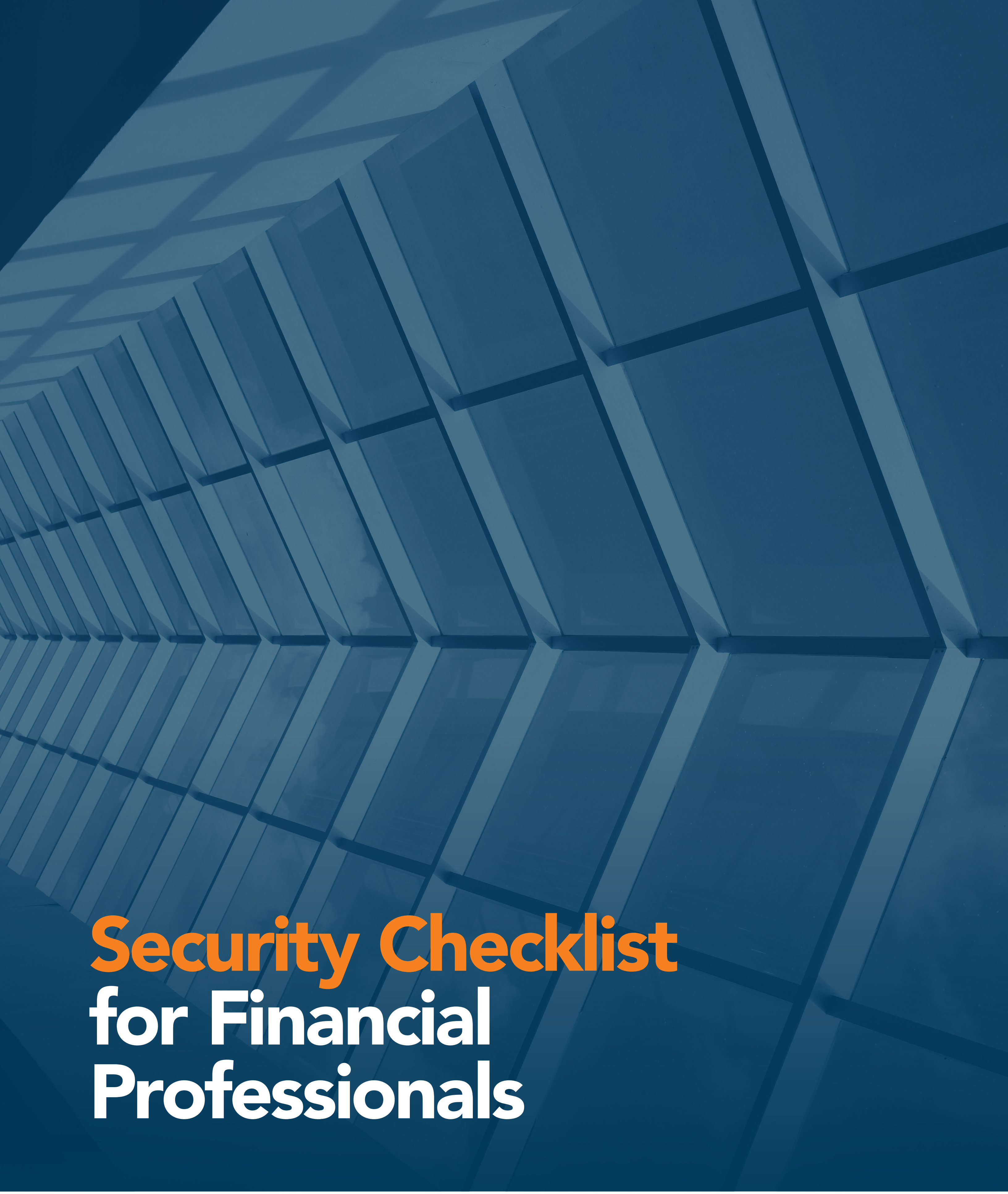

Security Checklist for Financial Professionals

ATRIA
Wealth Solutions

Cybersecurity preparedness is becoming a part of everyday life, both personally and professionally. It is critical to "get it right" in the current business and regulatory environment. FINRA, the SEC and other state-level regulatory agencies are prioritizing cybersecurity for audits, exams and compliance functions. This focus ensures that firms and financial professionals have adequate controls to secure client data protection.

We have created a cybersecurity preparedness self-assessment checklist to help you determine whether enhancements are necessary to increase your overall cybersecurity posture.

