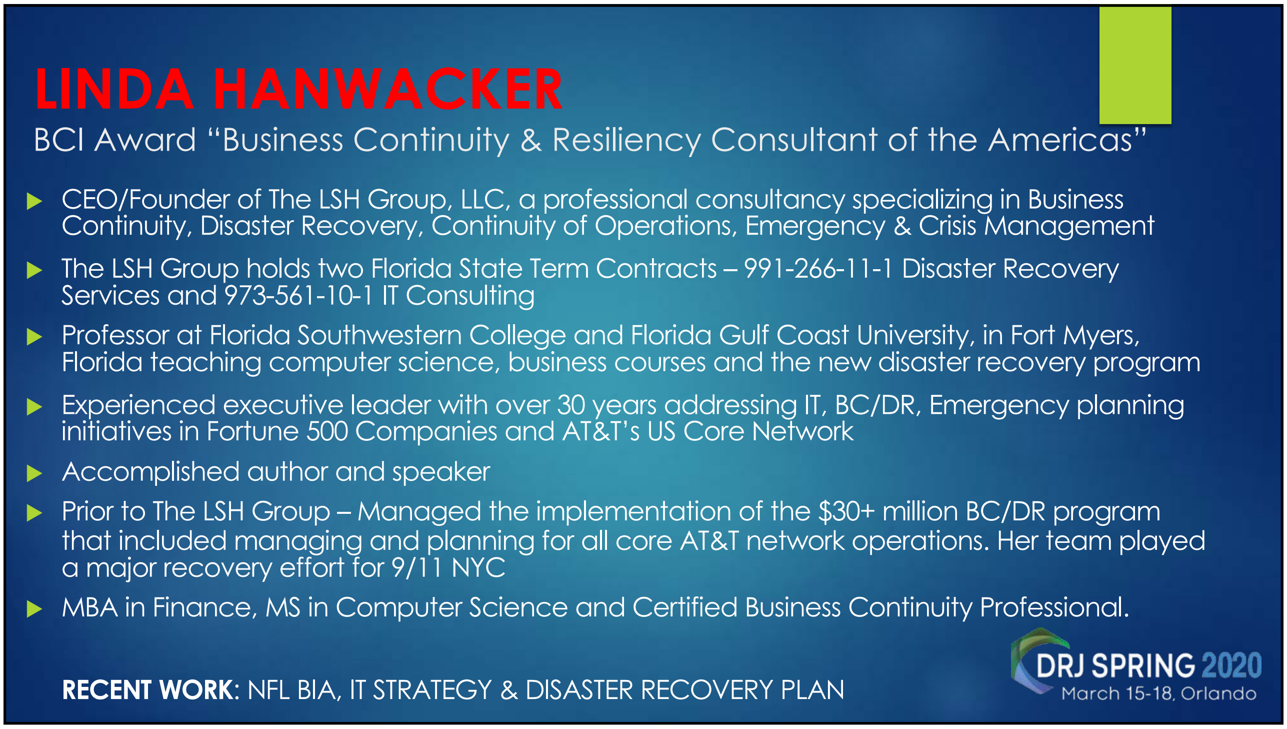
Interactive Workshop: Will You Be The Next Big Headline?

LINDA HANWACKER, MSCS. MBA, CBCP

DRJ SPRING 2020
March 15-18, Orlando

1



LINDA HANWACKER

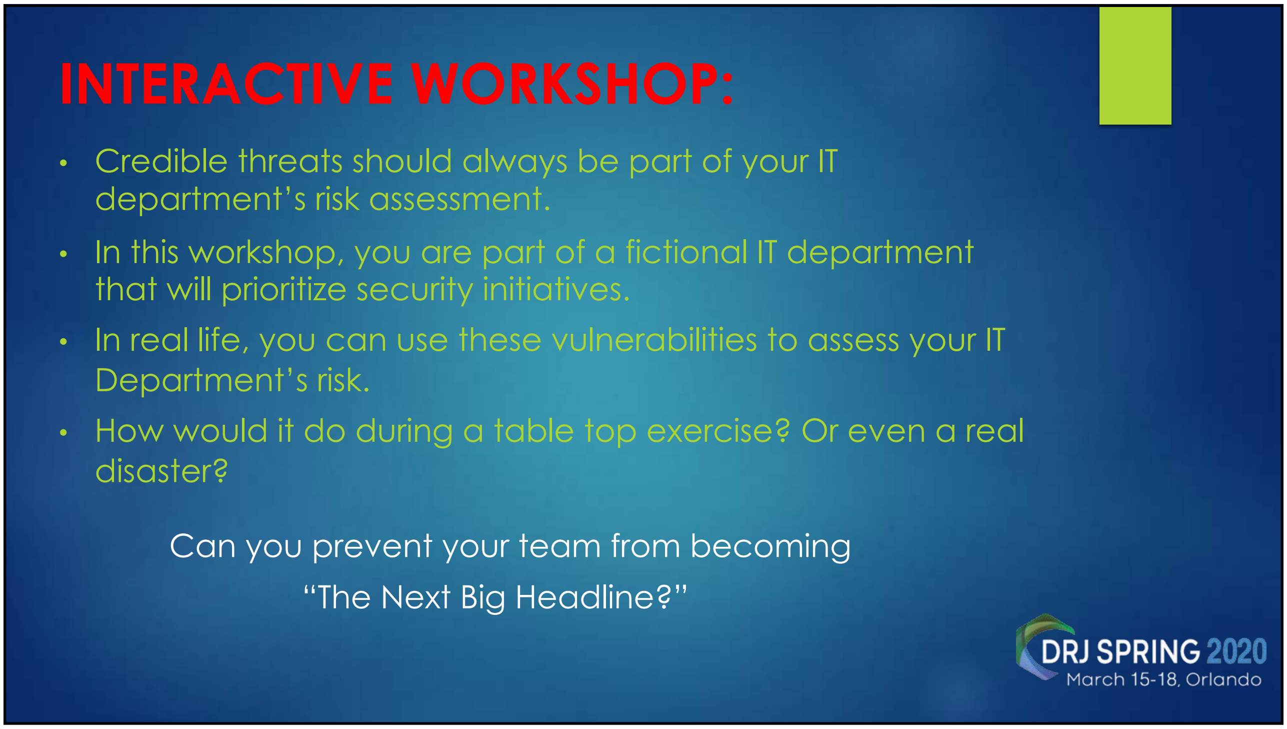
BCI Award "Business Continuity & Resiliency Consultant of the Americas"

- CEO/Founder of The LSH Group, LLC, a professional consultancy specializing in Business Continuity, Disaster Recovery, Continuity of Operations, Emergency & Crisis Management
- The LSH Group holds two Florida State Term Contracts – 991-266-11-1 Disaster Recovery Services and 973-561-10-1 IT Consulting
- Professor at Florida Southwestern College and Florida Gulf Coast University, in Fort Myers, Florida teaching computer science, business courses and the new disaster recovery program
- Experienced executive leader with over 30 years addressing IT, BC/DR, Emergency planning initiatives in Fortune 500 Companies and AT&T's US Core Network
- Accomplished author and speaker
- Prior to The LSH Group – Managed the implementation of the $30+ million BC/DR program that included managing and planning for all core AT&T network operations. Her team played a major recovery effort for 9/11 NYC
- MBA in Finance, MS in Computer Science and Certified Business Continuity Professional.

RECENT WORK: NFL BIA, IT STRATEGY & DISASTER RECOVERY PLAN

DRJ SPRING 2020
March 15-18, Orlando

2



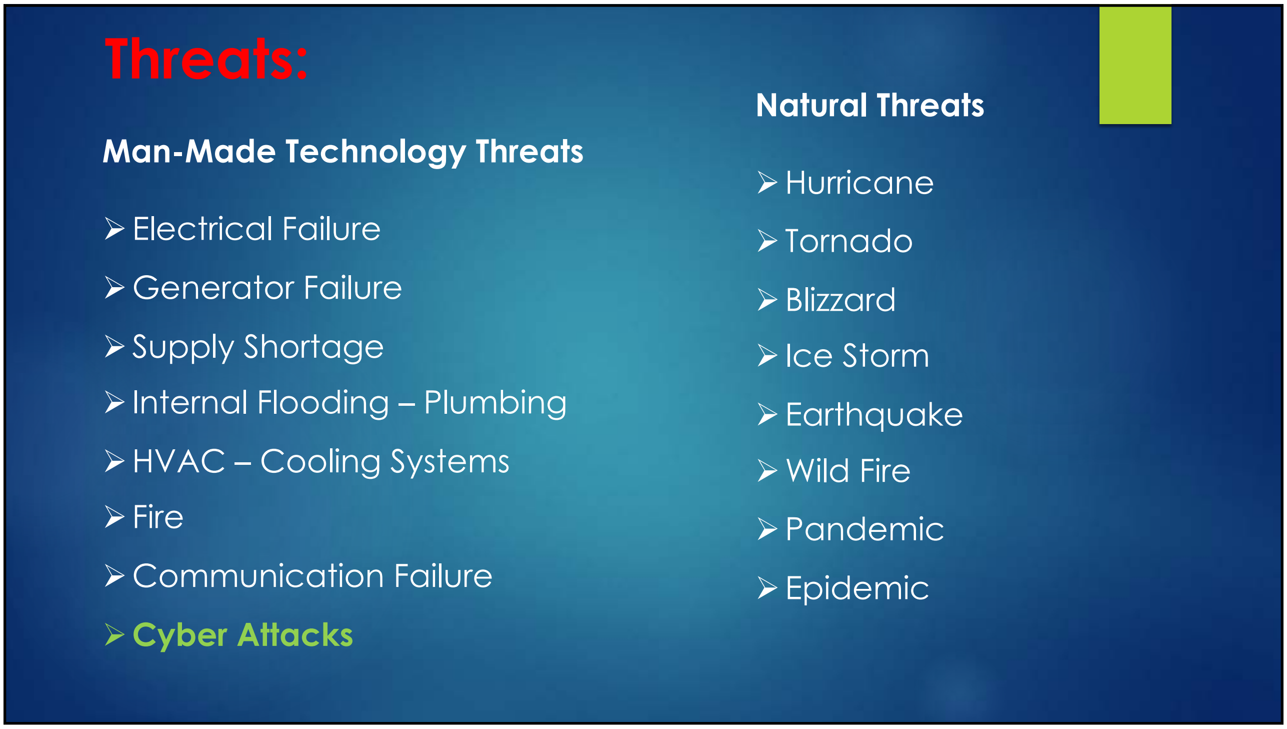
INTERACTIVE WORKSHOP:

- Credible threats should always be part of your IT department's risk assessment.
- In this workshop, you are part of a fictional IT department that will prioritize security initiatives.
- In real life, you can use these vulnerabilities to assess your IT Department's risk.
- How would it do during a table top exercise? Or even a real disaster?

