waystone | Compliance Solutions

Cyber Risk in Financial Services, Are You Ready or Just Hoping You Are?

August 18, 2025

If you're in financial services today, cyber risk isn't theoretical. It's a growing, persistent threat and it's hitting firms in the UAE more frequently than ever.

This isn't based on headlines or scare tactics, it's based on what we've seen first-hand. Over the past few months alone, we've either been made aware or helped clients respond to more than 15 cyber-related incidents.

These weren't isolated cases. They cut across different sectors, firm sizes, and business models. And in most cases, the breach didn't start with a sophisticated hack, it started with something small, overlooked, or wrongly assumed to be "under control".

Whether you're in asset management, insurance, wealth advisory, or investment services, one thing is clear: you need to be prepared before, not after, an incident occur.

The Basics of Readiness, Without the Buzzwords

A well-functioning Cyber Risk Management Framework ('CRMF') isn't a document that sits in a policy folder. It's something that actually guides how your firm operates day-to-day. It should help you prevent what you can, detect issues early, respond quickly, and recover with control and transparency.

From the work we've done recently, here are the things that really matter.

1. Know What You're Protecting

Too many firms still don't have a clear inventory of what systems they use, who manages them, what data they hold, or how they connect with each other. That's a major blind spot.

Tip, do a short exercise: ask each team what platforms they use, where they store data, and what would happen if those systems went down. The results are often surprising.

2. Have a Real, Tested Response Plan

A policy that's never been tested isn't much use during a breach. You need a plan that is practical, well understood, and actionable; especially within the first 30 to 60 minutes.

Tip, run a tabletop exercise. Make it realistic. Simulate a phishing attack or account compromise. See what happens when you walk through the actual steps with your team.

3. Train for What Actually Happens

We've seen breaches start from one mistaken click on fake internal email. Many firms had awareness training in place, but not enough to change behaviour or prompt staff to act quickly.

Tip, make training relevant. Show real phishing examples. Talk about how attackers imitate trusted contacts (e.g. SEO/CEO fraud). Build this into onboarding and regular staff refreshers.

Some firms have gone the extra mile and try to get a fake invoice paid, or change an existing clients bank details through email, with clear oversight and controls in place, this is another way of testing your controls, would yours pass?

4. Understand What Regulators Will Expect

Following a breach, regulators are asking detailed questions. They want to understand what controls were in place before the incident, what data may have been accessed, how quickly you detected the issue, and whether internal processes were followed.

Tip, ask yourself now: if this happened to us, could we explain what went wrong, show the audit trail, and demonstrate how we've fixed it? Does your breach register clearly evidence this and was a breach report completed and signed off?

5. Get the Board Engaged

Cyber is a governance issue. Boards need visibility, not just IT updates. They need to understand the risks, the readiness, and the gaps, and they need to be asking the right questions.

Tip, put cyber risk on your next board or EXCO agenda. Start with a short, plain-language briefing on the top risks and your current controls. Then talk about what's missing.

On that point, the budget is always going to be a concern, but the cost (e.g. fixing the issue, time to report, update regulator, produce reports, loss business, etc) of incident or breach could be double or more that asking a third party to assist!

6. Don't Overlook Third Parties

In several recent incidents we've helped with, the problem didn't originate within the firm. It started with a vendor, a service provider, or a cloud platform. But the impact landed squarely on the regulated firm.

Tip, review your vendor list. Are cyber risks considered in your due diligence? Do your contracts include clear expectations? Would you know what to do if a third party suffered a breach?

7. Build a Culture That Expects the Unexpected

Cyber resilience isn't about eliminating every risk. It's about being able to spot issues early, respond fast, and learn every time something goes wrong.

Tip, keep an internal log of incidents and near misses. Use it to evolve your controls and update your CRMF. It shows maturity, and it strengthens your position if you're ever asked to explain your approach.

We've Seen This First-Hand! And It's Getting Worse

The number of breaches we've supported in just the past few months is more than we saw over the entire previous year. That trend should concern every firm operating in the regulated space.

But the good news is, preparation works. The firms that had tested plans, clear escalation paths, and trained staff were able to manage their incidents with confidence and transparency. Others needed more support, and that's exactly where a partner with real-world experience can make a difference. Once again, the point is not to eliminate all risks, because that's simply not possible, but rather to ensure that the firm is prepared. The difference in impact between being prepared and unprepared when an incident occurs is like night and day.

A Better Question to Ask

Too many firms still ask, "do we have a cyber policy in place?", however, a better question to ask is, "if we were breached tomorrow, would we know exactly what to do?"

If the answer is no, you're not alone, but now is the time to act.

You don't need to become experts overnight. But you do need to know your gaps and take steps to close them. A targeted cyber review, gap analysis, or response walkthrough tailored to your firm can mean the difference between a controlled incident and a regulatory headache.

Being prepared doesn't guarantee you'll avoid an incident. But it does mean you'll be ready when (not IF) it happens.

The Waystone Cybersecurity Team is well-equipped to assist organisations in navigating the complexities of these regulations, implementing effective cybersecurity frameworks, and staying ahead of both global and regional cyber threats. Contact us today to learn how we can support your firm in building a robust and compliant IT risk management strategy.

Contact Us →