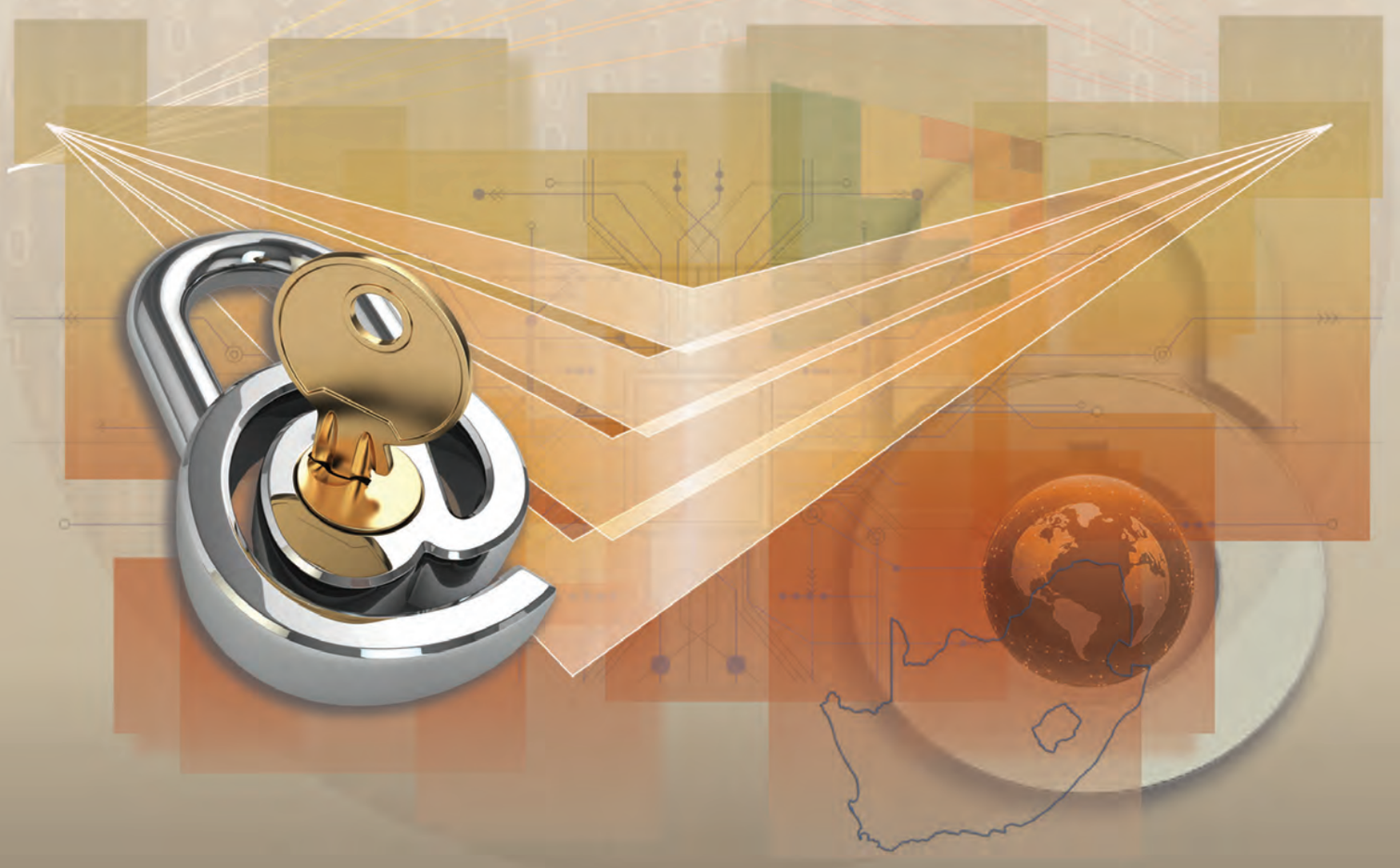
telecommunications
& postal services
Department:
Telecommunications and Postal Services
REPUBLIC OF SOUTH AFRICA

A Baseline Study on Cybersecurity Readiness

A Report of the Department of Telecommunications and Postal Services



Cybersecurity Readiness

Cybersecurity Readiness Report 2017

Published by the Department of Telecommunications and Postal Services, South Africa, Private Bag X860, Pretoria 0001

This report is available on the website: www.dtps.gov.za

Copies are obtainable from: ICT Infrastucture Support, Department of Telecommunications and Postal Services

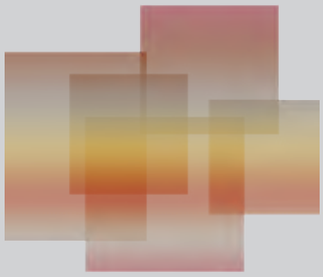
Emai: KiPillay@dtps.gov.za

Tel: +27(0)12 427 8000

www.dtps.gov.za

2017

Contents



1 Foreword by the Minister

Dr Siyabonga Cwele

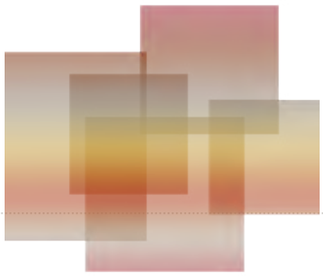
The introduction of ICTs into many aspects of everyday life has led to the development of the modern concept of the information society. Essential services such as water and electricity supply now rely on ICTs, as do most businesses and organisations, as well as citizens. The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries.

ICT applications such as e-government, e-commerce, e-education, e-health and e-environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services. ICT applications can facilitate the achievement of the Sustainable Development Goals, reducing poverty and improving health and environmental conditions in developing countries.

