FORVIS

GLBA and Ransomware

Important Compliance and Technical Risks ED Has to Address

Johnny Sanders

Meet the Presenter

Johnny Sanders
PCI QSA, CISM, CISA, Security+
Director
FORVIS Cyber
Johnny.sanders@forvis.com

FORVIS

Breach Data

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

FORVIS Cyber

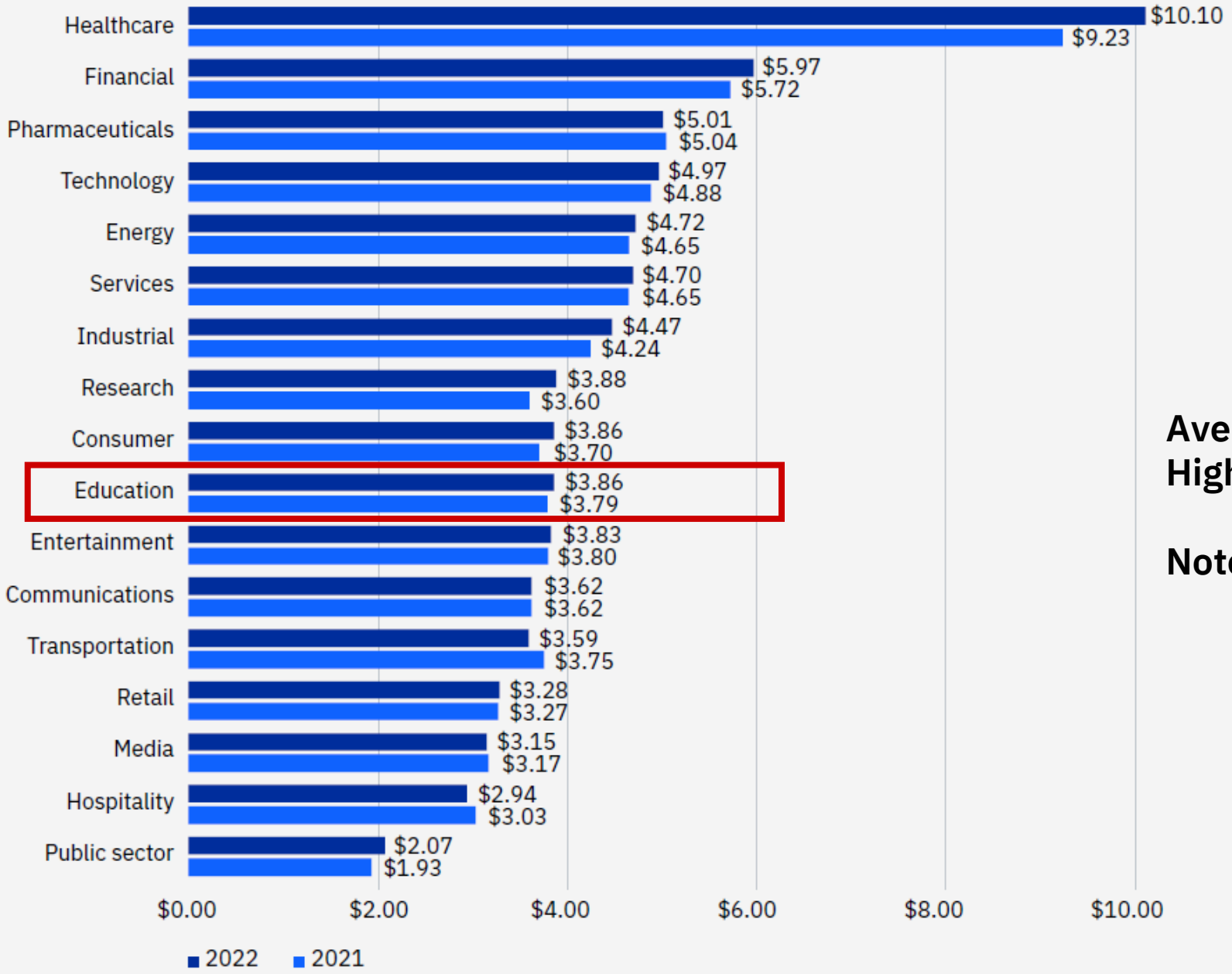
