BMA
BERMUDA MONETARY AUTHORITY

Bermuda Insurance Sector Operational Cyber Risk Management — 2022 Report

Contents

ABOUT THE AUTHORITY

The Bermuda Monetary Authority (Authority or BMA) 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 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 and the Bermuda Credit Union.

BACKGROUND

This report is based on the enhanced 2021 Bermuda Solvency Capital Requirement (BSCR) cyber filing returns. The BMA issues this communication to provide insights on the information obtained in the 2021 year-end filing from insurance managers, commercial insurers, brokers and agents.

EXECUTIVE SUMMARY AND KEY FINDINGS

The Authority is pleased with industry's continued focus on cyber risk. The 2021 data indicates that overall, the industry's cyber risk posture is improving year on year. Nevertheless, for some cyber risks, a lower-than-expected percentage of insurers have controls in place. These areas are:

1. **Network security Defence in Depth (DiD) controls** (a multi-layered approach) — the following controls are a snapshot of network security best practices:

    - Regular firewall ruleset reviews
    - Network segregation
    - Regular penetration testing
    - Regular external vulnerability scanning

    The 2021 data suggests that some entities would benefit from reviewing their network security risks and the status of their corresponding controls. Although this finding was not included in the 2021 report covering 2020 data, the subsequent collection of more detailed data has resulted in this finding.

2. **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 Information Technology (IT) services, should consider having contractual clauses in place to ensure its security requirements are met. Only 79% of entities have reviewed the cyber risk associated with their third-party IT providers in the last 12 months. Although this is an improvement over the 60% reported in 2020, the overall percentages have room for further improvement. Please refer to graph 1.3 for a year-on-year comparison.

3. **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. Only 66% of respondents have completed the classification of their data. This is largely unchanged from the 65% reported in both 2020 and 2019.

4. **Data Loss Prevention (DLP) controls** — registrants must perform an assessment of their DLP control requirements and implement controls to prevent data from leaving the enterprise in an unauthorised manner. Incidents resulting in data breaches often lead to financial loss and reputational damage. DLP requirements should be assessed against data criticality and regulatory and contractual requirements. Only 80% of entities stated they have DLP controls in place. Although the trend is up compared to 71% in 2019 and 77% in 2020, overall percentages are still lower than expected.

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

The final version of the Code was published in October 2020. The Code came into effect on 1 January 2021 and became enforceable on 1 January 2022.

The Code is designed to promote the stable and secure management of regulated entities' IT systems. The Authority is not adopting a 'one-size-fits-all' approach. It expects cyber risk controls to be proportional to the organisation's nature, scale and complexity. The BMA acknowledges that some entities will use a third party to provide technology services and 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 events to the Authority. Complete guidance on the requirements is given in section 6.5 of the Code.

It should be noted that only cyber-reporting events resulting in a significant adverse impact on 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 there is either a determination or confirmation of an event.

An incident report containing known details of the incident, the root cause, actions taken to minimise the impact and any actual adverse impact to the organisation must be submitted within 14 days of the initial incident notification date. If the full root cause is not known by the 14-day submission, the Authority may request further information or the full root cause report when the entity concludes investigations.

Cyber reporting events are treated in complete confidence. The Authority analyses reported events, and this data is used as one of the inputs for cyber risk profiling. The Authority places high importance on keeping up to date with the fast-changing nature of cyber risks and their potential impact on registrants and the insurance sector as a whole.

Key Findings from Cyber-Reporting Events Reported in 2021

1. E-mail is commonly targeted successfully by malicious attackers.

2. Data breaches include e-mail breaches where unstructured data is exfiltrated from an entity. When data is 'unstructured' (i.e., not arranged in a pre-set schema, and therefore, not stored in a traditional database), it leads to a situation where it is not known what data has been exfiltrated, to whom that data belongs or who should be notified of the breach under contractual law and the relevant regulatory requirements.

3. Poor security testing practices lead to undetected vulnerabilities, which attackers then exploit.

4. Security incidents are impacting third-party IT service providers. The trend continues to be businesses utilising different cloud services including Software as a Service (SaaS) solutions. Business processes are also being outsourced. Examples include processes related to 'know your customer', customer service operations, human resources services and IT services.

   The two most common attack vectors that impact third-party provided IT services are:

   a) Attacking the administrative accounts of IT administrators to gain access into a network; and

   b) Attacking the weaknesses of internet-facing systems. Once access is gained, the target is most often Personally Identifiable Information (PII) or gaining access to financial systems for financial gain.

5. Ransomware continues to be a threat. Successful ransomware attacks have led to the encryption of both desktop and server infrastructure, leading to the loss of availability of systems. Note that ransomware is also sometimes associated with attempts to exfiltrate data.

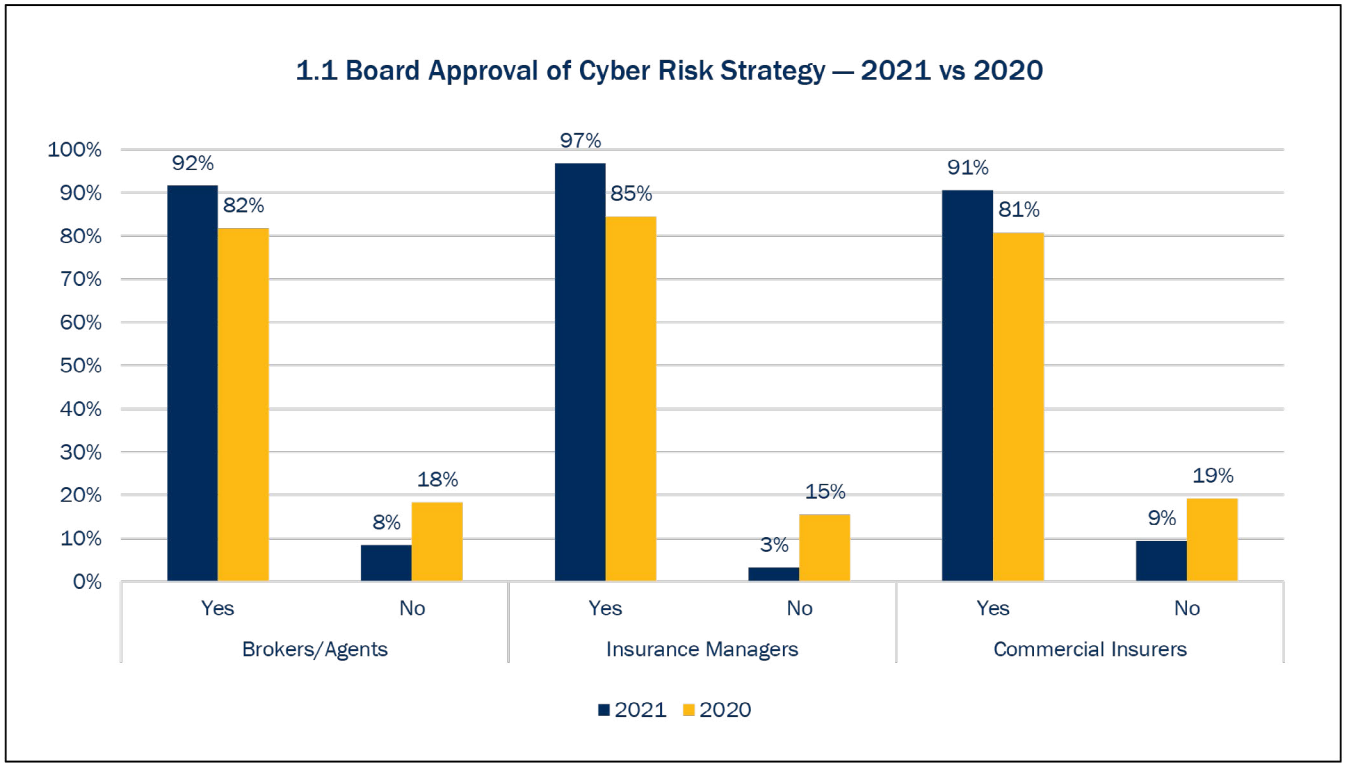
Next the Authority will:

- Continue to monitor the evolving nature of the cyber risk threat landscape
- Continue to assess cyber risk filing returns
- Propose and introduce ways to streamline the cyber risk filing return
- Continue to review cyber reporting events to further understand the risk profile of individual insurers and the sector as a whole
- Review registrants' compliance with the Code as part of the supervisory review process
- Continue to consult proactively with the insurance sector
- Continue to require that companies clearly detail operational cyber risk in the Commercial Insurer Solvency Self-Assessment/Group Solvency Self-Assessment process

