Data as Capital

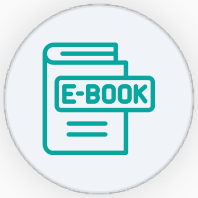
A Cybersecurity Primer for Wealth Management Leaders

Visory

Author:

Ed Vasko

Why Data Security Has Become a Strategic Risk for Wealth Managers



This ebook draws from articles by **Ed Vasko**, Chief Operating Officer at Visory, examining how digital data has become a strategic asset, rivaling traditional resources like oil.

In his **Modern Data: Wealth, Weapons & Data** series, Vasko explores how data is collected, exploited and leveraged by adversaries, and why private enterprises are now central to economic and geopolitical conflict.

The articles underpinning this ebook make a clear argument: **data is no longer just a business byproduct. Data is a resource to be extracted, manipulated and weaponized at scale.**

Wealth management firms handle sensitive personal data, long-term financial intelligence, and increasingly rely on AI. This creates a risk environment for which most firms are unprepared and where traditional cybersecurity models fall short.

Visory

The Industry Reality: Wealth Management Is Now a Data Business

According to a recent **Ernst & Young survey of the wealth and asset management sector**, AI adoption is no longer experimental:

91%
of asset managers are already using or actively planning to use AI in portfolio construction and research

82%
cite regulation as their top growth constraint

45%
of CEOs see generative AI as more risk than opportunity

This creates a **dangerous gap**:
AI is moving faster than data governance.

Key Takeaway

Wealth management firms are racing to adopt AI, but without strong data governance and security, they risk exposing their most valuable asset trust.

Where RISK Lives Now

AI tools extend your data beyond your firm's walls.

Portfolio Modeling

- Client Data
- Financial Plans

Cloud Platforms

- Storage
- Processing

Vendors

- Integrations
- Third-party access

AI Models

- Analysis
- Automation

THE RISK SHIFT

Every new connection creates another point where sensitive client data can be exposed, shared, stored, or manipulated.

AI is moving faster than data governance.

Visory

Why Wealth Management Data Is Uniquely Valuable

From a cybercriminal's perspective, stolen wealth management data is valuable. From a nation-state adversary's perspective, it is strategic.

Aggregated wealth management data reveals:

- **Where capital** is concentrated
- **How portfolios** are positioned under stress
- **Liquidity trends** and sector exposure
- **Behavioral patterns** of high-net-worth individuals

This extends way beyond retail fraud intelligence into a more strategic **economic reconnaissance.**

That is why wealth management firms increasingly sit within the same targeting profiles as law firms, telecom providers and government advisors.

Visory

The Regulatory Landscape
You Must Navigate

Data protection in wealth management is no longer governed by a single regulation. Firms now operate within a multi-domain compliance environment:

REGULATION	REQUIREMENT
SEC Regulation S-P	Written cybersecurity policies, incident response and breach notification
SEC cybersecurity disclosure rules	Rapid reporting of material incidents
FINRA Rule 4370	Business continuity, supervision and communications oversight
GLBA Safeguards Rule	Financial data privacy and third-party oversight.
AI Governance Expectations	Model accountability, suitability and oversight
DOJ bulk data transfer restrictions (2025)	Limits on sensitive data flowing to countries of concern

The key challenge: wealth management firms using cloud providers or AI vendors with operations in, or data flows to, countries of concern may be navigating DOJ restrictions they haven't yet mapped. That is not a hypothetical compliance gap. It is a live one.

From Infrastructure Security to Data-Centric Security

Traditional cybersecurity focuses on devices, networks and perimeters.

But firms **don't lose trust** because a laptop is compromised.

