Delaware Life®

Financial Cybersecurity:

How Advisors Can Protect Client Data and Trust

Key Takeaways

Trust is built through protection. Clients care about how you handle their data as much as how you grow their money.

Start with small, smart habits. Multifactor authentication, password managers, and secure vendor relationships go a long way.

Cybersecurity is a client conversation. Use it to show leadership, not just compliance.

"It's hot out there—and it's getting hotter." That's how Christopher Kennedy, Chief Information Security Officer at Group 1001, describes today's cybersecurity landscape.

For financial advisors, information security isn't just a technology issue. It's also about trust. Cybersecurity is now a fundamental part of how clients evaluate their advisors. And when client data is compromised, so is the advisor-client relationship.

Protecting your clients' ability to live and invest—as well as the client-advisor relationship—means protecting data, especially in the financial sector. We're here to help you reduce risk, stay compliant, and most importantly—safeguard client trust.

According to Kennedy, today's top threats are:

- **Social engineering:** Convincing impersonations of clients, advisors, or staff designed to manipulate, extract information, or access money.
- **AI-based deepfakes:** Voice or video impersonations that appear frighteningly real.
- **Insider threats:** Mistakes or misconduct by employees or contractors with access to internal systems.
- **Ransomware and malware:** Systems locked down, data held hostage.
- **Distributed Denial of Services (DDoS) attacks:** Disruption that shuts down services just when clients need them.
- **Identity theft:** Fraudsters stealing personal and financial information to commit financial fraud.
- **Supply chain attacks:** Compromising third party vendors or software providers to infiltrate financial organizations. As Kennedy says, "The economic supply chain touches all of us. We're all reputationally at risk."

Five Steps Every Advisor Should Take to Proactively Secure Their Practice

Financial services companies are increasingly leveraging data risk analytics, monitoring data usage, and deploying automated response capabilities to identify and mitigate potential risks. But you don't need to be a tech expert to implement solid cybersecurity—you just need to start building strong security awareness and cybersecurity hygiene. To start, Kennedy recommends these five fundamentals that can have a big impact:

1 Lock Down Access: Multifactor Authentication Is Non-Negotiable

Use multifactor authentication (MFA) for all business platforms, especially anything tied to financial data protection. Skip text-based MFA when possible; authenticator apps are more secure. Don't reuse passwords. Use a password manager. And keep personal and business accounts separate.

Access management is also essential for controlling user privileges and preventing unauthorized access, forming a critical part of a robust security framework.

Want a quick reference for enabling MFA and other everyday protections? See our Online Safety vs. Cyber Scams Checklist for 10 easy, commonsense steps to reduce your risk.

2 Know Your Vendors (and Their Vendors)

Cloud platforms make business efficient—but every integration is a potential risk. Ask your vendors the right questions:

- Do you encrypt data in transit and at rest?
- Who has access to my clients' data?
- What's your breach response process?

Think of it like building a house: You still need to walk the floors every day. Conduct regular security audits of vendors to identify vulnerabilities and ensure ongoing protection. Even if you use third-party platforms, your reputation is still on the line.

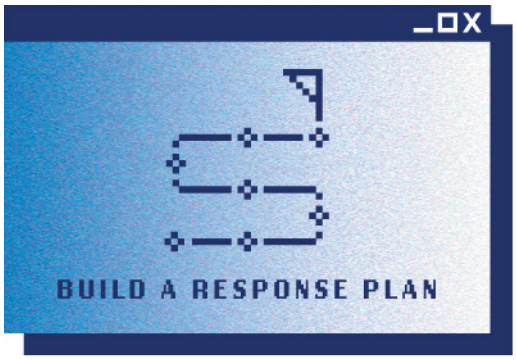
> "If you're not **demanding security** from your business partners, who is?" Kennedy asks. "It's your brand, it's your business, and **your clients' trust is on the line.** Regulatory compliance alone doesn't make you secure...The demand signal for security has to come from within the business, not from the regulator."

3 Train Like It Matters (Because It Does)

Social engineering isn't just happening to big firms. Train your team to pause and verify requests for money, data, or access. Teach clients how to recognize suspicious activity with communication about common threats and transparency if something goes wrong. And be proactive—don't wait until something goes wrong to explain your process.

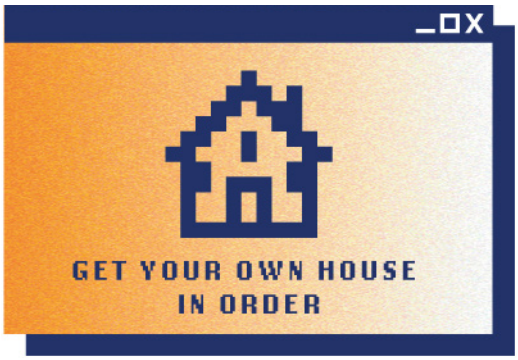
For more client-ready talking points on spotting phishing, deepfakes, and other online scams, explore our Beware of Cyber Crimes flyer.

4 Build a Response Plan You Hope You'll Never Need

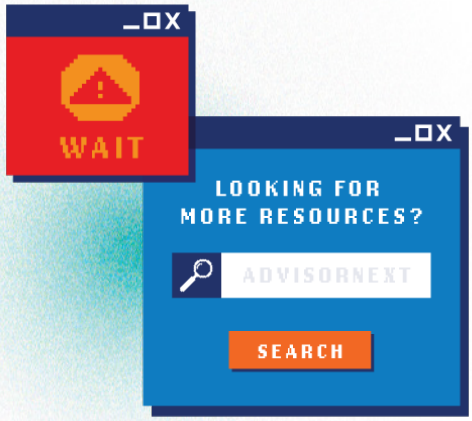


Most incidents fail not because of the breach, but because no one knew what to do next. Create a plan. Know who to call. Document what systems are mission-critical. Even small firms should have a breach response protocol in place. If something does go wrong, fast response builds trust.

5 Get Your Own House in Order



Cybersecurity for financial services starts with you. If your personal laptop isn't updated, your email isn't secured, and your social media is wide open—you're a target. As Kennedy says: "If you're not managing your own data well, how can you credibly protect your clients'?"



Cybersecurity and Keeping Clients Informed

Don't treat cybersecurity as a hidden back-office issue. Use it to strengthen your client relationships:

- Offer secure portals and explain how they protect financial data.
- Help clients enroll in MFA.
- Share tips on avoiding phishing and impersonation scams.
- Reassure clients with your preparedness and process.

Remember: **Protecting financial data is protecting financial futures.**

Delaware Life: A Partner in Data Protection

We don't just talk about cybersecurity. As part of Group 1001, Delaware Life is committed to proactive threat detection, secure advisor platforms, and timely communication about emerging risks. Financial cybersecurity isn't about doing everything – it's about doing the right things.

For more educational content and practice management resources, be sure to explore our advisor content hub at **AdvisorNext.**