1 Analysis of Filing Return Data 2021 – Brokers and Agents, Insurance Managers and Commercial Insurers

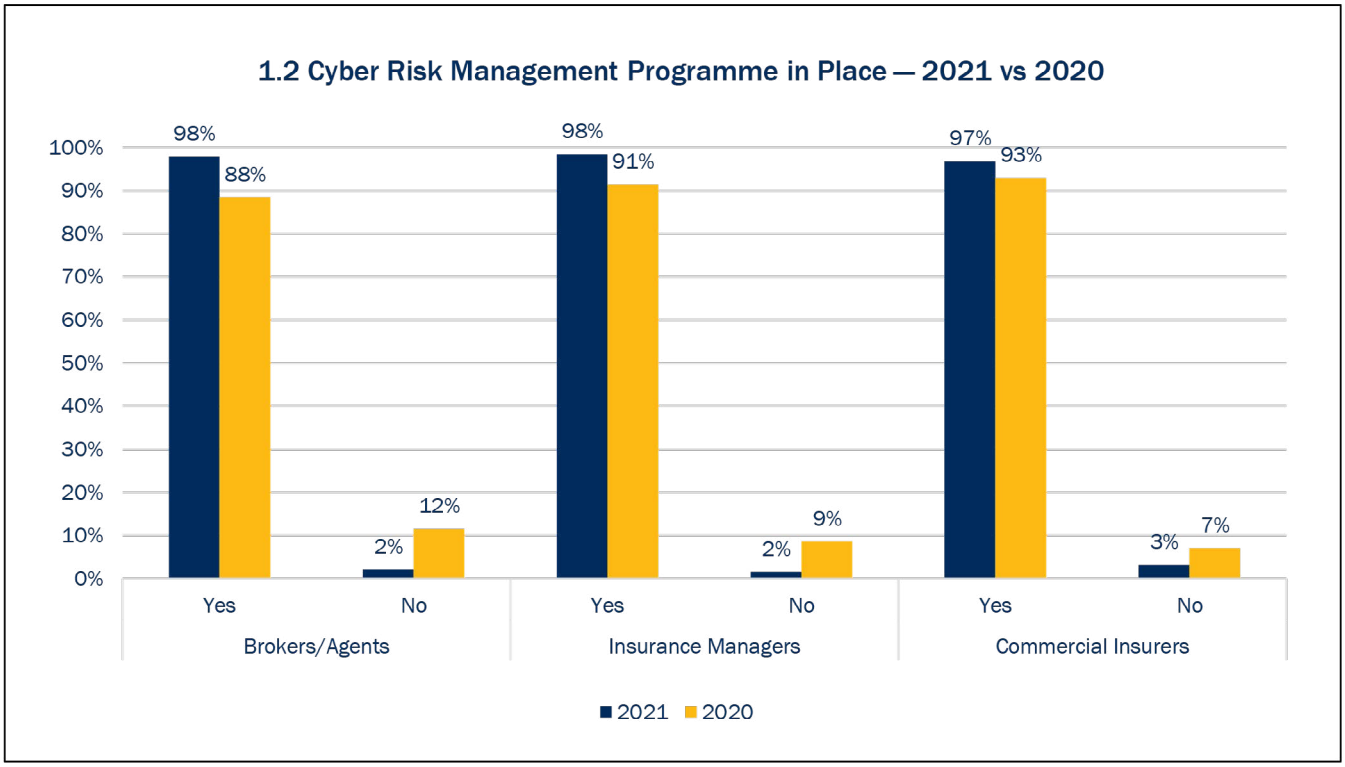
This section is based on 2021 filing returns data, which was completed by brokers, agents and insurance managers, combined with commercial insurers' data to provide an overall insurance sector analysis. The following graphs within this section compare findings from 2021 and 2020 filing returns data, which display a trend of continued improvement in cybersecurity practices across the insurance sector.

1.1 Board Approval of Cyber Risk Strategy



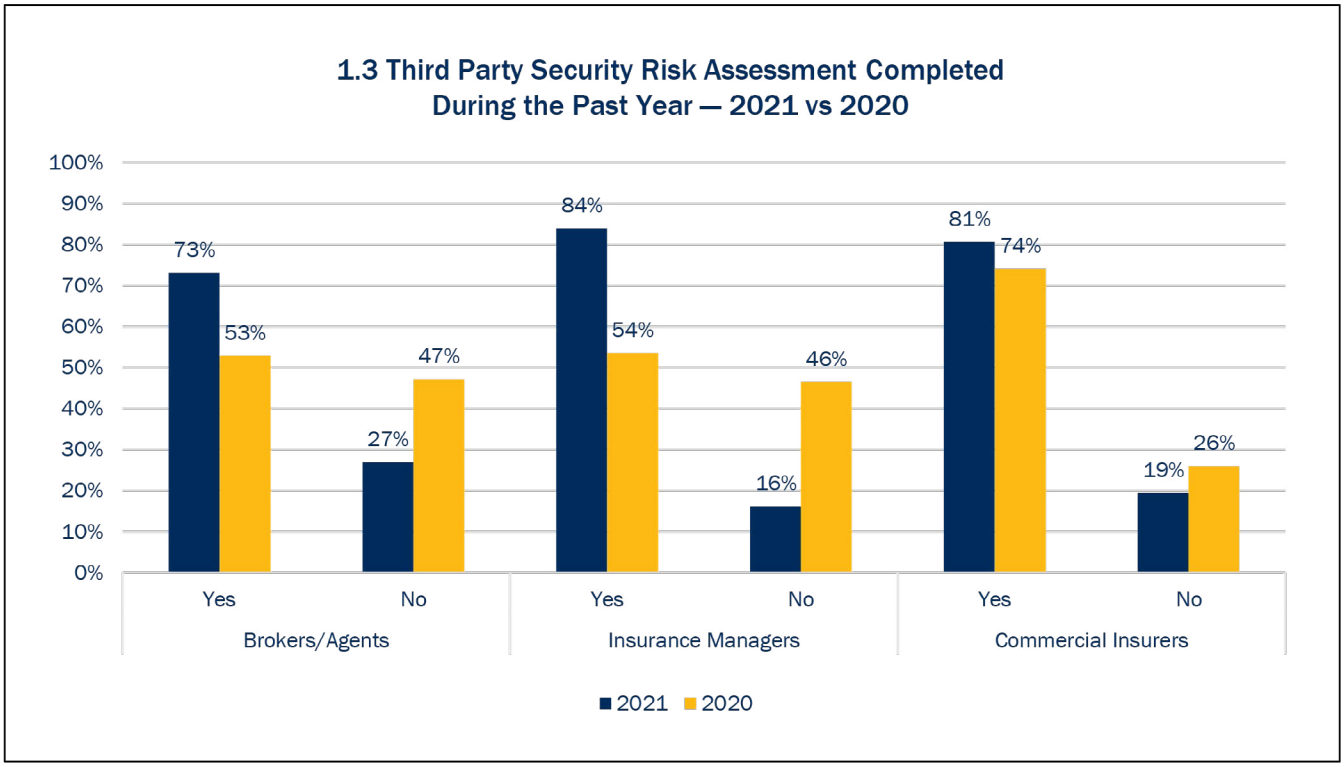
The board of directors and senior management team must have oversight of the cyber risk strategy. An average of 93% (2020 - 82%) of respondents reported that they have board approval for their cyber risk strategy. Nevertheless, the overall percentages are still below expectations. Therefore, inadequate board approval levels for cyber risk strategy remain a key finding.

