BAKER TILLY

Protect Your Institution with Effective Cybersecurity Governance

Your presenter

Mike Cullen, Senior Manager, Baker Tilly
CISA, CISSP, CIPP/US

> Leads the firm’s Higher Education Technology Risk Services team, focused on IT audit and cybersecurity

> Collaborates with institutions to assess IT risks, review practices, meet compliance requirements, and recommend practical, pragmatic improvements

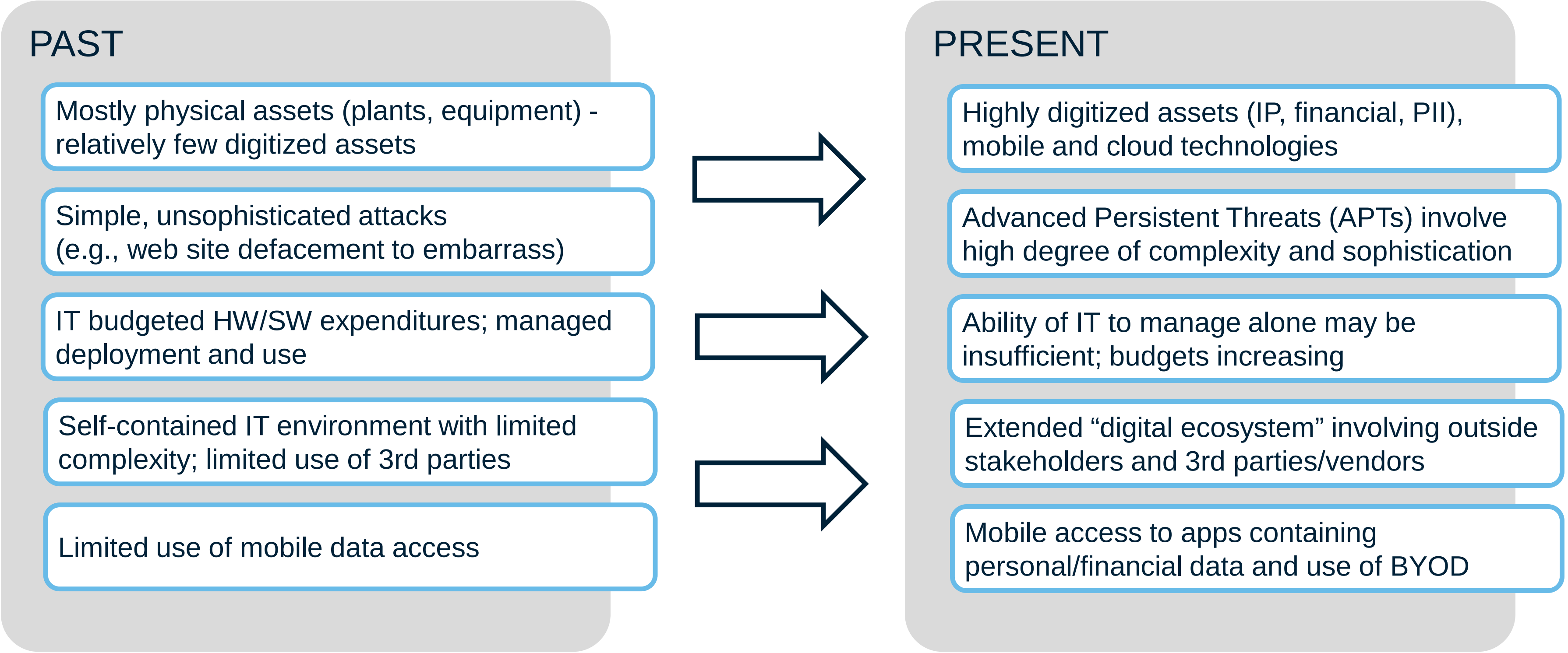
> Presents to a variety of audiences, including ACUA, various IIA conferences, and at multiple universities

Objectives

- How the cybersecurity risk landscape has changed
- Why cybersecurity risk must be managed as an enterprise-wide concern, not just an IT issue
- What the key foundational elements are of an effective cybersecurity program
- How to audit and present on cybersecurity program effectiveness to the institution's board and leadership