Accessing Breach Data

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

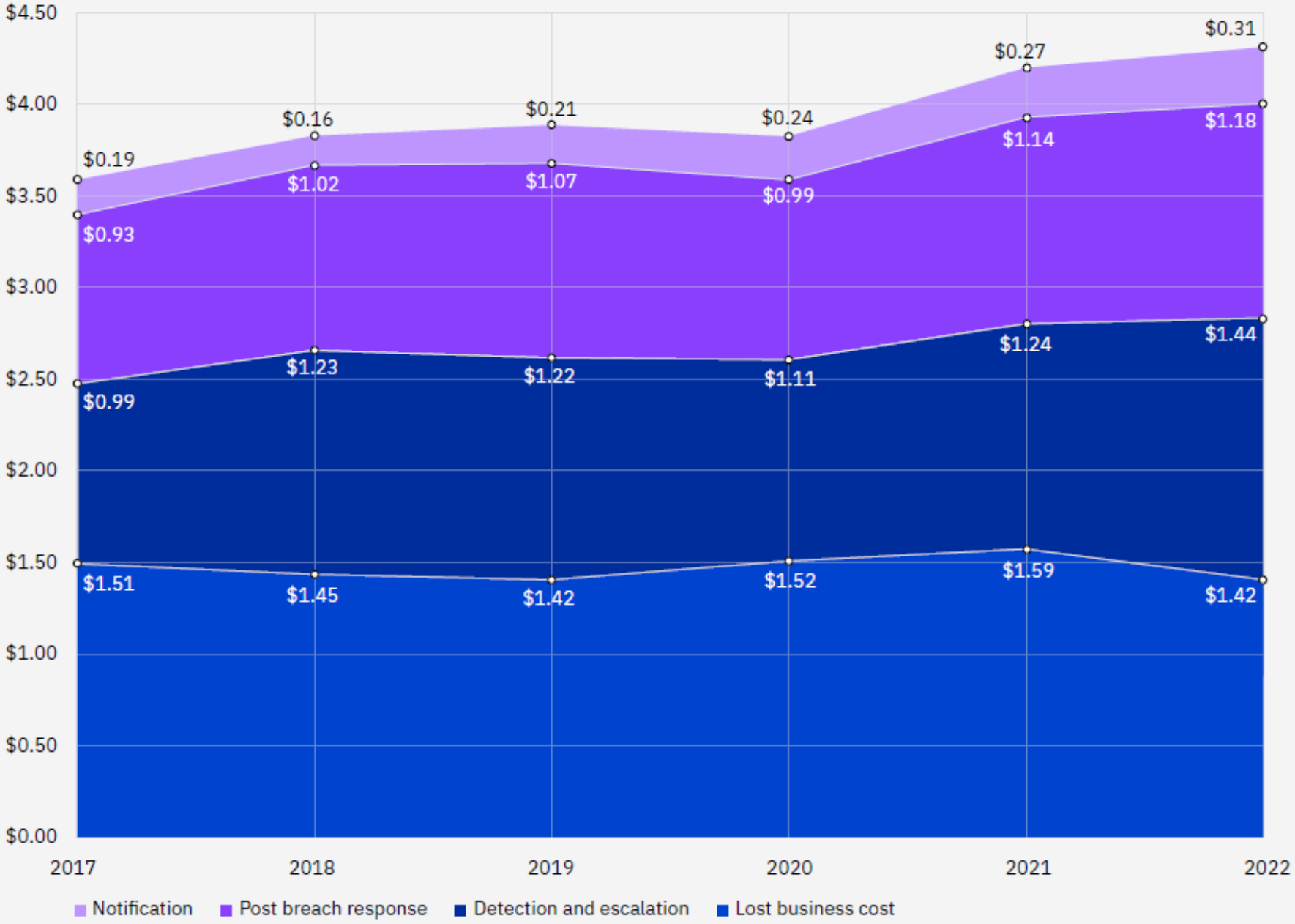


Average Cost of a Breach in Higher Education in 2021

Note: This is a global average.

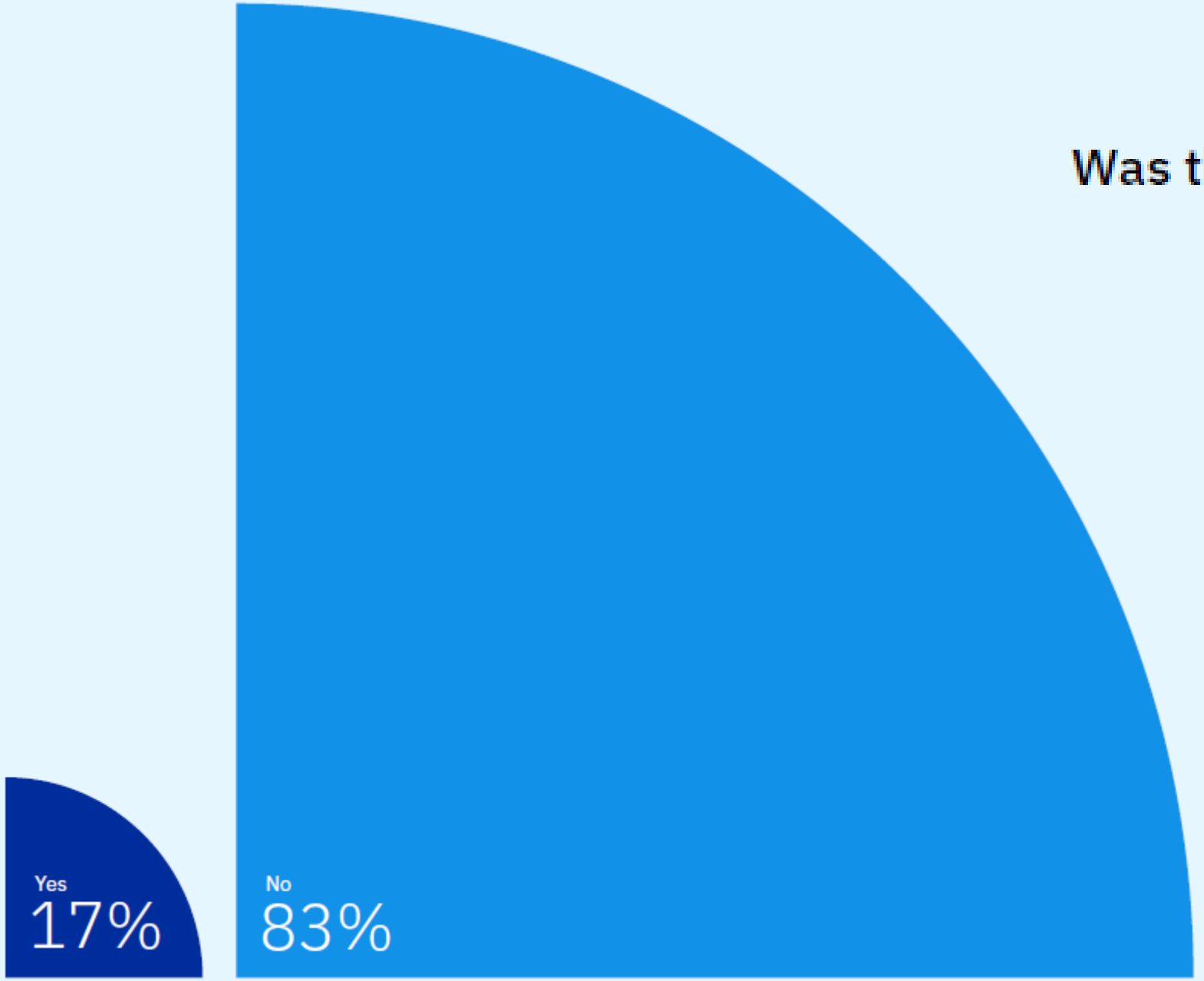
2022 Cost of a Data Breach Report – Ponemon Institute, IBM Security

