

FORVIS

Higher Education Security & GLBA Compliance

December 15, 2022

TO RECEIVE CPE CREDIT

▪ Individuals

- Participate in entire webinar
- Answer polls when they are provided

▪ Groups

- Group leader is the person who registered & logged on to the webinar
- Answer polls when they are provided
- Complete group attendance form
- Group leader sign bottom of form
- Submit group attendance form to cpecompliance@forvis.com within 24 hours of webinar
- If all eligibility requirements are met, each participant will be emailed their CPE certificate within 15 business days of webinar

Meet the Presenters

Johnny Sanders

PCI QSA, CISM, CISA, Security+
Director

FORVIS Cyber

johnny.sanders@forvis.com

The logo for FORVIS, featuring the word "FORVIS" in white, bold, sans-serif capital letters on a red rectangular background.

Dave Smith

Director of IT for Security
University of Mount Union, Ohio
smithdr@mountunion.edu

FORVIS

Agenda

- Higher Education-Specific Breach Data
- Ransomware
- “Why” Do We Have to Be GLBA Compliant?
- Recent Changes in the GLBA
- Cybersecurity Insurance
- Culture of Security – University of Mount Union
- Summary/Questions

Breach Data

Cost of a Data Breach & Learning
from the Pain of Others

FORVIS Cyber

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office

Accessing Breach Data

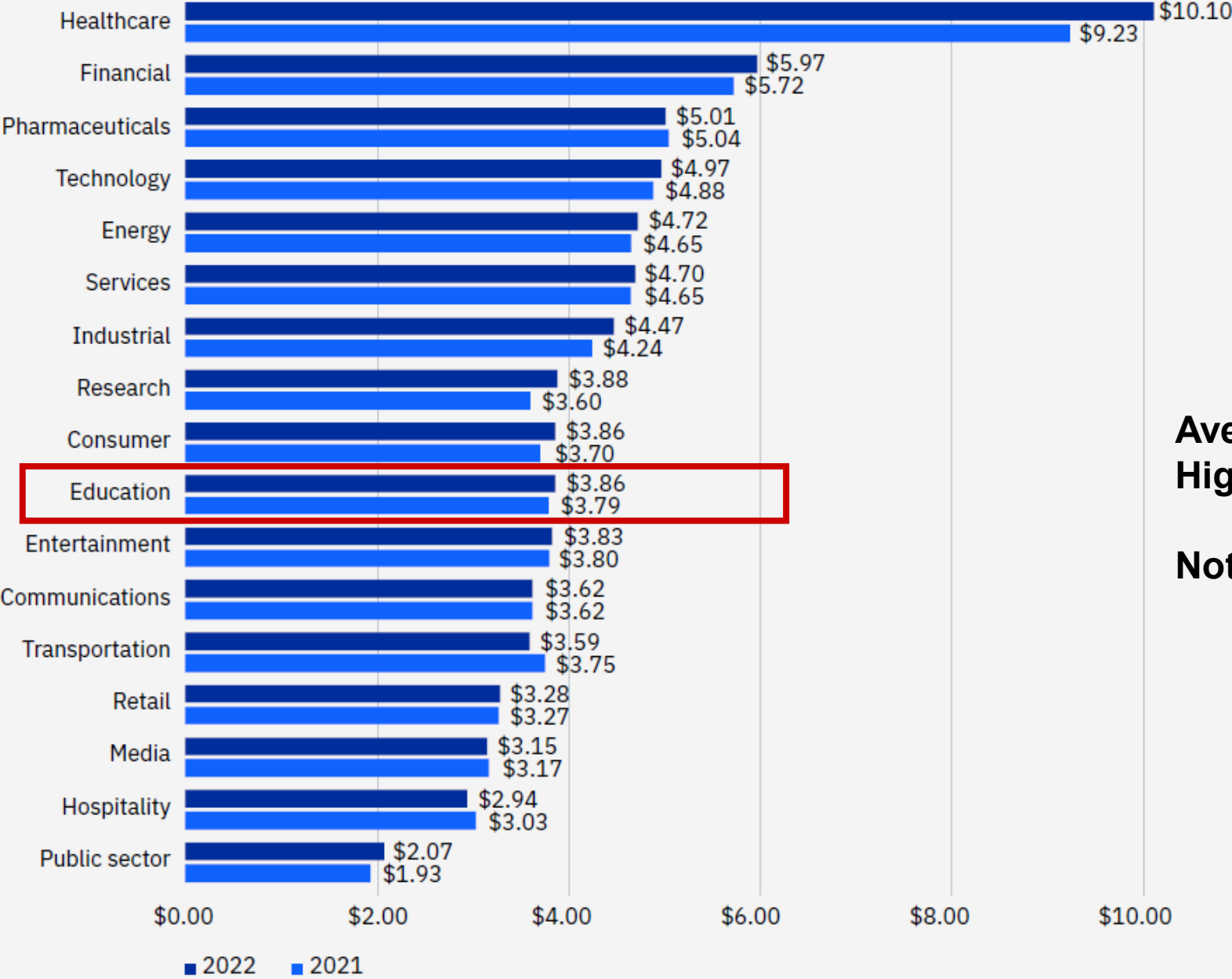
Cost of a Data Breach
Report 2022 **IBM.**



