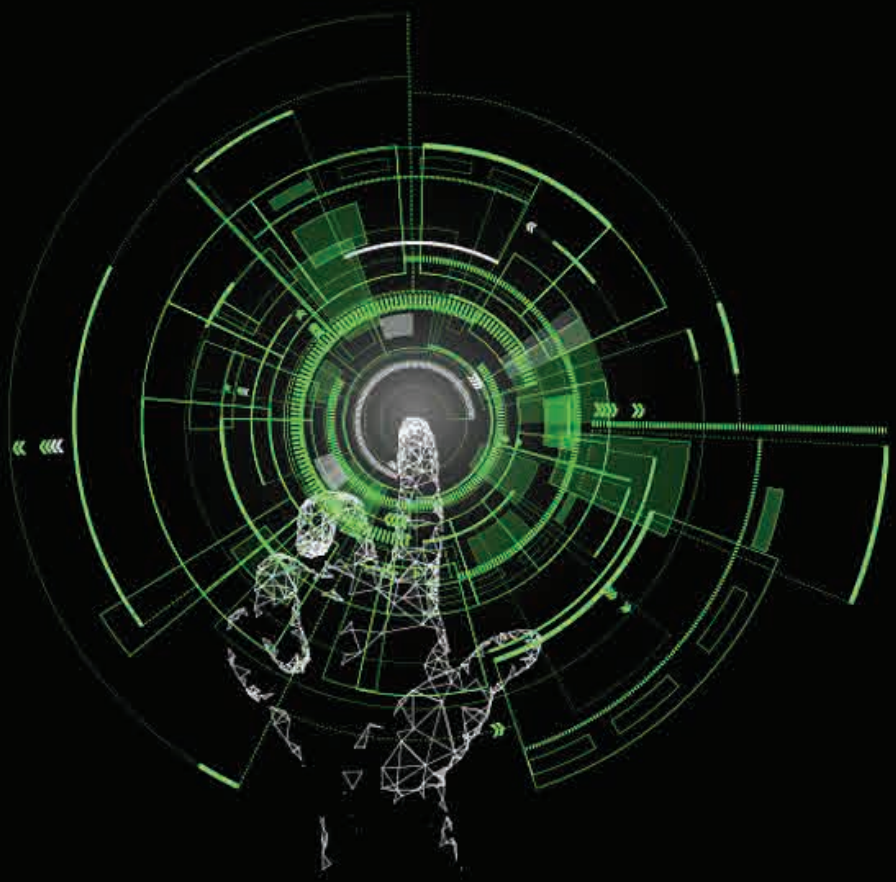
Deloitte.



Keeping an eye on what matters

Cybersecurity Survey for Mozambique

MAKING AN IMPACT THAT MATTERS since 1845

Content

It is with great pleasure that we present the relevant observations of the Deloitte Cybersecurity Survey for **Mozambique**. This survey covers both public and private entities and our aim is for this report to serve as a catalyst for contemplation, in-depth discussions and improvement of cybersecurity awareness and active cyber threat management in the country.

Foreword

With the proliferation of Internet-enabled devices, cyber culture is growing more rapidly than cybersecurity. Everything that depends on cyberspace is potentially at risk. Private data, intellectual property, cyber infrastructure, and even military and national security can be compromised by deliberate attacks, inadvertent security lapses, and the vulnerabilities of a relatively immature, unregulated global Internet.

With the recent increase in remote work due to the COVID-19 pandemic and the increasing use of digital platforms, cyberattacks have multiplied. The Cybersecurity Ventures*, world's leading researcher and publisher on global cyber economy and a trusted source for cybersecurity facts, figures, and statistics, predicts that the* costs of cybercrime will reach USD 10.5 trillion per year by 2025*. Moreover, according to the IMC Group's article, since the beginning of the pandemic, the FBI has reported a 300% increase in cybercrime.*

Reports on cybersecurity point to the growing sophistication of hackers and other adversaries as a particularly intractable problem and some deliberate over whether being secure is even possible in today's rapidly evolving landscape of cyberattacks. *In Mozambique, about 30 government portals were attacked by hackers in February 2022 which has called for further attention to the challenges of securing confidential data of both private and government organisations and increasing the need for investment in cyber protection programs.*

Important questions, though, remain unaddressed. In particular:
How ready are the Mozambican organisations to manage cyber risks?

Deloitte has decided to conduct this cybersecurity survey in Mozambique with the aim of understanding how organisations are managing and responding to cyber risks, what is the level of human capital for cybersecurity (available competencies in the country), ascertain if companies are investing in cyber and lastly identify the main gaps faced by organisations.

Methodology:

The survey has been done through face-to-face interviews, via an electronic survey and was directed at the person chiefly responsible for the oversight and strategic management of information security, such as: The Chief Security Officer (CSO), The Chief Information Officer (CIO); The IT Director, IT Manager, of the largest companies in Mozambique's public and private sector. The sectors covered are: **Banking & Capital Markets; Transportation, Services & Hospitality; Oil &Gas; Insurance; Industrial Products & Construction; Government & Public Services; Consumer Products.**

The answers reported in this survey are anonymous, and we have taken care to ensure that information is a fair reflection of the responses received. We would like to extend our appreciation to the respondents for the time and enthusiasm devoted to providing comprehensive responses. We hope this report will contribute to regulators and organisations operating in Mozambique with the effective adoption, implementation and application of strong policies, procedures, and controls to mitigate and respond to the growing cybersecurity threat since the beginning of the COVID-19 pandemic.

Cybersecurity in Mozambique

The cyberspace opens many opportunities for society and an open market, but its use is subject to attacks by cybercriminals meaning harm to society and the economy.

The National Cybersecurity Policy

According to the resolution **n. º 69/2021** published on "Boletim da República" - December 31st 2021 – that approves the Cybersecurity Policy and Strategy implementation, in the last years Mozambique has registered an increase in the number of cases of harassment and abuse in the cyberspace, the spread of false information, scams, identity theft, financial crimes, cyberterrorism, and others. These cases are a concern for the authorities which apply efforts to guarantee a safe cyberspace and to protect critical information infrastructures.

The country has been adopting laws and regulation that govern the use and development of Information Technology (IT) as it pays a big role in the modernisation, transformation, and development of key social-economic areas. In order to mitigate the damages caused by cyberattacks and incidents, the National Cybersecurity Policy (PENSC) is working on building a common platform for resilience to cyberattacks.

The status of Cybersecurity in Mozambique

The 2018 report on Global Cybersecurity Index (GCI) by the International Telecommunication Union (ITU), a United Nations (UN) technology sector agency, placed Mozambique amongst the countries with the worst cybersecurity. Mozambique occupied the 26th position at the continental level and the 132nd position at the global level. In 2020, Mozambique rose 9 positions in the same report occupying the 123rd rank out of 193 countries evaluated.

On the other hand, the country has shown some progress in cybersecurity awareness and in actions taken to develop security in the cyberspace.

Cyber Threats

With the increased use of Information and Communications Technology (ICT), cyber threats tend to grow and the cyberspace gets more exposed to attacks on critical information infrastructure, systems, political and business espionage, cyberwarfare amongst others. One of the preferred targets for cybercriminals are websites, which appear to be more vulnerable in Mozambique, especially the **Government & Public Services** sector websites. The **Banking & Capital Markets** sector is another preferred target with attacks such as Bank website cloning scams, card cloning, phishing and identity theft. There's also a growing number of ransomware attacks and others that are performed through the "Dark Web" and "Deep Web" which involve selling of valid credit card numbers list, among other illicit activities. Attacks using mobile devices also have increased as they facilitate cybercrimes.

According to the 2018 study "Analysis of Mozambican Websites: How they Protect their Users", 32% out of 240 analysed websites have been deemed vulnerable and the majority belong to the **Government & Public**

Services Sector, who has not implemented the recommended technology to protect against cyberattacks.

Legal Framework

Some of the key national legal framework to attend cybersecurity challenges include:

- Telecommunications Law, Law no. 4/2016, of June 3rd;
- Law on Electronic Transactions, Law no. 3/2017, of December 9th;
- Regulation of the Electronic Government Interoperability Framework, Decree No. 67/2017, of December 1st;
- African Union Convention on Cybersecurity and Personal Data Protection, Resolution No. 5/2019, of June 20th;
- Regulation of the Digital Certification System of Mozambique, Decree No. 59/2019, of December 1st;
- Regulation of the .mz Domain, Decree No. 82/2020, of September 10th.

At the level of the African continent, only 20% of the countries have cybersecurity related legislation.

Mozambique has already adopted the African Union Convention on Cybersecurity and Protection of Personal Data. The adoption of the legislation must go in accordance with the criminal justice capacities, from the establishment of specialised units in cybercrime investigation and computer forensics, to strengthening law enforcement and judicial training, interagency cooperation, financial investigations, child protection public-private and international cooperation.

Section 01

Results

The results of this survey are based upon the respondent's self-assessment with no modification or adjustments whatsoever of their answers to preserve the integrity and anonymity of the responses.

According to the answers of the survey, most of the respondents have the feeling that they are aware of cyber risk management techniques, have a positive approach towards it and have the adequate skills and capacity to deal with information security threats. **Despite this, a substantial amount of the respondents have faced cyber incidents in the past years or are unsure about incidents that occurred** which shows the opposite: lack of concern on cyber risk management.

Overall, this Deloitte Cybersecurity Survey for Mozambique indicates that there is inconsistent appreciation of cybersecurity management in the market. The survey shows that companies have safeguards applied to cyber risk, however most of them do not follow industry best practices. Additionally, Business Continuity Plan implementation and maintenance, cyber training programs, Vulnerability Assessment and Penetration Testing are areas that have not been adequately addressed by respondents.

It is clear from responses that despite the awareness of cybersecurity risks and increased commitment to appropriate responses in certain sectors, Mozambique is still in the infancy of cybersecurity management. The Financial Services sector is the leading industry in dealing with cybersecurity.

Below are some other high level finding of this survey:

- Most of the Board of Directors are not aware of Cyber Risk, which means that most companies are not used to investing in this area or drive management decisions to deal with such issues;
- The most common threat has been ransomware, a type of malware that threatens to publish the victim's personal data or permanently block

access to it unless a ransom is paid off;

- The biggest threats rated are: Financial Losses, loss of brand reputation and trust and sensitive information theft;
- Cyber Risk Insurance is not in place for most organisations,
- The budget allocated to cybersecurity management is not adequate to cover the increasing cyber threat landscape;
- Most organisations are not prepared to respond to cyber incidents due to the lack of a Cyber Incidence Response Plan.

The current thread landscape is already challenging. It only takes one key vulnerability for an entire organisation's security to be compromised. The current complexity and size of organisations raises the question: **"to what extent do organisations rely on their current defence capabilities?"**. If we collaborate towards common cybersecurity goals, we can make the most out the digitalisation trend in Mozambique.

