What SOC Reports Reveal About Vendor Cyber Risk

May 2026

forvis mazars

What SOC Reports Reveal About Vendor Cyber Risk

Meet Our Presenters

Karen Cardillo
Managing Director, SOC & HITRUST

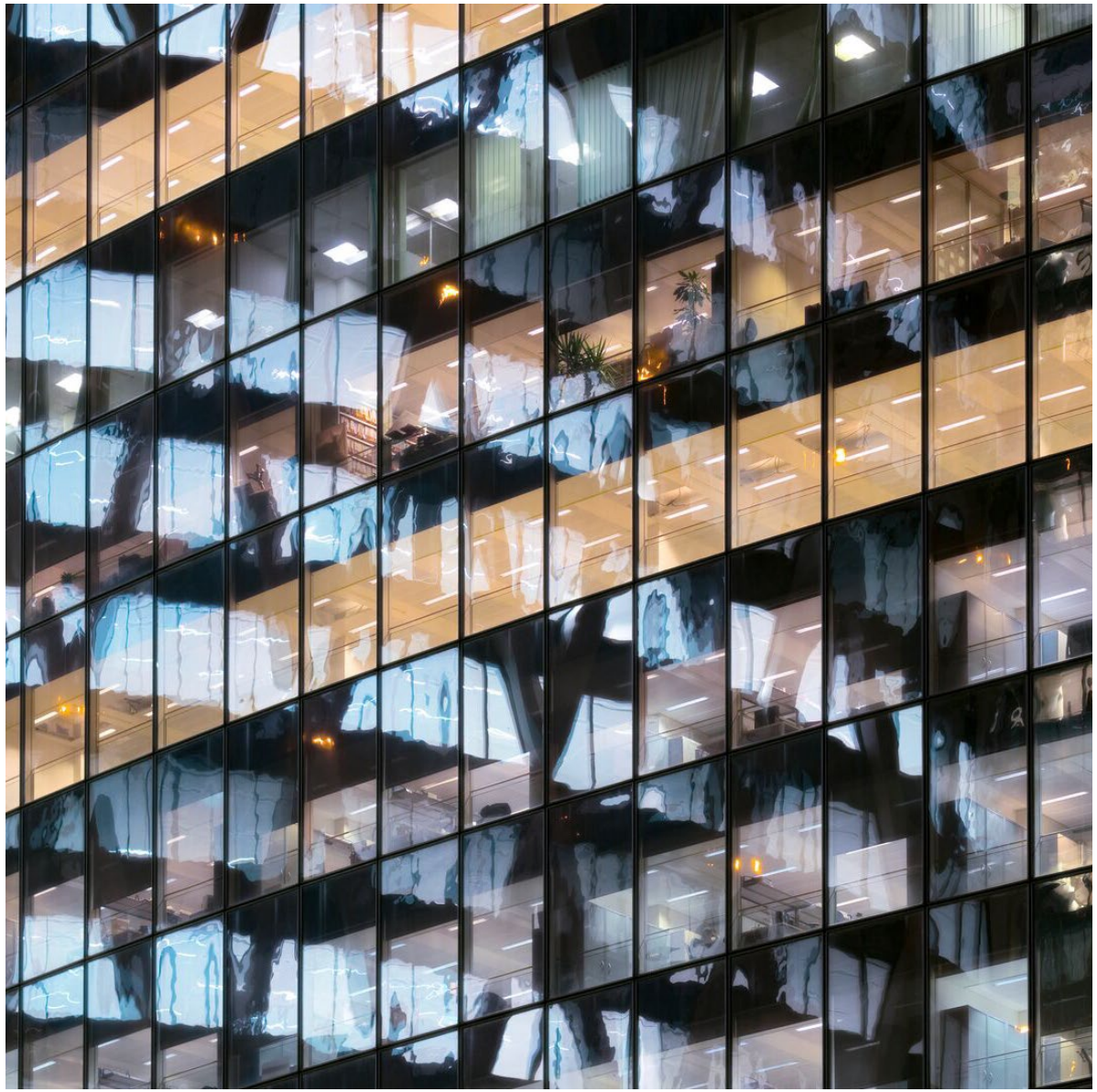
336.259.6611
karen.cardillo@us.forvismazars.com

Ryan Boggs
Principal, SOC & HITRUST

828.989.3176
ryan.boggs@us.forvismazars.com

Agenda

1. Introductions
2. Cybersecurity Update
3. Third-Party Risk & Internal Controls
4. SOC Suite of Services
5. How to Read & Evaluate a SOC Report
6. Closing



2026 Cybersecurity Legal Landscape Updates

There are several data privacy law updates in 2026, including the following:

State privacy "patchwork" is now the default: 20 states have comprehensive consumer privacy laws, driving multistate compliance programs

Federal focus sharpened on cross-border data: DOJ's EO 14117 "Bulk Data" rule restricts certain data transactions with "countries of concern"

Incident reporting remains in flux: CISA delayed CIRCIA final rules to May 2026; organizations still rely on existing breach notification regimes

Financial services bar rose: SEC amended Regulation S-P (incident response + 30-day customer notice) & NYDFS Part 500 final requirements took effect Nov 1, 2025

Children's data protection tightened: FTC updated COPPA with expanded "personal information" & mandated written security/retention controls

International regimes matter: EU DORA applies from Jan 17, 2025; UK Data (Use & Access) Act 2025 updates UK data protection rules

U.S. State Privacy Laws
Patchwork Expands

State Updates

Twenty states have enacted comprehensive consumer privacy laws.

- *e.g.*, CA, VA, CO, CT, UT, TX, FL, MD, MN, OR, NJ, KY, NE, RI, etc.