Can you prevent your team from becoming
"The Next Big Headline?"

DRJ SPRING 2020
March 15-18, Orlando

3



Threats:

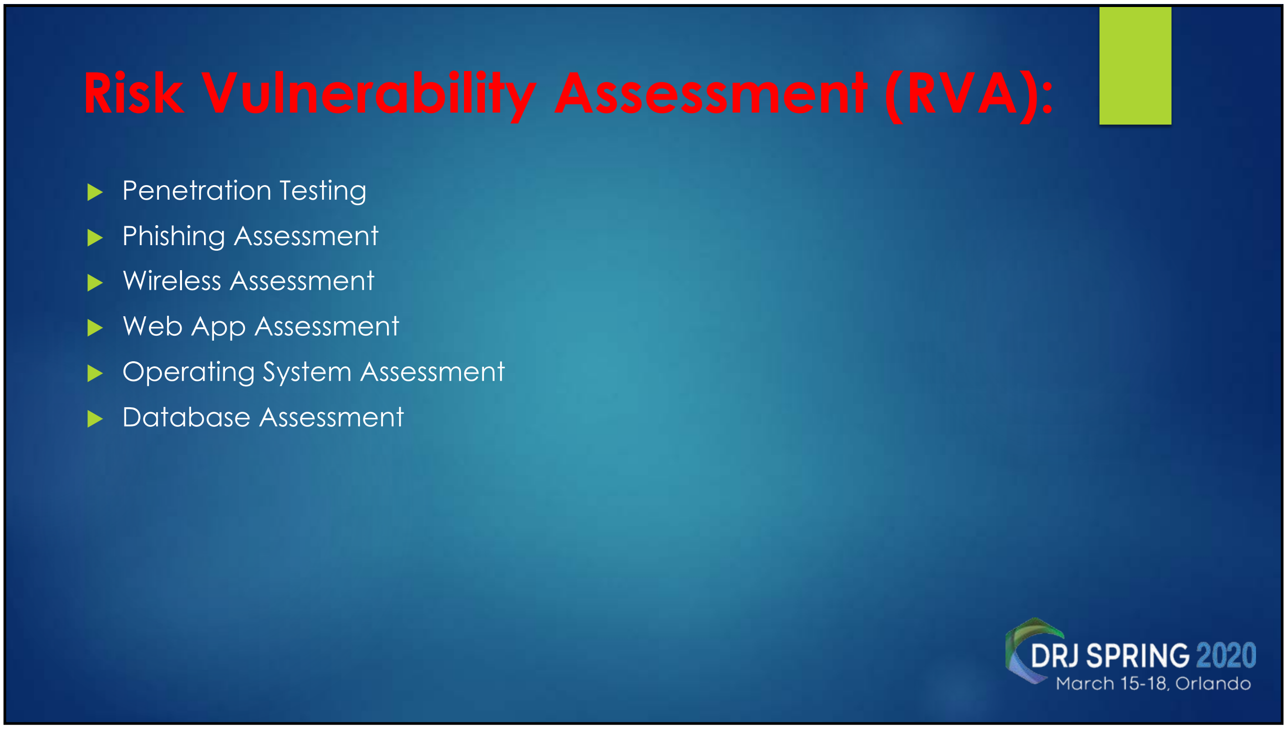
Man-Made Technology Threats

- ➢ Electrical Failure
- ➢ Generator Failure
- ➢ Supply Shortage
- ➢ Internal Flooding – Plumbing
- ➢ HVAC – Cooling Systems
- ➢ Fire
- ➢ Communication Failure
- ➢ **Cyber Attacks**

Natural Threats

- ➢ Hurricane
- ➢ Tornado
- ➢ Blizzard
- ➢ Ice Storm
- ➢ Earthquake
- ➢ Wild Fire
- ➢ Pandemic
- ➢ Epidemic

4

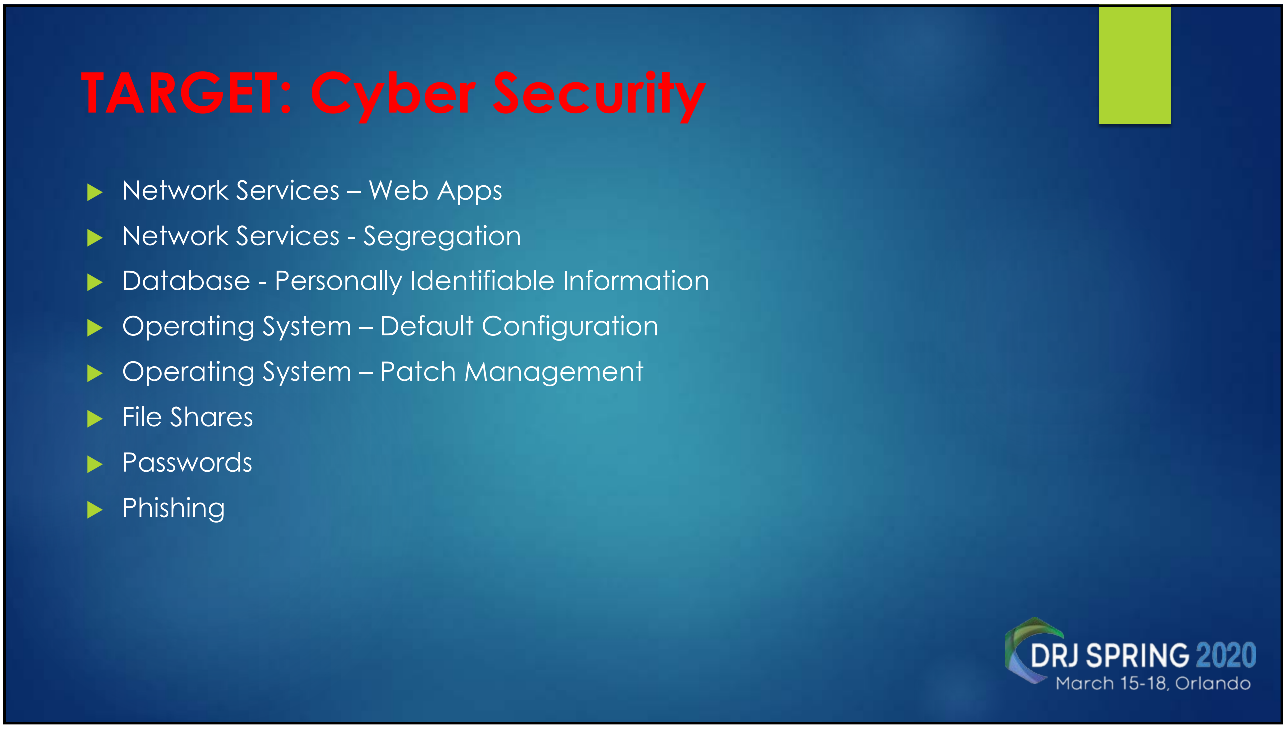


Risk Vulnerability Assessment (RVA):

- Penetration Testing
- Phishing Assessment
- Wireless Assessment
- Web App Assessment
- Operating System Assessment
- Database Assessment

DRJ SPRING 2020
March 15-18, Orlando

5

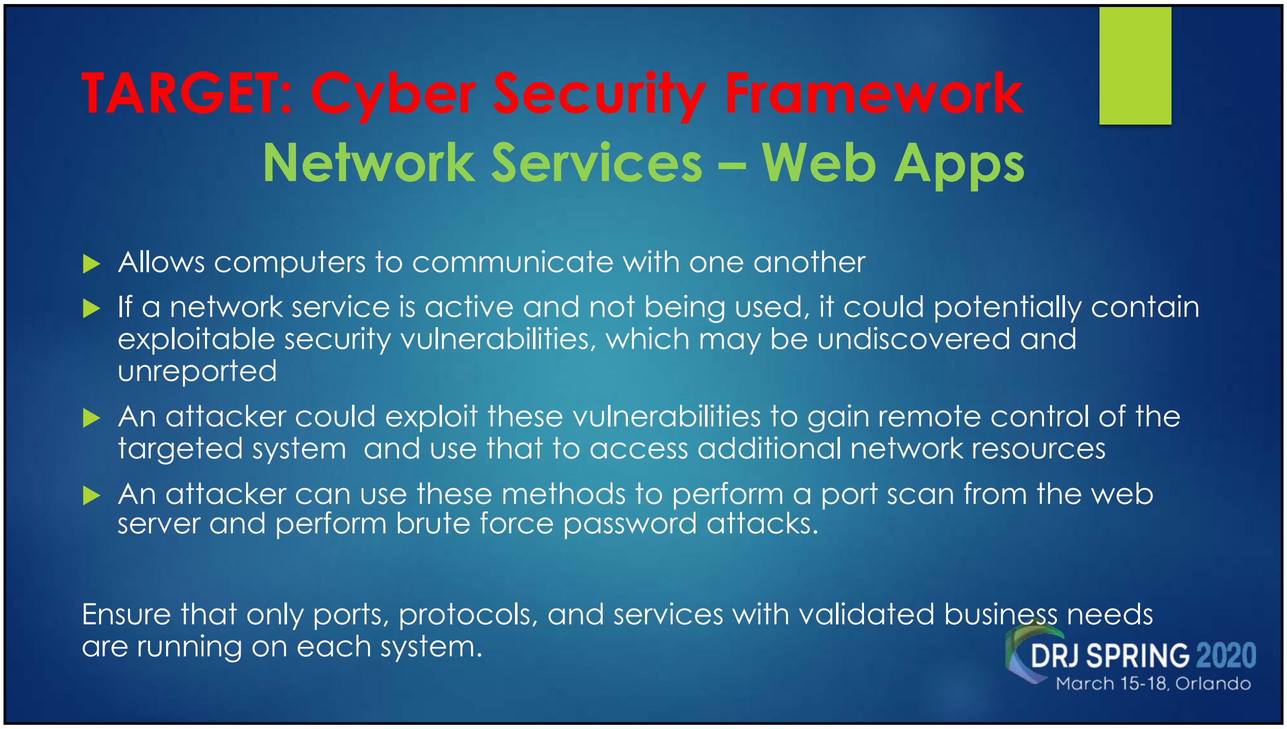


TARGET: Cyber Security

- Network Services – Web Apps
- Network Services - Segregation
- Database - Personally Identifiable Information
- Operating System – Default Configuration
- Operating System – Patch Management
- File Shares
- Passwords
- Phishing

