it important to have a realistic Incident Response (IR) plan vs a check the box plan?
  - What is right for your organization?
  - Respond more quickly and efficiently
    - Tolerance for failure – Culture and Customers
    - Rate of change is escalating
    - Social Media
  - Reduce cost of an incident
    - Planning is cheaper than fixing
    - Legal, Financial, Reputational
  - Cyber Insurance Requirements

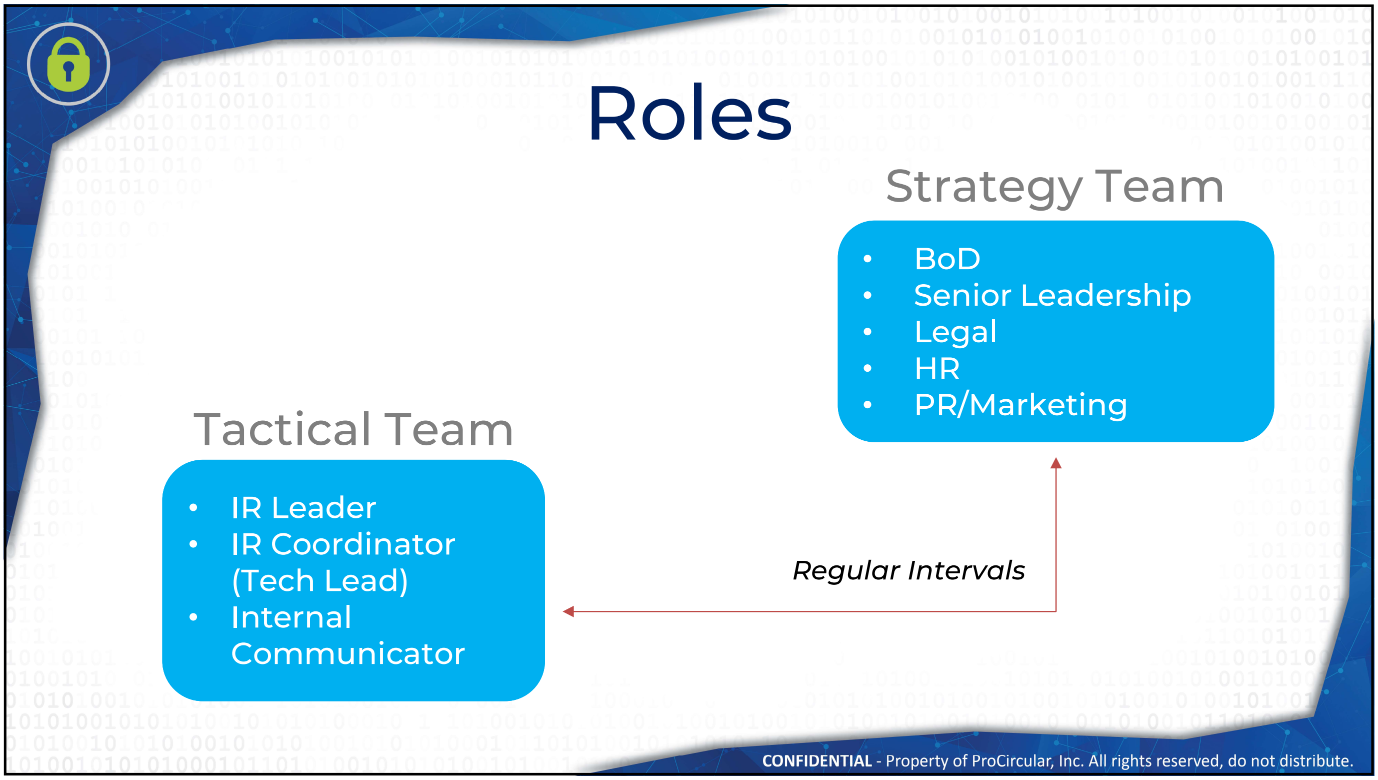
22


Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-Incident Activity

IR Phases

- ❖ Preparation
- ❖ Identification
- ❖ Containment
- ❖ Eradication
- ❖ Recovery
- ❖ Lessons Learned