Cybersecurity landscape

IT changes



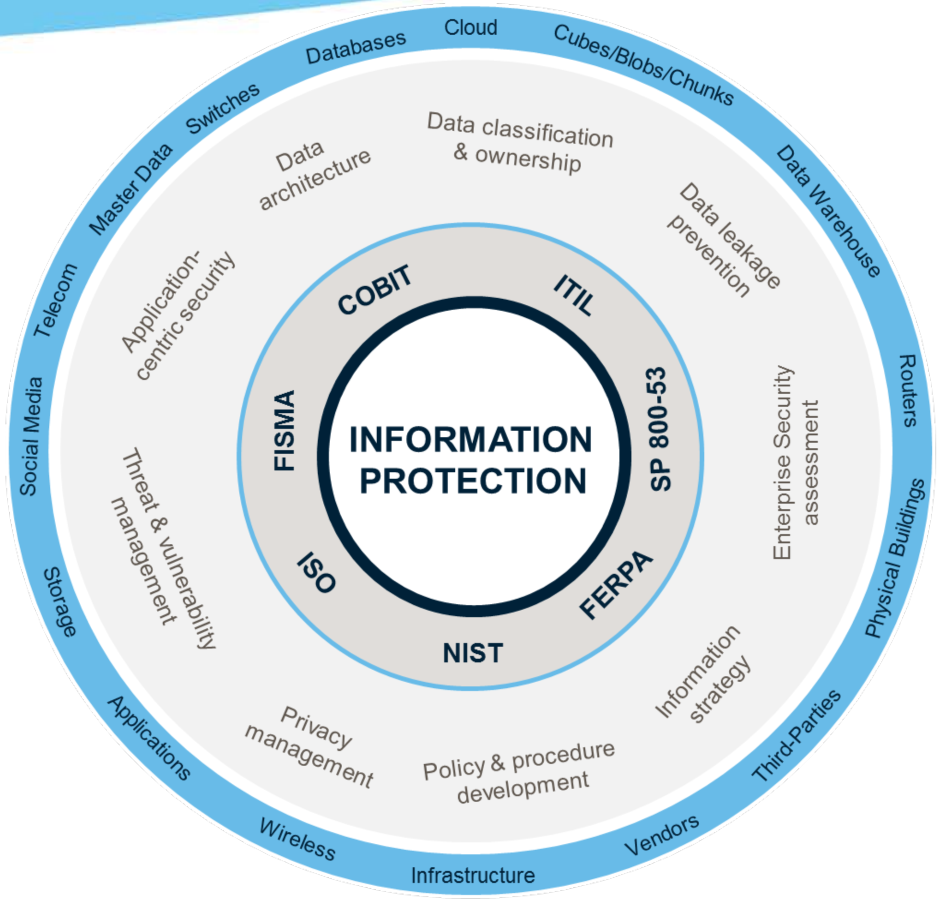
PAST

- Mostly physical assets (plants, equipment) - relatively few digitized assets
- Simple, unsophisticated attacks (e.g., web site defacement to embarrass)
- IT budgeted HW/SW expenditures; managed deployment and use
- Self-contained IT environment with limited complexity; limited use of 3rd parties
- Limited use of mobile data access

PRESENT

- Highly digitized assets (IP, financial, PII), mobile and cloud technologies
- Advanced Persistent Threats (APTs) involve high degree of complexity and sophistication
- Ability of IT to manage alone may be insufficient; budgets increasing
- Extended “digital ecosystem” involving outside stakeholders and 3rd parties/vendors
- Mobile access to apps containing personal/financial data and use of BYOD

