KEY AREAS OF RISK FOR THE FINANCIAL SERVICES INDUSTRY

CohnReznick
ADVISORY • ASSURANCE • TAX

As business operations continue to shift to a "work from anywhere" model, financial services organizations should be aware of these four key areas of cybersecurity and privacy risks and take steps to remain vigilant, secure, and better prepared for what's next.

	Scams & information overload	Compromised data	Regulatory compliance issues	Data privacy
RISKS	• There has been an increase in phishing/social-engineering scams such as impersonating legitimate companies or organizations with the objective of obtaining credentials and/or installing malware (e.g., spyware) on the remote worker's machine. • The 24/7 stream of information (and frequent misinformation) is highly distracting, creating a chaotic environment in which workers may be less vigilant about cybersecurity and the source of information, which could lead to misinformed investment decisions.	• Increased use of remote storage and transfer of data with mobile and home desktops increases the risk of client data leakage. • Accelerated migration to cloud and virtual desktop environments may mean policies and procedures were not set up properly. • Trade strategies and positions or client data may be compromised via spying through improperly secured remote conferencing software. • Traders' being geographically dispersed can result in time synchronization discrepancies across servers and workstations, which can interfere with sequencing. • Added complexity with record-keeping/client communications can pose risks. • High-value data and large cash movements make funds an attractive target for cybercriminals.	• Regulatory risks associated with unfamiliarity with new mandates specific to remote work issued by the FTC, SEC, and Federal Reserve for financial services companies. • Non-compliance with existing regulations including the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and NYDFS Cybersecurity Regulation, which are still being enforced. • Gathering protected health information (PHI), such as employee health data, without adhering to Health Information Privacy and Portability Act (HIPPA) requirements.	• Many organizations' processes, policies, and cultures were not designed to support a remote workforce, which introduces a raft of new risks to systems, data, and privacy. • New technologies that gather health, productivity, and preference data of employees, visitors, and customers create new endpoint vulnerabilities and could potentially jeopardize sensitive personal information. • Use of third-party vendors to gather data increases the potential for data leakage of sensitive personal information.
CYBER AND PRIVACY ACTIONS	• Whitelist and flag external emails, and inform employees about an expected increase in phishing attempts and ask them not to click on unknown suspicious links. • Ensure that all mobile devices that are used to access email and corporate networks, including personal devices, are secured with passwords and anti-malware applications. • Use anti-spam/anti-phishing tools and methods, including behavioral analytics to detect suspicious activities.	• Require VPN or other virtual desktop technologies when accessing sensitive information. • Manage security in the cloud and virtual environments. • Train employees on best practices for accessing and uploading/downloading sensitive information from/to personal laptops or devices. • Review trading software and ensure that trades are timestamped centrally to the extent possible. • For any files on personal devices, check the company's policy related to file storage and backup. • Evaluate collaboration tool privacy and security policies related to access, storage, and sharing of data at your organization, your investors, and critical third-party vendors.	• Ensure that your legal team has reviewed the legal and liability implications of remote work. • Review and prioritize your compliance program commitments to align with current deadlines. • Review and update your current cybersecurity policies and procedures to align with remote workplace safeguards. • Perform an analysis of your current cybersecurity resources (in-house and outsourced) to align with your current workplace environment.	• Ensure that your organization's IT/cybersecurity risk profile reflects the strategy, goals, and objectives for the organization's short-, mid-, and long-term plans. • Ensure that privacy policies communicate, in plain English, what personal data is being collected, stored, and shared for what specific purposes. • Perform a security and resiliency due diligence on critical third-party vendors and offshore resources in the supply chain.