Statutes

New statutes took effect through 2025–early 2026, increasing obligations for notices, consumer rights handling (access/correct/delete/opt-out), & vendor contracts.

Practical Implication

Build a single “highest common denominator” privacy program with state-specific deltas (thresholds, sensitive data, opt-out signals, appeal rights).

forvis mazars

U.S. Federal
“Bulk Data” Restrictions & CIRCIA Delay

- DOJ’s final rule implements Executive Order 14117 by prohibiting/restricting certain covered data transactions with designated “countries of concern” & covered persons
  - Rule effective April 8, 2025; compliance provisions phase in, emphasizing controls around sensitive personal data & data brokerage-type transfers
- CIRCIA incident reporting: CISA delayed publication of final rules to May 2026 (proposed rule published April 4, 2024)
- **Implication**: Continue meeting existing state/sector breach notification duties while preparing IR reporting workflows that can adapt to CIRCIA once final

forvis mazars

Financial Services

Tougher Cybersecurity & Breach Notice

SEC Regulation S-P amendments require covered institutions to implement written incident response programs & provide customer notice within 30 days (with limited exceptions)

Amendments also require service provider oversight via written policies & procedures & enhanced record-keeping

NYDFS Part 500: Final phase of Second Amendment requirements took effect November 1, 2025—expanded MFA & written asset inventory procedures for covered entities

Implication: Align SEC/NYDFS requirements with enterprise IAM (MFA), asset inventory, vendor risk governance, & breach notification playbooks

forvis mazars

Enforcement & Children's Data
Higher Scrutiny

- Regulators emphasized enforcement on opt-out mechanisms, disclosures, & "reasonable security" expectations as more state laws mature
- FTC's COPPA Rule update (effective June 23, 2025) expands "personal information" to include biometric identifiers & adds security/retention program requirements
- **Implication**: Strengthen identity lifecycle controls, monitoring, & data minimization, especially for products/services involving minors or sensitive data categories

International

Operational Resilience & UK Reform

EU DORA

EU DORA is an EU regulation that entered into force January 16, 2023, and applies as of January 17, 2025—setting digital operational resilience requirements for financial entities & ICT third-party risk management.

Use & Access

UK Data (Use & Access) Act 2025 – makes changes to UK GDPR / DPA 2018 / PECR.

- *e.g.*, automated decision making, subject access, complaints handling, international transfers

Practical Implication

Harmonize ICT risk, incident management, & third-party oversight across regions; update governance for cross-border operations & vendor ecosystems.

What to Do Now
Control-Focused Checklist

01

Data Mapping & Inventories
Confirm asset & data inventories (systems, vendors, cross-border flows) & classify “sensitive” data to meet EO 14117/sector rules

02

Identity & Access
Expand MFA coverage, tighten JML lifecycle (disable dormant accounts), & enforce least privilege for regulated environments

03

Incident Response
Update IR plan for 30-day customer notice (Reg S-P) & build adaptable reporting workflows anticipating CIRCIA timelines

04

Third-Party Governance
Enhance due diligence, contract clauses, & ongoing monitoring to meet SEC/NYDFS expectations & DORA-style ICT third-party risk controls

05

Children/Sensitive Data
Implement retention schedules, written security programs, & product reviews for biometric/minors data handling (COPPA + state laws)

Breach Costs Are Up

The U.S. continues to lead the average total cost of data breaches at $10.22 million.

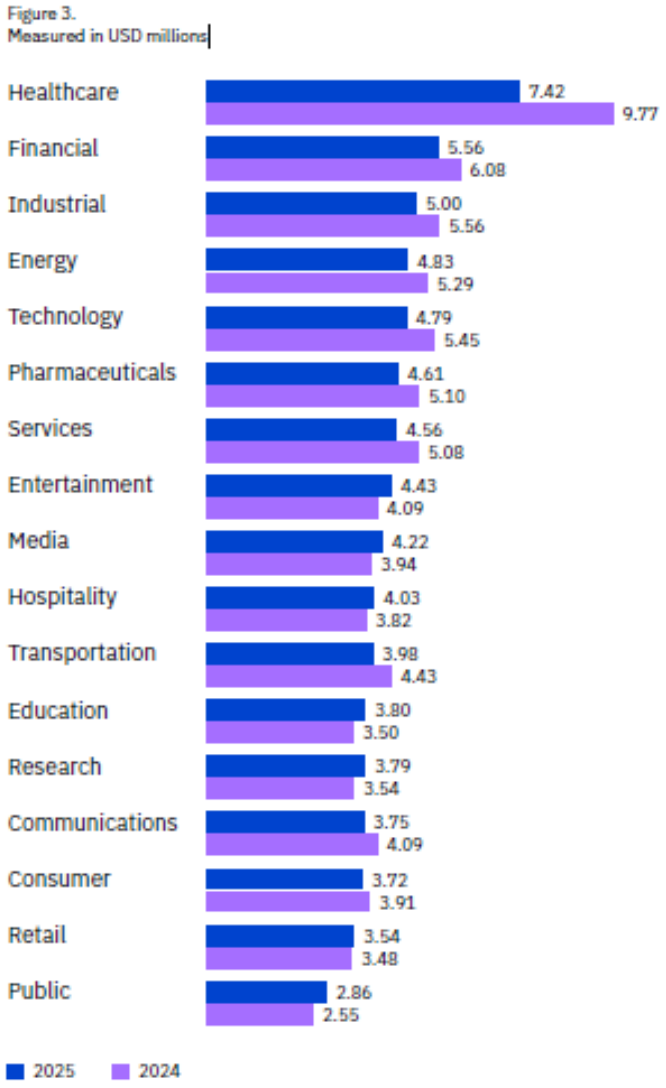
Figure 2.
Measured in USD millions

#	Country		2025	2024
1	United States	↑	$10.22	$9.36
2	Middle East	↓	$7.29	$8.75
3	Benelux	↑	$6.24	$5.90
4	Canada	↑	$4.84	$4.66
5	United Kingdom	↓	$4.14	$4.53
6	Germany	↓	$4.03	$5.31
7	Latin America	↓	$3.81	$4.16
8	France	↓	$3.73	$4.17