1.2 Cyber Risk Management Programme



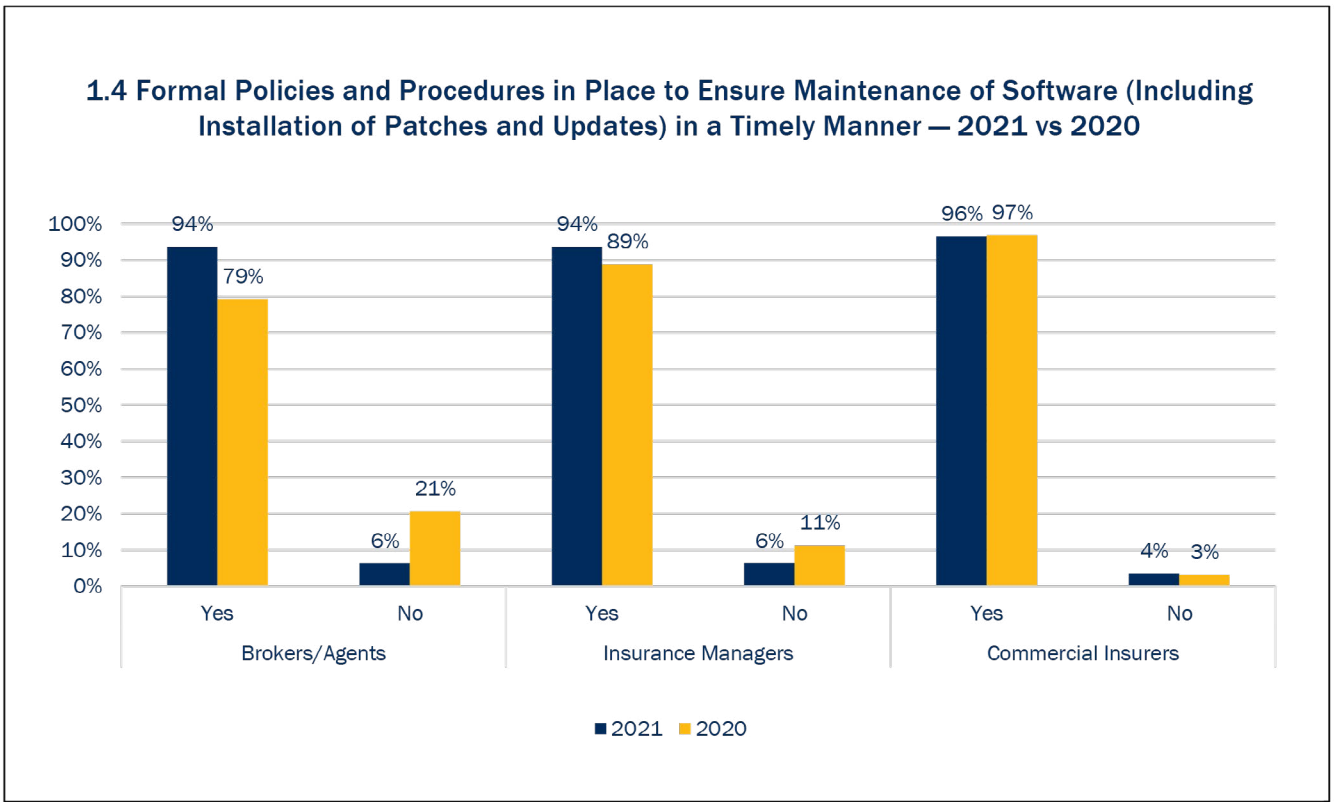
An average of 98% (2020 - 91%) of respondents have identified critical business functions, processes and assets. This is an essential part of determining the continuity requirements of each entity. It includes holding regular, documented business impact analysis exercises to determine the criticality of business processes and recovery and the likely impact resulting from different disaster scenarios. Business Continuity Plans (BCP) and Disaster Recovery (DR) plans should be tested at least annually.

1.3 Cyber Risk Assessment of Third Parties



An average of 79% (2020 - 60%) of respondents reported assessing the cyber risks related to their third-party providers, which remains much lower than anticipated. Computer networks are only as secure as their weakest link. When registrants outsource IT services, they must ensure sufficient oversight and governance are in place.

1.4 Formal Policies and Procedures to Ensure Maintenance of Software



On average, 95% (2020 - 88%) of respondents confirmed that they patch systems in a timely manner. Improvement was noted across the brokers/agents category (up 15%) and insurance managers category (up 5%); however, commercial insurers were down 1%. 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 Analysis of Filing Return Data — Commercial Insurers

This section assesses data from the enhanced 2021 BSCR cyber filing returns (Schedule Ve) completed by commercial insurers only.

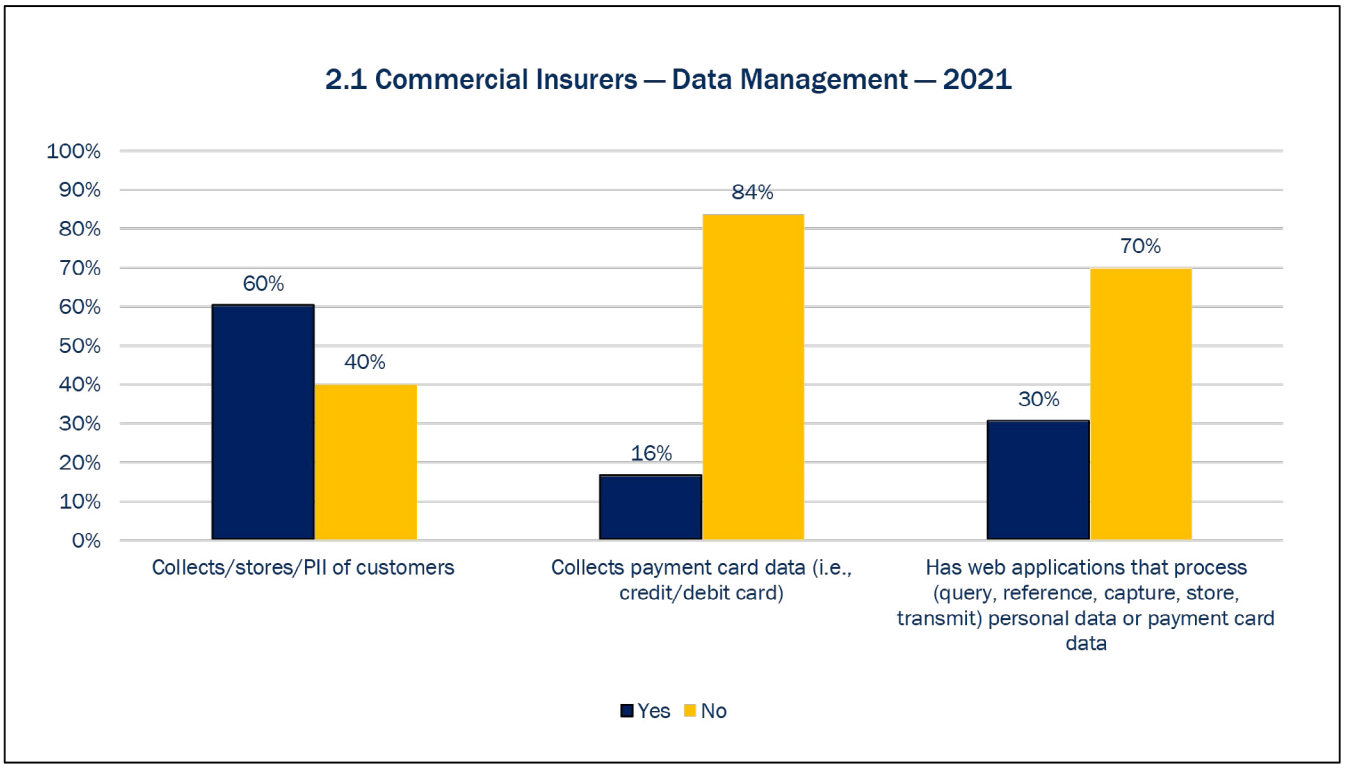
Inherent Risks for Commercial Insurers

Breach of PII — commercial insurers may collect, store and process customer PII. Therefore, its protection is considered a key control requirement. In 2021, 60% of commercial insurers reported collecting, storing and processing customer PII. It was also noted that 16% of commercial insurers reported collecting customer payment card data.

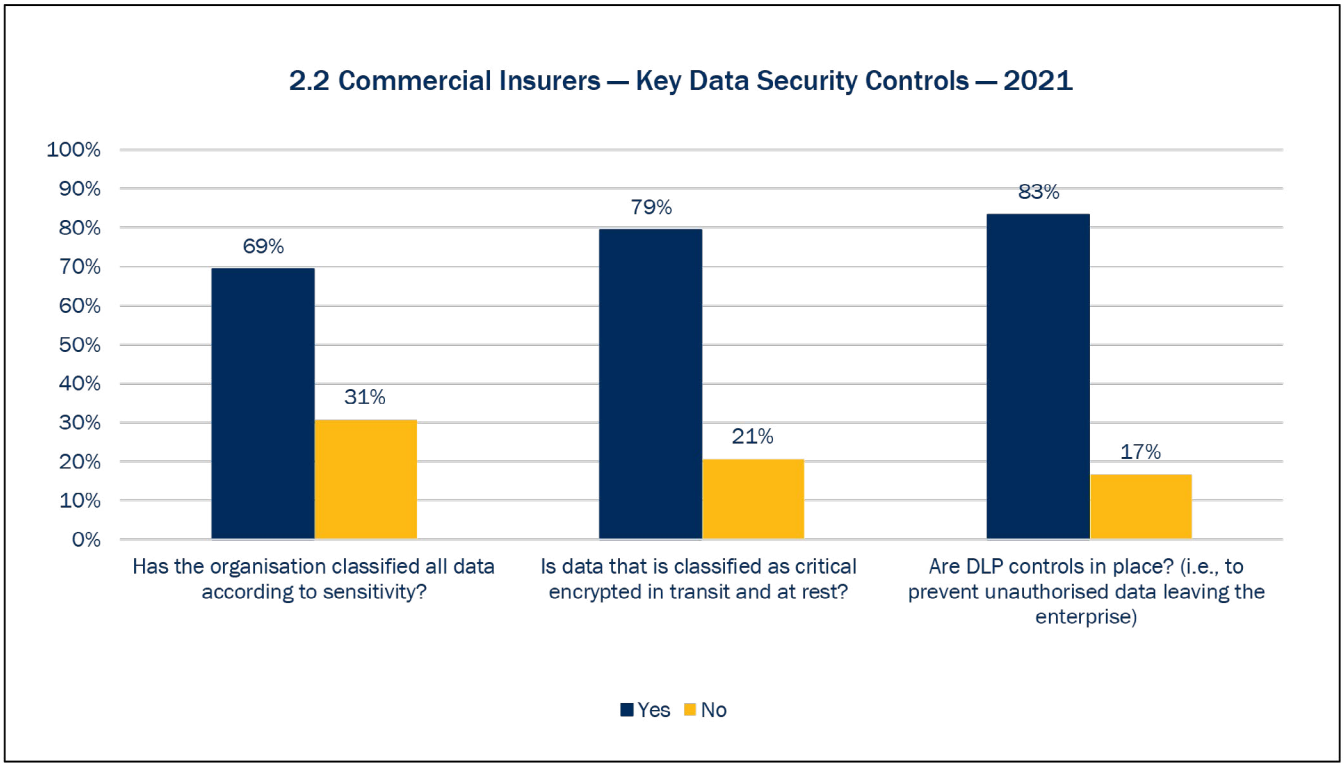
Breach of web applications — commercial insurers also use web applications (i.e., applications hosted on a web server and accessible over the internet). In 2021, 30% of commercial insurers reported using web applications.

