Cyber Considerations for Investment Advisors

Cyber liability presents significant challenges for businesses in every industry and market around the globe. Investment advisors and asset managers face notable exposure risks in this area specifically. Failure to comply with regulatory standards can result in fines and penalties, while data breach response and forensics can prove costly and time-consuming. This includes security evaluations, identifying and correcting compromised data, informing affected businesses and individuals, reassessing infrastructure, and more. Let's examine the risks involved, potential mitigation, and coverages to keep you operating when problems occur.

Here are some important statistics to consider from the past few years:

- Businesses in the financial industry experience approximately 5 times more phishing attacks than those in other industries
- Over 100,000 Americans above the age of 60 were victims of digital fraud, resulting in an average loss of more than $30,000 (more than $3b total)
- The FBI's Internet Crime Complaint Center received nearly 900,000 complaints, with potential losses exceeding $12 billion
- Phishing attacks have increased more than 4,000% since the launch of ChatGPT in 2022
- Over 40% of data affected by ransomware attacks is unrecoverable
- The average cost of data breaches in 2024 was $4.9m, and over $6m on average for breaches in the financial sector

© Windermere Insurance | All rights reserved | Confidential and Proprietary

Collective annual costs emanating from cybercrime are projected to exceed $20 **trillion** by 2027. The impact of cyber-attacks is massive, and the threat is pervasive and ever-growing. The financial industry has shifted into almost exclusively digital platforms, enshrining data security as a matter of foremost concern and relevance. With the rise of remote work, cloud storage, and online transactions, the threat landscape has become even more complex, and efforts to increase security and reduce risk must be proactive rather than reactive.

As the statistics have made apparent, cyber liability insurance should provide coverage for network and device breaches, funds sent to incorrect/fraudulent recipients, and other related issues. All major custodians now require some form of cybercrime coverage, but this can vary dramatically between policies and carriers. Ensuring that your organization possesses proper cyber security and liability protection is essential, as is helping clients to achieve the same level of preparedness.

Maintaining a robust compliance program often requires dedicated staff, external consultants, and technology solutions, all of which come with significant costs. These investments can prove invaluable, but they are never a guarantee. Cyber insurance plays a critical role in protecting investment advisors and their clients against the litany of threats and issues that can still arise – from critical breaches to human error and beyond.

Cyber security and cyber insurance are essential not only for protecting employees and clients, but also for averting regulatory compliance issues, loss of reputation and trust, and even critical financial failure. Understanding your risk profile, your mitigation strategies, and your cyber coverages can reduce the likelihood of breaches and other related issues while controlling costs during and after critical security events. Inspire confidence in your clients and prospects while deterring hostile agents by arming yourself with knowledge, technology, and allies.

© Windmere Insurance | All rights reserved | Confidential and Proprietary