

The background of the cover is a close-up, slightly blurred photograph of a laptop keyboard. A silver metal padlock is attached to the keyboard, and its shackle is open and hanging upwards. The lighting is dramatic, with strong highlights and deep shadows, creating a sense of security and digital protection.

THEMATIC

CYBERSECURITY REVIEW REPORT

ISSUED JUNE 2023

CONTENTS

Introduction

Scope and Synopsis of Thematic Review

Key Findings from the Thematic Cybersecurity Review

Cybersecurity Risk Management

Cybersecurity Corporate Governance

Cybersecurity Awareness, Training and Resources

Outsourcing

Concluding Remarks

INTRODUCTION

In today's world, cybersecurity and cyber resilience are key components of every financial institution and the loss of access to data or, potentially worse, the public disclosure of confidential or proprietary data can cause significant financial losses and reputational impact on financial institutions and their clients. Today's financial institutions are under constant threat by hackers using sophisticated methods to break into their information technology ("IT") and communications systems. Traditional cyber defences often rely on signatures of known viruses and exploits, but these methods are quickly losing effectiveness as financial institutions face ever-changing zero-day exploits.

Effective IT and cyber controls therefore demand that institutions not only take steps to protect against today's modern threats, but also put in place sufficient monitoring systems to detect a breach as quickly as it happens. Recognising that not all attacks can be prevented, institutions must also have well thought-out and documented incident response plans to stop, contain, and recover from breaches. As a result, institutions security personnel must continually enhance their technical knowledge and internal processes to ensure they remain vigilant and aware of the current and emerging threat landscape.

Given the dynamic nature of IT and Cybersecurity, and the associated threats posed to regulated entities, the Cayman Islands Monetary Authority (the "Authority"), in efforts to implement cyber risk regulation and supervision, issued a Rule and related Statement of Guidance on Cybersecurity for Regulated Entities in May 2020 for adoption by regulated entities across all financial 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.

In the wake of the Covid-19 pandemic, many financial institutions adopted remote working environments which were technologically intensive, thereby elevating already existing exposures and risks related to cybersecurity.

It is against this backdrop that the Authority conducted the cybersecurity thematic review (the "Thematic Review") of twelve (12) regulated entities (the "Selected Entities") spanning the Banking, Insurance and Securities sectors between April to December 2022. This resulting Thematic Review Report (the "Report") provides insight on identified good practices and areas of concerns within the key elements of the review as follows:

- Cybersecurity Framework
- Risk Management
- IT Systems Controls and Use of Internet
- Employee Selection, Training and Awareness
- Outsourcing and Intra-Group Arrangements
- Data Protection
- Accountability
- Notification Requirements

Summary of Overall Best Practices

Best practices were observed in the following areas:

- Consideration and alignment of cybersecurity frameworks with reputable international standards and frameworks such as the National Institute of Standards and Technology (“NIST”) and the International Organisation for Standardisation (“ISO”).
- Well-established control frameworks for managing IT systems including suitable governance and reporting structures with appropriate segregation of duties.
- Detailed Board approved cybersecurity strategies, policies and procedures.
- Adequate cyber risk insurance coverage.
- Well-documented notification protocols and incident response plans for cyber and data loss events and breach incidents, including containment and recovery measures for managing cyber-attacks, breaches or incidents.
- Implementation of appropriate cybersecurity training programmes for governance, staff, IT and cybersecurity personnel.

Summary of Overall Areas for Improvement

Weaknesses were observed in the following areas:

- Inadequate self-assessments performed on cybersecurity frameworks, including those reliant on Group frameworks to ensure that such frameworks are adequately implemented at Group Level and address local entity risks and Cayman Islands regulatory requirements.
- Inadequate cybersecurity risk management strategies which should include key components for risk identification, assessment, protection, monitoring and reporting and evaluation systems along with incident response, containment and recovery policies and procedures.
- Inadequate performance of comprehensive risk assessments and established risk appetite, tolerance levels and/or risk limits which should be approved by the governing body and maintained in an inventory of cybersecurity risks (“risk registers”) and applicable controls.
- Inadequate maintenance of risk registers which should contain identification and criticality classification of information system, current and emerging threats, risks, and vulnerabilities along with applicable controls.
- Inadequate implementation of appropriate cybersecurity training programmes for governance, staff, IT and cybersecurity personnel. The governing body training should ensure that governance is equipped with the requisite knowledge to competently exercise their oversight function and appraise the adequacy and effectiveness of the regulated entities overall cyber resilience programme. Formalised training plans

