



Introduction

Financial advisors handle some of the most sensitive data in existence: Social Security numbers, tax records, investment portfolios, and direct access to client funds. That combination makes registered investment advisors—and the firms that serve them—an exceptionally attractive target for cybercriminals.

At Liftman Insurance, we have specialized in protecting financial professionals since 1957. That is nearly seven decades of experience helping investment advisors, broker-dealers, hedge funds, and RIAs understand, manage, and transfer risk. In that time, we have watched cyber threats evolve from a niche technical concern into one of the most serious business risks facing firms of every size.

Recently, we sat down with Fayon Atkinson, Senior Manager of Cyber Risk Services at Travelers Bond & Specialty Insurance, and James Warren, AVP and Managing Director on Travelers' Financial Institutions underwriting team, to discuss what the data shows and steps financial professionals and their firms can take to help minimize these risks. Mark Liftman, President of Liftman Insurance, joined the conversation as well, contributing real-world perspective and client experiences.

Fayon is part of the cyber risk advisory team at Travelers, working directly with policyholders to help prevent cyber events. Her team offers tabletop exercises, incident response planning support, dark web monitoring, phishing simulations, and direct guidance on cyber risk topics. James manages a team of underwriters responsible for selecting and pricing cyber policies for financial institutions. Together, their perspectives span both sides of the coverage equation: prevention and response.

This white paper draws on their expertise - and on our own experience navigating the cyber landscape alongside advisory clients - to help you understand the threat environment, protect your firm, and make informed decisions about your coverage.



Fayon Atkinson
*Senior Manager,
Cyber Risk Services*
Travelers Bond
& Specialty
Insurance



James Warren
*AVP & Managing Director,
Financial Institution
Underwriting*
Travelers Bond
& Specialty Insurance



Mark Liftman
President
Liftman Insurance

Table of Contents

CHAPTER 1

Financial Advisors Are High-Value Targets, Whether They Know It or Not _____ **4**

CHAPTER 2

AI Is Changing the Rules of the Phishing Game _____ **6**

CHAPTER 3

Wire Fraud and Social Engineering _____ **8**

CHAPTER 4

Ransomware: It's No Longer a Question of If, but When _____ **10**

CHAPTER 5

You Are Only As Good As Your Backups _____ **12**

CHAPTER 6

What Happens When a Breach Occurs and
Why a Policy Without Service Isn't Enough _____ **14**

CHAPTER 7

Build the Plan Before You Need It _____ **16**

CHAPTER 8

Not All Cyber Policies Are Created Equal _____ **18**

CHAPTER 1

Financial Advisors Are High-Value Targets, Whether They Know It or Not

“Anyone's vulnerable. If they feel like they can make some money from this, they're going to target you. No one's safe...”



Many financial advisory firms assume they are too small to attract sophisticated cybercriminals. That assumption is both common and costly.

Fayon is direct about why advisory firms draw disproportionate attention: they sit at the intersection of two things attackers want most. First, they hold sensitive personal data: Social Security numbers, account details, tax identification numbers, and personal financial records. Second, they have direct access to client funds. As Fayon put it, that combination is a “sweet spot for hackers.”

“Anyone's vulnerable. If they feel like they can make some money from this, they're going to target you. No one's safe. As bad as it sounds, that's the reality.” - Fayon Atkinson

The larger banks and broker-dealers may have mature IT departments and dedicated cybersecurity infrastructure. The typical RIA, a firm of five to ten employees managing hundreds of millions in assets, often does not. That gap is exactly what attackers look for.

The starting point for any firm is understanding what it is actually protecting. A risk assessment asks: What data do we hold? Where is it stored? Who can access it? Which vendors have access to our systems or our clients' information? For smaller firms, this doesn't need to be a formal engagement, but it does need to happen.

BEST PRACTICE:

- Conduct a risk assessment before your next coverage renewal. Identify the sensitive data your firm holds, the systems that store it, and the vendors who have access. For firms without a dedicated IT team, this can be a structured conversation with your managed service provider, but document the findings. Understanding your exposure is the first step toward reducing it.

