CACUBO
Central Association of College
& University Business Officers

nelnet
CAMPUS COMMERCE

When, Not If

The Realities of Cybersecurity in Higher Education

Virgil Lloyd, Sr. BDE
Nelnet Campus Commerce

CACUBO
Central Association of College
& University Business Officers

- This webinar is part of our monthly webinar series to bring programming of interest to our members.
- The webinar is eligible for CPE. If you are interested in receiving CPE credit for this webinar, please e-mail me (Marty Mickey) at mmickey@nl.edu now. During the webinar, there will be four check-in questions for you to answer. **In order to receive CPE, you must answer three of these questions.**
- Copies of the slides for this presentation and a recording of the webinar will be available on the CACUBO website in a couple of days.
- We will send out a survey afterwards to solicit thoughts and topics for future webinars. If you would be willing to present in a future webinar, please e-mail me at mmickey@nl.edu.
- Save space on your calendars for the **2024 CACUBO Annual Conference which is September 29-October 1 in Indianapolis**. Great networking and CPE opportunities. Concurrent session proposals are now being accepted at https://cacubo.memberclicks.net/am-concurrent-session-proposal-topics.
- **Our next webinar will be February 29 on Diversity, Equity and Inclusion**.

Learning Objectives

- Unique Aspects of HE
- Ransomware
- PCI-DSS v4.0
- What to Do?

On the Virg

- Father of 5
- Softball coach
- Guitar and golf
- Higher Ed for 25 years
- Nelnet for 6+ years
- Covering Pacific and Midwest
- My cybersecurity story

Unique Aspects of Higher Ed

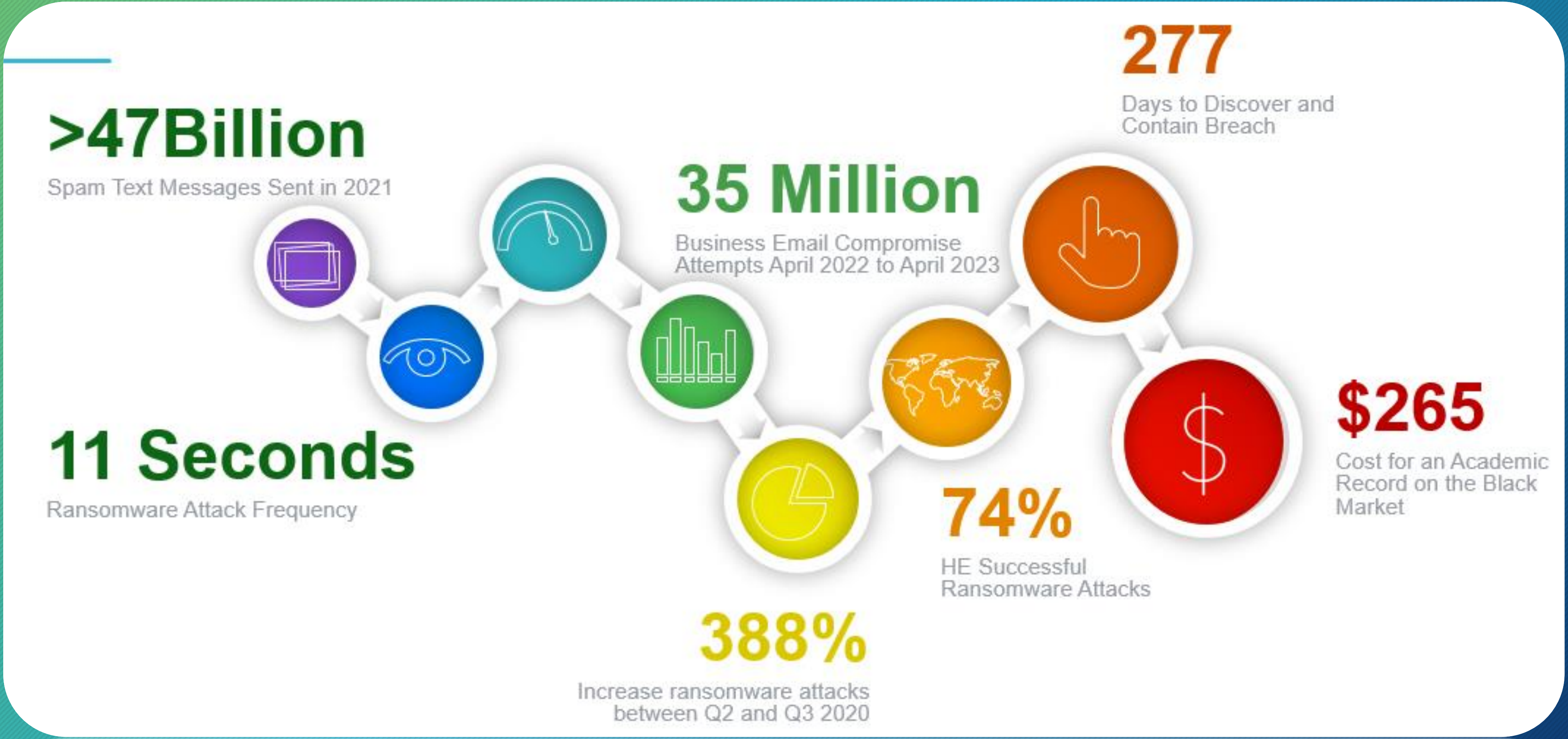
- Valuable Data
  - ✓ Student/Staff PII
  - ✓ Patient Medical Records
  - ✓ Research Data
  - ✓ Lab Equipment
- More Decentralized
- Collaborative by design
- Spending on Cyber lags other industries of similar size

Current Threat Environment

- Ransomware
- Compromise as a Service/Cybercrime as a Service
- Generative AI
- Nation State Actors
  - ✓ 200 Institutions reported research data and IP theft in 2021-2022
- "Teenagers" (18-25)
  - ✓ Lapsus$

    International extortion-focused hacker group known for its various cyberattacks against companies and government agencies

