JACKO LAW GROUP, PC

Legal Risk Management Tip
November 2023

How to Effectively Manage Your Cybersecurity Program

In the fast-paced and technology-driven landscape of the financial industry, managing cybersecurity risks is paramount. To ensure your organization's legal compliance, and to safeguard sensitive data, it's essential to maintain a robust incident response plan that is not only up to date but also routinely tested. In the financial industry, a reactive approach to cybersecurity is insufficient. To effectively manage legal risks associated with cyber threats, it is important to prioritize a proactive cybersecurity strategy.

Financial institutions should regularly conduct comprehensive cybersecurity audits and assessments to identify vulnerabilities and ensure compliance with relevant regulations. This proactive approach can help prevent legal repercussions while safeguarding sensitive financial data.

Regulatory bodies, such as the SEC, FINRA, and states require financial institutions to have comprehensive incident response plans in place. Failing to do so can result in significant fines and legal repercussions.

To effectively manage legal risks associated with cyber threats, we recommend implementing ongoing cybersecurity practices that encompass the following key areas:

Have a Dynamic Regulatory Compliance Program. Stay informed about industry-specific regulations and compliance requirements, such as General Data Protection Regulation ("GDPR"), state and federal privacy laws and cybersecurity regulations that apply to your business. Develop and implement robust cybersecurity policies that adhere to these regulatory requirements and take steps to ensure that required books and records related to your cybersecurity program are maintained.

Perform a Cyber Risk Assessment. Regularly evaluate the cybersecurity risks associated with your operations, products, and services. This assessment should include an analysis of potential threats, vulnerabilities, and the impact of a breach. Work closely with your IT provider and CISO, taking into consideration recent regulatory guidance on best practices.

Evaluate Third-Party Vendors' Cybersecurity Practices. Financial institutions often rely on third-party vendors for various services. Assess the cybersecurity measures of these vendors, ensuring they meet your institution's standards and regulatory requirements.

Develop a Robust Incident Response Plan. Develop and maintain a robust incident response plan that outlines the steps to be taken in case of a cybersecurity breach. Ensure that your legal

team is well-versed in the plan, as they will play a crucial role in managing critical aspects during and after a cyber breach.

Conduct Employee Cybersecurity Training Frequently and as Needed. Train your employees on cybersecurity best practices and policies. Employees are often the first line of defense against cyber threats, so their knowledge is vital in preventing breaches.

Spend Time to Educate Clients About Cybersecurity. Take time to educate clients about prudent cybersecurity practices, which includes only using secure links to upload personally identifiable information. Provide instructions not to directly email personal identifiers, such as driver's license numbers, social security numbers and account numbers. Also, explain the importance of why and how you will verify the customer's requests for wires and withdrawals, such as through verbal identification and use of a password.

Implement Data Encryption and Access Controls. Implement encryption for sensitive data and establish strict user access controls. Limit access to only those who require it and regularly review and update these controls.

Conduct Penetration and Vulnerability Testing Regularly. Conduct penetration testing to identify weaknesses in your cybersecurity measures, including where a hacker could gain access and expose your institution to cyber risks. In addition, vulnerability simulation tests and exercises should be conducted periodically to identify weaknesses in the IT environment so that such risks can be addressed.

Obtain Cybersecurity Insurance. Consider investing in cybersecurity insurance to mitigate potential financial losses resulting from a data breach. Review the policy carefully to ensure it adequately covers your institution's needs. Be aware of when and how to tender your cyber claim. Document Your Cybersecurity Activities. Keep comprehensive records of your cybersecurity activities, including audits, assessments, employee training, and incident response actions. These records can serve as valuable evidence in the event of a legal dispute or regulatory investigation. Engage Knowledgeable Legal Counsel. When developing and reviewing your cyber program, and in the event of a cyber breach, engage experienced legal counsel who understands cybersecurity and financial regulations. They can provide invaluable guidance in navigating the complex legal landscape and minimizing legal risks.

By implementing a comprehensive regulatory compliance monitoring system for cybersecurity, organizations can proactively manage cyber risks, protect sensitive data, and demonstrate to clients, regulators and the industry their commitment to maintaining cybersecurity protections. This approach will both help protect against potential cyber liabilities and also enhance trust among clients, regulators, and stakeholders – which is good for business.

Jacko Law Group offers regulatory and compliance legal counsel for companies and individuals in the securities and financial industries and works with them to ensure their cybersecurity compliance efforts meet regulatory requirements.

For more information on how JLG can assist with your cybersecurity efforts, please contact us at (619) 298-2880.

Author: Amanda Sobel, Paralegal and Michelle L. Jacko, Managing Partner, Jacko Law Group, PC ("JLG"). 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/.