BMA
BERMUDA MONETARY AUTHORITY

BERMUDA INSURANCE SECTOR OPERATIONAL CYBER RISK MANAGEMENT - 2020 REPORT

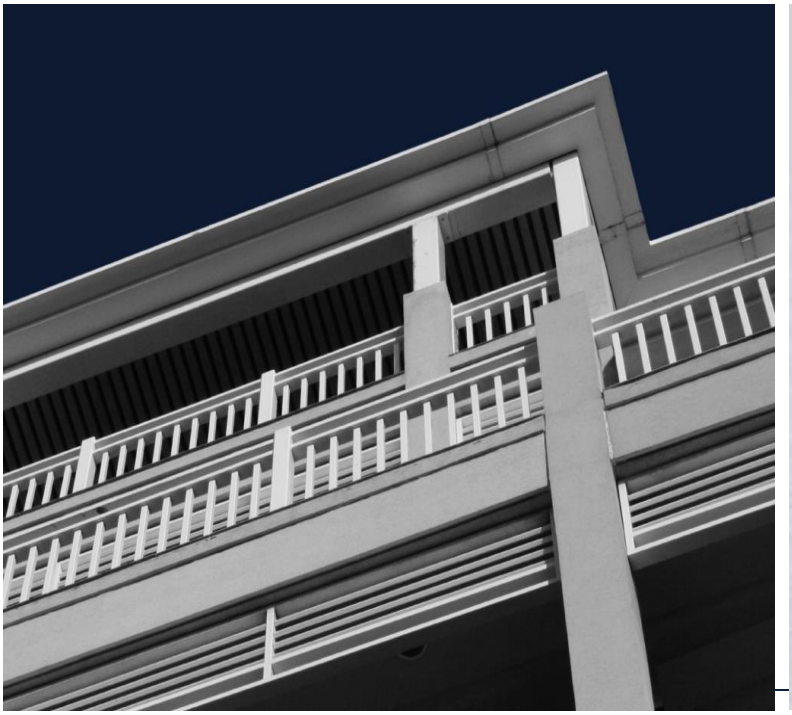


TABLE OF CONTENTS

Background

This report is based on the enhanced 2019 Bermuda Solvency Capital Requirement (BSCR) cyber filing returns. The Bermuda Monetary Authority (Authority or BMA) is issuing this communication to provide feedback on the information obtained in the 2019 year-end filing from insurance managers, commercial insurers and brokers and agents.

Executive Summary and Key Findings

The Authority is pleased with the industry's continued focus on cyber risk. However, the data indicates that for some cyber risks, a lower than expected percentage of insurers indicate they have controls in place. These areas include:

- **Third-party cyber risk management assessment** – Managing cyber risk from third parties and supply chains is an important part of cyber risk management. An insurer who trusts third parties with data, or to deliver IT services, should consider having contractual clauses in place to ensure their security requirements are met.

- **Data classification** – Information should be classified and protected in a manner commensurate with its sensitivity, value and criticality. An asset inventory should be put in place, detailing all information assets. The information must be classified in terms of its value, legal requirements, sensitivity and criticality to the organisation.

- **Board approval of cyber risk strategy/policy** – The Board of directors and senior management team must have oversight of cyber risks. The Board of directors must approve a cyber risk policy document at least annually. The cyber risk may be covered in a standalone cyber risk policy document or as a section in a broader risk policy document (e.g., the operational risk policy).

- **Data Loss Prevention (DLP)** – Registrants must perform an assessment of their DLP control requirements (i.e., controls to prevent data leaving the enterprise in an unauthorised manner). Typically, this assessment would reference the level of data classification, potential unauthorised data egress points and appropriate mitigating controls.

- **Maintenance of software (including installation of patches and updates)** – Registrants must have patch management procedures that define the identification, categorisation and prioritisation of security patches. Registrants must pay close attention to a vendor's end-of-support date as patches may no longer be available after this date.

Insurance Sector Operational Cyber Risk Management Code of Conduct (the Code)

The final version of the Code was published in October 2020. The Code came into effect on 1 January 2021. Companies have until 1 January 2022 to ensure their compliance.

The Code is designed to promote the stable and secure management of information technology systems of regulated entities. The Authority is not adopting a "one-size-fits-all" approach and expects cyber risk controls will be proportional to the nature, scale and complexity of the organisation. It is acknowledged some entities will use a third party to provide technology services and they may outsource their IT resources (e.g., to an insurance manager). All third-party and outsourced services should be subject to cyber risk review.

Notification of Cyber Reporting Events to the Authority

The Insurance Amendment Act 2020 came into force on 5 August 2020 requiring notification of cyber reporting to the Authority. Full guidance of requirements is given in section 6.5 of the Code.

It should be noted that only cyber reporting events resulting in a significantly adverse impact to the regulated entity's operations, policyholders or clients, must be reported to the Authority. When in doubt about whether an event is reportable, registrants should consult with the Authority for guidance.

A principal representative (for insurers) and appropriate officer (for insurance managers and intermediaries) must notify the Authority within 72 hours from the time that there is either a determination or a confirmation of an event.

An incident report containing known details of the incident, the root cause, actions taken to minimise impact and any actual adverse impact to the organisation must be submitted within 14 days of the initial incident notification date.

Remote Working and Cyber Resilience

The recent shift of many business operations to a remote working model may present a number of changes to organisations' cyber risk profiles. Cyber resilience, though, is the ability to prepare for and recover rapidly from disruptions resulting from deliberate attacks, accidents or naturally occurring threats or incidents—such as disruptions created by this shift to remote working. As such, cyber resilience should be managed as part of the overall operational risk process of an organisation.

In instances where new remote working services have been configured, the "attack surface" of companies have changed. New services that have not been subject to standard security hardening and testing will introduce new vulnerabilities. Remote services by nature are internet-facing and are at a high risk of exploitation by malicious actors. Companies should review the security posture of any new remote working services. This review should also assess any single points of failure and ensure that system redundancy is in place.

The recent invocation of remote working by many companies demonstrates the importance of Business Continuity Planning (BCP) and Disaster Recovery (DR). Organisations should have documented BCP and DR plans in place which have been tested to provide assurance on their effectiveness.