Section 02

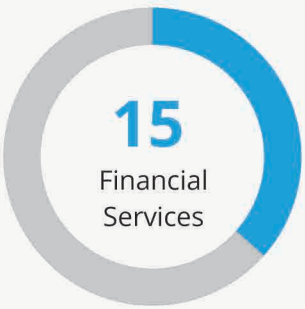
Overview of respondents in Mozambique

Cybersecurity is continuously **in motion**. It must be in order to keep up with the constantly changing cyber threats. In this increasingly digitized world with **distributed systems**, the importance of securing systems is clear and there in no sector in particular that is exempt from cyberattacks.

At **Deloitte**, we were keen to know where Mozambican organisations currently stand with respect to cybersecurity.

In this survey, we had the opportunity to work with noticeable organisations that are part of **4 industries** divided into **7 different sectors.**

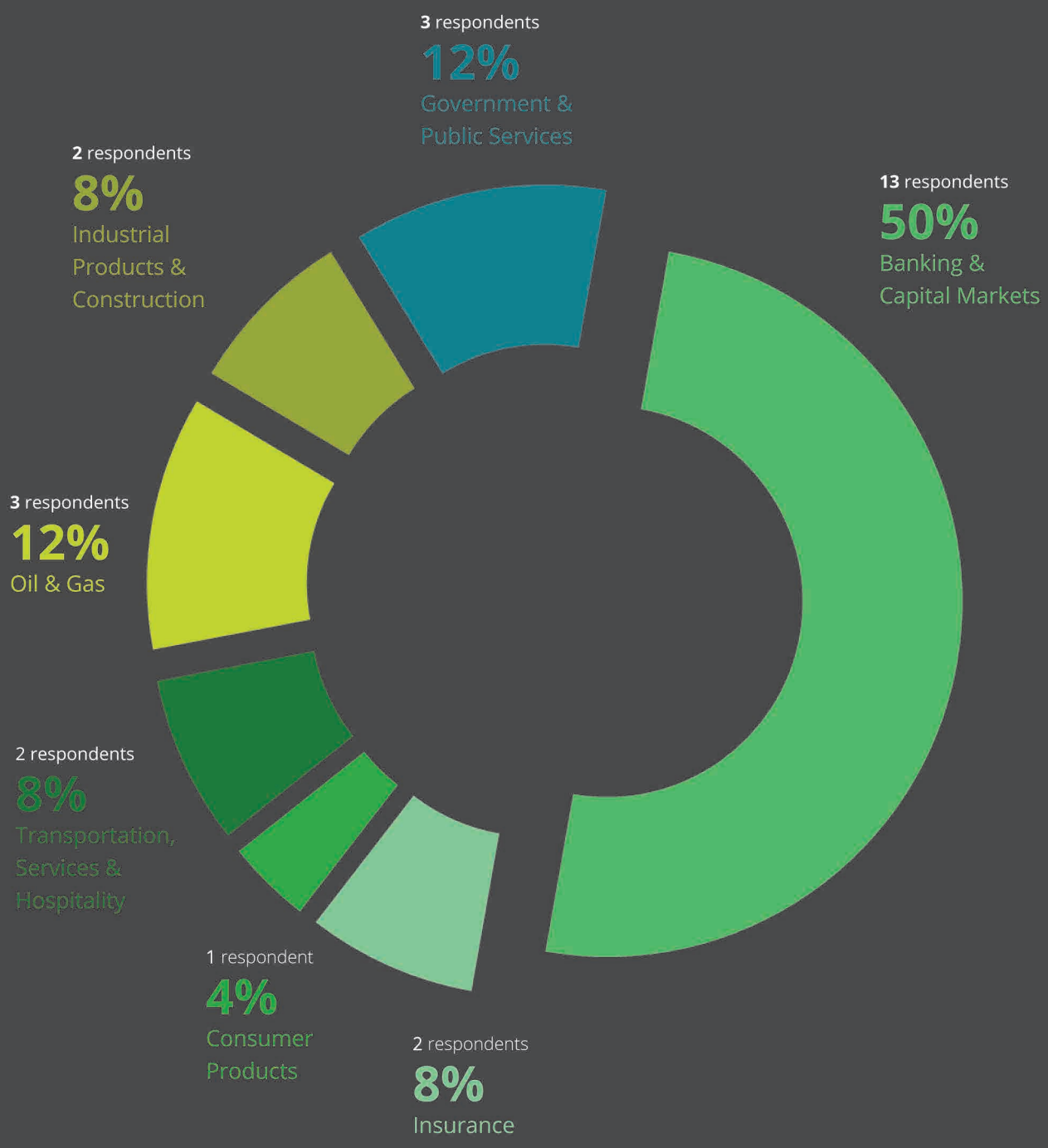
General Information
Respondents by Industry



General Information

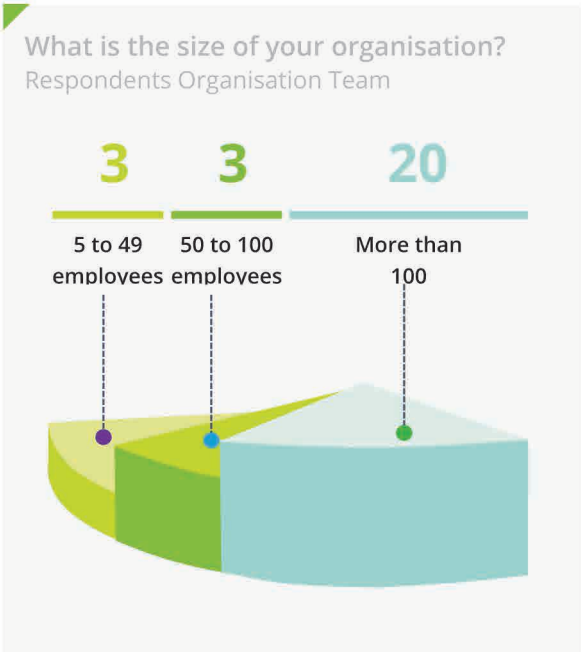
Respondents by Sector

Fifty percent (50%), that is, **thirteen (13)** participants of the survey are from the **Banking & Capital Market** sector. This is a sector that must be careful not to rest on their laurels, they must continuously test their environment for cybersecurity posture and close any gaps identified in order to prevent cyberattacks.



Size of Organisation

The respondents consisted roughly of **large entities**, enabling us to obtain information likely to be of value to a wide segment of the Mozambican market.



Person Responsible for Cyber Risk

All the respondents have at least two individuals responsible for cyber risk. In most cases, the responsibility to monitor and manage cyber risk, cyber incidents, and cybersecurity rests with the **IT Manager**, although we noted several entities made use of a dedicated **CSO, CIO and Risk Manager**. Some organisations outsource this service.

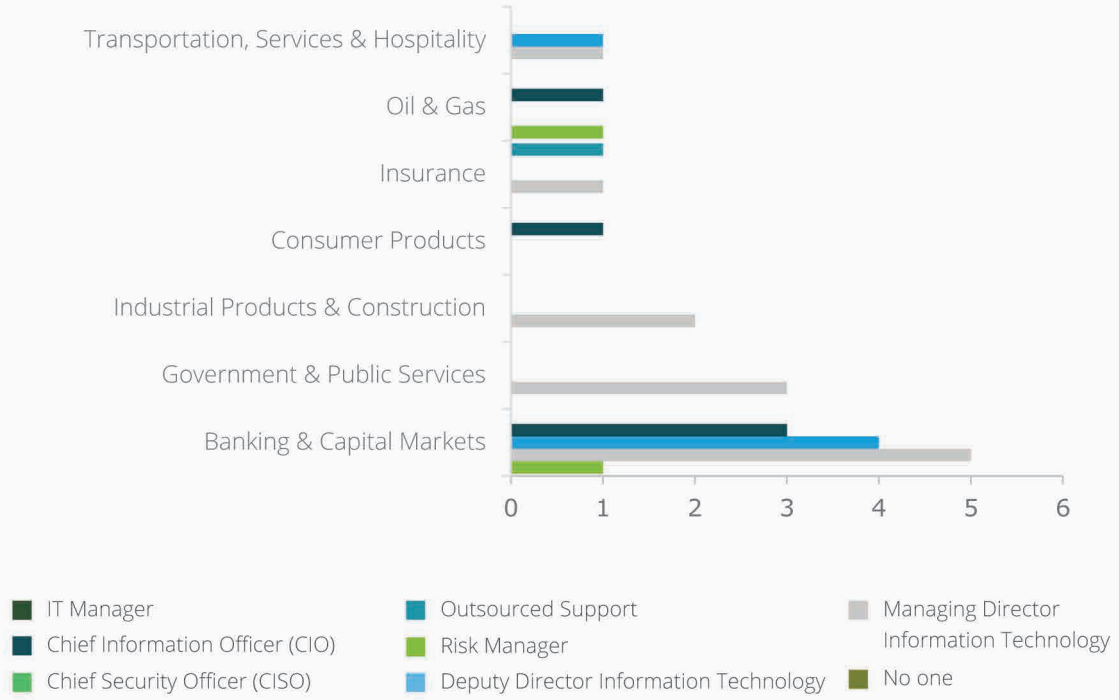
ISACA, the Information Systems Audit and Control Association, in their *Guidance for Boards of Directors and Executive Management* (2nd Edition, 2006), places the ultimate responsibility for IT governance and therefore IT security management with the Board of Directors and notes that due to the strategic importance of information security, the function requires C-level officer or executive direction and authority.

46%

of entities allocated responsibility for the monitoring and management of cyber risk at managerial level or below and 8% seek outsourced support.

Who is the person responsible for cyber risk within your organisation?

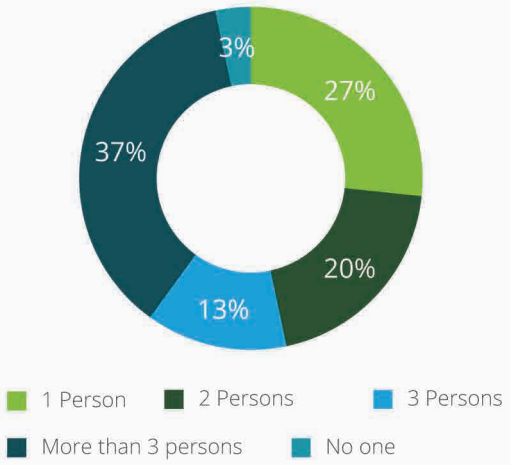
Persons responsible for Cyber Risk by Sector



In 37% of all entities, more than 3 persons were reported to be responsible for the monitoring and management of cyber risk and incidents, with **seven respondent** reporting that only **one individual** is involved in the management of cyber risk and incidents.

What is the size of your cyber risk team within your organisation?