should be in place for IT and cybersecurity personnel including technical training on IT systems and current and emerging cybersecurity and security principles to ensure that they are knowledgeable and aptly trained for their specific IT or cybersecurity roles and functions. Enterprise-wide on-going training should be provided to new and existing staff on cybersecurity to ensure increased awareness and enterprise-wide efforts to prevent or minimise cyber-attacks and cyber incidents, and employees should be trained to understand, at a minimum, the cyber risks to which the entity is exposed and the mitigating measures employed to reduce the occurrences of cyber incidents.

Inadequate dissemination of cybersecurity information and/ or other actions aimed at increasing clients' level of cybersecurity awareness.

- Where cybersecurity functions are outsourced (whether intra-group or to third parties), entities are to assess and gain a level of assurance that the frameworks implemented by the service providers are adequate and fit for purpose.
- Implement technology refresh plans to ensure adequate systems are in-place and software is kept up-to-date.

SCOPE & SYNOPSIS OF THE THEMATIC CYBERSECURITY REVIEW

The objectives of the Thematic Review were to assess the Selected Entities policies, procedures, governance and oversight mechanisms and internal control systems in relation to cybersecurity in order to ascertain compliance with the Monetary Authority Act (2020 Revision) (the "MAA"), the Bank and Trust Companies Act (2021 Revision) ("the "BTCA"), the Insurance Act (2010) (the "IA"), the Securities Investment Business Act (2020 Revision) (the "SIBA"), the Rule on Cybersecurity for Regulated Entities (the "Rule - Cybersecurity"), the Statement of Guidance on Cybersecurity for Regulated Entities (the "SOG - Cybersecurity") as well as other applicable legislations and accepted standards of best practice. Analysis of these areas allowed the Authority to gain a better understanding of the Selected Entities cybersecurity framework.

In order to achieve the stated objectives, the Thematic Review focused specifically on an assessment of:

- Governance oversight of cybersecurity, including its management framework and reporting structures;
- Cybersecurity strategies in place to promote and enhance cyber resilience;
- Adequacy of the cybersecurity risk management policies and procedures;
- Effectiveness of internal controls;
- Adequacy of the 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;
- Management's actions to remedy vulnerabilities;
- 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;
- Reliance on Group cybersecurity frameworks; and
- The overall effectiveness of the cybersecurity framework, supporting internal controls and oversight processes implemented by regulated entities.

This Report highlights the general themes observed across the Selected Entities including the good practices and areas of concern observed. Through bilateral communication, the Authority has outlined to each participating Selected Entity the deficiencies identified as well as the requirements in order to enhance the Selected Entity's cybersecurity framework.