DRJ SPRING 2020
March 15-18, Orlando

6



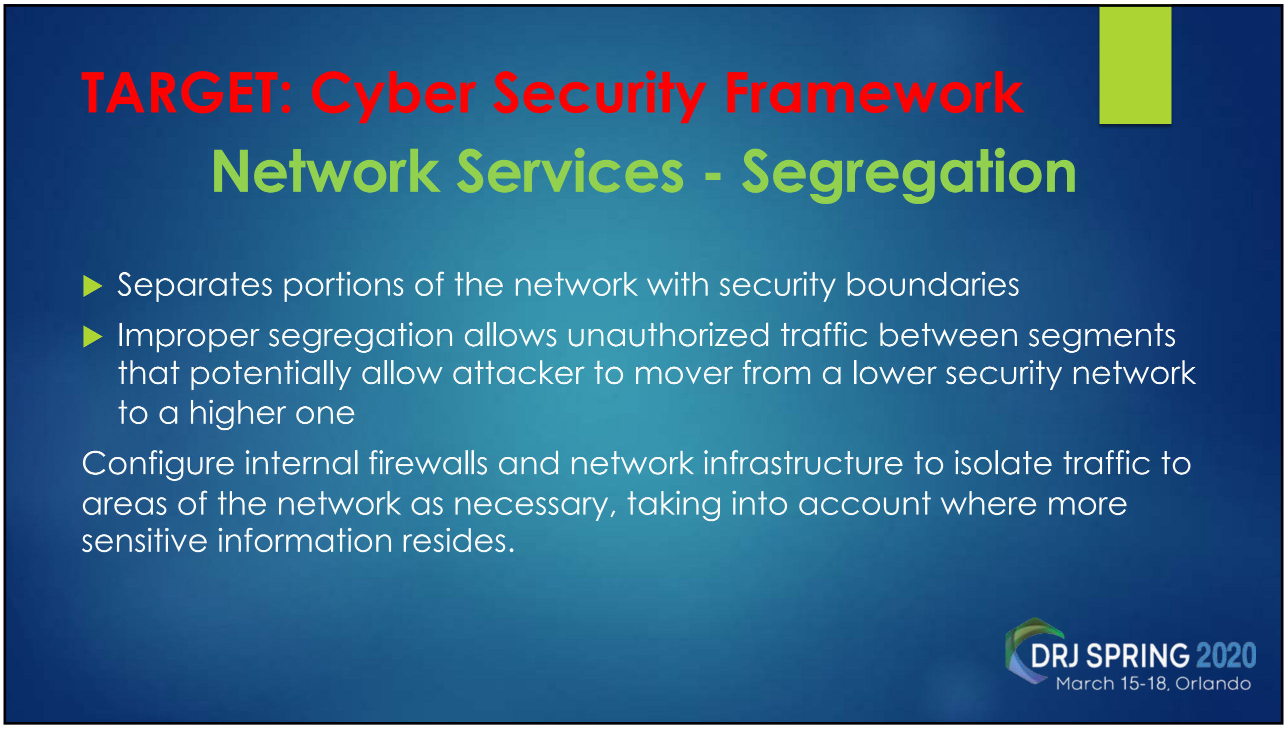
TARGET: Cyber Security Framework
Network Services – Web Apps

- Allows computers to communicate with one another
- If a network service is active and not being used, it could potentially contain exploitable security vulnerabilities, which may be undiscovered and unreported
- An attacker could exploit these vulnerabilities to gain remote control of the targeted system and use that to access additional network resources
- An attacker can use these methods to perform a port scan from the web server and perform brute force password attacks.

Ensure that only ports, protocols, and services with validated business needs are running on each system.

DRJ SPRING 2020
March 15-18, Orlando

7



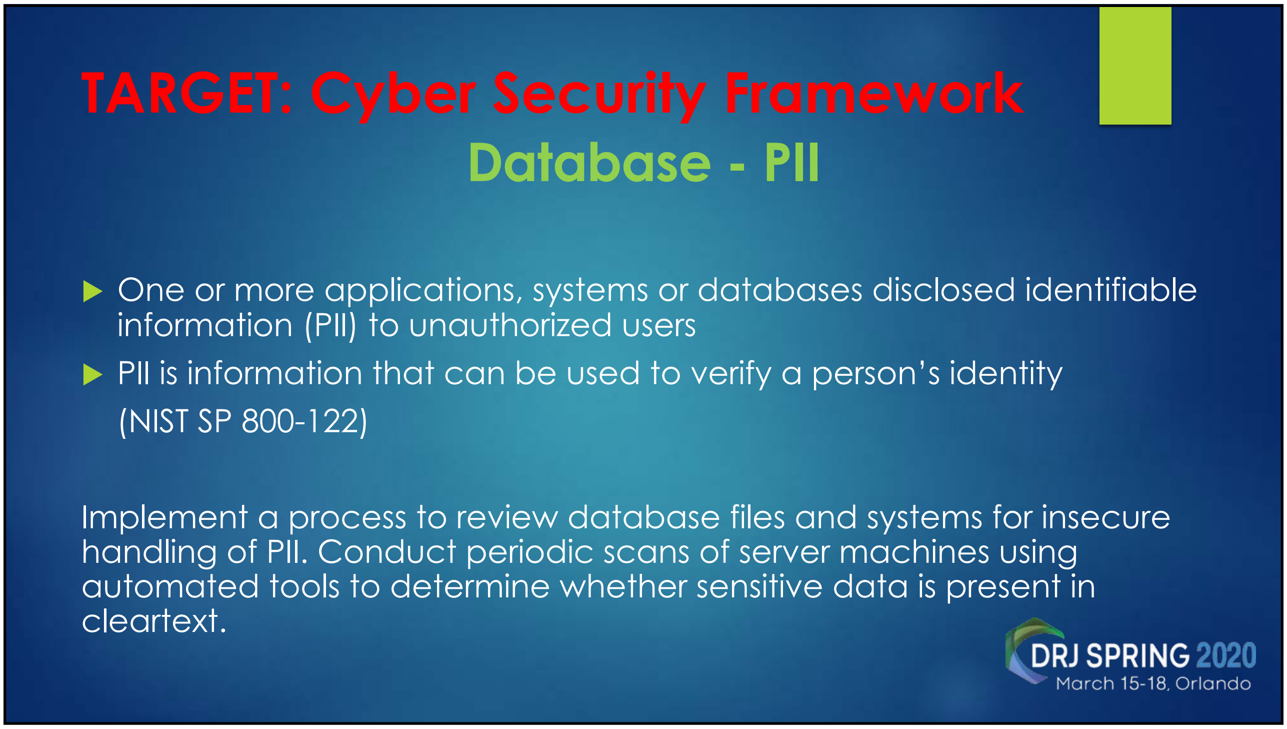
TARGET: Cyber Security Framework
Network Services - Segregation

- Separates portions of the network with security boundaries
- Improper segregation allows unauthorized traffic between segments that potentially allow attacker to mover from a lower security network to a higher one

Configure internal firewalls and network infrastructure to isolate traffic to areas of the network as necessary, taking into account where more sensitive information resides.