FEDERAL BUREAU of INVESTIGATION
Internet Crime Report
2021

FORVIS Cyber

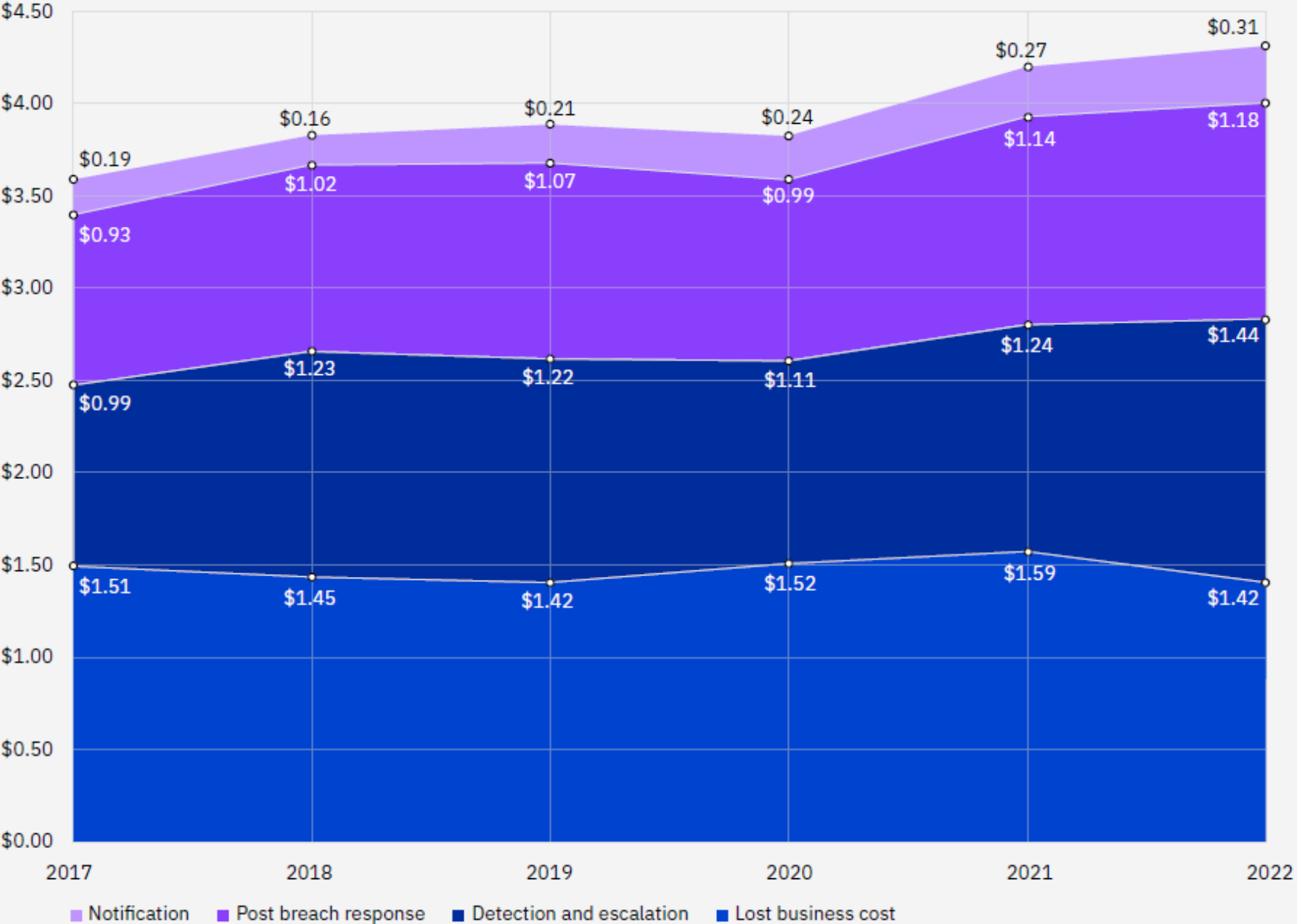
Average cost of a data breach by industry



Average Cost of a Breach in Higher Education in 2021

Note: This is a global average

Average cost of a data breach divided into four segments



- Notification
- Post breach response
- Detection and escalation
- Lost business cost

