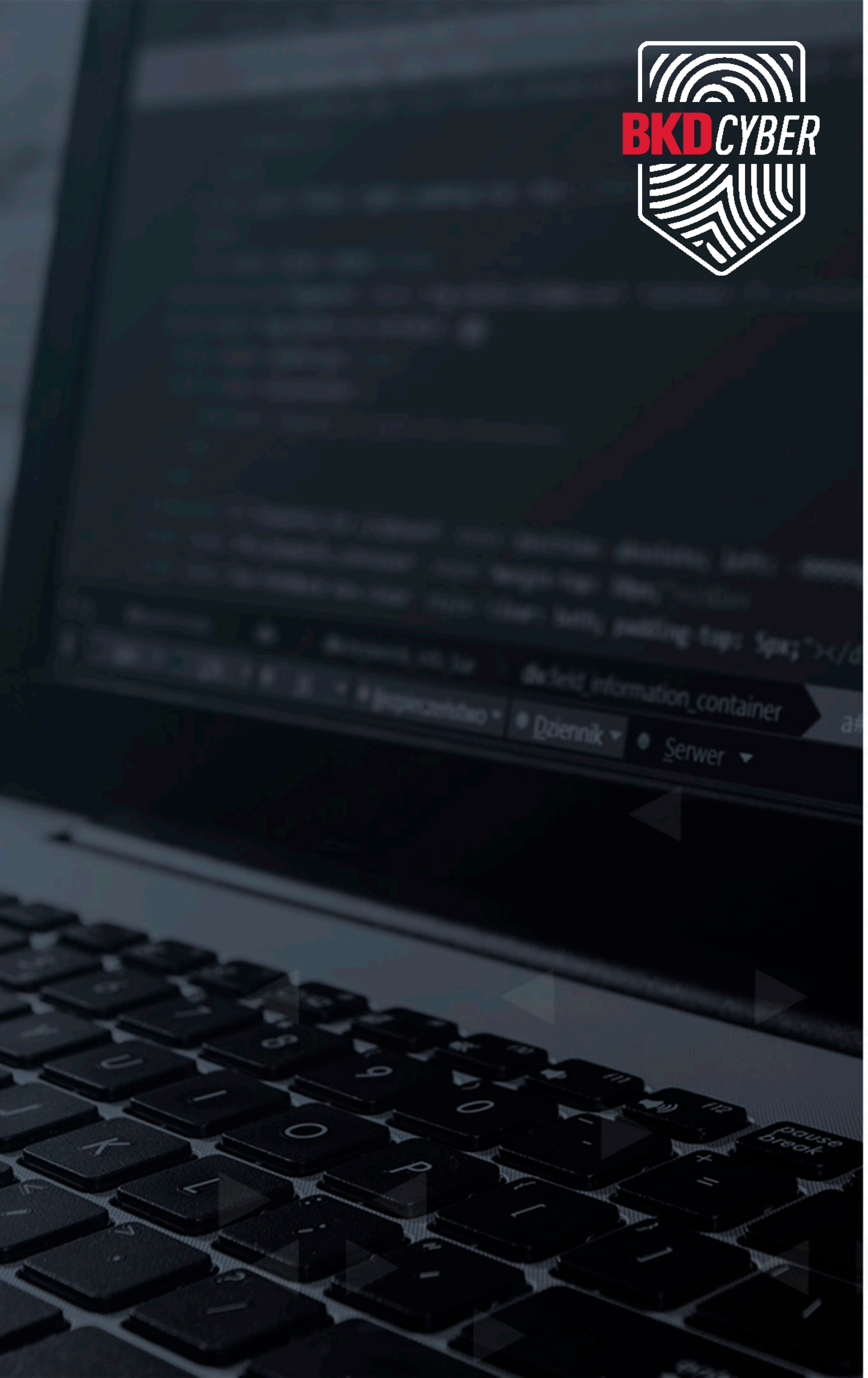
Everyone needs a trusted advisor. Who's yours?



BKD CYBER

The Connecticut Conference of Independent Colleges

CCIC

Est. 1932

Cybersecurity, A Boardroom, or Server Room Responsibility?