DRJ SPRING 2020
March 15-18, Orlando

8



TARGET: Cyber Security Framework

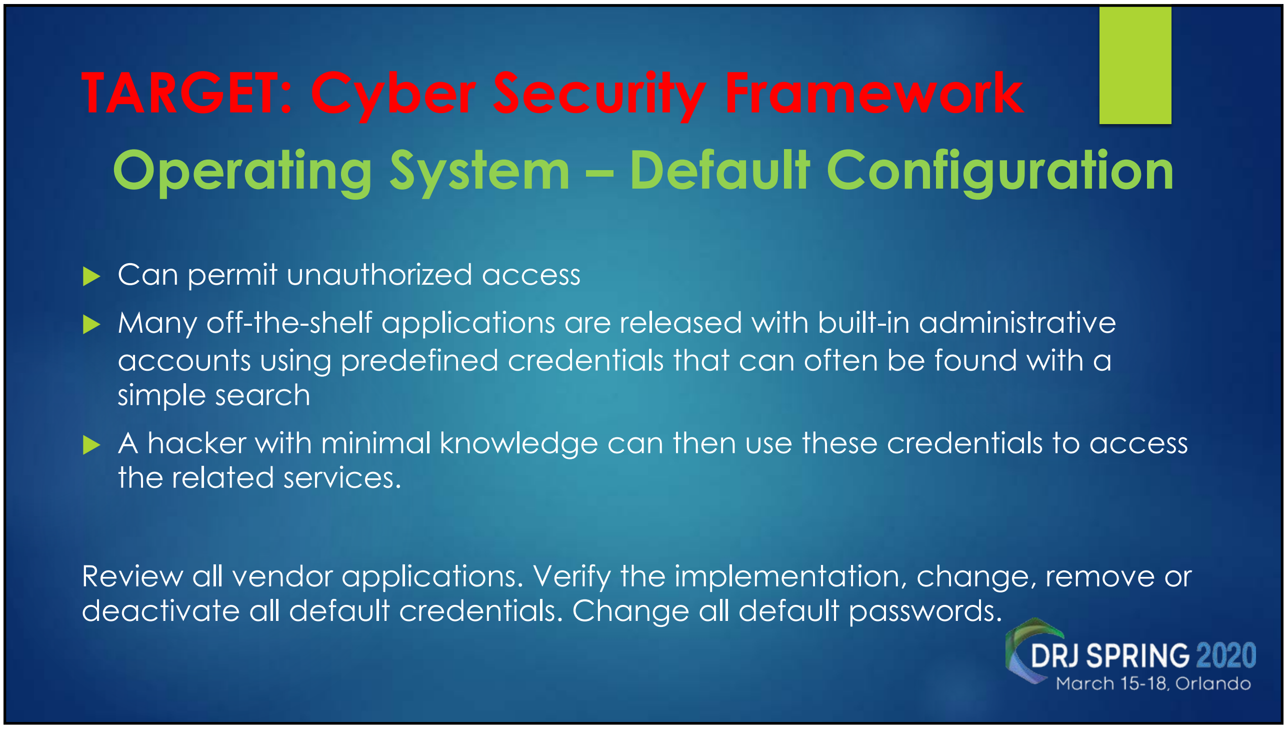
Database - PII

- One or more applications, systems or databases disclosed identifiable information (PII) to unauthorized users
- PII is information that can be used to verify a person's identity (NIST SP 800-122)

Implement a process to review database files and systems for insecure handling of PII. Conduct periodic scans of server machines using automated tools to determine whether sensitive data is present in cleartext.

DRJ SPRING 2020
March 15-18, Orlando

9



TARGET: Cyber Security Framework

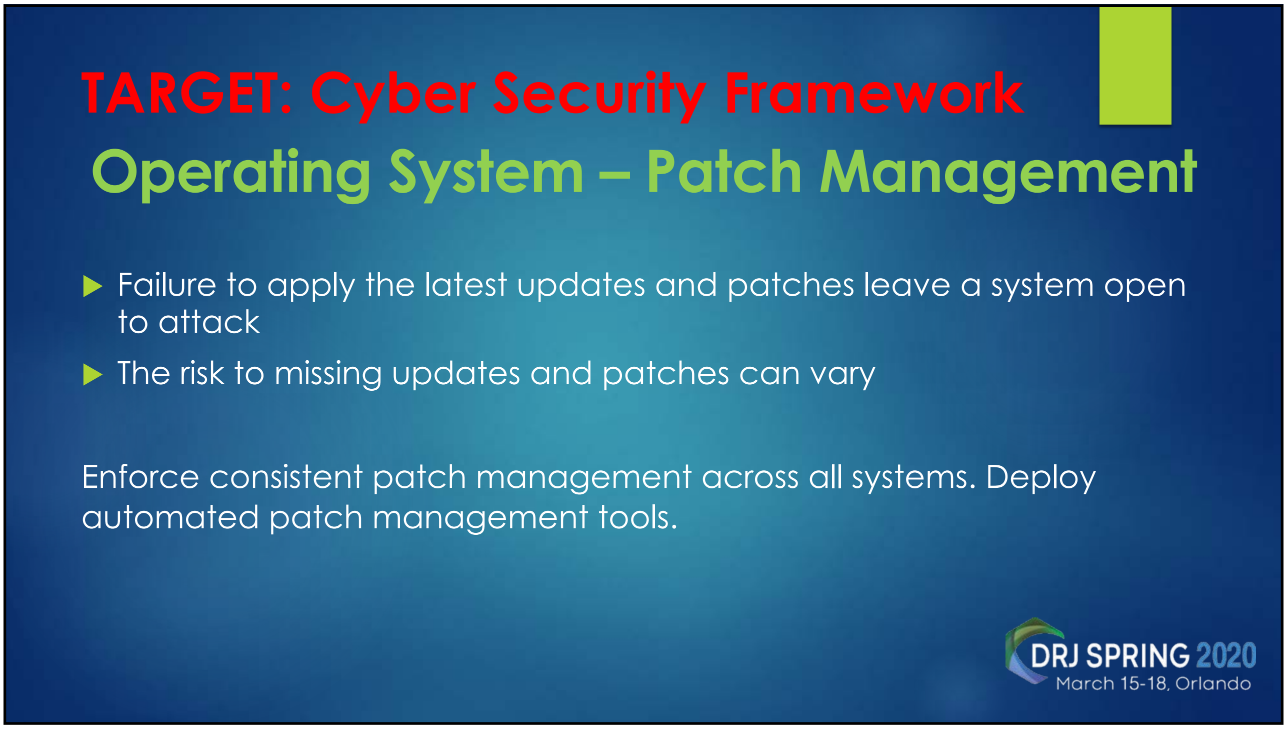
Operating System – Default Configuration

- Can permit unauthorized access
- Many off-the-shelf applications are released with built-in administrative accounts using predefined credentials that can often be found with a simple search
- A hacker with minimal knowledge can then use these credentials to access the related services.

Review all vendor applications. Verify the implementation, change, remove or deactivate all default credentials. Change all default passwords.

DRJ SPRING 2020
March 15-18, Orlando

10



TARGET: Cyber Security Framework

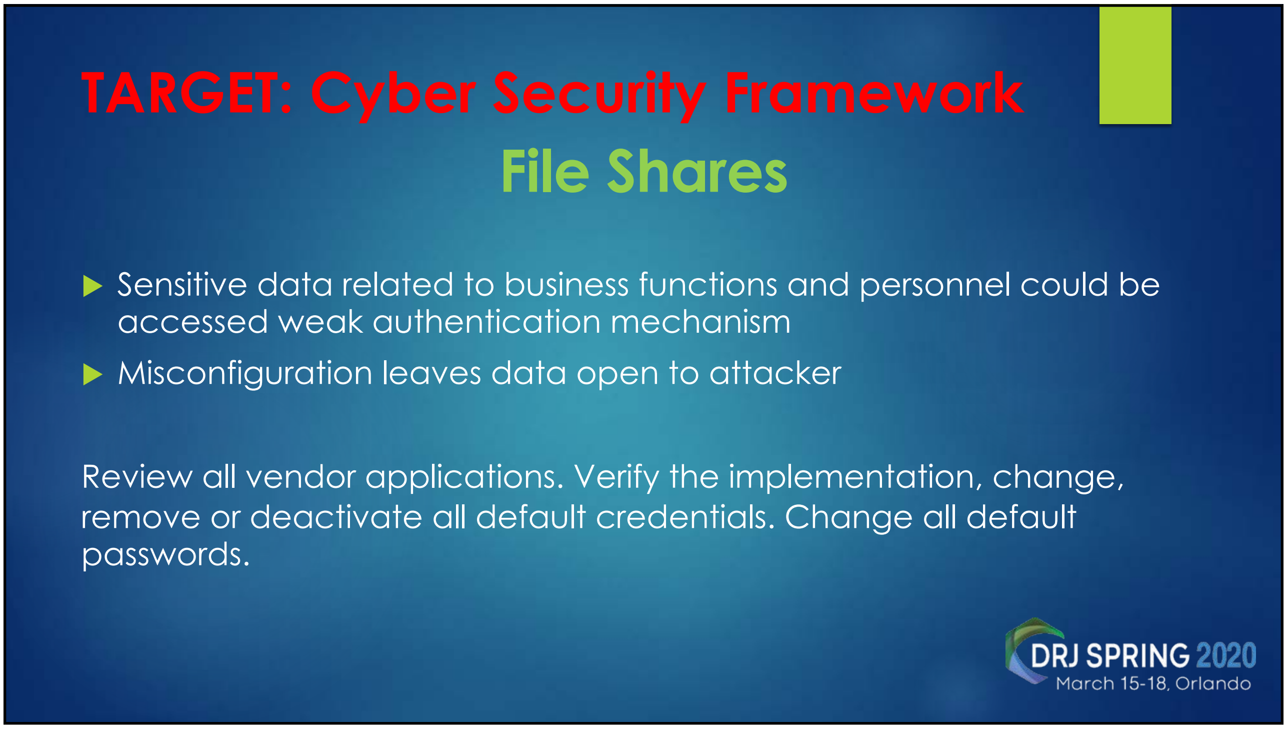
Operating System – Patch Management

- Failure to apply the latest updates and patches leave a system open to attack
- The risk to missing updates and patches can vary

Enforce consistent patch management across all systems. Deploy automated patch management tools.

