charles SCHWAB

# Five steps to strengthen your cybersecurity program

Cybersecurity is top of mind for many advisors given the persistent threat of fraud and data security breaches, and the increased focus from regulators.

Our five-step methodology will guide you through the process of organizing, developing, and strengthening your firm's cybersecurity program. Use this checklist as a quick reference to get you started and visit our online Cybersecurity Resource Center to download additional tools and resources for enhancing your program.

## 1 Set the stage

Establish a strong foundation to enable your success in strengthening your firm's cybersecurity program.

## 2 Perform assessment

Perform an assessment to help identify gaps within your current security infrastructure that may need to be remediated to better protect against fraud and cybersecurity threats.

## 3 Create action plan

Assess security control gaps, and define and prioritize actions to remediate gaps. Assign execution owners and target completion dates. Identify and plan for potential risks and challenges.

## 4 Implement and document

Execute your action plan, making sure you inform stakeholders of any changes to existing policies and procedures resulting from your implementation. Document your progress and final outcomes (e.g., leadership communications, key decisions, training), and communicate these to your firm's leadership.

## 5 Establish ongoing maintenance

Keep your cybersecurity program relevant and effective with ongoing testing, monitoring, and auditing of your security controls. Maintain your asset inventory, and conduct periodic assessments, ongoing training, and monitoring of the regulatory environment and industry trends.

# 1 Set the stage

Establish a strong foundation to enable your success in strengthening your firm's cybersecurity program.

- ☐ Establish governance and roles
- ☐ Understand regulatory environment
- ☐ Align and communicate leadership expectations
- ☐ Take inventory of firm hardware, software, data, vendors, and third parties

# 2 Perform assessment

Perform an assessment to help identify gaps within your current security infrastructure that may need to be remediated to better protect against fraud and cybersecurity threats.

- ☐ Define your current state
- ☐ Define your target state
- ☐ Identify security control gaps

# 3 Create action plan

Assess security control gaps, and define and prioritize actions to remediate gaps. Assign execution owners and target completion dates. Identify and plan for potential risks and challenges.

- ☐ Assess gaps and define actions
- ☐ Prioritize actions to be implemented
- ☐ Assign execution owners and completion timeline(s)
- ☐ Identify and plan for potential risks and challenges

# 4 Implement and document

Execute your action plan, making sure you inform stakeholders of any changes to existing policies and procedures resulting from your implementation. Document your progress and final outcomes (e.g., leadership communications, key decisions, training), and communicate these to your firm's leadership.

- ☐ Execute your action plan
- ☐ Communicate with firm leadership
- ☐ Document, implement and communicate policies and procedures
- ☐ Conduct training

# 5 Establishing ongoing maintenance

Keep your cybersecurity program relevant and effective with ongoing testing, monitoring, and auditing of your security controls. Maintain your asset inventory, and conduct periodic assessments, ongoing training, and monitoring of the regulatory environment and industry trends.

- ☐ Test, monitor, and audit your program regularly
- ☐ Maintain your inventories and conduct periodic risk assessments
- ☐ Provide ongoing training and education to staff and clients
- ☐ Monitor regulatory environment and industry trends