Current Landscape



>47Billion
Spam Text Messages Sent in 2021

11 Seconds
Ransomware Attack Frequency

35 Million
Business Email Compromise
Attempts April 2022 to April 2023

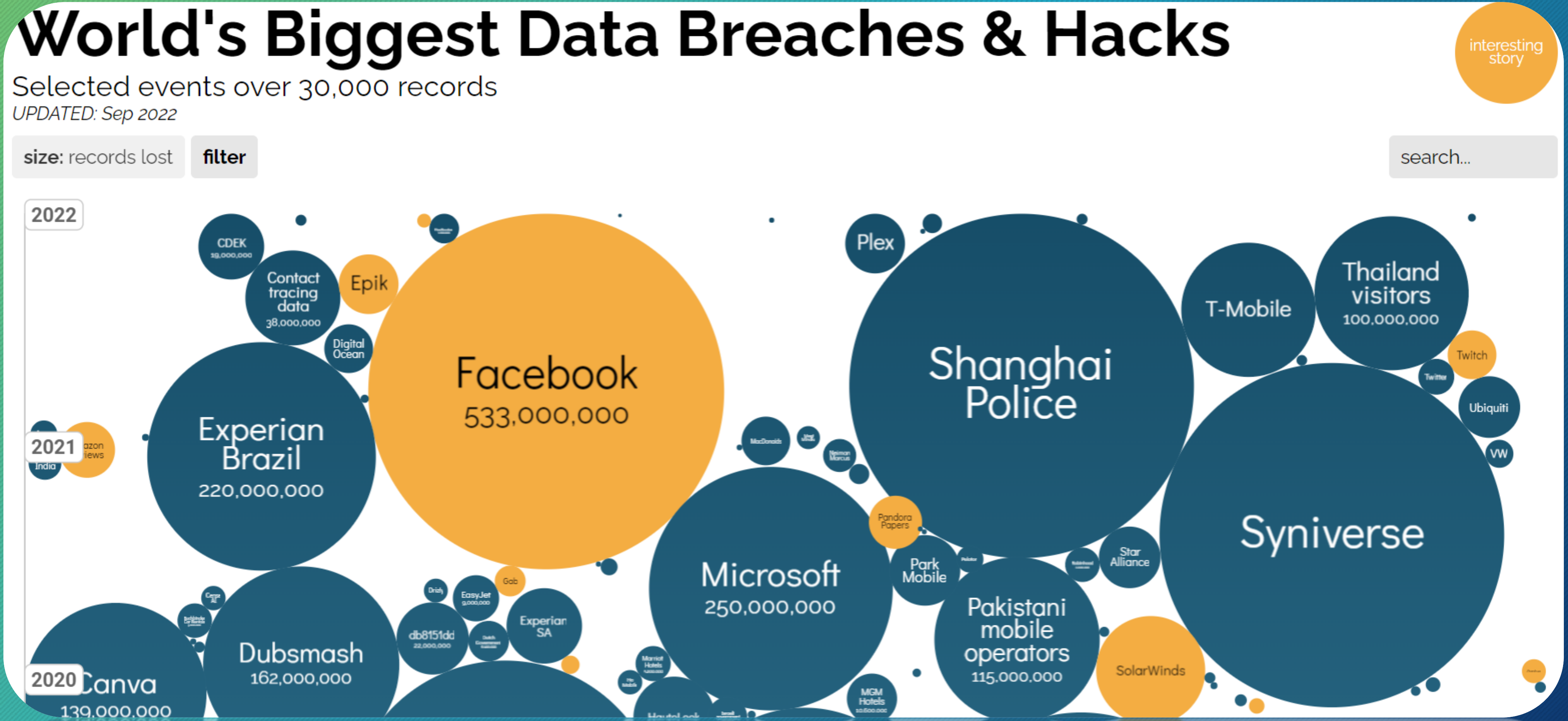
388%
Increase ransomware attacks
between Q2 and Q3 2020

74%
HE Successful
Ransomware Attacks

277
Days to Discover and
Contain Breach

$265
Cost for an Academic
Record on the Black
Market

Current Landscape



World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Sep 2022

Q&A

The majority of Higher Ed ransomware attacks in 2023 were caused by what?