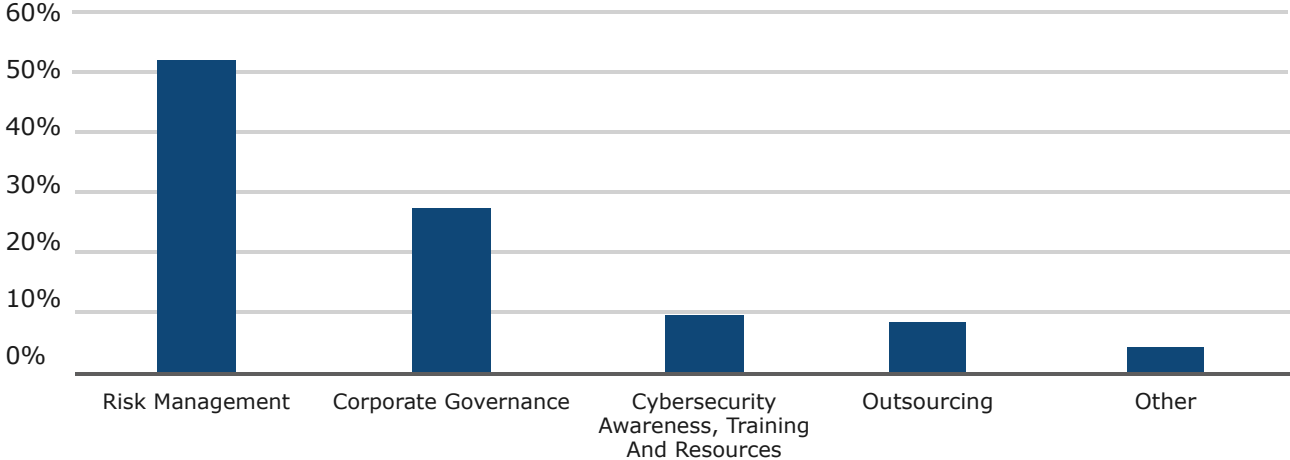
KEY FINDINGS FROM THE THEMATIC CYBERSECURITY REVIEW

The Thematic Review highlighted good practices and revealed weaknesses in the following areas:

- Risk Identification, Assessment, Mitigation and Monitoring, including incidence management and data protection;
- Governance and Oversight;
- Cybersecurity Awareness, Training and Resources; and
- Outsourced IT and Cybersecurity functions.

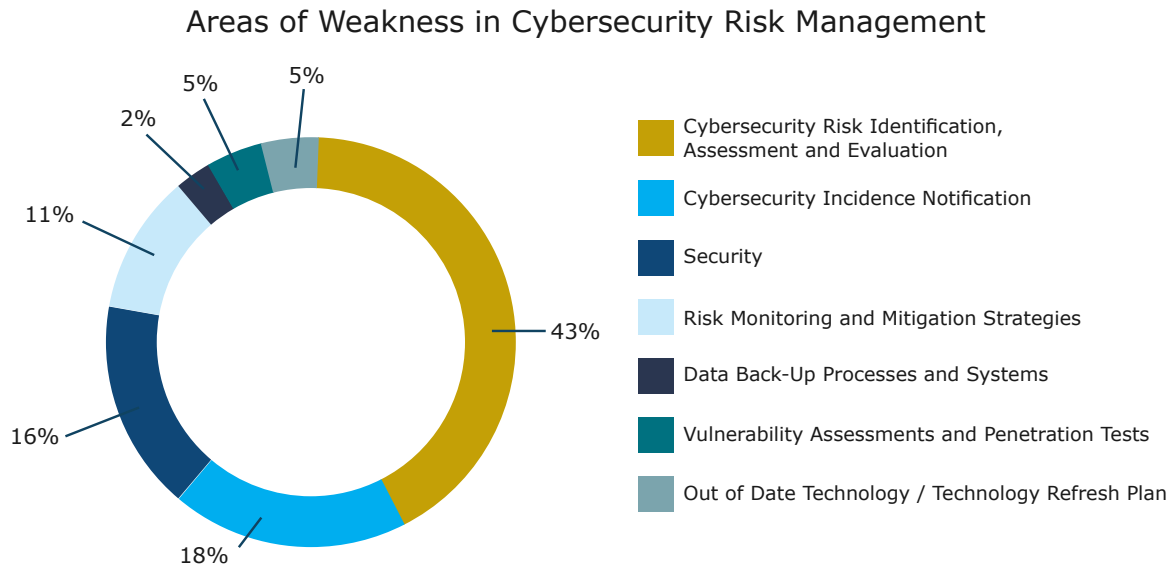
The below graph illustrates the distribution of weaknesses across the above-mentioned themes highlighted by the review:

Distribution of Cybersecurity Weaknesses



Notably, two key areas account for seventy-nine (79%) of the findings across the review: cybersecurity risk management and corporate governance. In addition, seventeen (17%) of the findings emanated from training and awareness and in intra-group and third-party outsourcing for entities with such arrangements in place. The Authority reiterates that good practices were also observed in these areas across some of the Selected Entities as included in summary tables throughout this report.

