Vendor Security Framework and Contract Considerations

Item 6 – Group Insurance Board

Steve Hurley, Director, Office of Policy, Privacy and Compliance

David Maradiaga, Chief Information Security Officer, Bureau of Information Security Management

Renee Walk, Director, Office of Strategic Health Policy

Informational Item Only

- No Board action is required.

Background

- Requirement for SOC-2, Type II issued by Board in November 2023.
- Further review of Board contracts and other ETF programs raised questions and additional considerations.
- November motion suspended in May 2024, pending alternatives.

Privacy and Information Protection

State Level Requirements

- Wis. Stat. § 40.07: Individual Personal Information (IPI / PII), and Medical Record information
- Wis. Stat. § 134.98: Notice of Unauthorized Acquisition of Personal Information (Non-HIPAA breaches)

Federal Level

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: Protected Health Information

(Ref. GIB | 08.14.24 | 6, page 2-3)

HIPAA-Covered Board Programs

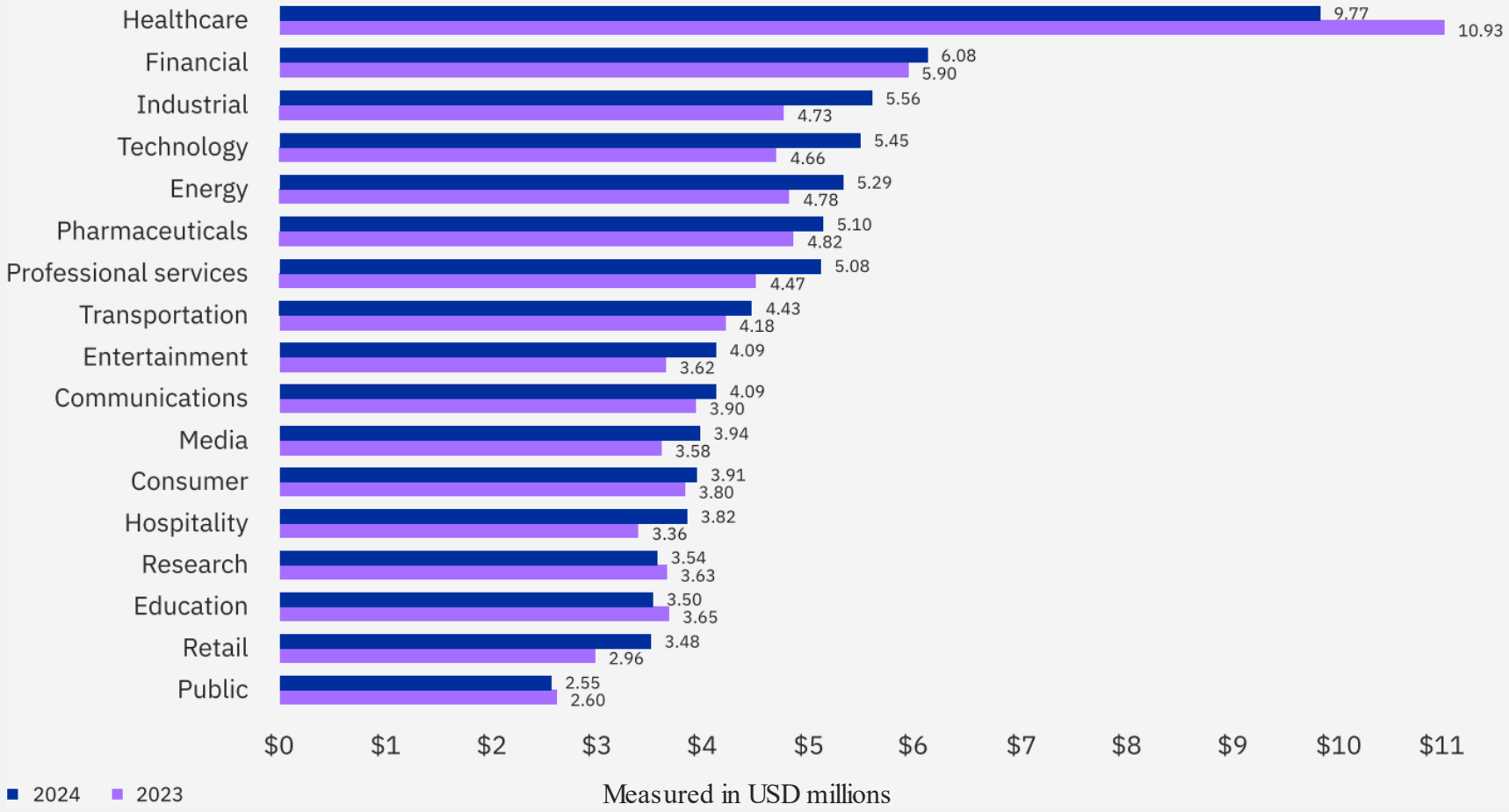
GIB Benefit Program/Area	HIPAA-Covered
State/Local Group Health Insurance Plan	Yes
Pharmacy Benefits	Yes
Wellness Program	Yes
Dental Insurance (Self-Insured)	Yes
Health Savings Accounts	Yes
Health Reimbursement Accounts/FSA	Yes
DAISI Data Warehouse	Yes
Long Term Care Insurance (Employee Pay-All)	Yes*