Average cost of a data breach divided into four segments



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

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



Was this your first data breach?

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

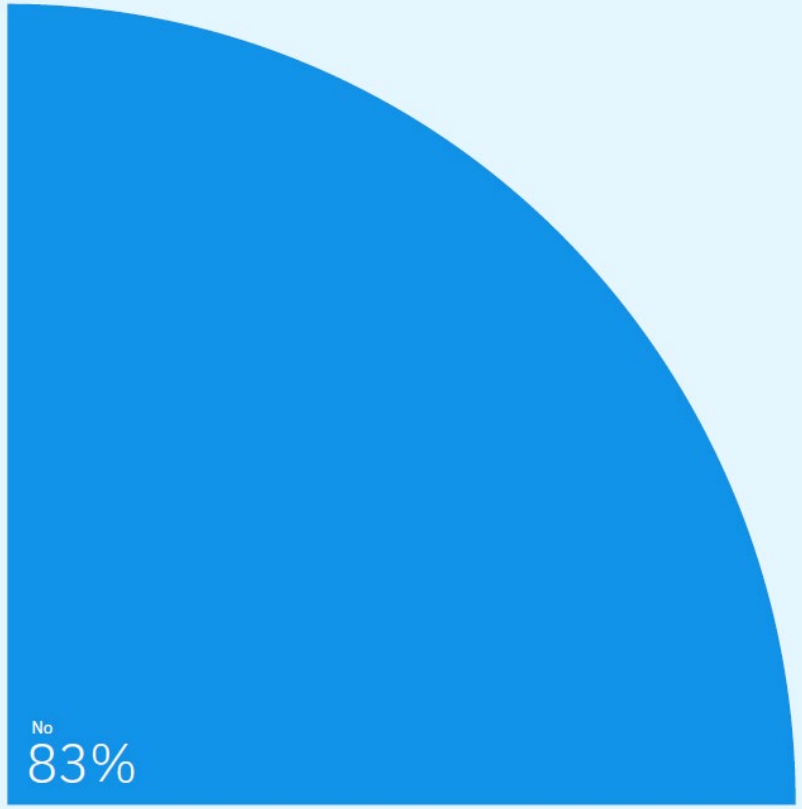
83% said this wasn't their first data breach.

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.

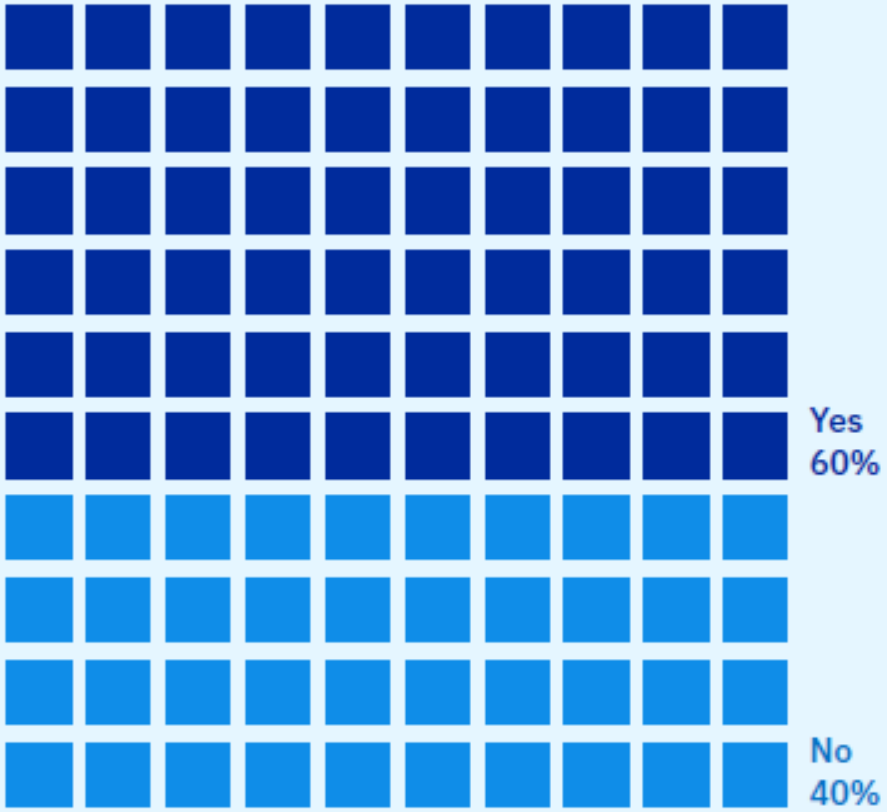
Are you investing in security staff? Training?