However, the growth of the information society is accompanied by new and serious threats. While technological introduces greater variety and convenience into our lives, it also opens more and more avenues for people to be targeted by cyber criminals. International and domestic cyber criminals increasingly view businesses and private individuals as attractive targets for a range of cybercrime.

Attacks against information infrastructure and Internet services have already taken place, while online fraud and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day. The financial damage caused by cybercrime is reported to be enormous.

This 'digital paradox' means that while governments and organisations can offer more services, more quickly, than ever before, yet at the same time cybercrime has become a powerful countervailing force that's limiting that potential.



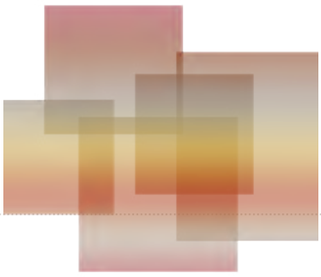
"The introduction of ICTs into many aspects of everyday life has led to the development of the modern concept of the information society"

Cybercrime has been defined as any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them, while 'cybersecurity' is the practice of making the networks that constitute cyberspace secure against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them.

The issue of cybersecurity is high on the agenda of many African governments, with many on the continent increasingly mindful of the shared public private responsibility for cybersecurity, and of the need to mobilise both public and private organisations within a multi-stakeholder model. A growing number of African countries have established - or are in the process of establishing - an enabling policy and legislative environment for cybersecurity.

The South African government's response to the issue of cybersecurity has been promulgation of the National Cybersecurity Policy Framework (NCPF) in 2012, which is aimed at a coherent and integrated Cybersecurity approach to address Cybersecurity threats. The NCPF has also given rise to the Cybercrimes and Cybersecurity Bill, which is currently before Parliament, and which will bring South Africa in line with international laws dealing with cybercrime.

One of the mandates of the Cybersecurity Hub as detailed in the National Cybersecurity Policy Framework (NCPF) is to conduct Cybersecurity audits, assessments and readiness exercises for the sector. In light of this the Department of Telecommunications and Postal Services via its Cybersecurity Hub conducted a nation-wide survey that sought to gather information on strategic initiatives relating to Cybersecurity readiness in South African organisations.



To date there is little reliable data available on the state of readiness of South African organisations (public and private) relating to Cybersecurity readiness. While some studies have been conducted, much of the evidence is anecdotal.

What is encouraging to note from the Survey is that:

- Currently, 37% of organisations have discussed a cybersecurity plan or strategy and will implement it in the future, while 29% have a fully functional plan.

- Notably, 42% of respondents reported that the number of incidents had not increased compared to previous years. This shows a positive trend if cyber incidents are decreasing and shows that controls and measures may be helping to curb an increase in attacks.

While trends point to a positive attitude towards cybersecurity it is incumbent on government and organisations remain vigilant to ensure that we build confidence in our citizens and institutions to transact and socialise in cyberspace.

Message from the Deputy Minister

2

Ms Stella Ndabeni-Abrahams

Cybercrime and cybersecurity are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cybersecurity addresses cybercrime as one major challenge underlines this. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.

2017 saw a large number of attacks against national infrastructure, data breaches involving the information of private citizens, and large-scale attacks against organisations. How governments respond is now under the spotlight and the type of enabling environment they foster to respond to these increasingly sophisticated attacks, is under scrutiny.

It is against the backdrop of the National Cybersecurity Policy Framework (NCPF) that the Department established a Cybersecurity Hub in October 2015, which is aimed at creating a platform for South Africans to report cyber incidents and assist victims of cybercrime. Part of the Hub's mandate is to implement a national Cybersecurity Awareness program, which is critical towards ensuring that citizens take advantage of the information age, whilst remaining conscious of the threats and vulnerabilities of cyberspace.

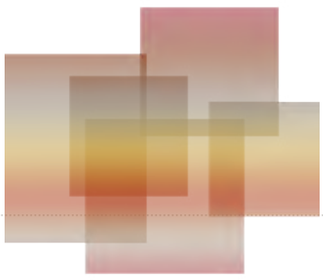
Cybersecurity is a national imperative and as such demands a coordinated and holistic approach. This is even more so for Cybersecurity Awareness initiatives which must reach all residents of a country. Currently, DTPS Cybersecurity Awareness programs are being disseminated utilising a mass media strategy (billboards, magazines etc.), and also through the Cybersecurity Hub's website. Sector-specific organisations such as SABRIC and ISPA already produce Awareness campaigns, whilst organisations such the South African Communications Forum have plans to produce awareness information.

Cybersecurity Awareness is a matter of cultural challenge and behavioural change. Getting people to act is the primary challenge; usually they will act only when they have been exposed to security problems, or somebody they know has been. Young users can be good promoters of a message and through educating them, parents can often be reached as well. The earlier the education starts, the stronger the effects on users' Internet behaviour.

The Department through the Cybersecurity Hub has also developed a national Cybersecurity Awareness Portal which will be the repository for all Awareness material and the main conduit for the dissemination of Cybersecurity Awareness programs and information. The Awareness Portal will be kept current with content via relationships with the private sector with organisations such as the South African Banking Risk Information Centre (SABRIC) having agreed to partner on rolling out programs via the Portal.