They lose trust because **data is exposed, altered, or misused.**

In today's environment, wealth data **exists across**:

01

Cloud Platforms

02

Fintech Integrations

03

AI training Environments

04

Model Outputs

05

Client Communications

Protecting it requires knowing where data lives, how it moves, and how it is used, **not just where it is stored.**

Visory

Understanding
Data Projection Threats

Most firms focus on protecting data **at rest.**
The greater risk increasingly lies in **data projection:** what happens when data is processed and emitted by AI systems.
Key data projection risks in wealth management include:

Manipulated AI investment recommendations
Small amounts of poisoned input data can significantly skew AI-driven portfolio outputs.

Prompt injection against internal AI tools
Internal copilots used for summaries, compliance drafts or client emails are vulnerable to manipulation.

AI-generated client communications errors
Hallucinated or misaligned outputs can expose sensitive information or violate suitability standards.

Unauthorized use of client data for AI training
Vendor AI improvement using client interactions may violate privacy and regulatory requirements.

Deepfake impersonation fraud
AI-generated voice and video impersonation of advisors or clients is a growing threat in financial services.

Most firms monitor access.
Very few monitor how AI systems transform and emit data once accessed.

Visory

A Practical Assessment Framework for Wealth Firms

This simplified framework helps leadership teams assess exposure, without turning security into a technical exercise.

01

Data Governance

- Is client data classified by sensitivity and regulatory requirement?
- Can the firm trace where data originates, moves, and ends up?
- Do leaders know which AI tools access which client data?

02

AI Governance

- Are AI systems documented with known data sources?
- Is there human review of AI-generated advice and communications?
- Are AI-specific risks (hallucinations, manipulation) addressed?

03

Cloud & Storage

- Is sensitive data encrypted across all environments?
- Are identifiers tokenized and AI training environments isolated?
- Is data location documented and monitored?

04

Third-Party Risk

- Do vendor contracts address AI training on client data?
- Are vendors subject to geographic and regulatory review?
- Is there a secure exit plan for vendor changes?

05

Monitoring & Response

- Is data movement monitored across AI and cloud systems?
- Is there an AI-specific incident response plan?
- Are deepfake impersonation scenarios addressed?

This is more than a checklist. **It helps firms identify blind spots, assess risk exposure, and make informed decisions about data, AI, and operational resilience.**

Source Material

This ebook draws from the following original articles by Ed Vasko, Visory Chief Operating Officer, along with cited research and regulatory references.

- Modern Data: Wealth, Weapons & Data - Part 1
- Modern Data: Wealth, Weapons & Data - Part 2
- Modern Data: Wealth, Weapons & Data - Part 3
- The Wealth Management Milkshake: Why Your Client's Financial Data Is the New Natural Resource

About the Author

Ed Vasko

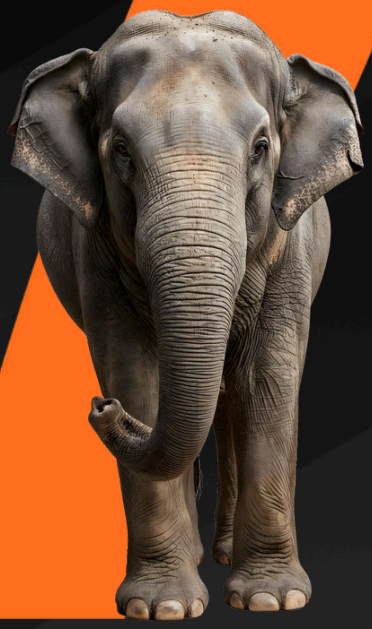
Chief Operating Officer

Visory

Ed Vasko is Chief Operating Officer at Visory, where he helps lead the firm's strategy across cybersecurity, cloud, and data governance for regulated industries, including wealth management.

In his role, Vasko works closely with CISOs, compliance leaders and executive teams to address how modern data practices, particularly the adoption of artificial intelligence, reshape rish, regulation and enterprise security.

Through his writing and operational work, Vasko brings a national security informed perspective to private enterprise, emphasizing that data protection is no longer just an IT concern; it is a matter of trust, fiduciary responsibility and longterm economic resilience.



THANK YOU

Visory