GIB Benefit Program/Area	HIPAA-Covered
Vision Insurance (Employee Pay-All)	Yes*
Dental (Employee Pay-All)	Yes*
Board Actuaries	Yes
Accident Insurance (Employee Pay-All)	No
Long Term Disability Insurance	No
Income Continuation Insurance	No
Group Life Insurance	No

* ETF provides no PHI, but administrator itself is regulated by HIPAA

(Ref. GIB | 08.14.24 | 6, page 3-4)

Cost of Breaches by Industry



"Healthcare topped industry costs, again. The average breach cost for healthcare fell 10.6%, to USD 9.77 million. But that factor wasn't enough to remove it from the top costliest industry for breaches—a spot it's held since 2011. Healthcare remains a target for attackers since the industry often suffers from existing technologies and is highly vulnerable to disruption, which can put patient safety at stake."

Source: *IBM Cost of Data Breach Annual Report.* (July 2024).

Vendor Risk Management Framework

ETF assessment built on National Institute of Standards and Technology (NIST) standards.

Framework assesses risk profile of a vendor across cyber security functions.

Vendors will provide a report to demonstrate control effectiveness.

In some cases, SOC-2, Type II may meet the highest level of control reporting.

Other reports approved on a case-by-case basis.

(Ref. GIB | 08.14.24 | 6, page 4)

Post-Framework Risk Scoring

ETF will provide a risk-based score based on the provided report.

Three risk levels: low, medium, and high

Risk levels of existing Board vendors will be shared each November.

Risk levels of new/potential vendors will be shared when recommendations are made to the Board.

(Ref. GIB | 08.14.24 | 6, page 4-5)

Vendors Unable to Report

If a vendor cannot provide a report, ETF will attempt to negotiate alternatives.

If unable to negotiate alternatives, ETF will bring the Board options, considering:

- Necessity of contracting with the specific vendor
- Financial risks to the program with/without vendor
- Reputational risks with/without vendor
- Options to mitigate risks

(Ref. GIB | 08.14.24 | 6, page 5)

Vendors with Medium/High Risk Scores

- ETF will report to Board each November on all vendors.
- Medium or High-risk scores due to findings will require a corrective action plan.
- ETF will report on corrective action plans periodically as appropriate, depending upon progress.

(Ref. GIB | 08.14.24 | 6, page 5)

Application of Framework

- Framework applied to all vendors, not just those affiliated with GIB.
- All vendors will be reviewed versus framework by December 2025.
- ETF will negotiate any needed reporting changes at next contract renewal.
- For in-progress procurements:
  - Comprehensive SOC-2, Type II will typically meet the reporting required.
  - Addendum issued to allow “alternative independent service auditor reports,” which will be evaluated for sufficiency versus the framework.

(Ref. GIB | 08.14.24 | 6, page 5)

Questions?