FINGARDE
YOUR RIA TECHNOLOGY PARTNER

Short and Sweet Risk Assessment

This tool is designed to provide a general indication of your overall cybersecurity posture. It's important to keep in mind that simply completing the assessment based on your initial impressions or "feelings" about your IT environment may not provide an accurate result. To get the most accurate assessment, think through these questions from a compliance perspective – can you support your answers with concrete evidence (and if so, how quickly)? Honesty and a comprehensive evaluation of your current practices will offer valuable insights into areas where your firm may need to enhance its cybersecurity measures. Keep in mind that cybercriminals and the SEC will not be swayed by the results of this assessment; only a well-managed, secure, and compliant environment will make a difference.

Instructions: For each question, select the answer that best describes your firm's current cybersecurity practices. Add up the points to determine your total score on a scale of 10 to 50.

1) **When logging onto a website, which authentication method(s) do you use?**
    a) Username and password only (1 point)
    b) Additional security questions (2 points)
    c) Two-factor authentication (e.g., SMS Code) (4 points)
    d) Multi-factor authentication (e.g., Duo MFA, Hardware Security Token) (5 points)
2) **Do you have an email security solution in place to protect against phishing and spam?**
    a) No email security solution (1 point)
    b) Basic spam filtering (2 points)
    c) Advanced spam filtering and phishing protection (4 points)
    d) Comprehensive email security, including phishing protection, attachment scanning, and URL filtering (5 points)
3) **How do you manage the complexity and uniqueness of your passwords?**
    a) All my passwords are the same (1 point)
    b) Some of my passwords are unique (2 points)
    c) All passwords are unique and of moderate complexity (4 points)
    d) All passwords are unique, randomly generated to the maximum length possible, and stored securely in a password manager (5 points)

4) **How do you handle software updates and security patches?**
    a) Rarely or never (1 point)
    b) Only for critical updates (2 points)
    c) Regularly, but with some delay (4 points)
    d) Promptly and consistently (5 points)
5) **What type of network protection do you have in place?**
    a) No firewall or antivirus (1 point)
    b) Basic antivirus software only (2 points)
    c) Firewall and antivirus software (4 points)
    d) Advanced threat protection with firewall, antivirus, and intrusion detection/prevention (5 points)
6) **How often do you back up your data (including cloud/hosted data)?**
    a) No backups (1 point)
    b) Local backups only (2 points)
    c) Regular offsite backups (4 points)
    d) Regular offsite and local backups with redundancy (5 points)
7) **What kind of employee training do you provide on cybersecurity?**
    a) No training (1 point)
    b) Basic awareness training (2 points)
    c) Regular training on phishing and social engineering attacks (4 points)
    d) Comprehensive and ongoing training, including simulations (5 points)
8) **How robust is your cybersecurity policy?**
    a) No written policy (1 point)
    b) Basic policy covering general guidelines (2 points)
    c) Detailed policy with roles, responsibilities, and best practices (4 points)
    d) Comprehensive and regularly reviewed policy, with clear procedures for reporting and handling incidents (5 points)
9) **Do you have an incident response plan in place?**
    a) No plan (1 point)
    b) Informal plan with basic guidelines (2 points)
    c) Detailed plan with roles and responsibilities (4 points)
    d) Well-defined plan, regularly reviewed and tested (5 points)

10) How do you secure mobile devices and remote access?

a) No security measures in place (1 point)

b) Password protection and basic device security (2 points)

c) Encrypted connections and mobile device management (4 points)

d) Comprehensive protection, including VPN, encryption, and secure remote access policies (5 points)

Total Score: ___ / 50

Interpreting Your Score:

- 45-50: Excellent - Your firm is well-prepared to protect against cyber threats.
- 35-44: Good - Your firm has implemented some cybersecurity measures, but there is room for improvement.
- 25-34: Fair - Your firm has a basic level of cybersecurity, but significant gaps remain.
- Below 25: You should call FinGarde right now.

If you have questions about this assessment, or you would like to have a complete cyber security review, please reach out to our team: 740-334-4493.