Next the Authority will:

- Continue to monitor cyber risk filing returns, as well as the evolving nature of the cyber risk threat landscape
- Review registrants' compliance to the Code as part of the supervisory review process
- Continue to consult with the insurance sector in a proactive manner
- Continue to require that companies clearly detail operational cyber risk in the Commercial Insurer Solvency Self-Assessment/Group Solvency Self-Assessment (CISSA/GSSA) process

About the Authority

The Authority was established by statute in 1969. Its role has evolved over the years to meet the changing needs in Bermuda's financial services sector. Today it supervises, regulates and inspects financial institutions operating in the jurisdiction. It also issues Bermuda's national currency, manages exchange control transactions, assists other authorities with detecting and preventing financial crime, and advises Government on banking and other financial and monetary matters.

The Authority develops risk-based financial regulations that apply to the supervision of Bermuda's banks, trust companies, investment businesses, investment funds, fund administrators, money service businesses, corporate service providers, insurance companies, digital asset businesses and digital asset issuances. It also regulates the Bermuda Stock Exchange (BSX) and the credit union.

BMA Contact Information

Bermuda Monetary Authority
BMA House
43 Victoria Street
Hamilton

P.O. Box 2447
Hamilton HMJX
Bermuda

Tel: (441) 295 5278
Fax: (441) 292 7471

E-mail: enquiries@bma.bm

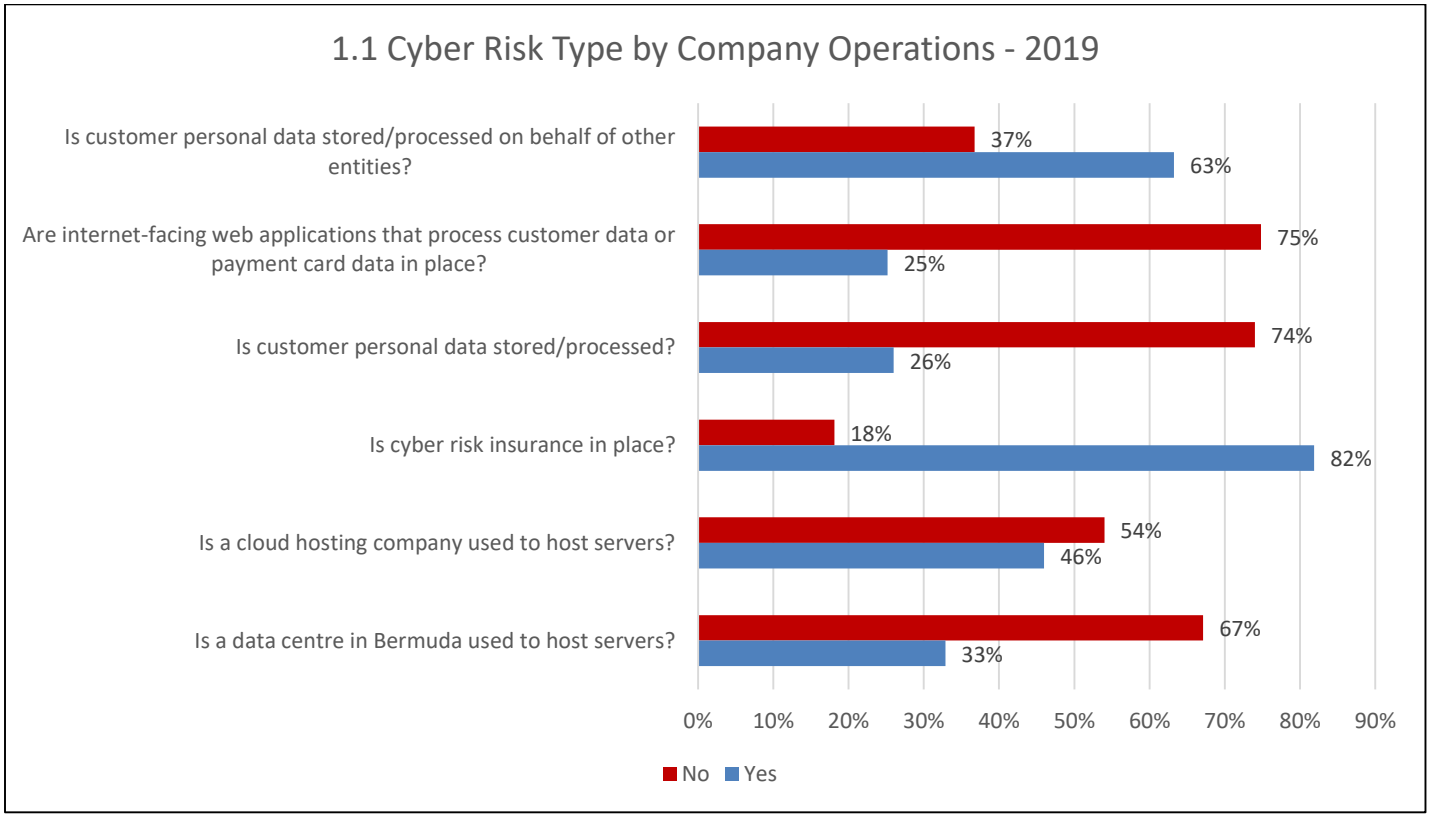
This publication is available on the BMA website www.bma.bm

1. Assessment of Data – Commercial Insurers

This section assesses data from the enhanced 2019 BSCR cyber filing returns (Schedule Ve) completed by commercial insurers.