Availability of services — the availability of both internal IT services and IT services that provide internet-facing customer services is considered a key risk. The status of some key recovery controls is listed below in section 2.4.

2.1 Data Management



2.2 Key Data Security Controls

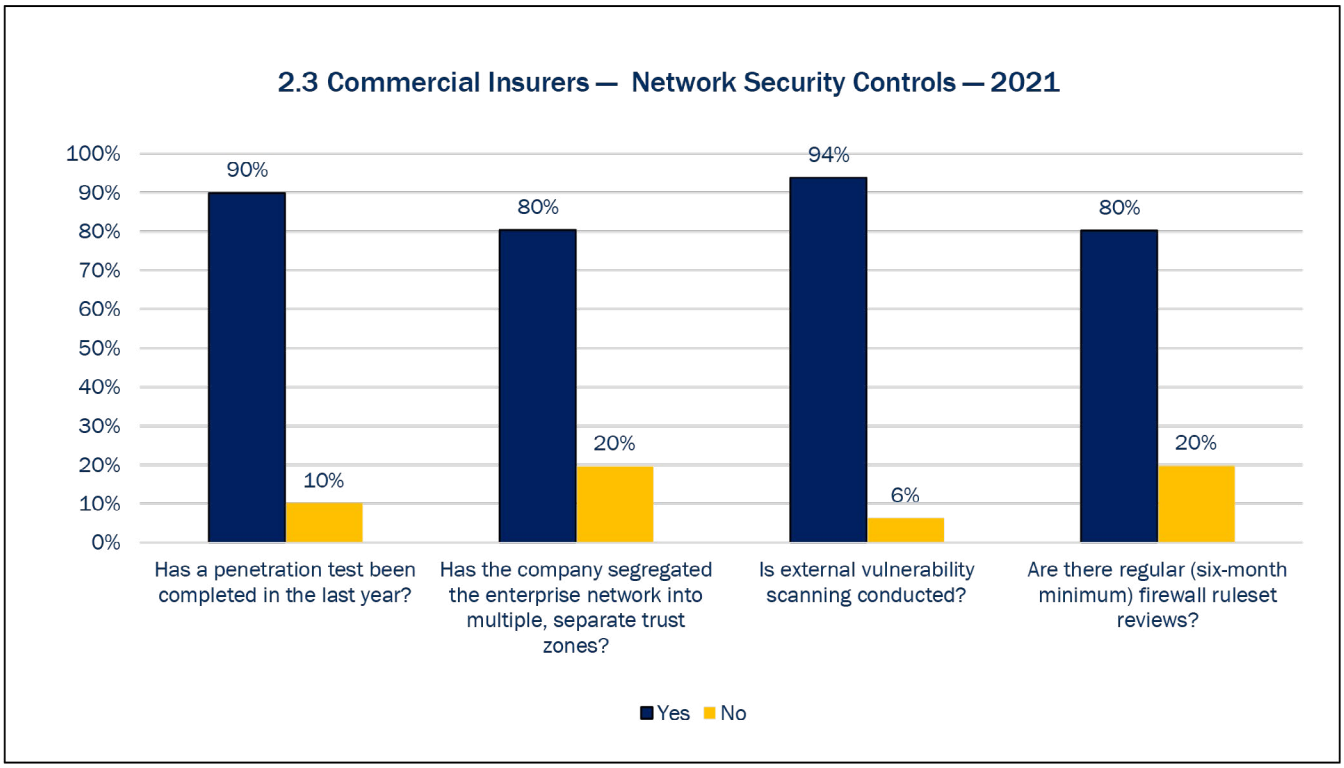


Data classification — it is important that the data processed by insurers is appropriately classified and that data protection controls put in place are commensurate with the level of criticality. This exercise must include data stored by internal IT support services and any outsourced third-party support services. Only 69% of commercial insurers reported that they had completed data classification. This is considered low and commercial insurers should review their risk exposure.

Encryption of data in transit and at rest — this is considered a necessary core security control; however, just 79% of commercial insurers reported that their data is encrypted in transit and at rest. The Code clearly states regulatory expectations for these cyber controls. Commercial insurers should review their risk exposure, controls and compliance with the Code.

DLP — DLP controls can be configured at different layers of a network, for example: email software, internet proxy server and restrictions on port access on end-user devices. DLP controls are required to reduce the risk of accidental and malicious data exfiltration from a network. Only 79% of commercial insurers reported having DLP controls in place. This is considered low and commercial insurers should review their risk exposure.

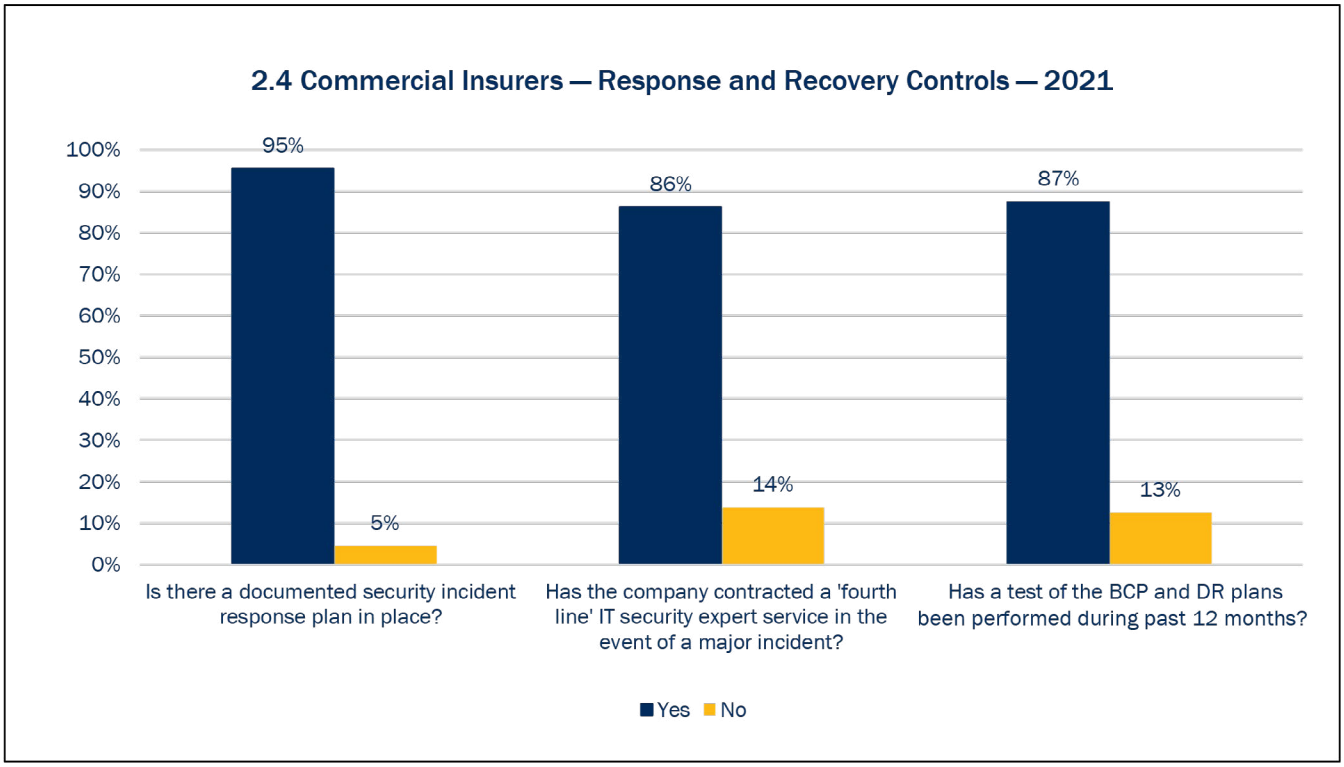
2.3 Network Security Controls



Ensuring that internet-facing systems are secure requires a DiD (or multi-layered approach). The Authority has selected four key controls for analysis.