Enforcing Data Security in Accordance with GLBA, FTC, NIST

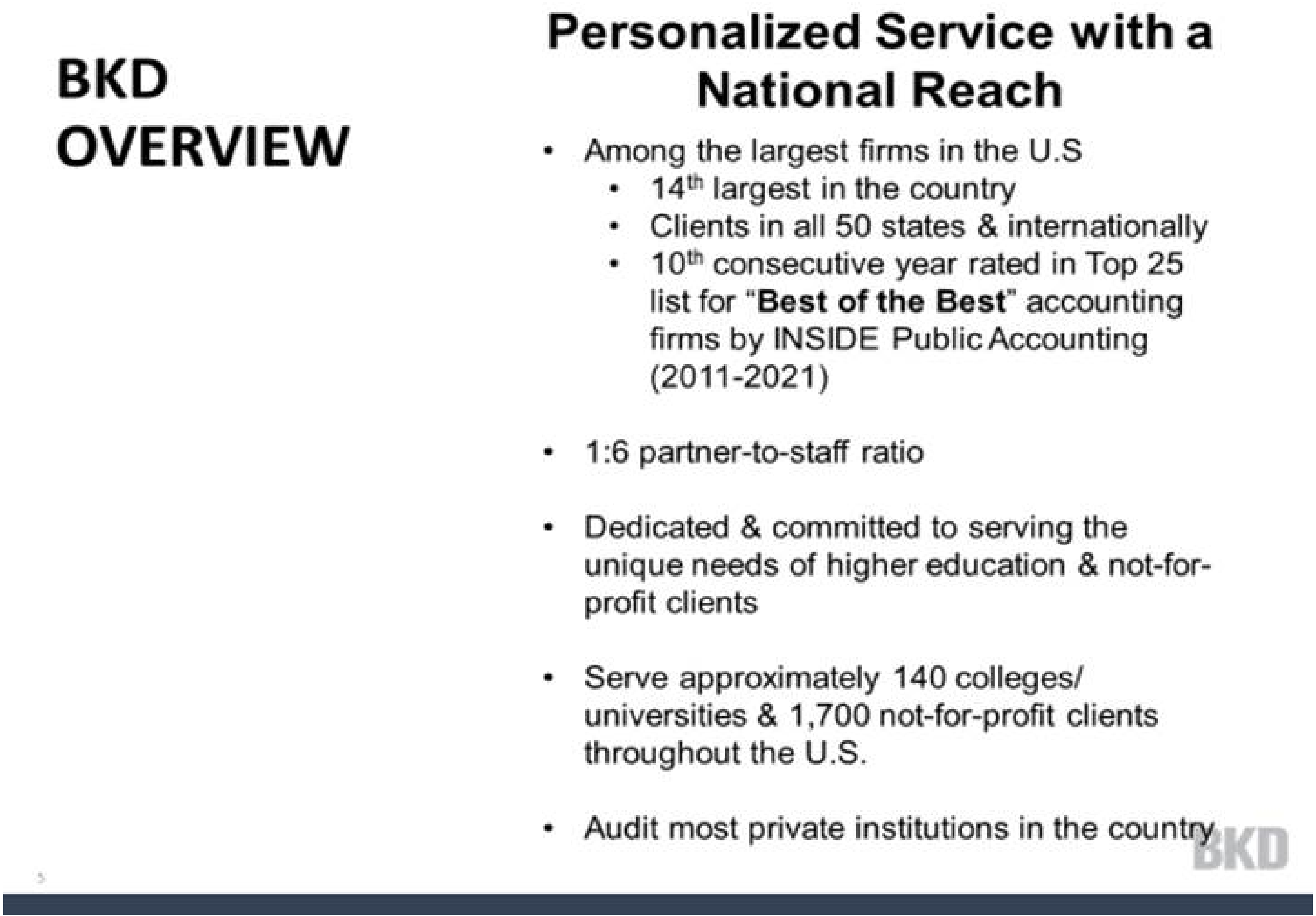
Data Protection Compliance Requirements

BKD CYBER

Introduction

Richard A. Cole, CPA
Partner
BKD, LLP.
rcole@bkd.com

BKD OVERVIEW



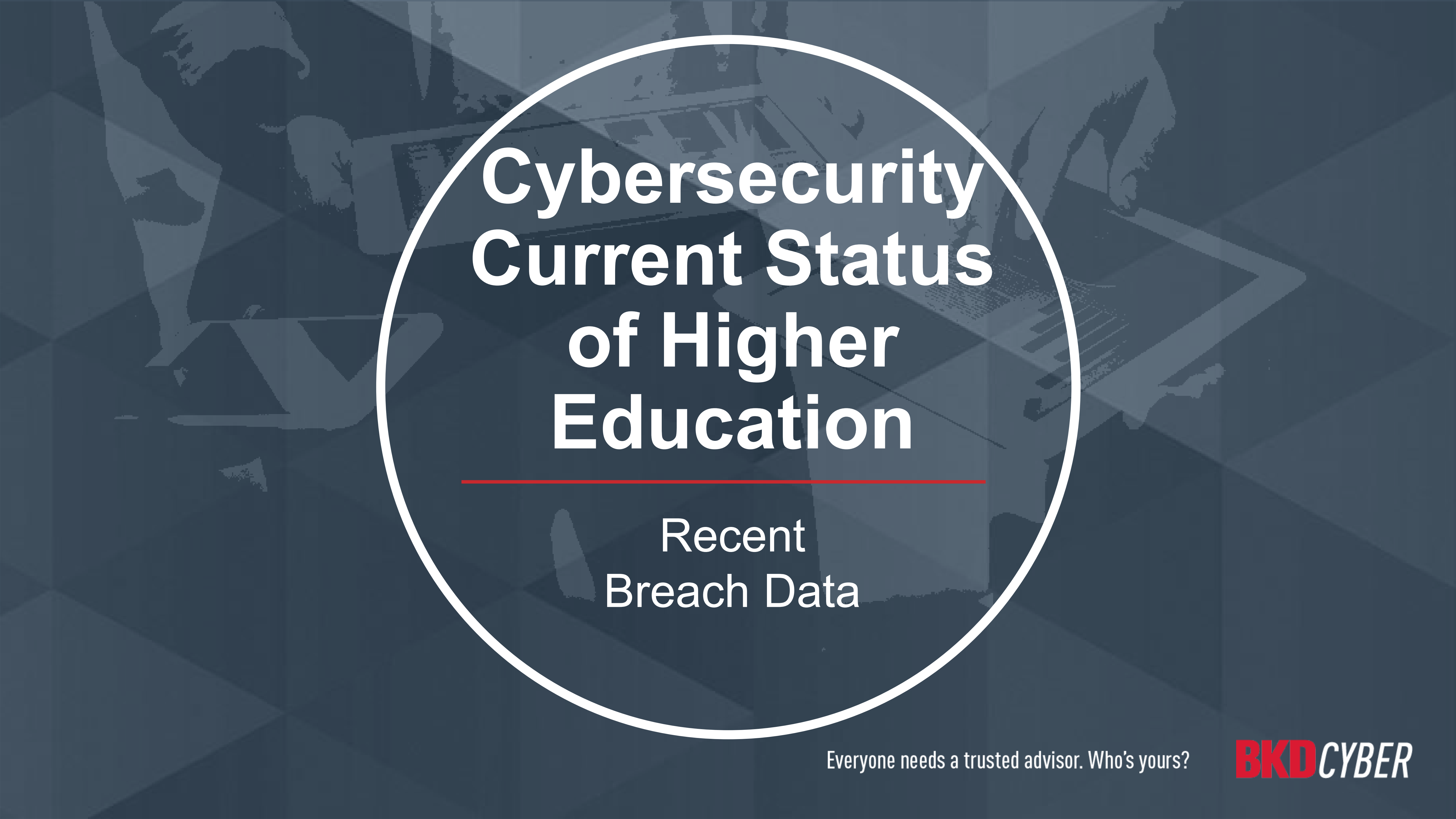
Personalized Service with a National Reach

- Among the largest firms in the U.S
  - 14th largest in the country
  - Clients in all 50 states & internationally
  - 10th consecutive year rated in Top 25 list for "**Best of the Best**" accounting firms by INSIDE Public Accounting (2011-2021)
- 1:6 partner-to-staff ratio
- Dedicated & committed to serving the unique needs of higher education & not-for-profit clients
- Serve approximately 140 colleges/ universities & 1,700 not-for-profit clients throughout the U.S.
- Audit most private institutions in the country

