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

ADDITIONAL CYBERSECURITY PROGRAM BASICS

Business Continuity Planning – Largely a separate area of concentration from information security, its critical role and overlap with cybersecurity preparedness is highlighted during the 2020 global pandemic. Typically, planning focused on relatively short-term disruptions to operations with strategy to minimize impact to the enterprise and its clients. During 2020 the focus changed most notably to large scale (global) disruption, long-term remote work, and returning employees to offices safely. The events of 2020 will permanently change firm's business continuity planning.

Additional Resources:

https://www.continuitycentral.com/

https://www.thebci.org/

https://continuityinsights.com/

Information Technology Controls – Typically, a subset of an enterprise's internal controls but specific activities performed by persons or systems designed to ensure that business objectives are met. As hundreds of thousands of employees around the globe were asked to work remotely, IT controls had to be closely monitored as the threat landscape expanded dramatically. Specifically, the above change brought increased threats and risks that changed control requirements.

Additional Resources:

https://www.isaca.org/resources/cobit

https://www.coso.org/Pages/default.aspx

Inventory and Control of Software & Hardware – Shadow IT, where technology, both hardware and applications is set up within a business without approval or knowledge that may introduce new risks (e.g. security, data loss, etc.), inefficiencies, and compatibility concerns. In addition, inappropriate or illegitimate access to systems and data can, at a minimum, impact the integrity of data as well as compliance with regulations such as GDPR.

Additional Resources:

https://www.cisecurity.org/

https://www.asd.gov.au/

https://www.csoonline.com/article/3083775/shadow-it-mitigating-security-risks.html

Principle of Least Privilege – Every process, user or program should access only the information and resources necessary for its legitimate use. Segmentation of the network based on data classification stored on servers as well as locating critical or sensitive data separately. This should also incorporate a Data Loss Prevention program that covers people, process, and systems that monitors and protects data in use, motion, and rest.

Additional Resources:

https://www.cisecurity.org/

https://nvd.nist.gov/800-53/Rev4/control/AC-6

https://www.sans.org/webcasts/design-privilege-architecture-aws-112925

Work From Home Considerations – At some point during the 2020 global pandemic most of us were asked to work from home. While for business continuity purposes this has proved effective there are some security concerns as the 'home office' is an unknown environment. Some suggestions to help manage security considerations include making certain a corporate device is used for business purposes, connect to the enterprise via a virtual private network, secure your home Wi-Fi, update your router's firmware, or replace the router (if necessary), and implement two factor authentication among others.

Additional Resources:

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/working-from-home-here-s-what-you-need-for-a-secure-setup

Computerworld

https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home

Secure Configuration – Typically, when an individual or enterprise acquires a device it is configured for ease of use rather than security. The device will arrive with default configurations, out of date or unneeded software, enabled/open services, etc. Securely configuring the device is a process as software decays and configurations are changed so the process must be continuously managed. Omitting this step will permit attackers to exploit services and software.

Additional Resources:

https://www.cisecurity.org/

https://www.itgovernance.co.uk/secure-configuration

https://www.nist.gov/news-events/news/2019/10/guide-security-focused-configuration-management-information-systems-nist