Source: Nist.gov



Roles

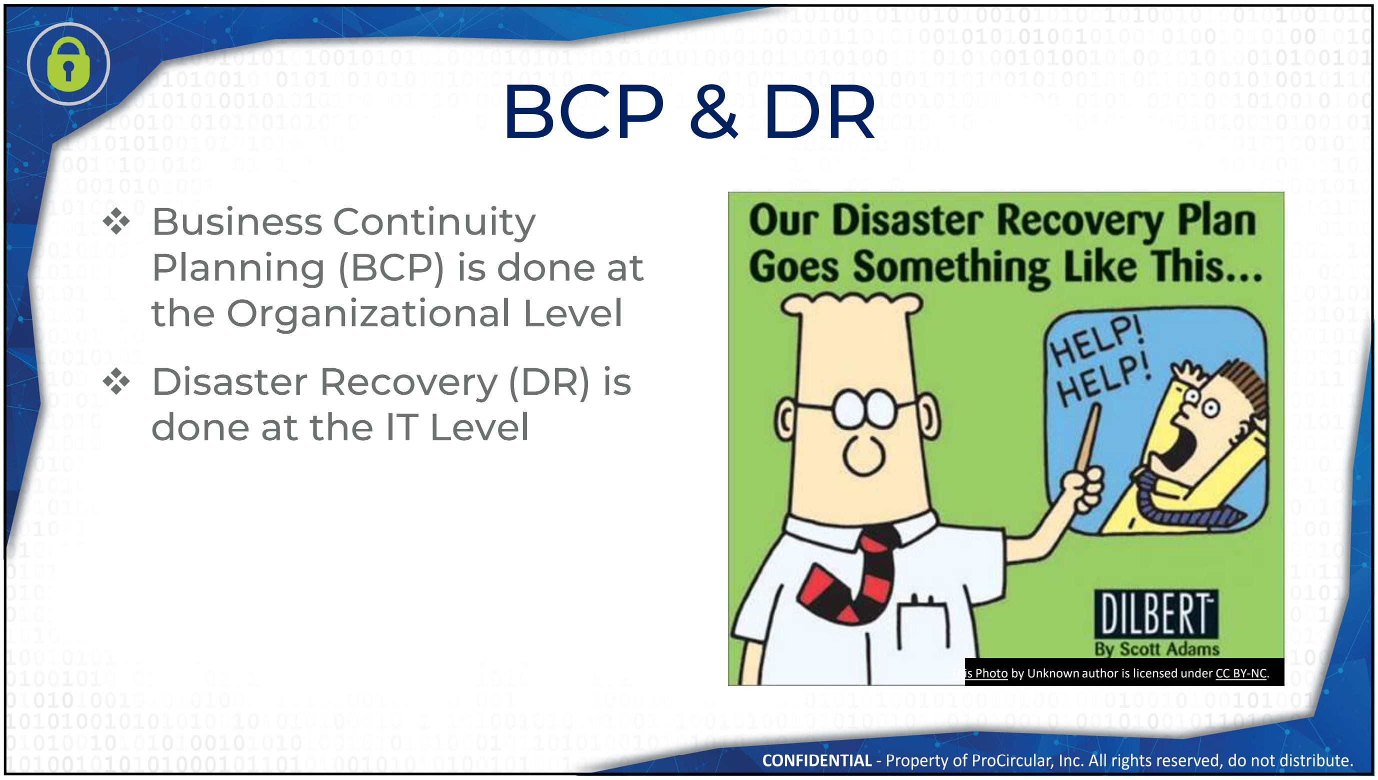
Strategy Team

- BoD
- Senior Leadership
- Legal
- HR
- PR/Marketing

Tactical Team

- IR Leader
- IR Coordinator (Tech Lead)
- Internal Communicator

Regular Intervals

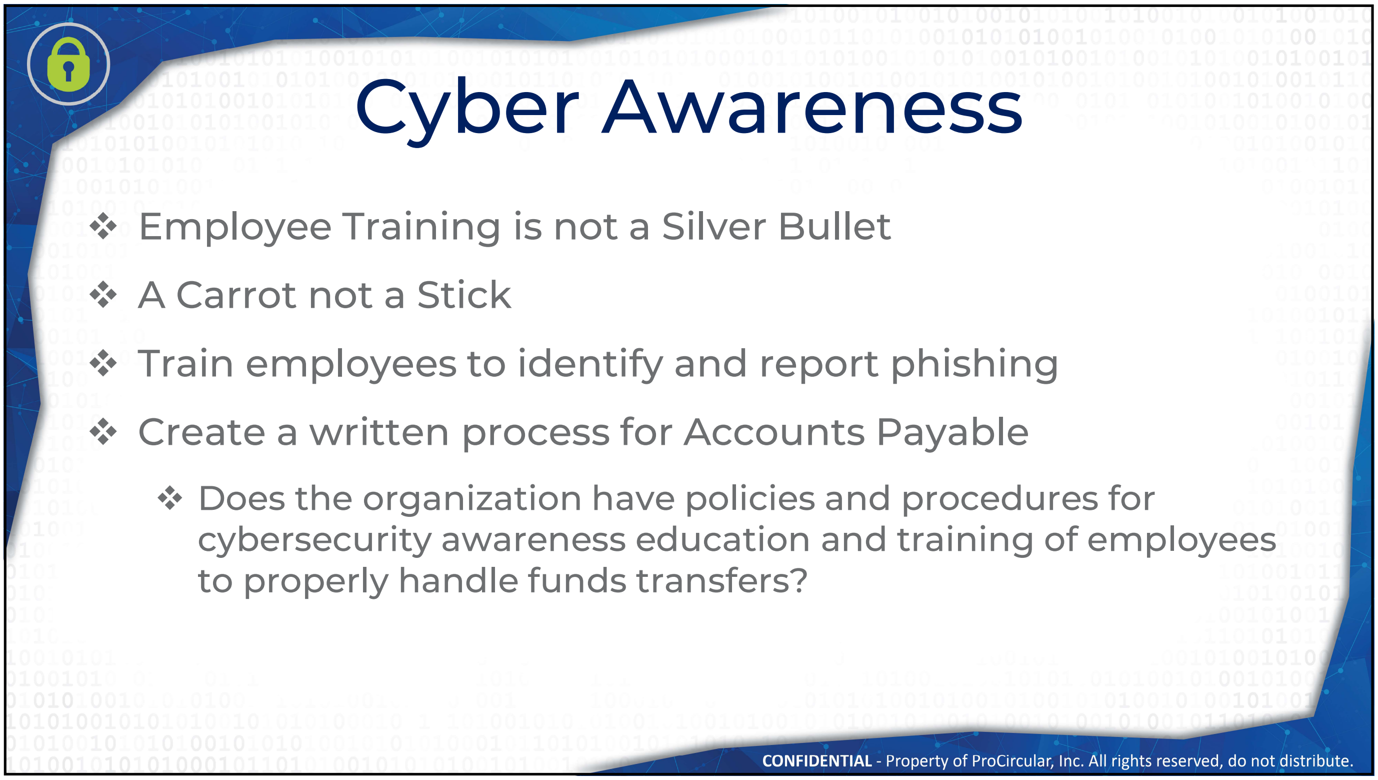


BCP & DR

- ❖ Business Continuity Planning (BCP) is done at the Organizational Level
- ❖ Disaster Recovery (DR) is done at the IT Level

s Photo by Unknown author is licensed under CC BY-NC.

25



Cyber Awareness

- ❖ Employee Training is not a Silver Bullet
- ❖ A Carrot not a Stick
- ❖ Train employees to identify and report phishing
- ❖ Create a written process for Accounts Payable
  - ❖ Does the organization have policies and procedures for cybersecurity awareness education and training of employees to properly handle funds transfers?