Presenter

Johnny Sanders. PCI QSA, CISM, CISA, Security+

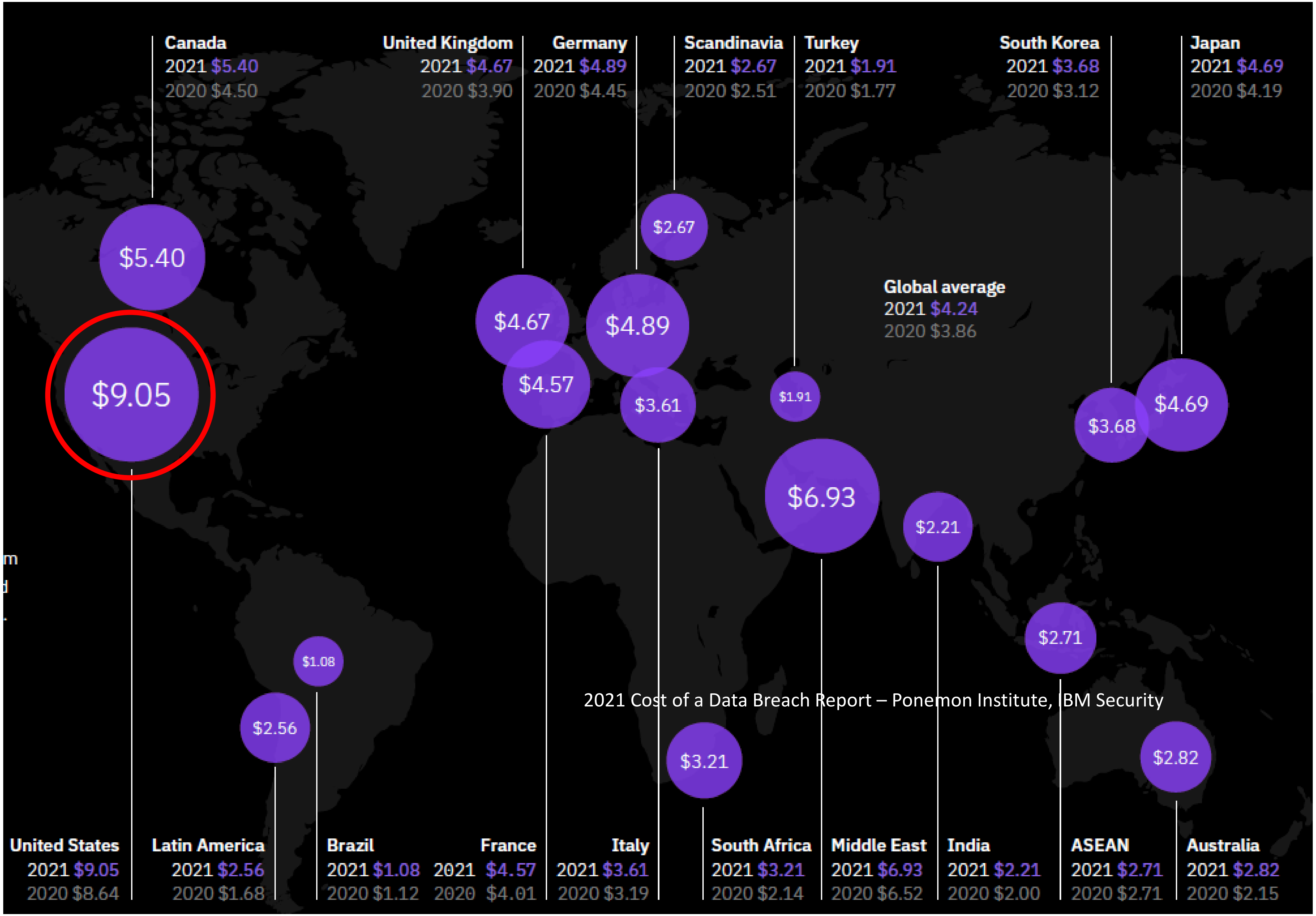
Senior Managing Consultant
BKD Cyber
jlsanders@bkd.com



Cybersecurity Current Status of Higher Education

Recent
Breach Data

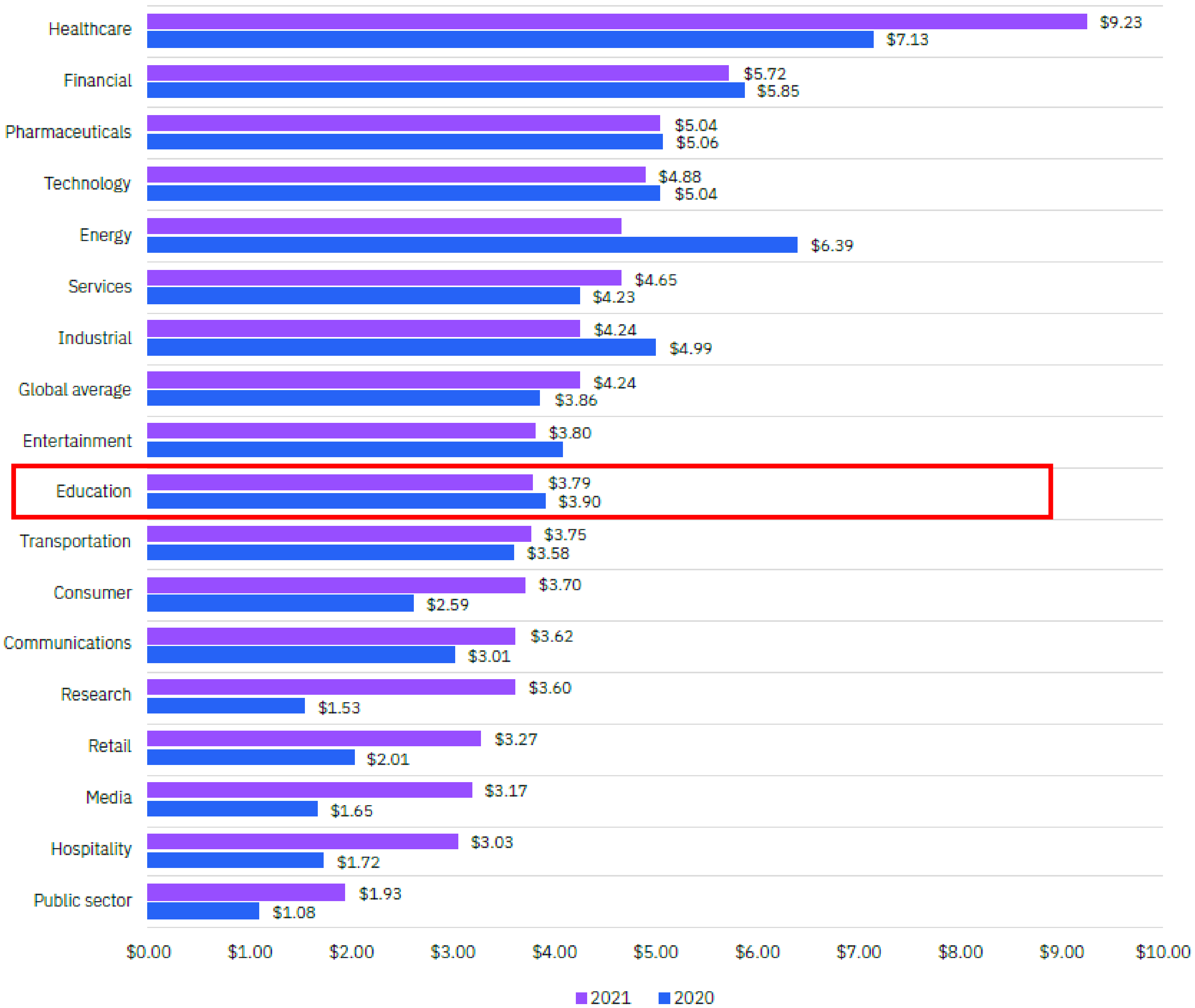
Breach Costs are up: The United States was the top country for average total cost of a data breach for the **eleventh year in a row**.