1. **Penetration testing** — 90% of commercial insurers reported that a penetration test was completed in the last year.
2. **Network segregation** — 80% of commercial insurers reported having network segregation controls in place. This is considered low and commercial insurers should review their risk exposure.
3. **External vulnerability scanning** — 94% of commercial insurers reported that external vulnerability scanning is conducted.
4. **Firewall ruleset review** — 80% of commercial insurers reported reviewing their firewall rulesets every six months. This is considered low and commercial insurers should review their risk exposure.

2.4 Response and Recovery Controls



Security incident response plan — 95% of commercial insurers reported that a documented security incident response plan was in place. These include communication plans for internal and external stakeholders and a defined crisis management process.

Contracted fourth-line IT security expert service — in the event of a major cyber incident, these Subject Matter Expert (SME) services would typically provide expert assistance in mitigating impact and recovering to normal business operations. Commercial insurers contracting a security expert service was reported by 86% of respondents.

BCP test and DR test — 87% of commercial insurers reported that a BCP and DR test had been completed in the last 12 months. BCP and DR plans should be tested at least annually.

3 Analysis of Filing Return Data 2021 – Insurance Managers

Inherent Risks for Insurance Managers

Insurance managers typically provide IT services to other entities on an outsourced basis. They provide these services to multiple limited-purpose insurers, including captive insurance entities. Insurance managers may operate their internal business unit operations on a network segregated from the managed service platform.

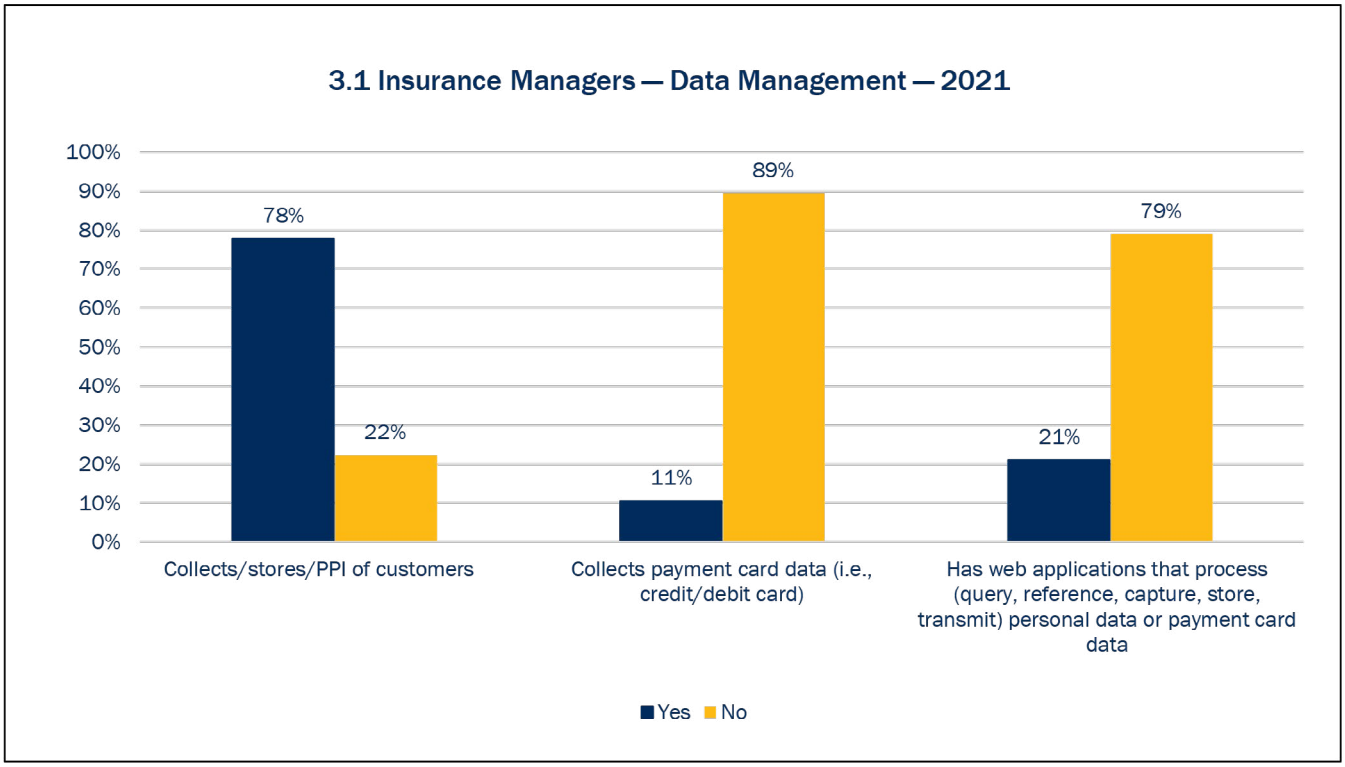
Contagion — there is an inherent risk of contagion where an incident impacts an entity on the managed service platform. This incident could spread and impact other entities. In addition, contagion could occur between the insurance manager's internal operations and the managed service platform.

Breach of PII — insurance managers typically collect, store and process customer PII; therefore, its protection is considered a key control requirement. As per 3.1 below, in 2021, 78% of the insurance managers reported collecting, storing and processing customer PII (this includes PII stored on behalf of client entities). It was also noted that only 11% of insurance managers reported they collect customer payment card data.

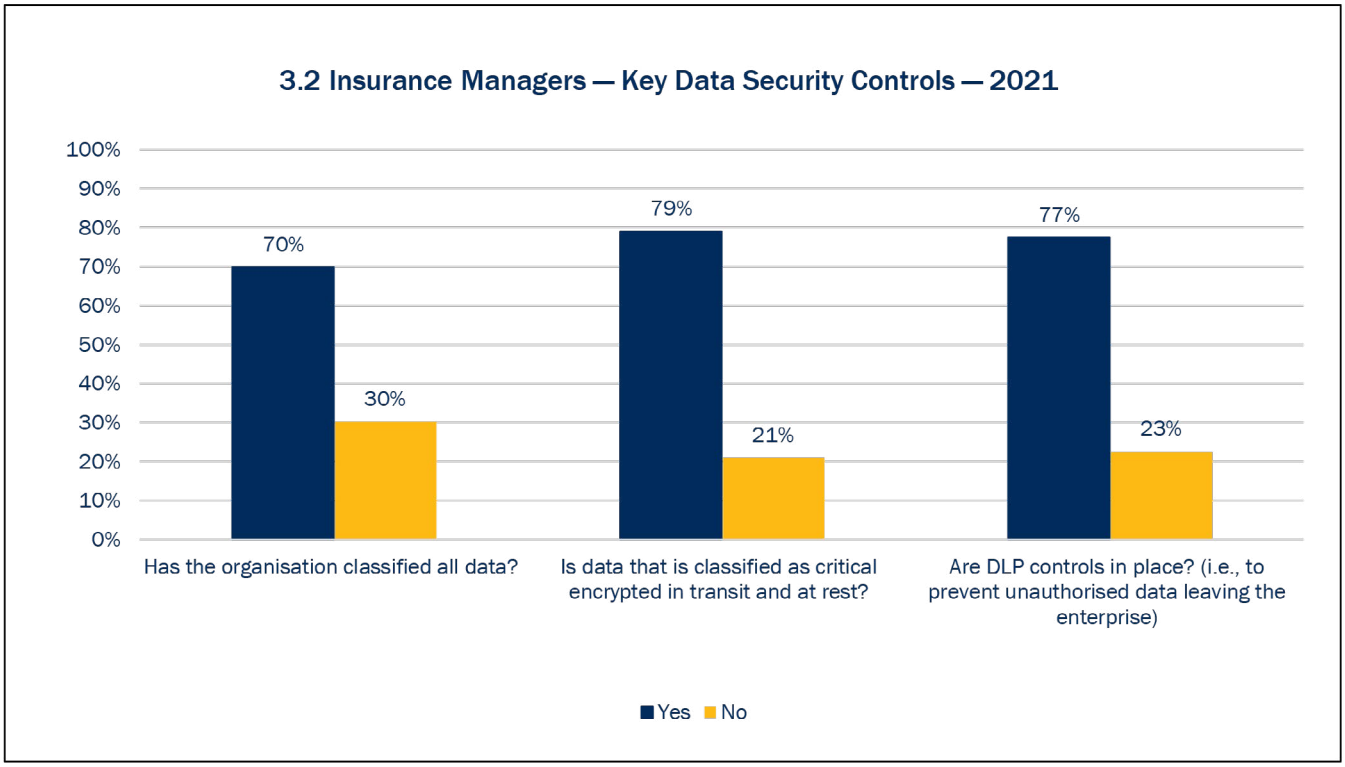
Breach of web applications — insurance managers also use web applications (i.e., applications hosted on a web server and accessible over the internet). As per 3.1 below, in 2021, just 21% of insurance managers reported using web applications.

Availability of services — the availability of services hosted for entities is a key risk for insurance managers. The status of some key recovery controls is listed below in section 3.4.

