Bermuda Insurance Sector Operational Cyber Risk Management

2019 Report

EXECUTIVE SUMMARY

The Authority assesses both cyber underwriting and operational cyber risk within its supervision of registrants. This report focuses on operational cyber risk findings. Cyber underwriting risk findings are published in a separate report.

In 2018, the Authority included questions in its 2018 year-end Commercial Insurer Capital and Solvency Return (CSR) filing designed to assess information security, cybersecurity and data privacy preparedness of (re)insurers. A subset of those questions was included in the 2018 year-end filings for limited purpose insurers and intermediaries. The Authority is issuing this Operational Cyber Risk Management Report to provide feedback on the information obtained in these 2018 year-end filings.

Operational cyber risk is a critical risk that should be managed as part of an organisation's Enterprise Risk Management (ERM) process. As circumstances may vary greatly from entity to entity, the Authority recognises that there is no "one-size-fits-all" approach to addressing operational cyber risk. Each company must assess its risks and choose an appropriate risk response. The Authority expects the Board of Directors (the Board) to evaluate operational cyber risks regularly and ensure prudent policies, procedures and controls are in place and embedded within the organisation.

Internationally, the number and complexity of cyber threats, as well as the number of successful cyber-attacks, is increasing. The common impacts to organizations are reputational damage and financial loss. Regulators around the globe are publishing Codes of Conduct and applying more focus to this key enterprise-level risk.

A growing number of Bermuda registrants, especially those that proportionally might be said to have the most considerable operational cyber risk exposure, appear to have improved their resilience to cyber-attacks. There is also evidence of increased resources being dedicated to mitigating these risks. However, based on the Authority's review of the 2018 year-end filings, the following areas appear to need further improvement:

- Board approval of Operational Cyber Risk Strategy/Policy
- Third-Party Operational Cyber Risk Management Assessment
- Data Classification and Data Loss Prevention (DLP) controls

- Testing of Business Continuity Planning (BCP) and Disaster Recovery (DR)
- Scenario rehearsal "table top testing" of the Security Incident Response Plan
- Monitoring of anomalous network activity

Key Points:

What is the source of data used in this report?

This report is split into two sections. Section A assesses data from the enhanced 2018 Bermuda Solvency and Capital Return (BSCR) Cyber filing returns (Schedule Ve) for commercial insurers. Section B assesses data from the subset of questions in the 2018 filing returns completed by limited purpose insurers and intermediaries (including insurance managers). Moving forward, the Authority plans to establish a single set of questions to be completed by all registrants.

Does the BMA use any international frameworks as a reference for control requirements?

Whilst the Authority does not restrict itself to any single standard or framework, the BMA is aligned to the Cybersecurity Framework authored by the US National Institute of Standards and Technology (NIST).

How will the Authority provide clarity on the cyber risk controls it expects to be in place?

The Authority is currently in a consultation phase for the introduction of a new Operational Cyber Risk Management Code of Conduct (Code) which will apply to all insurance entities and classes. This Code recognises the differing nature, scale and complexity of registrants in the sector and sets out the BMA's expectations for companies to demonstrate prudent cyber risk management processes and technical controls over its operational cyber risk. The Code is expected to come into effect January 2021 with enforcement commencing in June 2021.

How will the BMA continue to monitor insurance sector operational cyber risks?

The Authority will continue close monitoring and ensure that operational cyber risk assessments are integrated into all key supervisory processes, such as the year-end filing review, on-site visits and supervisory college discussions, as applicable.

Does this report give assurance on control effectiveness?

In the sections below, the Authority discusses its findings and expectations on various aspects of

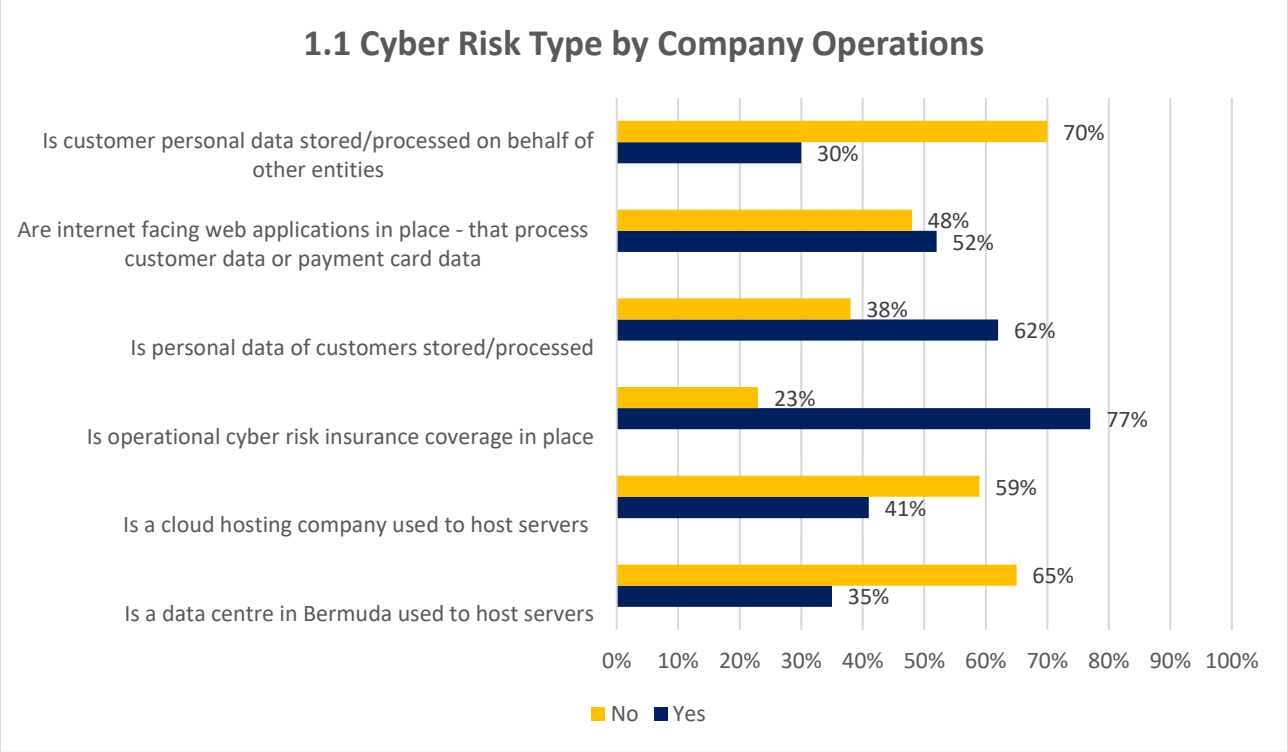
operational cyber risk as it applies to the insurance sector. It should be noted that the statistics presented in these sections reflect the information gathered from the filing submissions and do not speak to the effectiveness of the controls in each of the areas outlined.