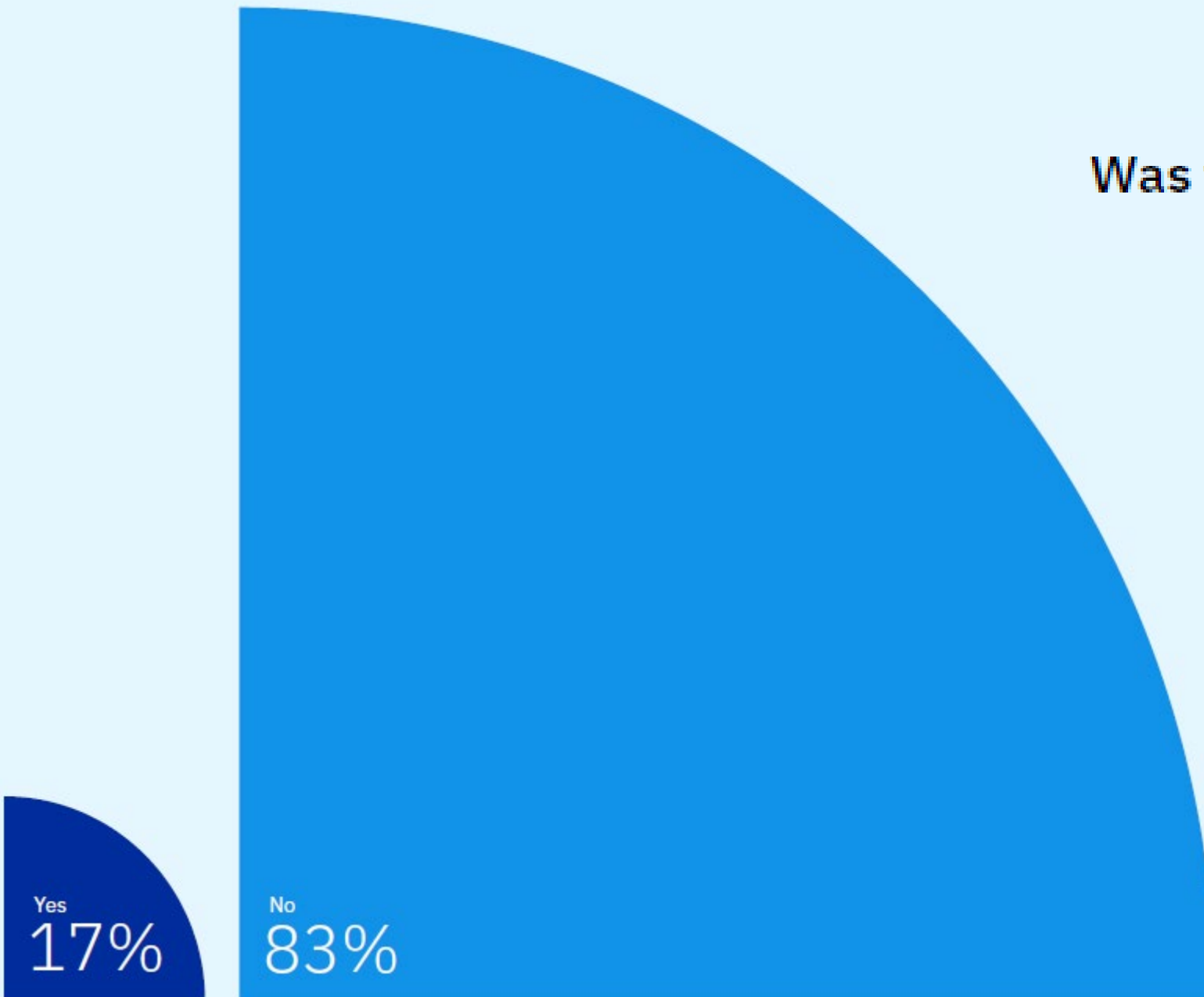
Was this your first data breach?

17% of those in the study said this was their first data breach.

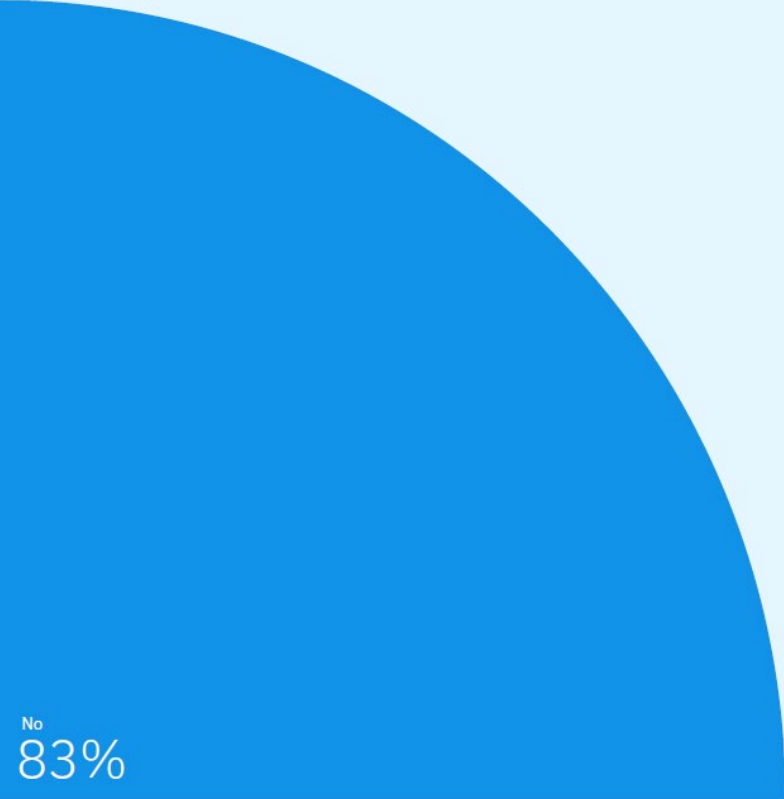
83% said this wasn't their first data breach.