2025 Cost of a Data Breach Report – Ponemon Institute, IBM Security

forvis mazars

Average Total Cost of a Data Breach by Industry
Measured in US$ millions



Attackers continue to value & target the industry's patient personal identification information (PII), which can be used for identity theft, insurance fraud, & other financial crimes.

Healthcare $7.42 million

DOWN from $9.77 million

12

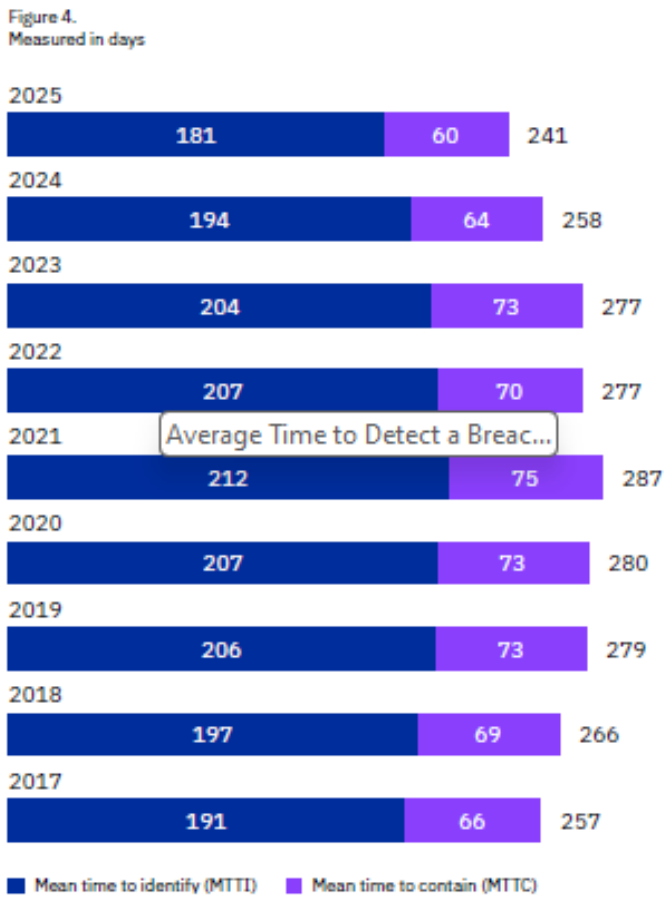
Consecutive years Healthcare had the highest industry cost of a breach