1.1 Cyber Risk Type by Company Operations

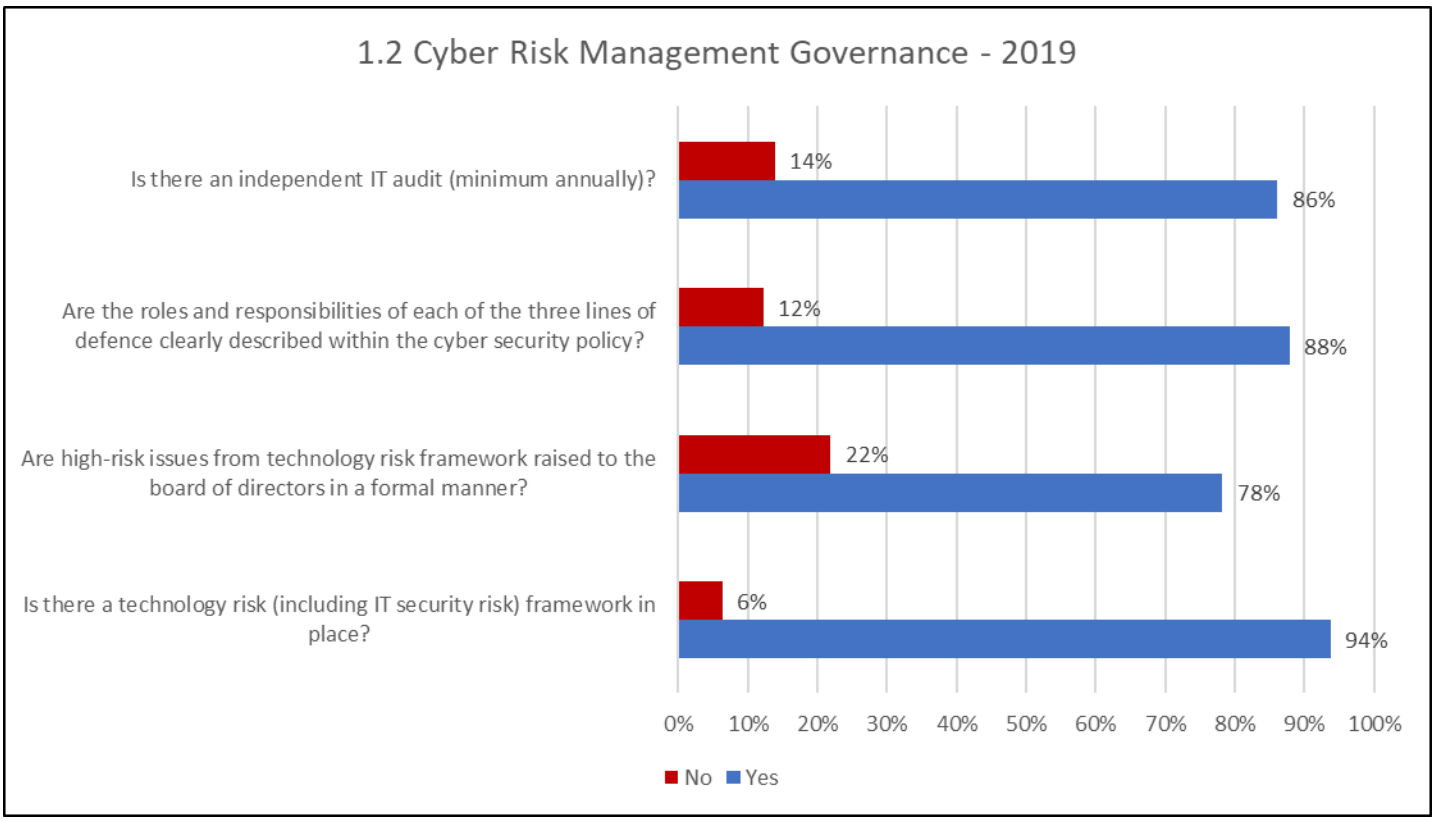
It is important that the data processed by insurers is appropriately classified and data protection controls put in place are commensurate with the level of criticality. The BMA recognises that there are many different types of commercial insurers in the jurisdiction with varying models of business and IT services, resulting in different cyber risk profiles.



Cloud computing services: The above graph illustrates that 33% of commercial insurers reported having data centres physically hosted in Bermuda, while 46% use a cloud hosting service. Cloud computing services present a different set of risks and it is important that risk assessments of these services are performed.

Customer data processed: Graph 1.1 shows that 26% of commercial insurers reported processing customer personal data, with 63% reporting that they store/process customer data on behalf of another entity.

