axos
ADVISOR SERVICES

Advisor Insights

Cybersecurity



How to defend your digital data.

It seems that hardly a week goes by without news headlines about a major cyberattack or cyber security breach. Advisors should take inventory of their digital assets to determine where hackers might exploit points of entry or how data may be lost to system errors.

Cybersecurity is becoming less of an esoteric topic for advisors – something that's avoided or relegated to IT personnel to handle. Increasingly, it has become front-page news. Many clients have also picked up on the concern, and have begun asking their advisors questions like:

- "Where is my data being stored?"
- "Who has access?"
- "How are communications being secured?"
- "What happens to my data if our relationship ends?"

Cybersecurity risks have increased over the past few years, with approximately 44,000 attacks daily. To put that into context, every 14 seconds, a company falls victim to a ransomware attack.[1] Multiple factors contribute to this, such as remote workers using mobile devices, new digital tools used for customer data, and customers directing third parties to access their data. New actors have emerged too, with generative AI involved in sophisticated cyberattack campaigns over the past year, according to the 2025 CrowdStrike Global Threat Report.[2]

Before clients and regulators show up asking questions, you may want to review your business's protections and preparedness for potential data breaches.

> **93% of investment management firm executives reported at least one cyber incident in the past year.**
>
> – 2025 Omega Systems 2025 Financial Services Cyber Resilience Report

Reasonable steps are required.

As part of its Code of Ethics and Standards of Conduct, the CFP Board requires financial advisors to take reasonable steps to protect the security of all non-public client information they store electronically. Regulators like the SEC and FINRA also have their own guidance on cybersecurity for financial advisors. This means that advisors can no longer just respond after-the-fact to cybersecurity incidents. Instead, you need to take proactive steps to protect your firm and your clients' data from cyberattacks.

According to 2025 research from Boston Consulting Group, AI-powered attacks are the number one issue keeping Chief Information Security Officers (CISOs) up at night, a 19 percentage-point-increase over 2024 data.[3] A 2025 Accenture study further illustrates the threat, reporting that 90% of companies are unable to defend against AI-related threats.[4]

These figures signal a fundamental shift: AI is no longer a future threat—it is the present reality, and the defensive gap is widening. For independent advisors and broker-dealers, the stakes are especially high. Unlike wirehouses with dedicated enterprise security divisions, most advisory firms operate with leaner resources, making them prime targets for automated, intelligent attacks that conventional tools struggle to catch. A breach here does not just disrupt operations; it erodes client trust and the regulatory standing that forms the foundation of your practice.

This means cybersecurity must move from the back office to the boardroom. It is no longer enough to react after an incident; advisors need resilient, institution-grade protection woven into the fabric of their daily workflows. We built our custody and clearing platform with exactly that philosophy—security by design, continuous monitoring, and adaptive controls that operate behind the scenes so you can focus on serving clients, not chasing threat vectors. Because in an era where AI-powered attacks outpace traditional defenses, your peace of mind depends on having a partner that treats protecting your firm as a shared priority.

Evaluating your cybersecurity preparedness.

Ransomware is just one form of an outside attack. Threats to financial data also include natural disasters and power failures, employees stealing information and other hacker tactics, like phishing. The first step in measuring your cybersecurity is to track your metrics. Track your history of:

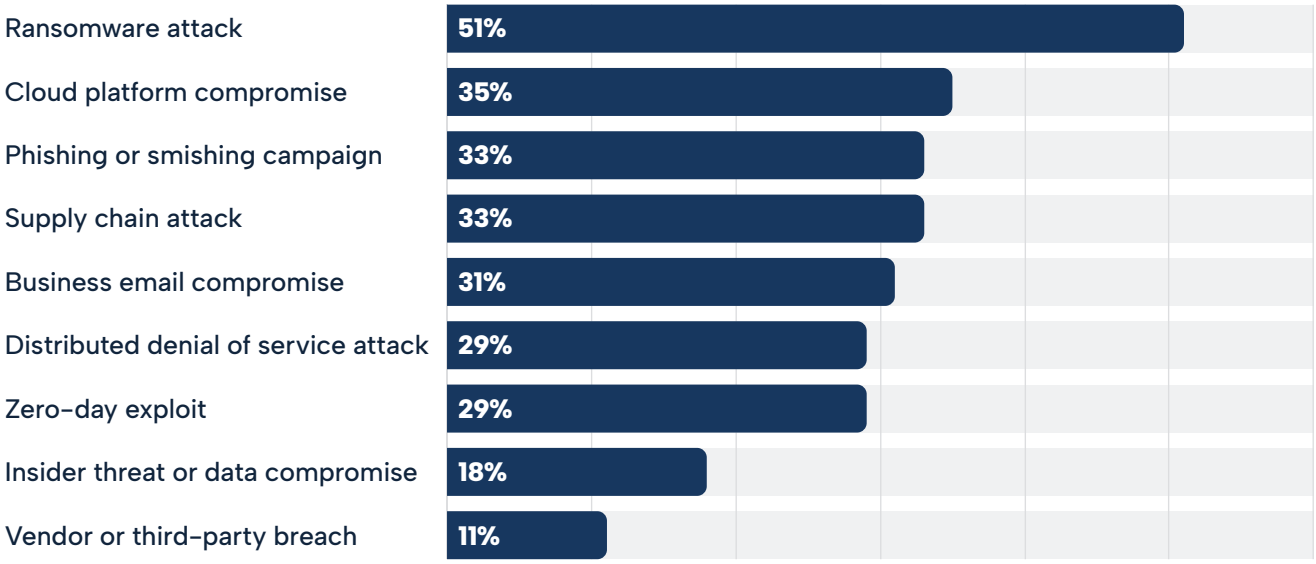
- Cyberattacks or attempts (distributed denial of service, network intrusions and data theft)
- Procedures in place (encryption for all devices and email, Adobe Patch Coverage, Microsoft Patch Coverage, anti-virus coverage)
- Security awareness among employees

There is a checklist from FINRA and a Cybersecurity Assessment Tool from the Federal Financial Institutions Examination Council (FFIEC) available for advisors to organize their data and determine risk levels. You can also take advantage of free web server encryption tests which probe and analyze communication security.

Of course, the complicated layers of technology connection types, delivery channels, online products and services and organizational structures within each practice make every advisor's risk unique. Consider hiring an outside IT advisor with credentials in cybersecurity and financial services to make the most of these assessments. Smaller operations where one person may be responsible for compliance, legal functions and the cybersecurity program are particularly advised to hire extra help.

As you evaluate how you'll protect client information and your own system operations, be sure to evaluate how your insurance will protect your business. Some firms and independent advisors leave it up to a cyber-coverage rider attached to their traditional errors-and-omissions coverage. These policies may not cover regulatory fines or all claims, therefore you may want to consider a standalone policy.

What types of cyberattacks do you feel unprepared to effectively recover from?



Source: *2025 Financial Services Cyber Resilience Report, Omega Systems*

Preparing for potential cyberattack threats.

Once you've understood your digital strengths and weaknesses, it's time to document detailed policies and procedures for all areas of your business. Consider these six key cybersecurity areas:

1 Remote Work

Many of the same challenges brought on by the rise of remote work are likely to remain and grow in popularity due to the convenience and access they offer. According to Cybersecurity Ventures, cybercrime was projected to total $9.5 trillion globally in 2024, the equivalent of the world's third-largest economy, following the United States and China.[5]

2 Authentication Practices

While multi-factor authentication (MFA) remains a strong method for securing client information, challenges remain. Prove Identity's 2023 State of MFA Report found that one-third of consumers do not enable MFA because they find it annoying, and over half (58%) prefer mobile-based authentication.[6] The OTP strategy has known security limitations, while geolocation is a more complex issue because it involves customer privacy and compliance. Although limiting the functionality that can be performed on mobile devices is being used by at least a third of organizations, it poses a customer experience challenge as the mobile channel grows, introducing friction for the customer and increasing the risk of customer attrition.

3 Third-Party Access

Business leaders are keenly aware of the growing demands by customer-directed third-party applications seeking access to their data. Anytime a consumer uses an online tax service, e.g., H&R Block, a personal financial management app, e.g., Intuit's Mint, or a digital mortgage provider, e.g., Rocket Mortgage, the third-party reaches out to a financial services company for access to the customer's own data. The challenge then becomes how to safely provide access and manage the process.

