# Help Me With HIPAA Podcast Education Documentation Form

On _____, _____ listened to the following podcast episode for additional HIPAA Compliance education.

**Spend Smarter Before the Breach - Ep 575**

Aug 28, 2026




There are two times to spend money on cybersecurity: before something goes wrong, when you still have choices, and after something goes wrong, when your choices have packed a bag and left town. With the average U.S. data breach now costing $11.5 million, the question isn't whether security costs money. It's whether you're spending that money on the things most likely to keep a bad day from becoming a very long, very expensive year. The latest breach-cost research offers some surprisingly practical clues, including faster detection, smarter access controls, employee training, encryption, simpler systems, qualified security help, and properly managed AI. And there's an important catch: outsourcing the work doesn't outsource the accountability. This episode digs into how to spend smarter while you still have the luxury of deciding where the money goes.

## In this episode:

## Spend Smarter Before the Breach - Ep 575

### Today's Episode is brought to you by:

### Kardon

### and

### HIPAA for MSPs with Security First IT

Subscribe on Apple Podcast. Share us on Social Media. Rate us wherever you find the opportunity.

**Great idea! Share Help Me With HIPAA with one person this week!**

**Learn about offerings from the Kardon Club**

**and HIPAA for MSPs!**

**Thanks to our donors. We appreciate your support!**

**If you would like to donate to the cause you can do that at HelpMeWithHIPAA.com**

**Like us and leave a review on our Facebook page:** www.Facebook.com/HelpMeWithHIPAA

---

## Episode Roadmap


[00:00] Why Spending Before a Breach Actually Saves You

[01:09] Left of Boom vs. Right of Boom: Thinking Ahead on Breach Costs

[02:54] IBM/Ponemon Cost of a Data Breach Study—Why It Matters in Healthcare

[06:49] How AI-Driven Attacks Are Speeding Up and Raising Costs

[10:14] Breaking Down What Really Drives Breach Expenses

[13:00] Healthcare's 13-Year Streak: Most Expensive Breach Costs

[16:20] Average 247 Days to Identify and Contain: The Real Risk of Delays

[23:00] Why Owners and Compliance Officers Can't Fully Outsource Cybersecurity

[31:38] Full Recovery from a Breach—What It Actually Takes

[32:38] Spend Smarter: Security by Design, Testing, and Training That Matter Most

[42:19] Complexity, Shadow IT, and Vendor Risk: Why Simpler Wins

[49:14] AI and Quantum: How Fast Tech is Changing the Security Game

[52:42] Key Takeaways: Fix AI Governance, Vendor Management, and Remember It's About People


---

# Spend Smarter Before the Breach

Cost of a Data Breach Report 2026 | IBM

# Why We Keep Coming Back to This Report

- One of our favorite annual reports
- Useful for risk management priorities
- Helps answer:
    - Where do we get the most bang for our buck?
    - What investments may reduce breach costs?
    - What tends to make breach costs worse?
- Helpful when explaining spending priorities to leadership
- Evidence for deciding where limited time, money, and people should go

# About the Study

- 21st annual report
- Research dates back to 2005
- 7,087 organizations studied since the research began
- 602 organizations in the 2026 study
- 3,558 interviews
- 17 industries
- 16 countries and regions
- Breaches from March 2025 through February 2026
- Breach sizes:
    - 2,590 to 115,380 compromised records
- Healthcare represented 2% of this year's sample or about 12 of the 602 organizations
- Nonstatistical benchmark research
- Use as decision-support evidence, not a prediction for every organization

Don't worry, we will get to AI eventually here is a quote to let you know how AI is important:

> "*AI-driven attacks increased 56% over last year's study. The financial consequences were not minor. AI-driven attacks added an average of USD 1 million per breach as AI tools allow attackers to increase their velocity and scale. That speed is reshaping breach economics—and not in a good way.*"

# The Big Numbers

- Global average breach cost: $4.99 million
- Up 12%
- US average: $11.5 million
- Detection, escalation, and lost business drove much of the cost

Discussion:

- Breach cost is much bigger than fixing technology
- Disruption

- Investigation
- Lost business
- Legal and regulatory response
- Recovery

## Healthcare Is Still Number One

- Highest average breach cost for the 13th consecutive year
- 2026 healthcare average: $6.64 million
- 2025 healthcare average: $7.42 million
- Down 10.5%
- Still highest among all industries studied

Healthcare root causes:

- 59% malicious/criminal
- 21% human error
- 20% IT failure

## Time Is Money

- Average identify + contain time: 247 days
- Reversed several years of improvement

Cost by breach lifecycle:

- Under 200 days: $4.32 million
- Over 200 days: $5.65 million

Who found it fastest:

- Internal IT/security: 209 days
- MSSP: 230 days
- Attacker disclosure: 268 days
- Third party: 281 days

SMB translation:

- You do not need your own SOC
- You do need to know:
    - Who is watching?
    - Who gets notified?
    - Who responds?
    - How fast can they act?