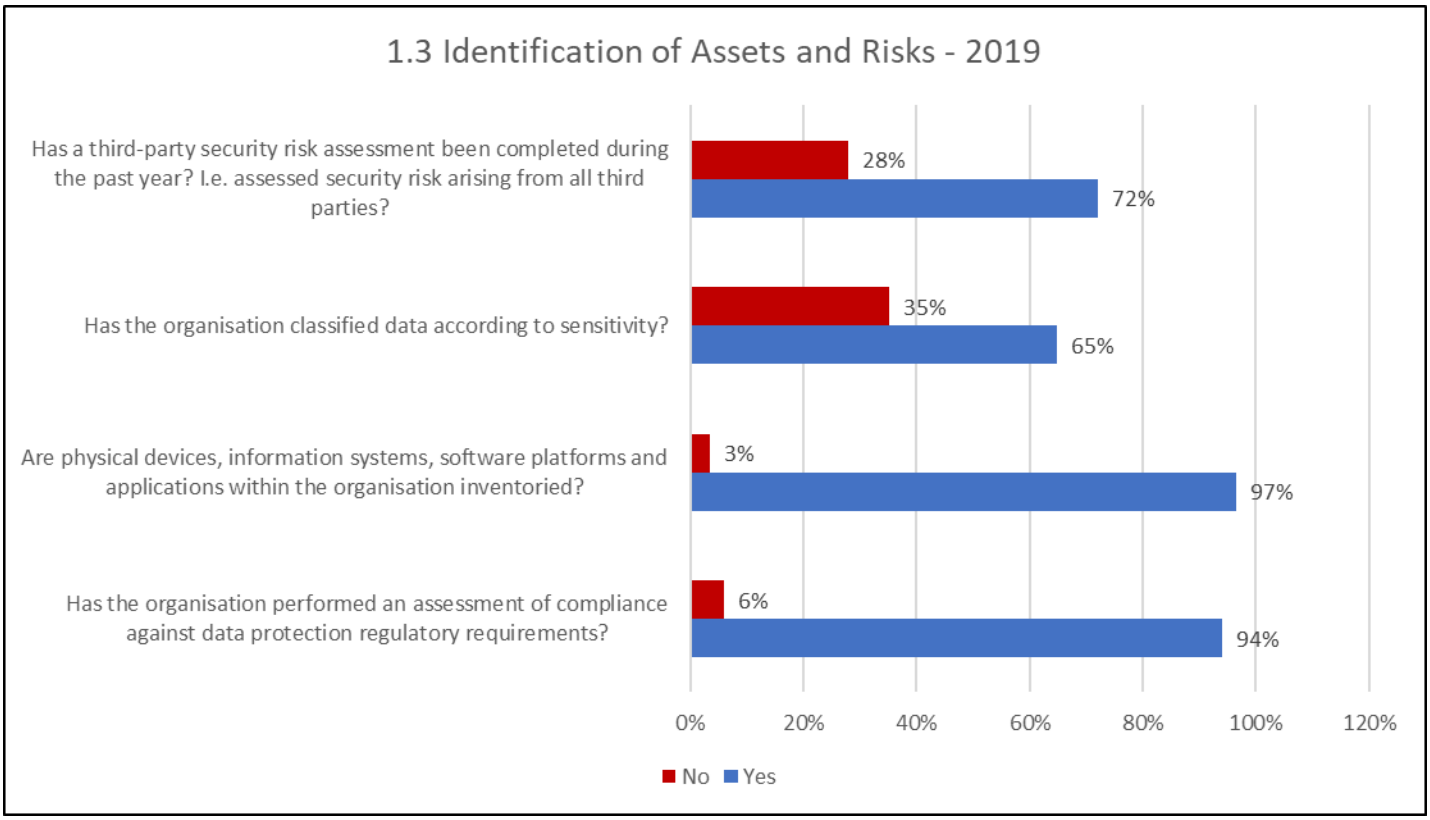
1.2 Cyber Risk Management Governance



Cyber risk framework and board oversight: The graph illustrates that 94% of commercial insurers reported that a technology risk framework was in place and 78% reported that technology risks rated as 'high' were formally raised and visible to the Board.

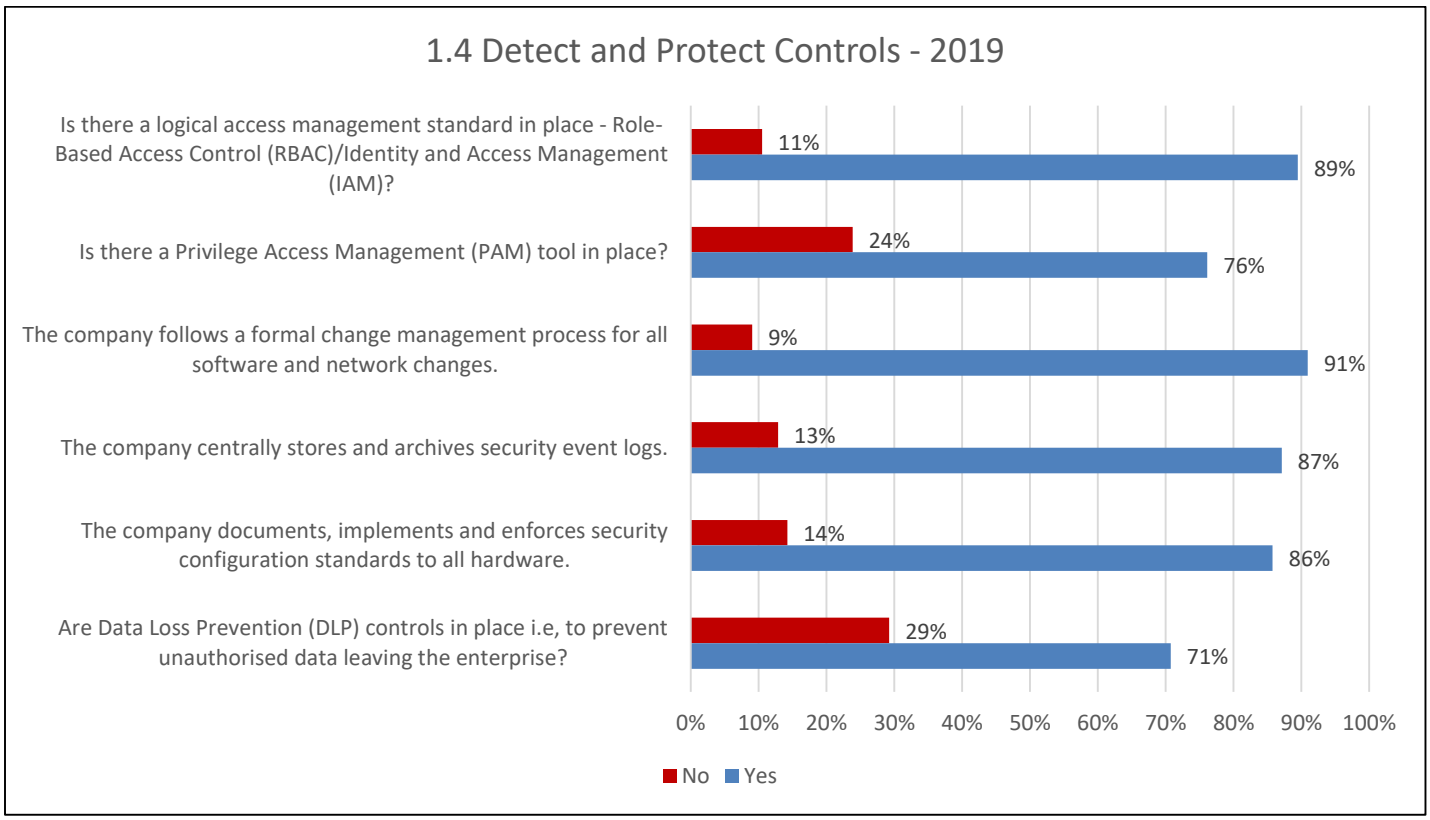
Independent IT audit: Data collected shows that 86% of commercial insurers reported that an independent IT audit took place annually as a minimum. It is the responsibility of a company's audit committee to decide the assurance they require against different IT risks and controls. This process can be evidenced in an annual audit plan.

1.3 Identification of Assets and Risks



Asset management: Graph 1.3 shows that 97% of commercial insurers reported they had inventoried their IT assets (i.e., their physical devices, information systems, software platforms and applications). However, only 65% reported that they had classified data according to sensitivity.