1. Analysis of Data from Commercial Insurers

This section assesses data from the enhanced 2018 BSCR Cyber filing returns (Schedule Ve) completed by the commercial insurer Classes.

1.1 Cyber Risk Type by Company Operations

Commercial insurers have different types of operational cyber risk depending on the nature of their business and Information Technology (IT) operations. The BMA recognises there are many different types of commercial insurers in the jurisdiction with different business models and IT services, resulting in operational different cyber risk profiles. Therefore, the Authority expects insurers to assess the operational cyber risks applicable to their individual businesses and decide appropriate risk responses.



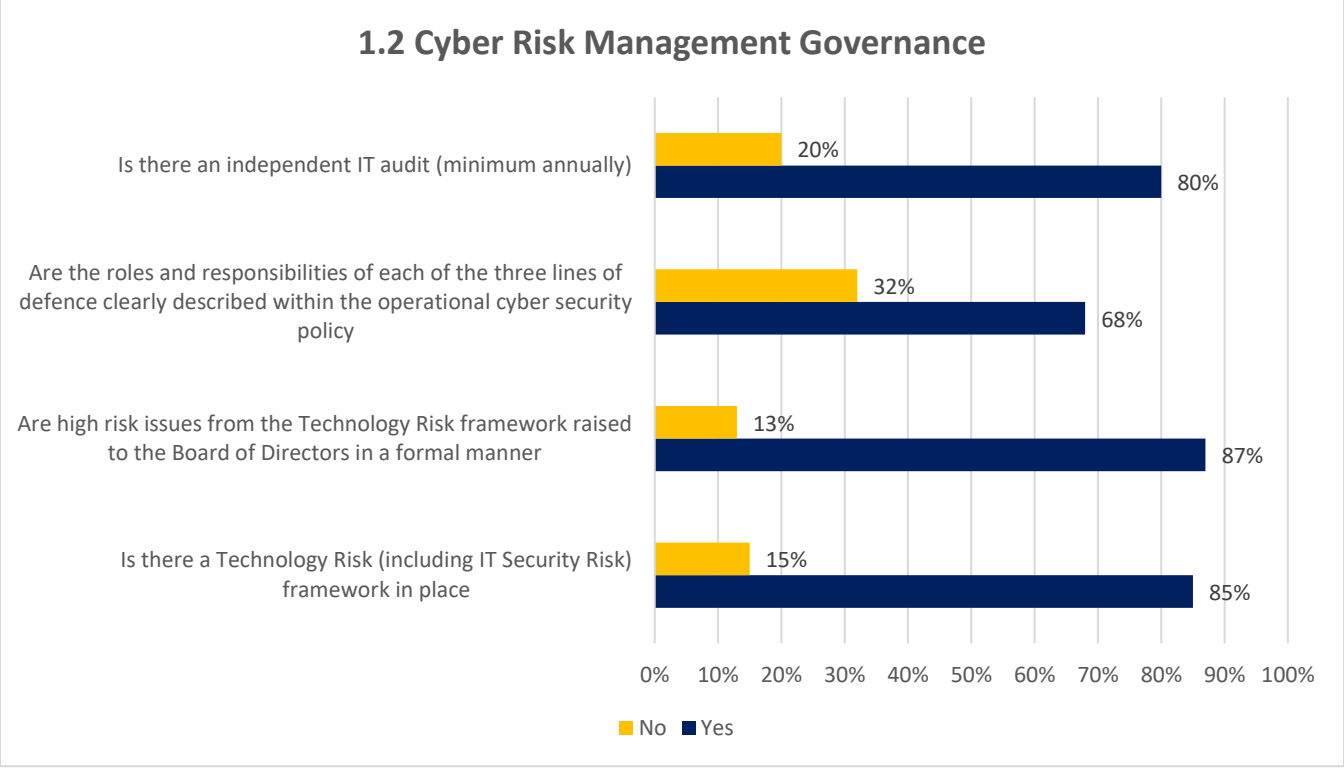
Cloud Computing Services: The above graph illustrates that 35% of commercial insurers reported having data centres physically hosted in Bermuda, whilst 41% use a cloud hosting service. Cloud computing services do not necessarily present higher risk, however, they do present a different set of risks.

Customer Data Processed: 62% of commercial insurers reported processing customer personal data, with 30% reporting that they store/process customer data on behalf of another entity. 52% of insurers reported that they have internet-facing web applications that process customer data. Insurers should appropriately classify processed data and put in place data protection controls commensurate with the level of criticality.