Size of Cyber Risk Team



While there are certainly several functions within an entity in which cyber risk and incident management may naturally fall, a risk that arises as the result of allocation of responsibility to multiple roles or persons is that **measures put in place are ineffective, duplicated, or not reported consistently.**

Section 03

How ready are Mozambican companies to manage cyber risks

Cyber Risks can come from many directions, including internal actors aiming to sabotage a production environment, processing fraudulent transactions, competitors seeking to cause brand damage, and external parties, such as **activist groups**, wanting to **shut down operations or collect sensitive information.**

Consider the following cyber risk scenarios, which are recent trends, not even possible a few years ago:

- Insecure remote access communication allows a cybercriminal to hijack a process control system and push production to unsafe levels;
- Poor security practices by a third-party contractor allows a virus to migrate into the production environment, shutting down critical Supervisory Control and Data Acquisition (SCADA) systems and creating unsafe working conditions;
- Improper testing of IT systems prior to deployment results in a system crash, leading to disruption or shutdown of operations;
- Technology acquired directly by a facility, without adequate testing and evaluation, goes unpatched and introduces a vulnerability which allows members of an adversarial community to gain remote access to Programmable Logic Controllers (PLC), thus giving them the ability to disrupt the production process at will.

If your organisation does not invest in effective risk management, independent of the sector, it will always be considered a risky business.

Risk Management

It is our experience that entities are inclined to see the responsibility for cyber risk and business continuity to be mainly that of the IT function, with limited ownership of the risk lying with the business overall.

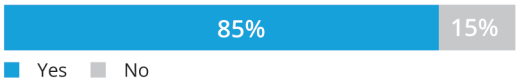
This may result in a lack of strategic direction and alignment to business objectives and may risk legal liability. This tendency is evident in the large number of IT managers solely responsible for the monitoring and management of cyber risk as illustrated in the next graphs.

Risk management includes the existence of a Business Continuity Plan (BCP), which is an enterprise-wide contingency plan for a variety of likely scenarios, encompasses all departments of the organisation, and also includes an IT continuity or Disaster Recovery Plan (DRP). By inference, a DRP is only a small portion of the bigger whole of a BCP and addresses the arguably most likely risk of IT system downtime.

85%

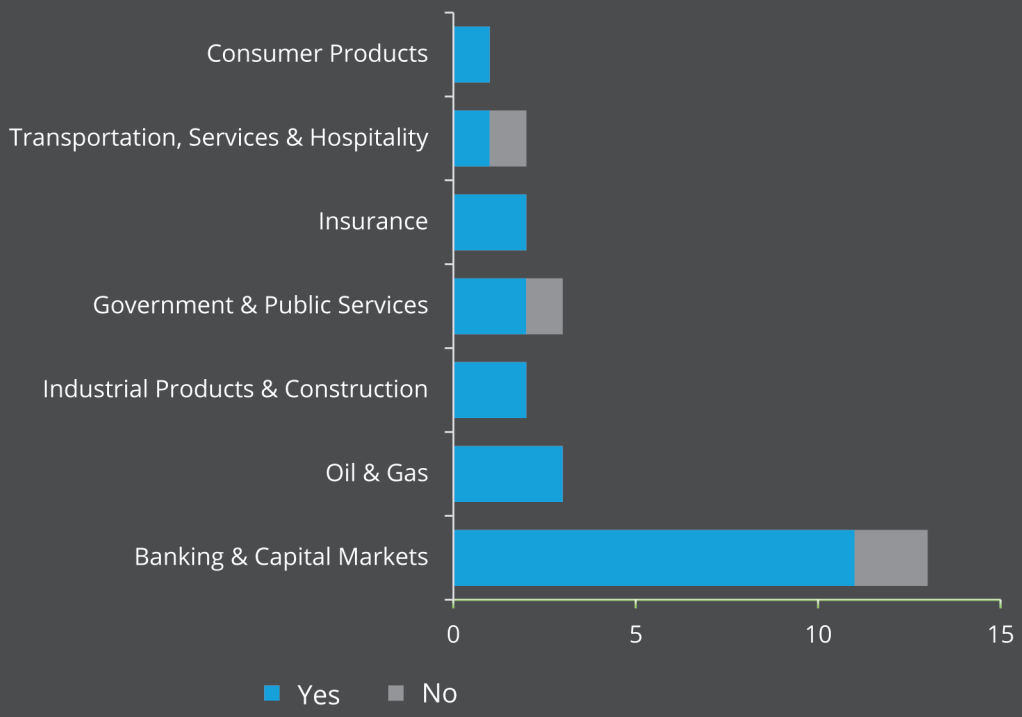
of respondents felt that their organisation manages cyber risk actively.

Business Risk Management



The responsibility for cyber risk and business continuity are mainly directed to IT Managers, with limited ownership of the risk lying with the business overall.

Business Risk Management
By Sector



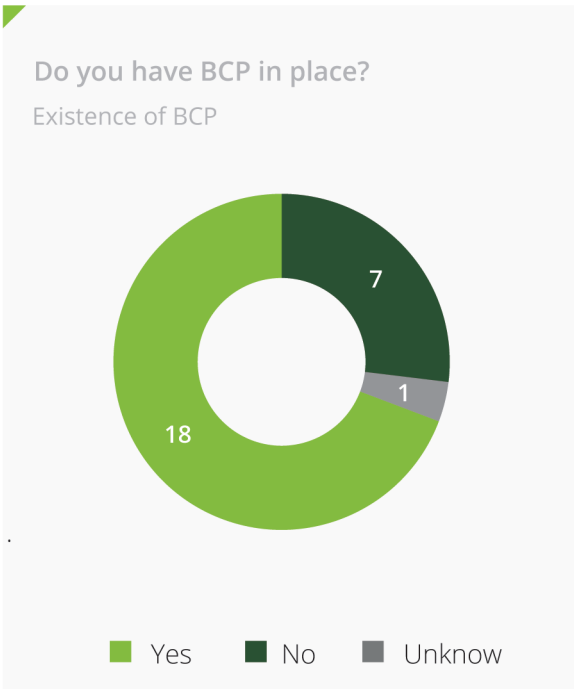
Business Continuity Plans

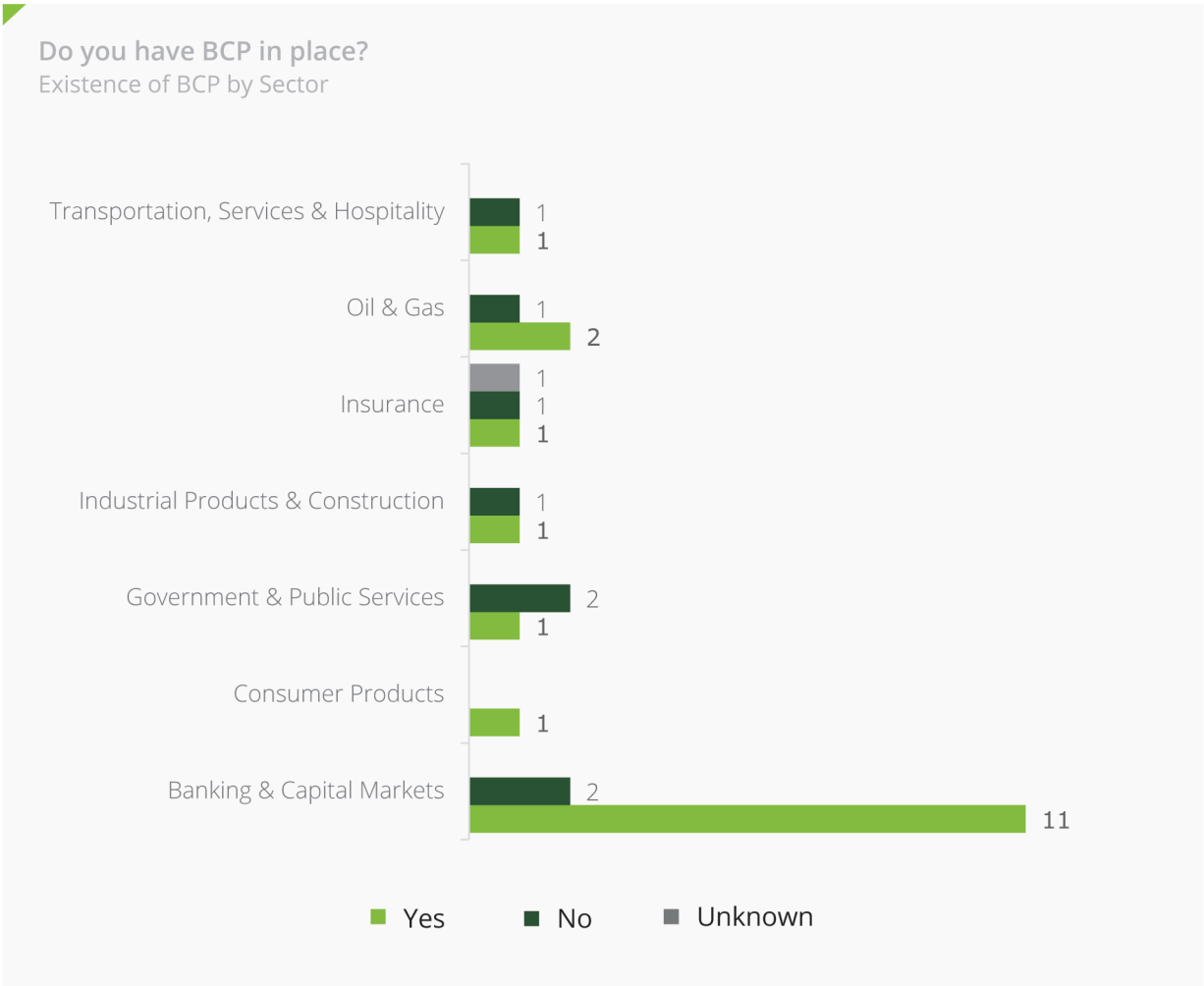
18 entities surveyed that actively manage risk in their organisations.

69%

have a disseminated business continuity or disaster recovery plan.