Cybersecurity Risk Management



Cybersecurity Risk Identification, Assessment, and Evaluation

From the chart above, forty three percent forty-three percent (43%) of the weaknesses in cybersecurity risk management arose mainly due to lack of formal risk assessments and/or business impact assessments being conducted, as well as lack of documented cybersecurity risk mitigation and control strategies, discussed in more detail below.

Analysis revealed that several Selected Entities inspected had not formulated and documented a risk appetite statement/tolerance limit and established a cybersecurity risk register or inventory of cybersecurity risks.

Further analysis revealed that some Selected Entities had not conducted a formal risk assessment in relation to cybersecurity risks, including but not limited to, the identification and assessment of current and emerging threats, risks and vulnerabilities as well as an analysis and evaluation of the probability, potential impact and the consequences of identified risks on the overall business and operations in the occurrence of an adverse event.

Additionally, the Authority noted that several Selected Entities had not identified their key information systems and the criticality of each to their operations. It was further noted that entities had not conducted a risk or business impact assessment to identify the potential

impact and consequences of identified risk exposures and considered appropriate safeguards to ensure critical products and services are available, as well as the Selected Entities ability to prevent, mitigate or contain the impact of a potential cybersecurity event.

The Authority noted that some of Selected Entities did not have documented cybersecurity risk mitigation and control strategies in place that align with their business strategy, value of information assets, risk tolerance and client interests.

The Authority expects all regulated entities to maintain well established cybersecurity risk management frameworks, including risk appetite statements, risk registers and applicable controls and components for identifying current and emerging threats, risks, and vulnerabilities as well as the impact and likely impact to its IT environment.

Additionally, the Authority expects all regulated entities to have clear policies which detail the level of protection required based on the risk and criticality rating of the information systems, and consider appropriate safeguards to ensure critical products and services are available as well as the regulated entity's ability to prevent, mitigate, or contain the impact of a potential cybersecurity event. Regulated entities should conduct comprehensive risk or business impact assessments as support for determining the level of protection required.

To ensure robust risk monitoring and reporting systems are maintained, regulated entities should conduct periodic reviews and updates of their cybersecurity risk management processes, re-evaluating past risk-control methods with improved testing as well as assessing the adequacy and effectiveness of their cybersecurity risk management processes.

Summary of Good Practices

- Well documented cyber risk registers including inherent risks, the controls in place to mitigate such risks and residual risks after controls are applied.
- Formalised and Board approved cybersecurity risk appetite.

Summary of Areas for Improvement

- Need for entities to set out their cybersecurity risk appetites, tolerance levels or risk limits.
- Identification and classification of information systems and the maintenance of an inventory of cyber risks and applicable controls through risk registers.
- Analysis and evaluation of the probability of and potential impact and consequences of the identified cybersecurity risk exposures.
- Need for entities to assess their risk mitigants/controls and residual cybersecurity risks after controls are applied to determine whether inherent cybersecurity risks are managed within defined cybersecurity risk appetites through implementation of adequate mitigants/controls.
- Need to document remediation plans for deficient risk mitigants/controls.

Cybersecurity Incident Notification

It was noted during the review, that the policies and procedures of several Selected Entities did not adequately address the notification requirements to the Authority in instances of Cybersecurity breaches. Per Section 7 of the Rule - Cybersecurity, regulated entities should define incident criticality in their incident management framework. When in doubt about the level of seriousness of an event, regulated entities should consult the Authority.

The Authority wishes to remind all Regulated Entities of their responsibilities to immediately notify the Authority, in writing, of an incident when it is deemed to have a material impact or has the potential to become a material incident, no later than 72 hours following the discovery of said incident. Section 8 of the Rule – Cybersecurity (April 2023 release) further outlines notification requirements, including reportable incidents that fall under one or more of the following:

- Material impact to the regulated entity’s internal operations.
- The event results in the unauthorised dissemination of any personal data either internally or externally.
- Significant operational impact to internal users that is material to customers or business operations.
- Extended disruptions to critical business systems or internal operations.
- Number of external customers impacted is significant or growing.
- If determined that there is potential reputational impact, either to the entity or the Cayman Islands, notification to the Authority must occur immediately if there is any risk of premature public disclosure.
- Any loss of any card payment information, beneficial owner details, or any personally identifiable information.
- Loss or exposure of any data in violation of any applicable data protection laws and other regulatory requirements both foreign and domestic.

