Cybersecurity for $800, Alex:

Staying Safe is No Game

Tobin Conley, CAE
DelCor Technology Solutions

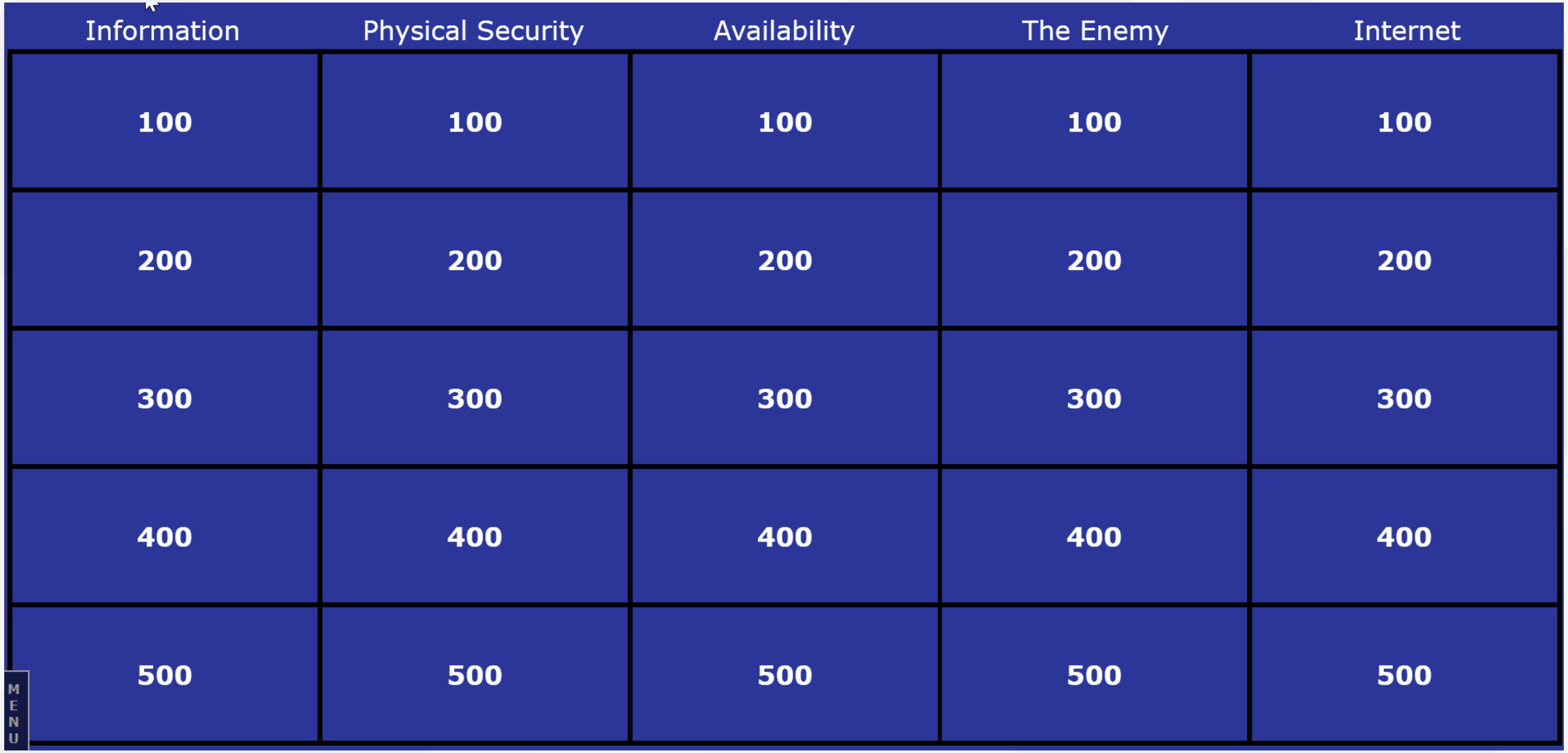
ACCESSE23

JULY 11–13, 2023 ■ DETROIT, MI

Overview

- The ***Lightning Round***
- **Who, why, what, where,** and **how**
- **Risk** and **prevention**
- **The IT Systems Triangle**: Striking a balance
- **Table Stakes**: Basic (reactionary) Cybersecurity
- **Upping the Ante**: Advanced (proactive) Cybersecurity
- **5 things** to start doing today/**5 questions** to ask
- **Small group discussion** and report out/Q&A

Let the Games Begin……



Information	Physical Security	Availability	The Enemy	Internet
100	100	100	100	100
200	200	200	200	200
300	300	300	300	300
400	400	400	400	400
500	500	500	500	500

Who and Why?