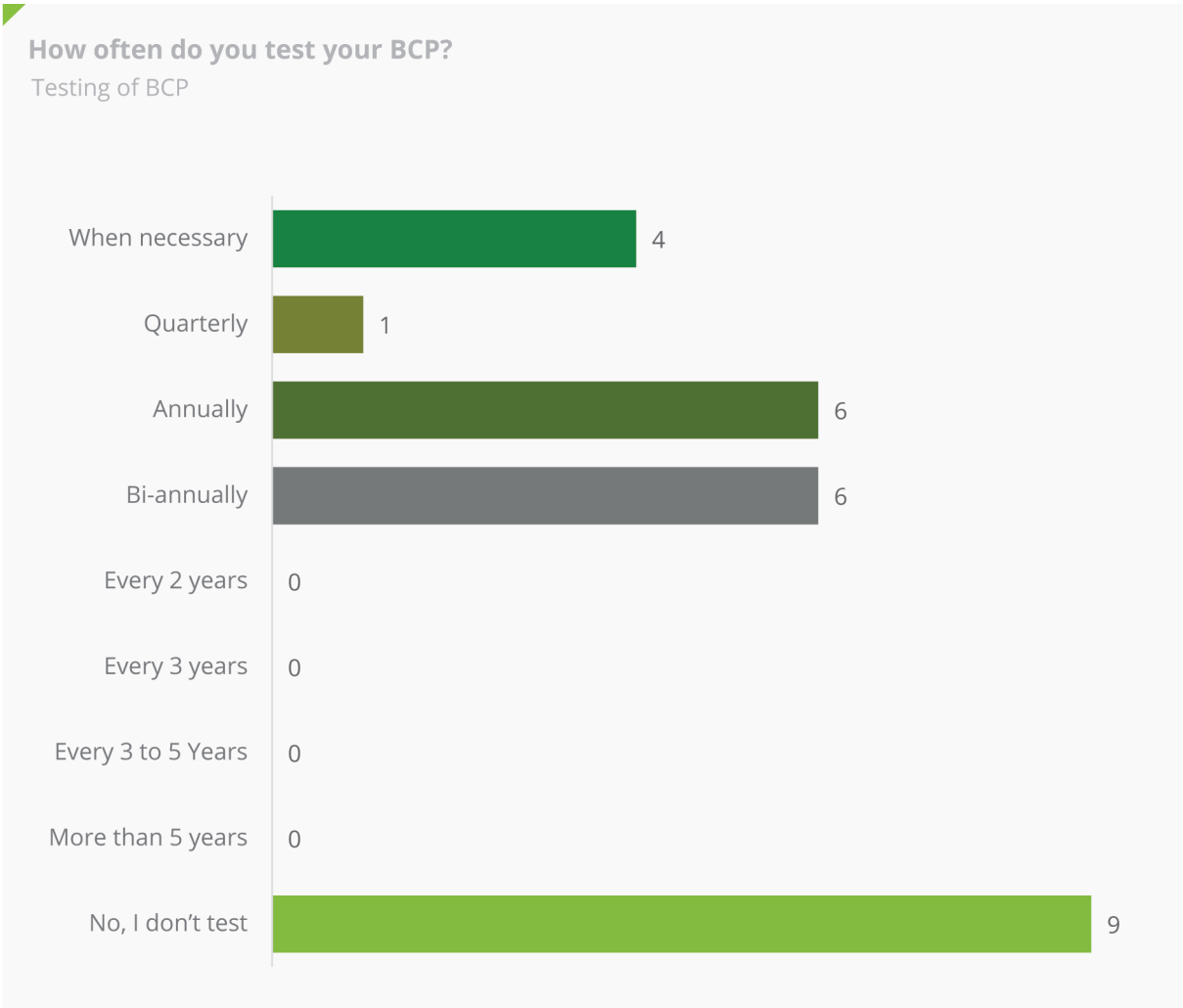
From this group, **31% is unsure** or **does not have** any BCP or DRP. As a cyber incident may well cause system downtime, a well-documented BCP or at an absolute minimum a DRP is a critical component of cyber risk management.





In order to respond to disruptions, it is a good practice to have a BCP in place, which will reduce the impact on the business. Experience shows that businesses without an effective BCP ultimately fail after a major crisis.

35% of entities did not test their BCP at all.



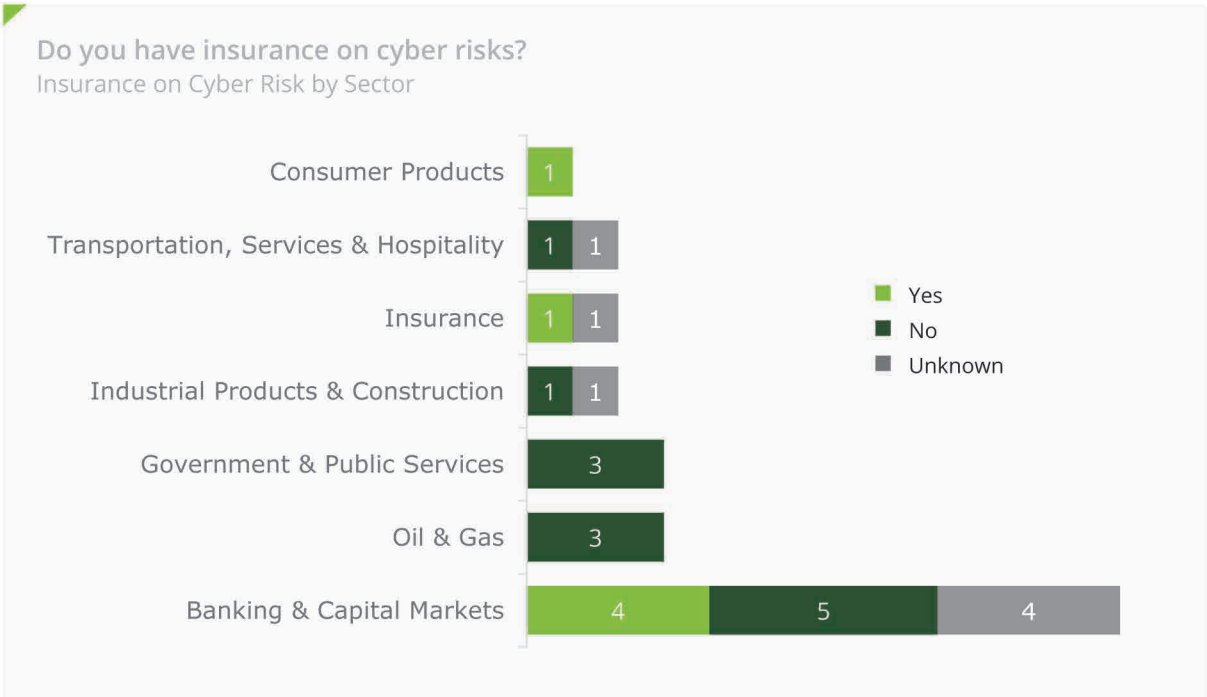
Insurance on cyber risk

While cyber risk insurance coverage is a relatively new concept for Mozambique,

23%

of respondents indicated that their insurance covers cyber incidents

77% is unsure or **does not have** any insurance coverage. In the absence of risk prevention methods or where such methods are considered cost-ineffective, insurance may be an appropriate risk management strategy. However, most insurance companies are likely to require certain risk prevention measures to be put in place. Insurance isn't enough to cover the damages associated with a disaster. It can cover the **costs of repairs**, but in terms of loss of revenue and business prospects due to downtime, it has little effect.



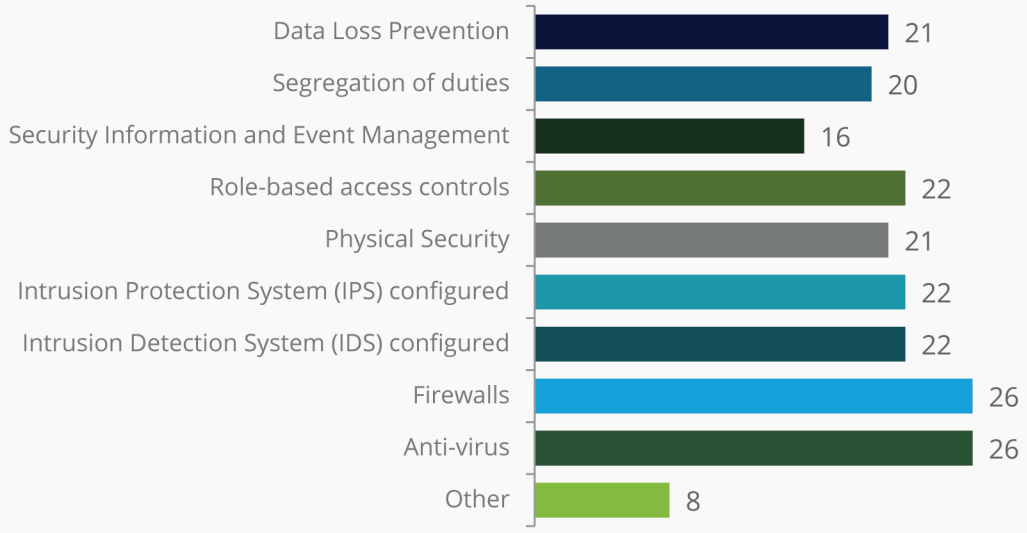
Safeguards applied

All entities surveyed applied **at least one** form of safeguard for their most sensitive information, with the most common forms being **firewalls** and **Anti-virus**.

19%

of entities don't apply physical security measures.

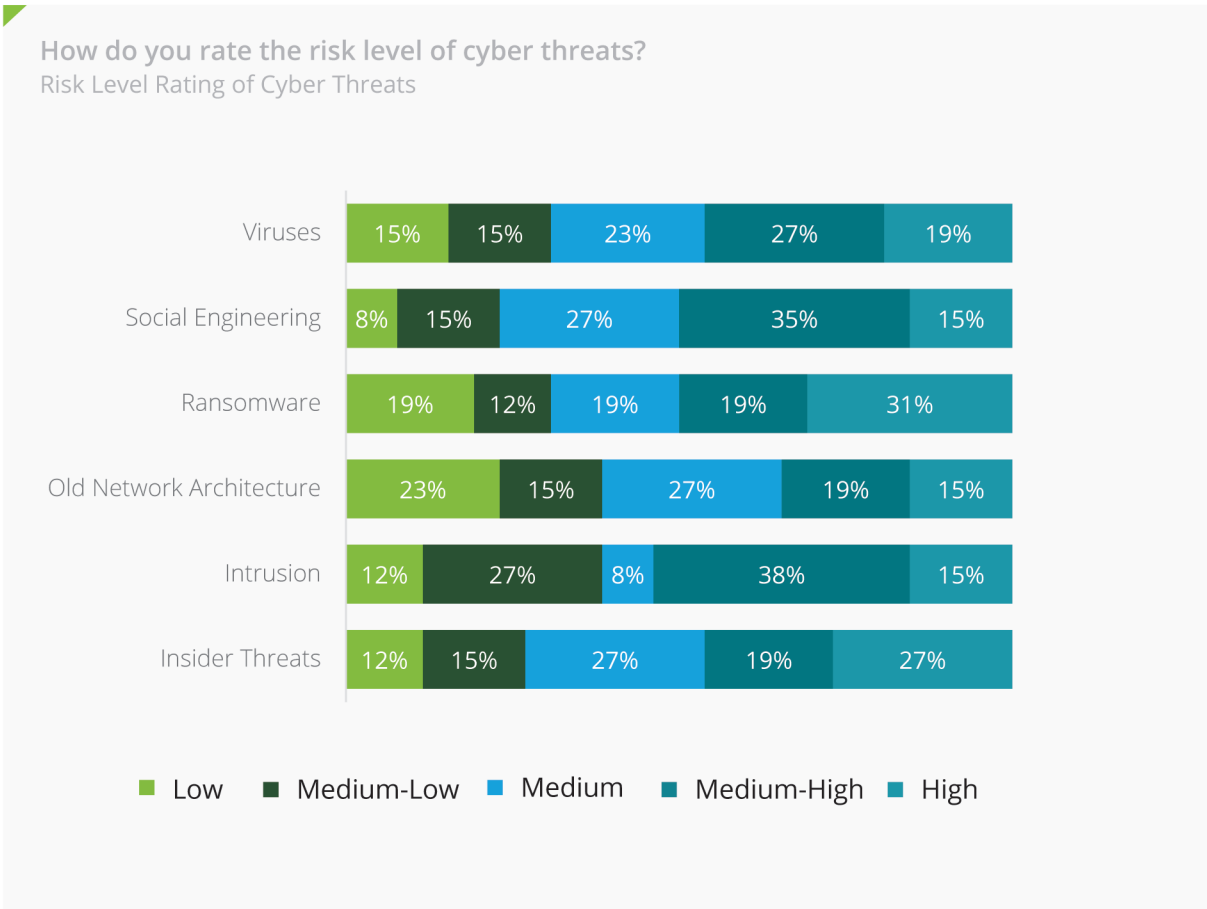
Which of the following safeguards do you have for cyber risks?
Safeguards Applied For Cyber Risks



46% of entities apply **all the safeguards** listed.