Information protection changes

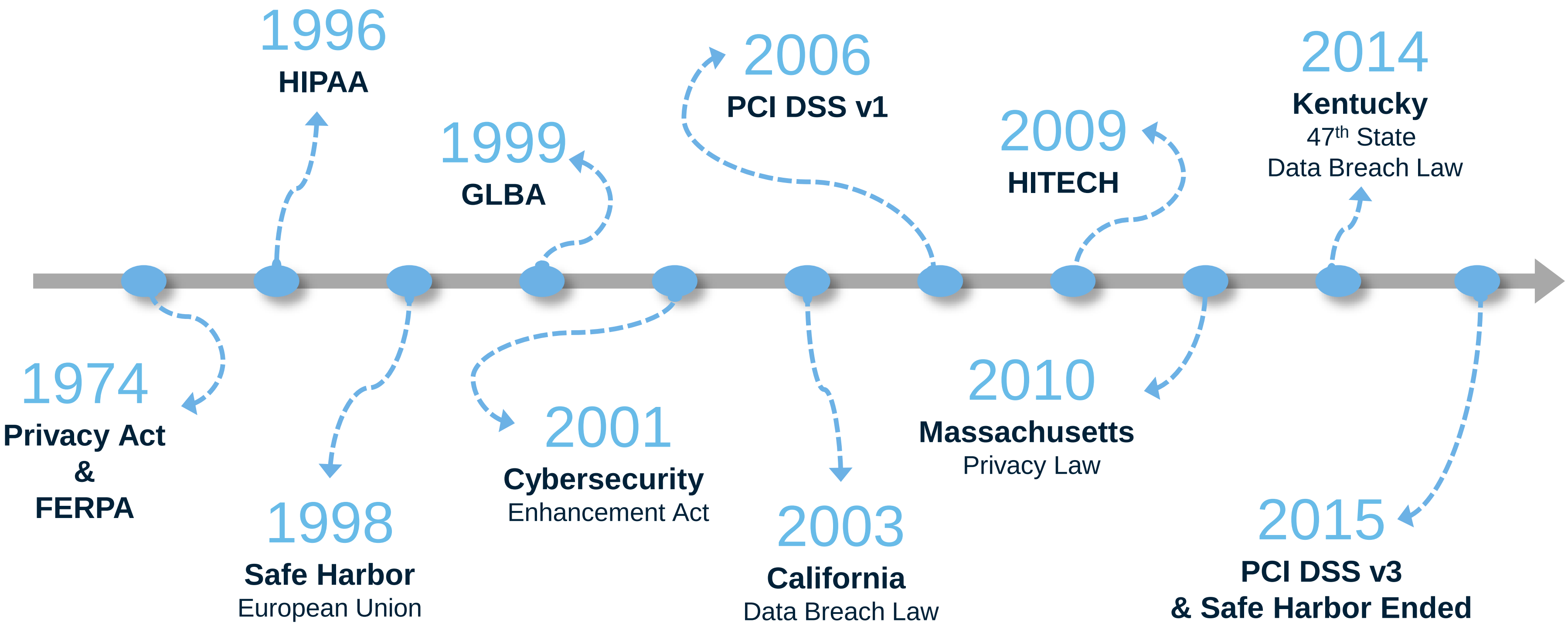


© Baker Tilly Virchow Krause, LLP

Complex threat landscape

- APT
- Cybercrime
- DDOS
- Insider
- Malware
- Ransomware
- Social Engineering
- Unpatched Systems