Cyber Risk Insurance: 77% of commercial insurers reported having operational cyber risk insurance in place. This offers a range of benefits, depending on the type of coverage selected. The Authority notes that operational cyber risk insurance is an essential part of a company's risk management framework. However, insurance protection should not be viewed as a replacement for prudent operational cyber risk management practices. The Authority also emphasises the importance of having a comprehensive assessment of risk to aid commercial insurers in determining the adequacy of purchased cyber policies. This can then be a regular review which companies can incorporate as part of their governance processes.

1.2 Cyber Risk Management Governance

The Authority expects that the company's Board is ultimately responsible for visibility and oversight of operational cyber risk management. While the day-to-day execution of this function may be outsourced, responsibility cannot be delegated.



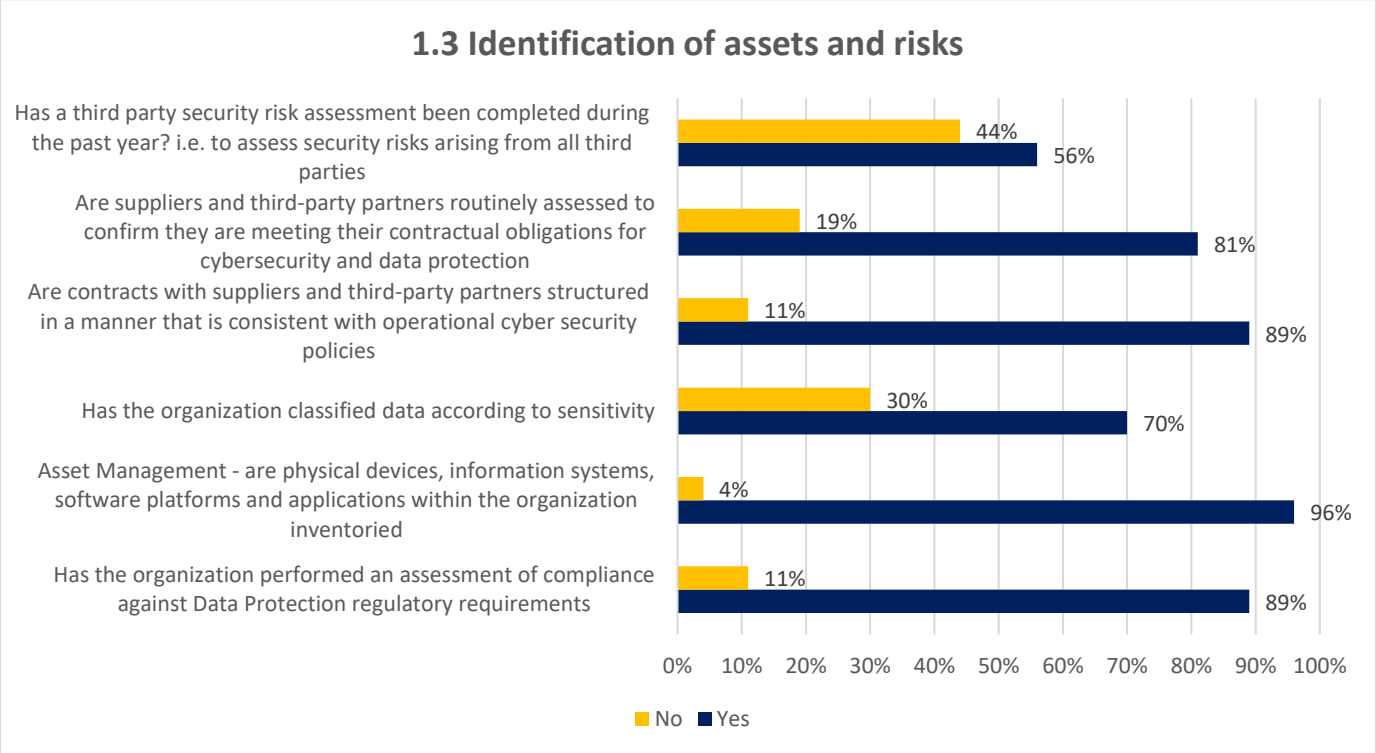
Cyber Risk Framework & Board Oversight: 85% of commercial insurers reported that an operational cyber risk framework was in place, and 87% reported that cyber risks rated as high were formally raised and visible to the Board. While these percentages are encouraging, this also suggests that a small minority of commercial insurers are not equipped with adequate operational cyber risk governance.

Three Lines of Defense: The Authority recognises the 'Three Lines of Defense' model as a best practice for effective operational cyber risk management (i.e. operational control owner, risk function, audit). It was noted that only 68% of commercial insurers reported that the three lines of defence are clearly described in their operational cyber risk management policies. This is lower than expected and companies should increase effort incorporating this in their own risk assessment.

Independent IT Audit: 80% of commercial insurers reported that an independent IT audit took place annually as a minimum. The Authority does not seek to mandate the frequency of independent cyber audits. It is the responsibility of a company's Audit Committee to decide the assurance they require against different IT risks and controls, and that this process can be evidenced in an annual audit plan.

1.3 Identification of Assets and Risks

The first stage of risk identification is asset identification and classification to determine asset criticality.