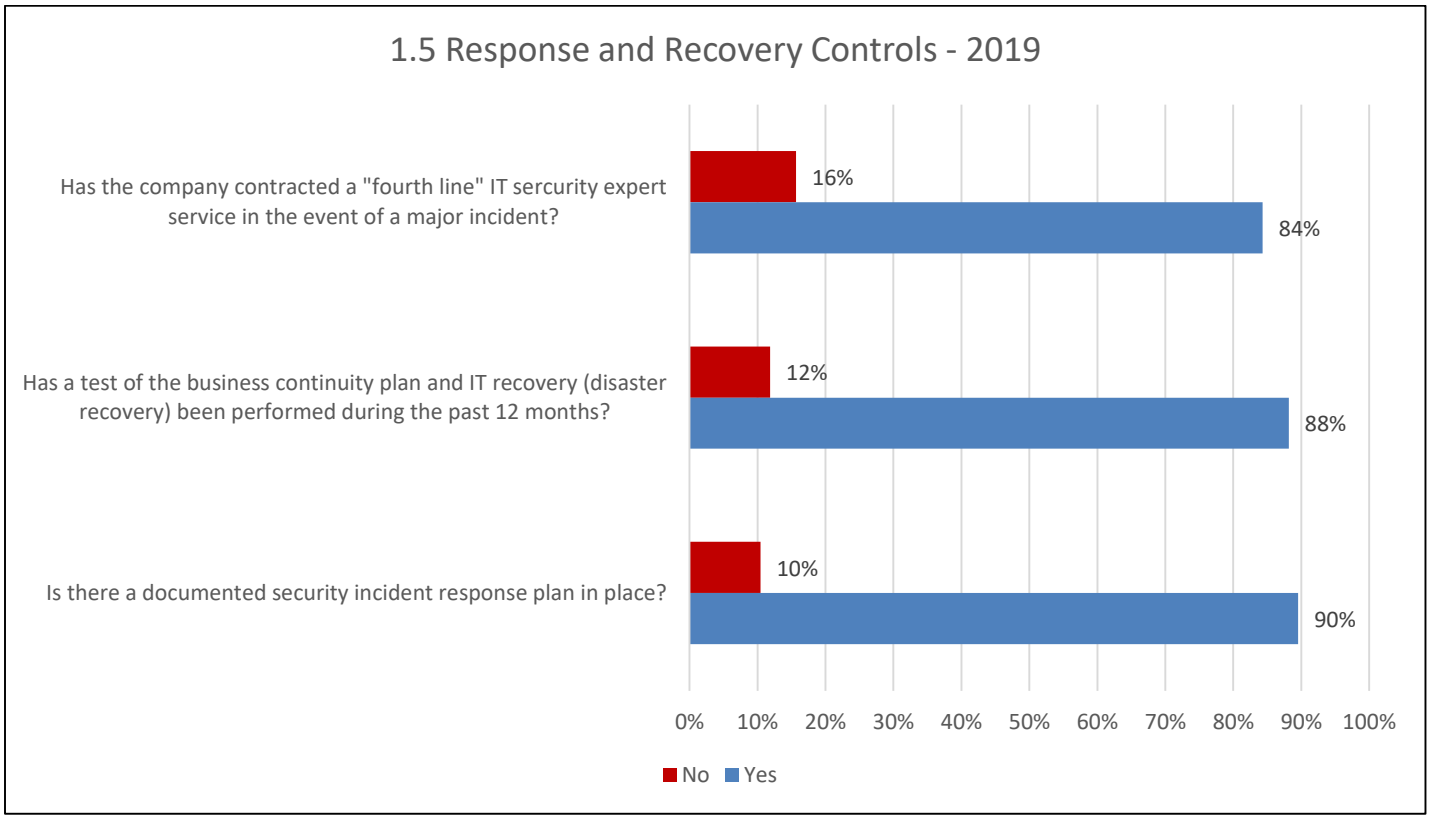
1.4 Detect and Protect Controls



Security configuration standards: The data reveals that 86% of commercial insurers reported they document, implement and enforce security configuration standards to all hardware and software assets on the network.

DLP: Graph 1.4 illustrates that 71% of commercial insurers reported that DLP controls were in place (i.e., controls to prevent data leaving the enterprise in an unauthorised manner). Incidents resulting in data breach often lead to both financial loss and reputational damage. DLP requirements should be assessed against data criticality, regulatory and contractual requirements.

1.5 Response and Recovery Controls



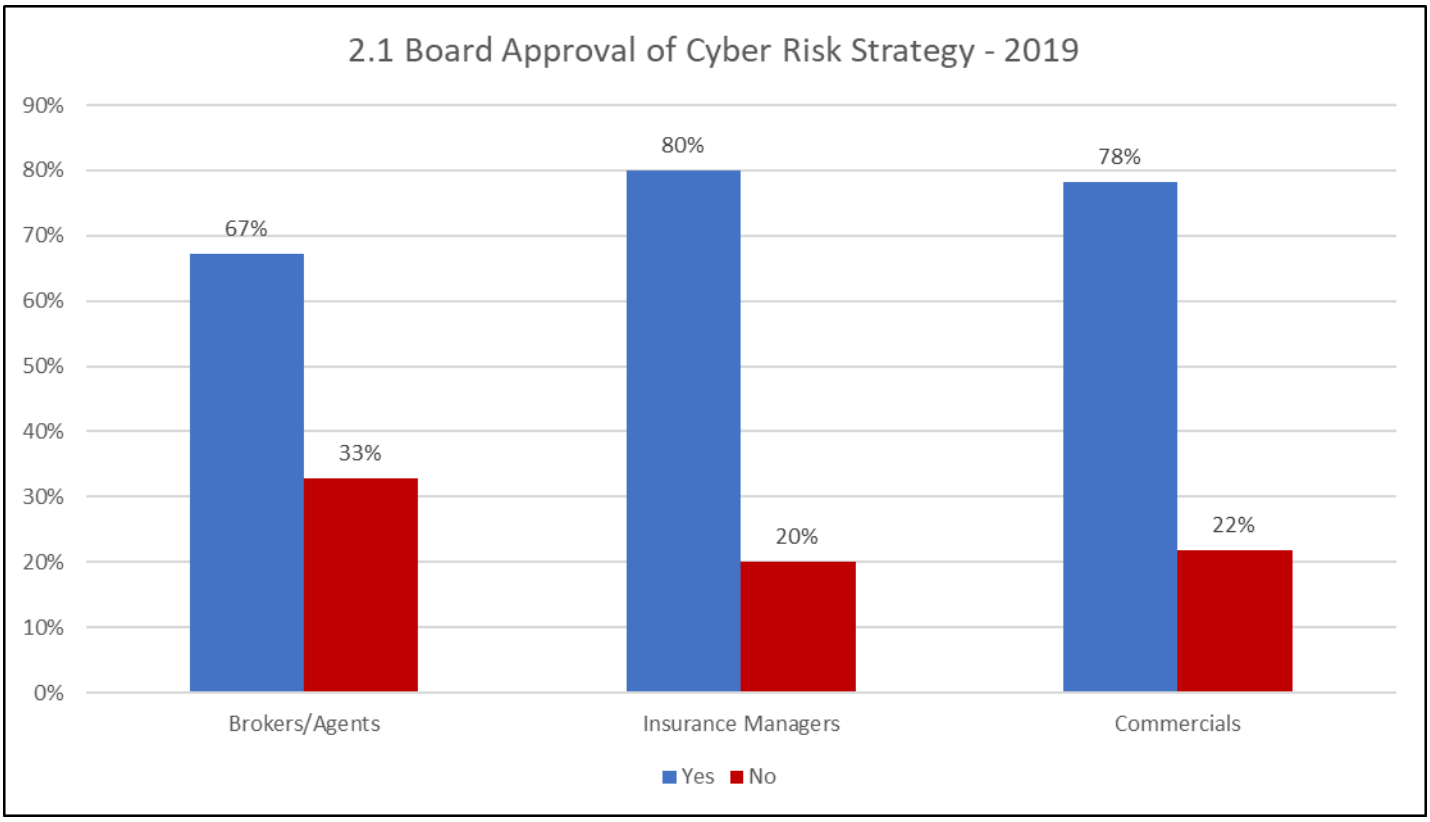
Security incident response plans: Of commercial insurer respondents, 90% reported a security incident response plan in place. Scenario-based or "tabletop" response exercises should be held to test the processes in place and prepare for any real incidents that may occur.

