

2024/2025



E-Guide

What every **RIA** should know about Cybersecurity and Managed IT -- a **CFO's Perspective**.



A service of Visory.net
Solutions. Support. Security.

Expertise in:
Wealth Management

Inside



Business Risk **03**

Employee Training **07**

Regulatory Demands **04**

Building Client Trust **08**

Risk Management **05**

The CFOs Role **09**

Cost Effective Solutions **06**

Thank you



Cybersecurity as a Business Risk



Cybersecurity is no longer solely an IT issue; it's a business-critical risk. For CFOs, it's essential to view cybersecurity investments as protections for the firm's bottom line. Financial damages from a breach — including direct losses, regulatory fines, and client distrust — can far outweigh preventive costs. CFOs should lead efforts to evaluate cyber risks and budget adequately for protection measures.



Studies have shown that the average cost of a data breach continues to rise each year. According to IBM's 2024 Cost of a Data Breach Report, data breaches set the average U.S. company back \$5 million.





Compliance and Regulatory Demands

Increased Scrutiny:

Regulatory bodies like the SEC are actively monitoring and enforcing stricter data protection rules, putting pressure on RIAs to strengthen their cybersecurity practices.

Client Data Protection:

RIAs handle sensitive client information like financial details and personal data, making robust cybersecurity crucial to protect against potential data breaches.

SEC Cybersecurity Guidelines:

These guidelines mandate specific security measures that RIAs must implement to safeguard client data, including robust risk management, employee training, incident response plans, and access controls.

Compliance is Essential:

Failure to comply with SEC cybersecurity regulations can lead to significant penalties and reputational damage for RIAs.

As regulators increase scrutiny on data protection, compliance with cybersecurity standards is essential. Policies like the SEC's cybersecurity guidelines demand that RIAs implement rigorous measures to secure client data.

Non-compliance not only incurs fines but damages firm reputation. CFOs should ensure the IT team has the resources and structure needed to meet these regulatory requirements.





Risk Management through Robust IT Strategy

A comprehensive managed IT strategy provides proactive monitoring, regular updates, and rapid response to threats. For CFOs, an outsourced managed IT partner can offer scalability and specialized expertise, saving time and resources while enhancing security. Managed IT services also provide strategic support, enabling the firm to anticipate and address potential risks before they escalate.



While cyber threats are rising, less than 8% of companies perform regular monthly cyber risk assessments, with only 40% conducting them annually. Source: [ISACA](#)





Cost-Effective Solutions with Strategic Budgeting

50%

of CEOs perceive cybersecurity as more pressing than previous years.

\$10.5T

The global cost of cybercrime is estimated to reach this amount in 2025.

77%

of organizations lack an incident response plan.



Balancing cybersecurity costs with business needs is a CFO's challenge. While a high level of security is essential, smart budgeting with targeted investments in necessary areas — like firewalls, endpoint protection, and employee training — can create strong security without overspending. CFOs should work with IT leaders to identify critical investments that yield the highest return on security.

Sources: [Norton](#), [Varons](#), [EFTsure](#)





Employee Training as the First Line of Defense



Many cyber breaches begin with employee mistakes, from phishing scams to weak passwords. Regular training empowers employees to identify potential threats, making them an effective first line of defense. CFOs can champion cybersecurity training programs that foster a culture of security awareness, protecting firm assets and client data.

74%

of data breaches originate from human factors.

80%

of breaches occur in cloud environments from simple errors.

\$4.88B

globally which includes regulatory fines, post-breach customer service, and reputation damage.

Sources: [Secureframe](#), [Varonis](#), [StationX](#), [T|H|E Journal](#)



Building Client Trust

with Cybersecurity Transparency

Clients trust RIAs with their most sensitive financial data. Demonstrating strong cybersecurity measures and managed IT infrastructure shows a commitment to protecting their information.

CFOs play a vital role in communicating the firm's security practices to clients, turning cybersecurity into a competitive advantage that builds long-term trust.





Investing in Cybersecurity and IT — The CFO's Role in Firm Stability



For CFOs at RIAs, managing cybersecurity and IT is essential for risk mitigation, compliance, and client confidence. By viewing cybersecurity through the lens of financial stability and strategic investment, CFOs can help safeguard the firm's future while fostering a culture of security that resonates with clients and regulators alike.

Three actions to take today:

01

Prioritize Risk Assessment and Budget Allocation

02

Establish Cross-Functional Collaboration

03

Invest in Cyber Resilience and Incident Response

Sources: IBM, 2024, Verizon DBIR, 2024



Only 25% of advisory firms surveyed for the T3 2024 Inside Information Advisor Software Survey use cybersecurity solutions.

Ready to get started?



Contact Us



888.252.2990



visoryRIA@visory.net



www.visory.net

Thank you.



 **Visory**