The Department, in line with international initiatives, has adopted October as National Cyber Security Awareness Month, which is an annual campaign to raise awareness about cybersecurity. The campaign further seeks to:

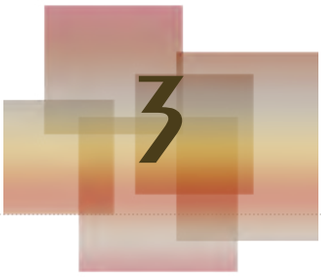
"Cybercrime and cybersecurity are issues that can hardly be separated"



- Promote engagement between national and Provincial Government Departments to start a platform of dealing with cyber security.
- Stimulate relevant industries to increase Cyber Security in South Africa.
- Provide a platform for Cyber Security Companies to provide their services to the South African Community.
- Mobilise service providers to focus on delivering improved cyber security at the homes (communities) in South Africa.
- Create awareness to communities, learners, youth, business and Government.

With regards to Awareness and training, it is pleasing to note that 57% of the organizations reported having implemented cybersecurity awareness programs with at least 70% of their core business staff attending such training sessions. This is observably something to be built upon and the Department is actively encouraging and pursuing the development of training programs.

Cybersecurity is indeed a shared responsibility. It is against this background that the department intends to partner with both public and private organisations to jointly run programs that will spread the cybersecurity messages and ensure that South Africans are "cyber-astute".



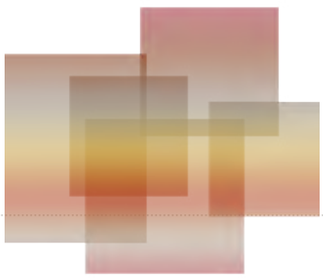
Introduction

Attacks against information infrastructure and Internet services are now commonplace, and 2017, in particular, has seen a large number of attacks, which has placed the burden of protecting citizens firmly on governments and organisations. Cyber-attacks can cost a country in terms of lost revenue, availability of services and diminished reputation and the economy and indeed the citizens need to be protected against harmful cyber-attacks. As a developing nation, South Africa will almost invariably become a target for cyber-attacks and with more services becoming digital, the potential for cyber-attack also increases. Cyber knowledge, especially in developing areas, may not be strong enough to defend against even the more common type of attacks such as phishing, malware infection or identity theft.

The Cybersecurity Hub is one of the national Computer Security Incident Response Teams (CSIRTs) mandated by the country's National Cybersecurity Policy Framework (NCPF), under the Department of Telecommunications and Postal Services (DTPS),One of the mandates of the Hub is to co-ordinate attack information and provide support for cyber incidents. This initiative of surveying the current state of cyber readiness in certain sectors of the country is aimed at determining the current levels of cybersecurity resiliency, planning and contingency. The main objective of this survey is to report on the current level of governance, threat, awareness and incident response capability.

The Cybersecurity Readiness Survey assesses whether critical business functions and infrastructure can remain operational and be minimally affected by unplanned or malicious interruptions.

In this, the first instalment of the Cybersecurity Readiness Survey, we begin the process of looking at the current state of cyber readiness in South Africa. It is important to identify the current state of cyber readiness and establish a baseline of current cyber readiness capability. A valuable contribution made by the survey are the details on current cyber readiness capabilities, skills and areas of concern.



1.1 NCPF and the Cybersecurity Hub

South Africa's response to the issue of Cybersecurity is premised on the NCPF, which was passed in 2012. The NCPF provides the over-arching framework and strategy within which an emerging legislative and regulatory framework will be established.

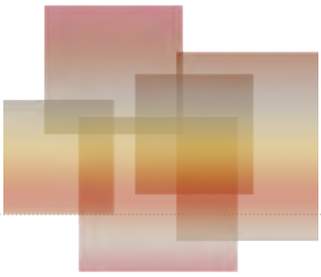
The NCPF provides a broad framework and specifically mandates the establishment of multiple national CSIRTs, including the Cybersecurity Hub under the DTPS, which has a mandate to coordinate and promote cybersecurity measures within the private sector and civil society. The Cybersecurity Hub works closely with the other national CSIRTs.

1.2 Readiness Survey

Part of the mandate of the Cybersecurity Hub is to determine the cybersecurity posture of the country, conduct readiness exercises and provide guidance and best practice guidelines. We believe that these initiatives are best achieved by projects that are rooted in empirical research. With this in mind, the Cybersecurity Hub, together with its research partner, the CSIR, conducted a nation-wide Cybersecurity readiness survey that sought to gather information on strategic initiatives related to cybersecurity in South African organisations. The survey gathered information on, *inter alia:*

- The status of strategic cybersecurity plans in organisations;
- Governance relating to the cybersecurity function in organisations;
- Potential cybersecurity vulnerabilities and risks that have been identified in organisations;
- The capability of organisations to respond to, and recover from a cybersecurity related attack.

[1] Data has been rounded during the analysis and the interpretation phase.



The objective of the survey was to determine a baseline with respect to cybersecurity readiness and planning across multiple sectors. The survey was divided into seven sections:

- Cybersecurity Strategy/Plan
- Governance
- Standards
- Sector CSIR Establishment
- Cybersecurity Awareness
- Vulnerabilities and Risk Assessment
- Incident Management and Business Continuity

The report commences with an Executive Summary that provides the most pertinent findings.[1]

Executive Summary

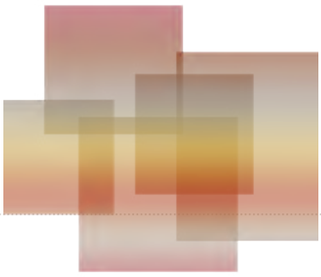
The DTPS, together with the CSIR as its research partner, conducted a Cybersecurity Readiness Survey in 2017, in order to establish a baseline of the current security status in key sectors in the country. Limited research has been published regarding the current cybersecurity strategies/plans, governance, use of standards, establishment of CSIRTs, awareness, risk assessments, incident management and business continuity. It is envisaged that the survey results will assist respondents to become more aware of the value of the data and help better align and streamline their organisations to respond to and prepare for cyber-attacks.