- A **hacker** (individual or group) bypasses systems and passwords to access confidential information
- **Motivations**
  - Political
  - $$$ (extortion, cc fraud, company secrets)
  - Fun

What data can be targeted?

- **Member data**—*Personally Identifiable Information* [PII]
  - Can be used for identity theft/credit card fraud
- **Proprietary information** about your organization's work
- **No data**—attacker may want to compromise your workstation to use for another attack (DDoS, spamming)

Where can attack or breach come from?

- **Inside**
  - Someone within your company/network
  - Someone within the web site you’re trying to access
  - External party on “your” network (shared wifi at Starbucks)

- **Outside**
  - Attempting to get in to your network/computer
  - Attempting to get into the site you’re trying to access

How is data compromised?

- **Social engineering** – tricking someone into giving a username/password (also: “Phishing”)
- **Ransomware** – data is stolen/locked, and a ransom demanded for its return
- “**Cracking**” – trying many username/password combinations until one works
- **Virus, keylogger** – once installed, sends data back to attacker
- **Internal risk** – (ex)employee, consultant, intern with knowledge of/access to system

Social Engineering

RISK

- Tricking someone into revealing user data or credentials
- “Hi, this is Comcast, can you verify your account information?”
- “Hi, this is user X and I forgot my password, can you reset it for me?”
- Phishing – making a malicious web site look legitimate to entice users to input their data.
    - Spear phishing—targeting or falsely posing as an executive

PREVENTION

- End user training/follow-up
- Critical thinking. Does it make sense that someone would ask you for this info?
- Does the web site look suspicious?
- NEVER give out sensitive information over an open line.
- When in doubt, call or email company separately to confirm.

Ransomware

RISK

- Clicking on a link that loads a program that steals or encrypts organization data
- Threat to restrict access to and/or publicize data
- Interruption of business and financial loss

PREVENTION

- End user training/follow-up
- Regularly scheduled (and tested) backups
- Tech tools (Firewall, endpoint protection, VPN)

Cracking

RISK

- Attacker tries many username and password combinations – “Brute Force” attack
- Once password is “guessed”, attacker has full access.
- If attacker gains access to email, can then reset passwords for other accounts

PREVENTION

- Do not use common passwords
- Unique passwords per account
- Two-factor authentication when possible
- Lockout timers when possible
- Get alerts when logins fail (for network admins

Malicious software (malware/virus)

RISK

- Tricking user to install by presenting a seemingly-legit link
- Infected USB drive or network (such as coworker's computer)
- Virus can be used for extortion, data extraction, manipulate computer to use for another attack

PREVENTION

- Spam filter
- Antivirus software
- Gateway antivirus (firewall) usually on corporate network
- Software-based firewall
- Do not use your computer as "administrator" unless needed