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

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

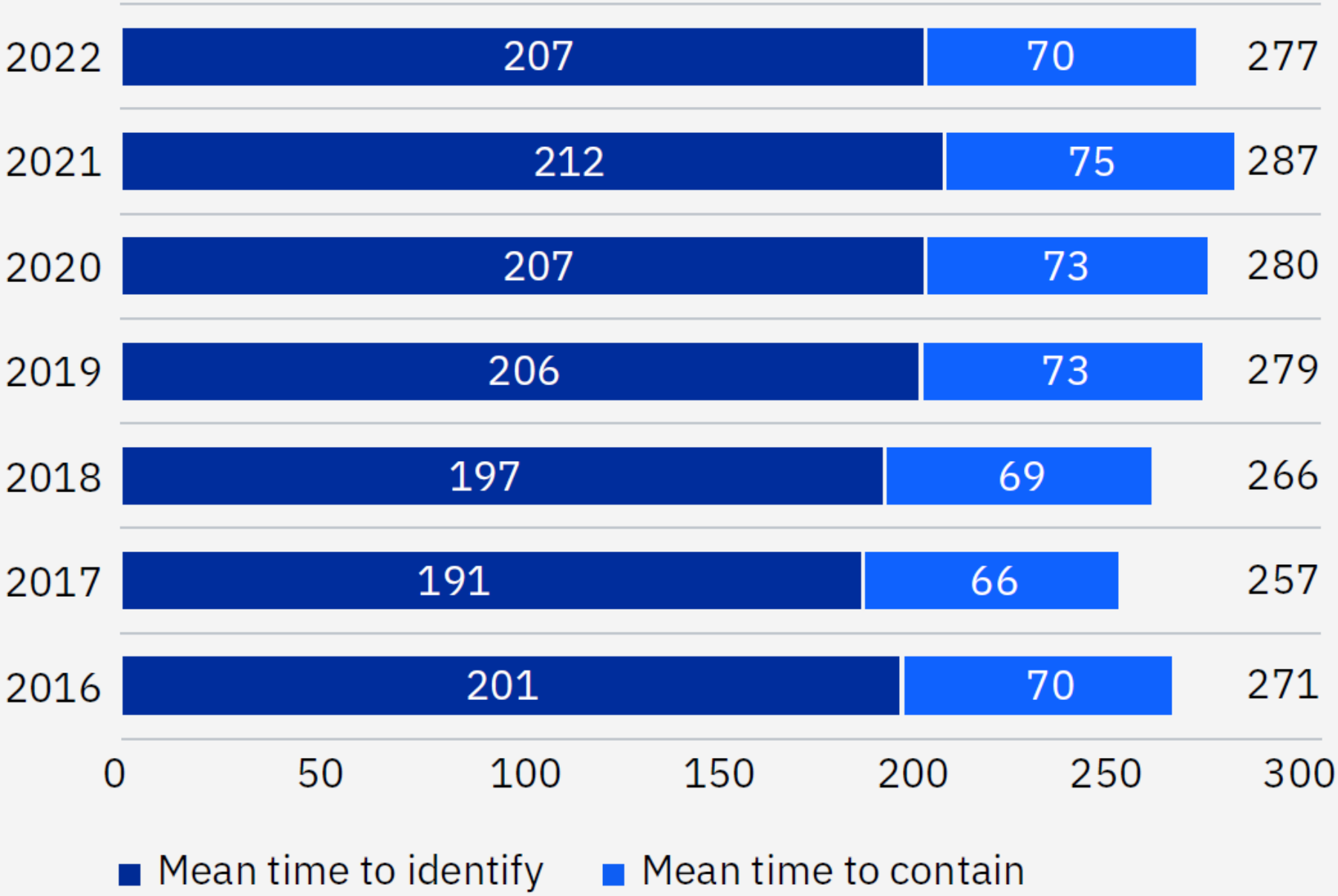


The study found that 40% of those previously breached did not invest any additional resources into security practices or services.