CHAPTER 2

AI Is Changing the Rules of the Phishing Game

“With the use of AI, it becomes impossible to spot.”



For years, financial professionals were taught to spot phishing emails by their telltale signs: misspellings, awkward phrasing, suspicious sender addresses. That playbook is becoming obsolete.

Attackers are now using artificial intelligence to craft communications that are grammatically flawless, contextually appropriate, and visually indistinguishable from legitimate messages. Fayon described the shift from what she sees in the field:

“Before, it would be super easy to detect an email that wasn’t legitimate because there would be spelling errors or it would just look off. Now, with the use

of AI, it becomes impossible to spot.” - Fayon Atkinson

The threat extends beyond email. “Deep fakes,” AI-generated audio or video that convincingly impersonates a real person, are emerging as tools for social engineering, particularly for higher-dollar fraud attempts. An attacker who can fabricate a voice message from a trusted contact has a powerful tool for bypassing human judgment.

AI also introduces risk from within the organization. Employees across every industry are using AI tools, sometimes with firm knowledge, sometimes without. The danger: an employee who inputs client data into an AI tool to draft a document or summarize information

may inadvertently share that data with an external service. Fayon is clear about the appropriate response: governance, not prohibition. Blanket bans are rarely effective. The goal is to make AI use visible, controlled, and bounded by clear rules about what information may and may not be shared.

BEST PRACTICE:

- Update employee security training to address AI-enhanced threats. The warning signs that once identified phishing emails no longer apply reliably. Train employees to verify unusual requests through a second channel rather than responding directly to the message.
- Establish an AI acceptable use policy. Specify which tools are permitted, what categories of client data may never be entered into AI systems, and who is responsible for oversight. A written policy provides clear guidance to reduce the risk of exposure. Ensure employees get training on how to safely use AI tools.

CHAPTER 3

Wire Fraud and Social Engineering

“ He clicked on a prompt to download an update.
Then the hackers were in his system. ”



One of the most damaging cyber incidents facing advisory firms today doesn't involve ransomware or a network breach.

It involves a convincing email and a wire transfer.

Business email compromise, in which attackers impersonate a client, counterparty, or colleague to redirect funds, is among the most prevalent and costly forms of cybercrime targeting the financial industry. Fayon explained how it typically unfolds, and why the standard instinct to “call and verify” can backfire:

“We have seen an increase in business email compromise, where there's a wire

transaction, and someone didn't follow the appropriate validation process. Attackers put their phone numbers in the emails all the time. So if you call that contact information, you're likely going to get an impersonator.” - Fayon Atkinson

The mechanics are straightforward: an attacker sends an email appearing to come from a known contact such as a client, a bank, or a counterparty, requesting a change in wire instructions. The email looks authentic. The urgency feels real. And if the recipient calls the number provided in that same email, they reach the attacker.

Mark shared a vivid example from his own client base. A client received what

appeared to be a routine software update prompt. He clicked through, not realizing it was a social engineering attack. When he returned from lunch, the damage was done.

"He clicked on a prompt to download an update. Then the hackers were in his system. He came back and \$100,000 was gone from his brokerage account." - Mark Liftman

Fayon noted that urgency is a deliberate tactic. "They push this level of urgency – sometimes they'll overload your email with messages, and then you're overwhelmed, you click the link." Slowing down – even briefly – is one of the most effective defenses available.

BEST PRACTICES:

- Establish a written policy for any wire transfer or change in banking instructions. Before funds move, verify through a second channel using contact information already on file—never the phone number provided in the message you are responding to.
- Train employees to pause before acting on any communication that creates urgency, especially requests involving payments, account changes, or system access. A quick call using a known number costs seconds. A fraudulent wire transfer may be impossible to reverse.

CHAPTER 4

Ransomware: It's No Longer a Question of If, but When

“You want to have your defenses up.”



Ransomware, malicious software that encrypts an organization's files and demands payment for the decryption key, has become one of the most pervasive cyber threats facing businesses of every kind. And according to Fayon, it is not going away.