2021 Cost of a Data Breach Report – Ponemon Institute, IBM Security

Average total cost of a data breach by industry

Measured in US$ millions



Education $3.79m

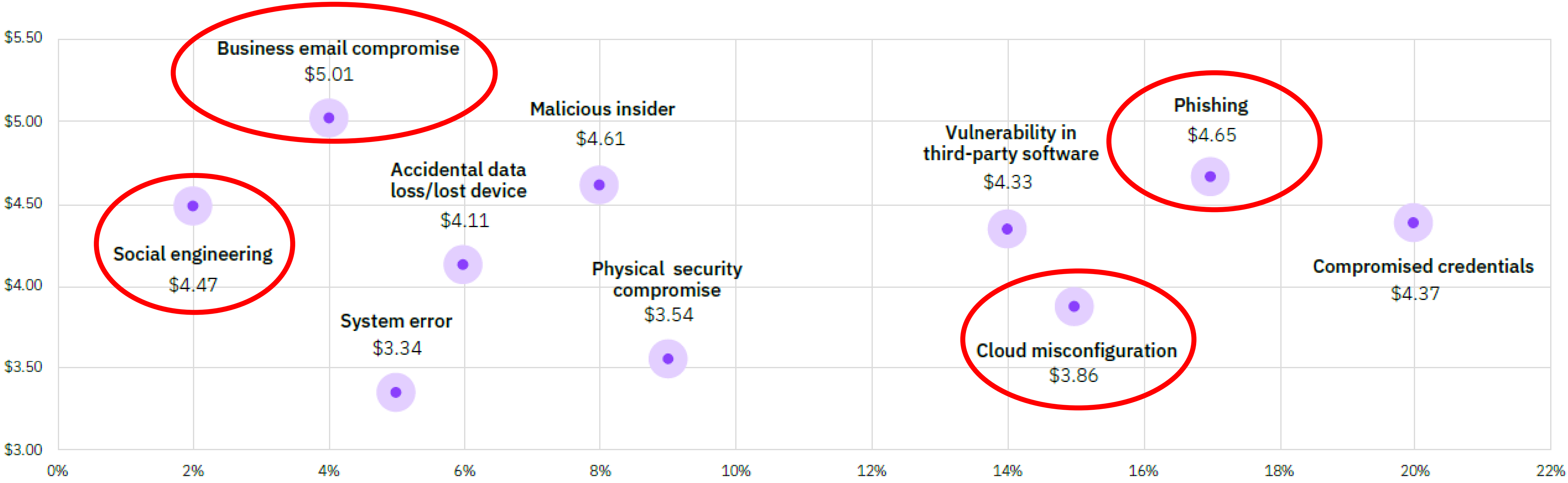
DOWN from $3.9m

2021 Cost of a Data Breach Report – Ponemon Institute, IBM Security

Average total cost and frequency of data breaches by initial attack vector

Measured in US$ millions

Education $3.79m



2021 Cost of a Data Breach Report – Ponemon Institute, IBM Security

Cell Phone Exercise

Testing Personal Data Protection

1. Remove your cell phone
2. Unlock it
3. While still unlocked, pass it to the person next to you
4. Feel free to explore the contents, data, email, photos and texts of the phone you now have
5. Take your time, you have until the end of this session to complete your search
6. No takers?
7. On average, how long do you think unauthorized parties (hackers) are inside the average company before they are detected?
8. 7 Months

2021 Cost of a Data Breach Report – IBM Security – Ponemon Institute

Breach Detection

Higher Education Averages:

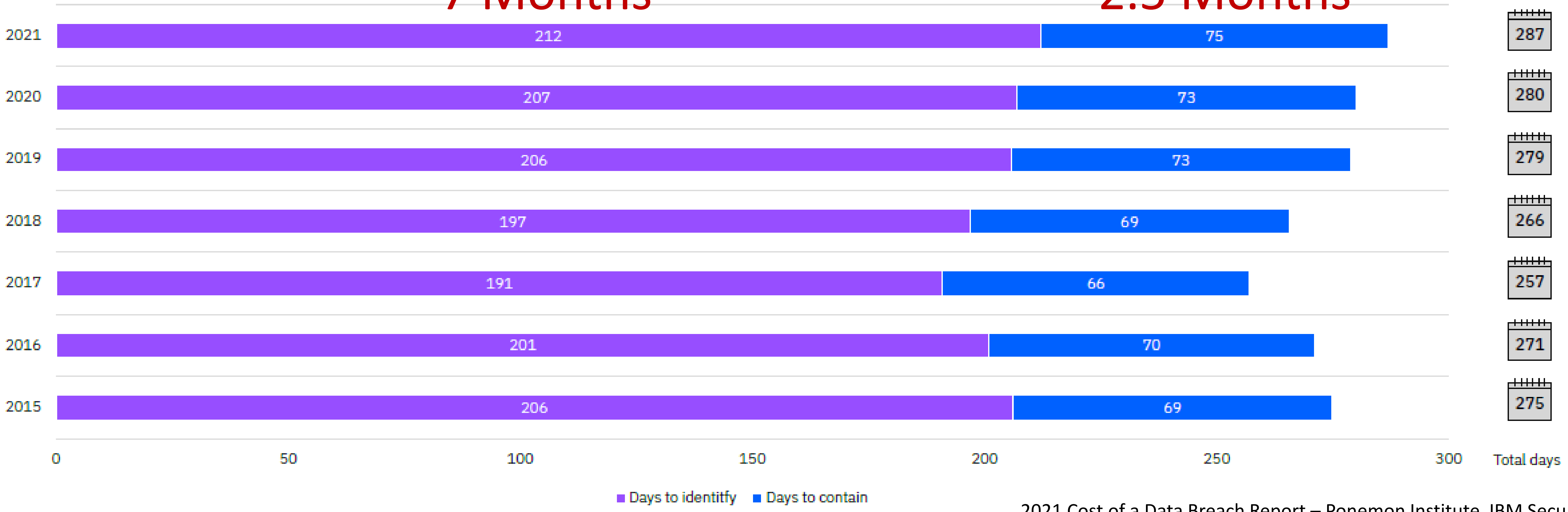
212 Days to detect a breach

Average time to identify and contain a data breach

Measured in days

7 Months

2.5 Months



2021 Cost of a Data Breach Report – Ponemon Institute, IBM Security

RANSOMWARE ATTACK

Your personal files are encrypted

You have 5 days to submit the payment!!!

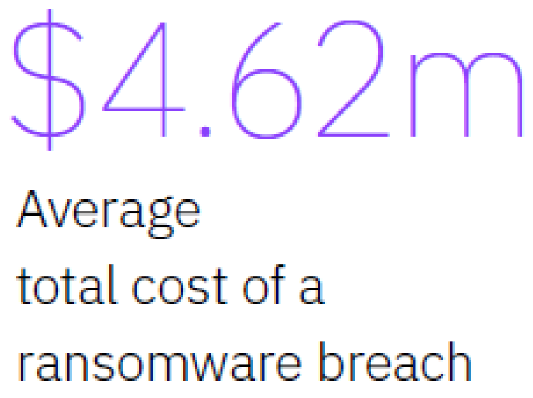
To retrieve the Private key you need to pay

Your files will be lost

Rank the data/industry you THINK is most targeted by hackers

1. NASA
2. Medical Research
3. Financial Systems
4. Healthcare (HIPAA)
5. Energy
6. Transportation
7. Retail
8. Payment Card
9. Government
10. Meatpacking/processor

The Value of YOUR Data



$4.62m

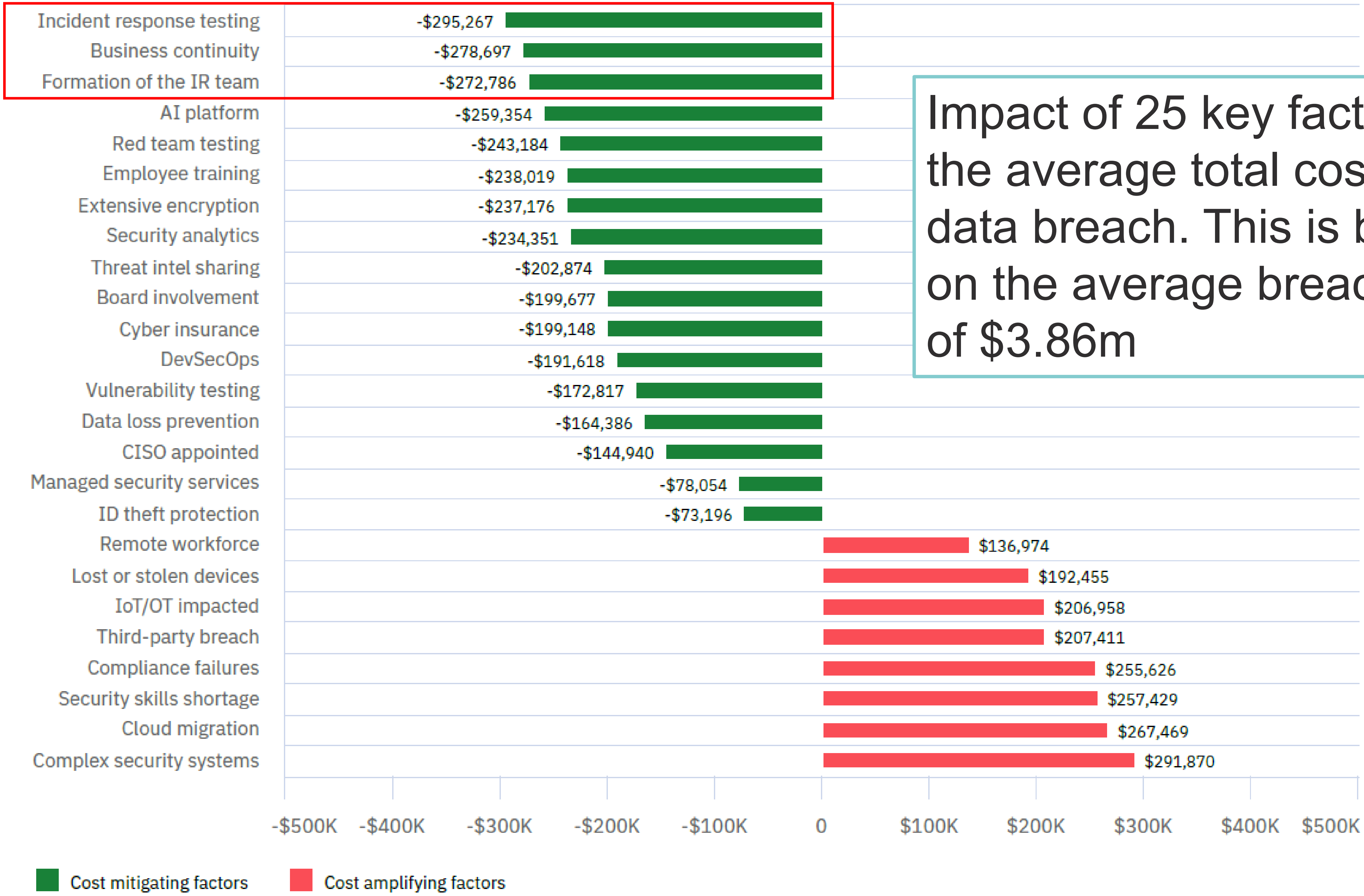
Average
total cost of a
ransomware breach

Daily business operations rely on data that may not be deemed critical.