Notably, 42% of respondents reported that the number of incidents had not increased compared to previous years. This shows a positive trend if cyber incidents are decreasing and shows that controls and measures may be helping to curb an increase in attacks. Furthermore, organisations have reported that, for the most part, the types of incidents have changed from previous years (42%). This indicates that organisations will need to prepare, adapt and respond to changing incident types and that they cannot rely on tried and tested methods of current attacks.

As is the case for most organisations, the cybersecurity budget formed part of the IT budget of 69% of the surveyed organisations. Similarly, the most common department contributing to the cybersecurity plan/strategy was the IT Department (80%). These results are to be expected, as cybersecurity tends to fall under the IT department in most organisations.

Only 28% of organisations had a Chief Information Security Officer, with 27% of organisations having a Chief Technology Officer. Most organisations (76%) had a Chief Information Officer/IT Executive. This links closely to the result that 53% of organisations had their Chief Information Officer/IT Executive lead the cybersecurity plan/strategy.

> "Only 28% of organisations had a Chief Information Security Officer"



The top three challenges facing organisations with regard to cybersecurity was insufficient skills (57%), lack of in-house skills (49%), and the lack of awareness (39%). This result indicates the importance of skills development/recruitment and creating awareness.

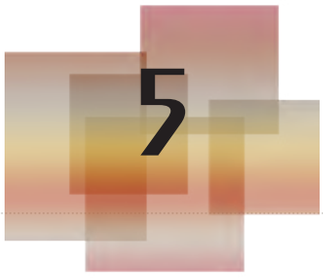
Targeted malicious emails and ransomware are the top threats that are of concern to organisations. Both targeted malicious emails and ransomware have become more widespread in recent years. Spam, phishing emails and attractive links can be crafted into tricking users into revealing personal information or clicking on links that encrypt their machines. These forms of computer network exploitation are a concern to organisations, as they may reveal or erase sensitive information. More awareness is required to educate organisations about the dangers of attachments and safe surfing practices, to prevent their systems from being taken hostage.

CSIRTs serve as a single point of contact for reporting incidents and they help to disseminate important incident-related information. Of the organisations surveyed, 45% belonged to a CSIRT and 22% were obliged to report incidents. CSIRTs can help coordinate response efforts with similar institutions and aid with intelligence gathering. Through CSIRTs, networking and sharing of incident information can help organisations to correct weaknesses.

Threat intelligence can provide useful capability in trying to manage the increase in cyber attacks, by collating data to gain new insights and determine trends. Threat intelligence can contribute significantly to the development of detective and reactive action, by investigating the source, motivation and capabilities of the perpetrators. Currently 25% of the surveyed respondents had a threat intelligence capability, with another 20% of respondents indicating this was in development. This shows that the large majority of organisations have recognised that threat intelligence is a growing requirement.

For most organisations surveyed, employees pose a bigger threat than criminals from outside the organisation. Insiders may try to abuse systems and information for fraudulent use, theft and personal gain. Insiders have the advantage of being in close proximity to the systems and data and may not need to hack into an organisation's network. Organisations may find it harder to protect their systems from insiders, who already have legitimate access to the organisation's information and assets.

About the Respondents



Most of the 83 respondents who participated in the 2017 Cyber Readiness Survey were security managers and mainly worked in the cyber security field. Respondents were required to have a basic cybersecurity background and knowledge of their organisation, in order to answer the questions posed.

5.1 Sector Types - The main sectors

The sectors represented in this survey include banking, finance, government, defence, higher education, research, information technology (IT) and telecommunications.

The sectors in which the respondents worked was as follows: government and defence – 31%; banking and finance – 29%; higher education and research – 19%; IT and telecommunications – 20%. See Figure 1.