Summary of Good Practices

- Well documented incidence management and response policies and procedures and business continuity/disaster recovery plans.
- Incidence management and response teams.

Summary of Areas for Improvement

- Need for entities to ensure that group policies include policies and procedures which address local risks and requirements.

Data Protection and Security

A number of Selected Entities had not implemented multi-factor authentication (MFA) for access to their cloud systems and virtual private networks (VPN). Further, several Selected Entities had not implemented adequate encryption on all endpoint devices (i.e., laptops, desktop computers, smart phones, etc.) to address the risks of data theft, data loss and data leakage from endpoint devices. In one instance this was in direct contradiction to a Selected Entity's internal policy related to encryption.

The Authority expects that all regulated entities have suitable logical access controls and encryption on end-point devices and storage media to prevent unapproved access to computer systems and unauthorised removal of information from devices and storage media.

Summary of Good Practices

- Multi-factor authentication enabled for access to all cloud or virtual networks.
- End-to-end encryption used for all data communication.

Summary of Areas for Improvement

- Need for entities to establish acceptable encryption protocols to ensure the safety of sensitive and confidential information stored on and accessed by end user devices.
- Need for entities to properly evaluate security requirements associated with their internet systems and adopt encryption algorithms, which are of well-established international standards and subjected to rigorous scrutiny.
- Need for entities to establish suitable controls to ensure that transactions performed over the internet as well as online login credentials, passwords, personal identification numbers and other sensitive personal or account information are adequately protected, authenticated and secured against exploits such as account takeovers, card cloning, hacking, phishing and malware.

Risk Monitoring, Reporting and Mitigation Strategies

It was noted that some Selected Entities did not have suitable Intrusion Detection Software in place to enable continuous monitoring for threats. In instances where these systems were in place, the Authority noted one instance where the regulated entity was unable to evidence remediation of vulnerabilities identified.

Regulated entities should ensure that their monitoring systems adequately performs continuous monitoring with a focus on highlighting key flags rather than relying on heavily manual processes in the monitoring and surveillance process that would prevent a regulated entity from identifying attacks or breaches in a timely manner and appropriately identifying current and emerging risks.

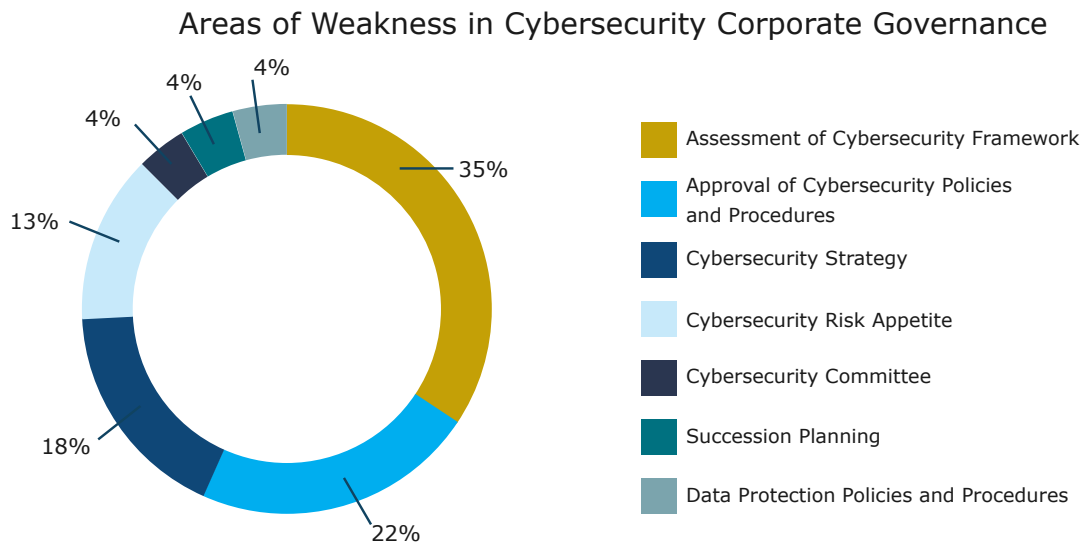
Summary of Good Practices

- Use of intrusion and detection systems to safeguard the entities' networks and emails.
- Establishment of thresholds for threat monitoring.
- Dedicated internal and external teams charged with monitoring, analysing, escalating and reporting on threats above the threshold.