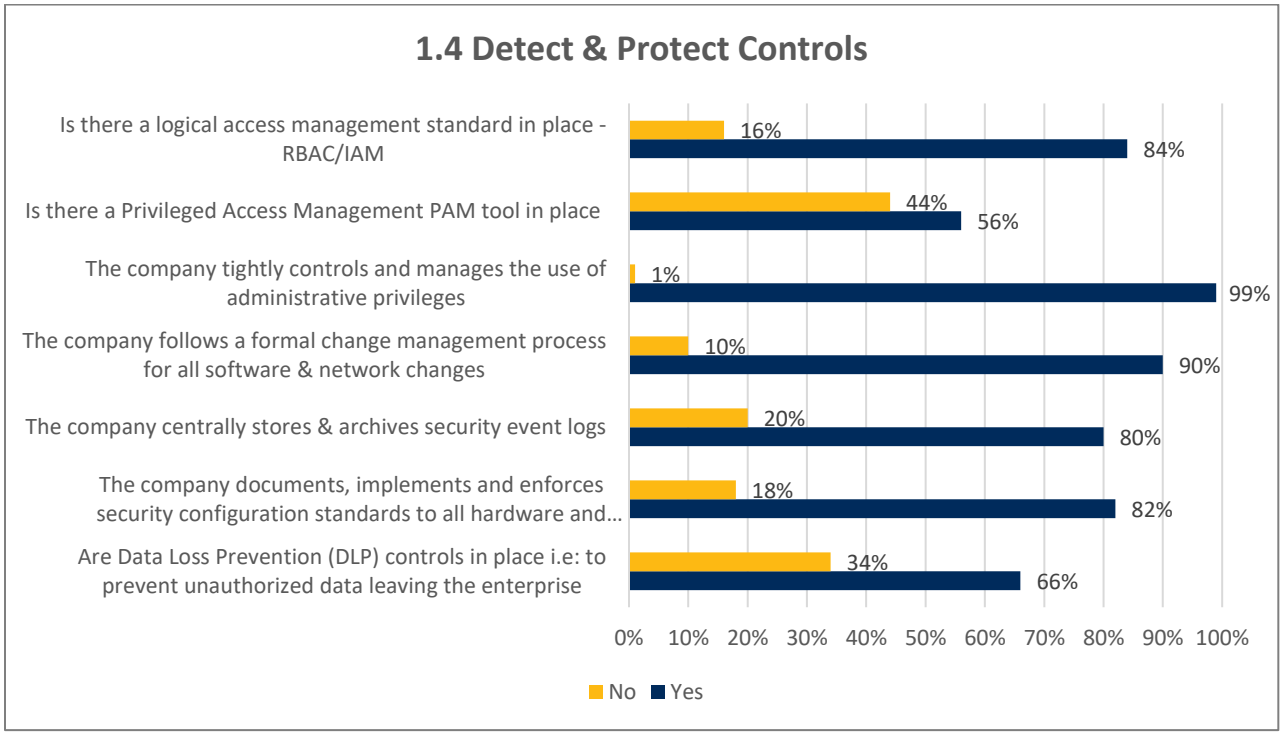


Asset Management: 96% of commercial insurers reported that they had inventoried their IT assets, i.e. their physical devices, information systems, software platforms and applications. However, only 70% reported that they had classified data according to sensitivity.

Third-Party Risk Management: Managing operational cyber risk from third parties and supply chains is a basic tenet of operational cyber risk management. An insurer who trusts third parties with data or the delivery of IT services should have contractual clauses in place to ensure their security requirements are met, and that the service provider is aware and compliant with any local regulations that apply to their clients. 81% of commercial insurers confirmed that third parties are assessed to confirm they are meeting their contractual obligations for cybersecurity. However, only 56% reported this had taken place in the last year. Commercial insurers should assess the risk from third parties and ensure the review period is commensurate with the identified level of risk.

1.4 Detect and Protect Controls

Central to any operational cyber risk management function are cyber security controls. The Authority recognises that insurers of different nature, scale and complexity operate in the jurisdiction and have different cyber security control requirements in place. The data below illustrates the status of several key 'Detect and Protect Controls' as reported by commercial insurers.



Event Log Archiving and Alerting: Event log monitoring enables an organisation to investigate potential incidents and deploy countermeasures to mitigate impacts. Where event logs have been overwritten and are not available, this may hinder the completion of incident route cause analysis.