3.1 Data Management



3.2 Key Data Security Controls

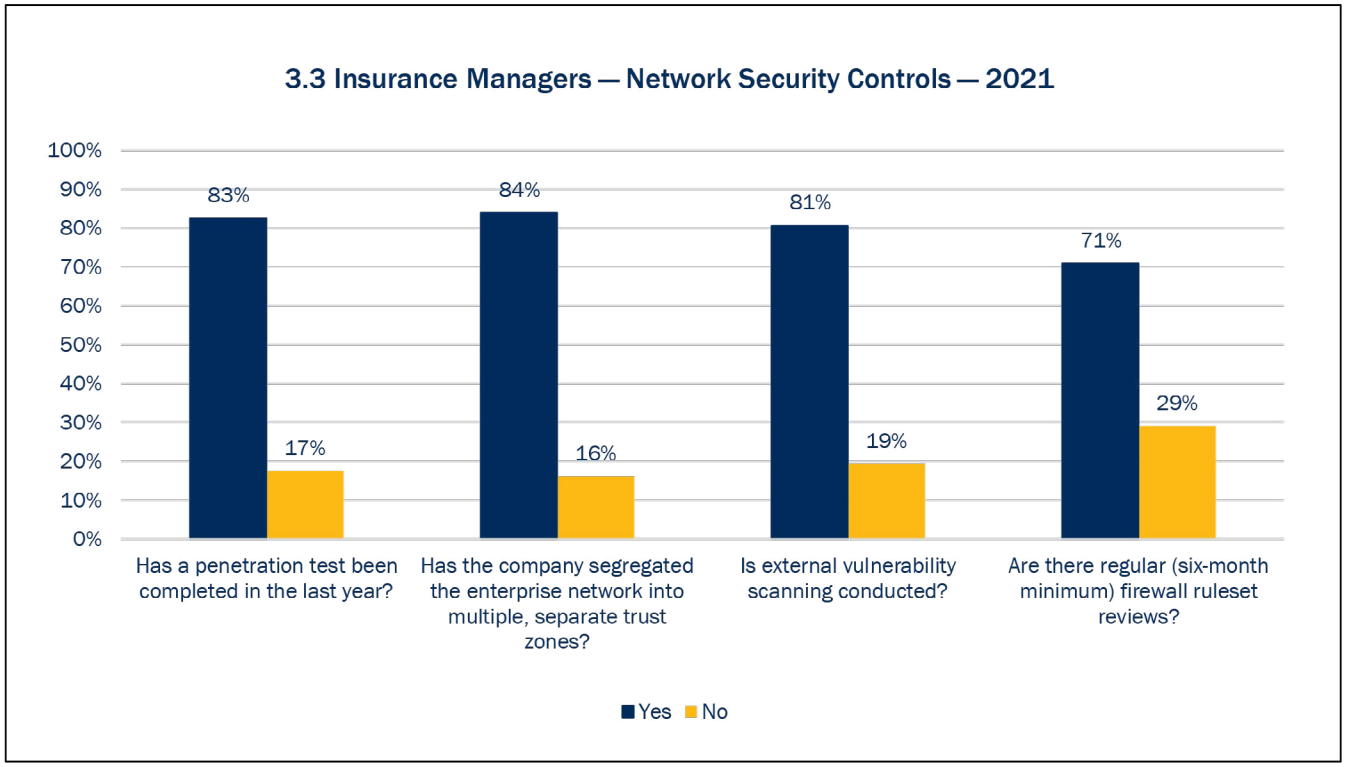


Data classification — it is important that the data processed by insurers is appropriately classified and that the data protection controls put in place are commensurate with the level of criticality. This exercise must include data stored by internal IT support services and any outsourced third-party support services. Only 70% of insurance managers reported that they had completed data classification. This is considered low, and insurance managers should review their risk exposure.

Encryption of data in transit and at rest — this is considered a basic necessary security control; however, just 79% of insurance managers reported that their data is encrypted in transit and at rest. The Code clearly states regulatory expectations for these cyber controls. This is considered low, and insurance managers should review their risk exposure.

DLP — DLP controls can be configured at different layers of a network, for example: email software, internet proxy server and restrictions on port access on end-user devices. DLP controls are required to reduce the risk of accidental and malicious data exfiltration from a network. Only 77% of insurance managers reported having DLP controls in place.

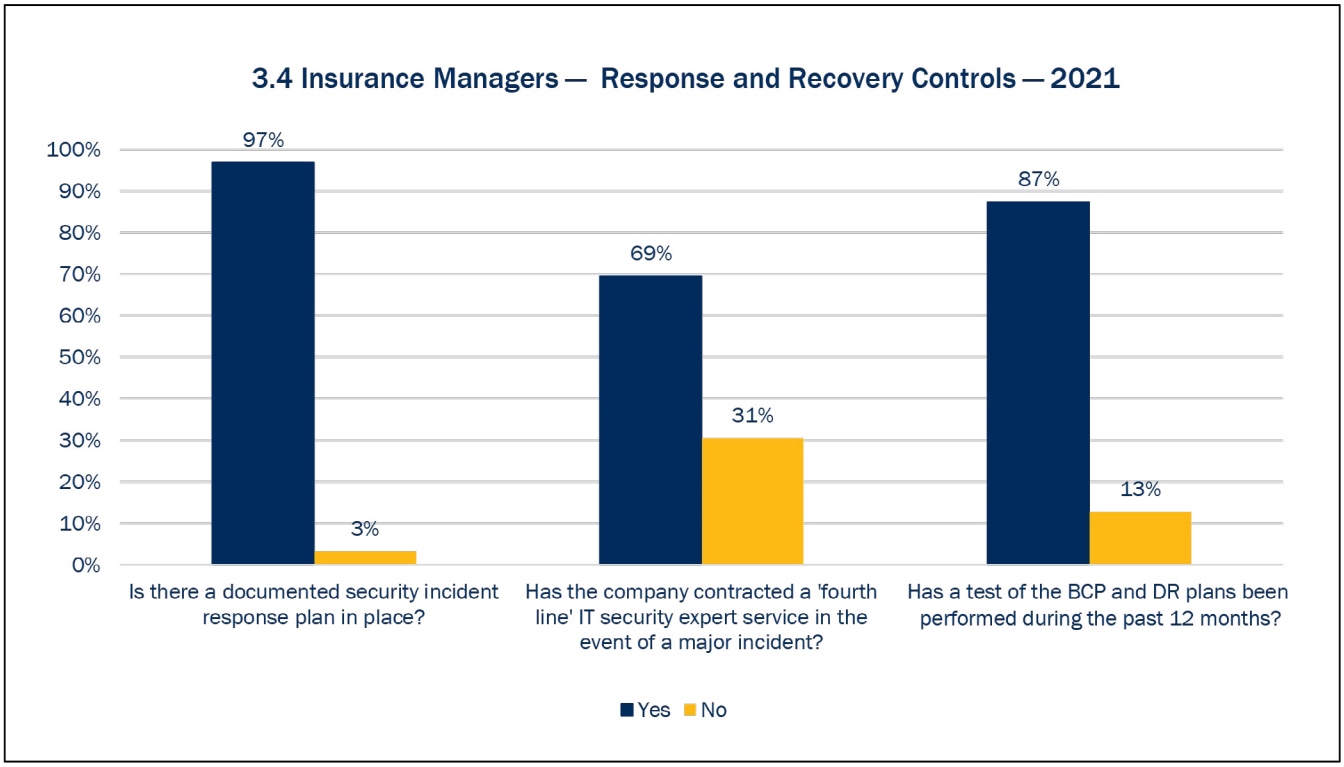
3.3 Network Security Controls



Ensuring that internet-facing systems are secure requires a DiD (or multi-layered approach). The Authority has selected four key controls for analysis of insurance managers' network security controls:

1. **Penetration testing** — 83% of insurance managers reported that a penetration test had been completed in the last year. This is considered low, and insurance managers should review their risk exposure;
2. **Network segregation** — 84% of insurance managers reported having network segregation controls in place. This is considered low, and insurance managers should review their risk exposure;
3. **External vulnerability scanning** — 81% of insurance managers reported that external vulnerability scanning is conducted. This is considered low, and insurance managers should review their risk exposure; and
4. **Firewall ruleset review** — 71% of insurance managers reported reviewing their firewall rulesets every six months. This is considered low, and insurance managers should review their risk exposure.

3.4 Response and Recovery Controls



Security incident response plan — 97% of insurance managers reported that a documented security incident response plan was in place. These include communication plans for internal and external stakeholders and a defined crisis management process.

Contracted fourth line security SME service — in the event of a major cyber incident, this SME service would typically provide expert assistance in mitigating impact and recovering to normal business operations. 69% of insurance managers reported a contracted SME service.

BCP test and DR test — 87% of insurance managers reported that a BCP and DR test had been completed in the last 12 months. BCP and DR plans should be tested at least annually.