Regulatory changes



1974
Privacy Act
&
FERPA

1996
HIPAA

1998
Safe Harbor
European Union

1999
GLBA

2001
Cybersecurity
Enhancement Act

2003
California
Data Breach Law

2006
PCI DSS v1

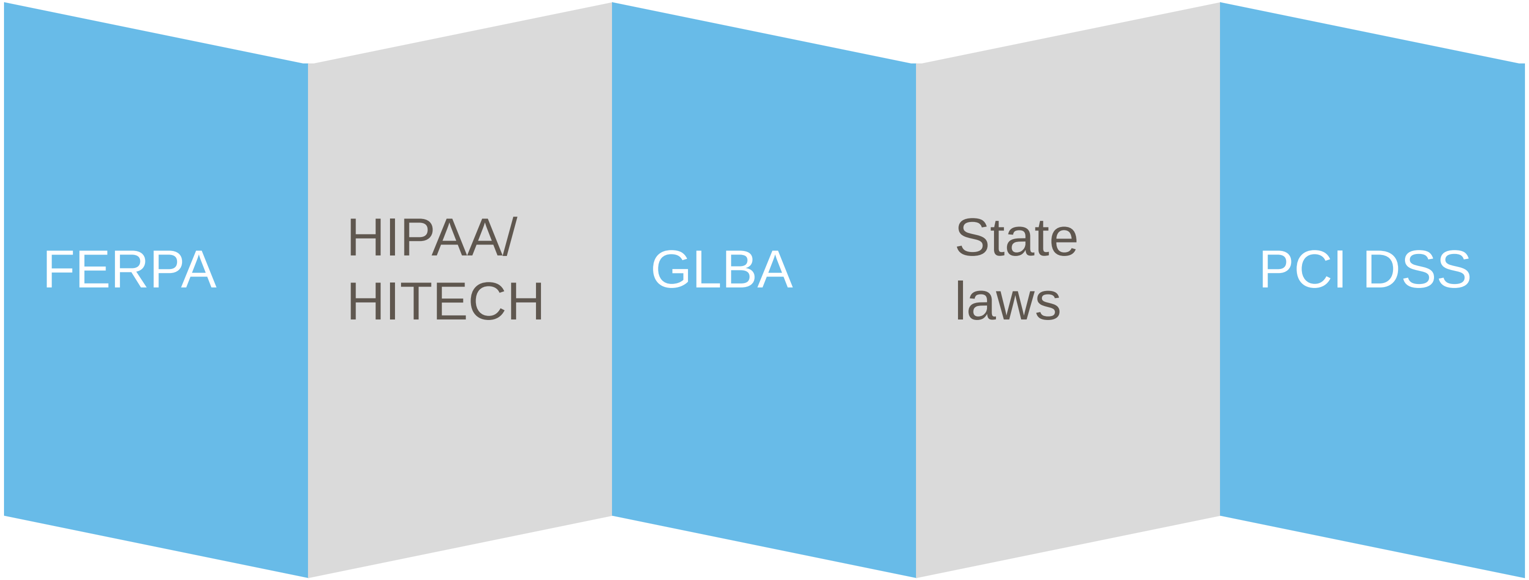
2009
HITECH

2010
Massachusetts
Privacy Law

2014
Kentucky
47th State
Data Breach Law

2015
PCI DSS v3
& Safe Harbor Ended

Higher education regulatory changes



FERPA

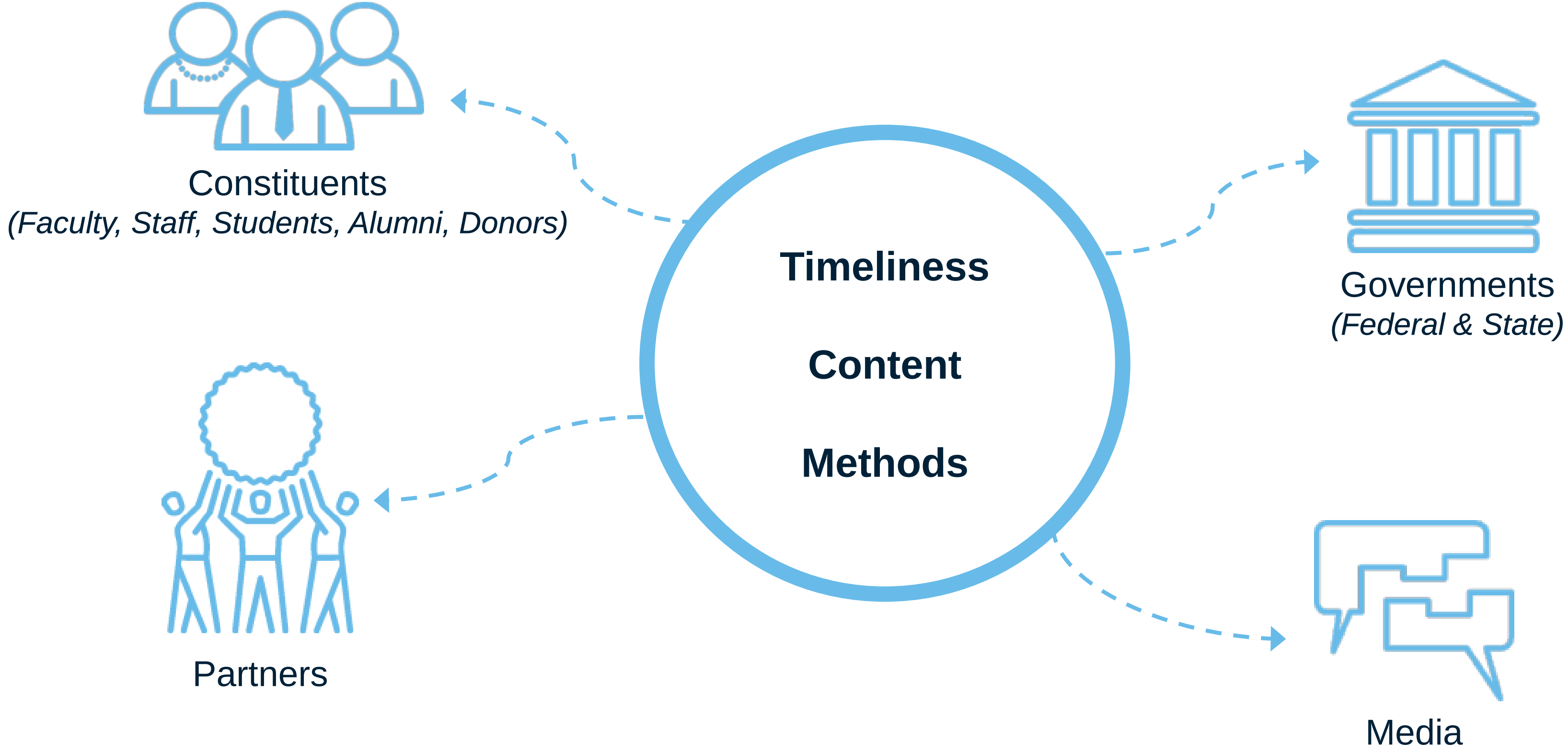
HIPAA/ HITECH

GLBA

State laws

PCI DSS

Changes in required disclosures



Timeliness

Content

Methods

Constituents
(Faculty, Staff, Students, Alumni, Donors)

Governments
(Federal & State)

Partners

Media

Cybersecurity as an enterprise-wide concern

Cyber attacks in the news

MAY 2015

“Chinese hackers force **Penn State** to unplug engineering computers”

Bloomberg

AUG 2015

“**UCLA** sued over recent hospital records hacking”

LA Times

JAN 2016

“FBI alerts **UVA** to employee information data breach”

NBC 29 WVIR-TV

FEB 2016

“**UCF** grads file suit in federal court over 63,000-person data hack”

Orlando Sentinel

Litigation involving cybersecurity and data breaches

- Boards have a duty to monitor and oversee risk, including cybersecurity
- A question is whether Boards utterly failed to implement any information system reporting, or consciously failed to monitor or oversee operations thus disabling themselves from being informed
- Litigation involving Boards and Officers for cybersecurity and data breaches is pending and there will be more data breaches and litigation going forward

Five principles boards should consider (NACD)

I

Boards need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue

II

Boards should understand the legal implications of cyber risks as they related to their company’s specific circumstances

III

Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda

Five principles boards should consider (NACD)

IV

Boards should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget

V

Board-management discussion of cyber-risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach

Cybersecurity frameworks

Common Frameworks

01 NIST Cybersecurity

02 ISO 27002

03 CIS Critical Security Controls

NIST Cybersecurity Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology	• Anomalies and Events • Detection Processes • Security Continuous Monitoring	• Communications • Improvements • Mitigation • Response Planning	• Communications • Improvements • Recovery Planning • Analysis

