grc outlook

Cybersecurity: Regulatory Compliance, Attacks, Risk Mitigation

CYBER SECURITY GRCINSIGHTS

In an increasingly digital world, cyber scams, particularly in the financial industry, are on the rise. 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.

For example, the financial sector was hit hard with cyberattacks last year with breach costs averaging $5.9 million.[1] The result is long-term brand damage as well as loss of consumer trust in financial institutions. This leads to consumer anxiety regarding the potential harm of personal data exposure, which increases the risk of identity theft and financial fraud.

Why is the Financial Sector such a target for cyber criminals?

As a hub for economic activity, the financial sector remains a prime target for cybercriminals seeking valuable personal data. One example is Private Equity firms. They are highly attractive to cybercriminals because they are high risk, high reward. A report by Accenture[2] on the topic offers that the primary components of such firms that make them especially appealing to criminals because of Private Equity Firms':

- Emphasis on rapid growth
- Access to a vast amount of capital
- Volume of stored personal and financial data
- Ranking of cybersecurity as a lower priority compared to other initiatives

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 exposing the personal and financial data of over 57,000 Bank of America customers was announced.[3] 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. With heavier reliance on third-party service providers, and/or failure to perform thorough due diligence on the service providers, the risk of cyberattacks remains a constant threat.

Lack of Adequate Cybersecurity 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[4] went into effect. The amended rules were in response to a widespread concern cyber preparedness by financial institutions (including investment advisers and others in the field) and were implemented to protect investors and promote cyber diligence and transparency.

Moreover, on May 16, 2024, the SEC adopted certain amendments to Regulation S-P ("Reg S-P"), which includes significant requirements to protect the non-public information of customers.[5] The amendments include requiring covered institutions to develop, implement and maintain policies and procedures for a response program to detect, respond to, and recover from unauthorized access to, or use of, customer information including customer notification procedures. The amended Reg S-P is a substantial expansion of the protections available to customers under the federal securities laws and establishes federal minimum standards for data breach notifications from institutional securities market participants.

Understanding the Risks

Cyberattacks on the financial sector can have severe consequences, including financial losses, reputational damage, and regulatory penalties. In addition to common cyber threats, many in the industry now face threats that come with the use of emerging technology. For example, Artificial Intelligence ("AI") offers a wide range of benefits but presents new and sophisticated risks such as data poisoning, which is when a nefarious character manipulates the training data used to train AI, or model extraction, which is when cybercriminals recreate AI models by learning how it responds to queries.

Risk Mitigation Strategies

To mitigate the risk of cyberattacks, all firms, and particularly those in the financial space, should prioritize cybersecurity, and take adequate measures tailored to their specific needs and risk profile. Some important strategies to consider:

1. **Risk Assessment:** Conduct regular risk assessments to identify potential vulnerabilities and explore how to address those vulnerabilities.
2. **Employee Training:** Conduct ongoing and comprehensive training to employees and other key members of the business 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 cybersecurity incidents.
7. **Vendor Management:** Assess the cybersecurity practices of third-party vendors and service providers to ensure they meet appropriate security standards.

Additional Financial Industry Compliance Requirements

Many of those who are in the financial industry 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 Non-public Information).
2. **GDPR Compliance:** Those firms that operate in the European Union (EU) and the United Kingdom (UK) or handle the personal data of EU and UK 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 its registrants (including registered investment advisers, broker-dealers and investment companies) to assess their cybersecurity preparedness and compliance with relevant regulations.
4. **Reporting Requirements:** Firms may be required to report cybersecurity incidents to regulatory authorities and law enforcement and notify affected clients in accordance with applicable laws and regulations.

Conclusion

Cyberattacks pose significant risks; however, with proactive risk mitigation strategies and compliance measures, firms can better protect themselves and their clients from cyber threats. By staying vigilant, investing in cybersecurity measures, and adhering to regulatory requirements, firms can enhance their resilience to cyberattacks and safeguard the integrity of the marketplace.

[1] Cost of a Data Breach in 2024 for the Financial Industry," Security Intelligence, Accessed October 10, 2024. https://securityintelligence.com/articles/cost-of-a-data-breach-2024-financial-industry/.

[2] Accenture. *Private Equity and the Rising Cost of Cyberattacks.* Accessed October 10, 2024. https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Private-Equity-And-Rising-Cost-Of-Cyberattacks.pdf.

[3] Ranjan, Ananya. "Data Breach Affects Bank of America Customers," Forbes, October 10, 2023. Accessed October 09,2024. https://www.forbes.com/advisor/personal-finance/data-breach-affects-bank-of-america-customers/.

[4] U.S. Securities and Exchange Commission. "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," Press Release 2023-139, October 2, 2023. Accessed October 09, 2024. https://www.sec.gov/newsroom/press-releases/2023-139.

[5] U.S. Securities and Exchange Commission. "SEC Adopts Rule Amendments to Regulation S-P to Enhance Protection of Customer Information." Press Release 2024-58, May 16, 2024. Accessed October 09,2024. https://www.sec.gov/newsroom/press-releases/2024-58.