4 Analysis of Filing Return Data 2021 – Brokers and Agents

Inherent Risks for Brokers and Agents

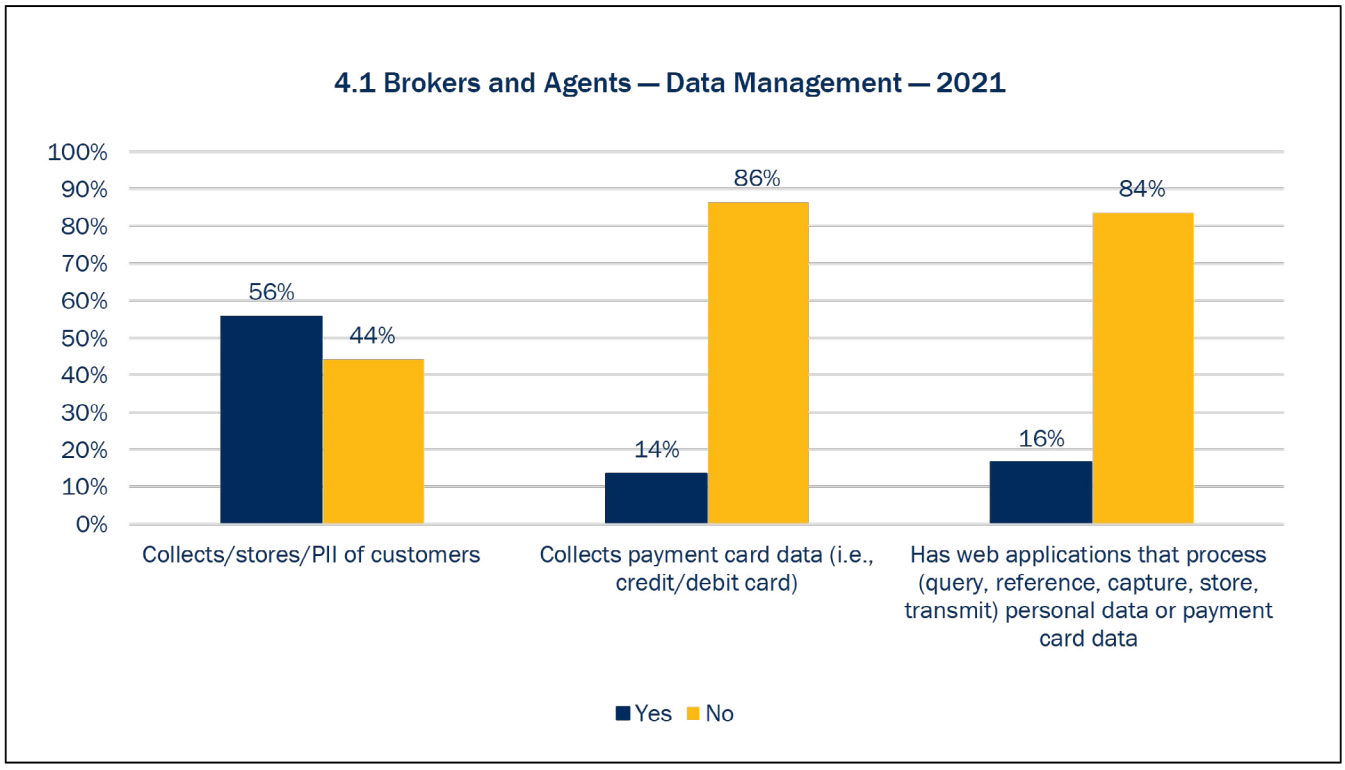
Brokers and agents have different inherent business models. Long-term brokers are more likely to store and process customer PII directly. Agents focusing on underwriting are less likely to store and process customer PII directly. It is acknowledged that brokers and agents vary in size and the number of employees.

Breach of PII — in 2021, 56% of brokers and agents reported collecting, storing and processing customer PII (this includes PII stored on behalf of client entities). It was also noted that 14% of brokers and agents reported collecting customer payment card data. PII data breach is a potential risk.

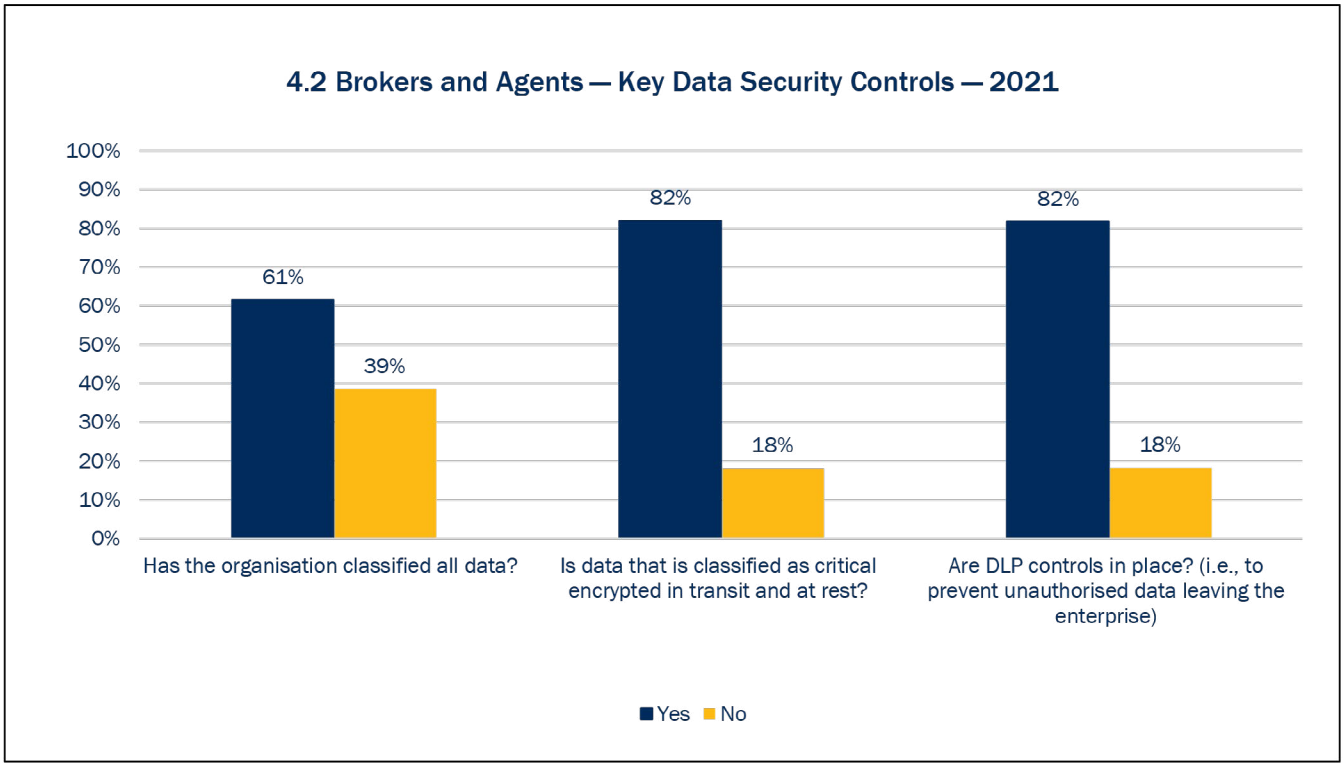
Breach of web applications — brokers and agents also use web applications (i.e., applications hosted on a web server and accessible over the internet). In 2021, 16% of brokers and agents reported using web applications.

Availability of services — the availability of services hosted for entities is a key risk for brokers and agents. The status of some key recovery controls is listed below in section 4.4. The data shows that 22% of brokers and agents had not completed a BCP and IT DR test in the last 12 months.