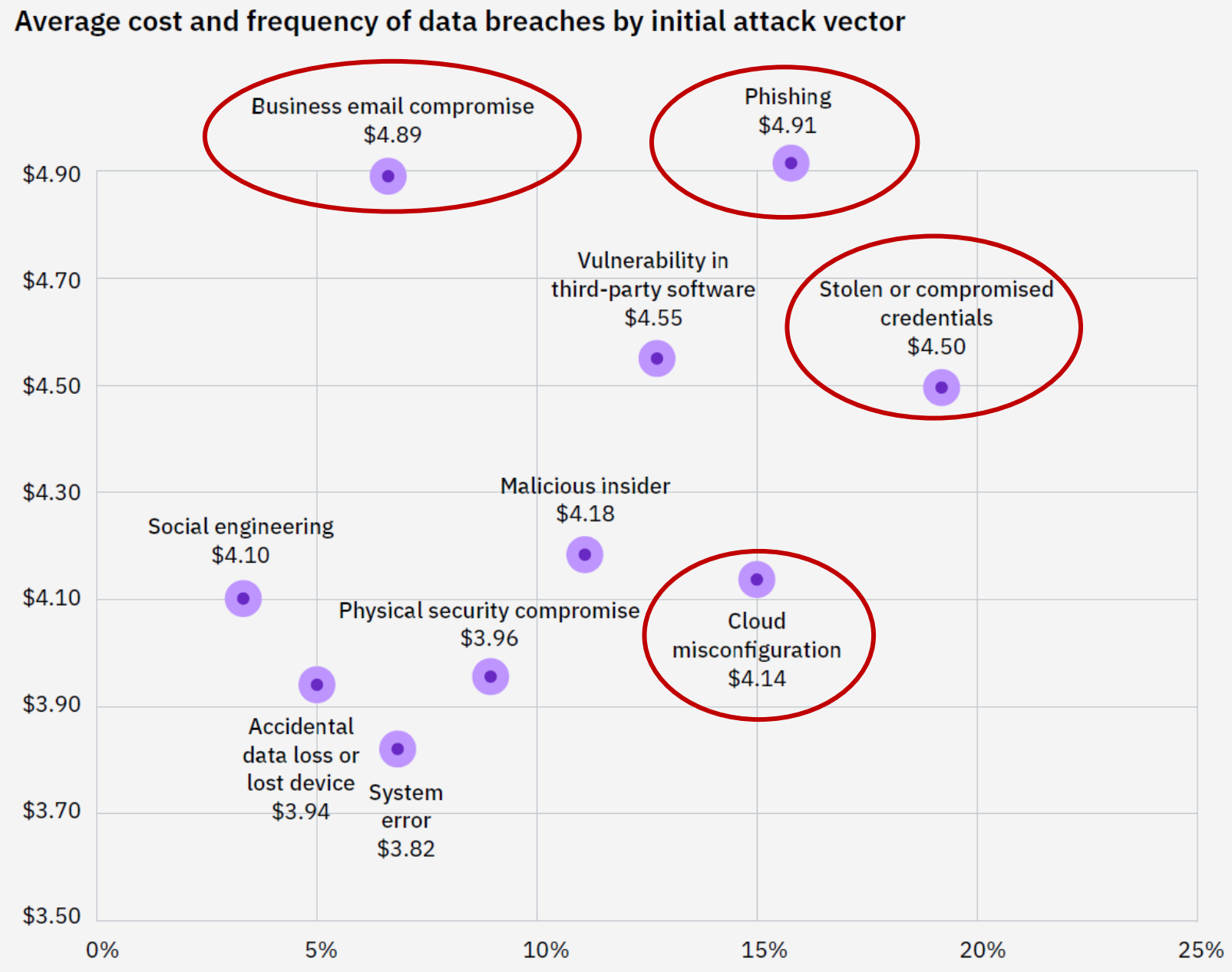


2022 Cost of a Data Breach Report –
Ponemon Institute, IBM Security

Average time to detect a breach?



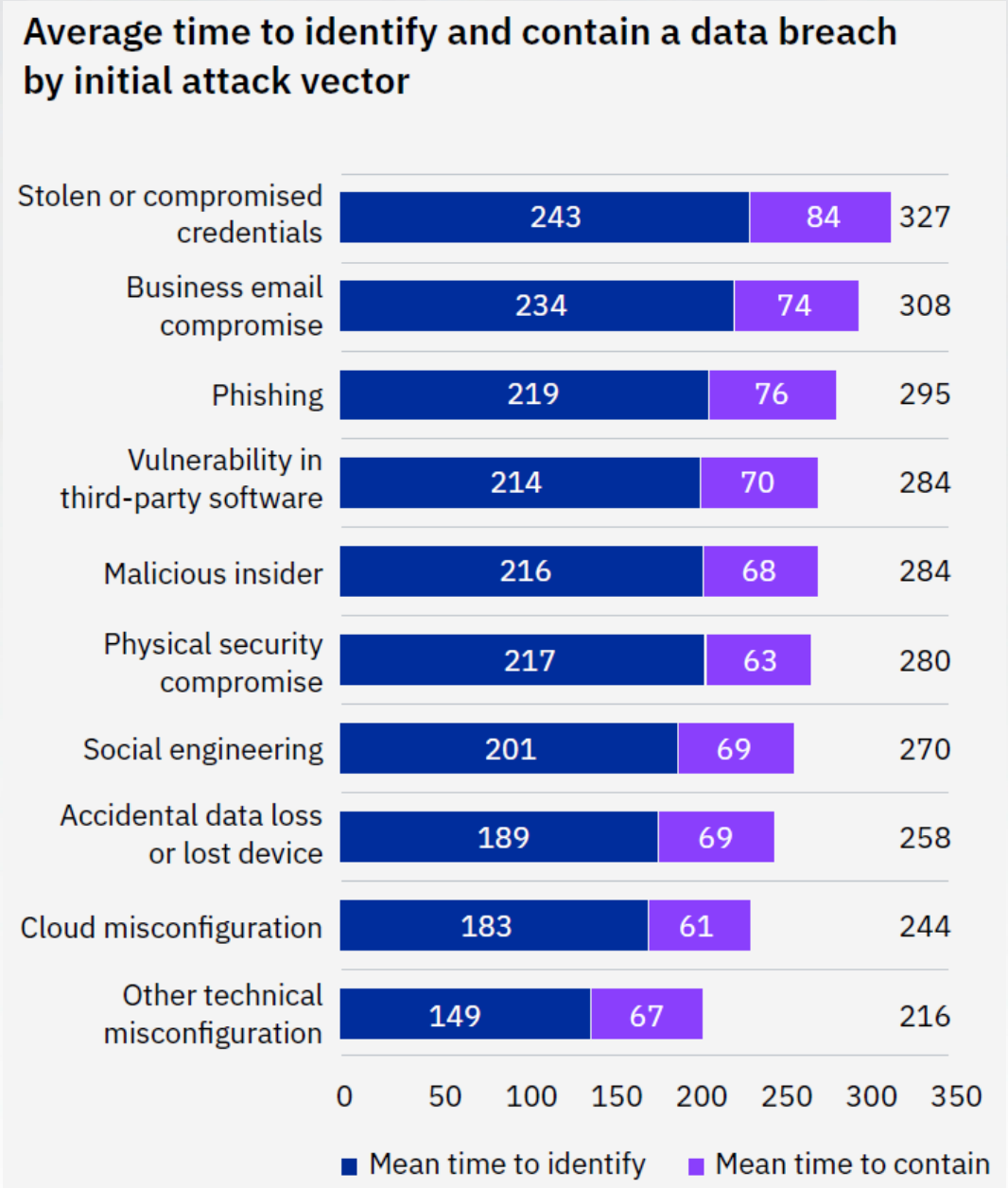
2022 Cost of a Data Breach Report – Ponemon Institute, IBM Security



How the method of attack changes the cost of a breach

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

FORVIS Cyber



How the method of attack changes the cost of a breach

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

Calculating the “Longtail” Cost

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.