2025 Cost of a Data Breach Report – Ponemon Institute, IBM Security

forvis mazars

Average Time to Detect a Breach in the U.S.
Average Time to Identify & Contain

Measured in days

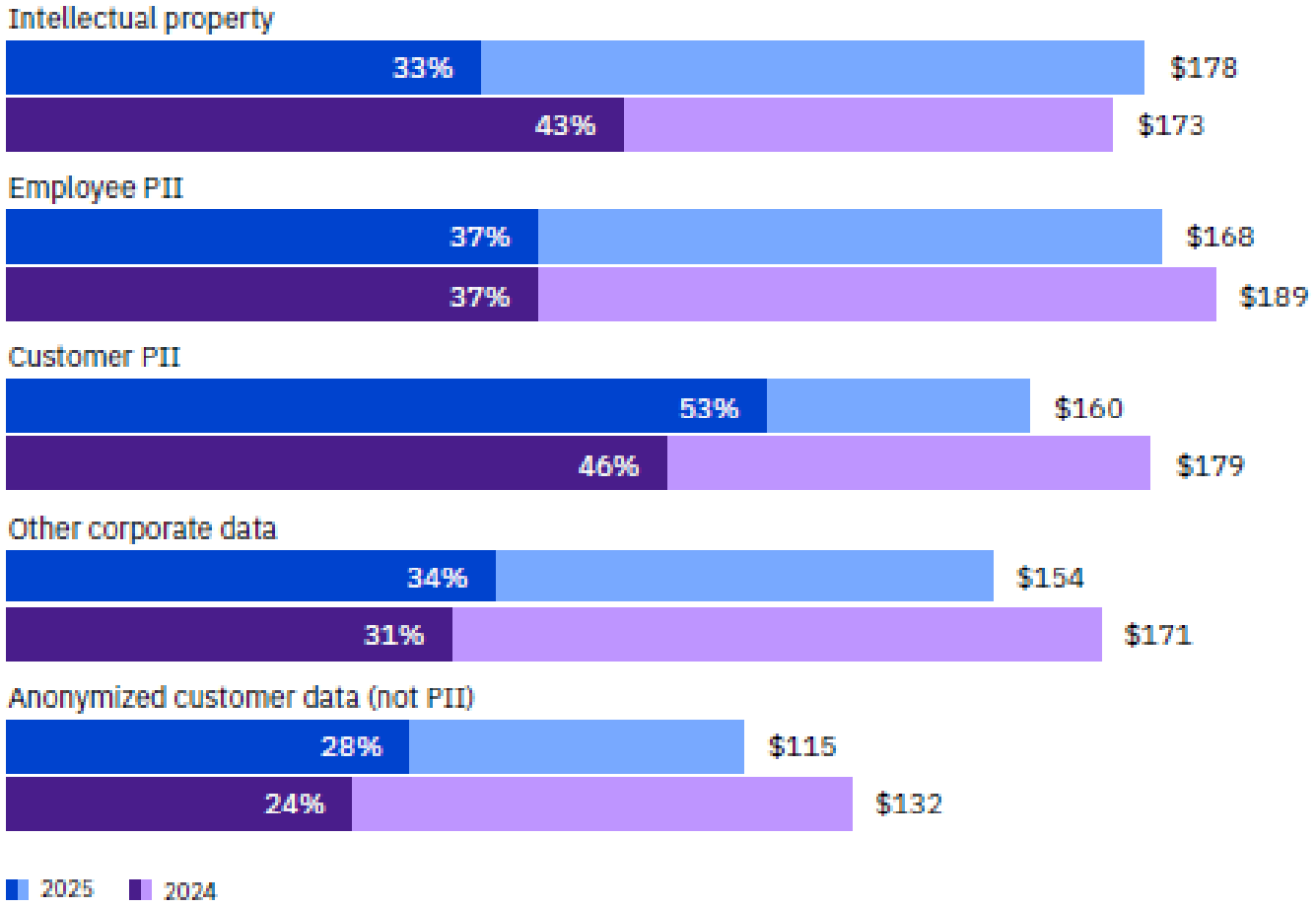


Time to identify & contain a breach decreased.

The mean time organizations took to identify & contain a breach fell to 241 days, reaching a nine-year low & continuing a downward trend that started after a 287-day peak in 2021.

2025 Cost of a Data Breach Report – Ponemon Institute, IBM Security

Type of Data Compromised

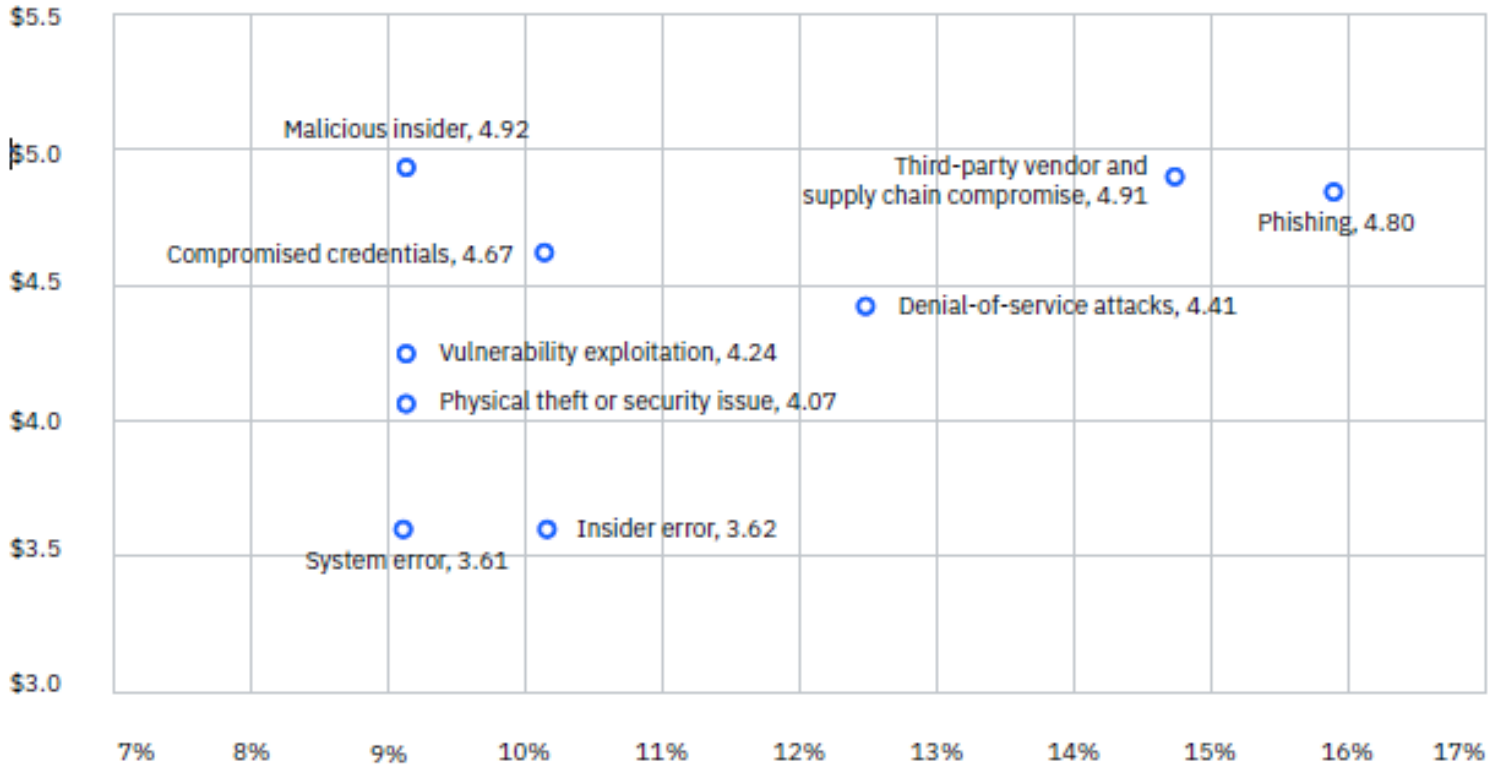


2025 Cost of a Data Breach Report – Ponemon Institute, IBM Security

Customer personal information continues to be the most common type of data compromised. On the other hand, company intellectual property (IP), while less commonly stolen or compromised, was the most costly (US$ 178 per record).