- □ *Compromised credentials*
- □ *Malware*
- □ *Remote Desktop Protocol (RDP)*

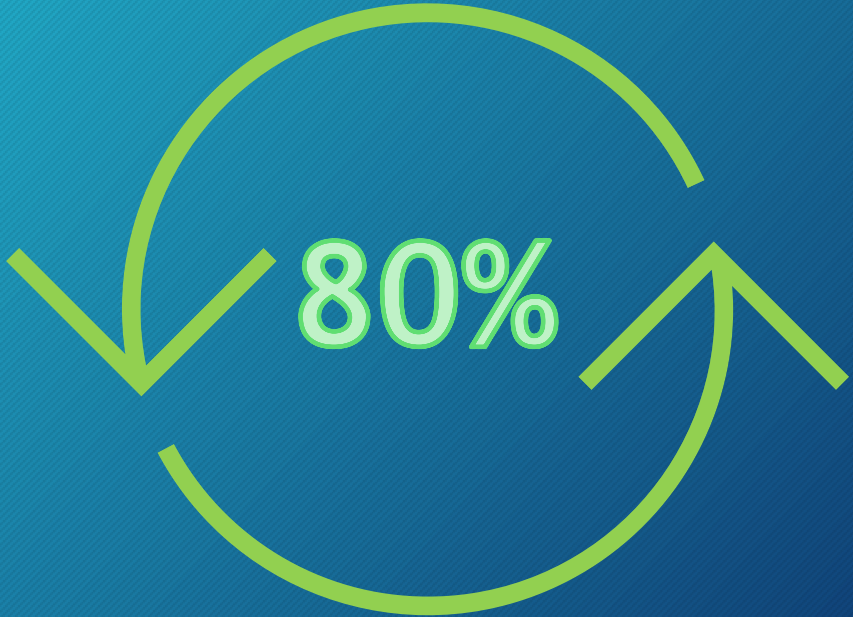
Data Exfiltration

41% China

10% Russia

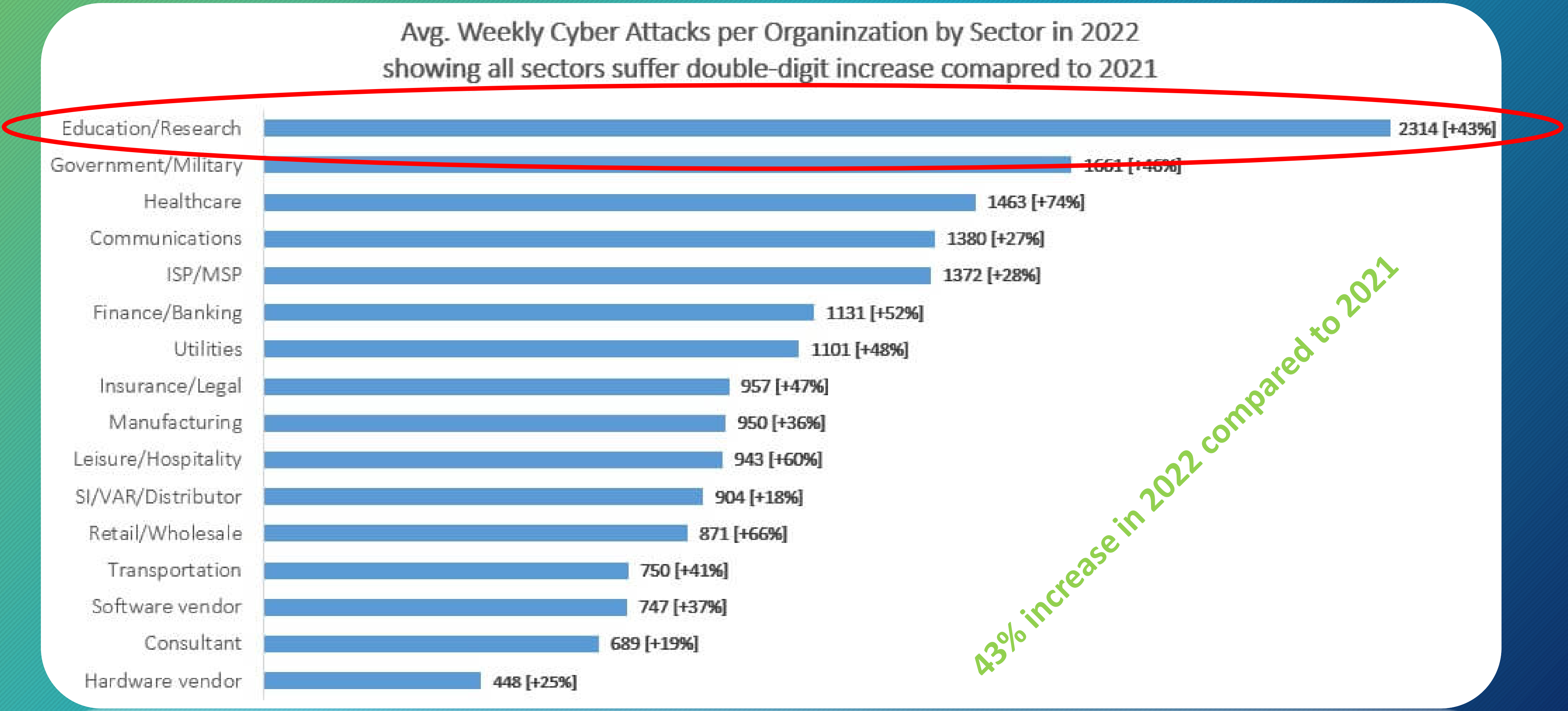
Frequency

- Experience repeat attack in 12 months



A ***replay attack*** occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants.

Growth in Higher Education



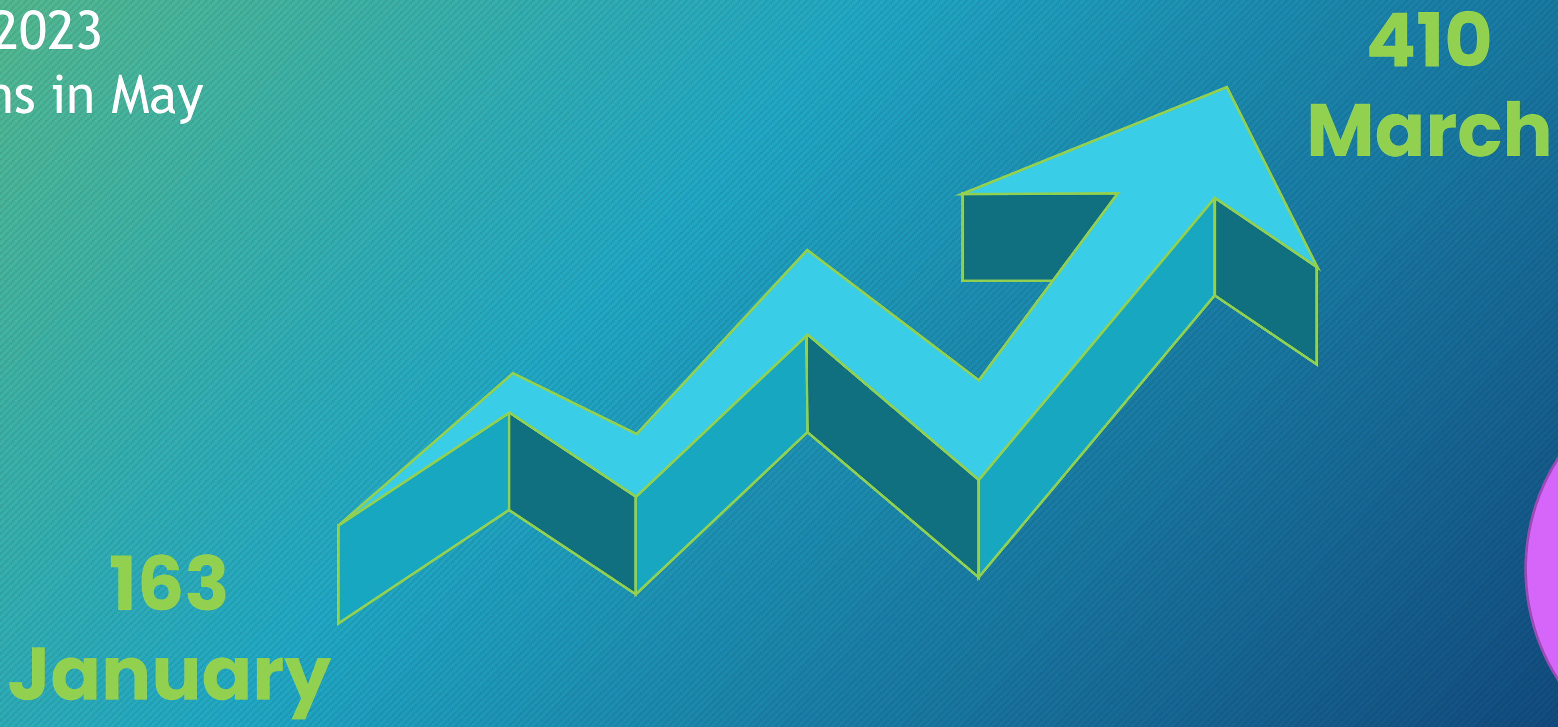
Avg. Weekly Cyber Attacks per Organinzation by Sector in 2022
showing all sectors suffer double-digit increase comapred to 2021

