

CMMC Should Scare You: Latest Developments and How to Prepare

SCCE Higher Education Conference
June 8, 2022



1

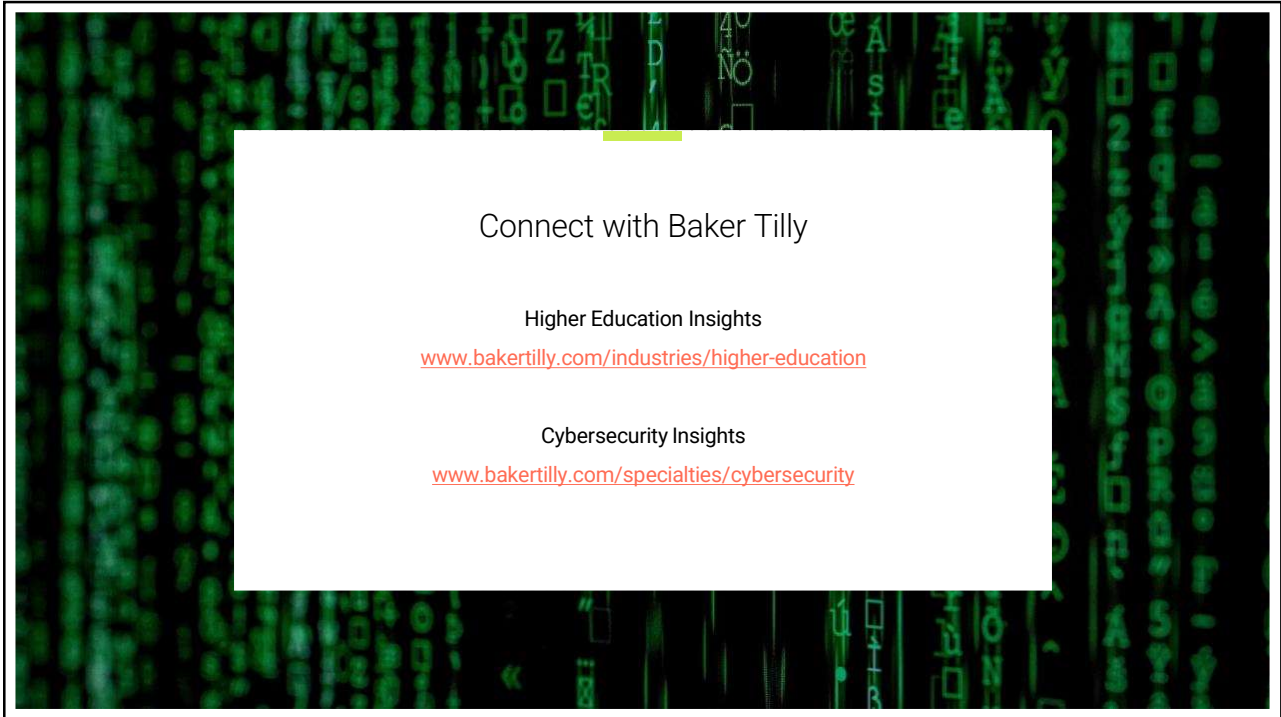


Presenters



Mike Cullen
CISA, CISSP, CIPP/US, CMMC PA
Cyber/IT Higher Education Leader
Baker Tilly

2



3



Agenda

- Cybersecurity challenges
- Regulatory and compliance requirements
- Challenging requirements
- Addressing challenges and requirements

4

Learning objectives

At the end of the workshop, participants will:

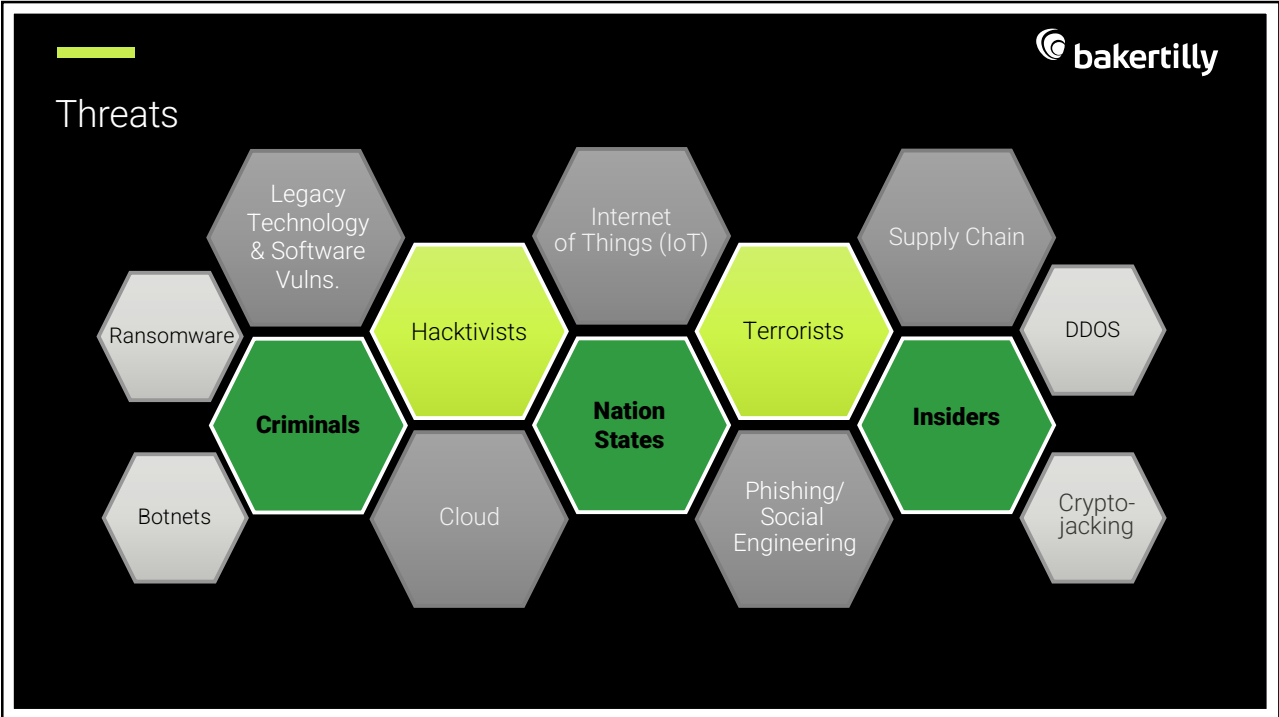
- Understand the latest CMMC developments and how it impacts higher education
- Gain insight into your specific questions on CMMC and how it impacts your institution
- Takeaway a list of challenging CMMC requirements and potential solutions