Summary of Areas for Improvement

- Need for entities to enhance their risk management and reporting mechanisms by implementing monitoring/surveillance and detection policies, techniques and systems that allow for real time and ongoing monitoring and detection of cybersecurity threats.

Cybersecurity Corporate Governance



Assessment of Cybersecurity Framework

It was observed that several Selected Entities had not performed a gap analysis of its cybersecurity framework against the Authority's Rule and SOG – Cybersecurity to ensure that their framework complies with applicable acts, regulations and relevant regulatory measures of the Cayman Islands.

The Authority expects that, as part of its cybersecurity risk management efforts, all regulated entities conduct regular self-assessments of their cybersecurity frameworks (including frameworks implemented by group entities and outsourced entities) against the Authority's Rule and Statement of Guidance – Cybersecurity to ensure that the frameworks comply with applicable acts, regulations and relevant regulatory measures of the Cayman Islands.

Summary of Good Practices

- Consideration and alignment of cybersecurity frameworks with reputable international standards and frameworks such as the NIST and the ISO frameworks.
- Cybersecurity frameworks commensurate with risks, size, nature and operating complexities of businesses.
- Three lines of defence model in management of cyber risks which includes involvement of the risk management and internal audit functions.

Summary of Areas for Improvement

- Entities who rely on group frameworks should receive written confirmation on the adequacy of the frameworks being managed at the Group level.
- The need to conduct regular self-assessments of cybersecurity frameworks against local requirements to ensure compliance.

Approval of Cybersecurity Policies and Procedures

Several Selected Entities' governing body and senior management had not reviewed and approved their cybersecurity frameworks, including but not limited to, policies and procedures relating to risk assessments, change management, data protection, and other pertinent components of the framework such as training and awareness programs and technology refresh plans.

Part of the duties and responsibilities of a regulated entities governing body and senior management entails periodic review and approval of their cybersecurity frameworks, including appropriate programmes, policies and procedures for cybersecurity, cyber resilience and IT management. In addition, the governing body and senior management are expected to ensure that effective internal controls and cybersecurity risk management practices are implemented to achieve ongoing security, reliability, resiliency and recoverability. Such internal controls and risk management practices should be implemented to ensure that regulated entities adequately identify, assess, mitigate, control, monitor and report on cyber risks that they are exposed to.

Summary of Good Practices

- Detailed cybersecurity policies, standards, and procedures.
- Policies, standards and procedures commensurate with risks, size, nature and operating complexities of entities.

Summary of Areas for Improvement

- Board approval of cybersecurity policies and procedures and internal controls.
- Need to provide a clear distinction between information security and cybersecurity.

Cybersecurity Strategy

A number of Selected Entities had not established and documented cybersecurity strategies which are aligned with their overall business strategies. In addition, it was observed that regulated entities with cybersecurity strategies in place had not ensured that such strategies are adequately updated, reviewed and approved by their governing bodies.

Regulated entities' governing bodies are ultimately responsible for cybersecurity and their duties must include the formulation and documentation of cybersecurity strategies which are aligned to, and coincide with, the overall business strategies and objectives, risk tolerance, consumer/client protection responsibilities and overall risk profile of their entities. In addition, the governing bodies are reminded of their responsibility to review and approve the cybersecurity strategies to ensure that such strategies are updated accordingly. Further, the governing bodies must ensure that management integrates cyber resilience and cyber risk assessments into the overall business strategy and enterprise-wide risk management, as well as budgeting and resource allocation.

Summary of Good Practices

- Detailed cybersecurity strategies with defined roadmaps, timeframes and resource allocation.
- Cybersecurity strategies which focus on people, processes and technology.