43% increase in 2022 compared to 2021

Ransomware Growth HE 2023

Education Sector

- 19% growth in ransomware attacks in April 2023
- 35 unique victims in May



Attackers intentionally delayed until students had returned to school

Why the Increase?

- Ukraine War Effort
- New entrants to the field
- *Akira*
  - ✓ Ransomware-as-a-Service (RaaS) group that started operations in March 2023
  - ✓ Dozens of schools and businesses in March

Notable Attacks

- *CommScope*
  - ✓ Network giant—schools, hospitals, federal
  - ✓ Specializes in network and telephony equipment for schools
- *Vice Society*
  - ✓ Specifically targets schools
  - ✓ Responsible for LA School District Attack
  - ✓ "Success in Mediocrity"
  - ✓ Responsible for CommScope attack

"All of your files have been encrypted by Vice Society."

How they Infiltrate

41%

Compromised by Social Engineering

43% of all attacks against education sector
were carried out by Social Engineering

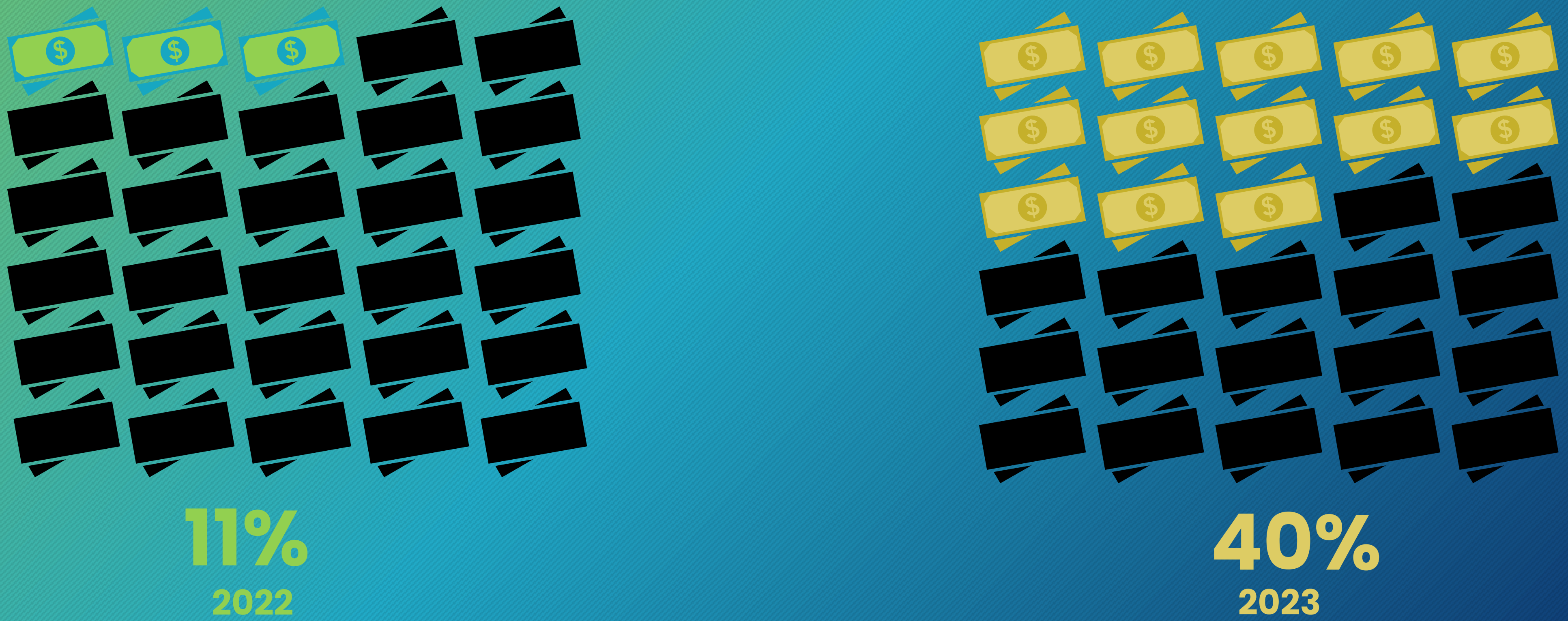
63%

Malware Targeting Education Sector

63% of all malware written specifically
targets education sector

Ransomware Payouts

The proportion of organizations paying seven-figure payouts



Responding to Ransomware

46%

Regained Data with Some or All Data Corrupted

51%

Successfully Regained All data

3%

Did Not Gain Access to Encrypted Data

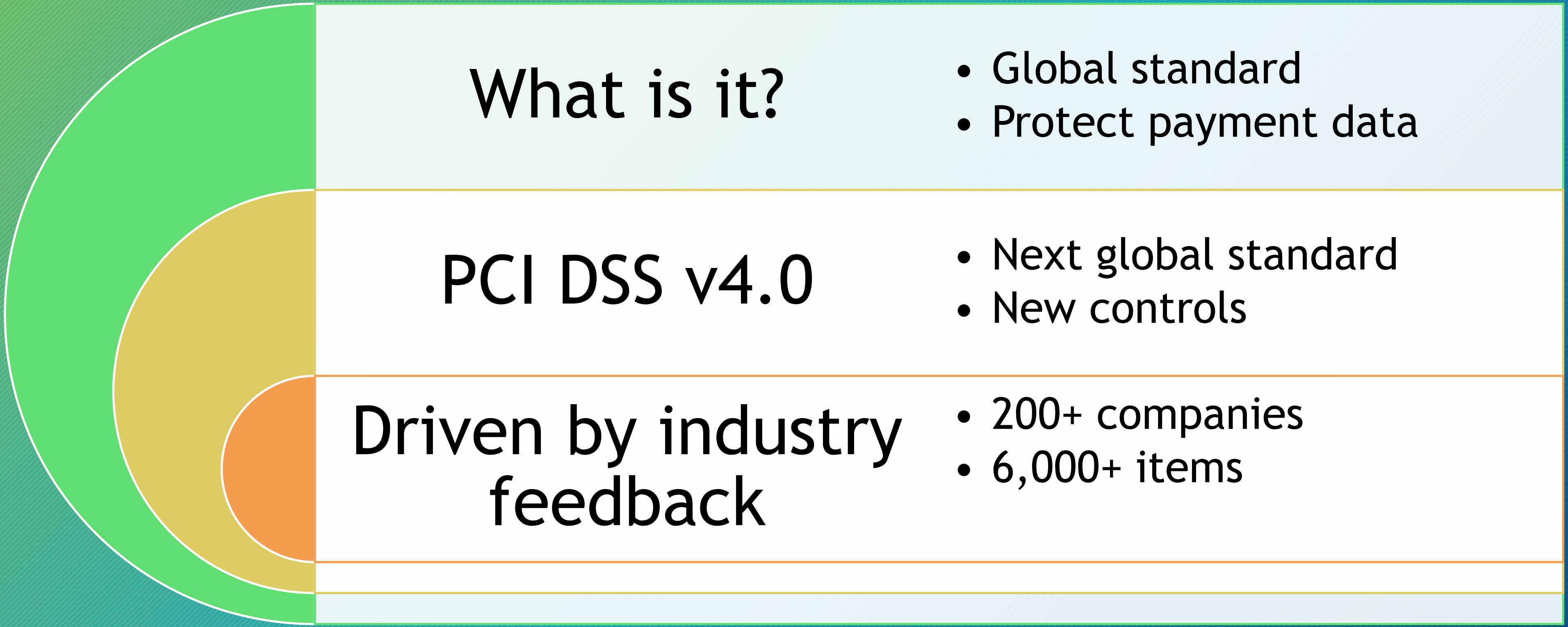
Marty's Story

Q&A

Has your campus been targeted with a cybersecurity breach in the last year?

- ❑ *YES*
- ❑ *NO*

PCI-DSS v4.0



What is it?

- Global standard
- Protect payment data

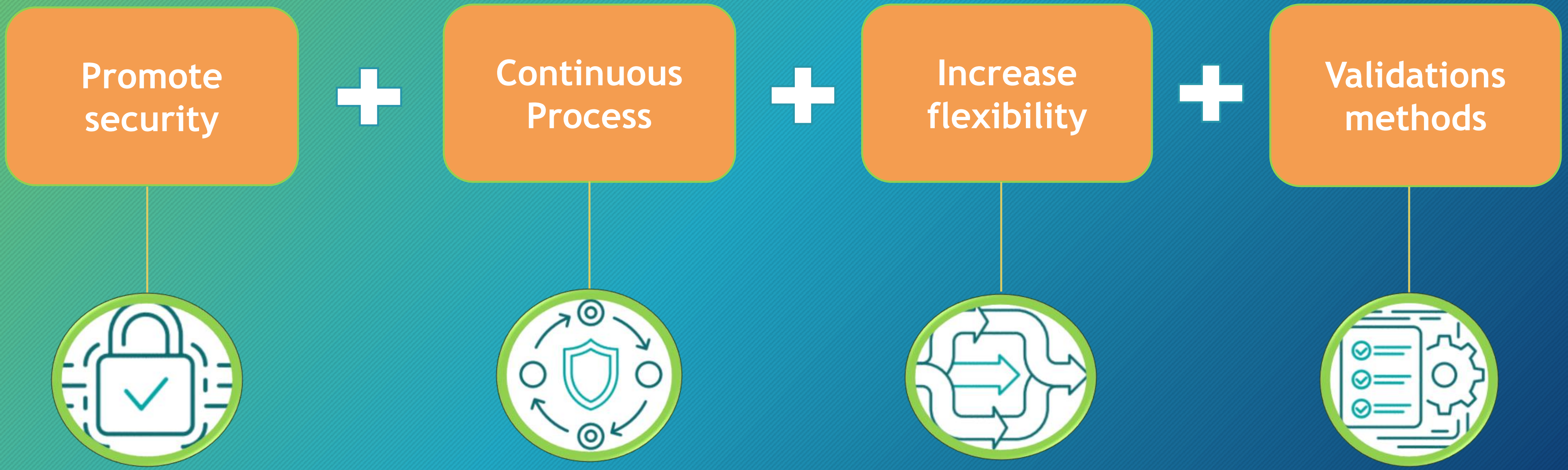
PCI DSS v4.0

- Next global standard
- New controls

Driven by industry feedback

- 200+ companies
- 6,000+ items

PCI-DSS v4.0



Promote security + Continuous Process + Increase flexibility + Validations methods