ISO 27002

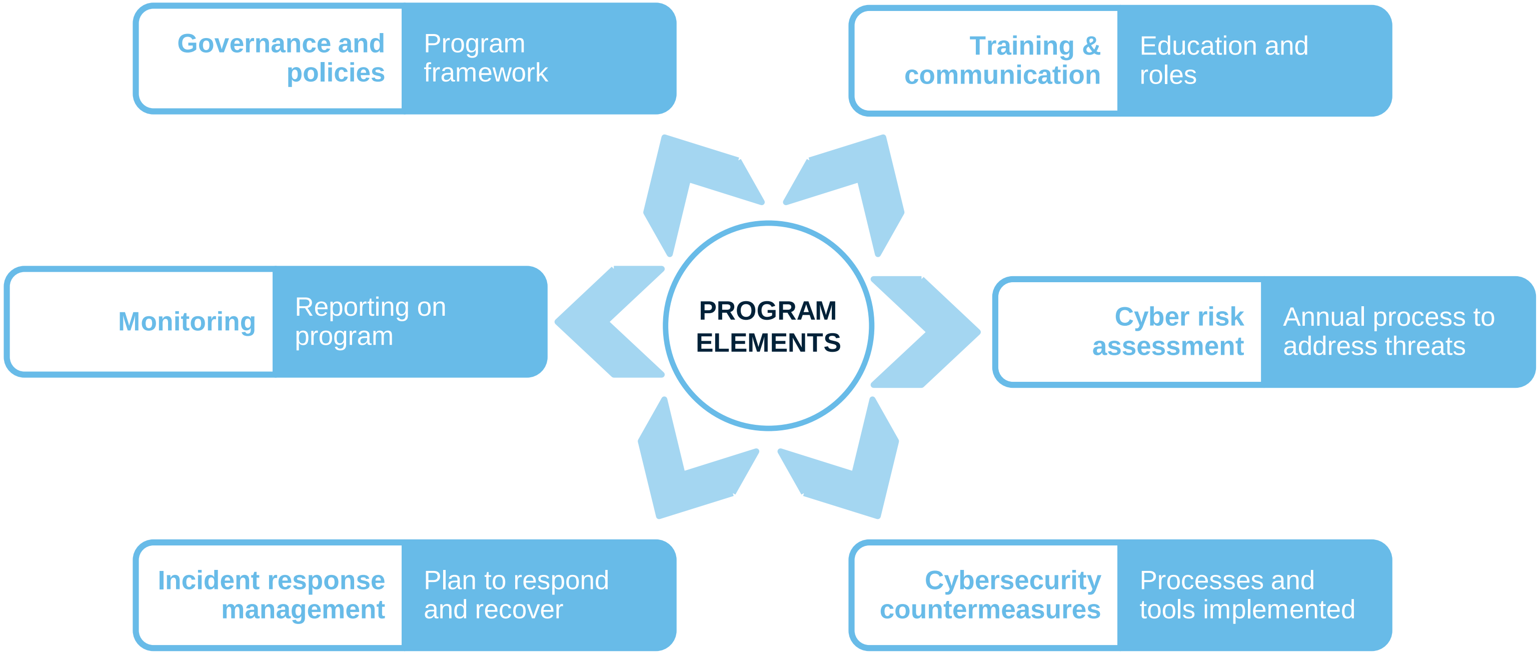
- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptology
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development, and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Information Security Aspects of Business Continuity
- Compliance

Center for Internet Security
Critical Security Controls

- #1: Inventory of Authorized and Unauthorized Devices
- #2: Inventory of Authorized and Unauthorized Software
- #3: Secure Configurations for Hardware and Software
- #4: Continuous Vulnerability Assessment and Remediation
- #5: Controlled Use of Administrative Privileges
- #6: Maintenance, Monitoring, and Analysis of Audit Logs
- #7: Email and Web Browser Protections
- #8: Malware Defenses
- #9: Limitation and Control of Network Ports
- #10: Data Recovery Capability
- #11: Secure Configurations for Network Devices
- #12: Boundary Defense
- #13: Data Protection
- #14: Controlled Access Based on the Need to Know
- #15: Wireless Access Control
- #16: Account Monitoring and Control
- #17: Security Skills Assessment and Appropriate Training to Fill Gaps
- #18: Application Software Security
- #19: Incident Response and Management
- #20: Penetration Tests and Red Team Exercises

Key elements of a cybersecurity program

Cybersecurity program elements



PROGRAM ELEMENTS

Governance and policies – Program framework

Training & communication – Education and roles

Monitoring – Reporting on program

Cyber risk assessment – Annual process to address threats

Incident response management – Plan to respond and recover

Cybersecurity countermeasures – Processes and tools implemented

Cybersecurity program element example

EDUCAUSE 2016
Top Strategic Info Sec Issues #1:
Ensuring that members of the institutional community (students, faculty, staff) receive information security education and training