With security teams handling more incidents every year and considering the impact of remote work on security, it's likely the recurrence of breaches is climbing.

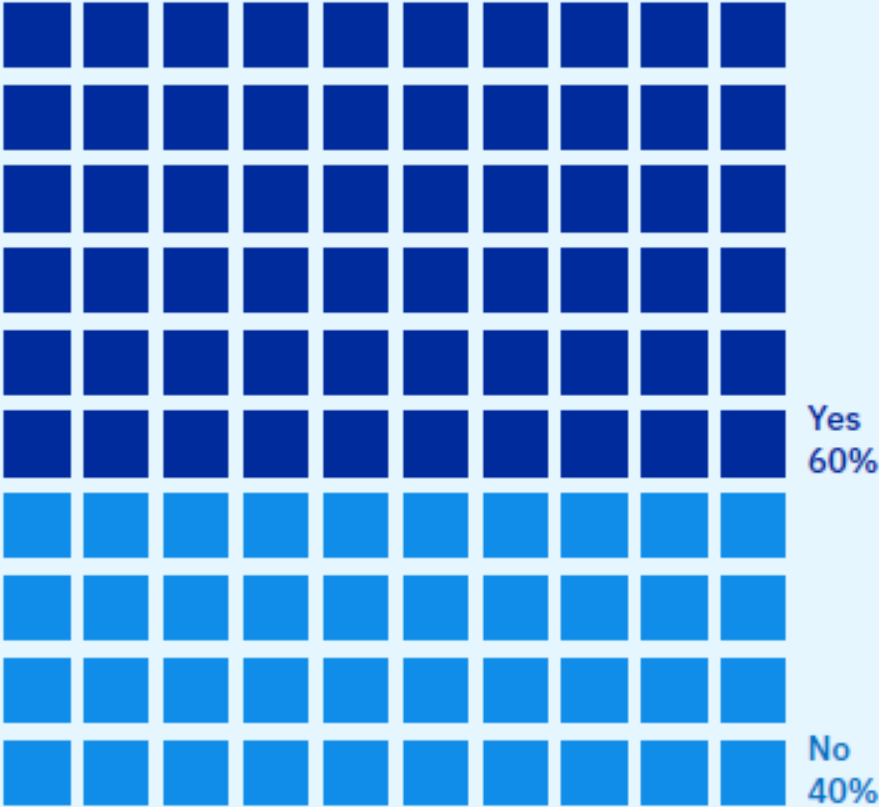
Are you investing in security staff?
Training?