Part of evaluating risk is maintaining data classification assessments.

Do not let yourself believe you are not a target.

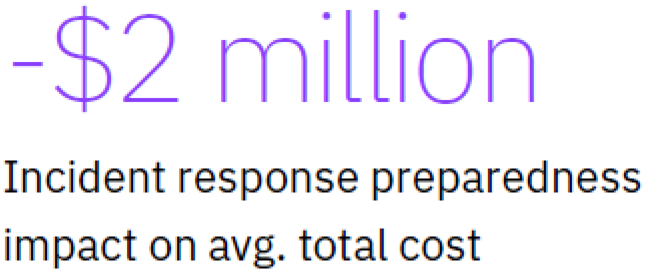
Impact of 25 key factors on the average total cost of a data breach. This is based on the average breach cost of $3.86m



BKDCYBER

Incident Response

GLBA Requirement, and Saves Money



-$2 million

Incident response preparedness impact on avg. total cost

"The average total cost of a data breach for companies with an IR team that also tested an IR plan using tabletop exercises or simulations was $3.29 million, compared to $5.29 million for companies with neither an IR team nor tests of the IR plan — **a difference of $2 million**. The cost difference between these groups was $1.23 million in the 2019 study."

2020 Cost of a Data Breach Report – IBM Security – Ponemon Institute

Where Do We Begin?

Why Information Security is a Management Function

Where do We Begin?

Are you without an established information security program? initiating one can be tough!

Set Goals
Where do we want to be? Management must set goals

Select a Framework
Agree to follow a security framework NIST/COBIT/ISO

Regulatory Requirements
Regulatory requirements will guide many security standards (GLBA)

Inventory and Classification
Identify all IT assets and determine their data classification levels

Risk Assessment
Identify risk and controls to remediate risk to an acceptable level

Guidance (Policies)
Policies and procedures should be established to enforce controls and provide guidance

So WHY is This a Boardroom Responsibility?

Stakeholders Establish goals and strategies

Senior Leadership must establish the security goals of the institution and set the overall tone of the program.

Examples:

- Seeking/demanding all staff and faculty support for compliance with institution’s security policies
- Making all users aware that new, more strict requirements to improve security are on their way
- Informing the institution that leadership supports the initiative that will result in better/more training, compliance with ED, Federal Government laws, and industry best practices for data security

What Rules Should Our Program Follow?

Selecting a Framework

Are we on the same page?

Every organization should select a security framework to follow. Framework examples:

- Payment Card Industry (PCI)
- ISO 27001/27002
- CIS Critical Security Controls
- NIST 800-53r5, 800-171, Cybersecurity Framework
- Cobit - Control Objectives for Information and Related Technology

Many frameworks have similar control suggestions, the key is to adopt something, organization wide.

What About Regulatory Requirements?

Guidance from the Department of Education and Federal Government

What does ED and the Government expect of us?

HEA (Higher Education Act)

FERPA (Family Educational Rights and Privacy Act)

Student Aid Internet Gateway (SAIG) Enrollment Agreement

FISMA Controls (NIST SP 800-53 rev 4)

Protecting CUI (NIST SP 800-171)

Gramm-Leach-Bliley Act (GLBA)

General Data Protection Regulation (GDPR)

NOTE: some security requirements only apply to those systems and users who have access to student aid, financial or other data deemed sensitive by management

What About Regulatory Requirements?

Guidance from the Department of Education and Federal Government

Dear Colleague Letters

DCL ID: GEN-15-18, July 29, 2015

In addition to other provisions within the SAIG Agreement, **FSA requires institutions to comply with the Gramm-Leach-Bliley Act**. Under Title V of the Gramm-Leach-Bliley Act, financial services organizations, including institutions of higher education, are required to ensure the security and confidentiality of customer records and information. This requirement was recently added to the Program Participation Agreement and is reflected in the Federal Student Aid Handbook

What About Regulatory Requirements?

Guidance from the Department of Education and Federal Government

Dear Colleague Letters

DCL ID: GEN-16-12, July 1, 2016

We also advise institutions that important information related to cybersecurity protection is included in the National Institute of Standards and Technology (NIST) Special Publication 800-171 (NIST SP 800-171). Specifically, the NIST SP 800-171 identifies recommended requirements for ensuring the appropriate long-term security of certain Federal information in the possession of institutions. **NOTE: NIST and the Cybersecurity Maturity Model Certification (CMMC) compliance are vital to departments receiving DoD funding.**

What does GLBA Mean for Higher ED

Protection Requirements

When did the Federal Trade Commission (FTC) first recognize institutions of higher learning as financial institutions and require you to be compliant with the GLBA?

A. 1999
B. 2002
C. 2015
D. 2019

2002

When were you expected to be compliant with the Safeguards Rule within the GLBA?

A. 2002
B. 2003
C. 2018
D. 2019

May 2003

What Does GLBA Mean?

Gramm-Leach-Bliley Act

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

314.1 (a) Purpose. This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth **standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information**.

What Does GLBA Mean?

Gramm-Leach-Bliley Act

§314.3 Standards for safeguarding customer information.
(a) Information security program

You shall **develop, implement, and maintain a comprehensive information security program that is written** in one or more readily accessible parts and **contains administrative, technical, and physical safeguards** that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.

What Does GLBA Mean?

Gramm-Leach-Bliley Act

§314.4 Elements

(a) **Designate an employee or employees to coordinate your information security program.**

The policy should address who has enforcement authority and overall oversight of the program.

Note: Information security programs should be implemented **institution wide**.

What Does GLBA Mean?