Summary of Areas for Improvement

- Board approval of cybersecurity strategies.
- Need for alignment of cybersecurity strategies with business strategies and objectives, risk tolerance, consumer/client protection responsibilities and overall risk profile.

Cybersecurity Risk Appetite

Instances were also observed where Selected Entities' governing bodies had not formulated nor formally documented and approved their cybersecurity risk appetite statement. An adequate cybersecurity framework should include the regulated entity's tolerance level or risk limit relating to cybersecurity risk. The risk tolerance should be approved by the governing body.

Thus, regulated entities should annually define and quantify the business risk tolerance relative to cybersecurity and cyber resilience and ensure that this is consistent with the strategy and risk appetite.

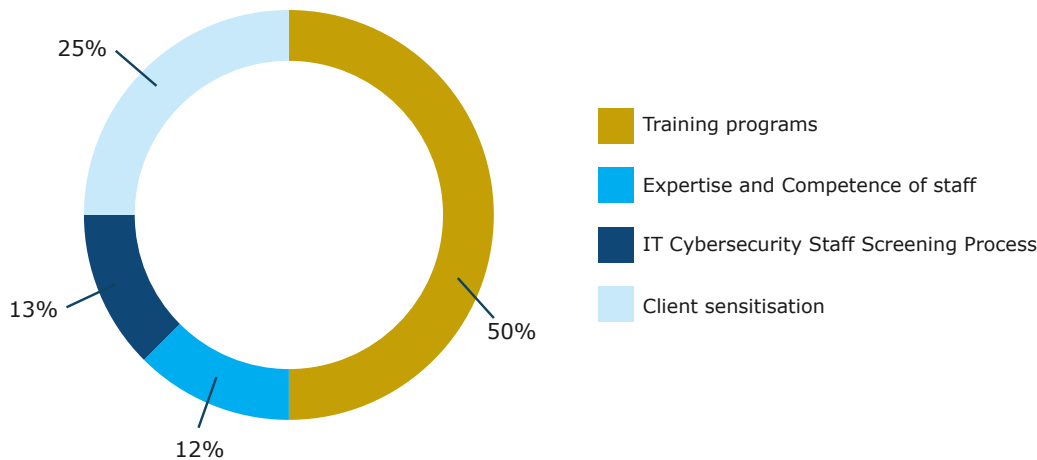
Summary of Good Practices

- Well defined cybersecurity risk appetites, tolerance levels or risk limits.

Summary of Areas for Improvement

- Need to carve out the cybersecurity risk appetite from overall operational risk appetite.
- Board approval of cybersecurity risk appetite.
- Alignment of cybersecurity risks and controls with the risk appetite.

Cybersecurity Awareness, Training and Resources



Training Programs

Some of the Selected Entities had not provided their employees with adequate cybersecurity training and awareness opportunities on an ongoing basis, including training on data protection. While the Entities had in place policies and procedures to support such trainings, there were no plans in place to facilitate the training. It was also observed that some of the Selected Entities were not sensitising their clients on cyber risks.

All regulated entities should ensure that all staff, including governing bodies are trained to understand at a minimum the cyber risks to which the entity is exposed, and the mitigating measures employed to reduce the occurrences of cyber incidents and that such training is conducted on a regular basis. In addition, regulated entities should make every effort to ensure that they regularly disseminate cybersecurity information to their clients or any other actions to help increase their clients' level of cybersecurity awareness.

Summary of Good Practices

- Mandatory training and awareness programs for the Board and all staff through in-house or third-party service providers.
- Technical training and certifications for cybersecurity personnel.
- Training needs assessment based on cybersecurity testing success or failure rates.

Summary of Areas for Improvement

- Inclusion of data protection training in overall training strategies.
- Detailed plans for ongoing training and awareness.
- Increased efforts to raise clients' cybersecurity level of awareness.

Employee Selection, Expertise and Competence

It was observed that several Selected Entities did not have in place comprehensive screening and selection processes and criteria for staff who support technology functions. It was further observed that some of the staff involved in such functions did not have the requisite expertise and competence required to manage these functions.