Attack Vectors

Figure 9.
Measured in USD millions; percentage of all breaches



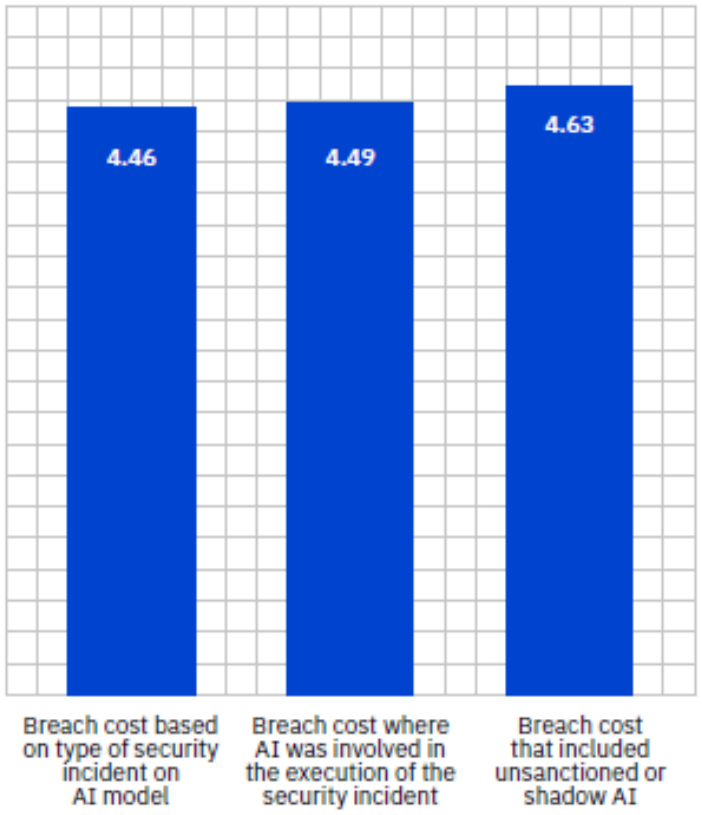
For the third year in a row, phishing was among the top attack vectors.

Vendor & supply chain compromise followed closely behind, overtaking compromised credentials as the number two attack vector.

2025 Cost of a Data Breach Report – Ponemon Institute, IBM Security

AI Risk

Figure 31.
Measured in USD millions



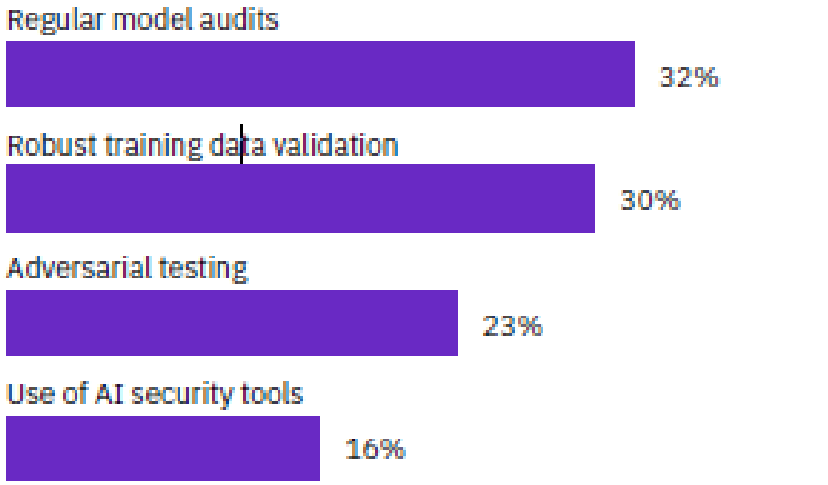
2025 Cost of a Data Breach Report – Ponemon Institute, IBM Security

1 in 6

Number of breaches involving AI-driven attacks

Effect of AI on data breach costs
The average cost of the breach was similar (US$ 4.49 million & US$ 4.46 million, respectively) whether AI was used or not. However, if the breach involved a security incident with **shadow AI**, the average cost was higher (US$ 4.63 million).

Figure 32.
Percentage of breaches involving an AI model; more than one response permitted



87% of organizations said they have no governance policies or processes to mitigate AI risk. Nearly two-thirds of breached organizations didn't perform regular audits on their AI models to mitigate risk.

Single Biggest Risk? Users
Importance of Awareness Training

Your Staff

Your own employees: An estimated 65% of breaches are caused by an organization's users.

Your C-Suite

C-level executives are **12x** more likely to be the target of social engineering attacks.

Training

Are **all employees & contractors** required to complete information security training?

Risk Assessments
The Value of Your Data

- Daily business operations rely on data that may not be deemed critical
- Part of evaluating risk is maintaining data classification assessments
- **You ARE a target!**
- **Note**: Global meat processor paid ransom of $11 million

