NEON VINIMAY PVT. LTD.
Regd. Office : 510, Kamalalaya Centre, 156-A Lenin Sarani, Kolkata - 700 013
Phone : (033) 4062-7201 to 7213, CIN : U51109WB1993PTC057361
E.mail : backoffice@neonvinimay.com, neonvinimay04@gmail.com

Process To Identify Cyber Threats And Risk

Procedure for identifying cyber risks, threats, and vulnerabilities, assessing their likelihood and impact on stock broking business, and deploying appropriate controls based on criticality:

1. **Establishing a Cyber Risk Assessment Team:**
    - Assigning a dedicated team consisting of IT professionals, security experts, and relevant stakeholders from different departments to conduct the assessment.
    - Ensuring the team has a clear understanding of the stockbroking business processes, systems, and technologies involved.
2. **Identifying Assets and Critical Processes:**
    - Identifying and listing all critical assets, such as customer data, financial systems, trading platforms, communication networks, and intellectual property.
    - Identifying the key processes dependent on these assets for smooth business operations.
3. **Identifying Threats and Vulnerabilities:**
    - Conducting a comprehensive analysis to identify potential cyber threats specific to the stockbroking industry, such as unauthorized access, data breaches, phishing attacks, ransom ware, and insider threats.
    - Identifying vulnerabilities within the IT infrastructure, software applications, hardware devices, network architecture, and human factors.
4. **Assessing Likelihood and Impact:**
    - Evaluating the likelihood of each identified threat occurring, considering historical data, industry trends, and expert opinions.
    - Assessing the potential impact of each threat on your stockbroking business, including financial loss, reputational damage, regulatory non-compliance, and operational disruptions.
5. **Prioritizing Risks:**
    - Prioritizing risks based on their likelihood and impact scores to identify high-priority risks that require immediate attention.
    - Considering the criticality of the assets and processes affected by each risk to determine the level of priority.
6. **Developing Controls:**

Regd. Office : 510, Kamalalaya Centre, 156-A Lenin Sarani, Kolkata - 700 013
Phone : (033) 4062-7201 to 7213, CIN : U51109WB1993PTC057361
E.mail : backoffice@neonvinimay.com, neonvinimay04@gmail.com

- Identifying and developing appropriate controls and countermeasures to mitigate the identified risks.
- Implementing a defence-in-depth strategy, including technical controls (firewalls, antivirus software, intrusion detection systems), policies and procedures, employee training and awareness programs, and incident response plans.

7. Review and Test Controls:

- Regularly reviewing and updating the effectiveness of implemented controls.
- Conducting vulnerability assessments, penetration testing, and security audits to identify any weaknesses and ensure that controls are functioning as intended.

8. Monitor and Respond:

- Implementing a robust monitoring system to detect and respond to potential cyber threats in real-time.
- Establishing an incident response team and an incident response plan to effectively manage and mitigate cyber incidents.

9. Regular Review and Improvement:

- Conducting periodic reviews of the entire cyber risk assessment process to identify areas for improvement.
- Staying updated on emerging threats, vulnerabilities, and industry best practices to enhance your cyber risk management strategy.

10. Documentation and Communication:

- Documenting all cyber risk assessment activities, findings, and control measures implemented.
- Communicating the cyber risk assessment results and control measures to relevant stakeholders, including senior management, employees, and clients.

For NEON VINIMAY PVT. LTD.

DIRECTOR