What has made ransomware so much more common in recent years is a development Fayon calls “ransomware as a service.” Criminal organizations now license their malware tools to other groups who deploy them at scale. The technical expertise required to launch a ransomware attack has dropped dramatically; the number of victims has climbed accordingly.

“It's not about if you're compromised — it's really when. So you want to have your defenses up.” - Fayon Atkinson

Three defensive measures stand out as consistently effective:

Multi-Factor Authentication (MFA). Fayon describes MFA as “low-hanging fruit” for reducing an attacker's ability to gain access. But not all MFA is equal. Passkeys and

FIDO2 security keys are the strongest form. Authentication (fingerprint, facial recognition) and authenticator apps are robust but not the strongest option.

Text-message codes (SMS) are the weakest form. Critically, MFA must apply to elevated and administrative users —not just email — because IT administrators without internal MFA remain a significant vulnerability.

Patch Management. Vulnerabilities in software, including VPNs, operating systems, and applications, are frequently made public before patches are widely applied. Attackers move fast once a vulnerability is disclosed. Ignoring update prompts is one of the most common and preventable mistakes she encounters.

Network Segmentation. In many small-firm environments, an attacker who gains access to one system can traverse the entire network. Segmenting the network, ensuring that, for example, HR and accounting systems cannot communicate directly, limits how far an attacker can move once inside.

BEST PRACTICE:

- Enforce MFA on every remote access point, every email account, and every system that holds client data. Use app-based or biometric authentication rather than SMS codes wherever possible, and do not exempt IT administrators from MFA requirements on internal systems.
- Establish a patch management policy and follow it. When a software update is available, apply it promptly. Vulnerability disclosures are often public knowledge, and attackers move quickly to exploit systems that have not yet been patched.
- Discuss network segmentation with your IT provider. Access to one part of your environment should not automatically mean access to all of it.

CHAPTER 5

You Are Only As Good As Your Backups

“If you have no viable backup,
there's no way for you to operate.”



Many firms believe they are protected from the worst-case ransomware scenario because they back up their data. That belief is only partially correct, and attackers know exactly how to exploit the gap.

Before triggering the encryption that locks a victim out of their files, sophisticated attackers will first locate and delete the victim's backups. Without a backup to restore from, the firm's options narrow to one: pay the ransom. That is the goal.

“Hackers lock up the production environment and threaten to delete the backup, which forces your hand. If you have no viable backup, there's no way

for you to operate. That's the tactic to force you to make that payment.” - Fayon Atkinson

The solution is a backup strategy that accounts for this threat. Fayon introduced a framework known as 3-2-1:

- 3 copies of your data—your active data plus two backups.
- 2 different media types—for example, a cloud-based service plus a physical drive or third-party backup service.
- 1 copy offline or air-gapped—not directly connected to your primary network, so it cannot be reached by an attacker who has infiltrated that network.

Fayon also noted that, as a last line of defense, one copy of the backup data should be immutable so that it cannot be altered or deleted, even by someone with administrative access. James underscored the stakes plainly: "You are in a much better position if you've got your 3-2-1 and you're all backed up in multiple places across multiple environments than you are if you have a single backup that also got compromised, and now you're like, holy cow, they want X number of Bitcoin."

One additional consideration often surprises firms: even when backups are intact, restoring systems takes time. Business interruption, the downtime between a ransomware attack and full operational recovery, is itself a significant cost, and one that a well-structured business continuity plan should address.

BEST PRACTICE:

- Implement the 3-2-1 backup framework. Ensure at least one copy of your data is offline or air-gapped and cannot be deleted or altered remotely.
- Test your backups. Knowing that files are being backed up is not the same as knowing they can be successfully restored. Run a recovery test at least once a year.
- Plan for business interruption. Restoration takes time even when backups are available. Account for that downtime in your business continuity planning, and confirm that your cyber coverage addresses lost revenue during the recovery period.