26

Tech Tools of the Trade

- ❖ Multi-Factor Authentication (MFA)
- ❖ Regular Backups. Seriously.
- ❖ Patch Management
- ❖ Advanced Endpoint Detection & Continuous Monitoring
- ❖ Scanning & Regular Assessment

Tone from the Top

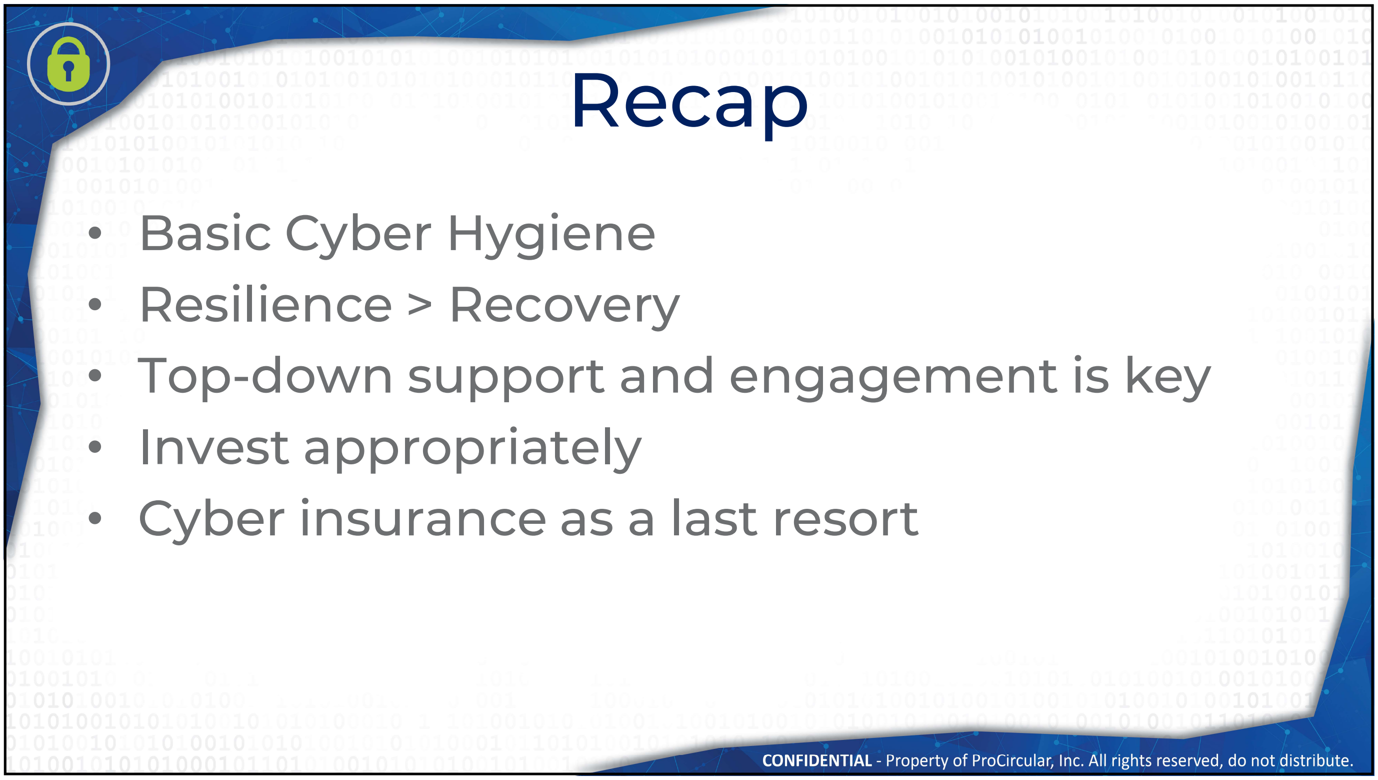
BOARD MEMBER IMPACT

Why Cyber is a Board-Level Issue

- Cybersecurity is for everybody, not just technology companies.
- It's about empowering and supporting people and process.
  - Not just technology.
- Cybersecurity is for everybody, not just technology companies.
- Risk Appetite Statement – What are we willing to accept?
- One Board Member with Cyber knowledge
- Board should have access to INDEPENDENT accessors