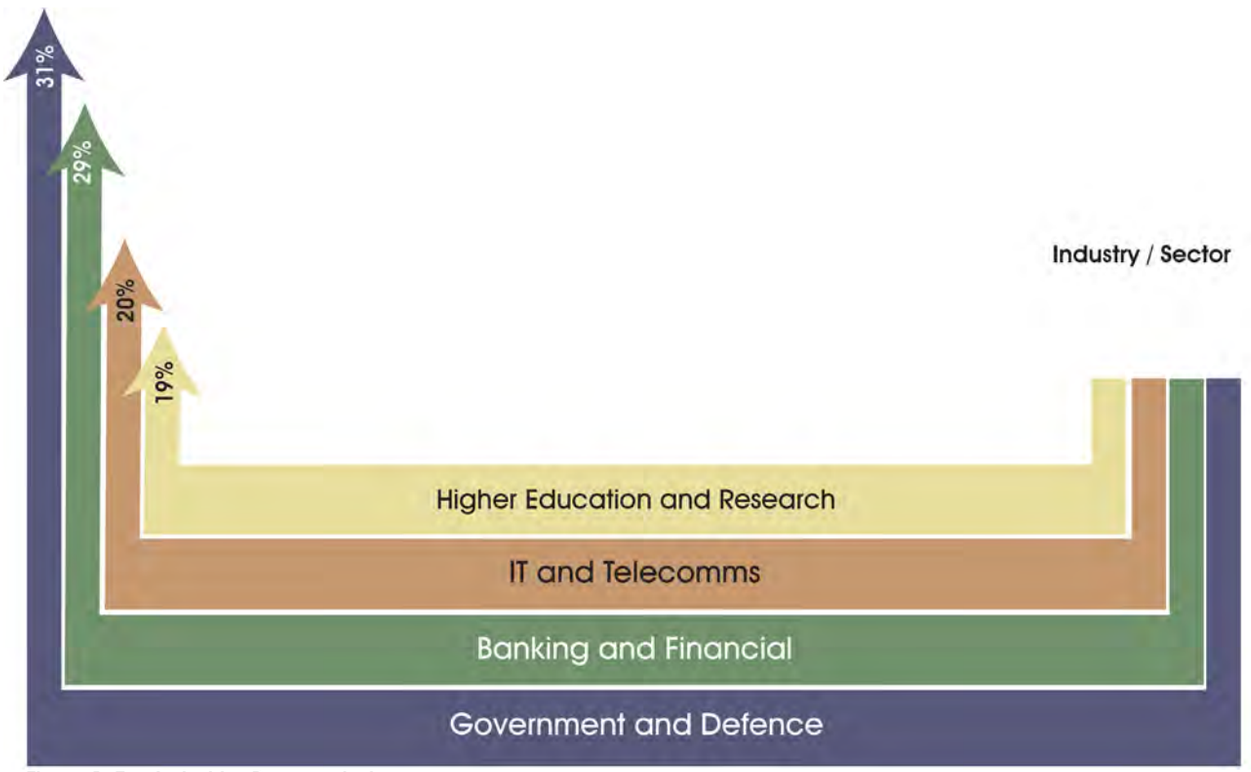


Figure 1: Top Industries Represented

5.2 Size of Organisations

Organisation size represented in the survey were largely in favour of very small organisations, with 55% having 1-999 employees. Just over 17% of the respondents work in a large organisation with more than 5000 employees; 11% are from medium-size organisations that have 2000-3999 employees; while another 17% work for small organisation that have 1000-1999 employees. (See Figure 2).

It is worth noting that for small to medium organisations, organisational size does not significantly affect the readiness of an organisation for cybersecurity. It is when the organisation becomes large that the readiness of the cybersecurity organisation becomes impacted. An increase in the number of cyber security experts within an organisation is needed to protect a large organisation.

Figure 2: Respondent Organisation Size

Results

6

Data about cyber readiness can help organisations determine their ability to respond to cyber incidents and manage cybersecurity. The collection of data in this survey helps to establish a baseline of the current state of cyber readiness in the country. It is useful to provide indicators for governance, planning, awareness, incident readiness, CSIRT membership and risk assessment trends.

In this section, the results of the survey are presented. The first section addresses questions relating to an organisation's cybersecurity strategy/plan.

"In this section, the results of the survey are presented"

6.1 Cybersecurity Strategy/Plan

6.1.1 Current state of plans

The state of an organisation's security and prosperity lies in strong digital and governance foundations. A key component of the foundation is a sound cyber plan/strategy. A cyber plan/strategy lays the foundation and provides the fundamental principles for how an organisation plans to tackle cybersecurity, including key aspects such as risk management, awareness, standards and incident response.

Currently: 37% of organisations have discussed a cybersecurity plan/strategy and will implement it in the future; 29% have a fully functional plan. Of the organisations surveyed: 18% are in the process of developing a plan and are aiming for implementation in the next 6-12 months; 7% have no plan in place; 8% are uncertain about their organisation's current cyber security plan/strategy. (See Figure 3).

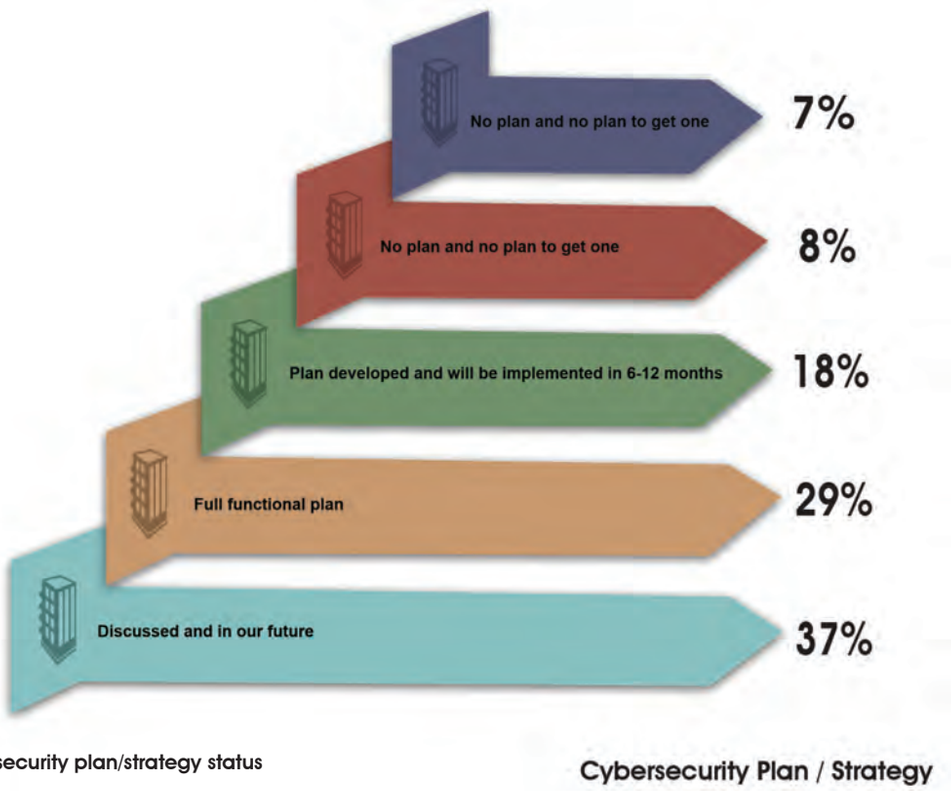


Figure 3: Cybersecurity plan/strategy status

6.1.2 Review of cybersecurity strategy/plan

Most organisations review their plans annually (33%). A number of organisations do not have a plan (20%) or review it intermittently (18%); 7% of the organisations surveyed never review their cybersecurity strategy/plan.

