The International Investment Funds Association
L'Association internationale des fonds d'investissement

CYBERSECURITY PROGRAM BASICS

Establish a Framework – A cybersecurity framework is much like a set of blueprints. It helps identify the scope of information to be protected and provides standards, guidelines and best practices to manage cybersecurity related risk. There are several widely recognized and effective frameworks that set out a process for establishing effective controls through standard methodologies that are cost effective that promote the protection and resilience of systems. This does not mean, however, that a firm need only reference one framework. Taking the parts of different frameworks that are most appropriate for your firm can also be effective.

Additional Resources:

https://www.nist.gov/cyberframework

https://www.iso.org/isoiec-27001-information-security.html

http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

https://www.cisecurity.org/controls/

Conduct Security Awareness Training - Staff interact with clients, colleagues, third-party service providers and others and are the "human factor" that is so often exploited by attackers. One effective defense against those who want to exploit your staff is security awareness training. In order for this training to have maximum impact, it must be on-going, engaging, and tested at random intervals. Helping staff appreciate the areas that attackers may try to leverage (at work and in their personal lives) such as spam, phishing, social engineering, ransomware and other exploits will help reduce the success of such exploits.

Additional Resources:

https://resources.infosecinstitute.com/components-successful-security-awareness-program/#gref

https://www.sans.org/security-awareness-training

Have an Incident Response Plan – An incident response plan is a set of instructions to help staff detect, respond to, and recover from network security incidents. It provides for a course of action for all significant incidents (which must be defined by each firm). When a significant disruption occurs, your firm needs a thorough, detailed incident response plan to help staff stop, contain, and control the incident quickly. A threat to an organization, whether virtual or physical can be crippling, and an incident response plan can help mitigate and prepare for a range of events. The incident response plan should be tested and updated regularly.

Additional Resources:

https://www.ibm.com/downloads/cas/PY31LRX2

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Incident-Management-and-Response.aspx

Conduct Table Top Exercises - A well-thought-out incident response plan that sits on a shelf and does not get exercised or updated is not fulfilling its purpose. Incident response plans need to be tested so gaps are identified, changes made, and mitigation strategies improved. Likewise, staff members need to get comfortable with their roles and responsibilities during a serious cyber incident. Like many endeavors, what is required is practice.

Assuming you've already identified the correct participants, when conducting a cybersecurity table top exercise, you want to first set a goal regarding the scope of the scenario you will simulate—for example, a distributed denial-of-service attack—and detail how complicated you want the exercise to be. You also should establish separate goals for what you want the test to accomplish—for example, how well existing policies and procedures are designed to respond to a threat, and whether contact information is up to date. As your firm walks through the scenario, the exercise will provide an opportunity to validate this and other information. It is important that someone document the exercise's findings, so any gaps in procedures can be addressed as appropriate.

Additional Resources:

https://www.cisecurity.org/white-papers/six-tabletop-exercises-prepare-cybersecurity-team/

https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

Establish and Monitor Normal Network Activity – Normal network activity is about employees as much as networks. Establishing a baseline for normal network and employee behavior is prudent. Make certain that employees only have access to the parts of the network they need to fulfill their roles, know which IP addresses can (or usually) talk to your network, and know what peak and off-peak traffic loads look like. Understanding and monitoring normal network activity will help you identify anomalies that should be investigated.

Additional Resources:

https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/monitoring

Participate in Trusted Information Sharing – The cybersecurity threat we all face is a "neighborhood risk." In other words, we are all in this together and likewise we are all stronger together. Forming networks or communities of peers is a good starting point for staff with cybersecurity responsibilities to connect with others confronting the same risks. Informal networks, such as sharing non-competitive information about vulnerabilities and threats is a good way for staff from different firms to build trust. Information exchange works best when there is a trust component between participants.

Additional Resources:

https://www.fsisac.com/

https://en.wikipedia.org/wiki/Computer_emergency_response_team