Cybersecurity Readiness Assessment & Action Planner

Why complete this assessment?

Every financial advisory firm depends on technology to deliver advice, protect confidential client information, and operate efficiently.

Unfortunately, cybersecurity threats have evolved dramatically in recent years, oftentimes looped in with the benefits of technology advancement and improved business capabilities.

Today's attacks are increasingly driven by:

- Stolen identities rather than stolen devices
- Artificial intelligence
- Compromised vendors
- Employee actions and mistakes
- Weak passwords and poor access controls

Cybersecurity is no longer simply an IT responsibility. It’s a business continuity issue, a governance issue, a client trust issue and, ultimately, an existential threat to your business and professional viability.

This assessment will help you:

- Explore your firm's current level of cyber readiness
- Identify vulnerabilities
- Prioritize improvements
- Develop a practical 90-day action plan

Unlike a formal cybersecurity audit, this assessment is intended for business owners and leadership teams. It does not require technical expertise beyond this knowledge shared by SagePath Consulting.

Completing this assessment and action plan doesn't guarantee you won't experience a cybersecurity incident, but it's designed to increase your awareness so you can take action.

How to use this guide

Depending on the size of your firm, have the following people participate:

- Managing partner(s)
- Operations manager or senior operations team member
- Technology lead
- Compliance lead
- Anyone responsible for overseeing vendors

Discuss each question openly. Where opinions differ, capture them in the notes. And remember: the discussion is often more valuable than the score.

Use this scoring system for the topics and statements below:

✓ Fully implemented – Consistently in place/followed across the firm.

◐ Partially implemented – In place but inconsistently applied/followed

✖ Not implemented – Not currently in place

? Unsure – We don't know

Step 1

Technology Foundations

Identity & Access	Score
Multi-factor authentication is enabled everywhere.	
Password managers are used.	
Former employees/advisors immediately lose access.	
Administrator access is limited.	
User access is reviewed annually.	
Temporary staff, contractors and third parties have defined access permissions.	
Notes:	
Devices	**Score**
All firm devices are encrypted.	
Devices update automatically.	
Antivirus/EDR (endpoint detection and response) is centrally managed.	
Lost devices can be remotely erased.	
Personal devices follow firm policy.	
Notes:	
Data Protection	**Score**
Client information is encrypted.	
Backups occur automatically.	
Backups are tested.	
Sensitive information isn't stored locally.	
Critical files have version history.	
Notes:	
Cloud Services	**Score**
Cloud applications are inventoried.	
Access permissions are reviewed.	
Data sharing settings are controlled.	
Vendor security responsibilities are understood.	

Critical SaaS (software as a service) applications, such as your CRM, are monitored.	
Notes:	

What are the two or three biggest technology-related risks facing your firm today?

What improvements would have the greatest impact over the next 90 days?

Step 2

People & Culture

Employees remain one of the largest cyber risks, and one of your strongest defenses.

Security Awareness & Training	**Score**
All employees receive cybersecurity awareness training at least annually.	
New employees complete cybersecurity training as part of onboarding.	
Employees understand how to recognize phishing emails, suspicious links and social engineering attempts.	
Staff know how and where to report suspected cyber incidents immediately.	
Security reminders or awareness tips are shared throughout the year.	
Notes:	
Policies & Safe Practices	**Score**
Employees understand the firm's acceptable use policies for technology and client information.	

Staff know what information can and cannot be shared through email, text or collaboration tools.	
The firm has guidelines governing the use of AI tools when handling client information.	
Employees understand their responsibilities when working remotely or from home.	
Confidential documents are disposed of securely when no longer required.	
Notes:	
Security Culture	**Score**
Employees feel comfortable reporting mistakes or suspicious activity without fear of blame.	
Cybersecurity is discussed regularly by leadership — not only after incidents occur.	
Roles and responsibilities during a cyber incident are clearly understood and documented in a critical response plan.	
Each year, the firm practices responding to a cyber incident through a tabletop exercise or simulation.	
Leadership treats cybersecurity as a business risk, not simply an IT responsibility.	
Notes:	

What are the two or three biggest people-related risks facing your firm today?

What improvements would have the greatest impact over the next 90 days?

Step 3

Vendor Risk

Financial advisory firms rely on third parties to deliver many essential services. Assess how well your firm understands, monitors and manages the risks created by vendors that access systems, support operations or handle client information.

Vendor Selection & Due Diligence	**Score**
We complete appropriate due diligence before selecting vendors that will access firm systems or client information.	
We assess whether prospective vendors have appropriate cyber security and privacy controls.	
We consider a vendor's financial stability, reputation and ability to support our firm over time.	
We confirm where vendor systems and client data are hosted, including whether information may be stored outside Canada.	
We involve the appropriate technology, compliance, privacy or legal resources when reviewing critical vendors.	
Notes:	
Contracts & Responsibilities	**Score**
Vendor agreements clearly define responsibilities for protecting confidential and personal information.	
Contracts require vendors to notify us promptly of cyber security incidents, privacy breaches or service disruptions.	
Agreements explain what happens to our data when the relationship ends.	
We understand which security responsibilities belong to the vendor and which remain with our firm.	
Contracts include appropriate confidentiality, access, service-level and business continuity provisions.	
Notes:	
Access & Data Protection	**Score**
Vendors receive access only to the systems and information required to perform their work.	

Multi-factor authentication is required for vendor access wherever possible	
Vendor accounts and permissions are reviewed regularly.	
Vendor access is removed promptly when it is no longer required or when the relationship ends.	
We know which vendors store, process, transmit or back up client information.	
Notes:	
Monitoring & Oversight	**Score**
We maintain a current inventory of critical vendors and the services they provide.	
Critical vendors are reviewed periodically, not only when their contracts are renewed.	
We monitor significant changes to vendors, including ownership, service model, data practices, and security posture.	
We document and follow up on vendor-related concerns, incidents and service failures.	
Responsibility for managing each critical vendor is clearly assigned within our firm.	
Notes:	
Business Continuity & Exit Planning	**Score**
We understand how a prolonged outage at each critical vendor would affect client service and firm operations.	
We know how to contact critical vendors during an emergency or service disruption.	
We have alternative processes or contingency plans for our most critical vendor dependencies.	
We can retrieve or transfer our data if a critical vendor fails, is acquired or the relationship ends.	
Vendor-related risks are considered in our incident response and business continuity plans.	
Notes:	

Which vendors would create the greatest operational or client impact if they became unavailable?

Which vendors have access to the most sensitive client or firm information?

What vendor-related improvements should be prioritized over the next 90 days**?**

Step 4

Identify Your Top Three Priorities

Name of Priority	Business Impact	Difficulty	Person Responsible Within the Firm	Target Date

Step 5

If You Experienced a Significant Cyber Incident Tomorrow

How confident are you that you could:

- Continue serving clients?
- Protect confidential information?
- Recover operations?
- Meet regulatory obligations?
- Communicate effectively?
- Preserve client trust?
- Do you have appropriate insurance coverage in place?

Step 6

Additional Steps to Consider

If your assessment identified multiple areas of concern, consider:

- Completing the Critical Incident Response Framework available in the Emergency Planning & Succession section of this website
- Conducting a tabletop exercise
- Reviewing vendor partner security and systems/software configuration
- Working with an external expert to conduct an independent cybersecurity assessment
- Developing a longer-term technology risk and security management roadmap
- Providing training to your staff