Internal risk: Threat from Within

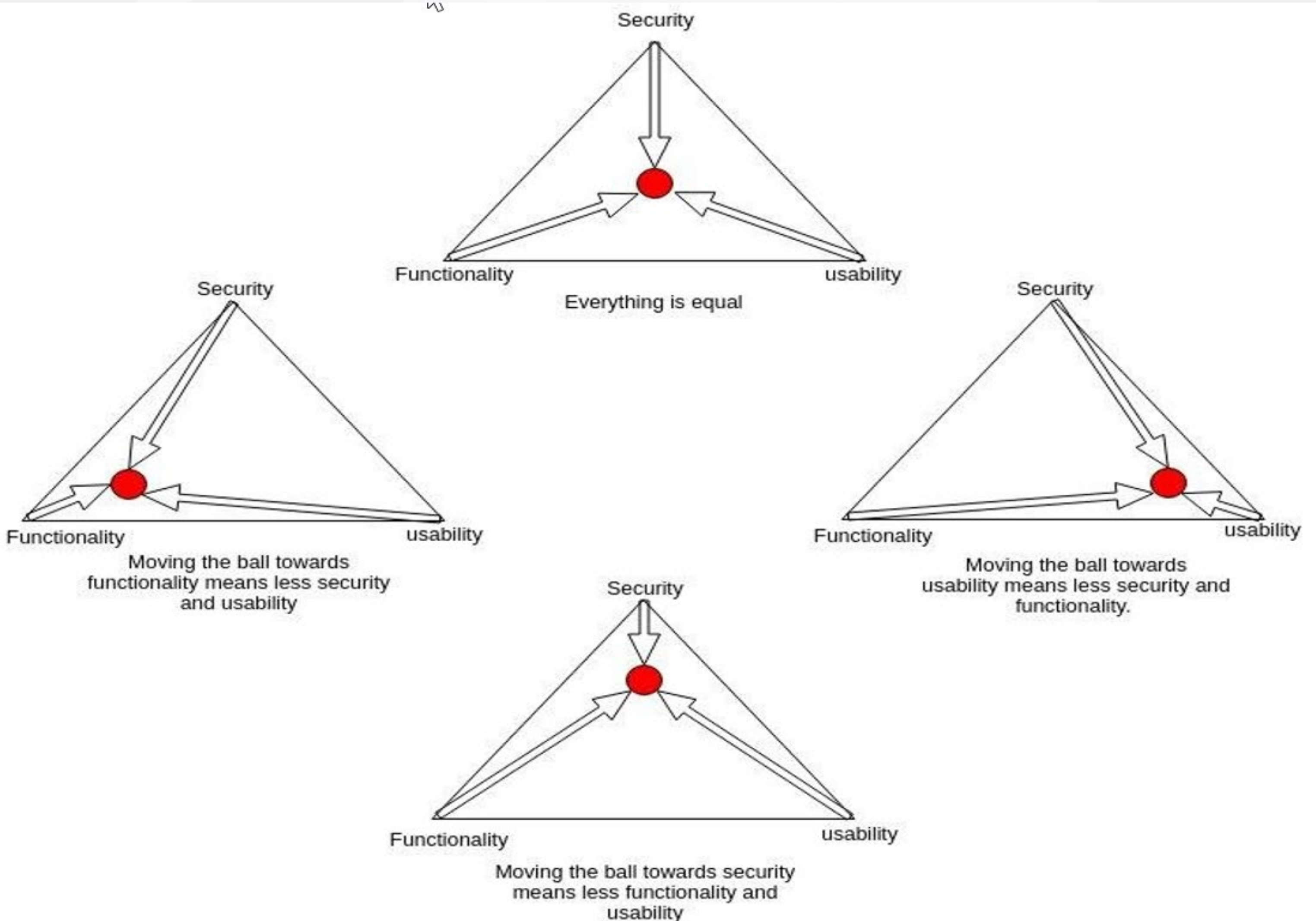
RISK

- Former or current employee has knowledge of username or password
- Ability to log in as legitimate user
- Problem usually not identified until much later if ever.

PREVENTION

- Change passwords often
- Do not share passwords: “Passwords are like toothbrushes”
- Apply access control to data on as-needed basis
- Audit user account and access control regularly

The IT Triangle: Security, Functionality, Usability


Security
Functionality
usability
Everything is equal
Security
Functionality
usability
Moving the ball towards functionality means less security and usability
Security
Functionality
usability
Moving the ball towards usability means less security and functionality.
Security
Functionality
usability
Moving the ball towards security means less functionality and usability

PRIVACY: Potential 'Fourth Dimension'

ACCESSE23
JULY 11–13, 2023 ▪ DETROIT, MI

Basic Cyber Security: Where to Start

- Multi-Factor Authentication (MFA)
- Antivirus (AV)
- Backups
- Remote Management
- User Awareness Training

Proactive Cybersecurity: Next Steps

- Web Access Firewall (WAF)
- Protection for Members' Information
- IT Policy and Procedures
- Disaster Recovery (DR)
- Incident Response (IR)
- Recovery Metrics (i.e., RPO/RTO)
- Security Operations Center (SOC)

IT Trade-offs: Proceed as Practical

- Vendor management is always easier than security management.
- Never spend more to protect something than it’s worth.
- Advancing from reactive to proactive doesn’t have to be a solo journey.

5 things to start doing today

1. Engage in **end-user training** (e.g. KnowBe4)
2. Unique **passwords**, changed regularly
    1. Use a “password manager” to keep track of/generate passwords (e.g., Keeper, 1Password)
3. Use **Multi-factor Authentication** for sensitive data
4. Keep multiple backups (and **test** them regularly)
5. Antivirus + exercise **common sense**

5 questions to ask

1. What is our password **policy**? And “where are the keys?”
2. Are our **firewall**, **antivirus** and **patch management** solutions up to date – and how are we protecting IT assets outside of the local network?
3. Do we have **off-site backups** of all critical data, and how/how often are they tested?
4. Can we **remote wipe** data?
5. What is the security posture of our key **partners/vendors**?

Time to Share:
Small Group Exercise

- What's **keeping *you* up at night** regarding your key exposures?
- What security achievement are you **most proud of** accomplishing?
- What is the **one thing you would share** with your colleagues that we haven't discussed today?

Contact Us

☎ 877-4DELCOR
301.585.4222

@delcortech

@delcor

@delcortech

@delcortech

DelCor Technology Solutions

Resource Page: https://www.delcor.com/resource-center

Contact info:

Tobin Conley, CAE
Director, Research & Learning
DelCor Technology Solutions www.delcor.com
tconley@delcor.com

ACCESSE23

JULY 11–13, 2023 ■ DETROIT, MI