Investments in Cyber

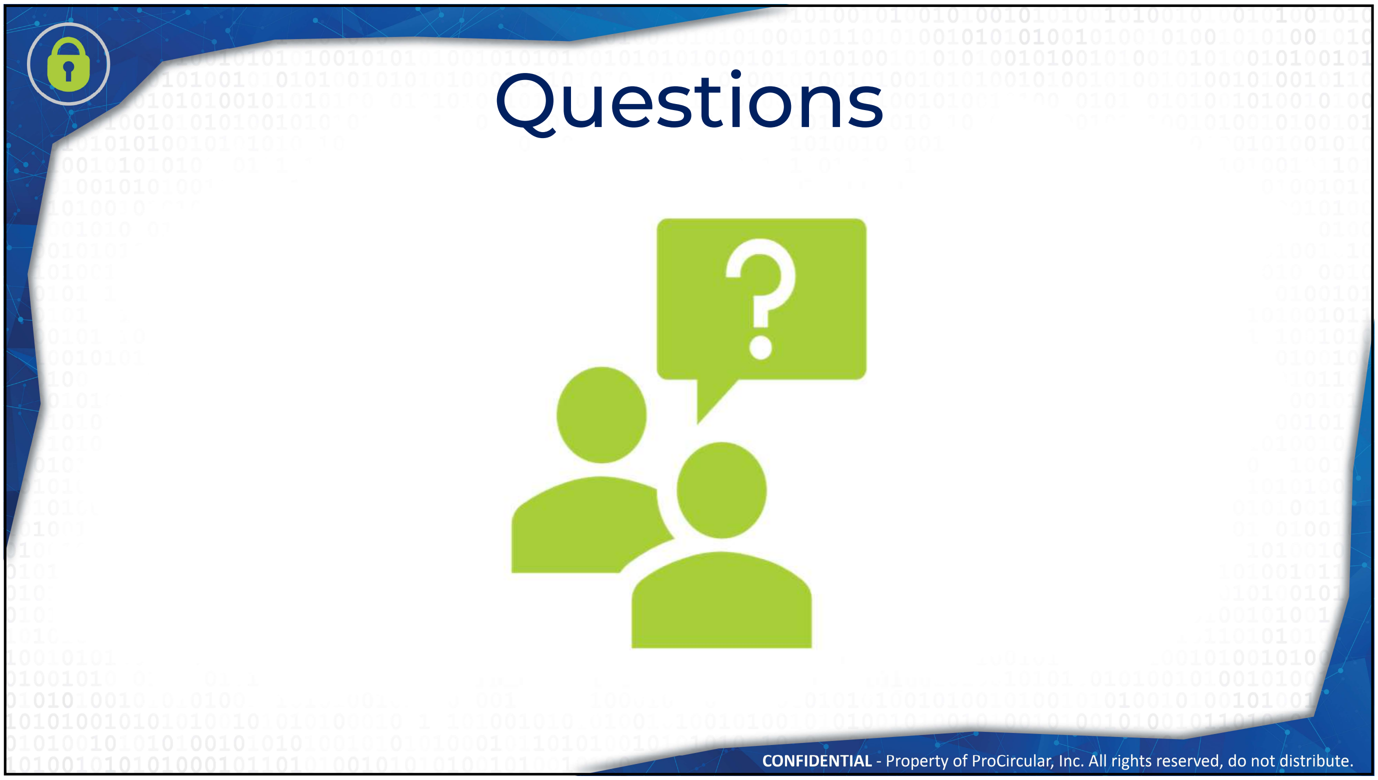
- Ask Board level questions
- Have a relationship with your Chief Information Security Officer
- 65% of board members think their org is at risk of cyber attack