PCI-DSS v4.0

Expand MFA • Updated password requirements • ***New e-commerce*** and phishing requirements

Security must evolve

Clear roles and responsibilities • Added guidance implement and maintain security • More transparency for report reviewers

Criminals never sleep

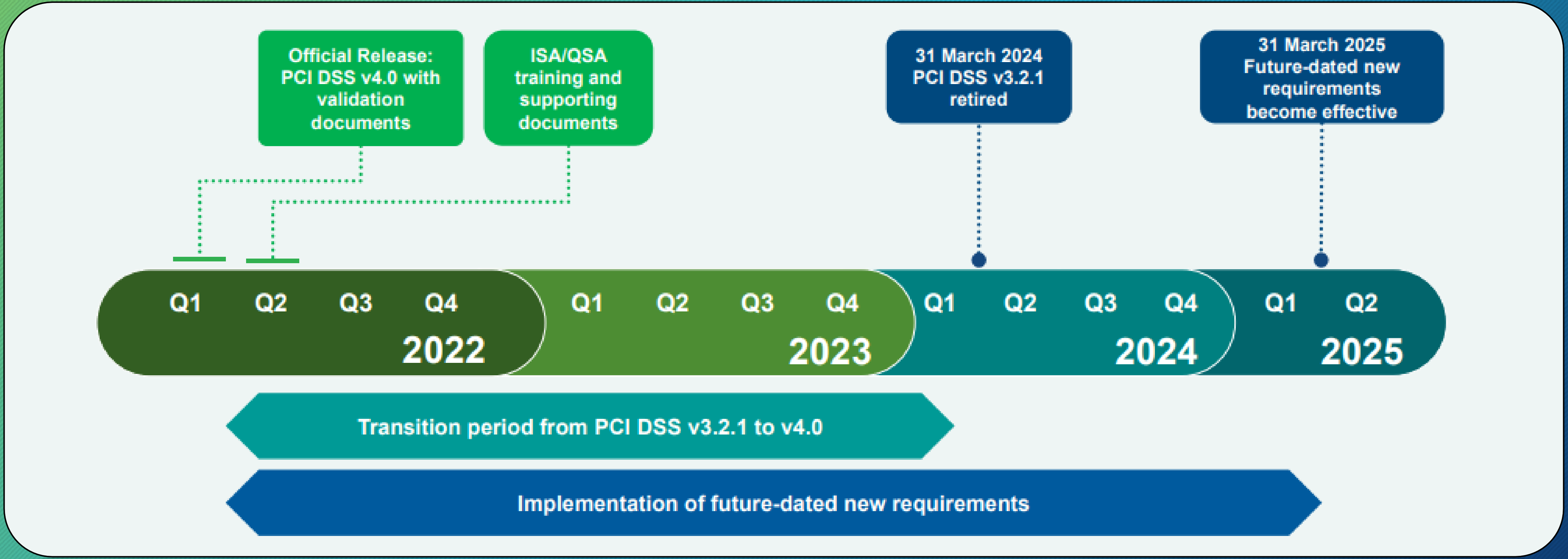
Allowance of shared accounts • Targeted risk • Customized approach to implement and validate

Flexibility supports innovation

Alignment between reporting and SAQ and info summarized in AOC

Transparency and granularity

PCI-DSS v4.0



Official Release: PCI DSS v4.0 with validation documents

ISA/QSA training and supporting documents

31 March 2024 PCI DSS v3.2.1 retired

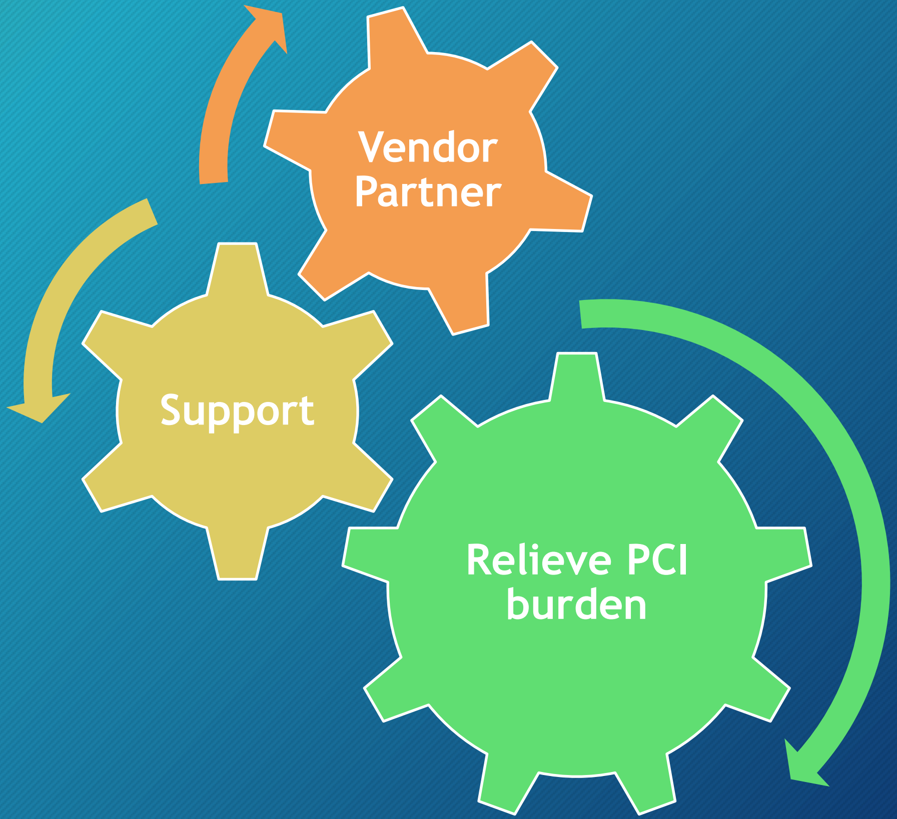
31 March 2025 Future-dated new requirements become effective

Transition period from PCI DSS v3.2.1 to v4.0

Implementation of future-dated new requirements

PCI-DSS v4.0

- Outsourcing to third party
- Are they maintaining compliance & gearing up for v4.0?
- How are they working to prevent malicious code?
- Applying innovations?
- Embrace MFA



Vendor Partner

Support

Relieve PCI burden

Compliance vs. Security

- Compliance is ***<u>not</u>*** Security
- Equifax was 100% compliant when they were breached

Q&A

How is your campus preparing for the transition to PCI-DSS v4.0?