## Recovery Is Bigger Than Containment

- 42% fully recovered
- Only 4% recovered in less than 50 days

IBM's recovery definition includes:

- Operations back to normal
- Compliance obligations completed
- Customer confidence restored
- Employee trust restored
- Controls and expertise added to reduce recurrence

## Where Do We Spend the Money?

Cost reducers included:

- DevSecOps
- IAM
- Key lifecycle management
- Encryption
- Offensive security testing
- SOAR
- Employee training
- EDR
- MSSP support




SMB translation:

- Build security into changes
- Control access
- Encrypt sensitive data
- Test for weaknesses
- Automate response where practical
- Train people
- Monitor endpoints
- Use qualified outside help when needed

Main point:

- SMBs do not need the same tools as large enterprises
- They need the same security outcomes at an appropriate scale

## What Makes Breaches More Expensive?

Top cost-increasing factors:

- Supply chain compromise
- Security complexity
- Lack of application visibility / shadow IT
- Regulatory noncompliance
- Mismanaged secrets and keys
- Inability to prioritize threats
- Security skills shortage

- Excessive privileges / poor role management

Healthcare translation:
- Vendors
- MSPs
- Cloud apps
- Forgotten systems
- Too much access
- Nobody owning the process

Recurring point:
- Outsourcing the work does not outsource accountability

# Encryption: How Do You Not Know?

- 53% did not encrypt sensitive data at rest and in motion
- 10% were unsure
- 37% said yes

Discussion:
- Forget whether encryption solves everything
- How do you not know whether sensitive data is encrypted?
- Inventory issue
- Governance issue
- Evidence issue
- SRA issue
- Risk management issue

# The Fundamentals Are Still the Fundamentals

- Phishing still top initial attack vector
- Fourth year in a row
- Voice/SMS phishing: $5.29 million average
- Social engineering: $5.23 million
- Valid account abuse still expensive
- Supply chain compromises took among the longest to identify and contain

Main point:
- AI changes the speed
- The basic problems are still:
    - Credentials
    - Phishing
    - Access
    - Vulnerabilities
    - Third parties

# Now Bring In AI

- AI-driven attacks increased 56%

- More than 1 in 4 malicious attacks were AI-driven
- AI-driven malicious breaches added about $1 million on average
- Deepfake / impersonation biggest AI-driven category
- AI-related breaches increased to 21%
- 92% of organizations with an AI-related breach lacked proper AI access controls
- Shadow AI incidents increased to 43%

Main point:
- AI did not replace the fundamentals
- AI made weak governance and weak controls easier to exploit faster

# AI on the Defender Side

Extensive AI and automation use:
- $4.00 million average breach cost

No use:
- $5.93 million

Difference:
- $1.93 million

Time difference:
- Extensive users were 65 days faster identifying and containing breaches

SMB translation:
- Does not mean every practice needs an AI security platform
- May mean:
    - MSP
    - MDR
    - EDR
    - Email security
    - Other providers are using automation effectively

Question:
- What is the technology helping you accomplish?
- Not just: "Does it have AI?"

# Bigger Picture

Use the report to help prioritize:
- What helps us detect faster?
- What helps us contain faster?
- What reduces disruption?
- What improves recovery?
- What can we reasonably implement?
- What can we sustain?
- What evidence supports the spending decision?

Main takeaway:

- Risk management is about making defensible priorities
- Limited resources require choices
- This report helps support those choices

Healthcare connection:

- Breach costs are measured in dollars
- Healthcare consequences can also include:
    - Delayed care
    - Unavailable systems
    - Inaccessible information
    - Operational disruption
    - Patient safety impact

---

The cheapest breach is the one you prevent, but the next best thing is making sure a breach doesn't get an all-access pass to your organization and 247 days to enjoy it. Spending smarter means focusing on the fundamentals that actually change the outcome: controlling access, training people, encrypting data, monitoring systems, managing vendors, reducing unnecessary complexity, and knowing who will respond when something goes wrong. Technology will keep changing, AI will keep making everything faster, and the acronyms will probably keep multiplying, but the basics haven't suddenly become obsolete. The real advantage comes from making thoughtful investments before the crisis, when you can still choose where your dollars go instead of having a breach choose for you.

Remember to follow us and share us on your favorite social media site. Rate us on your podcasting apps, we need your help to keep spreading the word.  As always, send in your questions and ideas!

***HIPAA is not about compliance,***
***it's about patient care.*** ™

Special thanks to our sponsors Security First IT and Kardon.