Assessment of Cyber Threats

In general, most respondents assessed the likelihood and impact of cyber threats as **medium** to **medium-high** which is in line with BROADCOM SOFTWARE's Symantec Security Summary (June 2020) that indicates an increase of attacks globally. Ransomware is one of the biggest cyber scourges. According to report from threat intelligence firm ProDaft, attackers using the Conti ransomware have collected at least $25.5 million in ransom payments since July 2021.
The recent attacks on **Mozambique Government Websites as of March 2022, that suspended all operations on the websites** servers as an example of a Medium-High risk cyberattacks.



Assessment of Risk Exposure

Once a cyberattack has occurred, there are several risk exposures an entity may face.

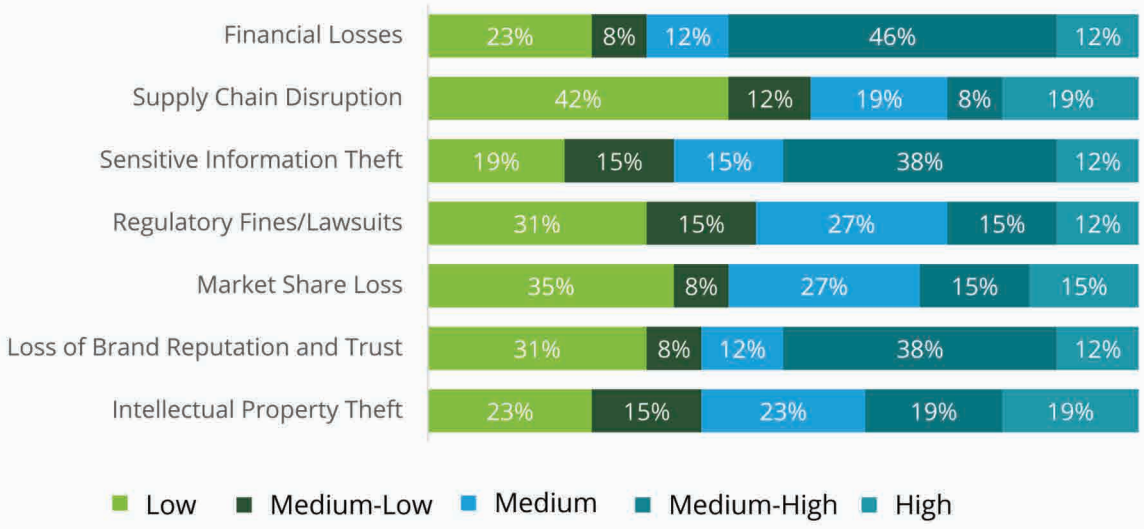
In general, these are:

- Financial Losses;
- Loss of Brand Reputation and Trust;
- Sensitive Information Theft;
- Regulatory Fines/Lawsuits;
- Market Share Loss;
- Supply Chain Disruption;
- Intellectual Property Theft.

Respondents rated **Financial Losses, loss of brand reputation and trust and sensitive information theft** as the **3 biggest threats** to their entity and supply chain disruption and market share loss as the lowest threats.

How do you rate the risk exposure on occurrence of cyberattacks?

Risk Exposure Rating on Occurrence Of Cyberattacks



Implementation of Plans and Policies

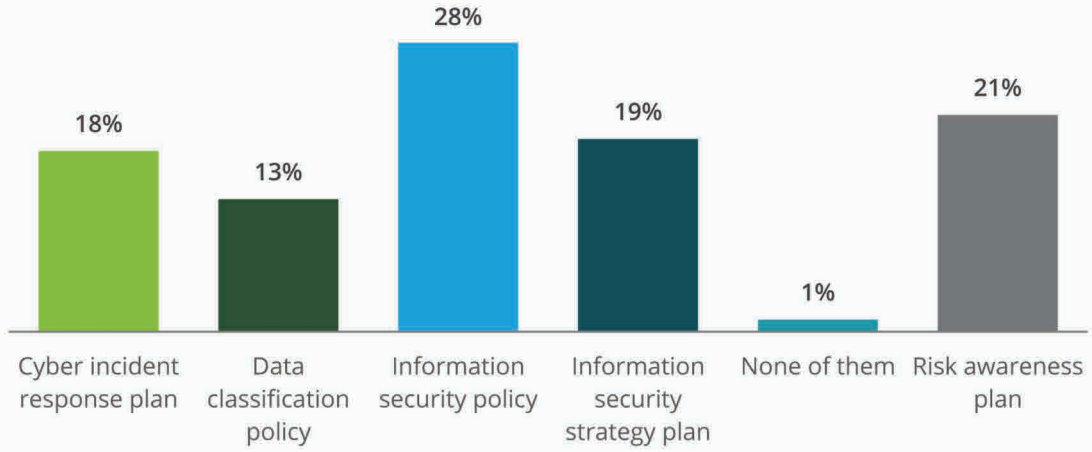
Reviews of the plans and policies are performed annually in **54% of cases**, with **23% of entities** performing reviews when necessary.

18% (only)

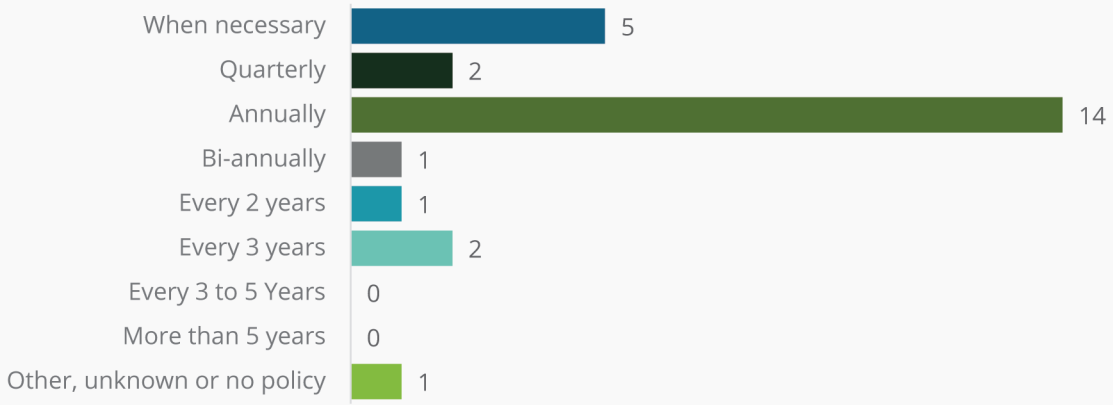
of respondents reported having a cyber incident response plan.

Which of the following Plans and Policies are designed and implemented in your company?

Implementation of Plans and Policies



How often are the information security documents reviewed?
Review Frequency of Information Security Documents



Board Awareness of The Cyber Risk

More and more organisations nowadays have at least a basic understanding of the importance of cybersecurity investments. Most have translated this into cybersecurity plans or strategies, and almost half have seen a rise in the correspond budget per year.

31%

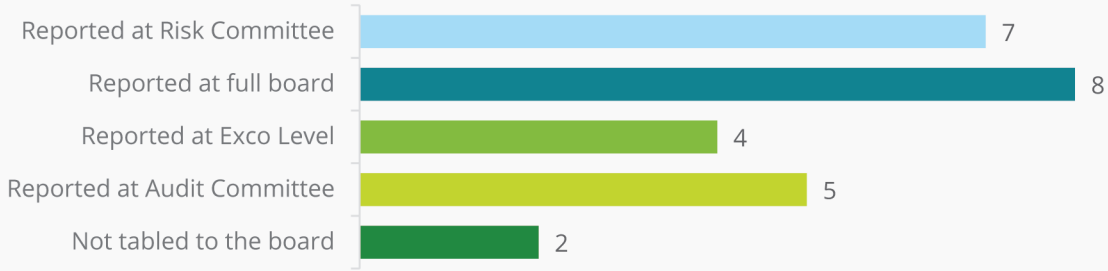
of respondents reported that the board is aware of cyber risk and its importance to the organisation.

Boards should understand the importance of cybersecurity within the organisation, the need for investment in this area and that cybersecurity is a shared responsibility upon which they must make joint decisions on realistic and pragmatic goals. This requires not only awareness of problems and solutions, but also commitment to make tough decisions.

It is difficult to prepare for the **threats of tomorrow** if you're not ready for the **threats of today**.

Board Awareness of The Cyber Risk

How the board is aware of the cyber risk?
Board Awareness of The Cyber Risk



Section 04

What is the level of human capital for cybersecurity?

Being cyber secure is not enough, either for individual organisations or for society. To continue our digital journey with confidence, we need to be able to take a blow and stand up again. In other words, we need to become cyber resilient. Making our organisations more cyber resilient is a shared responsibility.