- ❑ *Reviewing our vendor partners and discussing their preparedness*
- ❑ *We are applying new innovations including expanding our MFA*
- ❑ *We are updating our password requirements*
- ❑ *All of the above*

What to Do?

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

"The most effective Cyber Hygiene is fundamental and persistent end user training"

Phishing Training

- Not just identifying Phishing Emails
  - ✓ Driving Awareness
- Replicate Threats
- _80%_ of organizations that implement awareness training see a reduction in phishing susceptibility - *Proofpoint*

"Sutton's law tells us 'When diagnosing, first consider the obvious.' Thus, if you wonder why criminals phish, it is because email is where their targets are reachable."
-Verizon 2022 Data Breach Report

Practical Application

- Utilize MFA on *Everything*
- Consider a *Password Manager*
- Use Passphrases vs. Passwords
    - I drive a 1998 Honda
    - HondadrivesMe?1998!

KEEPER
Cybersecurity Starts Here
1Password
NordPass

Passwords

Don’t Reuse Passwords

“Passwords are like gum; Don’t share.”

Don’t Use Templates

WelcomeSpring2023
Welcome[Last Name]2023!

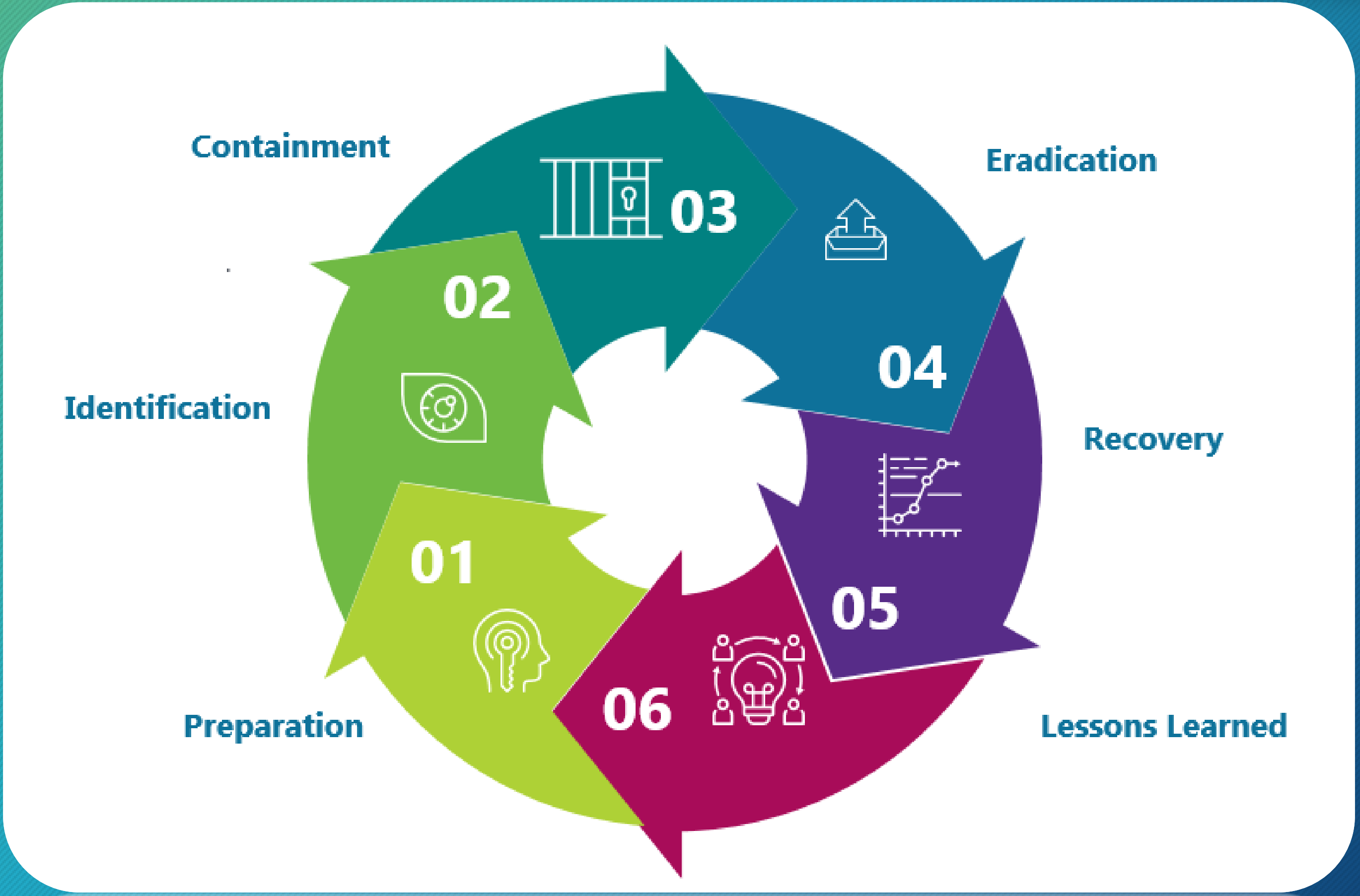
Utilize Password Manager

Beware!