DRJ SPRING 2020
March 15-18, Orlando

11



TARGET: Cyber Security Framework

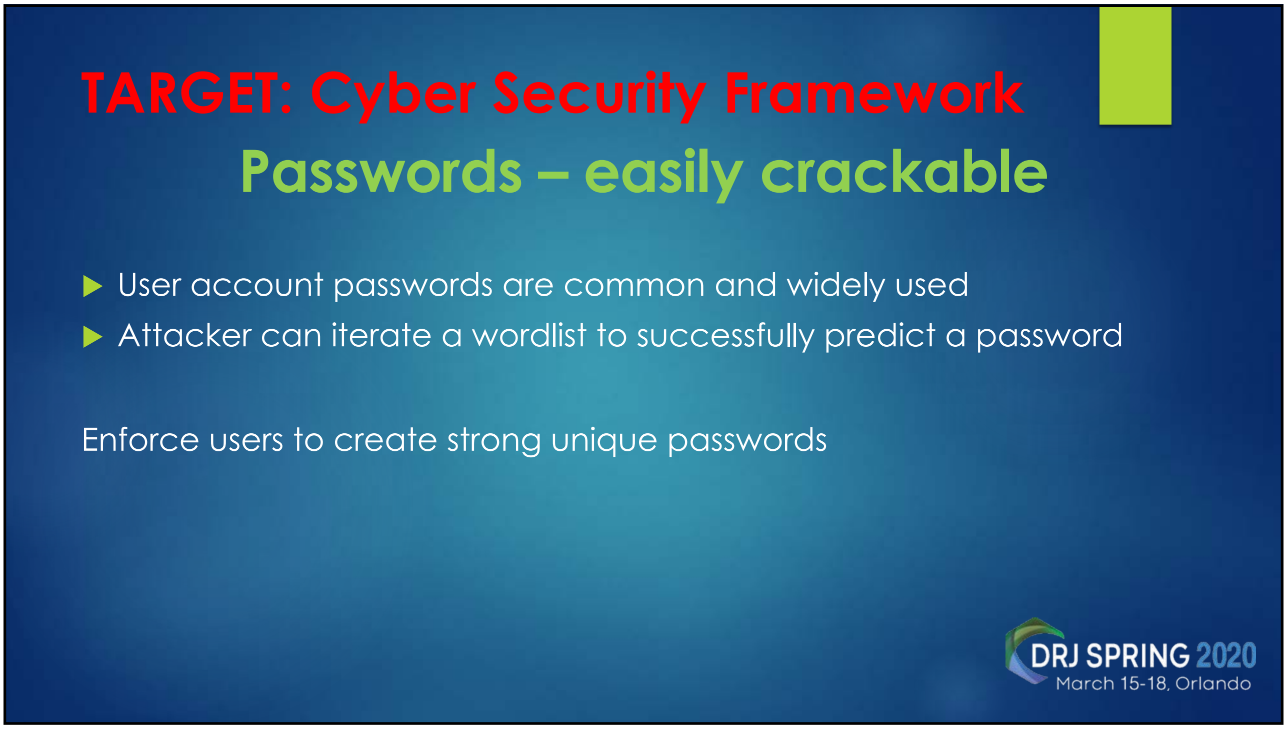
File Shares

- Sensitive data related to business functions and personnel could be accessed weak authentication mechanism
- Misconfiguration leaves data open to attacker

Review all vendor applications. Verify the implementation, change, remove or deactivate all default credentials. Change all default passwords.

DRJ SPRING 2020
March 15-18, Orlando

12



TARGET: Cyber Security Framework

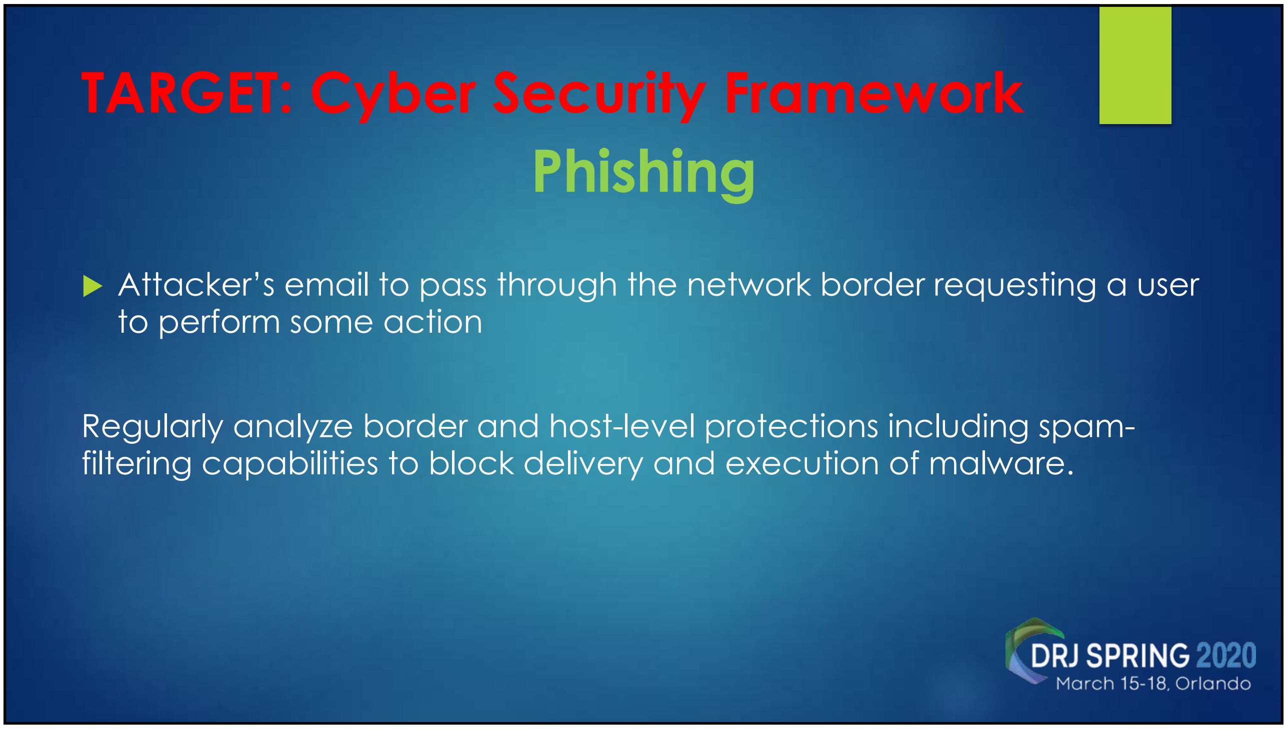
Passwords – easily crackable

- User account passwords are common and widely used
- Attacker can iterate a wordlist to successfully predict a password

Enforce users to create strong unique passwords

DRJ SPRING 2020
March 15-18, Orlando

13



TARGET: Cyber Security Framework

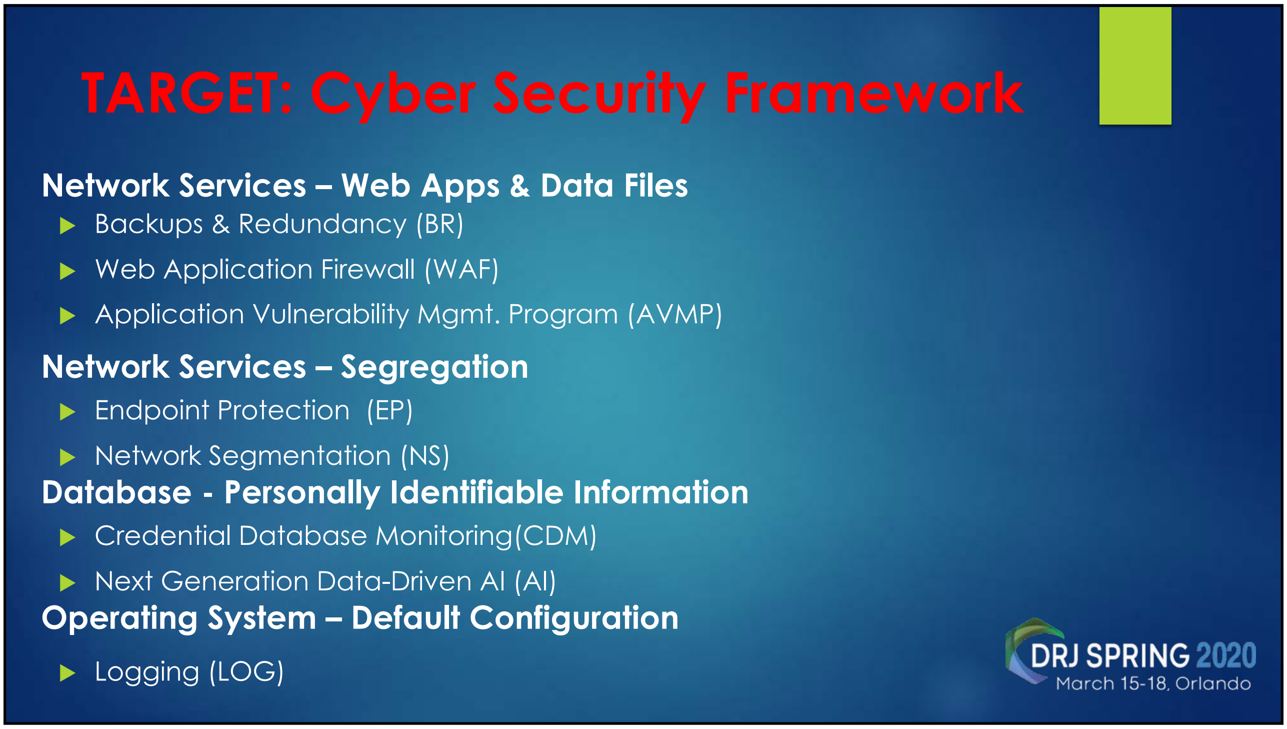
Phishing

- Attacker's email to pass through the network border requesting a user to perform some action

Regularly analyze border and host-level protections including spam-filtering capabilities to block delivery and execution of malware.