CHAPTER 6

What Happens When a Breach Occurs — and Why a Policy Without Service Isn't Enough

“Someone has discovered that there was a network breach.
And then there's a whole host of costs associated...”



No matter how well-prepared a firm is, breaches happen. What determines whether the outcome is manageable or catastrophic is not just the nature of the breach—it is what happens in the hours and days that follow.

James described the most common scenario: “Someone has discovered that there was a network breach. And then there’s a whole host of costs associated with figuring out: how’d they get in? What did they see? Was it a segmented network? Do you have notification responsibilities?”

When a breach is reported to the carrier, a response team assembles quickly. Forensic investigators trace how access was gained, what they saw and how long the attacker was present. Legal counsel evaluates what data was exposed and whether notification obligations are triggered, requirements that vary significantly by state and by the nature of the data involved.

Fayon, who spent time in breach response earlier in her career, described the emotional reality of that first call: “I know it’s usually a scary experience. No one wants to deal with that.” The presence of a coordinated response team makes the difference

between a chaotic incident and a managed recovery.

Audit logs matter enormously here. If logs are available, forensic investigators can reconstruct the attacker's movements with precision. Without them, investigators must make assumptions about what the attacker

may have accessed — assumptions that can lead to broader and more expensive notification obligations. Endpoint detection and response (EDR) tools provide an additional layer of visibility by flagging unusual activity in real time and preserving records that logs alone may not capture.

BEST PRACTICE:

- Notify your carrier immediately when you suspect a breach. Attempting to investigate or remediate on your own before notifying can jeopardize your coverage. Response teams are available precisely for this moment.
- Ensure your firm maintains audit logs for all systems that hold client data. Logs give forensic investigators the information they need to reconstruct what happened and limit notification exposure.
- When evaluating cyber coverage, ask explicitly what response services are included. Forensic investigation, legal counsel, breach notification support, and credit monitoring for affected clients are not optional extras, they are the core value of a well-designed cyber policy.

CHAPTER 7

Build the Plan Before You Need It

“Your entire network is down. You can't access your email.
How do you know who's handling what?”



When a cyber event occurs, decisions need to be made immediately: Who is responsible for what? Who has authority to bring in outside help? How do you communicate internally when your email is down? How do you reach clients when your network is offline?

Firms that have thought through these questions in advance and documented the answers recover faster and with less damage than those that have not. Those that have never considered them face those decisions under the worst possible conditions.

An incident response plan (IRP) is the document that answers these questions before the crisis arrives. An IRP includes:

- Roles and responsibilities - Who is in charge and who does what; making sure contact information for all stakeholders is defined;
- Incident categorization and prioritization - How an incident gets triaged, prescribing different steps based on type of incident; what does the response to that incident look like;
- Communications - Preventing having a single point of failure; if email is down, how

are we communicating with the rest of the stakeholders;

- Escalation and notification - Who is responsible for communicating with your cyber carrier; when do you need to get legal counsel; when do you notify the regulator.

Fayon runs tabletop exercises for Travelers policyholders to test whether those plans hold up under simulated pressure.

"Your entire network is down. You can't access your email. How do you know who's handling what?" - James Warren

James added a detail that consistently surprises even experienced teams: "You obviously need an incident response plan and business continuity plan, but you also need a physically printed copy. Because if it's stored on your network that just got compromised, and you can't access it, it's kind of useless."

A printed binder with your incident response plan, key contacts, and escalation procedures is not an outdated precaution. In the event of a full network outage, it may be the only guide available. Fayon asks this question in every tabletop exercise. The answer, more often than not, is that the plan is only accessible online.

BEST PRACTICE:

- Create a written incident response plan appropriate to the size of your firm. Even a brief document that identifies who to call first, what to do immediately, and how to escalate is more valuable than no plan at all.
- Keep physical/offline copies somewhere accessible that does not depend on your network being operational.
- Test it. Run an informal tabletop exercise at least once a year. Ask: if our network went down right now, what would we do? The answers should not require accessing a system you can no longer reach.