Training and communication

- > Embed security within key business processes
- > IT topics must be translated into meaningful information (common language)
- > Involve everyone; education and building consensus is critical among all stakeholders
- > Train continually, and look for active learning scenarios
- > Leadership must establish the tone at the top
- > Put messages in context of audience (e.g., faculty, staff, student workers, researchers)

Cybersecurity program element example

EDUCAUSE 2016
Top Strategic Info Sec Issues #2:
Developing an effective information security strategy that responds to institutional organization and culture and that elevates information security concerns to institutional leadership

Governance and policies

> Figure out which assets really matter (e.g., crown jewels)

> Understand all information systems at a granular level

> Must have documented and approved policies

> A clear definition of risk tolerance levels is required

> Program must be tailored to the institution and higher education environment

> Process must be iterative, dynamic to adapt to constant change

Cybersecurity program element example

EDUCAUSE 2016
Top Strategic Info Sec Issues #3:
Planning for and implementing next-generation security technologies to respond to evolving threats

Cybersecurity counter-measures

- > Policies and procedures are foundational
- > Layered security is critical (e.g., defense in depth)
- > Must use automated and modern systems to monitor and alert
- > Use a combination of preventative and detective controls in both IT and business processes
- > Technologies must address modern threats (e.g., APT, DDOS)
- > Ultimately, controls that are commensurate with the value of the assets you are trying to protect must be deployed

Cybersecurity audit and reporting

Example board and audit activities

Board questions

- What do we consider our most valuable assets?
- How does our IT system interact with those assets?
- Do we believe we can fully protect those assets?
- If not, what would it take to feel comfortable that our assets were protected?

Audit checklists

- Review data and system inventories for completeness and relationships
- Review data classification and records retention practices
- Review procedures and standards for securing data and systems against standards (e.g., NIST, SANS, CIS)

Example board and audit activities

Board questions

- Are we considering the cybersecurity aspects of our major decisions, such as partnerships, new programs, international expansion, and new vendors in a timely fashion?
- What is the institution doing to monitor and address cybersecurity legal, regulatory, and industry developments?

Audit checklists

- Assess cybersecurity roles and responsibilities for proactive involvement in major decisions
- Assess compliance with various cybersecurity related regulatory requirements (e.g., PCI, HIPAA)

Example board and audit activities

Board questions

- What training do employees receive regarding cybersecurity?
- What are criteria for a cyber incident to be communicated to the Board?
- When was institution’s cyber liability insurance coverage last reviewed, who reviewed it, and what were results of the review?

Audit checklists

- Review training program and participation rates
- Assess cyber incident reporting for type and amount of information at issue; legal, regulatory, and industry requirements and practices; financial amount at issue
- Review cyber liability insurance coverage for deductibles, amount, coverage

