CIMA Thematic Cybersecurity Review – key points for regulated entities

Insights - 12/07/2023

Good practices and areas of concern were identified within the key elements of the Cayman Islands Monetary Authority's Thematic Cybersecurity Review, issued at the end of June 2023. We recommend that all regulated entities (excluding funds) read the report and table it for consideration by their respective boards or governing bodies.

Background

The Cayman Islands Monetary Authority (**CIMA**), commenced cyber risk regulation in May 2020 when it issued a binding Rule and related Statement of Guidance on Cybersecurity for Regulated Entities in May 2020 for adoption by regulated entities across all sectors.

The Rule and Statement of Guidance set out the regulatory requirements and minimum expectations for managing cyber risks, to ensure that robust cybersecurity measures are in place to appropriately identify, protect, detect, respond to, and recover from cyber-related threats, incidents and breaches. The Rule was necessary to address cyber risk which had been identified as the key emerging threat for business and society.

Of course the Covid-19 pandemic necessitated and increased remote working environments using technology, thereby increasing cybersecurity exposures and risks. CIMA responded commendably to issue the Rule almost immediately after the pandemic resulted in global lock downs, including a complete and strict lock down in the Cayman Islands.

CIMA subsequently commenced supervision conducting a cybersecurity thematic review and the resultant report was issued at the end of June 2023. The thematic review involved 12 regulated entities from the banking, insurance and securities sectors.

The findings

Good practices and areas of concerns identified include cybersecurity framework, risk management and IT systems controls and use of internet.

Some areas are useful to highlight and provide comment on and proposed solutions:

- Employee Selection, Training and Awareness: One can see positive compliance rates among regulated firms regarding IT/cyber (assuming that the 12 firms sampled are representative of all). Cayman has aligned itself with more advanced jurisdictions and is showing maturity by proactively self-assessing progress of a very delicate and complex area of compliance.

- While we understand the insurance market to be hard in relation to cyber risk insurance, there are confident statements in the 'Summary of Overall Best Practices' which include "Adequate cyber risk insurance coverage". Of late we have seen insurers being extremely scrutinising over cyber controls to the point that being able to obtain insurance coverage may be taken as a positive assessment of those controls.

- The report suggested that we have advanced beyond the adoption stages of Cybersecurity best practices, with the 2020 guidance that was provided earlier having been for the most part adopted. Most of these are investment related, infrastructure building to NIST/ISO standards and implementing new training and IT solutions. While there are areas for improvement, with risk assessment and management a common theme, the indications are that the groundwork has mostly been done and that long-term processes now need to worked on.

- The most challenging and complex aspect to address is the relationship between the entities and outsourced providers. Most Cayman-based firms use some form of outsourcing whether it's at the cyber level, email or hosting. Since Microsoft 365 and AZURE products touch most of the regulated firms in Cayman and it is possible that many companies do not have any relationship documentation or, if they do, it does not align to the internal standards with the outsourced firms. Firms need to execute appropriate outsourcing agreements. The problem with all specialist support, including compliance, is that firms seek to rely on the specialist by outsourcing functions to it, yet it is the entities' responsibility to ensure standards within the company ICT environment and ensure outsourced environments are similar or rationalised if different.

How can Ogier help?

Ogier Regulatory Consulting can assist, be it by audits, GAP analysis, solutions advice and road mapping or continual review of:

- governance oversight of cybersecurity, including its management framework and reporting structures

- cybersecurity strategies to promote and enhance cyber resilience
- adequacy of the cybersecurity risk management policies and procedure
- effectiveness of internal controls
- internal and external audits and assessments, including vulnerability assessments and/or penetration tests and other audits performed on cybersecurity
- adequacy of incidence management and response plans and processes
- employee selection and resourcing of key IT and cyber related personnel
- adequacy of cybersecurity training and awareness programs
- compliance with relevant Data Protection Act and regulatory requirements
- outsourced cybersecurity and IT related functions
- the overall effectiveness of the cybersecurity framework

For further information, please feel free to contact the authors of this article.

About Ogier

Ogier is a professional services firm with the knowledge and expertise to handle the most demanding and complex transactions and provide expert, efficient and cost-effective services to all our clients. We regularly win awards for the quality of our client service, our work and our people.

Disclaimer

Meet the Author

Gavin Baxendale

Client Director

Cayman Islands

E: gavin.baxendale@ogier.com

T: +1 345 815 1915

Key Contacts

Georgia Scott

Head of Ogier Regulatory Consulting

Cayman Islands

E: georgia.scott@ogier.com

T: +1 345 815 1885

Lisa Bowyer

Client Director

London

E: lisa.bowyer@ogier.com

T: +44 203 830 8584

Related Services

Ogier Regulatory Consulting

Regulatory