Protect Your Institution with Effective Cybersecurity Governance

© Baker Tilly Virchow Krause, LLP

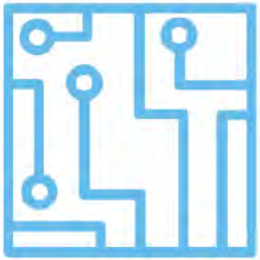
Objectives

BAKER TILLY

- Recall the changing cybersecurity risk landscape
- Describe key elements of an effective cybersecurity program
- Demonstrate strategies for auditing and presenting on cybersecurity program effectiveness

© Baker Tilly Virchow Krause, LLP

Cybersecurity landscape



© Baker Tilly Virchow Krause, LLP

IT changes

BAKER TILLY

PAST

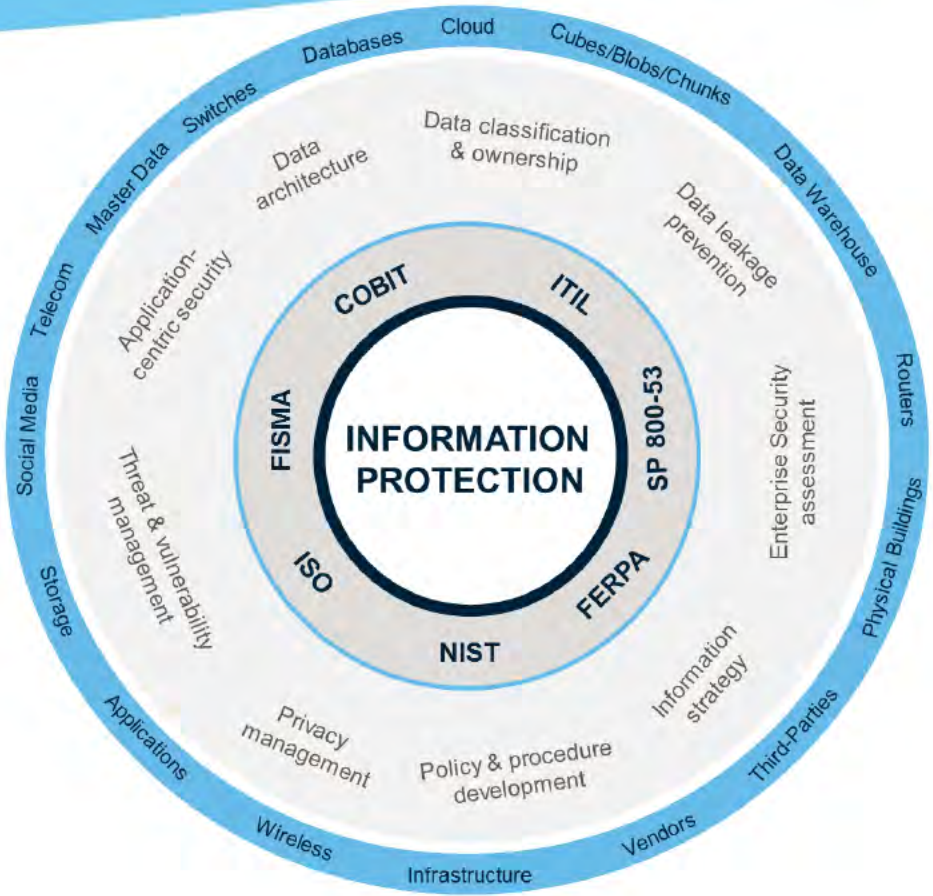
- Mostly physical assets (plants, equipment) - relatively few digitized assets
- Simple, unsophisticated attacks (e.g., web site defacement to embarrass)
- IT budgeted HW/SW expenditures; managed deployment and use
- Self-contained IT environment with limited complexity; limited use of third parties
- 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 third parties/vendors
- Mobile access to apps containing personal/financial data and use of BYOD