Testing BCP and IT DR Plans: Graph 1.5 reveals that 88% of commercial insurers had tested their BCP and IT DR plans in the preceding 12 months.

2. Assessment of Data – Brokers and Agents, Insurance Managers and Commercial Insurers

This section is based on data from the 2019 filing returns completed by brokers, agents, insurance managers, and commercial insurers.

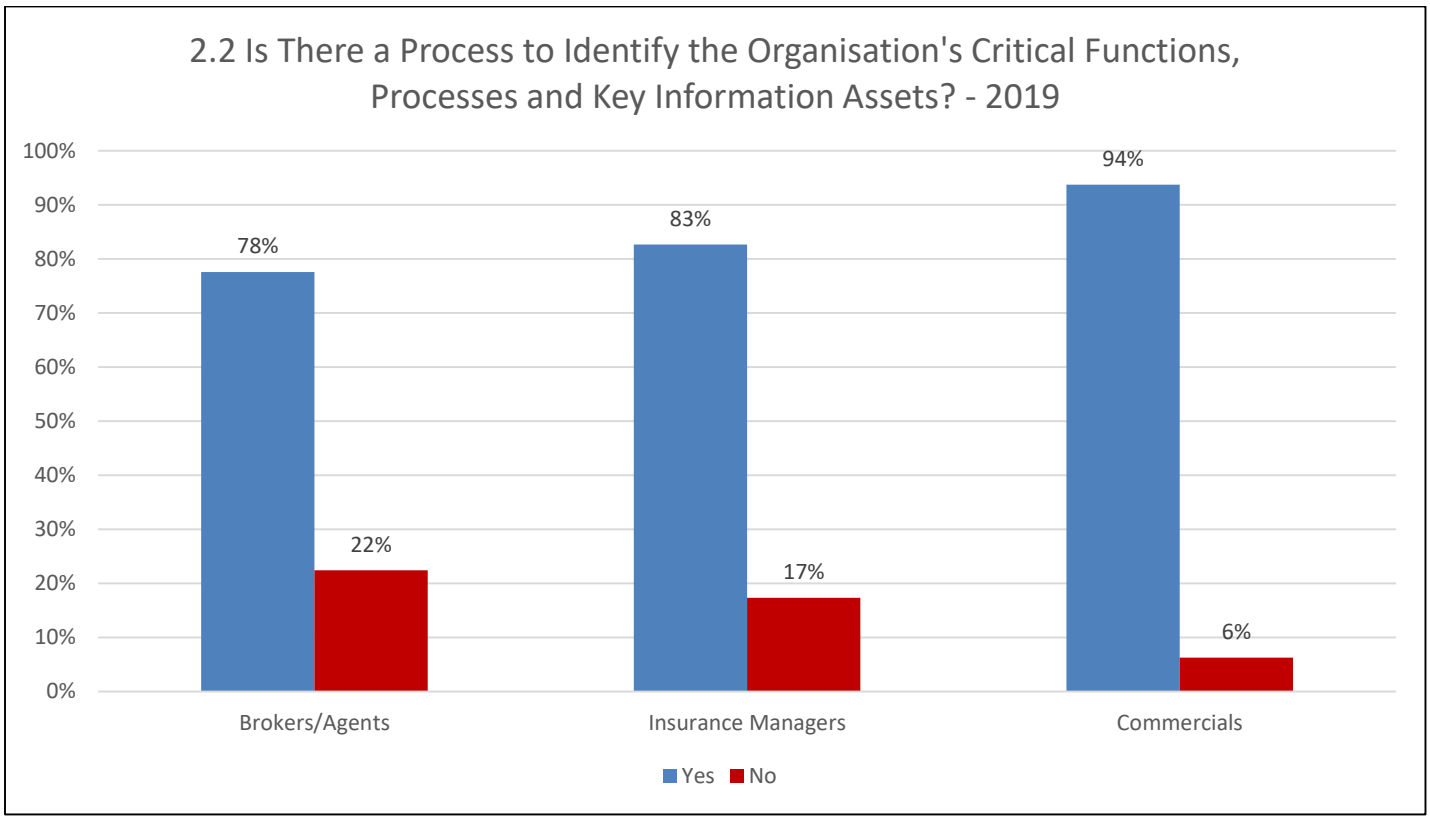
2.1 Board Approval of Cyber Risk Strategy