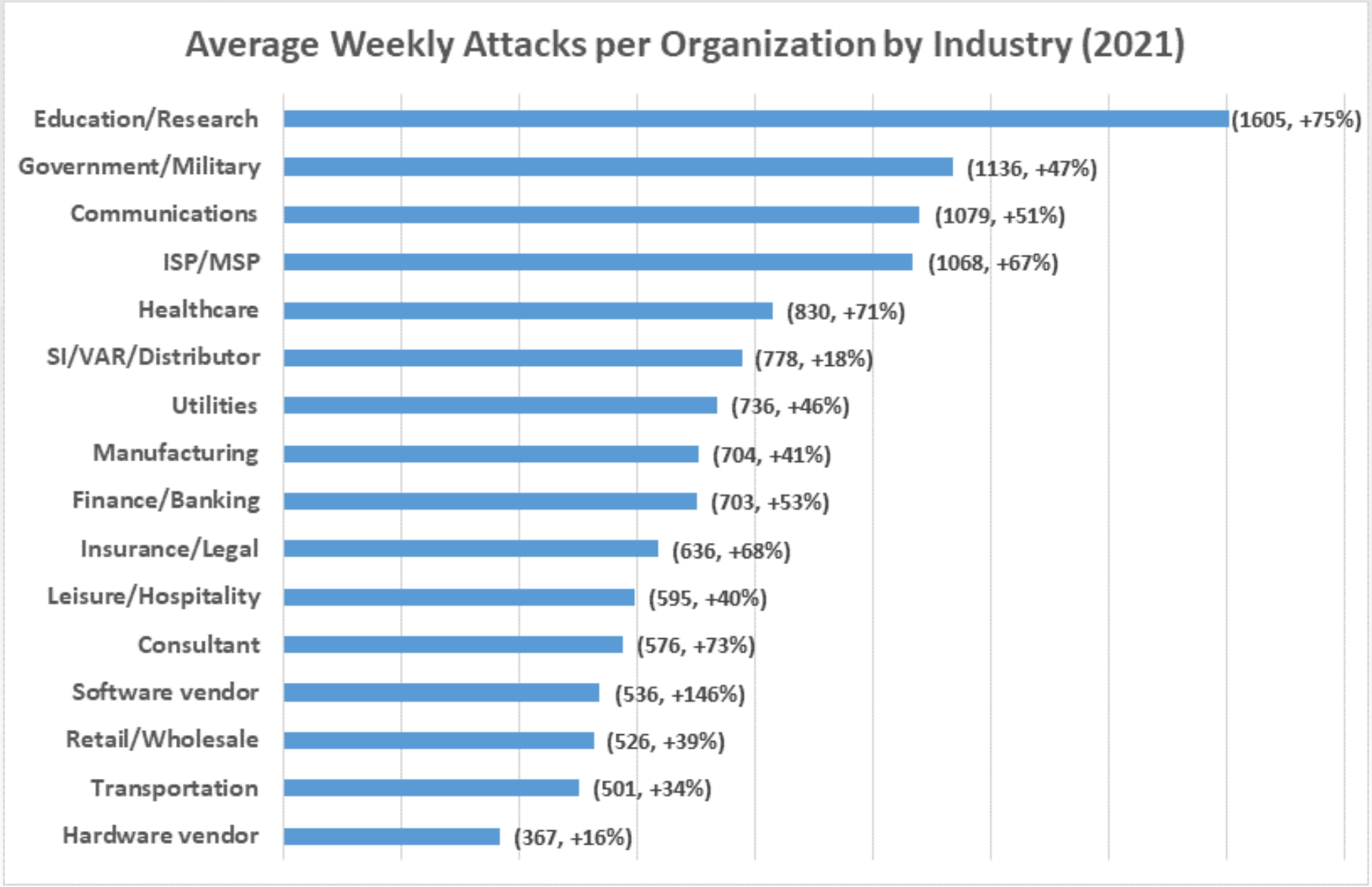
This result compares to an average of 8% of costs accrued more than two years after a breach in low regulatory environments.