Don’t Rely on Browser’s Manager

Response Plan

"By failing to plan you are preparing to fail."
- Benjamin Franklin



Response Plan

Test Your Backups

- How Long for Full Restore
- Are the Backup Immutable?
- How/Where Can You Access Backups?.

Test Failures of Systems

- SIS
- Physical Security/Cameras
- CRM
- Payroll

Have Conversations w Faculty/Staff

- What If?
- What Scenarios can they think of?
- Current Threats

Talk to Other Schools

Collaborate with Other Schools

User Organizations

Tabletop Exercises

- Combined exercise across multiple departments
  - ✓ Business Office
  - ✓ IT
  - ✓ Operations
  - ✓ HR
  - ✓ Compliance
  - ✓ Executive Leadership / Board
- Don’t be afraid to develop “no win” scenarios

Q&A

Are you trained regularly on cybersecurity threats and how to spot and respond to them?

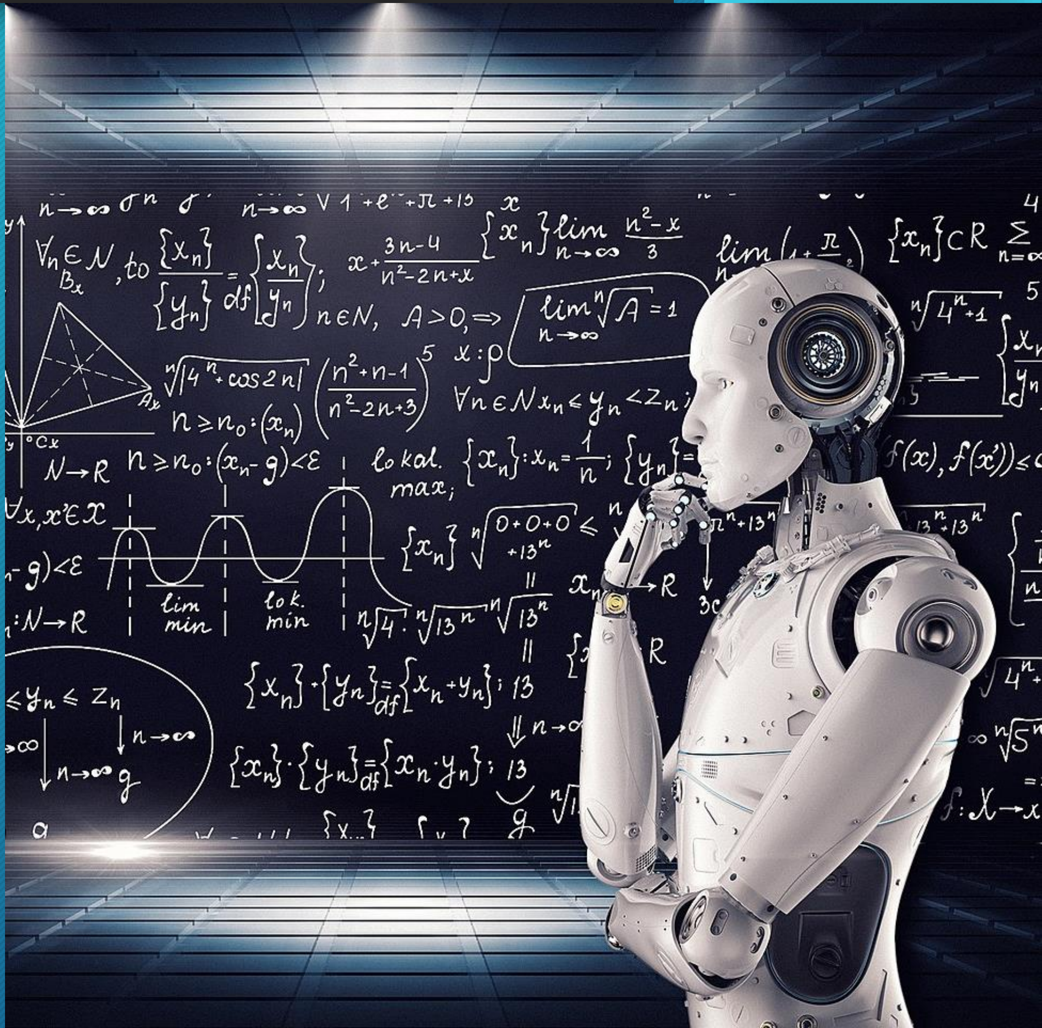
- ❑ *YES*
- ❑ *NO*

Burnout and Shortcuts

- Cybersecurity requires attention to detail
- Burnout compels people to engage in workarounds to retain energy
- Cyber hygiene is most likely to deteriorate when a person is burned out

Artificial Intelligence

- AI isn’t the “threat”
- It’s a tool, nothing more
- Phishing Threats
- New Attack Landscape
- Legacy Code Tools
- Daily Tasks



Summary

1.

Training

- Make cyber awareness training standard across all users.
- Consistent conversations about risk.

2.

Risk

- Develop a Risk Register.
- Prioritize risk based on role and criticality.

3.

Access

- Enable MFA for all accounts.
- Encourage use of strong passwords.
- Unique Passwords

4.

Patch

- Prioritize patch management as a standard practice.
- Maintain accurate inventory of all systems.

5.

Plan

- Plan for the compromise.
- Practice the plan regularly
- Involve all levels

“10 Immutable Laws of Security”

1. *Security success is ruining the attacker ROI*
2. *Not keeping up is falling behind*
3. *Productivity always wins*
4. *Attackers don’t care*
5. *Ruthless Prioritization is a survival skill*
6. *Cybersecurity is a team sport*
7. *Your network isn’t as trustworthy as you think it is*
8. *Isolated networks aren’t automatically secure*
9. *Encryption alone isn’t a deep protection solution*
10. *Technology doesn’t solve people and process problems*

nelnet®
CAMPUS COMMERCE

CACUBO
Central Association of College
& University Business Officers