Cybersecurity Policy

CIO Wealth Management, Inc. takes a comprehensive approach in maintaining the security of client information and its technology infrastructure which includes a cybersecurity framework. This framework incorporates a process that attempts to prevent, detect, identify, respond to, and recover from cyber-based attacks. As a result, we focus on the following five key areas to improve its cybersecurity preparedness.

1) **Cyber Risk Management & Oversight**

   Strong governance is an essential piece in the management and oversight of cyber risks. Establish robust policies and risk management strategies. Commit sufficient resources including expertise and training. Establish an enterprise-wide approach to manage cyber risks with a strong cybersecurity culture as its foundation.

2) **Threat Intelligence & Collaboration**

   Monitor threat information and intelligence to discover threats and identify the various attack methods being utilized. Leverage known intelligence sources, in order to develop preventative and responsive strategies. Share crucial threat information and intelligence with partners and stakeholders to strengthen your security posture.

3) **Cybersecurity Controls**

   Incorporate physical, logical, and other cybersecurity controls to prevent, detect, and mitigate cyber-attacks. Implement preventative controls to minimize the impact and likelihood of successful attacks, detective controls to identify attacks in early stages, and corrective controls to mitigate the impact.

4) **External Dependency Management**

   Identify critical external dependencies. Establish rigorous vendor management controls, including ongoing due diligence and monitoring. Define third parties' responsibilities and associated service level metrics. Evaluate vendors' incident response and resilience.

5) **Incident Management & Resilience**

   Mitigation and Recovery are a Must Prepare for potential cyber-attacks by establishing incident management procedures in order to speed your ability to respond and recover from a cyber incident. Mitigate the loss of customer confidence through timely and appropriate customer notification. Develop policies and implement adequate incident response programs. Define capabilities and required resources to address threats and recovery. Use monitoring tools to capture events, and to identify anomalous behaviors and attacks. Escalate and report cyber incidents to the institution's board of directors and senior management when warranted.

Responding to an Incident

Take appropriate steps to respond to a cyber incident:

- Assess the nature and scope of an incident and identify what information systems and types of information have been accessed or misused.
- Promptly notify your primary regulator when you become aware of an incident involving unauthorized access to or use of sensitive customer information, and generally, following any incident that could materially impact your institution.
- Comply with applicable suspicious activity reporting regulations and guidance. Ensure appropriate law enforcement authorities are notified in a timely manner.
- Take appropriate steps to contain and control the incident to prevent further unauthorized access to or misuse of information.

- Notify customers as soon as possible when it is determined that misuse of sensitive customer information has occurred or is reasonably possible.

Purpose

Rapidly evolving cybersecurity risks have reinforced the need for all institutions and their critical technology service providers to have appropriate methods for monitoring, sharing, and responding to threat and vulnerability information. This information is critical to safeguarding customer and other sensitive information and information technology systems. Participating in information-sharing forums is an important element of an institution's risk management processes and its ability to identify, respond to, and mitigate cybersecurity threats and incidents.

Background

Recent cyber-attacks and widely reported pervasive vulnerabilities highlight the rapidly changing cyber risk landscape. Financial institutions participating in information-sharing forums have improved their ability to identify attack tactics and successfully mitigate cyber-attacks on their systems. Additionally, these institutions have gained deeper insight into specific vulnerabilities and collected methods for identifying vulnerabilities on their systems and enhancing controls.

Risk

Financial institutions face a variety of risks from cyber-attacks including operational risks, fraud losses, liquidity, and capital risks. A financial institution's lack of information regarding cybersecurity threats poses undue risk to itself and other financial institutions.

Risk Mitigation

Our management team monitors and maintains sufficient awareness of cybersecurity threats and vulnerability information so we may evaluate risk and respond accordingly. Financial institution management also should establish procedures to evaluate and apply the various types and quantity of cyber threat and vulnerability information, in an effort to mitigate future threats and disruptions.

If you have any questions about our Cybersecurity Policy or its contents please contact:
Andrew R. Sullivan, President & CCO, at (978) 287-1405 or by email: andrew@ciowm.com