Plans and strategies require regular review, in order to ensure that they stay relevant and that cognisance is taken of emerging trends impacting organisations. (See Figure 4).

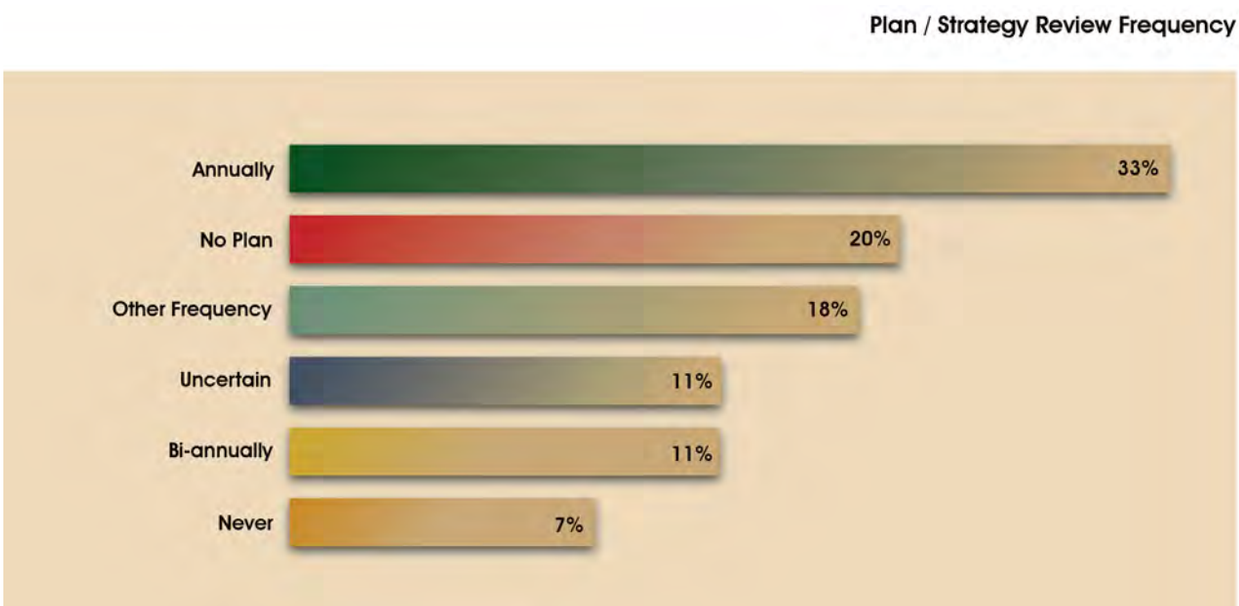


Figure 4: Plan/Strategy review frequency

6.1.3 Leads Development/ Revision of Cybersecurity Plan/Strategy

In more than half of the surveyed organisations (53%), the Chief Information Officer (CIO) or an IT Executive leads the development or revision of the Cybersecurity plan/strategy. 16% of the respondents were uncertain of who leads the development/revision of the plan/strategy in their organisation; 14% indicated it is led by the Chief Information Security Officer (CISO). The remainder 14% was divided into other categories like the Chief Operating Officer, Chief Risk Officer/Risk Executive, Chief Executive Officer/Managing Director, and Chief Financial Officer/Financial Executive (See Figure 5).

Many organisations may not have a CISO and therefore the cybersecurity strategy/plan tends to be led by the CIO.

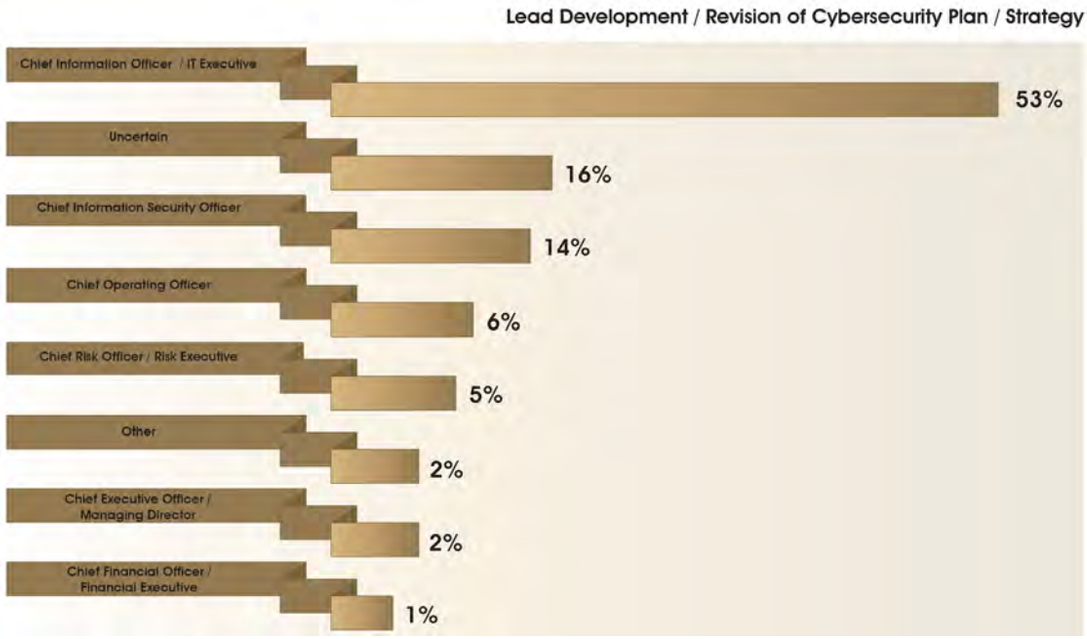


Figure 5: Lead Development/Revision of Cybersecurity Plan/Strategy

6.1.4 Departments contributing to cybersecurity strategy/plan

The majority of organisations have their IT department contributing to the development/ revision of the cybersecurity strategy or plan. Another major contributor in many organisations is the Audit and Risk Departments (42%). 12% of organisations receive contributions from the Finance Department (See Figure 6).

