Getting started with cybersecurity planning

It's not a matter of if, but when

Cybercriminals are tenacious and increasingly sophisticated. The risk to advisors and their clients is very real. In fact, 74% of advisors have experienced cyberattacks either directly or through one or more of their vendors. If you haven't yet developed an integrated cybersecurity plan, or aren't periodically assessing your plan's effectiveness, it's imperative that you get started as soon as possible. Knowing where to start can be daunting, but one good approach is to simply list the points where your firm could be vulnerable to attack. After you understand your potential exposures, it's time to address and resolve issues. We've summarized some of the top focus areas to consider as you begin thinking about your plan. These are part of Schwab's guided Cybersecurity Resource Program, which offers a broad portfolio of action-oriented resources to help you get organized and strengthen your firm's cybersecurity plan.

Know your vulnerabilities

Many of the biggest data breaches and cyberattacks result from the hacking of vendor platforms, fraudulent emails impersonating clients, and malware. In addition, human error is a critical factor in many incidents. As a result of the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) cybersecurity initiative, the commission has identified six focus areas of cyber risk for its next round of examinations. While not exhaustive, the questions below will help you gauge your level of cybersecurity.

Take action now

Get organized

Start by identifying sensitive firm and client information that needs protection and where it is stored. Use the "Take Inventory" Worksheet to track this critical information. Assess the current (and likely future) state of your firm's security plan, and prioritize any risks and gaps using the Schwab Cybersecurity Assessment and Action Plan Workbook.

Be proactive

Cybersecurity isn't a once-and-done initiative. Cybercriminals are constantly looking for new ways to steal information and assets. Your staff, vendors, and clients are your first and best defense against cyberattacks, so if you haven't incorporated their roles, education, and training in your cybersecurity plan, make it a priority. Go to the Employee and Client Education section of the Advisor Services Cybersecurity Resource Center to access tools to provide ongoing education to all your stakeholders.

Have a mitigation plan

No matter how effective your plan is, and no matter how carefully you maintain it, your firm is likely to experience a cyberattack. Regularly test your operations, technology, vendors, and staff to ensure your plan is keeping pace with evolving risks to data and your firm's reputation. Your cybersecurity plan should include options for mitigating risks and recovering from attacks, where and to whom to report incidents, and your responsibility for losses affecting clients. The Cybersecurity Reference Guide and the vast resources available in the Cybersecurity Resource Center can help you test for vulnerabilities.

Governance & Risk Assessment

- □ Is your comprehensive cybersecurity plan in place?
- □ Are your cybersecurity plan and processes customized for your business model?
- □ How often and by what means do you assess your cyber risks?
- □ Are your governing leaders informed and involved?

Access Rights and Controls

- □ How do you prevent unauthorized access to systems and information?
- □ How do your controls address remote access, logins, passwords, network segmentation, and tiered access for staff and clients?
- □ What is your process for establishing, changing, and terminating staff access rights?

Data Loss Prevention

- □ Are patch management and system configuration controls in place to address changing technology risks?
- □ How do you monitor the flow of content and attachments by vendors, clients, and staff?
- □ How do you verify the authenticity of client requests?

Vendor Management

- □ What cybersecurity plan and processes are in place by vendors?
- □ What does your firm require of each vendor in terms of periodic risk assessment, management, and performance measures?
- □ What contingency plan exists with vendors for conflicts of interest, bankruptcy, or changes that may compromise information security?

Training

- □ What training and validation of knowledge occurs for your staff regarding their cybersecurity role?
- □ What staff training and validation of knowledge do you require of your vendors?
- □ How often and by what means do you educate clients on ways to safeguard their information and assets against cybersecurity risks?

Incident Response

- □ What is your firm's operational contingency plan in the event of a cybersecurity incident?
- □ What is your firm's response and remediation plan when exposed to a cyberattack?
- □ Do you have cybersecurity insurance coverage?
- □ How and to whom will you report any incidents?

For details on the OCIE's cybersecurity focus areas, go to National Exam Program Risk Alert, Volume IV, Issue 8, September 15, 2015, OCIE's 2015 Cybersecurity Examination Initiative (https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf).

Schwab's Cybersecurity Resource Program

We're here to support you with the latest information, tools, and resources to help you build and strengthen your plan. Explore our self-guided tools and resources available through our Cybersecurity Resource Center. Whatever stage of the process you're in, visit our site to:

- Gain an understanding of the regulatory environment and fraud landscape
- Download critical tools to develop, strengthen, and maintain your cybersecurity program
- Access materials to educate your employees and clients on best practices for protecting against fraud and cyberattacks
- Sign up for events or read about the latest industry news

Best practices to protect client information and records

Passwords

□ Change passwords often, and store them only in a safe or safe deposit box—never online.

□ Make passwords *very* difficult to guess. Consider that social media provides a window into personal lives (location; college attended; the names of favorite people, places, and things), so passwords containing this information are easier to guess.

Security questions

□ As with passwords, make security questions very difficult to guess, or better yet, make the answers unrelated to the question. For example, if the question is, "What's your favorite color?" answer with "Paris."

Requests for funds transfer

□ Discuss with clients and staff the risk that fraudulent emails pose to clients' assets. Do not honor email requests for fund transfers, or insist that a direct conversation with the client also occur. Consider using a "safe" word known only to the advisor and the client to verbally confirm the client's identity.

Intended for institutional audiences. For informational purposes only. Neither Charles Schwab & Co., Inc. nor any of its affiliates or employees are responsible for any damages or other harm that might occur as a result of, or in spite of, use of any information, tools, resources, or processes described in these materials. Your firm alone is responsible for securing your systems and data, including compliance with all applicable laws, regulations, and regulatory guidance.

Schwab Advisor Services™ serves independent Registered Investment Advisors and includes the custody, trading, and support services of Schwab.

Independent investment advisors are not owned by, affiliated with, or supervised by Schwab.

charles
SCHWAB

Own your tomorrow®