Gramm-Leach-Bliley Act

§314.4 Elements

(b) **Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information** that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and **assess the sufficiency of any safeguards in place to control these risks**

Note: This is an information security/IT asset-based risk assessment. This document should capture threats, risk, and vulnerabilities and clearly identify the controls in place to reduce this risk.

What Does GLBA Mean?

Gramm-Leach-Bliley Act

§314.4 Elements

NOTE: Risk assessments belong to management

A key step in the risk assessment process is to communicate the assessment results and share risk-related information with stakeholders. The objective of this step is to ensure that decision makers across the organization have the appropriate risk-related information needed to inform and guide risk decisions.

What Does GLBA Mean?

Gramm-Leach-Bliley Act

§314.4 Elements

(c) **Design and implement information safeguards to control the risks you identify through risk assessment**, and **regularly test** or otherwise monitor the effectiveness of the safeguards' **key controls, systems, and procedures**.

This step addresses implementation of controls to reduce the risk and the requirement to regularly test these controls.

What Does GLBA Mean?

Gramm-Leach-Bliley Act

§314.4 Elements

(d) **Oversee service providers**, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

Vendor management programs are generally established to address this requirement. An important step is the annual review of key vendors to evaluate SOC reports and other testing.

What Does GLBA Mean?

Gramm-Leach-Bliley Act

§314.4 Elements

(e) **Evaluate and adjust** your information security program in light of the **results of the testing** and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

Basic requirement to monitor and maintain the information security program.

What Does GLBA Mean?

Gramm-Leach-Bliley Act

Understanding what GLBA means for HE institutions

Dear Colleague Letter GEN 16-12

“Under these GLBA requirements, Presidents and Chief Information Officers of institutions should have, at a minimum, evaluated and documented their current security posture against the requirements of GLBA and have taken immediate action to remediate any identified deficiencies.”

Information for Financial Aid Professionals (IFAP)

February 28, 2020

“The Gramm-Leach-Bliley Act (GLBA), which was signed into law on November 12, 1999, created a requirement that financial institutions must have certain information privacy protections and safeguards in place. The Federal Trade Commission (FTC) has enforcement authority for the requirements and has determined that institutions of higher education (institutions) are financial institutions under GLBA.”

“When an (financial) audit report that includes a GLBA audit finding is received by the Department, we will refer the audit to the FTC. Once the finding is referred to the FTC, that finding will be considered closed for the Department’s audit tracking purposes. The FTC will determine what action may be needed as a result of the GLBA audit finding.”

Why Do We Care About GLBA?

In addition to the security and privacy requirements of the Family Educational Rights and Privacy Act (FERPA), schools that participate in the Federal Title IV Educational Assistance Programs must comply with additional security requirements.

The most significant being, the GLBA. The lack of compliance with GLBA's privacy and security requirements can subject schools to GLBA penalties, but more importantly, **Title IV funding may be restricted or withheld**. If Title IV schools suffer cybersecurity breaches or are found to be deficient in cybersecurity protections, the Department of Education has made clear that such schools may face restrictions on Title IV funding, including a complete loss of eligibility.

Why Do We Care About GLBA?

Audit Findings

Auditors are expected to evaluate three information safeguard requirements of GLBA in audits of postsecondary institutions or third-party servicers under the regulations in 16 C.F.R. Part 314

1. The institution must designate an individual to coordinate its information security program.
2. The institution must perform a risk assessment that addresses three required areas described in 16 C.F.R. 314.4(b):
   a) Employee training and management;
   b) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
   c) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
3. The institution must document a safeguard for each risk identified in Step 2 above.

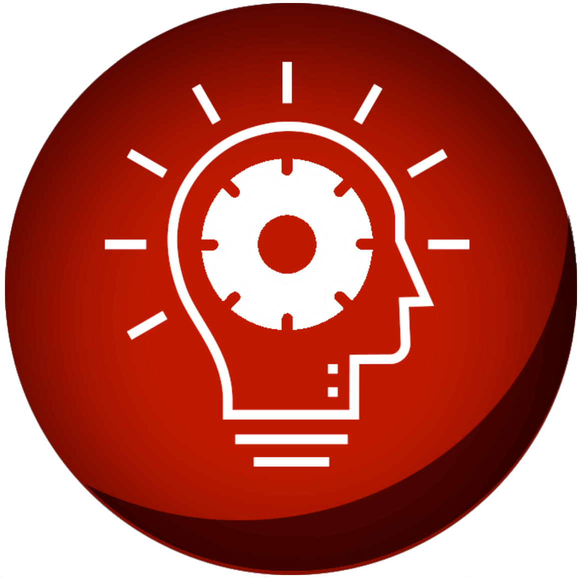
When an auditor determines that an institution or servicer has failed to comply with any of these GLBA requirements, the finding will be included in the institution's audit report..

Major Risks & Cybersecurity Gaps in HE

Information Security 101

Single Biggest Risk - Users

Importance of Awareness Training



Take me to your leader

C-level executives were 12 times more likely to be the target of social engineering attacks.

Training applies to everyone that has access to the institution network.

NOTE: The 2014 Target breach started with an HVAC Contractor

Verizon Data Breach Report

Single Biggest Risk - Users

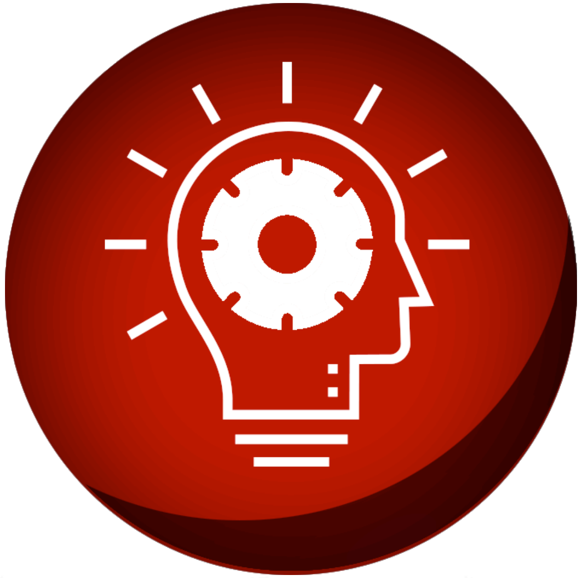
Importance of Awareness Training

The Johnny Rule: Treat all users like they are hostile

- We must protect institution, from us.
- **Enable Multi-Factor authentication, starting with high-risk users first (management, finance, student aid administrators etc.)**
- Johnny Rule # 2 – **"minimum required rights to perform daily duties."** Users with increased privileges will increase damage.
- **Most breaches are caused by human error**. This includes staff, faculty, system admins
- Remove admin rights at the local machine. End users with administrative privileges creates a significant risk and violates NIST 800-171 requirements.

