BERMUDA MONETARY AUTHORITY

Insurance Sector Operational Cyber Risk Management Code of Conduct

gnosis
knowledge is power

WHY CYBER SECURITY MATTERS

Cyber security is the practice of protecting your computers, laptops, servers, smartphones, other electronic devices, network, software, and system data from any malicious attacks and cyber threats.

The confidentiality, integrity and availability of information is crucial to the daily operation and continuity of any business and cyber risks can cause significant financial losses and/or reputational damage for companies and their stakeholders / clients.

NEW CYBER SECURITY REGULATIONS

The Operational Cyber Risk Management Code of Conduct (Cyber Code of Conduct) took effect as of 1st January 2021 and was developed to provide cyber security resilience within the local insurance industry in Bermuda. Overseen by the Office of the Privacy Commissioner and the Bermuda Monetary Authority (BMA), the Cyber Code of Conduct applies to all Bermuda registered Insurers, Insurance Managers, and Intermediaries (Agents, Brokers, Insurance Market Place Providers).

As a leading Bermudian IT consultancy, Gnosis is highly experienced in safeguarding businesses and their clients from cyber crime and ensuring compliance with the latest cyber security regulations.

This document seeks to outline the Cyber Code of Conduct and illustrate the new mandatory and recommended cyber security requirements for Bermudian businesses.

THE CYBER CODE OF CONDUCT STANDARDS

The new Cyber Code of Conduct consists of 3 Lines Of Defense (3LOD):

1. Identification of assets and risks
2. Detect and protect controls; and
3. Response and recovery controls

Outlined below each element and the minimum required standard.

SECTION I: IDENTIFICATION OF ASSETS AND RISKS

Management Responsibility:

- Board of Directors & management must have oversight of risks
- Create an asset inventory listing
- Appoint a CISO (Chief Information Security Officer) or outsource the role
- Consider a cyber insurance policy and review coverage at least annually
- Identify and understand cyber risk posture
- Measure the potential impact and consequences of risk
- Monitor & report – maintain a risk register
- Compliance and audit:
- Control environment should be continuously monitored and evaluated

SECTION II: DETECT AND PROTECT CONTROLS

IT Service Management, IT Incident Management & Security Incident Management:

- Establish a IT Operations program to manage:
- System/Service Optimization
- Configuration Changes
- Operational Risk
- Implement an incident manage process
- Establish a formal IT security incident response process
- Access Management for employees, third parties & customers
- Threat intelligence and vulnerability alerting services
- Control requirements:
- Data loss preventions (DLP)
- Data protection and governance
- Staff awareness and training
- 'Bring your own' device services must be subject to risk assessment
- Data backup management
- Penetration testing & vulnerability assessments
- Patch management
- Network security management
- Logging & monitoring

SECTION III: RESPONSE AND RECOVERY CONTROLS

Business Continuity Planning (BCP) & Disaster Recovery (DR):

- Implement effective BCP and DR policies
- Plans must be tested on at least an annual basis
- Tests must be documented, and any issues identified tracked for remediation

Notification of Cyber Reporting events to the BMA:

Cyber Reporting events resulting in significant adverse impact to a regulated entity's operations / policy holders / clients must be reported to the BMA within 72 hours from the time that there is a determination of confirmation of the event.

ASSESSING YOUR COMPLIANCE

The Code of Conduct is not a "one size fits all" approach for companies. The BMA developed the Code of Conduct as a flexible reference point and encourages companies to align their cyber risk profile to the nature, scale and complexity of the business.

Gnosis recommends that organizations undertake evaluative processes to assess their individual cyber security risks and conformance with BMA requirements, taking into account other new regulations such as GDPR and PIPA, and the potential for new and evolving cyber threats to develop over time.

HOW CAN GNOSIS HELP?

Gnosis' team of cyber security experts will work with your company to:

- Identify and assess cyber security risks and current conformance with the Code
- Develop a cyber security document tailored to your organization, in line with BMA requirements
- Develop document response and recovery processes
- Oversee design, implementation and monitoring (audit) of controls
- Provide ongoing support to maintain and grow a cyber security program

NEXT STEPS

To find out more about what the new Cyber Code of Conduct means for your business, and for help assessing and managing your cybersecurity program(s), contact Gnosis today:

COREY BRUNTON
Chief Operating Officer
+1 441 799 9898
corey.brunton@gnosis.bm

JON ARORA
Principal Cyber Security Consultant
+1 441 405 9900
jon.arora@gnosis.bm

gnosis
knowledge is power