Skills and Awareness

98%

of respondents felt that their organisation had adequate skills and capacity within to deal with information security activities and risks

Evaluation of skills and capacity in information security

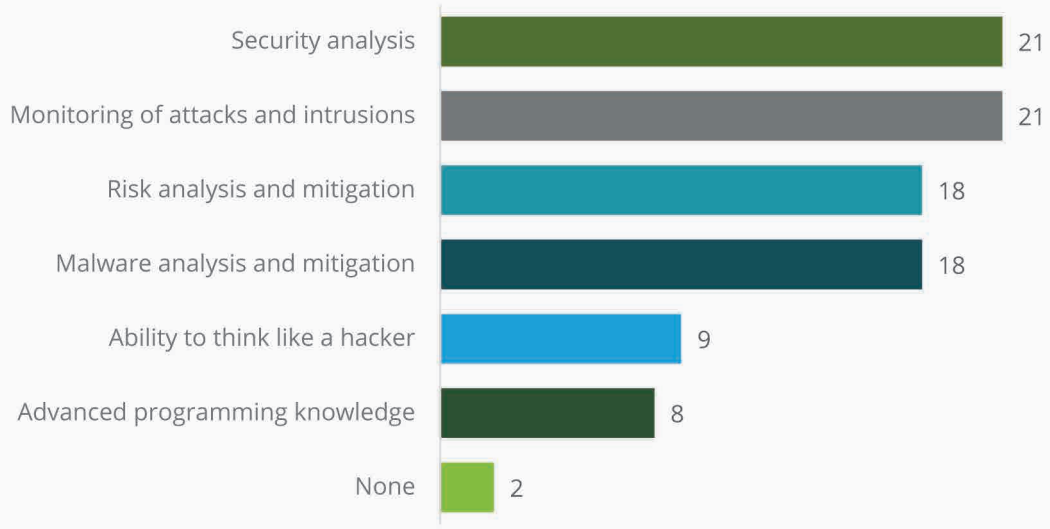
Yes No

Only 2% of the entities responded otherwise.

Training is a critical activity in reducing the likelihood of a successful attack using social engineering techniques to gain access to company critical systems and data. According to the Verizon Data Breach Investigations Report, 2020, **over 80% of breaches within Hacking** involve Brute force or the Use of lost or stolen credentials, moreover, it is reported that **Phishing** is the top incident in data breaches

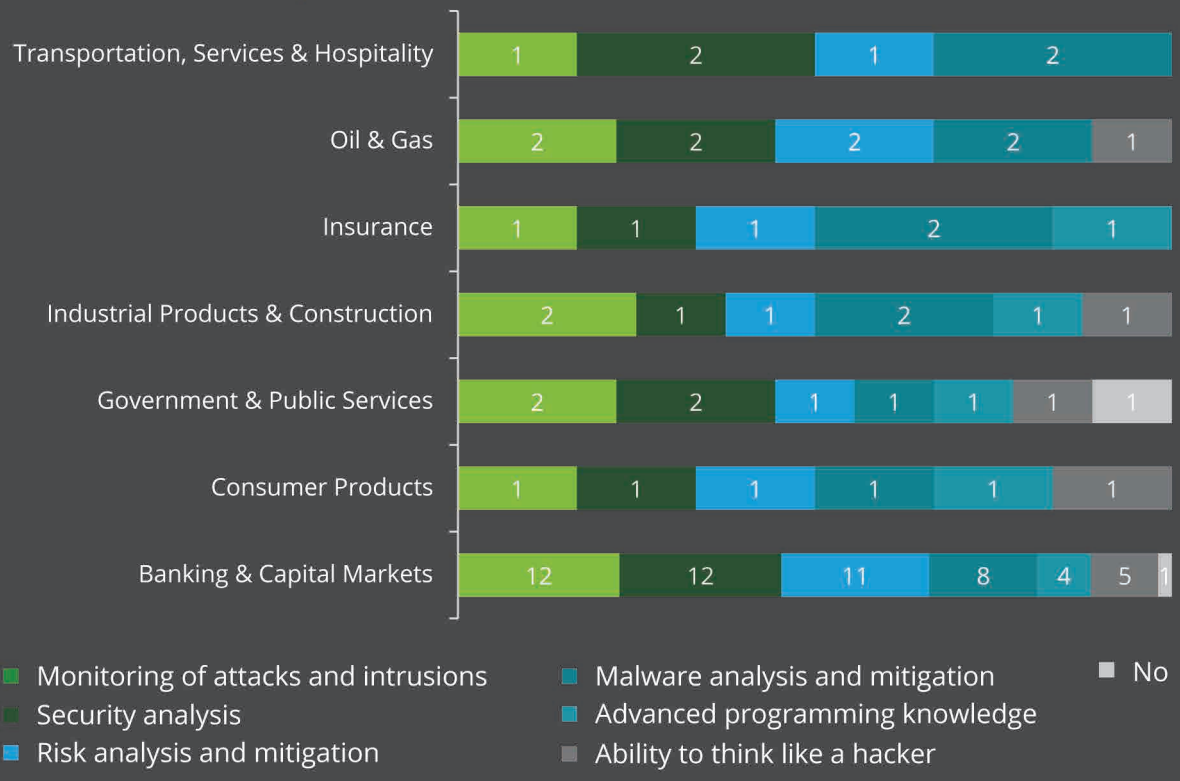
What appropriate skills and capacity to deal with cybersecurity activities and risks do you have?

Skills and awareness



What appropriate skills and capacity to deal with cybersecurity activities and risks do you have?

Skills and awareness by Sector



Cybersecurity Team Training

50%

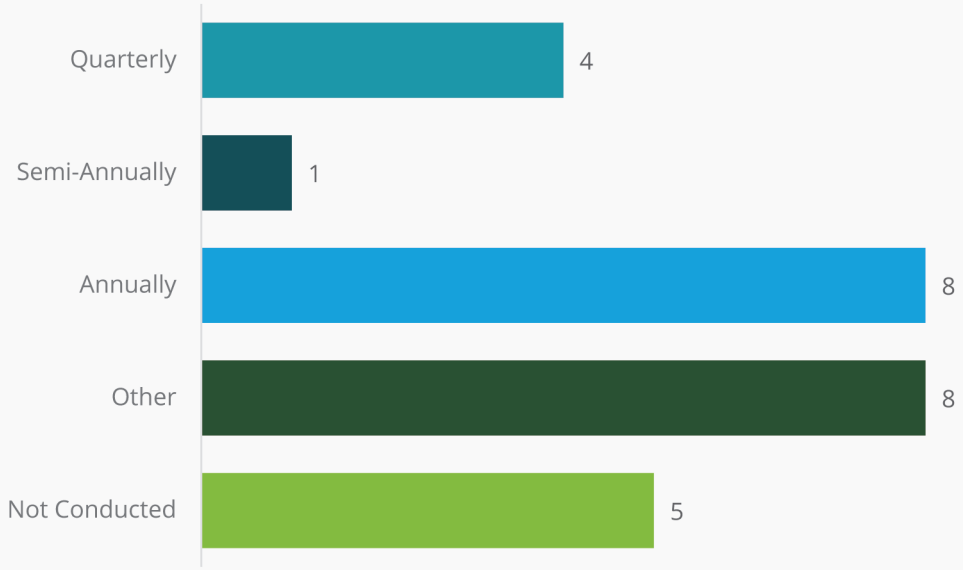
of entities did not conduct or are unsure if user training is conducted.

One of the most frequently cited success factors for achieving cybersecurity goals are clear cybersecurity awareness and training the organisational workforce to become more aware of cybersecurity matters. This is important for the organisation to increase cybersecurity risk maturity.

Some of the most familiar certifications available and recognised world-wide include the **Certified Information Systems Manager (CISM)** and **Certified Information Systems Security Professional (CISSP).**

How often does the cybersecurity team participate in training programs?

Cybersecurity Team Participation in Training Programs



Cybersecurity Challenges

The increased evolution of cyberattacks and their aftermath has raised the priority of cybersecurity among high level professionals besides CISOs. After all, protecting the cyber environment means protecting an organisation's production environment and crown jewels.

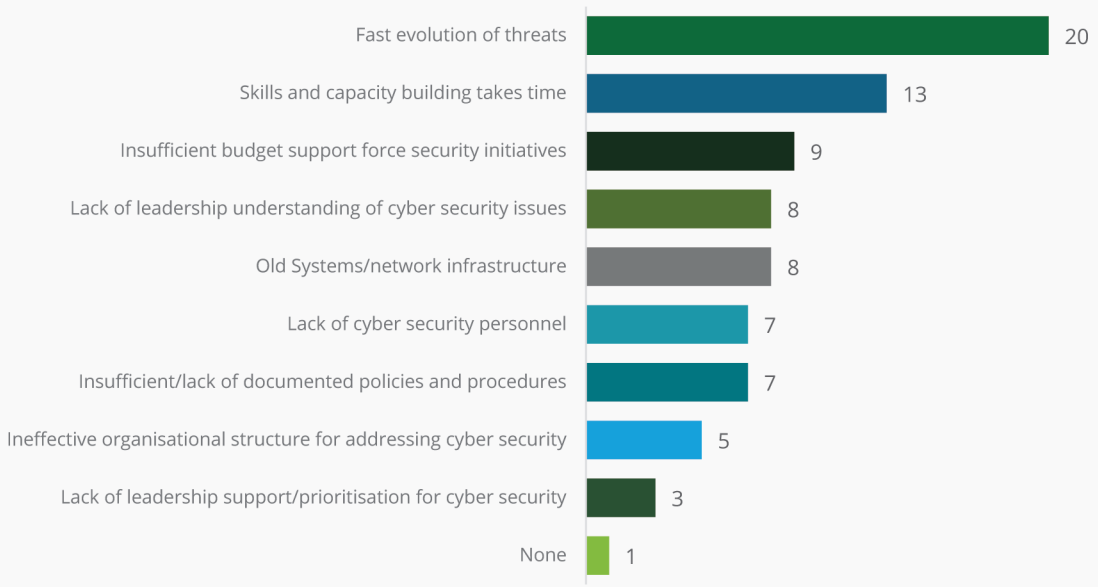
Therefore, it is no surprise that:

25%

of entities chose the fast evolution of threats as a challenge to cyber risk management

What are the common cybersecurity challenges experienced up until now?

Common Cybersecurity Challenges Experienced



What are the common cybersecurity challenges experienced up until now? (1/5)

The 2 most Common Cybersecurity Challenges Experienced by Sector

Skills and capacity building takes time

Banking & Capital Markets (38%)

Insurance (100%)

Oil & Gas (33%)

Government & Public Services (67%)

Transportation Services & Hospitality (0%)

Industrial Products & Construction (50%)

Consumer Products (0%)

Fast evolution of threats

Banking & Capital Markets (77%)

Insurance (50%)

Oil & Gas (33%)

Government & Public Services (67%)

Transportation Services & Hospitality (50%)

Industrial Products & Construction (50%)

Consumer Products (100%)

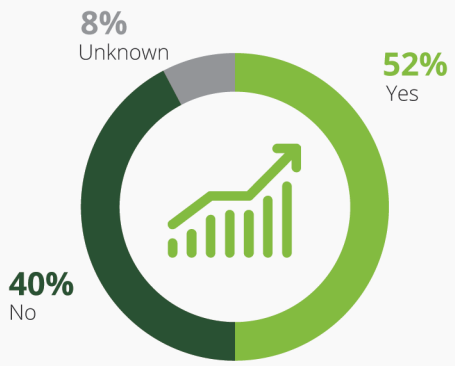
Monitoring and proactive incident management

48% of respondents have never performed or are not aware of the performance of Vulnerability Assessment and Penetration Testing (VAPT) or a review of software source code.