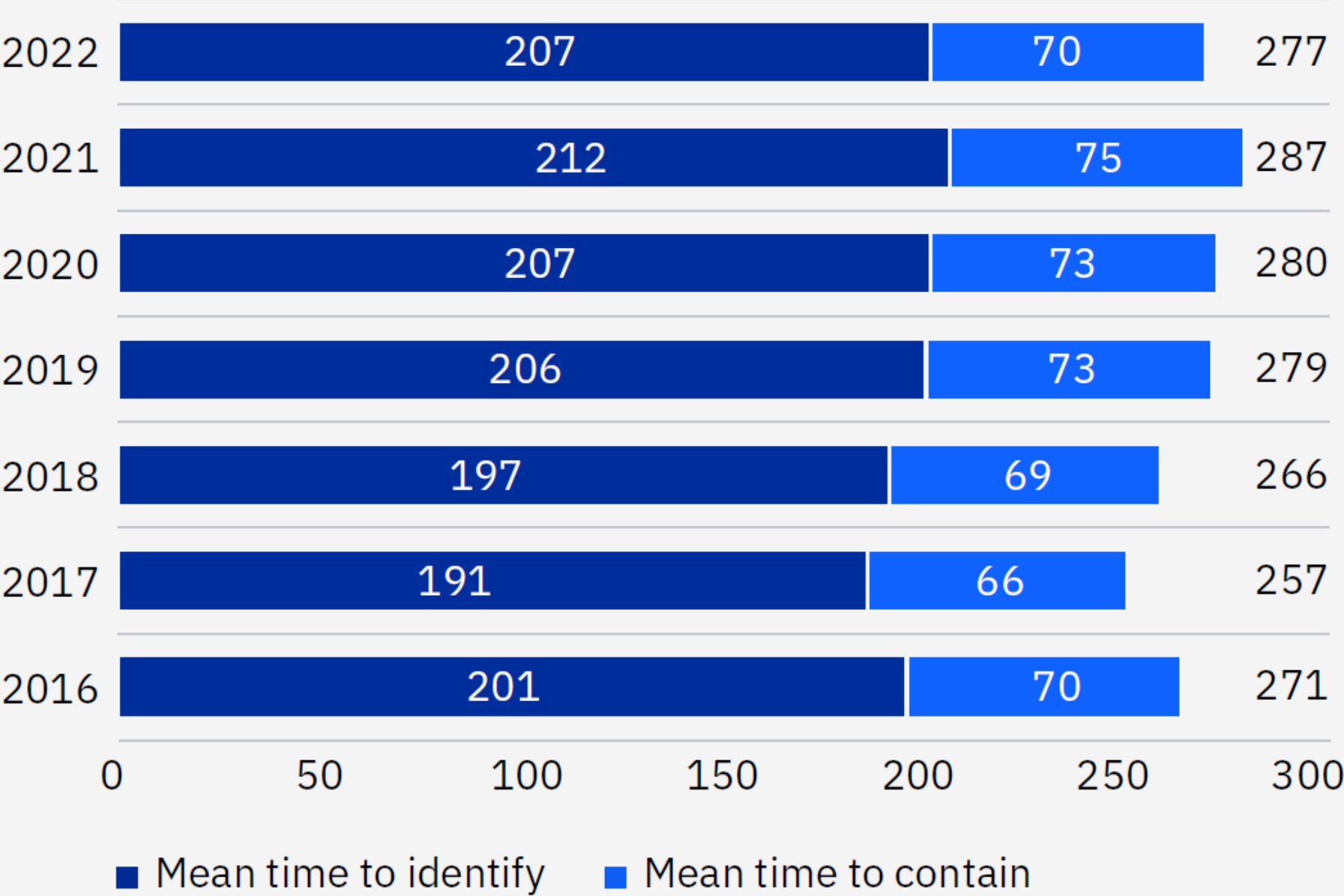
Did the 83% of those previously breached learn a lesson?



The study found that 40% of those previously breached did not invest any additional resources into security practices or services.



Average time to detect a breach?



2022 Cost of a Data Breach Report –
Ponemon Institute, IBM Security

Average cost and frequency of data breaches by initial attack vector



How the method of attack changes the cost of a breach

2022 Cost of a Data Breach Report –
Ponemon Institute, IBM Security

FORVIS Cyber

Calculating the “Longtail” Costs

CYBER

Data breaches in high data protection regulatory environments tended to see costs accrue in later years following the breach.

These include:

Healthcare

Financial

Energy

Pharmaceuticals

Education Industries

In highly regulated industries, **an average of 24% of data breach costs were accrued more than two years after the breach** occurred.

This result compares to an average of 8% of costs accrued more than two years after a breach in low regulatory environments.

These are called the “longtail” costs and they must be considered



FORVIS Cyber

2022 Cost of a Data Breach Report –
Ponemon Institute, IBM Security

Ransomware

Higher Education

FORVIS Cyber

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office

Ransomware

How expensive is it really?

If ransomware were a country ...

107	Honduras	23.83 Bn
108	Zimbabwe	23.15 Bn
109	Iceland	21.63 Bn
110	Trinidad and Tobago	21.39 Bn
111	Afghanistan	20.14 Bn
112	Bosnia and Herzegovina	19.95 Bn
113	Libya	19.21 Bn
114	Yemen	18.84 Bn
115	Laos	18.52 Bn

It would be **#109** on the GDP Rankings by Country (out of 190 listed) – \$22 Billion

#109 Ransomware

FORVIS Cyber

The State of Ransomware in Education 2022

Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries, including 730 respondents from the education sector.

64% of higher education respondents were hit by ransomware in the last year

Data encrypted in the attack



72%
lower education



74%
higher education



65%
global average

Ransomware impacted the ability to operate



94%
lower education



97%
higher education*

*Highest across all sectors

Cyber insurance drives improvement in cyber defenses

	HAVE CHANGED CYBER DEFENSES	HAVE IMPLEMENTED NEW TECHNOLOGIES/ SERVICES	HAVE INCREASED STAFF TRAINING/ EDUCATION ACTIVITIES	HAVE CHANGED PROCESSES/ BEHAVIORS
Lower education	95%	57%	53%	50%
Higher education	96%	68%	48%	49%
Global average	97%	64%	56%	52%

When it comes to increasing **cybersecurity training and education of staff**, **48% of higher education have invested in this area (the lowest across all sectors surveyed)**.

49% in higher education have changed processes/behaviors.