This is called the “longtail” costs and they must be considered

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

Higher Education

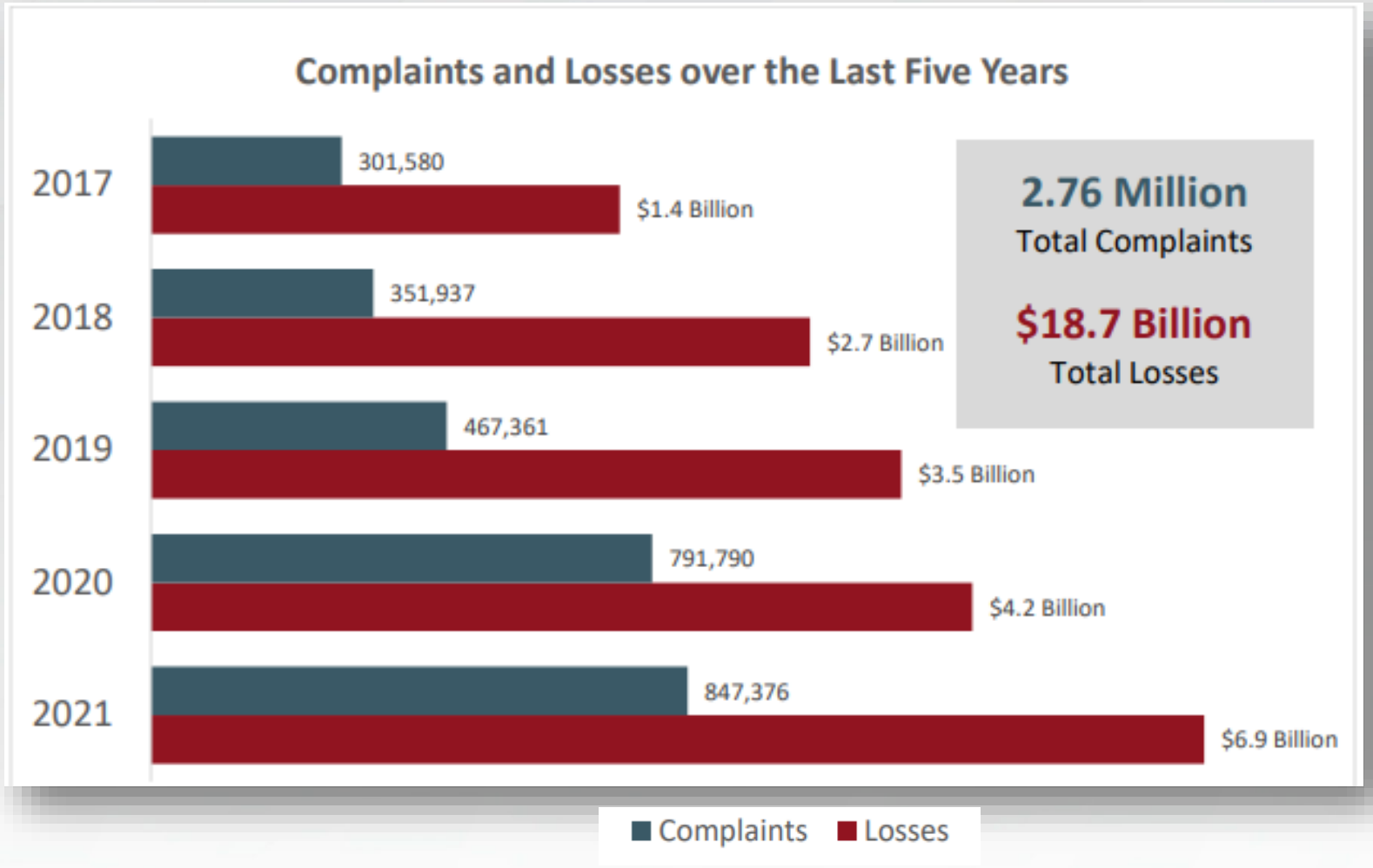
- The Most Attacked “industry” in 2021

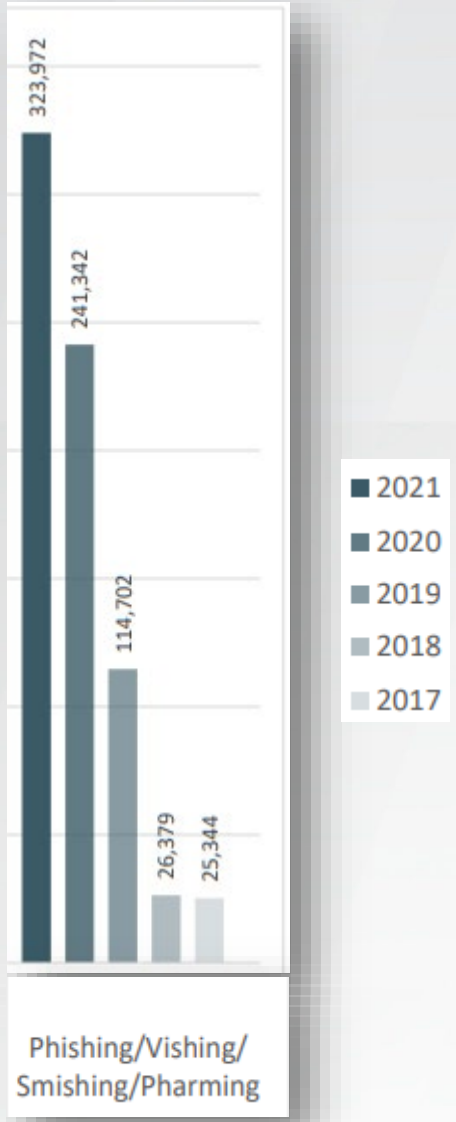


Check Point Software Technologies Ltd.

FORVIS *Cyber*

FBI's IC3 5 Year Statistics





2021 FBI IC3 Report

BUSINESS EMAIL COMPROMISE (BEC)

The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds or other malicious activities

Complaints:	Losses:
19,954 - *Reported*	Exceeding $2.4 billion

Trending Issues

Focusing on Trends to Assess Risk

FORVIS Cyber


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

Ransomware

How expensive is it really?

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

If ransomware were a country…..