Banking & Capital Markets appear to be ahead of the curve in this metric, which may be attributable to the requirements of the Payment Card Industry Data Security Standard (PCI DSS) to which most of entities of this sector would have to comply because of card service offerings. PCI DSS requires businesses to conduct regular security assessments and segmentation tests every **six months,** this will allow you to fix issues before a real attacker uses them.

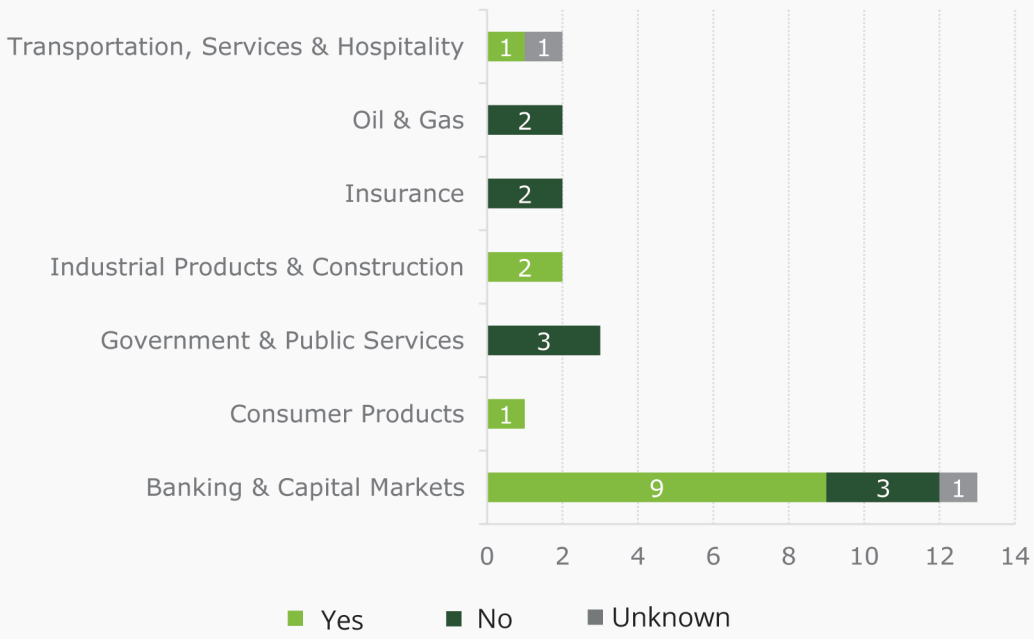
Has your organisation performed VAPT or code review?

Performance of vulnerability assessment



Has your organisation performed VAPT or code review?

Performance of vulnerability assessment by sector

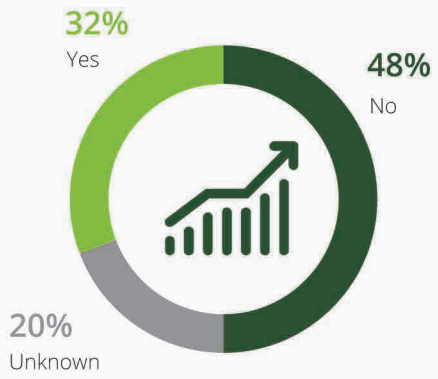


Only **32%** of respondents have indicated being aware of a cyber incident within their entity and have experienced interruptions due to such an incident.

According to Varonis, a pioneer company in data security and analytics, Banking & Capital Markets businesses take an average of 233 days to detect and contain a data breach, this means that in addition to being one of the most affected sectors, the discovery process takes time.

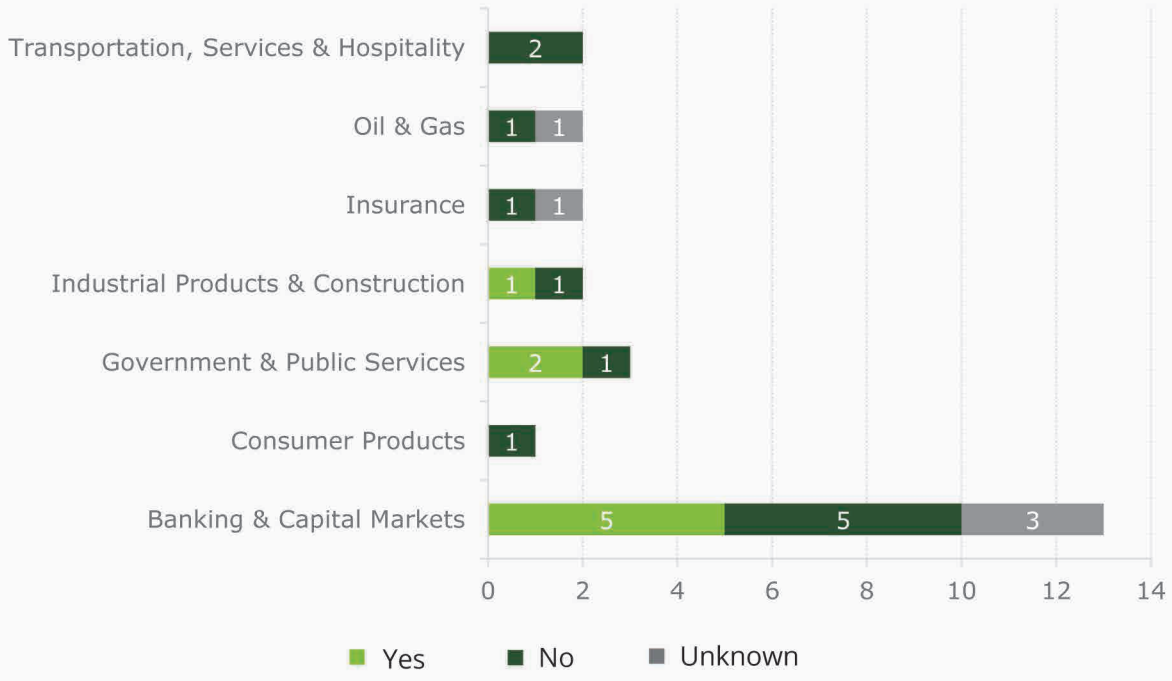
Have you experienced cyber incidents within your organisation?

Cyber Incidents Within Organisation



Have you experienced cyber incidents within your organisation?

Cyber Incidents within Organisation by Sector



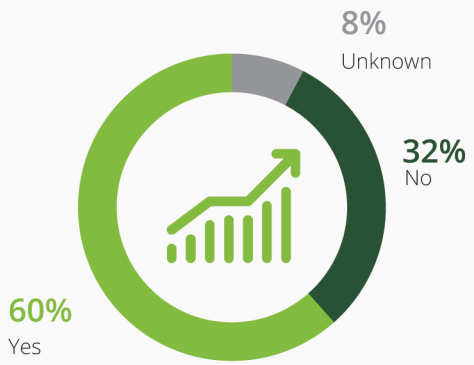
Covid-19 Context

The coronavirus pandemic has created new challenges for businesses as they adapted to an operating model in which working from home has become the 'new normal'. During this period, technology has become more important as more and more people are working from home. Despite the rise of technology need, organisations needed to be more aware of cyber risks in order to operate efficiently.

60% of respondents reported to notice an increase of cyberattack since the beginning of the COVID-19 Pandemic.

Have you seen an increase of cyber-attacks since the beginning of the COVID-19 pandemic?

Increase of Cyber-Attacks Since the Beginning of The Covid-19 Pandemic



The pandemic called for a greater focus on cybersecurity, because of the greater exposure to cyber risk. According to Tessian, **47% of employees cited distraction as the reason for falling for a phishing scam while working from home.** Hackers see the pandemic as an opportunity to step up their criminal activities by exploiting the vulnerability of employees working from home and capitalising on people's strong interest in coronavirus-related news (e.g., malicious fake coronavirus related websites).

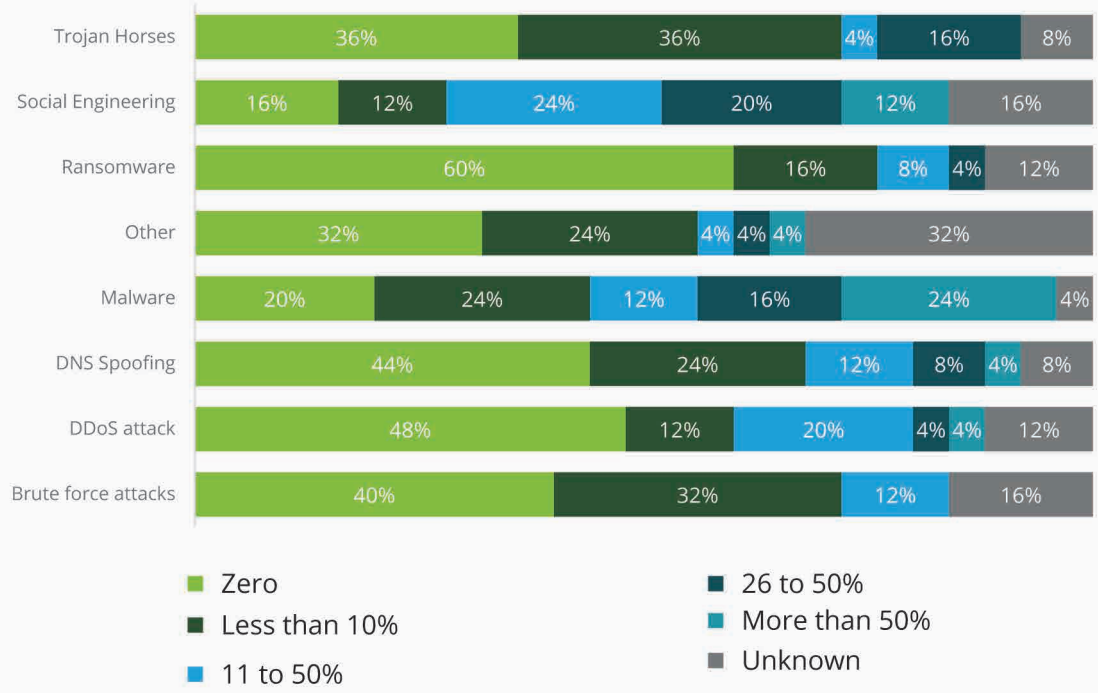
An example of criminals exploiting the cybersecurity weaknesses in remote working has been the series of cyberattacks on video conferencing services. Between February 2020 and May 2020 more than half a million people were affected by breaches in which the personal data of video conferencing services users (e.g., name, passwords, email addresses) was stolen and sold on the dark web.

Malware was the most common cyberattack faced amongst the respondents since the beginning of the pandemic with **24%** of the respondents reporting that it was the most frequent in relation to the others.

Which is in line with Google that indicates In the first month of the pandemic, Google blocked 18 million daily malware and phishing emails related to the coronavirus.