5

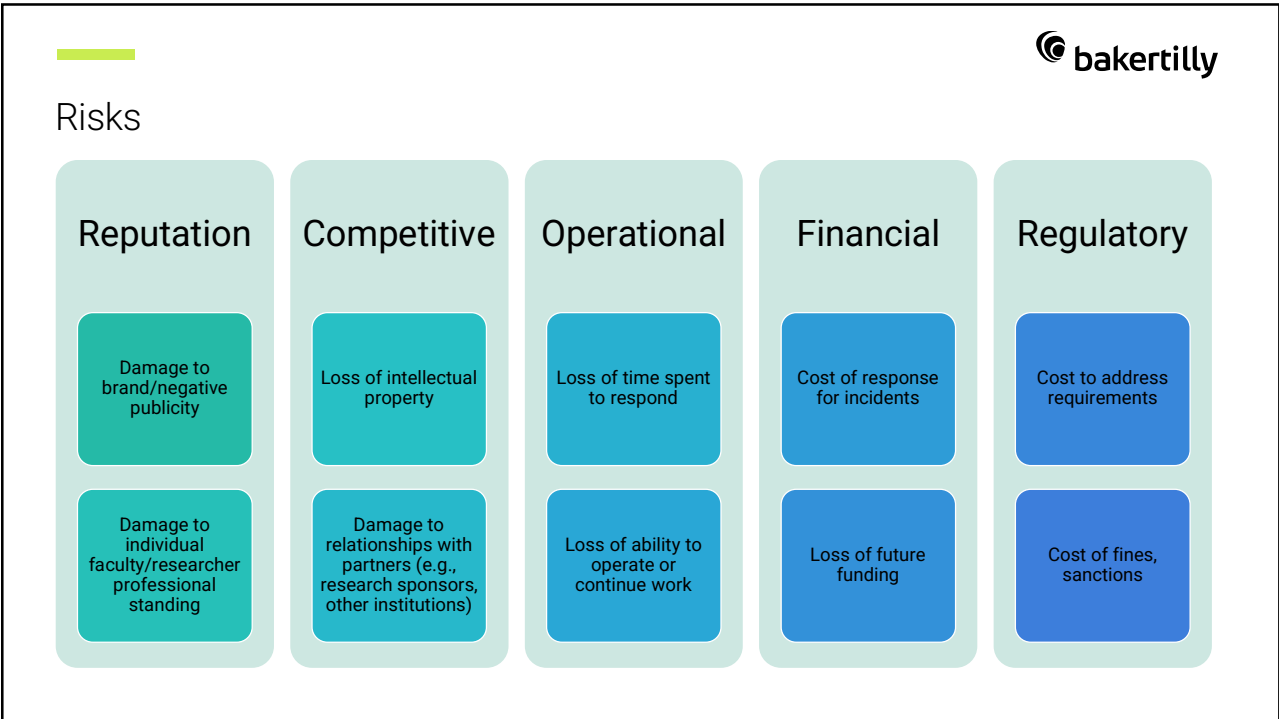
Cybersecurity challenges



6



7



8

Legacy perceptions

Researchers/PIs

- My funding, my way
- Data will be published, no need for security
- Regulations are guidelines, not requirements
- Do it "cheaper" buying/building own systems
- Mandatory training is useless

Support professionals (e.g., IT)

- Institution must be 100% compliant
- Research data should be treated the same as sensitive/confidential enterprise data
- Researchers should follow policies/procedures
- Only certain research covered by IRB or export controls really needs protections



9

Regulatory and compliance requirements



10

Example items where research data security requirements show up

Contracts and subcontracts	Grants and sub-awards	Cooperative agreements	Data Use Agreements (DUA)
Data Management Plans (DMP)	Data Licenses	Human Subject Protocols	Technology Control Plan (TCP)
Confidential & Non-Disclosure Agreements (CDA/NDA)	Material Transfer Agreements (MTA)	Memoranda of Understanding (MOU) with External Parties	Business Associate Agreements (BAA)

11

Examples of regulatory requirements

Federal Acquisition Regulation (FAR) 52.204-21: Basic Safeguarding

Department of Defense FAR Supplement (DFARS) clauses: 252.204-7012, 7019, 7020

Department of Defense Cybersecurity Maturity Model Certification (CMMC)

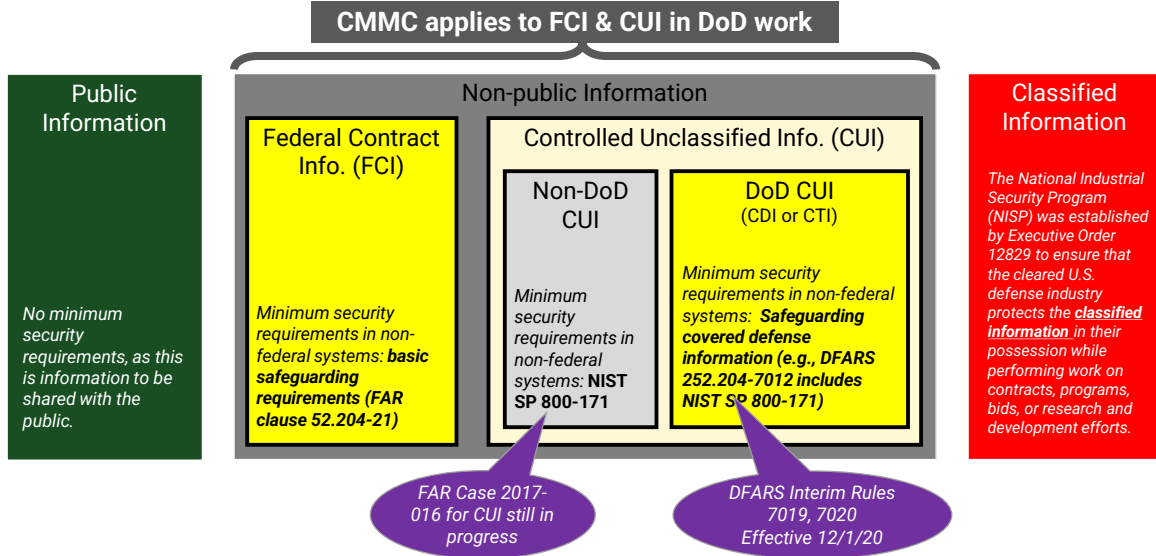
National Security Presidential Memo (NSPM) 33