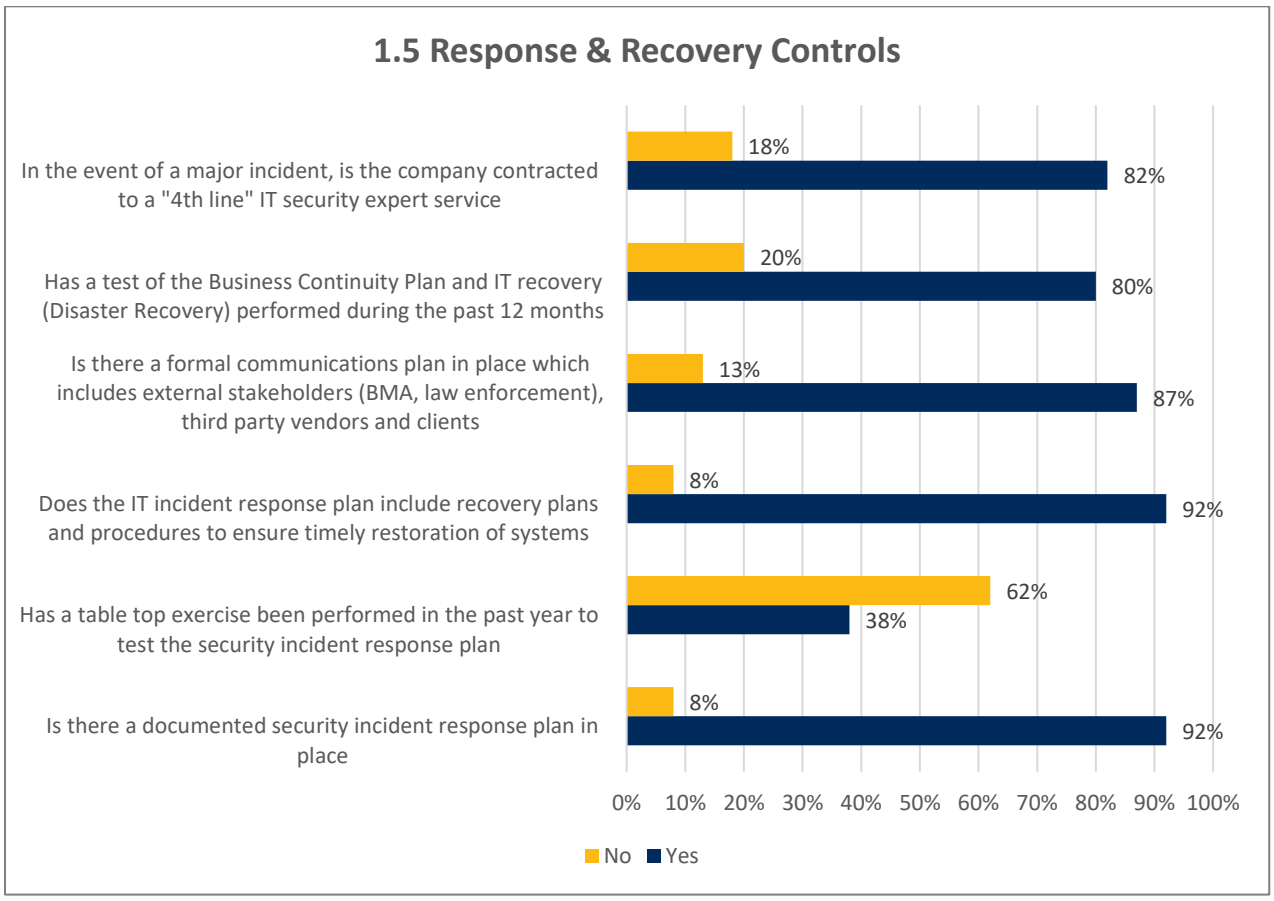
Security Configuration Standards: 82% of commercial insurers reported documentation, implementation and enforcement of security configuration standards to all hardware and software assets on the network. 80% confirmed that they centrally store and archive security event logs. Commercial insurers should review their log archiving and alerting capabilities.

Logical and Privileged Access Management: 99% of commercial insurers confirmed that the use of administrative privileges is tightly controlled. This would appear to give an appropriate level of assurance. However, only 56% reported that they use a Privileged Access Management (PAM) tool whilst 84% of respondents operate a Role-Based Access Control (RBAC) or Identity Access Management (IAM) process. Whilst the Authority is not of the view that formal PAM, RBAC and IAM systems and processes are required or suitable for all insurers, it believes it is prudent for companies to include an assessment of the benefits these tools offer.

Data Loss Prevention (DLP): 66% of commercial insurers reported that DLP controls were in place, i.e. controls to prevent data leaving the enterprise in an unauthorised manner. This is a lower percentage than expected; incidents resulting in data breach often lead to both financial loss and reputational damage. DLP requirements should be assessed against data criticality, and regulatory and contractual requirements.

1.5 Response and Recovery Controls:

Response and Recovery Controls are important tools to identify, investigate and employ to reduce the impact of potential cyber incidents.



Security Incident Response Plans: 92% of commercial insurers reported they have a security incident response plan in place which include recovery plans and procedures to ensure the timely restoration of systems. 87% reported they have a formal communications plan in place.

These figures demonstrate that the majority of commercial insurers have these basic controls in place but the question is raised as to why all commercial insurers do not have incident response plans in place. In terms of the level of maturity of these plans and how well they work in practice, it is noted that 38% of commercial insurers have performed a tabletop exercise in the past year to test the security incident response plan. Insurers should assess their incident response process maturity and consider the benefits of completing tabletop incident "rehearsal" exercises.

Testing of Business Continuity and IT Disaster Recovery Plans: 80% of commercial insurers had tested their Business Continuity and IT Disaster Recovery plans in the preceding 12 months. Commercial insurers should assess the risks presented by not carrying out these activities and confirm if this fits the risk appetite of the business.

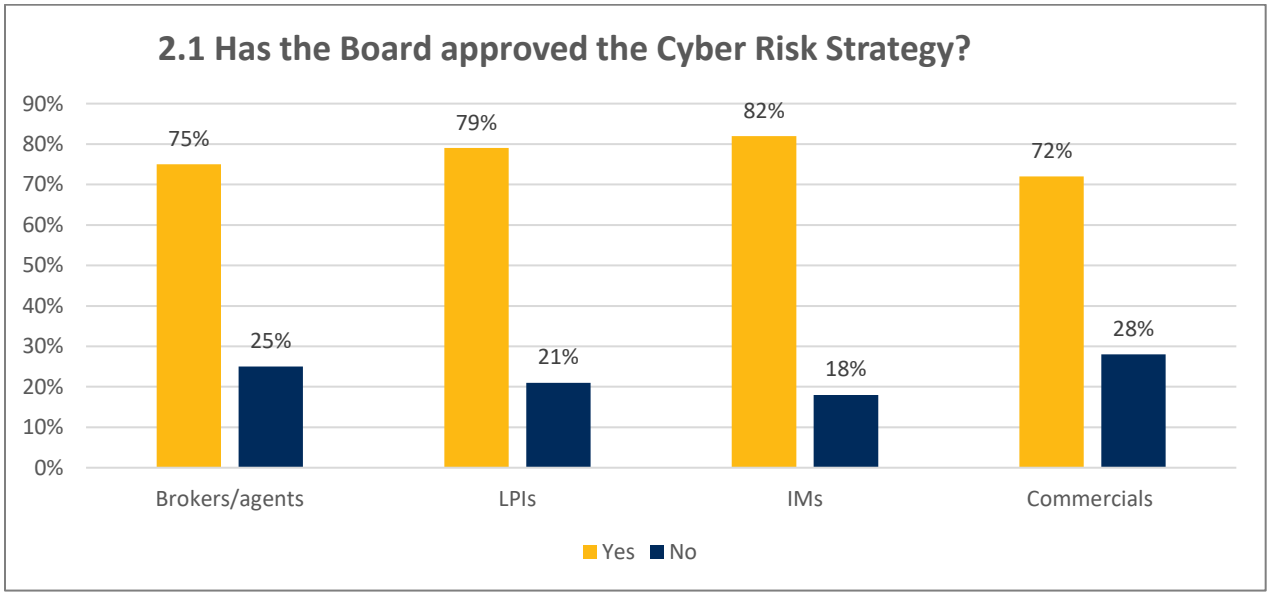
2. Analysis of data from all Insurance Classes