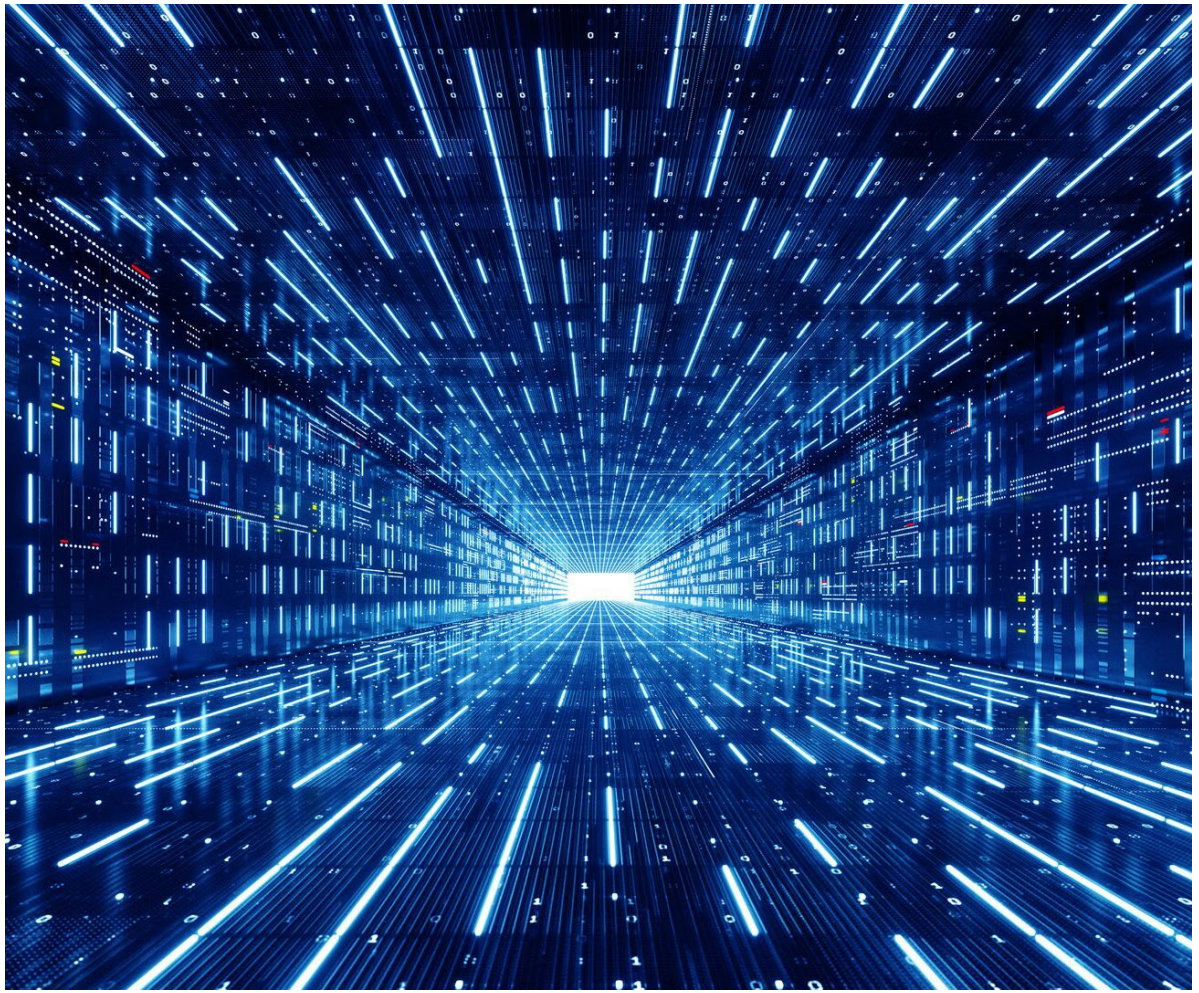
$5.08 million

Average total cost of a ransomware breach

forvis mazars

What Are 10 Best Practices?

1. Email Protection Systems
2. Endpoint Protection Systems & Device Security
3. Access Management
4. Data Protection & Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Device Security
10. Third-Party Risk Management



2026 Updates

Policy applications are more detailed than before: Incorrect statements on the application can lead to denied or reduced claim payouts

Multifactor authentication requirements: Applications are being denied or will have higher deductibles if MFA is not in place

Expect a forensics visit: Vital as they help close the gaps that permitted the breach, but they also reveal weak controls

One of the top five reasons for nonpayment: Failing to require or complete information security training

Poor control environments may reduce claim payouts

Third-Party Risk & Internal Controls

Third-Parties

A **Third-Party Service Provider** (TSP) is generally defined as an external person or company who provides a service or technology.

Vendors

In today's technology-driven business environment, organizations routinely share data with third parties, vendors, and other business partners.

Technologies

Some examples in your own control environment may include claims processing software, data center hosting providers, hosted general ledger applications, & other software-as-a-service solutions.

Third-Party Risk & Internal Controls

- **Third-Party Risks** are the potential risks that arise from companies relying on outside parties to perform business services or activities
- **Third-Party Risk Management** (TPRM) is a form of risk management that focuses on identifying & reducing risks related to the use of third-parties (sometimes referred to as vendors, suppliers, partners, contractors, or service providers)