Department of Justice Cyber Civil Initiative

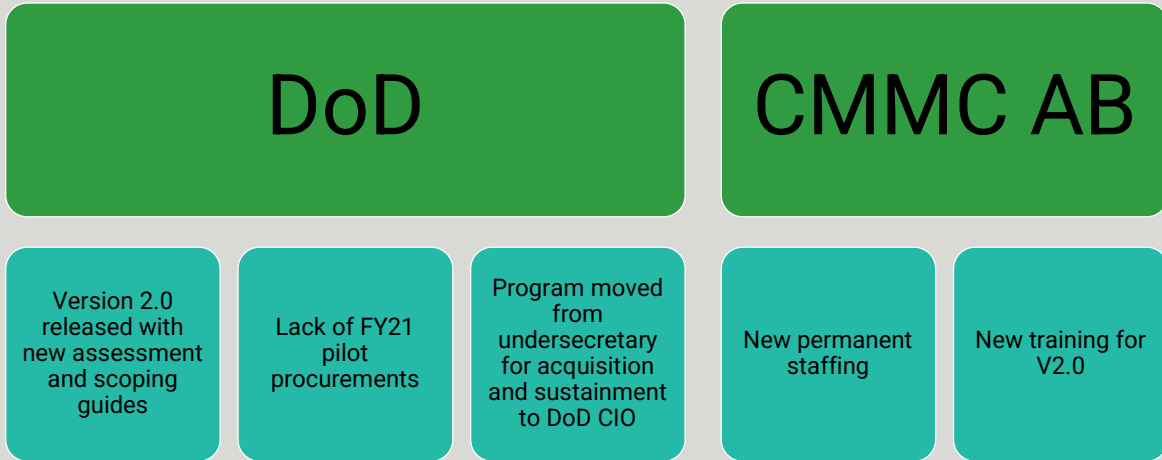
Export Controls (EAR/ITAR)