The IT department tends to be the largest contributor to the cybersecurity strategy/plan as cyber security typically falls within the domain of IT. The Audit and Risk Department may also contribute to the cybersecurity strategy plan as risk assessment forms a key component of cybersecurity governance. Risk identification and mitigation need to be addressed in the cybersecurity strategy/plan.

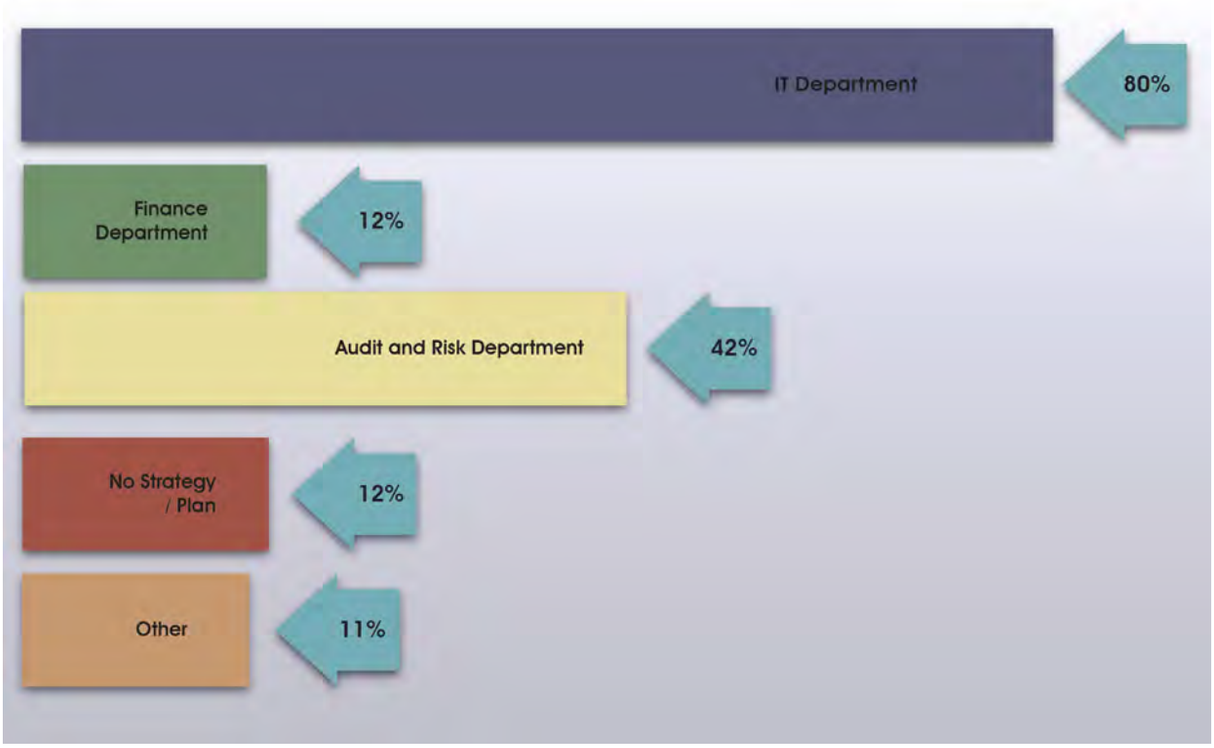


Figure 6: Departments contributing to cybersecurity strategy/plan

6.2 Governance

6.2.1 Separate Department for Security

Cybersecurity tends to fall in the overall IT budget, as it is a component of securing assets, infrastructure and systems. However, some organisations may allocate a separate budget to it, to ensure that dedicated funds are spent on security and not just on IT solutions.

The majority of respondents did not have a separate department/sub-department tasked with cybersecurity. A small percentage was not sure whether their organisations had a separate department/sub-department tasked with cybersecurity. (See Figure 7).