4.1 Data Management



4.2 Key Data Security Controls

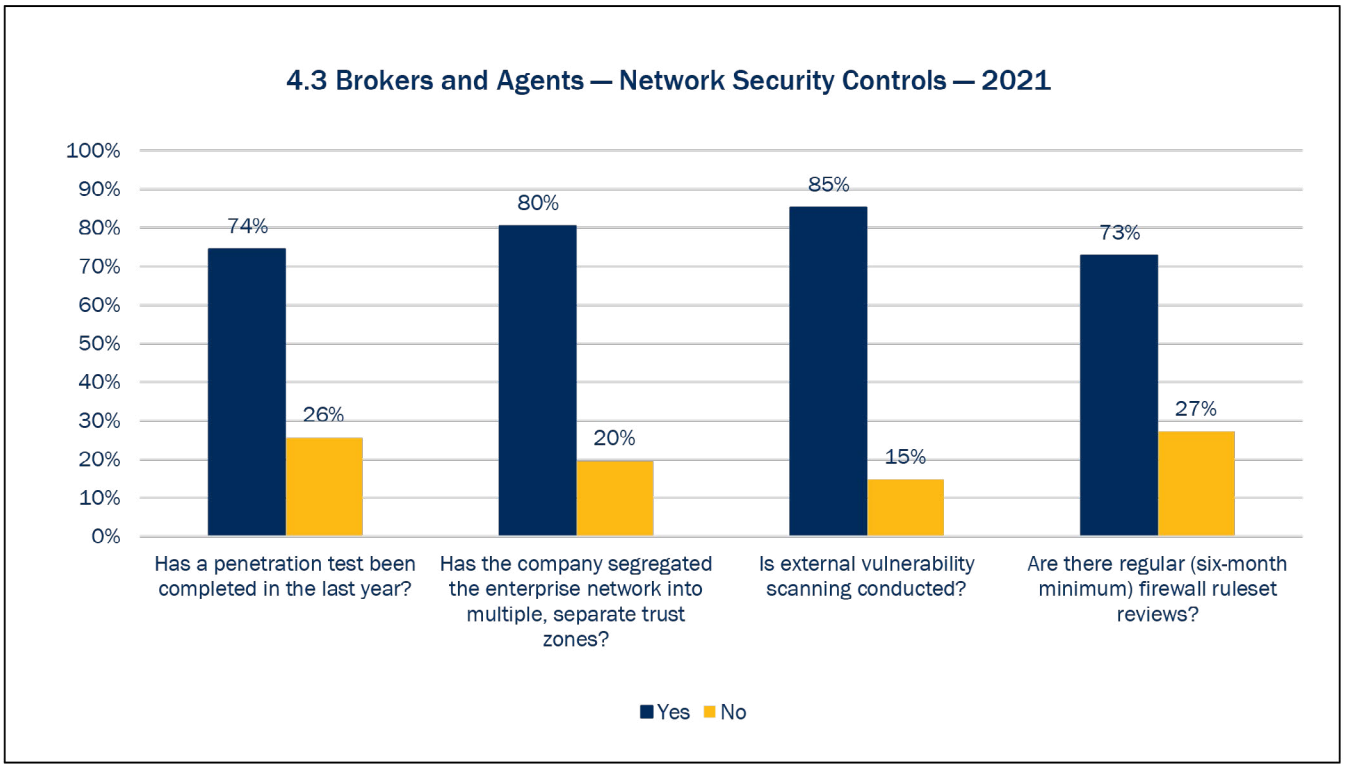


Data classification — it is important that the data processed by insurers is appropriately classified and that data protection controls put in place are commensurate with the level of criticality. This exercise must include data stored by internal IT support services and any outsourced third-party support services. Data collected revealed 61% of brokers and agents reported completing data classification. This is considered low. Brokers and agents should review and enhance their initiatives in this regard.

Encryption of data in transit and at rest — this is considered a basic necessary security control; however, just 82% of brokers and agents reported that their data is encrypted in transit and at rest. This is considered low, and brokers and agents should review their risk exposure.

DLP — DLP controls can be configured at different layers of a network, for example: email software, internet proxy server, restrictions on port access on end-user devices. DLP controls are required to reduce the risk of accidental and malicious data exfiltration from a network. Only 82% of brokers and agents reported that they have DLP controls in place. This is considered low, and brokers and agents should implement adequate DLP controls as it is a requirement of the Code.

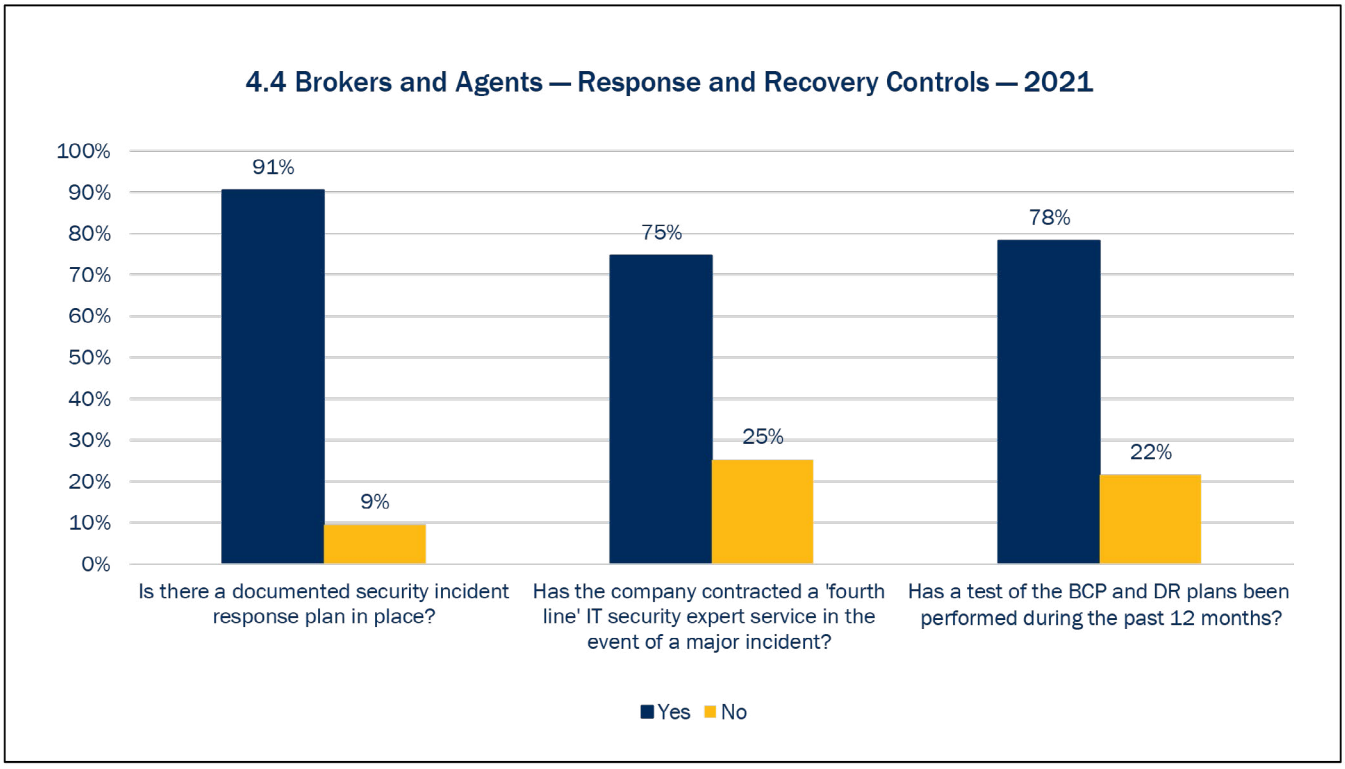
4.3 Network Security Controls



Ensuring that internet-facing systems are secure requires a DiD (or multi-layered approach). The Authority has selected four key controls for analysis of the brokers and agents' network security controls:

1. **Penetration testing** — 74% of brokers and agents reported that a penetration test had been completed in the last year. This is considered low; brokers and agents should review their risk exposure;
2. **Network segregation** — 80% of brokers and agents reported that they had network segregation controls in place. This is considered low; brokers and agents should review their risk exposure;
3. **External vulnerability scanning** — 85% of brokers and agents reported that external vulnerability scanning is conducted. Vulnerability scanning is essential and this figure is considered low; and
4. **Firewall ruleset review** — 73% of brokers and agents reported reviewing their firewall rulesets every six months. This is considered low; brokers and agents should review their risk exposure.

4.4 Response and Recovery Controls



Security incident response plan — 91% of brokers and agents reported having a documented security incident response plan. These include communication plans for internal and external stakeholders and a defined crisis management process.

Contracted fourth line security SME service — 75% of brokers and agents reported having a contracted SME service. This is considered low, as in the event of a major cyber incident this SME service would typically provide expert assistance in mitigating impact and recovering to normal business operations.

BCP test and DR test — 78% of brokers and agents reported that a BCP and DR test had been completed in the last 12 months. This is considered low; brokers and agents should review their risk exposure. BCP and DR plans should be tested at least annually.

Conclusion

The Authority continues to engage closely with the insurance sector and the focus on cyber risk will continue in 2023. The key findings in the executive summary list the main controls that require improvement according to the Authority. Taking into consideration that the business models and inherent risks differ between commercial insurers, insurance managers, and brokers and agents, the report has specific sections breaking down the data and provides analysis on the adequacy of controls for each insurer type to provide further clarity from previous editions. Overall, this report demonstrates that the cyber risk management posture across the sector is steadily improving, reducing the probability of incidents that potentially could cause financial and reputational damage to insurers licensed to operate in Bermuda.

Glossary

BCP — Business Continuity Plan

BMA — Bermuda Monetary Authority

BSCR — Bermuda Solvency Capital Requirement

Code — Insurance Sector Operational Cyber Risk Management Code of Conduct

DiD — Defence in Depth

DLP — Data Loss Prevention

DR — Disaster Recovery

IT — Information Technology

PII — Personally Identifiable Information

SaaS — Software as a Service

SME — Subject Matter Expert

BMA House

43 Victoria Street, Hamilton HM12, Bermuda
P.O. Box 2447, Hamilton HMJX, Bermuda

Tel: 441.295.5278 Fax: 441.292.7471

E-mail: enquiries@bma.bm

www.bma.bm