FORVIS Cyber

SOPHOS - The State of Ransomware in Education 2022

Percentage of data restored after paying the ransom



62%
lower education

Education-specific ransomware data



61%
higher education

The amount of data restored after paying the ransom is only 61%



61%
global average

The percentage that got ALL data back after paying the ransom



2%
lower education



2%
higher education

Globally, only 2% of those who pay the ransom get all of their data back



4%
global average

GLBA COMPLIANCE

**“Why do we have to comply with
banking rules?”**



- The GLBA was passed in 1999
- When did the Federal Trade Commission (FTC) first recognize institutions of higher learning as financial institutions & require you to be compliant with the GLBA?



2002

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

May 2003

FORVIS Cyber

Regulatory Requirements

Guidance from the Department of Education & 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**

FORVIS Cyber

Regulatory Requirements

Guidance from the Department of Education & 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.**



FORVIS Cyber

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.”

GLBA Changes

16 CFR Part 314 (up to date as of 6/23/2022)
Standards for Safeguarding Customer
Information

Change: December 9, 2021

Effective date of *new* changes: Dec 9, 2022

FORVIS Cyber

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office

Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC



§ 314.4 Elements.

- (a) **Designate a qualified individual** responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, “Qualified Individual”). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:
 - (1) Retain responsibility for compliance with this part;
 - (2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and
 - (3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (b) **Base your information security program on a risk assessment** that identifies reasonably foreseeable internal and external risks to the security
 - (1) The risk assessment shall be written and shall include:
 - (i) **Criteria for the evaluation and categorization** of identified security risks or threats you face;
 - (ii) **Criteria for the assessment of the confidentiality, integrity,** and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and



Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (b) Base your information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security
 - (1) The risk assessment shall be written and shall include:
 - (iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.



Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (b) *continued* Base your information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security
 - (2) You shall periodically perform additional risk assessments that reexamine the 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 reassess the sufficiency of any safeguards in place to control these risks.



Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (c) Design and implement safeguards to control the risks you identify through risk assessment
 - (1) Implementing and **periodically reviewing access controls**, including technical and, as appropriate, physical controls to:
 - (i) Authenticate and permit access **only to authorized users**; and
 - (ii) Limit authorized users' access only to customer information that they **need to perform their duties** and functions
 - (2) **Identify and manage** the data, personnel, devices, systems, and facilities **that enable you to achieve business purposes** in accordance with their relative importance to business objectives and your risk strategy;



Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (c) *continued* Design and implement safeguards to control the risks you identify through risk assessment
 - (3) **Protect by encryption** all customer information held or transmitted by you both in **transit over external networks and at rest**
 - (4) **Adopt secure development practices for in-house developed applications** utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;
 - (5) **Implement multi-factor authentication for any individual accessing any information system**



Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (c) *continued* Design and implement safeguards to control the risks you identity through risk assessment
 - 6 (i) Develop, implement, and maintain procedures for the secure disposal of customer information in any format **no later than two years after the last date the information is used in connection with the provision of a product or service** to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and
 - (ii) **Periodically review your data retention policy to minimize the unnecessary retention of data;**



Reference: PART 314 - STANDARDS FOR SAFEGUARDING
CUSTOMER INFORMATION

FORVIS Cyber

Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (c) *continued* Design and implement safeguards to control the risks you identify through risk assessment
 - (7) **Adopt procedures for change management;** and
 - (8) **Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.**



Reference: PART 314 - STANDARDS FOR SAFEGUARDING
CUSTOMER INFORMATION

FORVIS Cyber

Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (d)
 - (1) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.
 - (2) For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:



Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (d.2) Absent effective continuous monitoring ... you shall conduct:
 - (i) Annual penetration testing (internal and external) of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and
 - (ii) Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least **every six months**; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program



Reference: PART 314 - STANDARDS FOR
SAFEGUARDING CUSTOMER INFORMATION

FORVIS Cyber

Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (e) Implement policies and procedures to ensure that personnel are able to enact your information security program by:
 - (1) Providing your personnel with **security awareness training that is updated as necessary** to reflect risks identified by the risk assessment;
 - (2) **Utilizing qualified information security personnel** employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;
 - (3) **Providing information security personnel with security updates and training sufficient to address relevant security risks;** and
 - (4) **Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.**



Reference: PART 314 - STANDARDS FOR
SAFEGUARDING CUSTOMER INFORMATION

FORVIS Cyber

Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (f) 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;
 - (2) Requiring your service providers by contract to implement and maintain such safeguards; and
 - (3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.



Reference: PART 314 - STANDARDS FOR
SAFEGUARDING CUSTOMER INFORMATION

FORVIS Cyber

Recent Changes in GLBA Compliance

CYBER

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (g) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.



Reference: PART 314 - STANDARDS FOR
SAFEGUARDING CUSTOMER INFORMATION

FORVIS Cyber

Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC



Reference: PART 314 - STANDARDS FOR
SAFEGUARDING CUSTOMER INFORMATION

§ 314.4 Elements.