DRJ SPRING 2020
March 15-18, Orlando

14



TARGET: Cyber Security Framework

Network Services – Web Apps & Data Files

- Backups & Redundancy (BR)
- Web Application Firewall (WAF)
- Application Vulnerability Mgmt. Program (AVMP)

Network Services – Segregation

- Endpoint Protection (EP)
- Network Segmentation (NS)

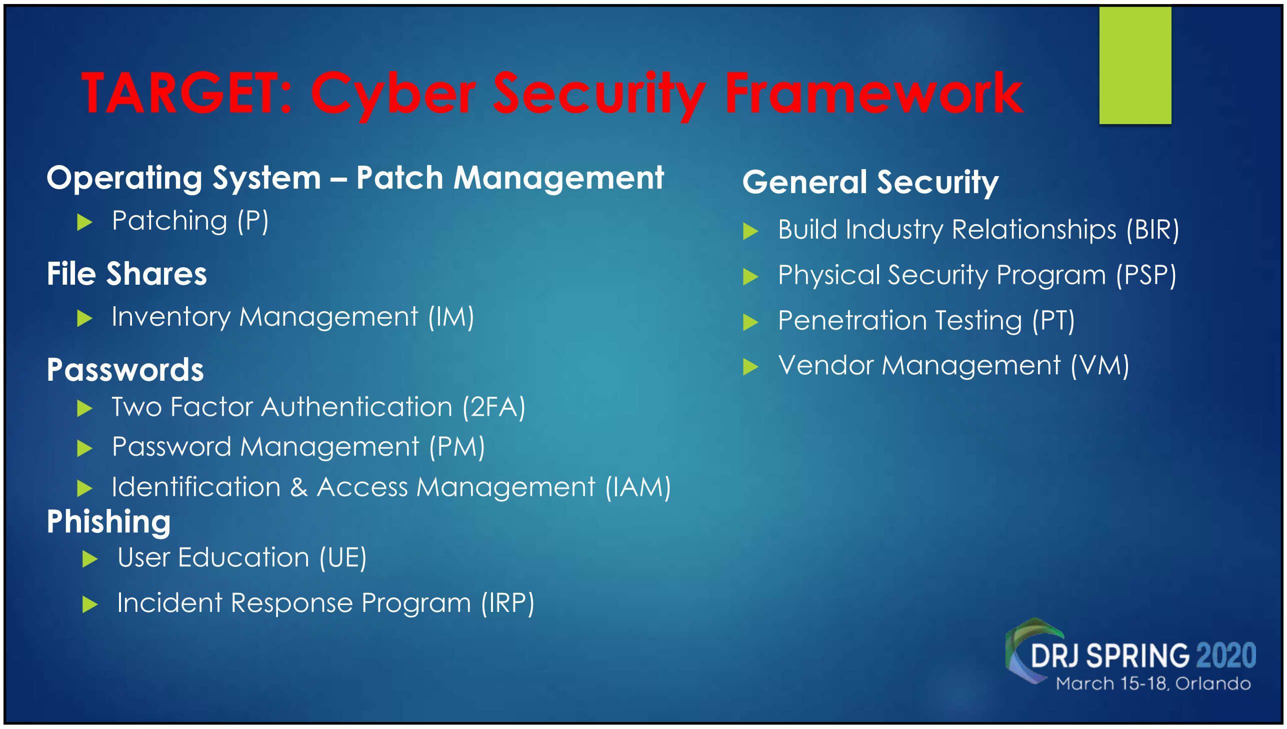
Database - Personally Identifiable Information

- Credential Database Monitoring(CDM)
- Next Generation Data-Driven AI (AI)

Operating System – Default Configuration

- Logging (LOG)

DRJ SPRING 2020
March 15-18, Orlando



TARGET: Cyber Security Framework

Operating System – Patch Management

- Patching (P)

File Shares

- Inventory Management (IM)

Passwords

- Two Factor Authentication (2FA)
- Password Management (PM)
- Identification & Access Management (IAM)

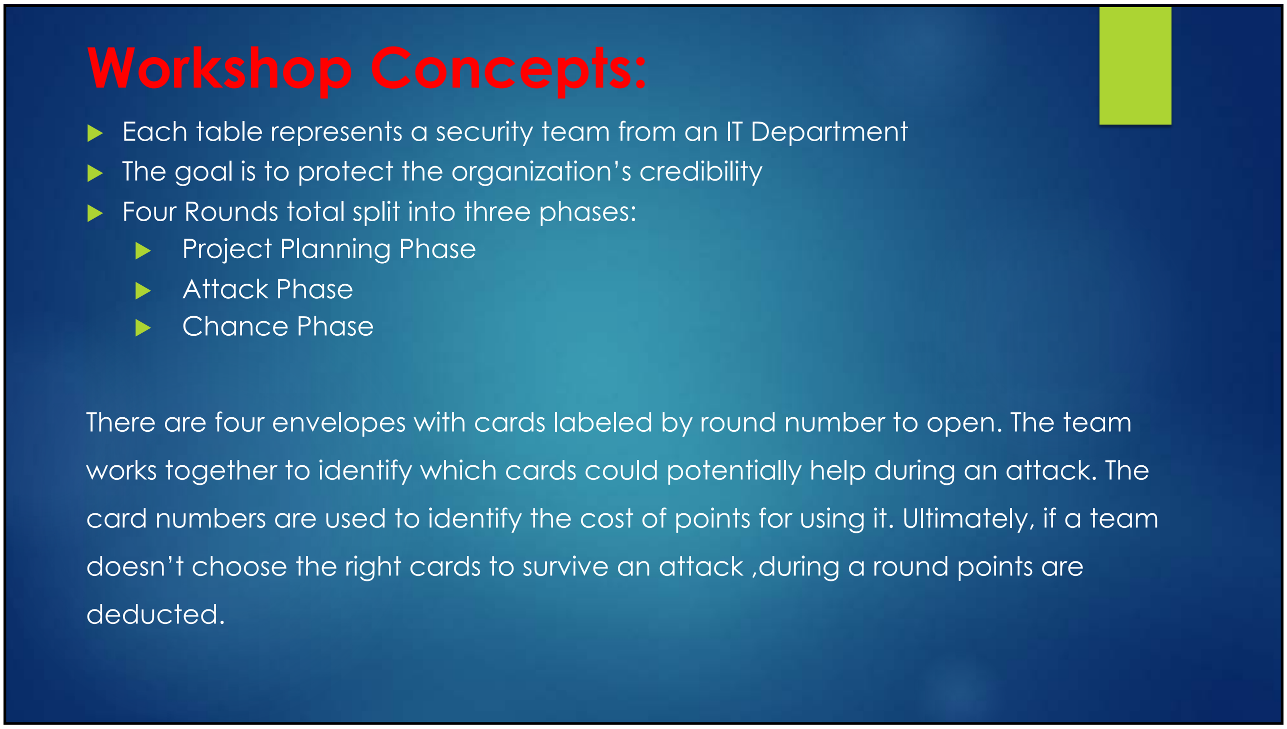
Phishing

- User Education (UE)
- Incident Response Program (IRP)

General Security

- Build Industry Relationships (BIR)
- Physical Security Program (PSP)
- Penetration Testing (PT)
- Vendor Management (VM)

DRJ SPRING 2020
March 15-18, Orlando

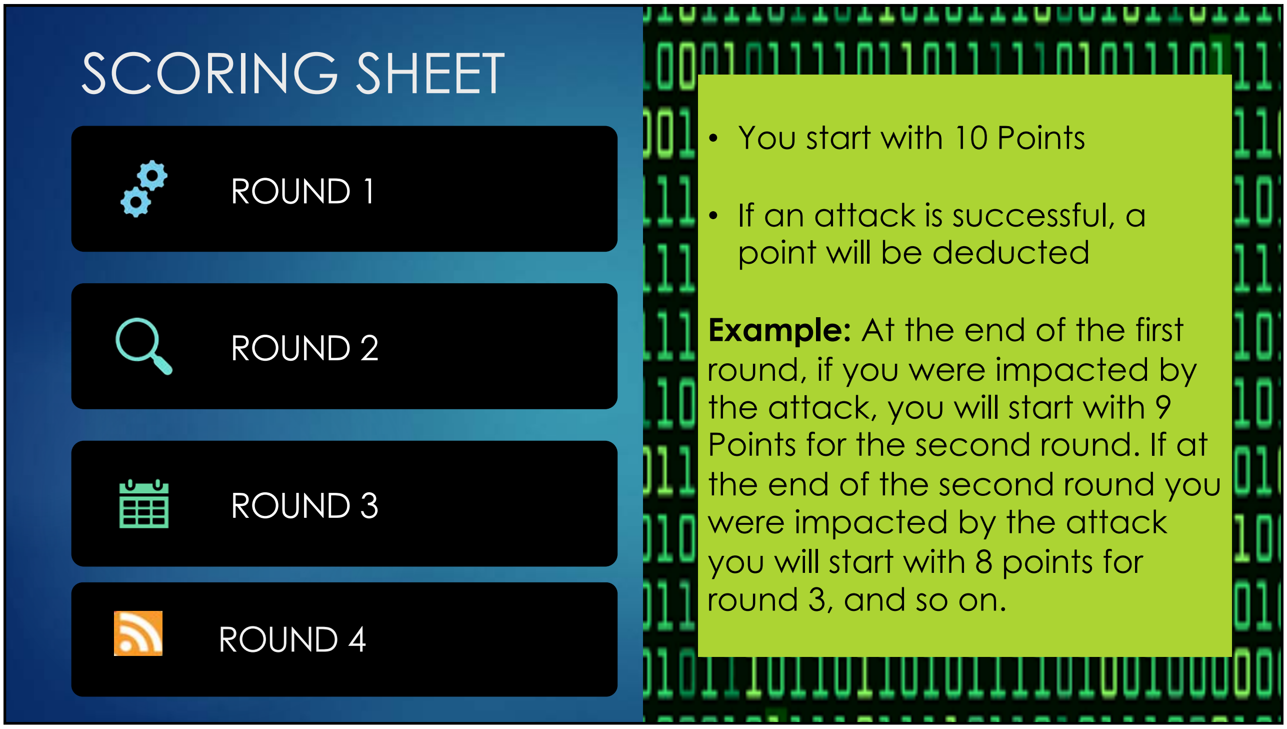


Workshop Concepts:

- Each table represents a security team from an IT Department
- The goal is to protect the organization's credibility
- Four Rounds total split into three phases:
  - Project Planning Phase
  - Attack Phase
  - Chance Phase

There are four envelopes with cards labeled by round number to open. The team works together to identify which cards could potentially help during an attack. The card numbers are used to identify the cost of points for using it. Ultimately, if a team doesn't choose the right cards to survive an attack ,during a round points are deducted.