CHAPTER 8

Not All Cyber Policies Are Created Equal

The cyber insurance market has expanded considerably, and the range of available coverage is wide. That breadth can make it difficult to understand what you are actually purchasing—or what you are missing.

James identified three broad categories of cyber buyers. The first attaches minimal coverage to a business owner's policy, getting "something better than nothing." The second purchases a standalone policy primarily to satisfy a client requirement or regulatory expectation, selecting the most cost-effective option available. The third is a buyer who wants to know what actually happens if something goes wrong, and is purchasing for the service as much as the coverage.

"Some clients don't look beyond the declarations page to realize what actual coverage they've purchased. You've got a million-dollar limit that covers noth-

ing. Cyber is something you can make very pared back, or you can make it very robust. The difference matters enormously when you actually need it." - James Warren



Cyber is one of the few policies that you can benefit from without actually having a claim.

The distinction that matters most is not the coverage limit but the services that accompany it. Travelers' approach has moved toward what James calls "service-first" cyber coverage, meaning policyholders have access to proactive, pre-breach advisory support as well as post-breach response resources. Fayon's team offers dark web monitoring,

proactive alerts when known vulnerabilities are detected in software policyholders use, incident response planning, tabletop exercises and direct access to cyber risk advisors.

James stated what this means for the value of the policy itself: “Cyber is one of the few policies that you can benefit from without actually having a claim. Most times, you’re only dealing with insurance during claims. Not the case for cyber.”

There is also a structural consideration specific to RIAs. Many carriers add cyber as an endorsement to an existing E&O policy, sharing the same limit across both types of claims. If a significant E&O matter and a cyber event occur in the same policy period, those shared limits can be exhausted quickly. Travelers provides dedicated cyber policies with separate limits, meaning your cyber coverage is not competing with your professional liability coverage.

BEST PRACTICE:

- When evaluating cyber coverage, look beyond the premium and the limit. Ask specifically what services are included—before a breach and after. Ask who responds when you call, how quickly, and what they will handle on your behalf.
- Ask about pre-breach services. Policyholders who engage with proactive services are less likely to experience a breach, and when breaches occur, they tend to be less severe. The investment in prevention pays dividends that a bare-bones policy cannot offer.
- Understand whether your cyber coverage shares a limit with your E&O policy. Shared limits reduce the protection available when you need both at the same time.

Why Advisors Choose Liftman Insurance

Since 1957, Liftman Insurance has been more than just a broker—we've been a trusted partner to over 2,000 financial advisory firms across the country. Founded by Theodore Liftman, a pioneer in the field of financial industry insurance, we've remained a family-run business focused solely on serving investment professionals.

What sets us apart? Depth of knowledge. Concierge-level service. And a legacy of doing the right thing—every time. Our team includes former underwriters who understand how carriers assess risk and price coverage. That insider expertise allows us to design policies that anticipate pitfalls and avoid surprises.

We don't just know the products—we know the people. We have long-standing relationships with underwriters, claims managers, and legal teams at the top insurance carriers. When coverage questions get murky, we're the ones who can pick up the phone and advocate for you directly.

We are available when others aren't. Whether it is a late-night concern about a suspicious email or a weekend question about a policy renewal, we answer the phone. Clients stay with us for decades because we earn that trust through action, not promises.



Mark Liftman

President

Liftman Insurance

Travelers Casualty and Surety Company of America and its property casualty affiliates. One Tower Square, Hartford, CT 06183
This material is for general informational purposes only and is not legal advice. It is not designed to be comprehensive and it may not apply to your particular facts and circumstances. Consult as needed with your own attorney or other professional adviser. This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond issued by Travelers. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.



Let's Talk About Your Cyber Coverage

Whether you're adding cyber coverage for the first time, reviewing an expiring policy, or wondering whether what you have is actually enough—Liftman Insurance can help you navigate these decisions with clarity and confidence.



Call 1-877-LIFTMAN



Visit www.liftman.com



**Or connect directly with a Liftman advisor
to schedule a risk consultation.**