Recap

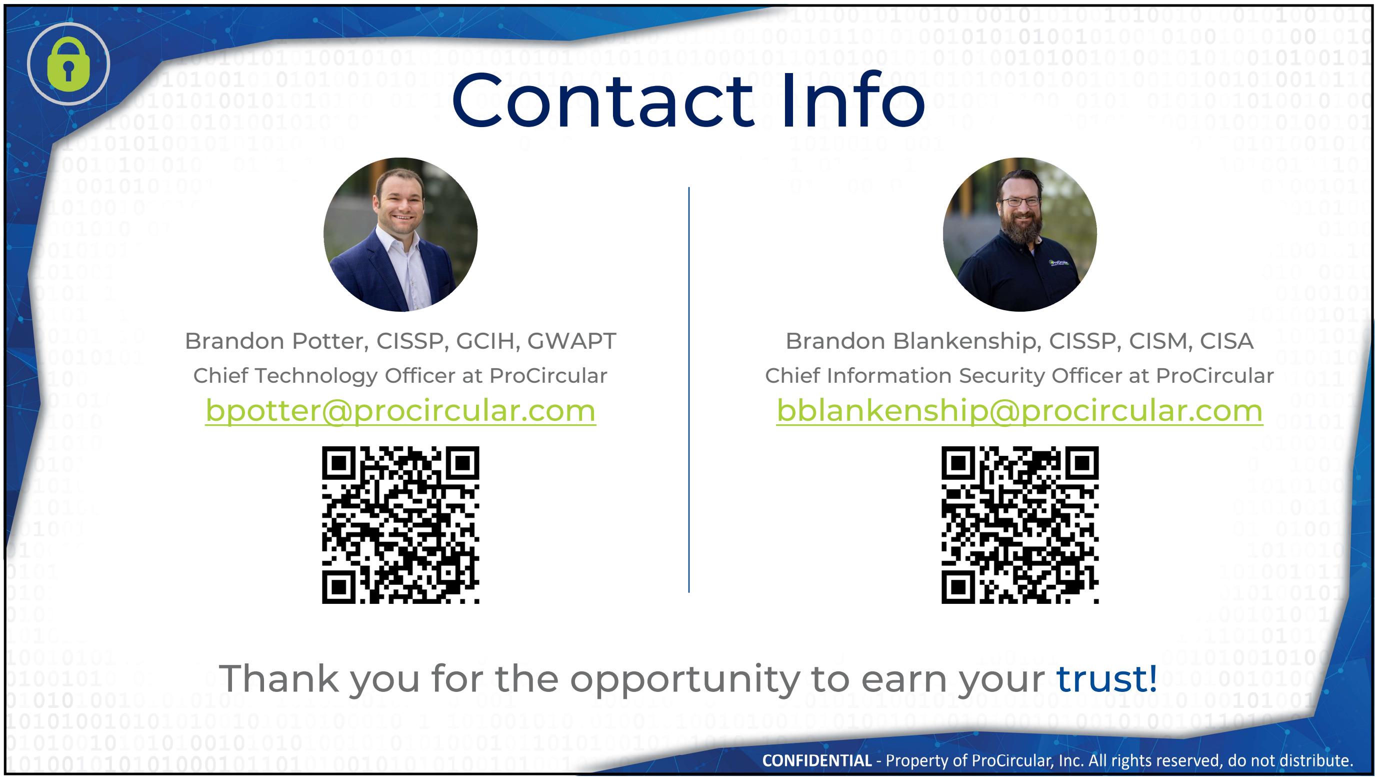
- Basic Cyber Hygiene
- Resilience > Recovery
- Top-down support and engagement is key
- Invest appropriately
- Cyber insurance as a last resort

31



Questions

32



Contact Info

Brandon Potter, CISSP, GCIH, GWAPT

Chief Technology Officer at ProCircular

bpotter@procircular.com

Brandon Blankenship, CISSP, CISM, CISA

Chief Information Security Officer at ProCircular

bblankenship@procircular.com

Thank you for the opportunity to earn your **trust!**

33