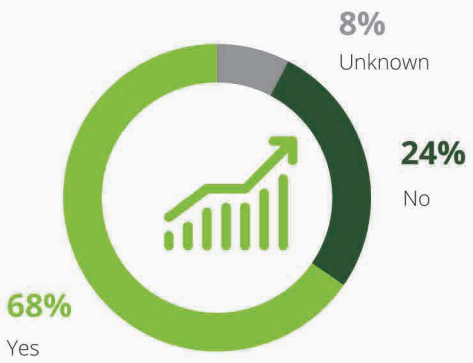
What size and types of cyber-attacks has your organisation experienced since the beginning of the COVID-19 pandemic?

Size and Types of cyber incidents experienced



Have you enforced additional security measures due to COVID-19 pandemic and while staff working remotely?

Enforcement of Security Measures



This pandemic has taught us that preparation is key to successfully limiting the risks related to cyberattacks. The ability to quickly react to unforeseen events helps reduce the impact of a cyberattack. Companies that already benefited from secure remote working capabilities will be better prepared to face the continuous increase of cyber threats.

68% of the oganisations have enforced Security Measures Due to Covid-19 Pandemic while staff working remotely

Section 05

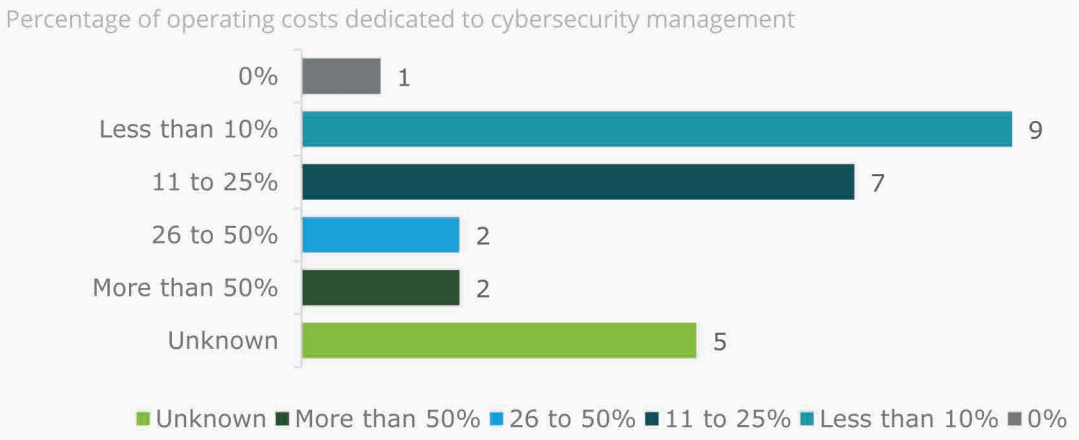
What are companies investing in Cyber

As organisations begin to move their **operations to the cloud** and **modernise their systems**, budget allocation on security safeguards and security awareness training becomes increasingly more important given the **threats** that may rise and the **strategies** to address them.

Budgetary expenditure on cybersecurity has a direct correlation to risk exposure and helps in understanding the relative level of investment to support the security of the total IT environment.

38% of entities reported to have **less than 10%** or **0%** of operational costs allocated to cybersecurity management.

What is the percentage of operational cost dedicated to Cybersecurity Management?

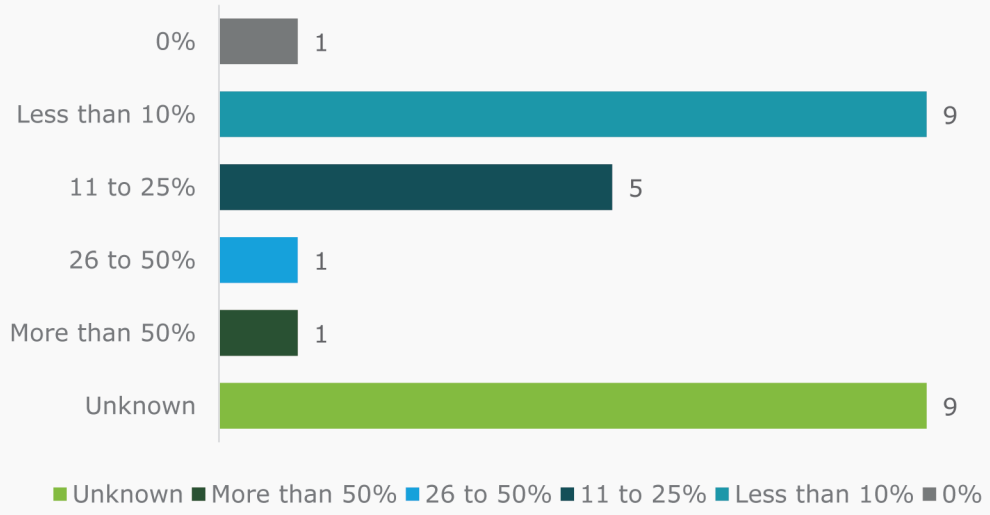


The BCP should consider investments and maintenance on cyber risk. According to Prescient & Strategic Intelligence, the **Global Business Continuity Management (BCM) market** was valued at **$359.2 million in 2018** and is further expected to generate **$875.7 million revenue by 2024**, which reflects an **increased spending** in implementation of BCP.

However, **35%** of respondents indicated that business continuity budget does not seem to be included as a **cost consideration** or how much spent on this **is unknown**.

What is the percentage of the Business Continuity budget dedicated to the Cybersecurity Management?

Percentage of Business Continuity Budget set aside for cybersecurity



Section 06

Final considerations

Comments from the respondents:

> “Lack of legislation on Cybersecurity makes difficult for cybersecurity to be addressed as high importance. Management sees cyber as cost and compliance matter, instead of a critical area.”
>
> Anonymous

> “It is necessary to create periodic forums for debates and provide recommendations for the financial sector, also Cyber initiatives/controls should be regulated. Another suggestions is greater involvement of the ARECOM in promoting cybersecurity debates and assessments in Mozambique.”
>
> Anonymous

> “The government regulation restricts the use of the cloud, which indicates that the information should be located in the country by state or state owned institutions. This situation limits the access or adoption of more advanced tools for the mitigation of cyber risks.”
>
> Anonymous

> “The Survey is welcome, because cybersecurity is a national concern.”
>
> Anonymous

Section 07

Background and definitions

IT Governance

IT governance can be considered as a framework that supports effective and efficient management of IT resources to facilitate the achievement of a company's strategic objectives.

Business Continuity Plan

The activity performed by a company to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. Preventing, mitigating, and recovering from disruption – The terms 'business resumption planning', 'disaster recovery planning' and 'contingency planning' also may be used in this context; they all concentrate on the recovery aspects of continuity.

Information security

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities.

IT Environment

An IT Environment may be defined as policies and procedures that an entity implements and the application systems, data warehouses, report writers, and IT infrastructure, which may also include interfaces or middleware entity uses to support business operations and achieve business strategies. The application systems, data warehouses, report writers, and IT infrastructure (databases, operating systems, and networks) are technology elements that are collectively referred to as an "IT Environment."

Cyber Risk

Risk arising from information technology systems that may cause damage to the reputation of an organisation, financial loss or disruption of operations.

Chief Security Officer
Executive with the responsibility to ensure physical and digital security, i.e., security of personnel, data, and physical assets.

Chief Information Officer
Executive responsible for the implementation and management of computer systems and technology in an organisation.

Crown Jewels
Critical assets, sensitive or high value data of an organisation.

Section 08

Contacts

Deloitte help business to understand their specific cyber threats and decide on investments that will contribute most to their overall cyber resilience. In less time and effort, we do a thorough analysis of the current & target maturity of an organisations unique cyber capabilities. We define a targeted roadmap, can ensure consistent quality and give access to benchmark data to compare results with industry peers. Our methodology is based on the expertise of our acclaimed cyber practioners around the world so companies can leverage the insights of a global network.

Contact our team for more information:

Frederico Macias
Partner
Risk Advisory – Cybersecurity Leader
Email: fremacias@deloitte.pt
Tel: +351 210422836
Cel: +351 966850347

Inácio Neves
Associate Partner
Risk Advisory
Email: ineves@deloitte.co.mz
Tel: +258 20 600 100
Cel: +258 84 831 7343

Mário Fernandes
Partner
Technology Consulting Leader
Email: marifernandes@deloitte.co.mz
Tel: +258 20 600 100
Cel: +258 84 324 1231

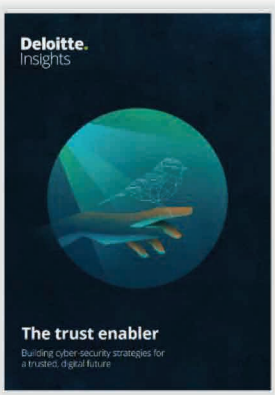
Ayad Issá
Manager
Risk Advisory
Email: ayissa@deloitte.co.mz
Tel: +258 20 600 100
Cel: +258 84 040 8351

Our Market Perspective

Deloitte creates comprehensive thought leadership perspectives for cybersecurity based on our client work and research.

The changing role of the board on cybersecurity: Robust oversight 'Now' for a secure 'Next' - 2021

Securing the public cloud: Addressing the technology and cybersecurity risks associated with public cloud adoption - 2021



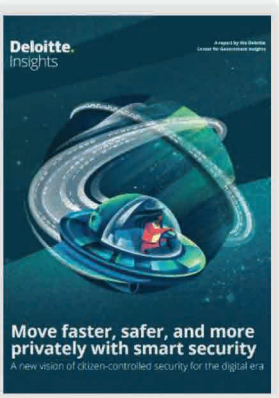
The trust enabler: Building cyber-security strategies for a trusted, digital future - 2021

Leading the way with an adversary focus: Government role in deterring cyberattacks - 2021

Preparing the trusted internet for the age of quantum computing; The data security threat may be more imminent than you think - 2021

Ransomware in critical infrastructure: Ten questions and actions to tackle this major threat - 2021

Future of cyber - 2020



Move faster, safer, and more privately with smart security: A new vision of citizen-controlled security for the digital era - 2019

References

(ITU), I. T. (2018). *Global Cybersecurity Index (GCI).* Geneva: ITUPublications. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Morgan, S. (2020, November 13). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Retrieved from Cybercrime Magazine: https://cybersecurityventures.com/cyberwarfare-report-intrusion/

Política de Segurança Cibernética. (2021, December 31). Moçambique: IMPRENSA NACIONAL DE MOÇAMBIQUE, E. P.

Vumo, A. P., Spillner, J., & Köpsell, S. (2017, August 17). Retrieved from https://digitalcollection.zhaw.ch/bitstream/11475/7417/1/mozambicanwebsites-archive.pdf

Walter, J. (2020, May 2). *COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes.* Retrieved from IMC Group: https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/

Notes:

Deloitte.