17



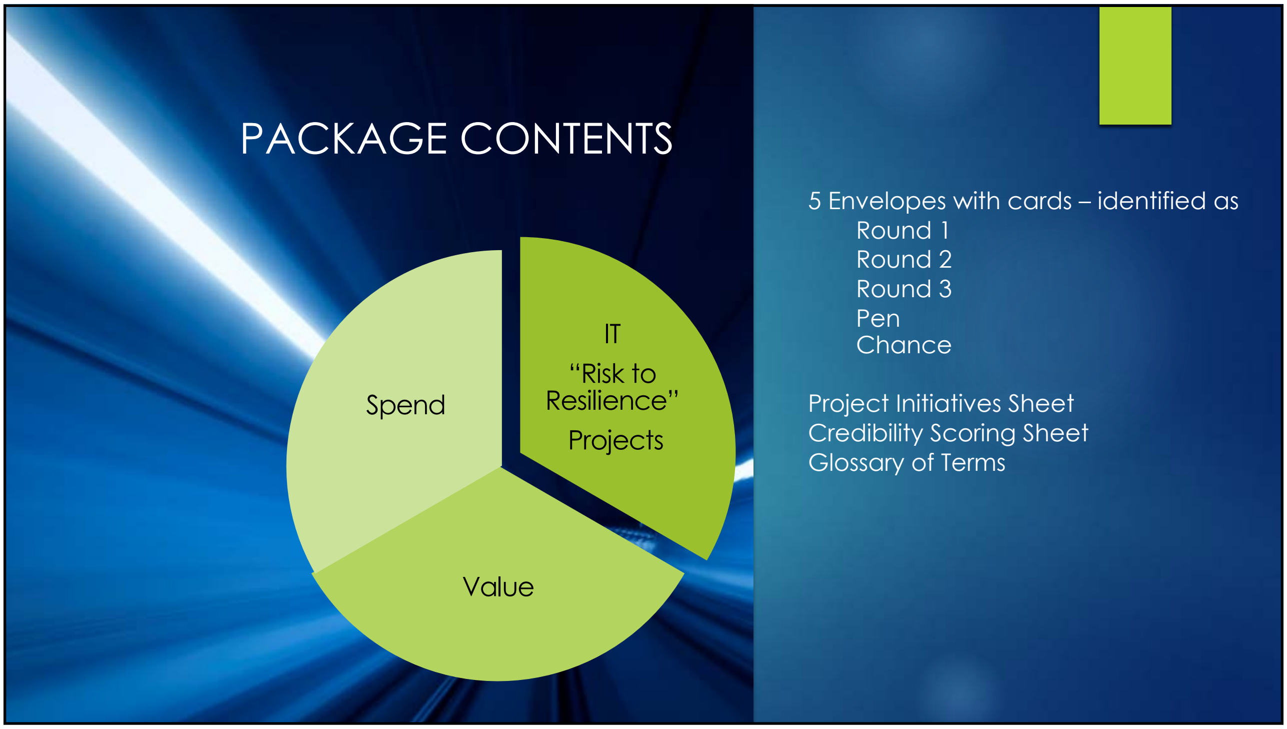
SCORING SHEET

- ROUND 1
- ROUND 2
- ROUND 3
- ROUND 4

- You start with 10 Points
- If an attack is successful, a point will be deducted

Example: At the end of the first round, if you were impacted by the attack, you will start with 9 Points for the second round. If at the end of the second round you were impacted by the attack you will start with 8 points for round 3, and so on.

18



PACKAGE CONTENTS

Spend

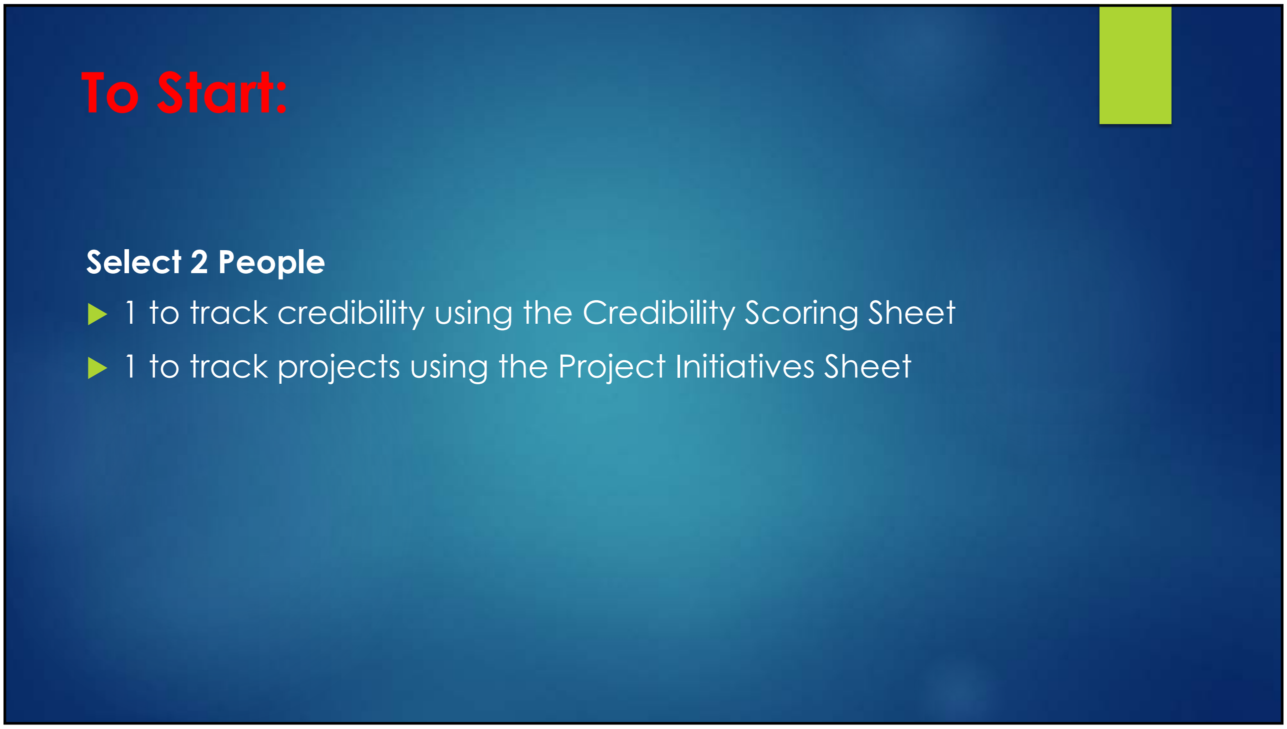
IT
"Risk to Resilience"
Projects

Value

5 Envelopes with cards – identified as
- Round 1
- Round 2
- Round 3
- Pen
- Chance

Project Initiatives Sheet
Credibility Scoring Sheet
Glossary of Terms

19

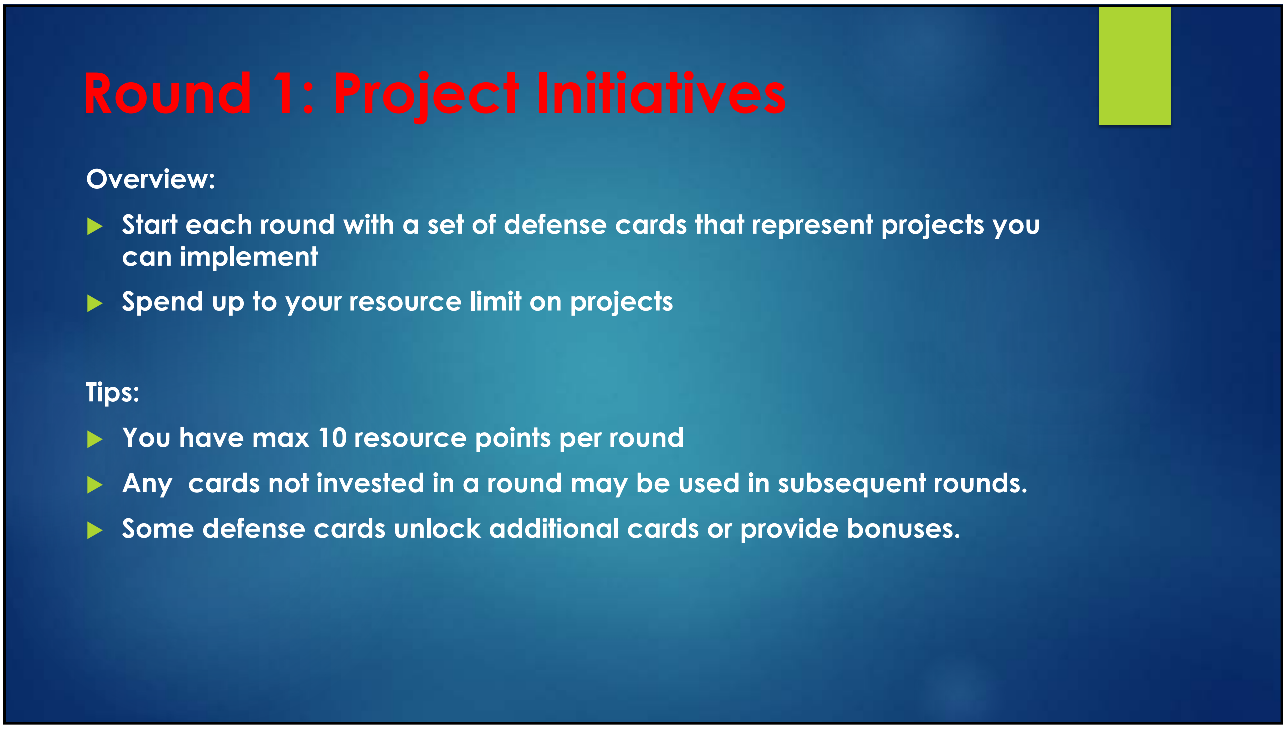


To Start:

Select 2 People

- 1 to track credibility using the Credibility Scoring Sheet
- 1 to track projects using the Project Initiatives Sheet