12

FAR/DFARS

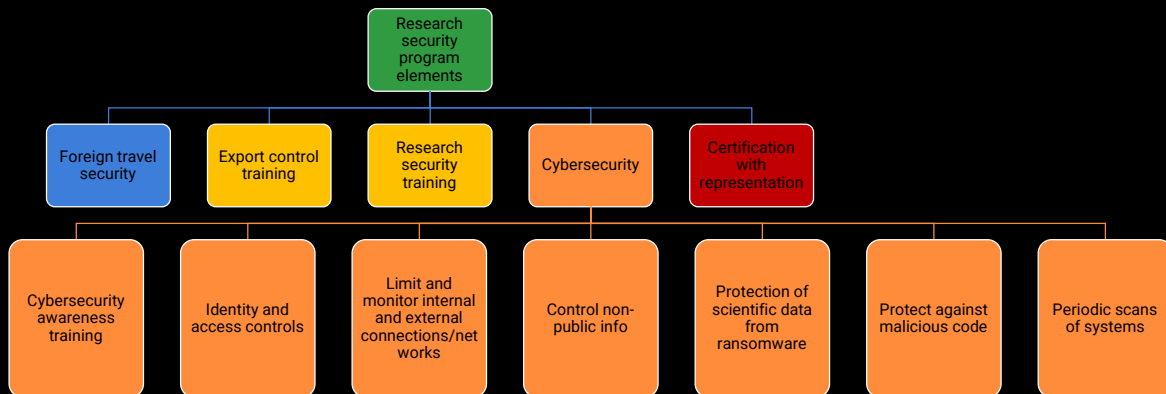


CMMC updates



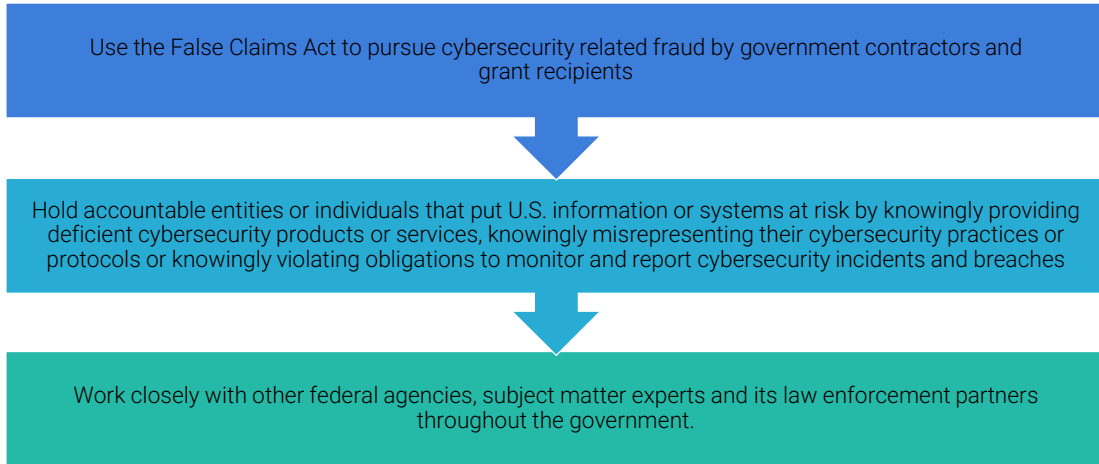
15

NSPM-33



16

Department of Justice civil cyber-fraud initiative



17

Export controls compliance program elements



◀ Elements that map/align to other regulatory cybersecurity requirements

18

Challenging requirements



19

Challenge: getting started

People

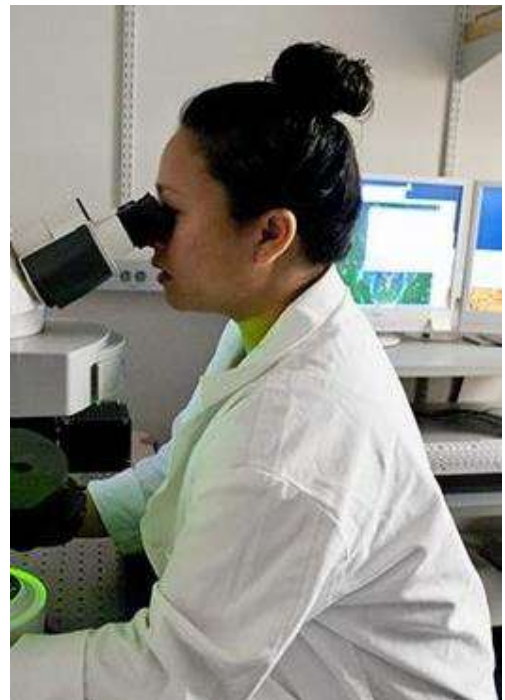
- Who will “own” the CMMC program?
- Who are the stakeholders?
- Who manages compliance?

Technology

- Who buys/builds solution?
- Cloud? On-premises? Special equipment?

Process

- Who funds the program?
- Who sustains the funding?