© Baker Tilly Virchow Krause, LLP

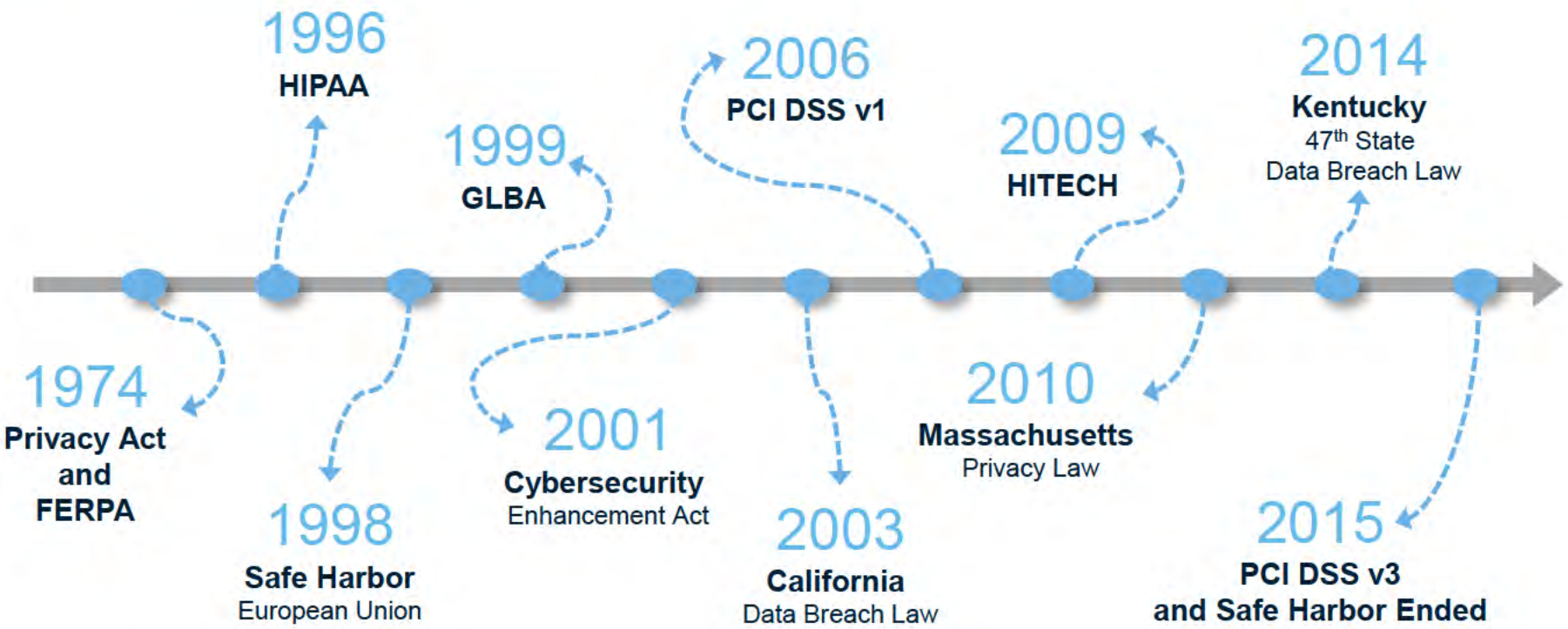
Information protection changes



© Baker Tilly Virchow Krause, LLP

Regulatory changes

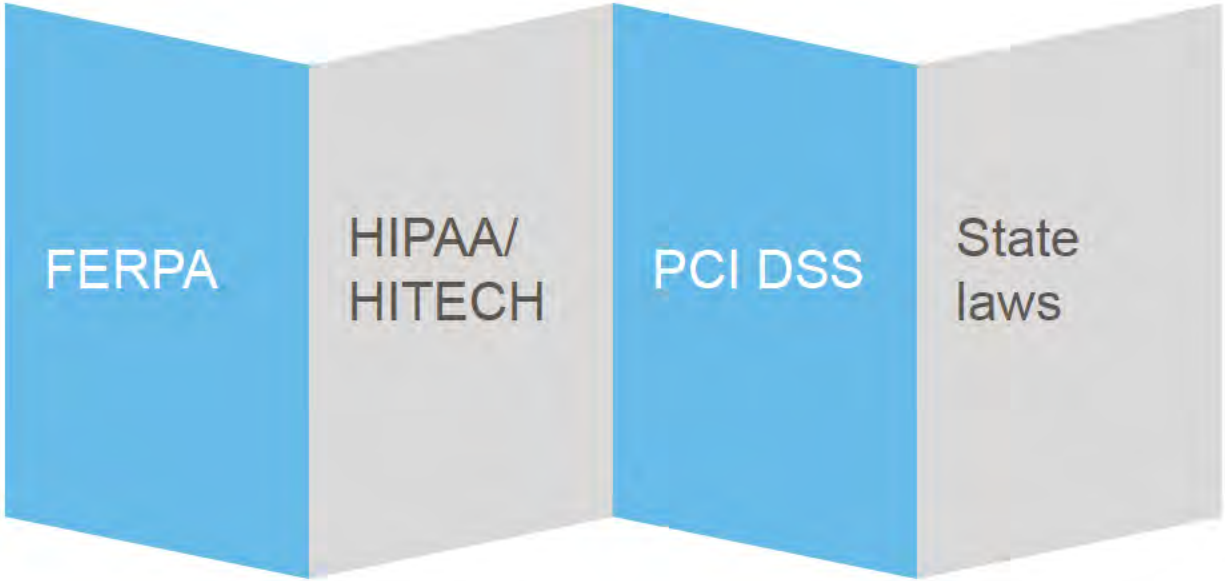
BAKER TILLY



© Baker Tilly Virchow Krause, LLP

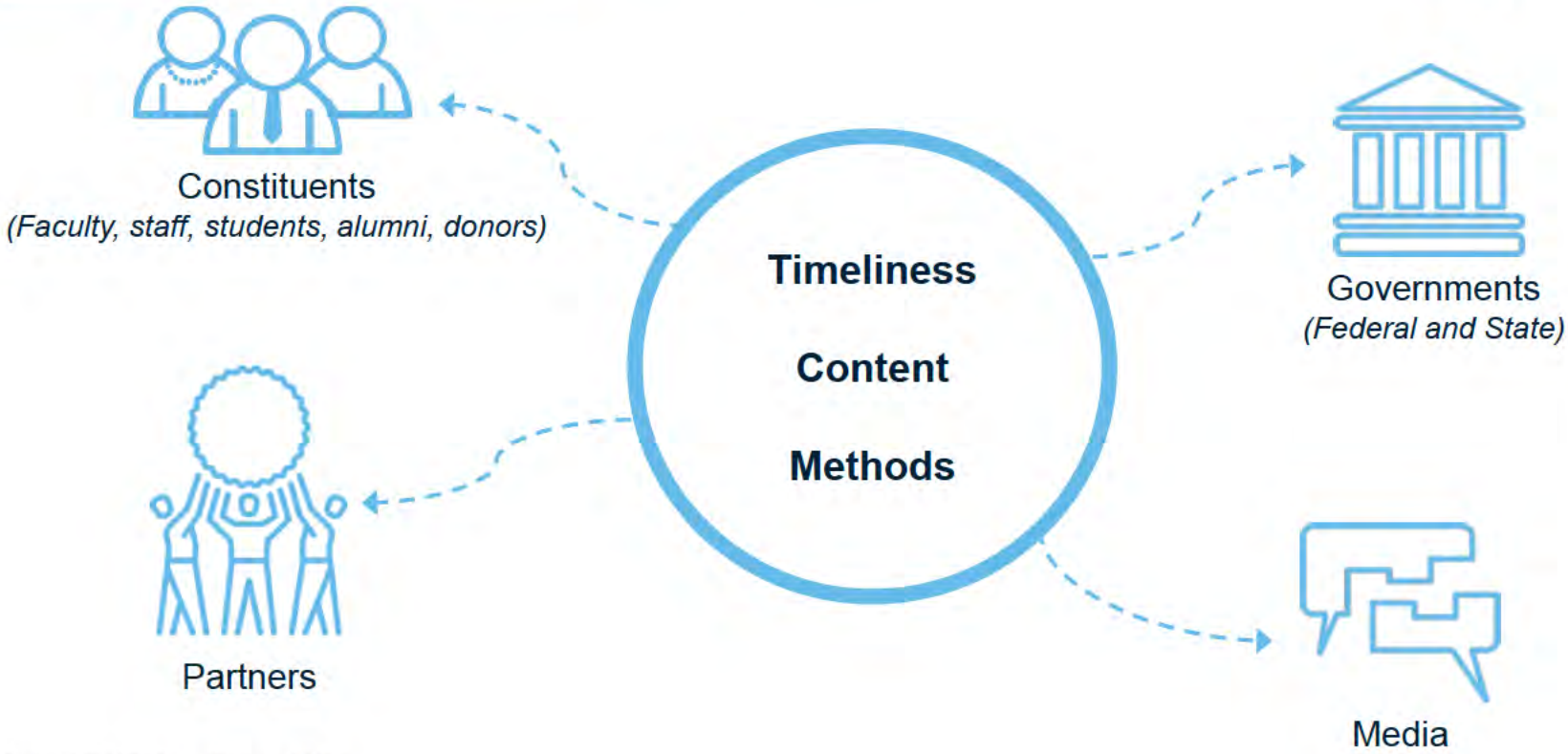
Higher education regulatory changes

BAKER TILLY



© Baker Tilly Virchow Krause, LLP