It would be #109 on the GDP Rankings by Country (out of 190 listed)

#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

SOPHOS - The State of Ransomware in Education 2022

Data encrypted in the attack

72%
lower education

74%
higher educatio

65%
global average

Ransomware impacted the ability to operate

94%
lower education

97%
higher education*

* Highest across all sectors

FORVIS

SOPHOS - The State of Ransomware in Education 2022

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% in 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

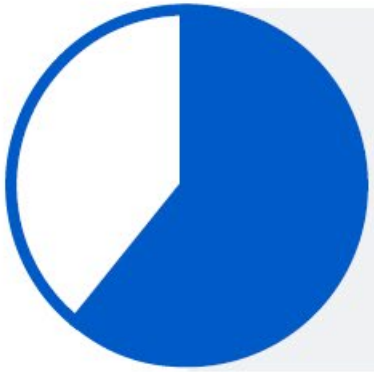
Percentage of data restored after paying the ransom

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

SOPHOS - The State of Ransomware in Education 2022

The percentage that got ALL data back after paying the ransom

2%
lower education

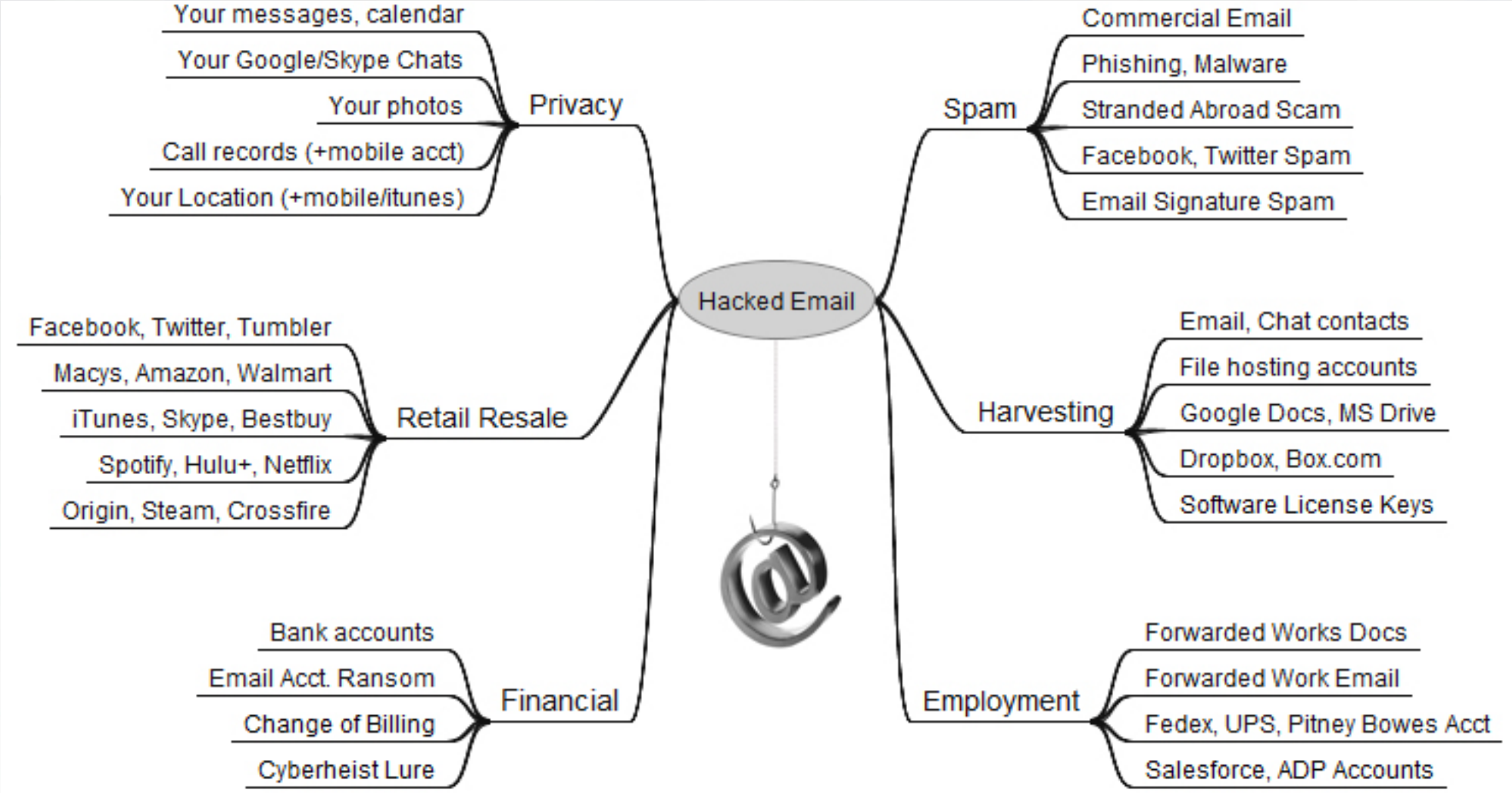
2%
higher education

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

4%
global average

SOPHOS - The State of Ransomware in Education 2022

The Ultimate Gateway – Email



FORVIS *Cyber*

“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 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

FORVIS Cyber

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

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.**

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*

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.

FORVIS Cyber

Reference: PART 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

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

FORVIS Cyber

Reference: PART 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

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.

FORVIS Cyber

Reference: PART 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

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
  - (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.

FORVIS Cyber

Reference: PART 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

§ 314.4 Elements.

- (c) Design and implement safeguards to control the risks you identity 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;

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 identity 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**

FORVIS

Reference: PART 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

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 identity 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:

FORVIS Cyber

Reference: PART 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

Reference: PART 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

§ 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

FORVIS Cyber

Recent Changes in GLBA Compliance

Updated Security Requirements from the FTC

Reference: PART 314 - STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

§ 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.

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

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

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 regulation 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.

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

FORVIS

Cybersecurity Insurance

Top 5 Reasons for Claim Denials

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

FORVIS

Questions?

Johnny Sanders
Johnny.sanders@forvis.com

forvis.com

FORVIS

Assurance / Tax / Advisory