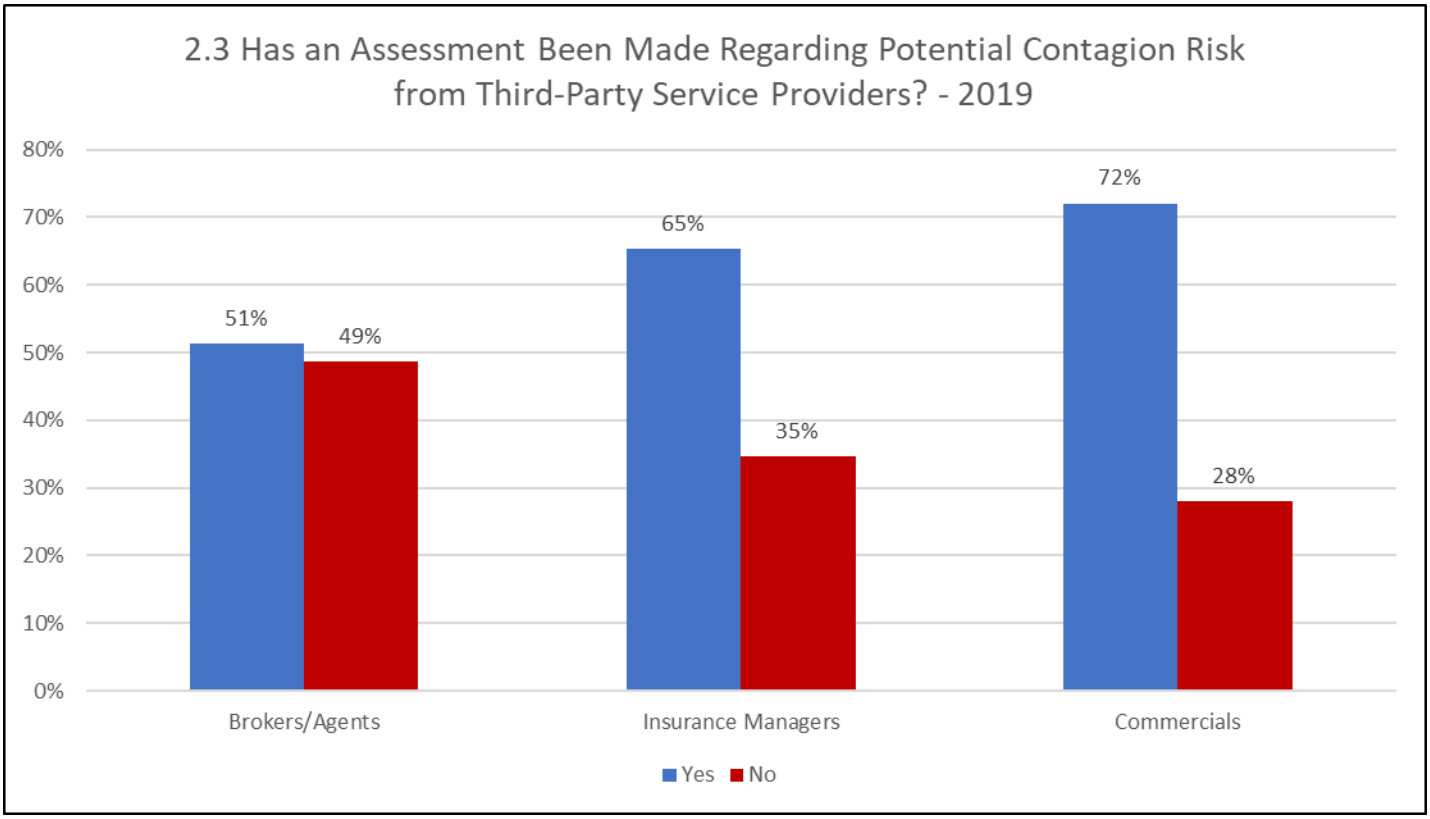
The board of directors and senior management team must have oversight of the cyber risk strategy. An average of 75% of respondents reported that they have board approval of their cyber risk strategy.

2.2 Identification of Critical Business Continuity Requirements

An average of 79% of respondents has identified critical business continuity requirements. This includes holding regular, documented business impact analysis exercises to determine the criticality of business process and recovery and the likely impact resulting from different disaster scenarios. Business Continuity and Disaster Recovery plans should be tested on a regular basis.

