SWK TECHNOLOGIES

CYBERSECURITY PREPAREDNESS CHECKLIST

Cybersecurity Evaluation: Cyber-threats have been on the rise with new and sophisticated attacks being launched every day. SWK has put together this comprehensive list of precautions walk you through considerations you NEED to address when evaluating your cybersecurity. In order to throughly assess your cybersecurity posture you should take the time to give thought into each answer. Use this checklist to determine if you have adequate cybersecurity protections in place for today's threats. If you have questions please feel free to reach out to us at any time.

Section 1 - Identify and Assess Risks to your Data:

As a financial service firm you will likely store, use or transmit personally identifiable information (PII) (PII includes social security numbers, DOBs, bank accounts, etc.) or sensitive internal files (financial records, client lists) electronically. In order to properly protect this data, you should ask yourself these questions:

Your Inventory of Data

☐ What client PII is being stored/used and where is it located?

☐ What sensitive data about the company is being stored and where is it located?

Minimize the Use of Data

Yes No

☐ ☐ Have you taken steps to minimize the electronic use and proliferation of PII or sensitive data?

☐ How and where is sensitive data being used?

Yes No

☐ ☐ Can you operate without this data being shared?

Yes No

☐ ☐ Where data must be shared, are there protective controls in place?

☐ What needs to be done to ensure this data is not externally exposed?

Yes No

☐ ☐ Are there internal permissions in place that decide who can access this data?

East Hanover, NJ
Phone: 877.979.5462
www.swktech.com | info@swktech.com

SWK TECHNOLOGIES

CYBERSECURITY PREPAREDNESS CHECKLIST

Section 2 - Protect your Data:

Have you deployed any tools and/or strategies for protecting data assets?

Protection of Information Assets

Yes ☐ No ☐ Have you deployed any tools and/or strategies for protecting data assets?

Do you have:

Yes ☐ No ☐ A Password policy in place?

Yes ☐ No ☐ Multi-Factor Authentication (MFA)?

Yes ☐ No ☐ A policy for regularly updating malware and anti-virus software?

Encryption Protections

Yes ☐ No ☐ Are your communications encrypted?

Yes ☐ No ☐ Is data encrypted when sent to external sources?

Yes ☐ No ☐ Is data encrypted when shared internally?

Yes ☐ No ☐ Is data encrypted when being backed up?

Staff Training and Protocols

Yes ☐ No ☐ Are your employees aware of your data security protocols?

Do you have the following policies/protocols in place?

Yes ☐ No ☐ Is data access to ex-employees, vendors, etc. terminated on departure?

Yes ☐ No ☐ Is access by employees and vendors being monitored?

Yes ☐ No ☐ Are accounts being shared by any employees?

Yes ☐ No ☐ Is there a cybersecurity training program in place?

Yes ☐ No ☐ If yes, is it conducted on regular intervals?

SWK TECHNOLOGIES

CYBERSECURITY PREPAREDNESS CHECKLIST

Key System Assets

Yes ☐ No ☐ Do you have assets that, if lost or made inoperable, would impact your firm's operations (e.g., trading or order management systems)?

☐ What assets do you have that would need to be protected?

☐ What protection measures are in place for these assets? (anti-virus, backups, passwords)

☐ How regularly are these measures updated?

Employee Device Use

Yes ☐ No ☐ Do your employees (or independent contractors) maintain devices that access PII or firm sensitive information?

Yes ☐ No ☐ Are permissions restricted and devices protected?

Yes ☐ No ☐ Do employees have access to PII or other sensitive data from personal devices?

Yes ☐ No ☐ Are their devices encrypted?

Yes ☐ No ☐ What level of risk do you associate with individuals and their access to information from personal devices?

Yes ☐ No ☐ Are protection levels set to gate data from certain employees?

East Hanover, NJ
Phone: 877.979.5462
www.swktech.com | info@swktech.com

SWK TECHNOLOGIES

CYBERSECURITY PREPAREDNESS CHECKLIST

Section 3 - Detect Potential Threats:

Penetration Testing

Yes ☐ No ☐ Have you had a third-party vulnerability/penetration test conducted in the past year?

Yes ☐ No ☐ If Yes, have you worked to improve upon the results of the last test?

Intrusion Detection

Yes ☐ No ☐ Do you have endpoint protection in place to monitor for possible intrusion attempts or breaches?

Section 4 - Incident Response Plan:

Response Plans

Yes ☐ No ☐ Do you have response plans in place for potential incidents? (Ex. Ransomware attack, natural disaster, data breach, etc.)

Section 5 - Business Continuity and Disaster Recovery:

Yes ☐ No ☐ If your systems, PII or firm sensitive information were made inoperable or stolen, would you need to recover them to conduct business?

Business Resilience

Yes ☐ No ☐ Do you have regularly scheduled backups?

☐ Where is this data stored and who handles it?

Yes ☐ No ☐ Do you have the ability to rebuild your systems if necessary?

☐ How fast can you restore your systems (including all critical data) and return online?

Yes ☐ No ☐ Do you have a backup in place that is completely separate from the main network?

Yes ☐ No ☐ If Yes, is it removed far enough to survive a local incident?

East Hanover, NJ
Phone: 877.979.5462
www.swktech.com | info@swktech.com

SWK TECHNOLOGIES

CYBERSECURITY PREPAREDNESS CHECKLIST

Conclusion:

If at any point you checked **NO** or were unsure - or unhappy - about your answer, you should contact SWK or your current network support provider (or both) to determine the steps to remedy the situation. Our Managed Cloud Services (MCS) practice has multiple solutions available ranging from data security and backup tools to background IT support and cybersecurity monitoring. We can help your existing IT resources successfully manage the ins and outs of your network on the day to day, or build a comprehensive cybersecurity and business continuity plan based around your current systems from the ground up.

A few of the solutions SWK Managed Cloud Services offers:

- Advanced Endpoint Protection & Enhanced Cybersecurity Monitoring
- Unified Security Information & Event Management (SIEM)
- User Security & Phishing Awareness Training
- Dark Web Monitoring
- Secure Encryption
- Network Vulnerability & Penetration Testing
- Co-managed IT Support & Services
- Secure Cloud Application Hosting

Don't hesitate to reach out to us ASAP to learn how you can better cybersecure your firm's data and strengthen your entire technology stack for FINRA compliance.

For questions or more information please contact:
SWK Managed Cloud Services
Phone: 877.979.5462
Email: info@swktech.com
SWK Technologies, Inc. | www.swktech.com