Changes in required disclosures



© Baker Tilly Virchow Krause, LLP

Cybersecurity as an enterprise-wide concern

© Baker Tilly Virchow Krause, LLP

Cyber attacks in the news

BAKER TILLY

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

© Baker Tilly Virchow Krause, LLP

Litigation involving cybersecurity and data breaches

BAKER TILLY

- 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

© Baker Tilly Virchow Krause, LLP

Five principles boards should consider (NACD)

BAKER TILLY

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

© Baker Tilly Virchow Krause, LLP

Five principles boards should consider (NACD)

BAKER TILLY

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

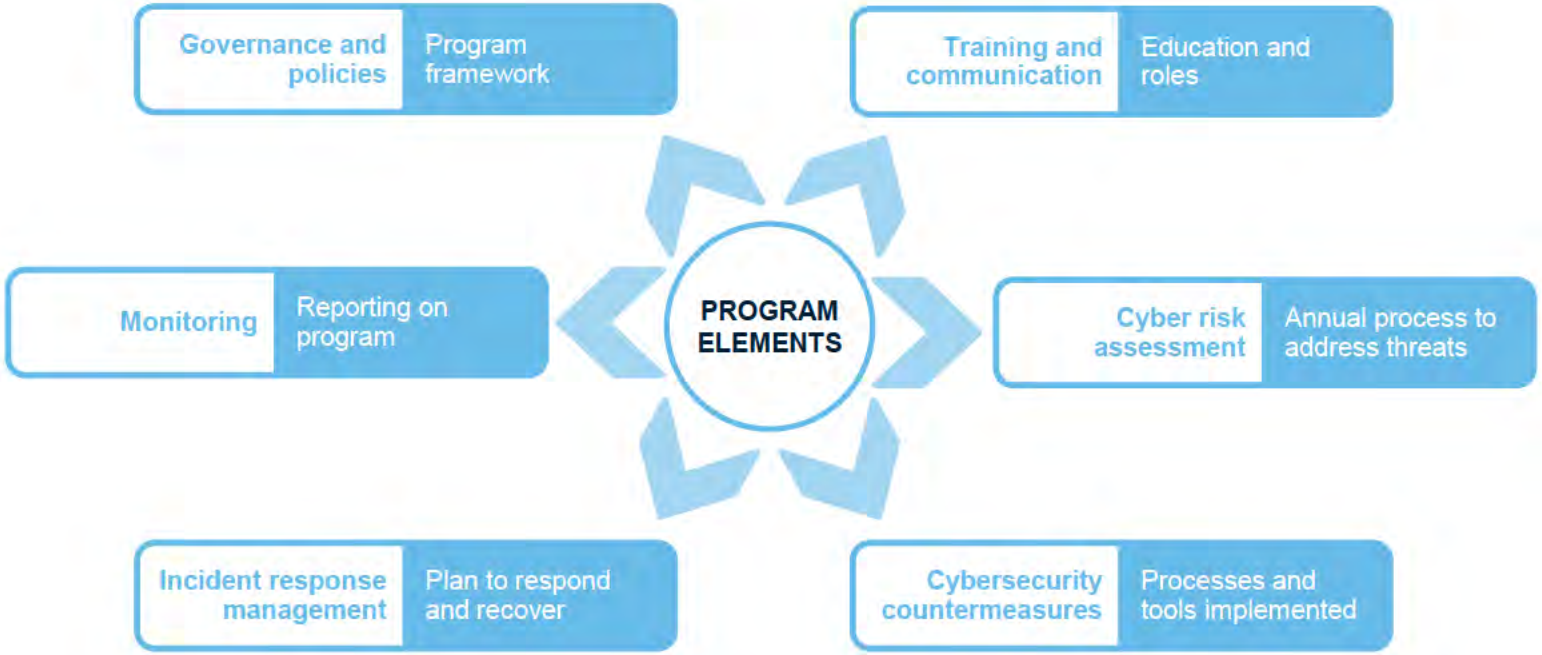
V Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach

© Baker Tilly Virchow Krause, LLP

Key elements of a cybersecurity program

© Baker Tilly Virchow Krause, LLP

Cybersecurity program elements



© Baker Tilly Virchow Krause, LLP

BAKER TILLY

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

© Baker Tilly Virchow Krause, LLP

BAKER TILLY

Cyber-risk assessment

- Figure out which assets really matter (e.g., crown jewels)
- Understand all information systems at a granular level
- A clear definition of risk tolerance levels is required
- The assessment must be tailored to the institution and higher education environment
- Process must be iterative, dynamic to adapt to constant change

© Baker Tilly Virchow Krause, LLP

BAKER TILLY

Cybersecurity counter-measures

- Policies and procedures must be documented
- Layered security is critical (e.g., multiple lines of defense in depth)
- Must use systems to automate and alert
- Use a combination of preventative and detective controls in both IT and business processes
- Ultimately, controls that are commensurate with the value of the assets you are trying to protect must be deployed

© Baker Tilly Virchow Krause, LLP

BAKER TILLY

Monitoring

- Practices must be documented
- Log event correlation is increasingly important
- Vendors and their systems should be included in monitoring activities
- Ongoing assessment of monitoring activities is critical to keep pace with change
- Frequent reporting must be done at multiple levels (e.g., department management, leadership, board)

© Baker Tilly Virchow Krause, LLP

Cybersecurity audit and reporting

© Baker Tilly Virchow Krause, LLP

Example board and audit activities

BAKER TILLY

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)

© Baker Tilly Virchow Krause, LLP

Example board and audit activities

BAKER TILLY

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)

© Baker Tilly Virchow Krause, LLP

Example board and audit activities

BAKER TILLY

Board questions

- What training do employees receive regarding cybersecurity?
- What are criteria for a cyber incident to be communicated to the Board?
- When was the institution's cyber liability insurance coverage last reviewed, who reviewed it, and what were the 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; and financial amount at issue
- Review cyber liability insurance coverage for deductibles, amount, and coverage

© Baker Tilly Virchow Krause, LLP

Potential metrics for reporting

BAKER TILLY

Cybersecurity governance sample metrics

Organizational and performance	Operational	Technological	Business process	Business value	Compliance
Employee training participation	Number of incidents per security events	Number of systems not current with security requirements	Number of business processes with sensitive data	Value of critical data by area	Number and status of regulatory requirements 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

© Baker Tilly Virchow Krause, LLP

Resources

BAKER TILLY

- CERT (http://www.cert.org/incident-management/)
- Department of Education Privacy Technical Assistance Center (PTAC) (http://ptac.ed.gov/)
- EDUCAUSE (www.educause.edu)
- Higher Education Information Security Council, HEISC (https://wiki.internet2.edu/confluence/display/2014infosecurityguide/)
- ISACA (www.isaca.org)
- NACD (www.nacdonline.org)
- NIST (www.nist.gov)

© Baker Tilly Virchow Krause, LLP