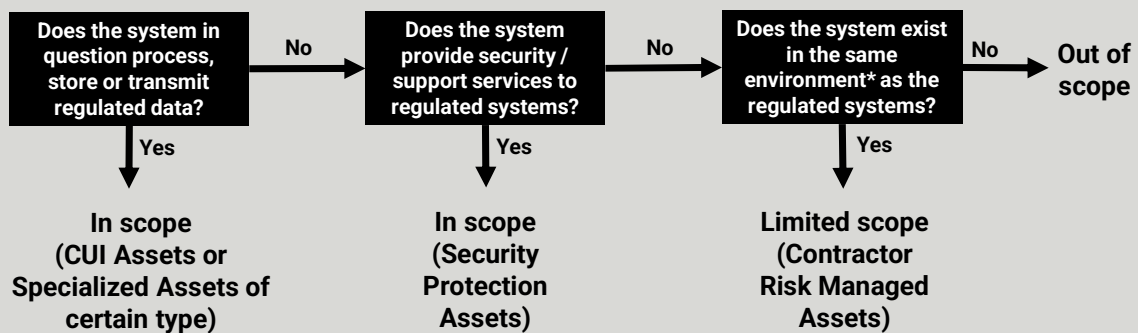
20

Challenges: data



21

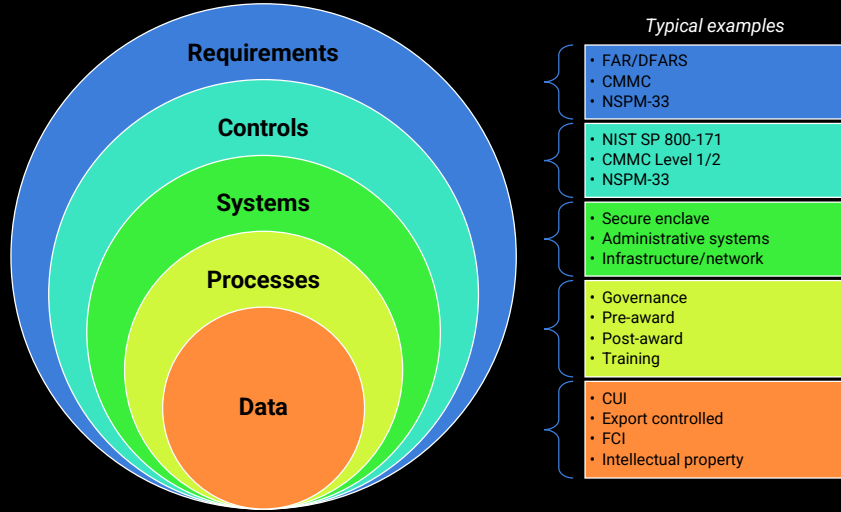
Challenge: scoping systems with CMMC research data



** Note – System can only be considered appropriately isolated from the regulated environment, if the system cannot access or connect to the regulated environment, typically through network controls/limitations (e.g., different segments, subnets or virtual networks)*

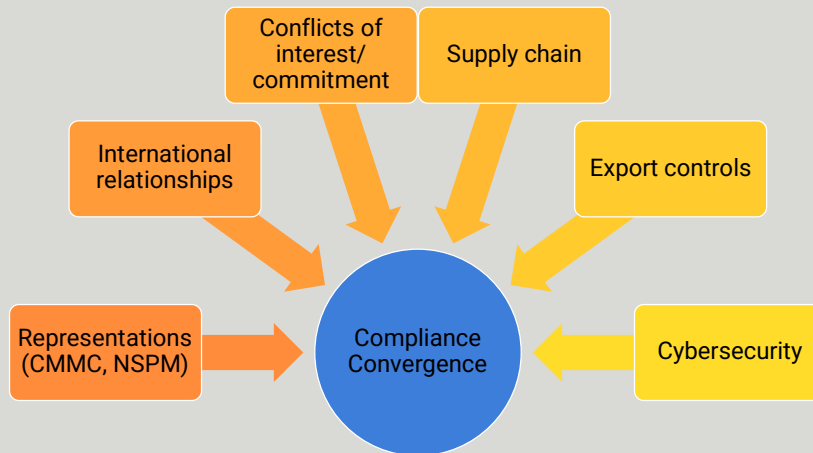
22

Challenge: relationships between all the components



23

Challenges: future requirement trends



24

Addressing challenges and requirements



25

People response: governance stakeholders

Research Focus

Faculty/Researchers/PIs

Research Leadership (Provost, VP/VC)