4 Vendor Management

Find out about your vendors' technical safeguards, such as limits on data access, virus protection, idle browser session timeouts, strong password requirements and encryption of data at rest or in transit. They should have regularly updated software and firewalls, as well as accredited audits. Ask about their physical and administrative safety; for example, data backups and shredding and disposal procedures. You'll want to complete this due diligence with each vendor on a regular basis, requesting verifying information for your records.

5 New Digital Tools

Financial leaders expect that the rise in third-party data access will require them to adapt to this ever-expanding access point. More than half (58%) state that third-party data access will require new policies and practices to manage these third-party encounters.[7] About half expect it will require changes in identity management practices and state it will require new customer validation procedures.

6 Mobile Device Use

Leaders are putting their resources into deploying two-factor authentication as a key strategy to serve their employees and third-party vendors more safely at 69% overall, followed by device registration at 51%, using OTPs at 41%, and geolocation and limiting mobile device functionality at 39% each. There are some notable differences within certain financial sectors in treating the different populations. In the insurance sector, device registration is the top strategy to serve customers more safely followed by two-factor authentication. However, when it comes to employees and vendors, two-factor authentication is the leading strategy, but device registration is second to last.

Where are firms making investments to their overall cybersecurity plan?

51%

Cloud adoption, migration & security

50%

Advanced threat detection & response (MDR, EDR, SOC)

41%

IT infrastructure modernization

39%

MFA & identity access management controls

37%

Network & perimeter security

36%

Backup & disaster recovery

Source: *2025 Financial Services Cyber Resilience Report, Omega Systems*

Training your staff and your clients.

When SEC examiners evaluate a business' cybersecurity preparedness, they may focus on how well you've trained employees to be responsible and how the education is tailored to specific job functions.

Make training intentional and keep staff updated. Rather than conducting two hours of training once a year, consider implementing 30-minute monthly sessions on topics such as phishing, fraudulent IRS calls, and client impersonation scams.

Get employees involved in writing and revising your policies and procedures for the six key cybersecurity areas. It may also help to set up leaders with specific knowledge and response roles for different kinds of security events your business faces.

Internal education and communication is necessary, but the responsibility extends to clients as well. The security of your operations is linked to the caution clients take with their information.

As you build client relationships, set some ground rules for secure communication, for example emailing to set up a phone call when discussing certain material. Teach clients how to recognize phishing scams and other threats that are beyond your business operation reach, but could still effect you in asset loss and data breach claims. Easy ways to educate clients and staff include sending articles and podcasts (try Cyberwire and Security Now), which outline cybersecurity news and practices.

Taking action in the event of a cyberattack.

Even with extra meetings and careful measures by staff and clients, data encryption and software updates, errors can happen Proofpoint's 2024 Voice of the CISO report found that 74% of CISOs cited human error as the leading cybersecurity risk.[8]

There are several resources to review when planning, including FINRA's guide which outlines steps to take in case of a security event. First contain and mitigate an event by shutting down a system or disconnecting from a network, depending on the type of incident. Then, identify affected assets within the organization, restore systems from clean backups or rebuild them from scratch, install patches, change passwords and tighten network perimeter security.

Investigate the extent of data and/or monetary loss and identify root causes, all the while keeping a log of this information for client communication and insurance claims purposes. And as soon as you think necessary, notify clients of the event and assure them you will make them whole by offering reimbursement or credit monitoring services. This is a way to assuage their future cybersecurity fears.

You may even want to visit your local FBI field office and get to know a nearby FINRA Regulatory Coordinator so you can plan collaboratively and proactively. It's useful to have investigators and regulators in your corner in the event of an attack or breach.

Use your resources by connecting with regulators and joining online groups (see the Financial Services Information Sharing and Analysis Center) to find threat and vulnerability information, conduct planning exercises and more.