This section is based on data from the 2018 filing returns completed by brokers and agents, insurance managers, limited purpose insurers and commercial insurers.

The Authority understands the varied nature of business models, scale and complexity of operations. Where insurers outsource IT and cyber security to insurance managers, the insurer should have clarity on what controls are in place, as well as control maturity and effectiveness. Any outsourced IT service should be subject to review as part of a third-party IT risk review process.

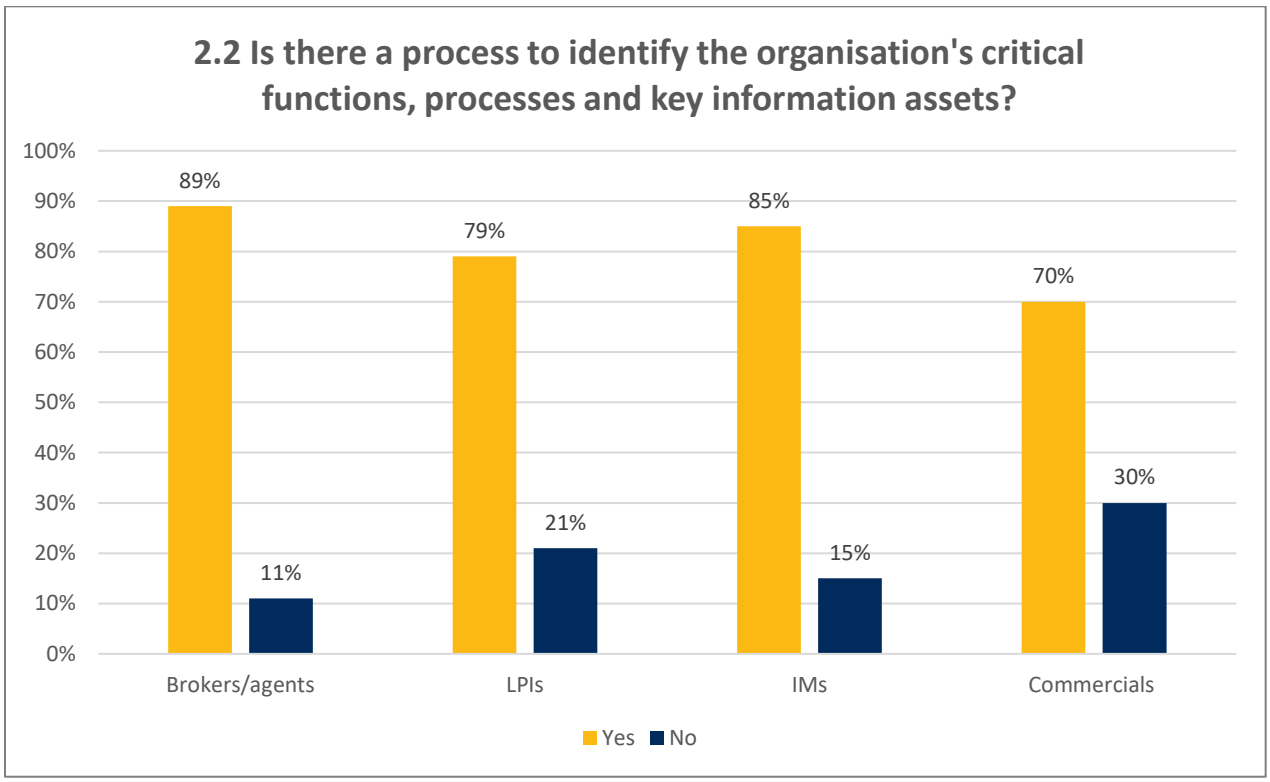
2.1 Board Approval of Cyber Risk Strategy

The graph below illustrates that board approval of cyber risk strategy is not at a uniform level across these subsectors. The insurance sector should review if their boards have an appropriate level of visibility of operational cyber risk strategy and approval status.