Deans/Dept. Heads

Institutional Review Board

Library

Tech Transfer/Commercialization

Research Admin/Compliance/Integrity

Support Focus

Information Security

Information Technology

General Counsel

Procurement

Privacy

Risk Management

Public Safety / Env. Health

26

Process response: key elements

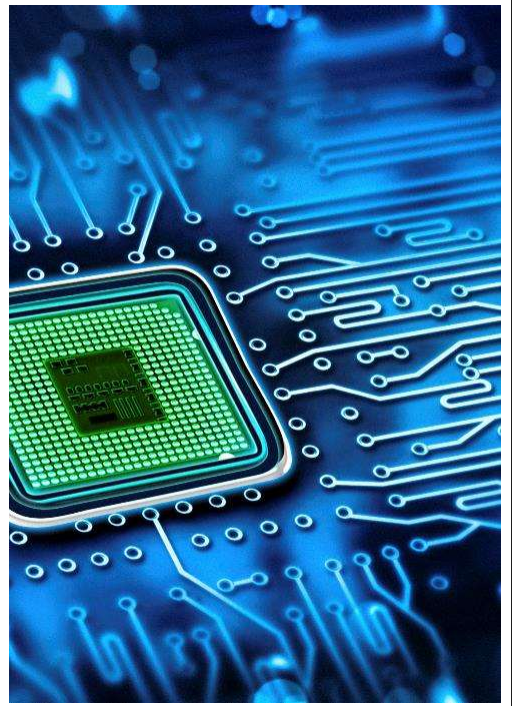
- Culture and values (Tone at the top)
- Risk assessment and management
- Policies and standards
- Outreach and education
- Monitoring and evaluation
- Audits and investigations
- Improvements and changes



27

Technology response: key elements

- Multi-factor authentication
- Anti-malware/virus/ransomware
- Network segmentation
- Security event monitoring
- Collaboration tool controls