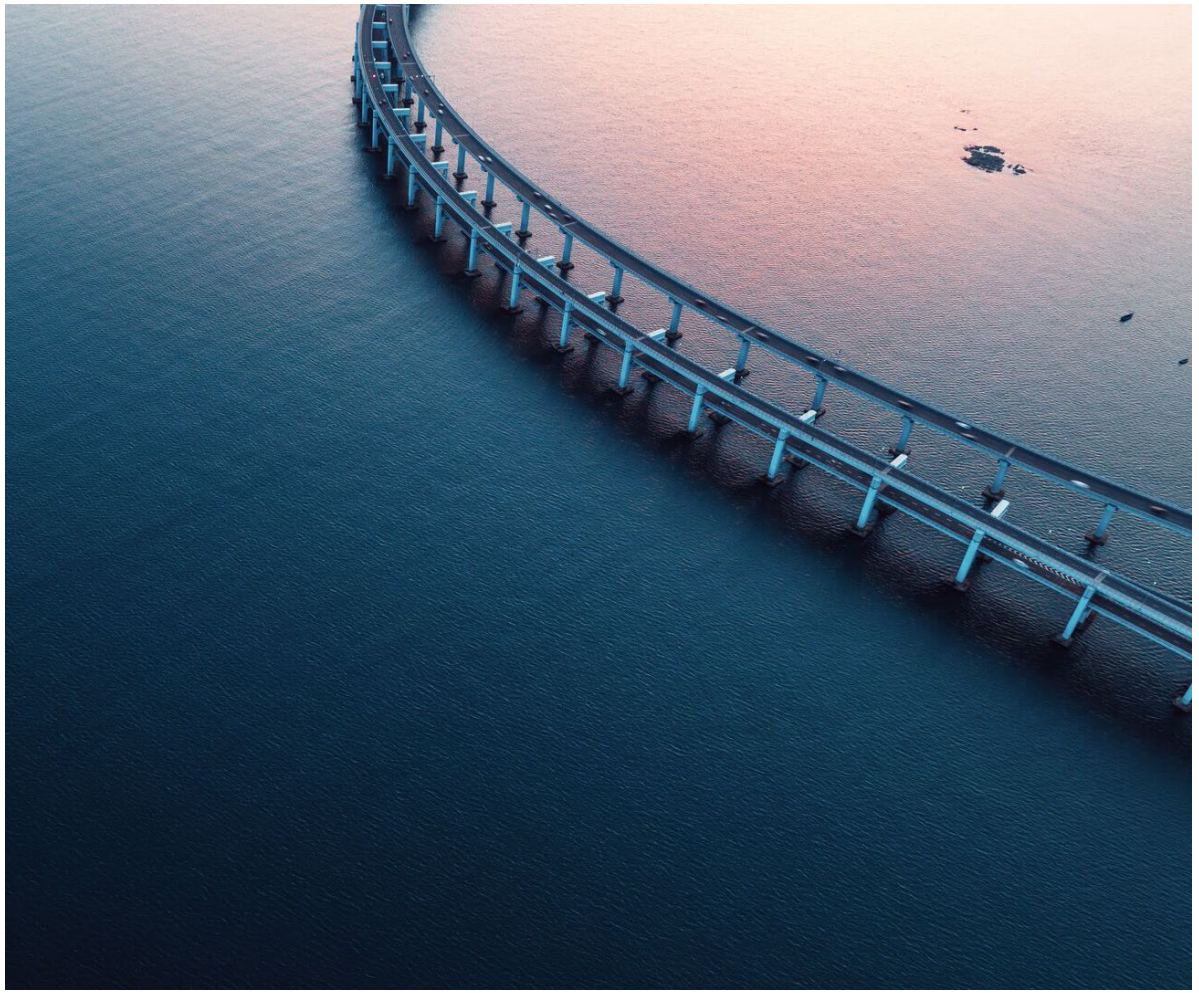
Vendor Management Program

- TSPs inherently expose customers to an array of risks including strategic, reputational, operational, transactional, & cybersecurity risks
- The purpose of a Vendor Management Program is to help identify, measure, monitor, & control the risks associated with TSPs
- The program establishes the authority, basis, & platform for the development, communication, implementation, interpretation, & enforcement of applicable operating standards & procedures to manage vendors

Vendor Management Program
Responsibility

So, who is responsible for a Vendor Management Program?

- Board of Directors?
- Chief Executive Officer?
- Compliance Officer?
- General Counsel?
- Chief Information Officer?



Vendor Management Program
Matrix Responsibility

So, who is responsible for a Vendor Management Program? *(continued)*

Each member of the organization plays a vital role in helping to ensure controls at vendors are properly implemented, managed, & monitored.

This matrix responsibility stems from senior leadership of a company providing direction & oversight all the way to individual users of the vendor's services that interact with the vendor on a day-to-day basis.

Vendor Management Program
Key Risk Summary

- This table summarizes the key third-party risks for which companies should plan to protect the interests of their clients, employees, & the overall health of their operations
- These risks may contribute to operational & reputational harm, with a potential for significant revenue impact, if not handled properly

Third-Party Risks	
Information Security/Data Privacy	Third party has insufficient experience & controls to protect the company's customers' information from unauthorized access, disclosure, modification, or destruction
Business Continuity	Third party cannot continuously maintain its services due to business disruption, *e.g.*, ineffective redundancy procedures
Financial Viability	Third party is not financially secure to continue to provide services at acceptable levels
Country/Credit	Ineffective oversight of vendors or civil unrest
Contract Compliance	Third-party's policies & procedures for products not consistent with users' policies
Legal/Regulatory	Third party does not possess necessary licenses to operate & remain compliant with domestic & international laws, if applicable

How to Manage Risk

Evaluation

Evaluate vendors based on risk to the company

- What data is held?
- How critical is the application to operations (availability)?
- Number of users?

Monitoring

Based on evaluation, perform monitoring procedures

- Continuous monitoring
- Annual vendor surveys & questionnaires
- Evaluate compliance reports, such as **SOC reports**

How to Manage Vendor Risk

Diligence

Pre-contract due diligence

- Identify clear requirements during the request for proposal (RFP) stage
- Require vendor security questionnaire & compliance attestations that clearly identify how each vendor will store & manage data to be completed
- Evaluate information provided

Reviews

Evaluate each vendor based on risk to the company at least annually

- What data is held?
- How critical is the application to operations (availability)?
- Number of users?

Monitoring

Based on evaluation, perform monitoring procedures

- Continuous monitoring
- Annual vendor surveys & questionnaires
- Evaluate compliance reports, such as **SOC reports**

What Are SOC Reports?