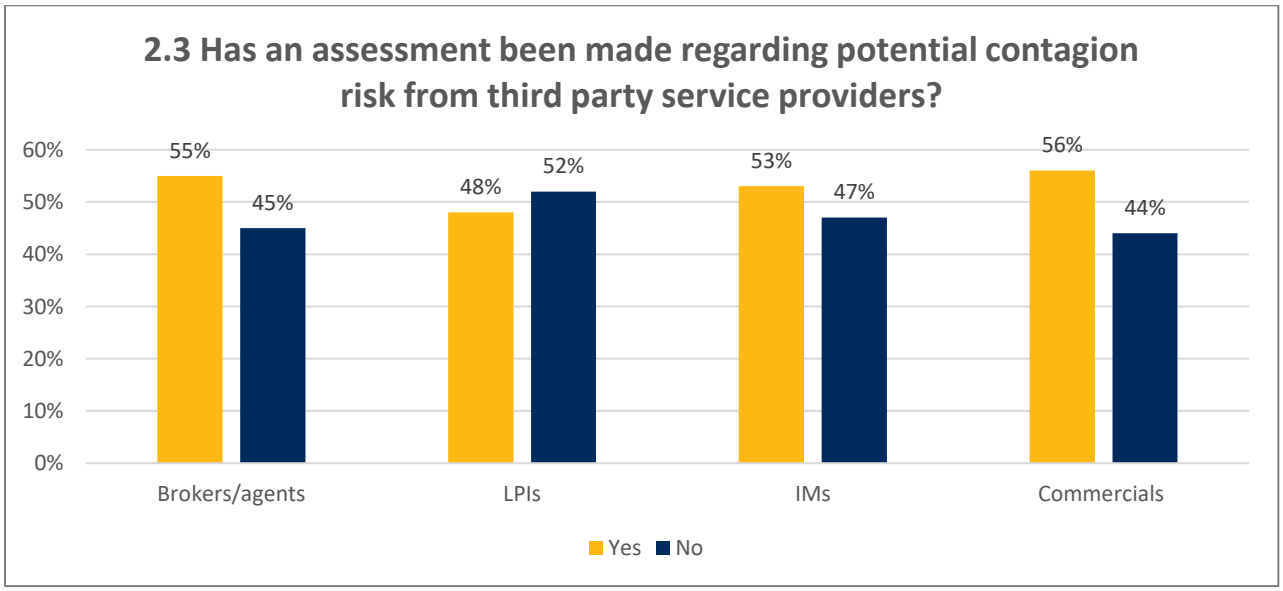
2.2 Assessment of Critical Functions, Processes and Key Information Assets

Organisations should identify critical business and IT functions, and decide appropriate continuity recovery requirements. Without this, the business may incorrectly assume security and recovery controls are in place, whilst instead there is a risk that critical functions and assets are not protected. This may lead to service outages and compromise of information assets.



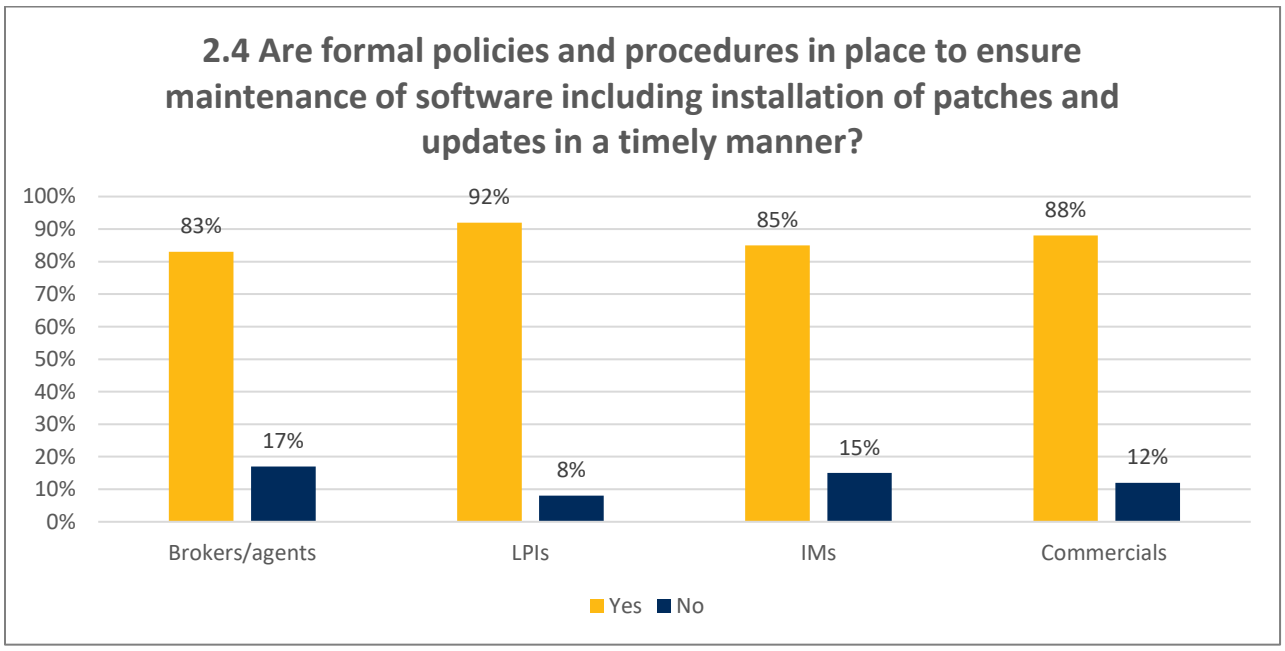
2.3 Cyber Risk Assessment of Third Parties

Computer networks and the data they store/process are only as secure as their weakest link. Therefore, the insurance sector must assess risks from their third-party providers. On average, 53% of respondents reported that they had assessed risks from their third-party providers, this is lower than anticipated and should be an area of focus for the sector. The Authority will pay attention to this area in our future onsite examinations and reviews.