Consider how investing in your cybersecurity plans can add to your value proposition. In 2024, FINRA examination findings continued to rank cybersecurity among the most frequent areas of deficiency at advisory and brokerage firms, particularly at smaller and mid-sized practices, where formal incident response protocols and dedicated external security partnerships are often missing.[9] The broader implication is that cybersecurity is no longer a back-office IT checkbox; it is a front-office trust issue. Clients and prospects are increasingly asking how their most sensitive financial data is safeguarded, and they can sense when defenses are fragmented or merely reactive. Firms that proactively close these gaps do more than avoid regulatory scrutiny, they convert data protection into a visible competitive advantage that deepens client confidence and signals institutional maturity. In other words, your cybersecurity posture is inseparable from the fiduciary brand you are building every day.

> **Allocating dollars and education, internally and externally, to cybersecurity measures could give your practice a competitive edge and the fortification your business needs to keep growing.**

A partner committed to protecting your client data.

Your clients entrust you with their most sensitive financial information, and that trust is the foundation of your practice. You deserve a custody partner that treats protecting that trust as seriously as you do.

We built our security architecture around one principle: enabling you to focus entirely on advising while we handle the invisible work of safeguarding every byte of client data. Our Information Security Program is independently reviewed by internal auditors and examined as part of ongoing regulatory examinations, giving you documented assurance to share with clients and compliance officers alike.

That protection operates across three layers designed specifically for the realities of wealth management:

Fortified Access Controls

Client data is guarded by advanced firewalls and rigorous authentication protocols, including challenge-response tokens and digital certificates that verify every identity before granting platform access. Whenever information moves between systems, it travels behind 256-bit Secure Socket Layer (SSL) encryption—the same standard relied upon by the world's largest financial institutions. You can reassure your clients that their data rests behind bank-grade infrastructure, because it does.

Intelligent Transaction Surveillance

Rather than waiting for an incident to respond, we continuously analyze transaction patterns and scan for anomalies across our network. Advanced analytical systems flag suspicious activity in real time, helping intercept unauthorized access before it affects your clients. Consider it a dedicated security team working around the clock so your firm does not have to build one.

Governed Privacy by Design

Access to sensitive account information is strictly limited to pre-screened personnel who need it to service an account. Every employee handling that data completes ongoing privacy and security training. For you, that translates to confidence that client confidentiality is maintained by protocol, not by chance—reinforcing the trust that drives your business forward.

Cybersecurity is not a static checklist; it is an evolving discipline. We continuously monitor our controls, collaborate with government agencies and industry partners, and refine our defenses as threats advance. That means when the next wave of AI-driven attacks emerges, your practice is already behind defenses that adapt faster than most firms can assemble on their own.

You chose independence to serve your clients without compromise. Your custody partner should protect that independence with security that never cuts corners. If you are ready to discuss how our infrastructure supports your fiduciary duty, let's start the conversation.

Partner with a team committed to protecting your data.

sales@axosadvisorservices.com 866-776-0218 axosadvisorservices.com

Sources:

[1]Astra Security, *How Many Cyber Attacks Happen Per Day?*, 2026

[2]CrowdStrike, *2025 Global Threat Report*

[3]Boston Consulting Group (BCG), *AI Creates Cyber Risks. Can It Also Resolve Them?*, 2025

[4]Accenture, *State of Cybersecurity 2025*

[5]Cybersecurity Ventures, *Cybersecurity Almanac 2024*

[6]Prove, *2023 State of MFA Report: Consumer Attitudes Toward Multi-Factor Authentication*

[7]Prove Identity, *2023 State of MFA Report*, April 2023

[8]Proofpoint, *2024 Voice of the CISO Report*, May 2024

[9]FINRA, *2024 Annual Regulatory Oversight Report*, January 2024

For Institutional Use Only.

Investment Products: Not FDIC Insured - No Bank Guarantee - May Lose Value.

Axos Advisor Services is a trade name of Axos Clearing LLC. Axos Clearing LLC provides back-office services for registered investment advisers. Axos Clearing LLC does not provide investment advice or make investment recommendations in any capacity. Securities products are offered by Axos Clearing LLC, Member FINRA & SIPC. Axos Clearing, LLC does not provide legal, accounting, or tax advice. Always consult your own legal, accounting, and tax advisors.

©2026 Axos Clearing LLC. Member FINRA & SIPC. All Rights Reserved.

2342368

axos ADVISOR SERVICES