The Authority expects that, as part of cybersecurity resources management, all regulated entities should implement a comprehensive and effective screening process with stringent selection criteria to ensure careful selection of staff who support technology functions and minimise cyber risks due to system failure, internal sabotage or fraud. Staff should be suitably qualified, experienced and have a good understanding and knowledge of IT systems and cybersecurity.

Summary of Good Practices

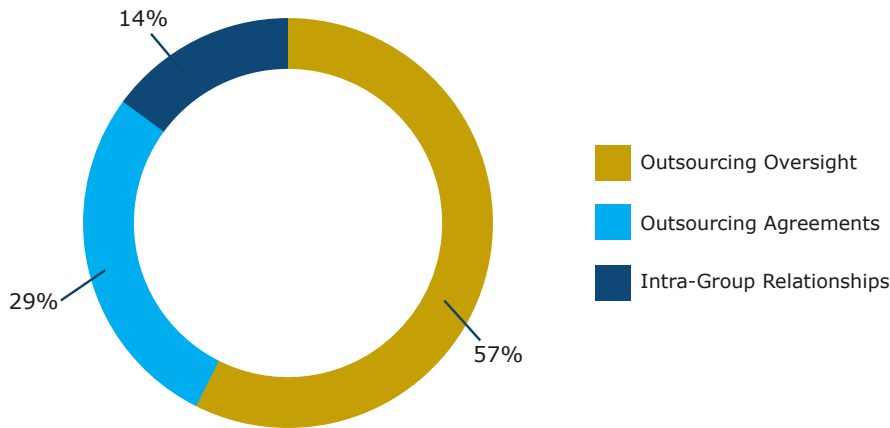
- Technical training and certifications for cybersecurity personnel.

Summary of Areas for Improvement

- Comprehensive and effective screening process, with stringent selection criteria to ensure careful selection of staff in cybersecurity roles.
- Appointment of suitably skilled and competent staff with relevant qualifications and experience.

Outsourcing

Areas of Weakness in Outsourcing



Outsourcing Oversight

There were instances where some of the Selected Entities with outsourced cybersecurity arrangements did not maintain adequate oversight of such arrangements including but not limited to, assessment(s) of the service providers’ compliance with the Rule and Statement of Guidance on Cybersecurity for Regulated Entities and the Statement of Guidance on Outsourcing. In addition, some of the Selected Entities did not have in place adequate and sufficient outsourcing agreements in place to support the services provided by third parties.

The Authority expects that the ultimate responsibility and accountability for outsourced IT cybersecurity arrangements and other third-party dependencies, supporting or potentially negatively impacting internet activities and IT systems, remain with regulated entities. Given that outsourcing arrangements could change the cybersecurity risk profile of regulated entities, matters such as contractual terms and conditions governing the roles, relationships, obligations, and responsibilities of all service providers should be set out fully in written agreements. The Authority also expects that intra-group arrangements would be treated in the same manner as third-party arrangements, even where intra-group arrangements pose a lower risk to the Regulated Entities.

Summary of Good Practices

- Detailed written agreements with intergroup or third-party service providers.
- Written confirmations on the adequacy of frameworks managed at the group level.

Summary of Areas for Improvement

- Entities who rely on group framework should receive written confirmation on the adequacy of the frameworks being managed at the Group level.
- The need to conduct regular assessment of intra-group and third-party cybersecurity frameworks against local requirements to ensure compliance.
- The need to ensure outsourcing agreements comply with local requirements.


CONCLUDING REMARKS


The Authority continues to remind all regulated entities of their statutory and regulatory obligations to adhere to regulatory rules and statements of guidance, and to ensure that their own policies, procedures, systems, and controls are of an appropriate standard and are adhered to consistently.

The Authority further encourages governing bodies to enhance their oversight on cybersecurity frameworks and to ensure that such frameworks are adequately implemented by senior management across all business lines and geographies, where applicable.



THEMATIC CYBERSECURITY REVIEW REPORT

 SIX, Cricket Square
PO Box 10052
Grand Cayman KY1-1001
Cayman Islands

 Tel: +1 (345) 949-7089

 www.cima.ky