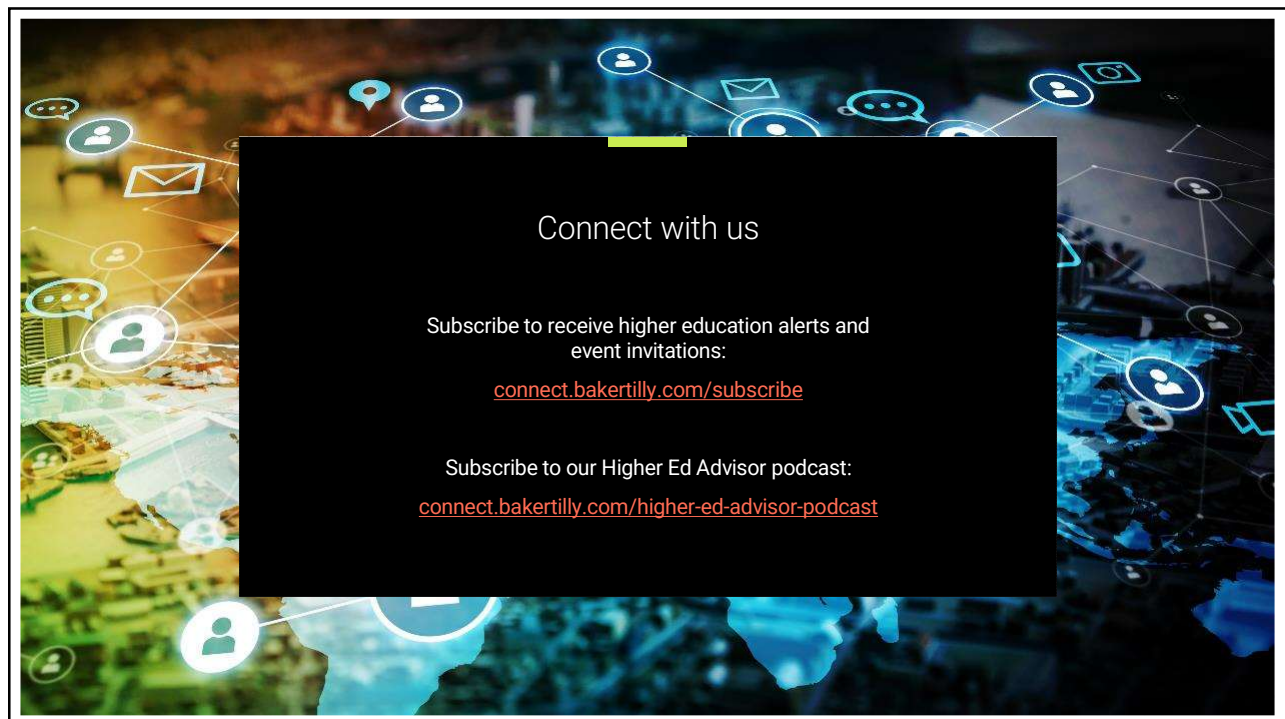


28

Contact us



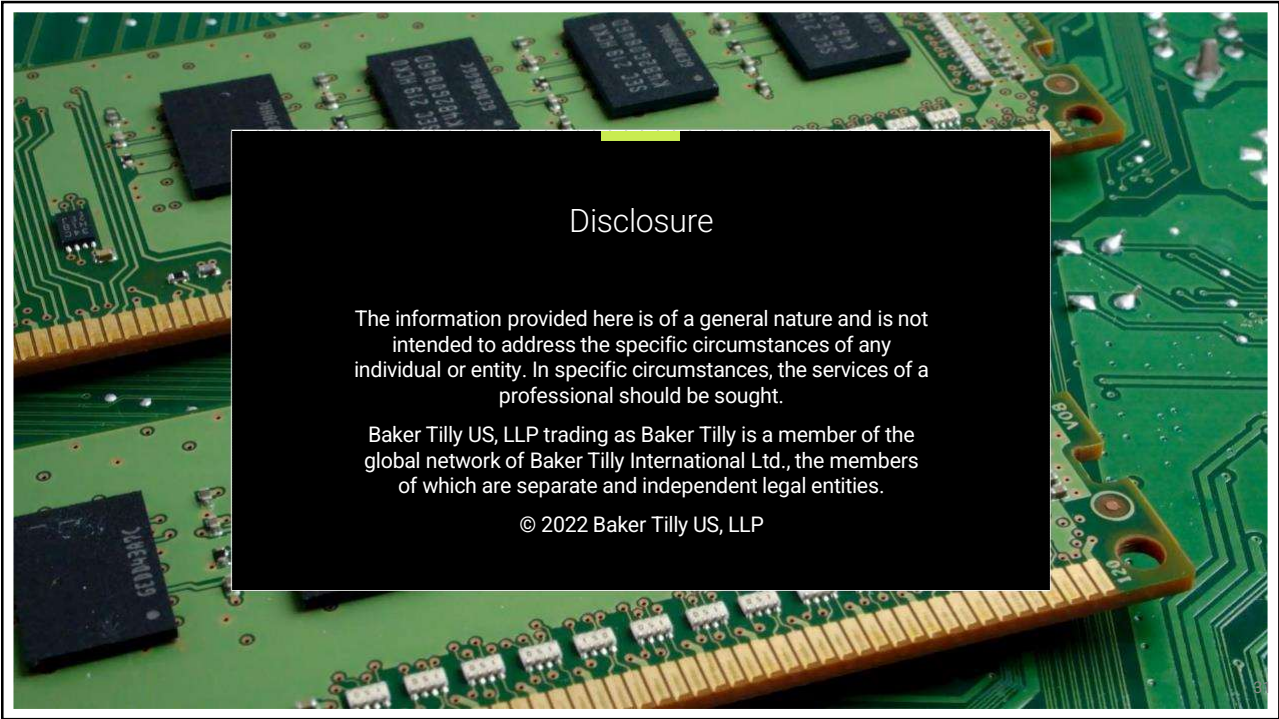
Mike Cullen
mike.cullen@bakertilly.com



Connect with us

Subscribe to receive higher education alerts and event invitations:
connect.bakertilly.com/subscribe

Subscribe to our Higher Ed Advisor podcast:
connect.bakertilly.com/higher-ed-advisor-podcast



Disclosure

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly US, LLP trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities.

© 2022 Baker Tilly US, LLP