- (h) Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address the following areas:
 - (1) The goals of the incident response plan;
 - (2) The internal processes for responding to a security event;
 - (3) The definition of clear roles, responsibilities, and levels of decision-making authority;
 - (4) External and internal communications and information sharing;
 - (5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
 - (6) Documentation and reporting regarding security events and related incident response activities; and
 - (7) The evaluation and revision as necessary of the incident response plan following a security event.

FORVIS Cyber

Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC



Reference: PART 314 - STANDARDS FOR
SAFEGUARDING CUSTOMER INFORMATION

§ 314.4 Elements.

- (i) Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:
 - (1) The overall status of the information security program and your compliance with this part; and
 - (2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

FORVIS Cyber

BREAKING NEWS

Update!

As of Tuesday, November 15th, a 6-month extension was granted to the new parts of the Safeguard Rule. New due date: June 9, 2023

PLEASE NOTE:

- We urge you NOT to wait on implementing security requirements
- Government regulations are generally several years behind
- While compliance with the Safeguard Rule has been extended, hackers remain active. Strive to comply with these new rules immediately

The background features a person's hands typing on a laptop. A large, glowing blue circular overlay with the text 'CYBER SECURITY' is centered over the laptop. The laptop screen displays various data visualization icons, including bar charts, pie charts, and a 'Quality Control' section. There are also several circular icons floating around the laptop, such as a cloud with an upward arrow, a group of people, and a circular flow diagram. An orange horizontal bar is located at the top left of the image.

We Have
Cybersecurity
Insurance!

But will it pay?

Cybersecurity Insurance



- 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**

Cybersecurity Insurance

Top Five Reasons for Claim Denials



- Inability to Demonstrate Proper Security Measures Are in Place
- Lack of Preventive Security Measures
- Inadequate Endpoint Security
- Weak Security Measures Within the Supply Chain
- Poor Internal Cybersecurity Training & Awareness
- **NOTE: Insurance companies can be great resources of information & help!**

Dave Smith

Director of IT for Security
University of Mount Union

Culture of Security

FORVIS Cyber

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office

University of Mount Union

About Mount Union



- Founded in 1846
- Located in Alliance, Ohio
 - 20 minutes east of Canton (HOF Village)
 - Between Cleveland and Pittsburgh
- Private Institution
- 2200 FTE students
 - Undergrad and Graduate programs
- 500 employees

FORV/S

University of Mount Union

About IT @ UMU



- 15 FT Staff
- 12 Helpdesk Student Workers
- Areas include:
 - Technical/Network Services
 - Security
 - Helpdesk/User Support
 - Administrative Systems
 - Classroom Technology
 - Technology Procurement

FORV/S

University of Mount Union

GLBA Compliancy Efforts



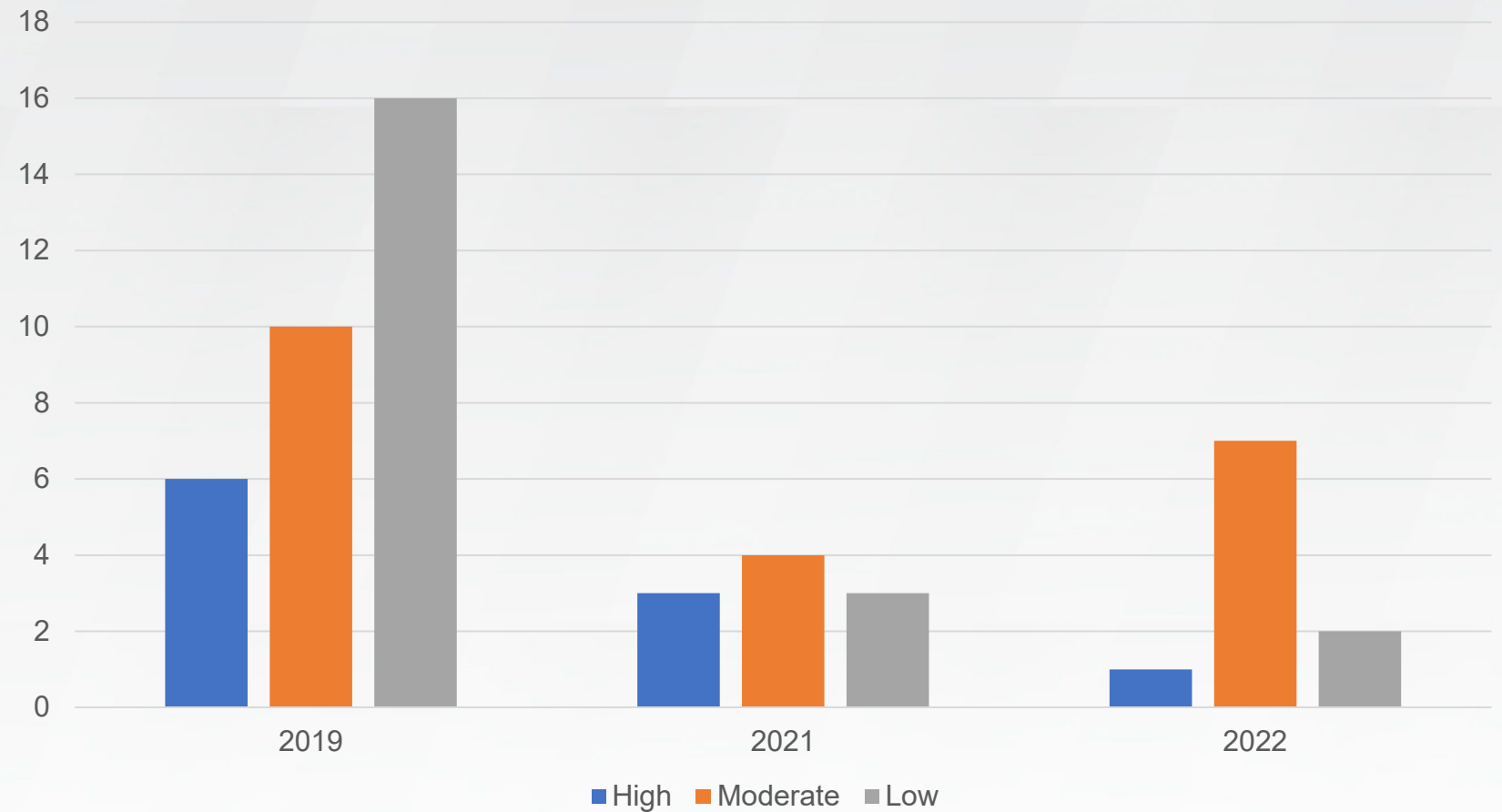
- 1st Assessment April 2019
 - 32 Findings (6 high, 10 moderate, 16 low)
- 2nd Assessment March 2021
 - 10 Findings (3 high, 4 moderate, 3 low)
- 3rd Assessment April 2022
 - 10 Findings (1 high, 7 moderate, 2 low)
- Next Assessment planned for April 2023