System & Organization Controls (SOC) for Service Organizations

- SOC for Service Organizations Reports are internal control reports on the services provided by a service organization providing valuable information that users need to assess & address risks associated with an outsourced service

Why SOC Reporting?

- As more companies use third-party service providers, there is more demand for a detailed understanding of the processes & controls of these third-party service providers (referred to as service organizations)
- Service organizations need to show their customers (referred to as user organizations) or prospective customers what processes & controls they have in place around internal controls over financial reporting &/or information security controls around the systems or services they provide

For CPAs

Provides information to user auditors & service auditors on understanding & performing SOC for Service Organizations Reports

For Users & User Entities

Provides information to user entities on how to mitigate the risks associated with outsourcing services

For Service Organizations

Provides information to service organizations that they can use to build trust & confidence in their systems

SOC Reporting Basics
Key Terms

Service Organization or Service Provider
Organization providing the outsourced service

Subservice Organization
Company used by the service organization to provide third-party services

User Organization or User Entity
Organization receiving the outsourced service

Service Auditor
Auditor performing SOC Examination of the service organization's controls

User Auditors
External auditors of the user organization/entity

SOC Suite of Services

SOC 1

These attestation reports are specifically intended to meet the needs of entities that use service organizations (user entities) as their financial statement auditors (user auditors) use these reports to help evaluate the effect of the controls at the service organization on the user entities' financial statements.

SOC 2

These attestation reports are intended to meet the needs of a broad range of users that need assurance about a service organization's controls as they relate to the security, availability, & processing integrity of the systems the service organization uses to process its users' data & the confidentiality & privacy of the information processed by those systems.

General Examination

These attestation reports are reports on which the Service Auditor issues an opinion about whether a subject matter is in accordance with (or based on) the criteria or the assertion is fairly stated, in all material respects. This type of report is highly customizable to whatever a service organization's needs may be & is intended to provide a service organization's user entities with reasonable assurance over a subject matter.

SOC 3

SOC 3 reports are designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing integrity, confidentiality, &/or privacy but do not have the need for or the knowledge necessary to make effective use of a SOC 2® Report. Since they are general use reports, SOC 3® reports can be freely distributed.

SOC Reporting Basics
Key Terms

SOC 1 & SOC 2 Reports are the most common & useful for vendor risk management purposes.

	SOC 1	SOC 2
What Is Covered by the Report?	Controls related to financial reporting for user organizations	Controls relevant to security, availability, confidentiality, processing integrity, &/or privacy
Intended Audience	Auditors & management of user organizations (“auditor to auditor communication”)	Auditors, stakeholders, *e.g.*, management, business partners, customers, regulators
Report Format	Long form which includes a detailed description of the system & controls	Long form which includes a detailed description of the system & controls

SOC Reporting Basics
Key Terms

Type 1

- Not to be confused with a SOC 1, a Type 1 Report signifies that the report is only as of a specific point in time
- This type of report includes design & implementation but does not include operating effectiveness of controls
- **Example**: SOC 1 Type 1 or SOC 2 Type 1

Type 2

- Not to be confused with a SOC 2, a Type 2 Report signifies that the report covers the operations of controls over a specified period of time
- This type of report includes design, implementation, & operating effectiveness of controls
- **Example**: SOC 1 Type 2 or SOC 2 Type 2

How to Evaluate a SOC Report
Initial Questions

User to Service Provider(s)

- What does the User (the company) outsource & to whom?
- How does that compare to the scope of the SOC 1 Report(s) received from those Service Providers?
  - Nature/type of services
  - Applications covered/not covered
  - Geographies/processing centers covered/not covered

Subservice Organization to Service Provider

- Is there anything that the Service Provider outsources to a third-party?
- If so, how is this handled in the opinion?

How to Evaluate a SOC Report
Anatomy

Section 1: Report of Independent Service Auditors (Opinion)

- Was the auditor's opinion qualified or not? If qualified, why was it qualified?

Section 2: Management's Written Assertion (Assertion)

- This section generally contains the same information as the opinion

Section 3: Management's Description of the System (Description)

- Review the scope of description to identify systems & applications covered
- Evaluate subservice organizations & potentially obtain SOC reports for any significant subservice organizations relevant to financial reporting
- Evaluate complementary user entity controls & verify these controls are within your environment

Section 4: Control Objectives & Control Activities (Controls & Testing Results if Type 2)

- This section includes tests & results, important to identify any issues noted by the Service Auditor & how they might impact your own control environment
- Important to evaluate whether or not tests are sufficient for your needs; inquiry alone is never sufficient

Section 5: Optional Section (May include management's responses to testing exceptions)

- Management can provide responses to testing exceptions here, which can be useful in determining impact to your own control environment

Forvis Mazars SOC & HITRUST®

Forvis Mazars can help with SOC Reporting needs.

- Forvis Mazars has a **dedicated team** that focuses only on helping third-party providers build trust with their prospective clients through compliance reporting vehicles such as SOC & HITRUST
- Our professionals use & deliver:
  - Transparent, **proven** methodologies
  - **Innovative technology** & tools that drive efficient & effective engagements
  - **Quality & credibility** you can trust
  - A **future-focused** approach

If you come across third parties from which you have asked for a SOC Report & they don't have one, please refer us!

Q&A

SOC & HITRUST® Solutions

Questions?

forvis mazars

Contact

Forvis Mazars

Karen Cardillo
Managing Director
336.259.6611
karen.cardillo@us.forvismazars.com

Ryan Boggs
Principal
828.989.3176
ryan.boggs@us.forvismazars.com

Scan to learn more about our SOC & HITRUST® Services

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 Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their 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.