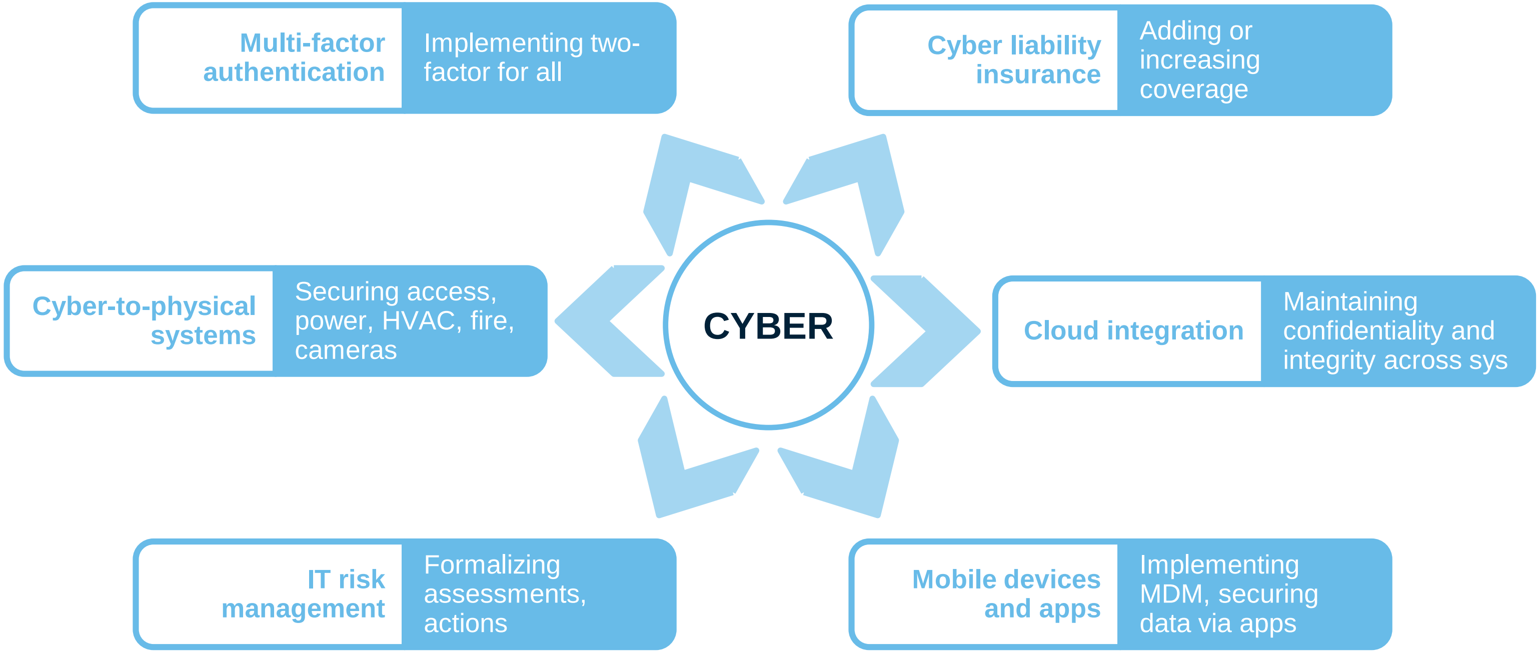
Potential metrics for reporting

Cybersecurity Governance Sample Metrics

Organizational & performance	Operational	Technological	Business process	Business value	Compliance
Employee training participation	Number of incidents per security events	Number of systems not current with security reqs.	Number of business processes with sensitive data	Value of critical data by area	Number and status of regulatory reqs. controls
Status of cybersecurity plan objectives	Number of successful and unsuccessful attacks	Number of vulnerabilities enumerated and remediated	Processes using vendor vs. in-house systems	Cyber liability insurance coverage	Number of policy exceptions implemented

Evolving areas of cybersecurity in higher education

Evolving cyber areas



CYBER

Multi-factor authentication – Implementing two-factor for all

Cyber liability insurance – Adding or increasing coverage

Cyber-to-physical systems – Securing access, power, HVAC, fire, cameras

Cloud integration – Maintaining confidentiality and integrity across sys

IT risk management – Formalizing assessments, actions

Mobile devices and apps – Implementing MDM, securing data via apps

Summary

Summary

Cybersecurity is now a more impactful enterprise-wide risk

Threats and regulatory requirements are more complex, especially in shared governance environment

Board, management, and internal audit all have a role in effective cybersecurity governance

Regardless of framework, there are key foundational elements for an effective cybersecurity program

Presenter contact info

Mike Cullen

mike.cullen@bakertilly.com

703 923 8339

Required disclosure and Circular 230 Prominent 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.

Pursuant to the rules of professional conduct set forth in Circular 230, as promulgated by the United States Department of the Treasury, nothing contained in this communication was intended or written to be used by any taxpayer for the purpose of avoiding penalties that may be imposed on the taxpayer by the Internal Revenue Service, and it cannot be used by any taxpayer for such purpose. No one, without our express prior written permission, may use or refer to any tax advice in this communication in promoting, marketing, or recommending a partnership or other entity, investment plan or arrangement to any other party.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International. © 2016 Baker Tilly Virchow Krause, LLP.