20



Round 1: Project Initiatives

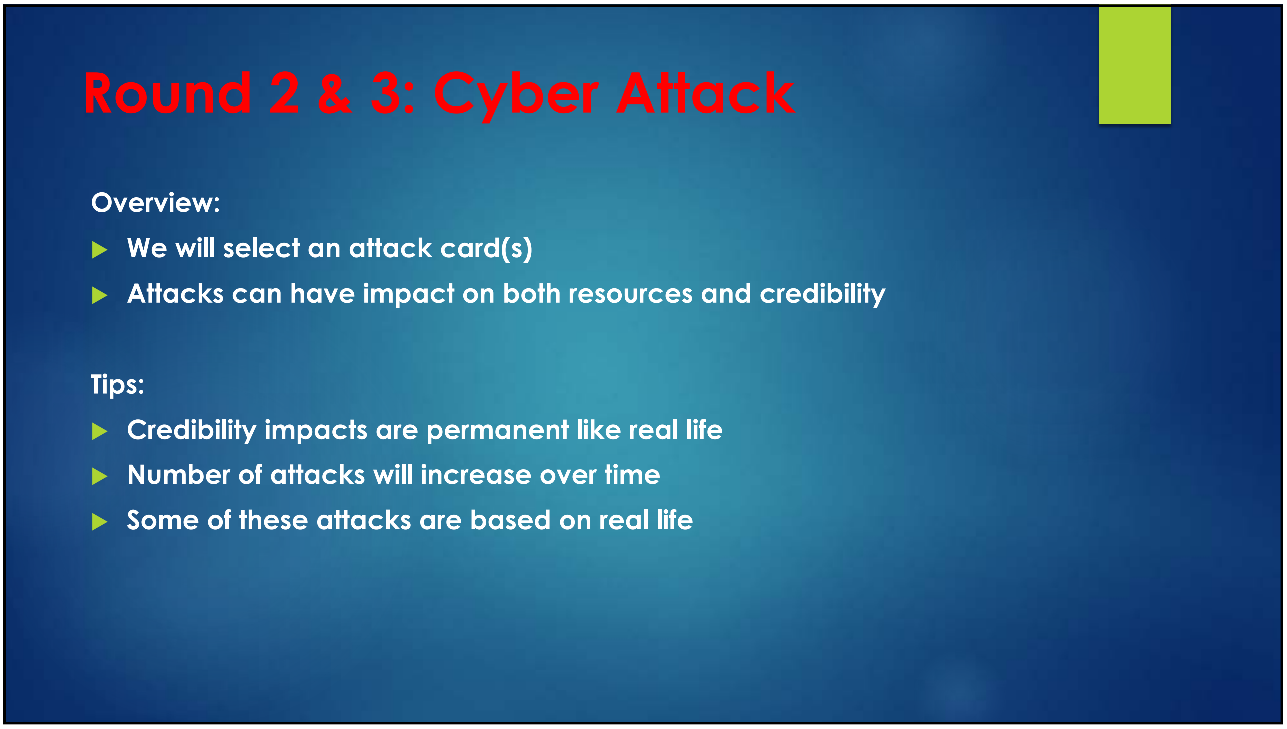
Overview:

- Start each round with a set of defense cards that represent projects you can implement
- Spend up to your resource limit on projects

Tips:

- You have max 10 resource points per round
- Any cards not invested in a round may be used in subsequent rounds.
- Some defense cards unlock additional cards or provide bonuses.

21



Round 2 & 3: Cyber Attack

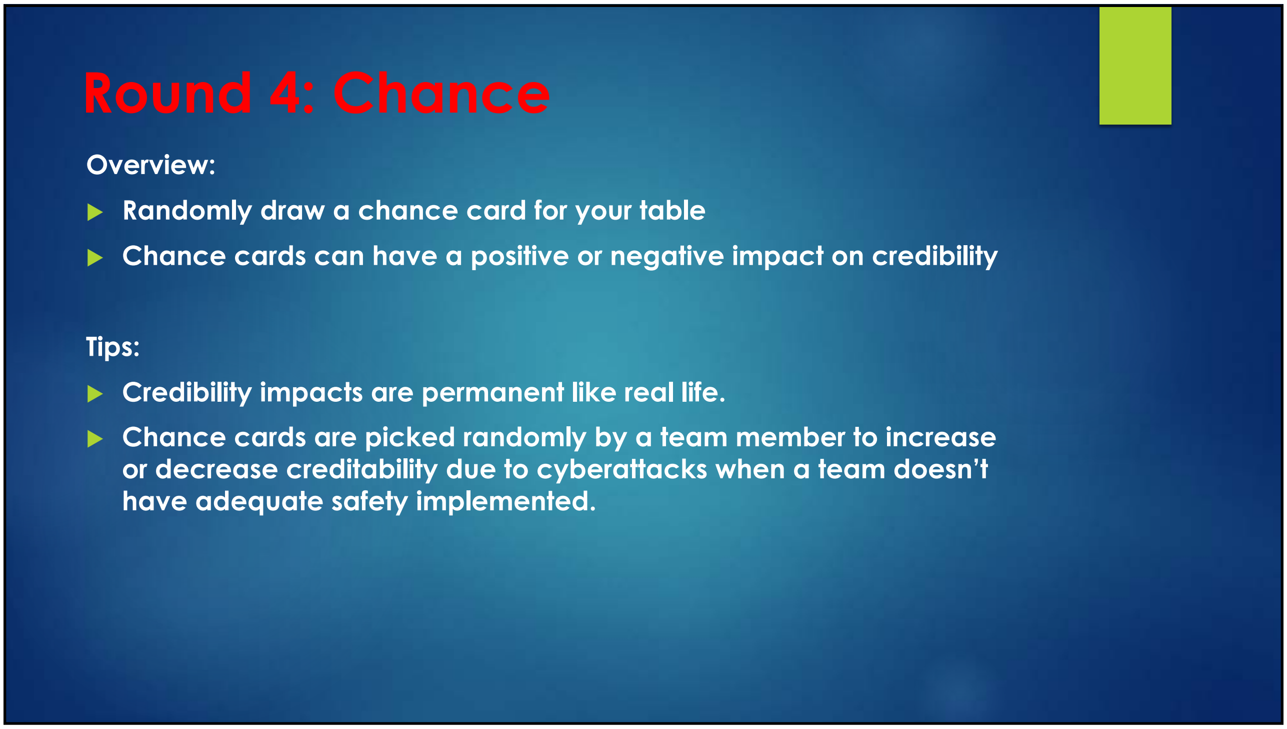
Overview:

- We will select an attack card(s)
- Attacks can have impact on both resources and credibility

Tips:

- Credibility impacts are permanent like real life
- Number of attacks will increase over time
- Some of these attacks are based on real life

22



Round 4: Chance

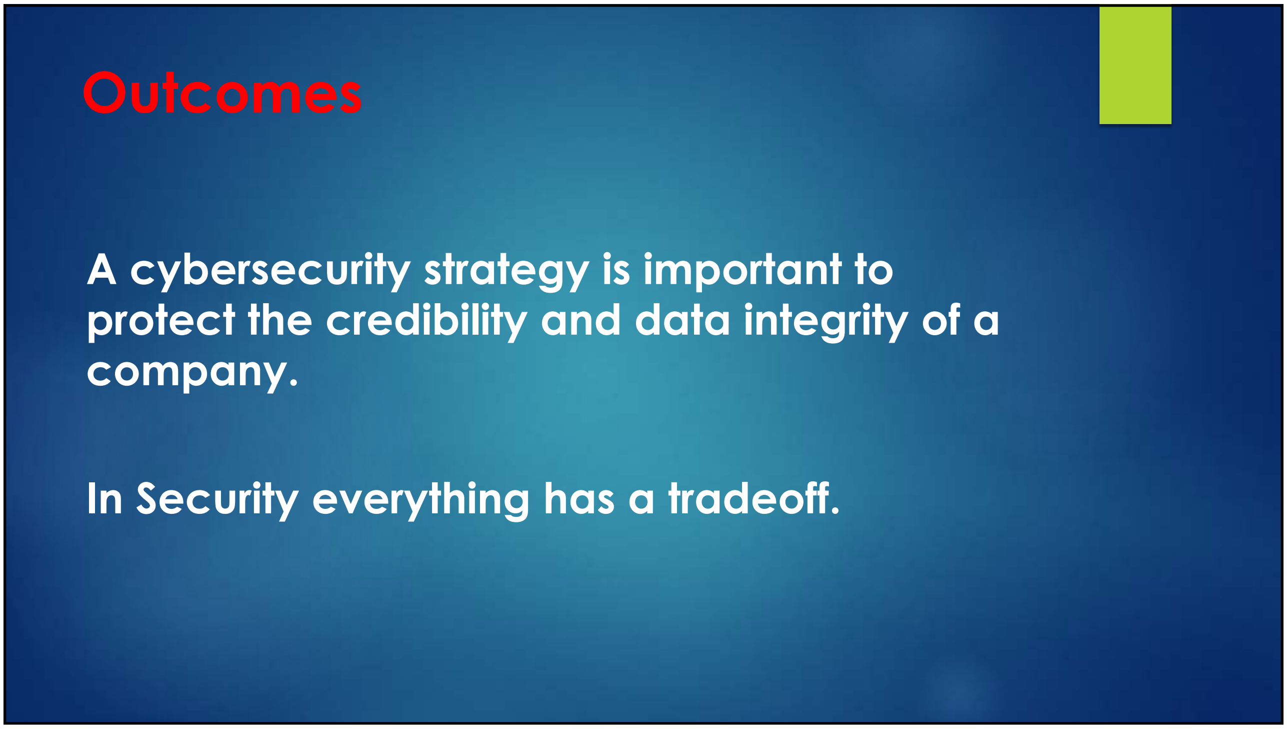
Overview:

- Randomly draw a chance card for your table
- Chance cards can have a positive or negative impact on credibility

Tips:

- Credibility impacts are permanent like real life.
- Chance cards are picked randomly by a team member to increase or decrease creditability due to cyberattacks when a team doesn’t have adequate safety implemented.

23



Outcomes

A cybersecurity strategy is important to protect the credibility and data integrity of a company.

In Security everything has a tradeoff.

24

For more information:

"BC/DR PLANNING AVE"

Business Continuity, Continuity of Operations, Emergency Mgmt. & Disaster Recovery Planning Specialists

The LSH Group, LLC

LINDA HANWACKER

CEO/FOUNDER

239-466-1170

HANWACKER@THELSHGROUP.COM

WWW. THELSHGROUP.COM

Thank You!

DRJ SPRING 2020
March 15-18, Orlando