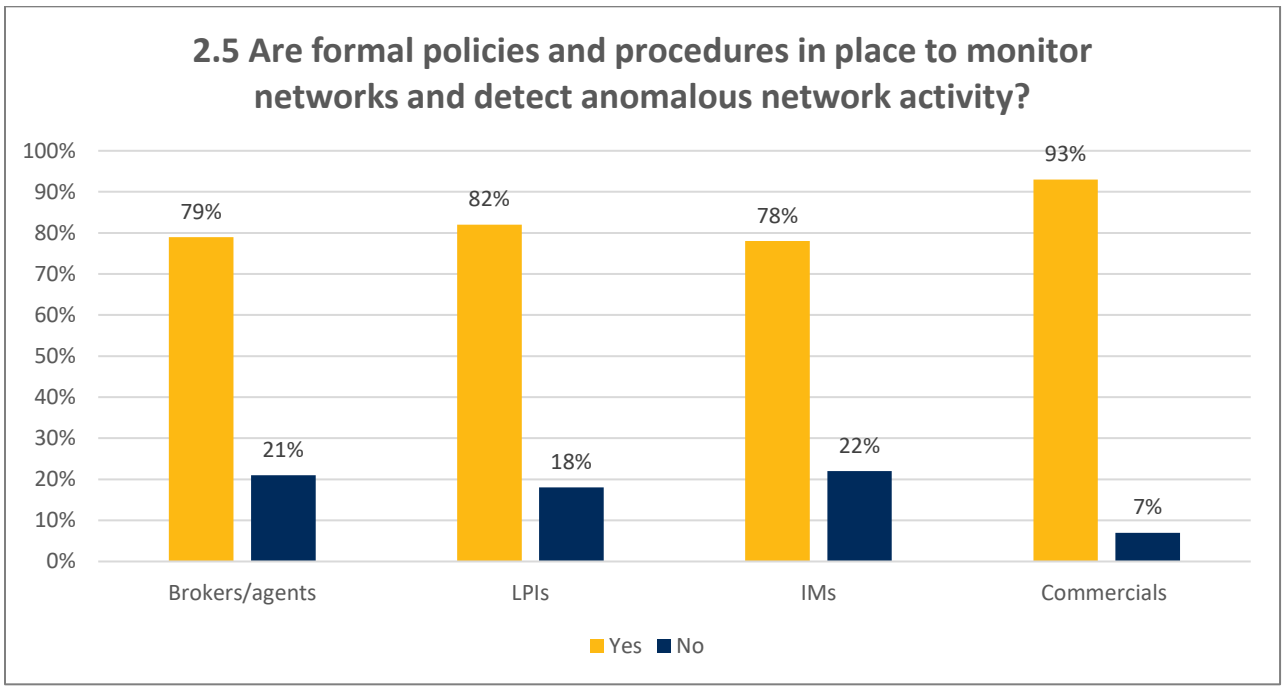
2.4 Are formal policies and procedures in place to ensure maintenance of software, including installation of patches and updates in a timely manner?

The maintenance and patching of software versions is one of the basic requirements of vulnerability management. Policies and procedures should be in place to formalise this activity. Reporting of version/patch status is then required to confirm that systems are updated in line with the documented requirements. The insurance sector should review their controls in this space and ensure they are fit for purpose.



2.5 Monitoring of Anomalous Network Activity

The insurance sector must monitor their networks to detect anomalous activity that may be malicious. Event monitoring, intrusion detection controls and associated processes would typically be used to do this. The percentage of companies that have reported as having these controls in place is lower than expected, and companies should review if the controls they have in place are adequate.



CONCLUSION AND NEXT STEPS

Conclusion

Overall, the BMA believes that companies must apply an appropriate degree of focus to their operational cyber risk management posture. Going forward, the Authority will continue to monitor the cyber risk filing returns as well as the evolving nature of the cyber risk threat landscape. The Authority expects registrants to review the key issues identified in this summary report and ensure that their operational cyber risk management controls are appropriate against the nature, size and complexity of their business.

Next steps

- The Authority will continue to assess the adequacy of Operational Cyber Risk Management postures during its ongoing supervisory engagements, on-site visits and supervisory colleges
- The Operational Cyber Risk Management Code of Conduct, once operational, will complement the general provisions mentioned in the various Codes of Conduct published for Insurers and Intermediaries
- The BMA is also looking to introduce a cyber-reporting event requirement for all insurance companies as part of its legislative agenda for 2020
- Additionally, the Authority will require companies to clearly detail operational cyber risk in the Commercial Insurer/Group Self Solvency Assessment (CISSA/GSSA) process and documentation

Definitions

- **Business Continuity Planning (BCP):** The process of creating systems of prevention and recovery to deal with potential threats to a registrant
- **Chief Information Security Officer (CISO):** This means the senior executive, by whatever title called, appointed by the registrant to oversee and implement its cyber risk programme and enforce its cyber risk policies
- **Data Loss Prevention (DLP) controls:** DLP is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network
- **Disaster Recovery (DR):** DR is a set of policies and procedures which focus on protecting an organisation from any significant effects in case of a negative event, which may include cyberattacks, natural disasters or building or device failures
- **Enterprise Risk Management (ERM) process**: ERM is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives
- **Identity Access Management (IAM)**: Defining and managing the roles and access privileges of individual network users and the circumstances in which users are granted (or denied) those privileges
- **Logical Access Management (LAM):** Logical access controls are tools and protocols used for identification, authentication, authorisation, and accountability in computer information systems
- **NIST**: National Institute of Standards and Technology
- **Privileged Access Management (PAM)**: A class of solutions that help secure, control, manage and monitor privileged access to critical assets
- **Role Based Access Control (RBAC):** RBAC is a policy-neutral access-control mechanism defined around roles and privileges; the components of RBAC (such as role-permissions, user-role and role-role relationships) make it simple to perform user assignments.
- **Technology Risk Framework**: The risk management framework provides a process that integrates security and risk management activities into the system development life cycle
- **Three Lines of Defence:** Management control is the first line of defence in risk management, the various risk control and compliance over-sight functions established by management are the second line of defence, and independent assurance is the third
- **Fourth line:** Escalating an issue or long-term project management to those with more expertise outside of an organisation