JACKO LAW GROUP, PC

Risk Mitigation Tip
Cybersecurity: Attacks, Risk Mitigation, and Regulatory Compliance

June 27, 2024, by Kathryn Konzen

In an increasingly digital world, where financial transactions and sensitive information are often stored and transmitted electronically, investment advisers face a growing threat from cyber-attacks. These attacks can range from data breaches and phishing scams to ransomware and insider threats, posing significant risks to both the advisers themselves and their clients.

2023 saw a concerning increase in cyber-attacks. Statista.Com reported 3,203 data compromises in 2023, which put the data of over 352 million individuals at risk, compared to 1802 data incidents in 2022.

In addition, about 744 companies in the financial sector experienced a cyberattack making it the second most affected sector in the US. Globally, the Manufacturing sector was the hardest hit last year, and accounted for about 25% of the total cyber-attacks. The Financial sector was a close second, accounting for 18% of attacks.

In the United States, the Healthcare industry remains one of the most targeted since the COVID-19 Pandemic followed, again, by the Finance sector. Both globally and in the US, cybercriminals continue to target the financial sector, including advisory firms and banking institutions. According to an article by the International Monetary Fund (IMF), the industry suffered from over 20,000 cyber-attacks over the last 20-years, losing approximately $12 billion.

The question remains:

Why is the Financial Sector such a target for cyber criminals?
The financial sector is a hot bed of sensitive personal and financial data. As an economic epicenter, money flows through banking institutions, insurance companies, investment advisory firms and others along with the associated data sought after by cyber criminals. There is an assumption that only large financial institutions are at risk. This is false. According to a report by Accenture, cyber-attacks on smaller businesses continue to rise.

Interestingly, Private Equity firms are also highly appealing to cyber criminals. A report by Accenture titled, "Private Equity: The Rising Cost of Cyber-attacks," offer that cyber criminals target Private Equity firms because they have a wealth of personal and financial data, access to capital and are considered High Cyber Risk takers because most PE firms are focused most on growth and speed, often relegating cyber security as a non-priority.

However, even more important, is the question,

Why is the Financial Sector so vulnerable to cyber-attacks?

JACKO LAW GROUP, PC

Cyber-attacks have become more sophisticated and harder to detect for longer. Not only have cyber criminals become more advanced in their methods but also in their strategies.

Third Party Vendors

In the financial industry, there is a heavy reliance on third-party service providers such as IT security vendors. Oftentimes, these vendors serve several firms in the industry exposing many companies to attack from one vulnerable spot – the vendor.

For example, in February 2024, a data breach exposed personal and financial data of over 57,000 Bank of America customers. However, the breach did not come through Bank of America, it came through third-party vendor, "Infosys McCamish", a software provider for the finance industry. In December 2023, sixty credit unions experienced outages as a result of a Ransomware that infiltrated the network system of cloud computing provider, "Ongoing Operation." With heavier reliance on third-party service providers, and/or failure to perform thorough due diligence on the service providers, the risk of cyber-attacks remains a constant threat.

Lack of Adequate Cyber Security Measures

Cyber preparedness and internal data protections is concerningly lackluster for many businesses in the finance sector. In July 2023, the new SEC Cybersecurity rules went into effect. The amended rules were in response to a widespread lack of cyber preparedness by investment advisers and others in the field and were implemented to protect investors and promote cyber diligence and transparency.

The new cyber security rules were primarily implemented for Public Companies, but, there has been a slew of SEC enforcement actions against smaller private companies for failure to meet cyber compliance requirements.

However, with proper risk mitigation strategies and compliance measures in place, investment advisers can better protect themselves and their clients from cyber threats, and meet compliance requirements.

Understanding the Risks

Cyber-attacks on investment advisers can have severe consequences, including financial losses, reputational damage, and regulatory penalties. Here are some common types of cyber threats that investment advisers may encounter:

1. **Data Breaches:** Unauthorized access to sensitive client information, such as personal and financial data, can lead to identity theft and financial fraud.
2. **Phishing Scams:** Cyber criminals may use deceptive emails or messages to trick employees into disclosing sensitive information or downloading malware.
3. **Ransomware:** Malicious software that encrypts data and demands a ransom for its release can disrupt operations and cause financial losses.

4. **Insider Threats:** Employees or contractors with access to sensitive information may intentionally or unintentionally misuse or disclose it.

Risk Mitigation Strategies

To mitigate the risk of cyber-attacks, investment advisers should implement robust cybersecurity measures tailored to their specific needs and risk profile. Here are some key strategies to consider:

1. **Risk Assessment:** Conduct regular risk assessments to identify potential vulnerabilities and prioritize cybersecurity investments and actions.
2. **Employee Training:** Provide comprehensive training to employees on cybersecurity best practices, including how to recognize and respond to phishing attempts and other security threats.
3. **Access Controls:** Implement strong authentication mechanisms, such as multi-factor authentication, to control access to sensitive data and systems.
4. **Data Encryption:** Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.
5. **Patch Management:** Keep software and systems up to date with the latest security patches and updates to address known vulnerabilities.
6. **Incident Response Plan:** Develop and regularly test an incident response plan to ensure a timely and effective response to cyber security incidents.
7. **Vendor Management:** Assess the cybersecurity practices of third-party vendors and service providers to ensure they meet appropriate security standards.

Compliance Requirements

Investment advisers are subject to various regulatory requirements related to cybersecurity and data protection. Compliance with these requirements is essential for protecting client assets and maintaining trust in the financial markets. Here are some key compliance considerations:

1. **SEC Regulations:** The U.S. Securities and Exchange Commission (SEC) provides guidance and requirements for cybersecurity risk management, including the Safeguard Rule and Regulation S-P (Privacy of Consumer Financial Information).
2. **GDPR Compliance:** Investment advisers that operate in the European Union or handle the personal data of EU residents must comply with the General Data Protection Regulation (GDPR), which sets strict requirements for the protection of personal data.
3. **Cybersecurity Examinations:** The SEC conducts examinations of registered investment advisers to assess their cybersecurity preparedness and compliance with relevant regulations.

4. **Reporting Requirements:** Investment advisers may be required to report cybersecurity incidents to regulatory authorities and affected clients in accordance with applicable laws and regulations.

Conclusion

Cyber-attacks pose significant risks to investment advisers, but with proactive risk mitigation strategies and compliance measures, they can better protect themselves and their clients from cyber threats. By staying vigilant, investing in cybersecurity measures, and adhering to regulatory requirements, investment advisers can enhance their resilience to cyber-attacks and safeguard the integrity of the financial markets.

Author: *Kathryn Konzen, Esq. is the Director of Operations and Counsel, at Jacko Law Group, PC ("JLG). With over 15 years of experience in the legal profession, she brings a diverse range of expertise in areas such as operations, eDiscovery consulting, business development, recruiting, and more. Her practice focuses on working closely with clients, assisting them with their Cybersecurity and AI legal needs.*

JLG works extensively with investment advisers, broker-dealers, investment companies, private equity and hedge funds, banks and corporate clients on securities and corporate counsel matters. For more information, please visit https://www.jackolg.com/.

[1] Service of process refers to the delivery of the legal documents that gives a defendant notice of the legal action filed against it and the opportunity to respond. Valid service of process on a defendant is required by the U.S. Constitution. Service of process must be accomplished by the plaintiff pursuant to the rules or statutes of the appropriate jurisdiction. These rules include how process documents can be delivered (such as in-hand delivery or certified or registered mail) and to whom that delivery can be made.