This document provides a high-level baseline risk assessment and checklist of items your office should perform.

We recognize that many offices are working with their own outsourced IT providers — therefore, we encourage you to work with your provider to complete this checklist.

Please do not hesitate to contact your broker-dealer if you require assistance or need help navigating this document.

Key areas to be reviewed:

- security of applications
- workstation
- mobile devices
- networks
- encryption
- vendors
- personally identifiable information (PII) handling
- remote access
- backups
- data retention
- training
- access controls
- incident responsiveness

Contents

Checklist for Financial Professionals and IT Service Providers

Question		Yes/No
1	Have you conducted a cybersecurity risk assessment? *(Best practice – at least annually or when adding/removing a product or service)*	
2	Does the office operate on supported operating systems, hardware and software?	
3	Does your office maintain system and software patches on a regular basis? (Hardware, software, operating system, etc.)	
4	Is antivirus/antimalware software installed and updated regularly on all computers in your office?	
5	Does your office maintain a Written Information Security Program (WISP)?	
6	Do computer screens lock automatically after a set amount of time? *(Max time – 15 minutes)*	
7	Passwords on any account used for business purposes meets industry standards for complexity and expiration *(Best practice – quarterly)*	
8	Does the office maintain a comprehensive list of all critical assets to include but not limited to computers, laptops, tablets, mobile devices, printers and copiers? *(Best practice – annually or when devices are added or removed)*	
9	All Personal Identifiable Information (PII) data needs to be stored with encryption. This includes PCs, laptops, hard drives, removable media, mobile devices, etc.	
10	All wireless networks that are utilized to conduct business must have WPA2 at a minimum enabled and all default passwords changed.	
11	Firewalls should be enabled on all PCs/laptops. In addition, a network-based firewall is recommended for office environments.	
12	Do you have a documented process for evaluating vendors' having access to PII prior to entering contractual obligations? This would include service providers, printers, cleaning crew, tech support, etc.	
13	All confidential email correspondence will need to be encrypted prior to sending.	
14	Is VPN utilized to secure remote connections to business systems?	
15	Is MFA enabled on all systems where it is available?	
16	Are computer files backed up and encrypted regularly? *(Best practice – daily, or at least weekly)*	
17	Are backups maintained in accordance with established books and records to meet regulatory and statutory requirements?	
18	Are copies of the encrypted backup data stored offsite? *(Best practice – safety deposit box or cloud storage)*	
19	Do you periodically remove/purge data no longer needed for legitimate business purposes?	
20	Does the office maintain a policy on how to securely dispose of both physical and logical assets? (Shredding, HD destruction, data destruction, etc.)	
21	Does the office have a security awareness program that is presented to the staff on at least an annual basis?	
22	Does your office maintain access control management? This would include granting least privileged access, termination procedures, annual access review of all systems and prohibiting shared accounts.	
23	Does your office maintain a Business Continuity Plan? How often is it updated and tested?	
24	Is there a process in place to promptly notify your firm of any cybersecurity-related events?	

Assessing Your Preparedness

1 **If you find that you or your IT service provider have answered "No" to one or more of the questions on the checklist, these are items that should be addressed.**

2 **Please work through your IT service provider to correct any deficiencies in your cybersecurity preparedness.**

3 **If your IT service provider is unable to resolve the items identified for further action, feel free to reach out to your broker-dealer for further guidance.**

Frequently Asked Questions

1. Where can I get help resolving any outstanding issue?

Work with your IT Service provider to ensure proper installation/configuration and to prevent an outage for your office.

2. How do we perform a risk assessment?

- Consider business critical functions
- Consider areas where critical/nonpublic information resides
- Consider the threats that could affect those areas
- Consider the likelihood and impact of the items above being impacted
- Review ways to reduce risk in this area
- Document how each area is protected and risk reduced to an acceptable, reasonable level

3. Does encryption slow down my system?

Using whole disk encryption to protect systems has very minimal impact on the overall performance of the system.

4. Do I have to encrypt all my external storage devices?

You should encrypt anything that contains personal client data or PII in general.

888.566.1482
atriawealth.com

ATRIA
Wealth Solutions

Atria Wealth Solutions Inc. ("Atria") is a modern wealth management solutions holding company and is not a Registered Investment Advisor (RIA) or broker-dealer entity. Investment products, services and advice are only provided through Atria broker-dealer and RIA subsidiaries.