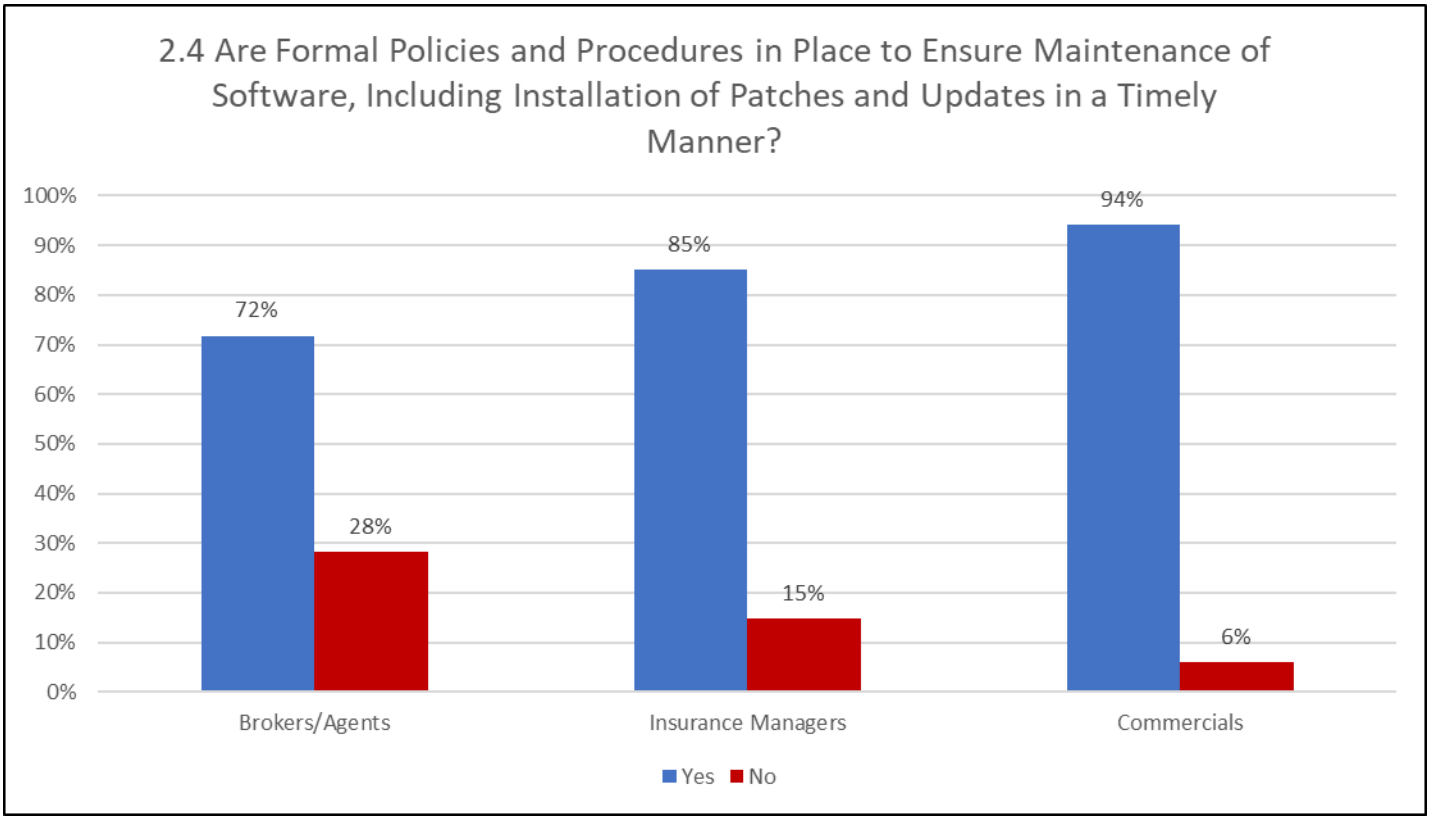


2.3 Cyber Risk Assessment of Third Parties



An average of 62% of respondents reported that they had assessed risks from their third-party providers, which is lower than anticipated. Computer networks are only as secure as their weakest link. Where the registrant outsources IT services, the registrant must ensure there is sufficient oversight and governance in place.

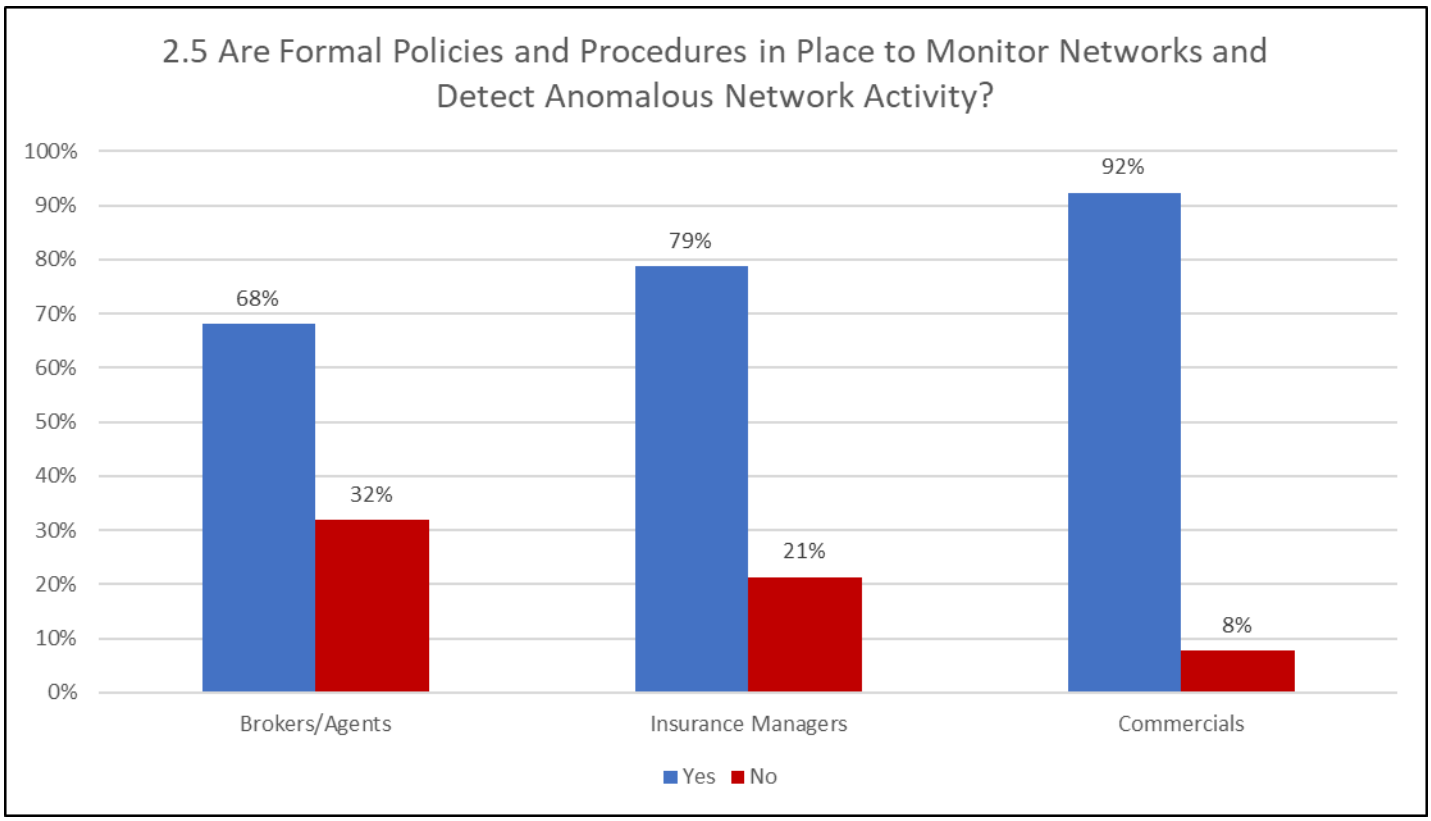
2.4 Formal Policies and Procedures to Ensure Maintenance of Software (Including Patches and Updates)



An average of 83% of respondents confirmed that they are patching systems in a timely manner. The maintenance of software versions and patching is one of the requirements of vulnerability management. Policies and procedures should be in place to formalise this activity.

2.5 Monitoring of Anomalous Network Activity

An average of 79% of companies reported that they monitor their networks to detect anomalous activity that may be malicious. The anomalous activity must be detected and investigated in order to understand the potential risk to the network. Network security tools should be used to detect network intrusions and to provide alerts when an intrusion occurs.


2.5 Are Formal Policies and Procedures in Place to Monitor Networks and Detect Anomalous Network Activity?
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
68%
32%
79%
21%
92%
8%
Brokers/Agents
Insurance Managers
Commercials
Yes
No