University of Mount Union

GLBA Compliancy Efforts



GLBA Assessment History



FORVIS

University of Mount Union

Culture of Security



■ Board of Trustees

- Annual Training (In Person)
- Regular Reporting through Audit Committee
- Established a Cyber Security Committee

■ President Council

- Annual Training (In Person or Virtually)
- Regular reporting (2-4 times a year)
- Supported establishment of Incident Response Team
- Supported removal of public directory
- Supported removal of access for those who are noncompliant

University of Mount Union

Culture of Security



- **Compliance Oversight Committee**
 - Annual Training (In Person or Virtually)
 - Regular Reporting on Cybersecurity Efforts
 - Compliancy Day Training
 - Policy Review Council
 - * Review and support of new policies
- **Safety and Risk Committee**
 - Annual Training (In Person or Virtually)
 - Regular Reporting on Cybersecurity Efforts
- **Incident Response Team**
 - Annual Desk Top Exercise
 - Special Training
 - Annual Cyber Security Training

FORV/S

University of Mount Union

Culture of Security



- IT Security Team (CIO, CISO, Tech Mgr)
 - Specialized Training, Conferences
 - Annual Tabletop Exercise
 - Assessment Results Next Steps
 - Partnership with Bytlift
 - Reporting, Communication, Policy, etc.
- Employees
 - Annual Cyber Security Training Required (In Person or Virtually)
 - Regular Reporting on Cybersecurity Efforts
 - Policy Review Council
 - Review and support of new policies
 - Phishing Exercises

FORV/S

University of Mount Union

Culture of Security



Phishing Test Results



FORV/S

University of Mount Union

Culture of Security

■ Close with some Comments

- Change isn't easy
- Many of the changes are unpopular
- We are in this together (The Entire University)
- Keep striving for the light...Know you will never reach it...It gets Brighter!
- Build good Partnerships
- Get the support of Administration and BOT
- Keep educating (the university and IT security)



FORV/S

QUESTIONS

FORV/S

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office

CONTINUING PROFESSIONAL EDUCATION (CPE) CREDIT



FORVIS, LLP is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

FORV/S

CPE CREDIT

- CPE credit may be awarded upon verification of participant attendance
- For questions, concerns, or comments regarding CPE credit, please email FORVIS at cpecompliance@forvis.com

Thank you!

Johnny Sanders
johnny.sanders@forvis.com

Dave Smith
smithdr@mountunion.edu

forvis.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by FORVIS or the author(s) as to any individual situation as situations are fact specific. The reader should perform its own analysis and form its own conclusions regarding any specific situation. Further, the author(s) conclusions may be revised without notice with or without changes in industry information and legal authorities. FORVIS has been registered in the U.S. Patent and Trademark Office, which registration is pending.

FORVIS

Assurance / Tax / Advisory