Single Biggest Risk - Users

Importance of Awareness Training



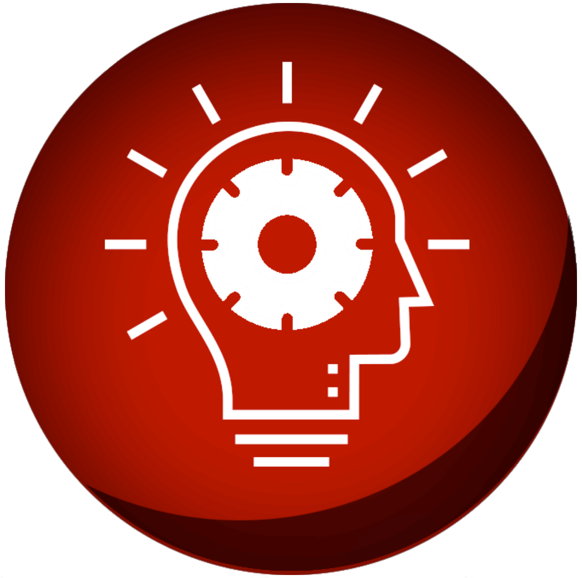
Training and Awareness

- Cybersecurity is as much a mindset as it is technical.
- Management, not IT, has to set this tone (verbally and through policies).
- Your staff and faculty must be willing participants in the process. They must be DATA DEFENDERS
- Your staff and faculty must be trained to be human firewalls
- Strong information security policies, strong acceptable use policy complete with consequences for failing to comply

Note: Average cost of a HE breach, $3.79 million

Single Biggest Risk - Users

Importance of Awareness Training



Training and Awareness – reducing the risk

- Keeping your HUMAN firewall up to date
- Annual Training, at a minimum
- Methods to notify staff of emerging issues (REN-ISAC, EDUCAUSE)
- Assess their ability to detect social engineering attacks through phishing tests.
- **85-90% of all breaches and incidents relate to human error. Most are the result of phishing campaigns according to Verizon Data Breach Study**

We Have Cybersecurity Insurance!

But will it pay?

Cybersecurity Insurance

Quick Notes

- Policy applications are more detailed than before
  - Incorrect statements on the application can lead to denied or reduced claim payout
- Multifactor authentication requirements
  - Higher co-pays or denied applications if MFA is not in place
- Expect a forensics visit – these visits are vital as they help close the gaps that permitted the breach, but they also reveal weak controls.
  - Poor control environments may reduce claim payout

Final Thoughts

Do not wait on regulatory enforcement to make security and technology changes

Innovation outpaces regulation by at least 2 or 3 years.

Final Thoughts

Before, or after the breach….

The cybersecurity bill
WILL be paid.

Summary

- **GLBA is the law. Noncompliance puts title IV funds at risk – Ensuring compliance is NOT an IT function**
- End users are the single biggest security weakness
- Many control implementations needed are often free and available in systems currently owned by the institution.
- Initiation of stronger controls begins with management support.
- The "roadmap" to compliance is approximately 3 years.
- Training should be mandatory for 100% of staff and faculty and completed at least annually.
- Information security risk assessments and supporting policies must be maintained, reviewed and approved by the Executive Cabinet at least annually.

Questions?

Richard A. Cole, CPA – Partner - New York | 212.867.4000 | rcole@bkd.com

Rick has more than 25 years of experience serving nonprofit organizations. He is based in the New York office and is a member of BKD Higher Education Center of Excellence, which is an internal committee focused on addressing issues important to the higher education industry. Rick focuses on audits and advisory services for nonprofit and higher education organizations.

Before joining BKD in 2019, he worked at FASB, where he served as a supervising project manager for almost six years. In that role, he was the project manager on Accounting Standards Update (ASU) 2016-14, Presentation of Financial Statements of Not-for-Profit Entities; ASU 2018-08, Clarifying the Scope and Accounting Guidance for Contributions Received and Contributions Made; and ASU 2019-03, Updating the Definition of Collections. He also was coordinator for FASB's Not-for-Profit Advisory Committee and Private Company Council. Prior to joining FASB, Rick was vice president and controller at a large national museum in New York for seven years and a senior manager with a large international accounting firm where he worked for 14 years and specialized in audits of higher education institutions and other nonprofit organizations.

Rick is a member of the American Institute of CPAs' Not-for-Profit Entities Expert Panel. He is a lecturer at Columbia University School of Professional Studies, New York, New York, in their Nonprofit Management program. He also has been a frequent speaker with National Association of College and University Business Officers, the American Institute of CPAs, and various state CPA societies.

He is a CPA in New York and New Jersey and is a member of the American Institute of CPAs and New York State Society of Certified Public Accountants.

Rick is a graduate of Montclair State University, New Jersey, with a B.S. degree and an M.B.A. degree.

Johnny L. Sanders, PCI-QSA, CISM® CISA®, CompTIA Security+
Senior Managing Consultant, Nashville, TN. jlsanders@bkd.com

Johnny has more than 25 years of information technology (IT) experience. His early experience was acquired during active duty in the U.S. Air Force, where he was a system administrator over multiple platforms as well as an information security officer (ISO).

He focuses on cybersecurity, PCI audits, IT audits, system security, policy, procedure, business continuity and disaster recovery reviews and electronic banking review testing for financial institutions and institutions of higher learning.

Before joining BKD, Johnny was senior engineer for a large IT company that managed a sizable international project for the Department of Defense. In addition to leading network and datacenter administration teams, he was responsible for system audits, security, and network accreditation. He also served as the chief operating officer for a regional broadband development company where he directly managed all installation and IT personnel, as well as overseeing network security and product development. Johnny also taught basic and advanced network design, network security and routing administration for Cisco Networking Academy at Arkansas State University.

He holds Payment Card Industry Qualified Security Assessor (QSA), Certified Information Security Manager ® (CISM®), Certified Information Systems Auditor® (CISA®) and CompTIA Security+ certifications.