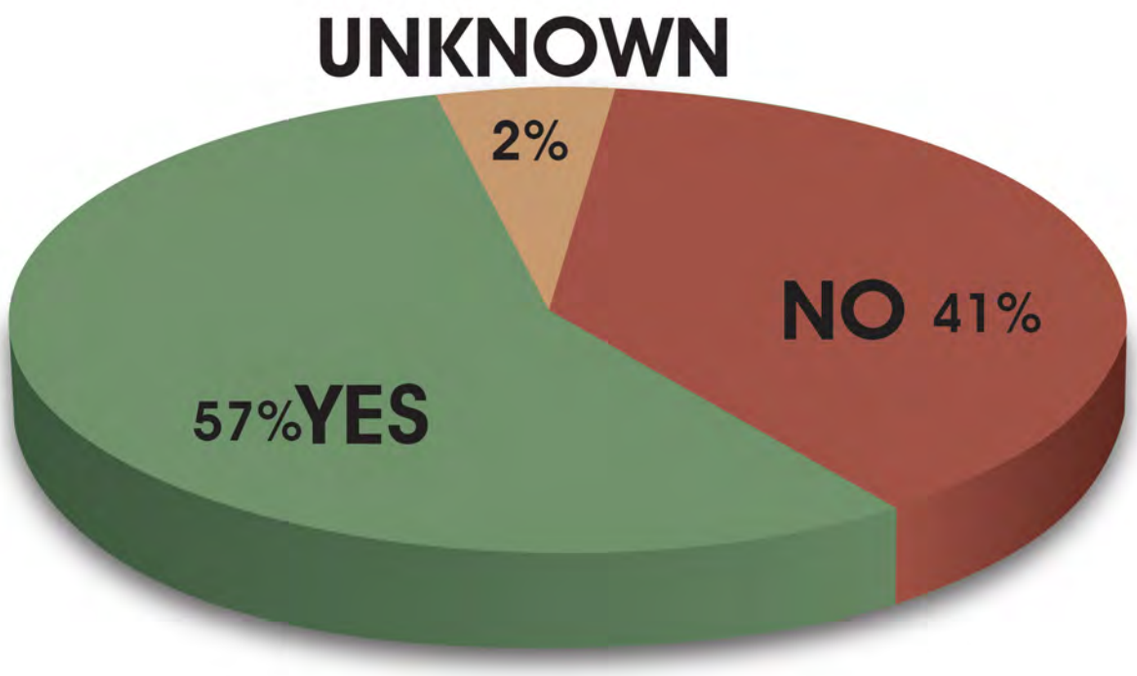


Figure 7: Separate Department for Cybersecurity

6.2.2 Security Roles Defined

The largest percentage of respondents (76%) had a Chief Information Officer(CIO)/IT Executive in their organisations; 48% had a Chief Risk Offer/Risk Executive, 28% had a CISO; and 27% had a Chief Technology Officer (CTO). (See Figure 8.)

The need for a separate C-suite for security helps prioritise the security of business information, infrastructure and systems. Many companies have a CIO and a CTO, but not a Chief Information Security Officer (CISO). A dedicated CISO serves as a dedicated security specialist who has deeper knowledge of the threat landscape, defensive approaches and insight into risk mitigation.

The main role of a CISO is to help assess threats and present this information to C-suite members, as input to critical decisions that have to be made for the organisation. As a specialised role, a CISO possesses expert cybersecurity skills that can be weaved into an organisation's operation.

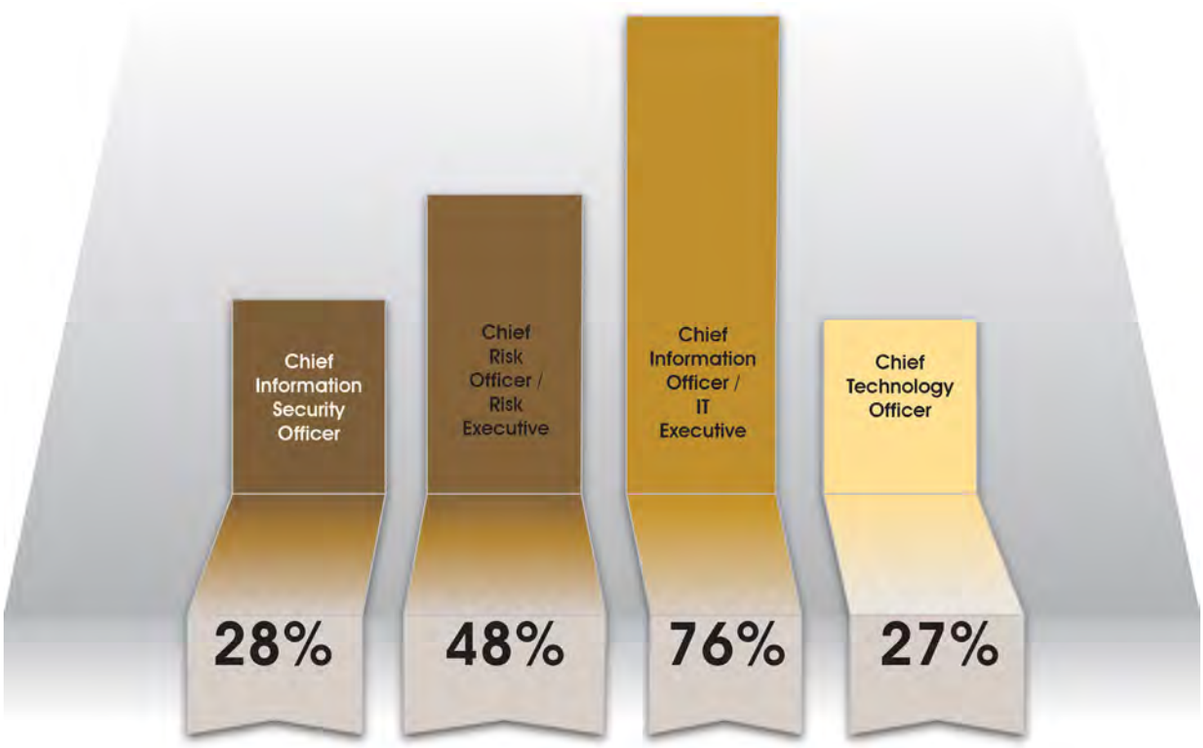


Figure 8: Cybersecurity Roles in the Organisation

6.2.3 Management Roles and responsibilities

Organisations need to protect their infrastructure and technology. In order to achieve this, various controls, roles and responsibilities need to be implemented. Currently, the most common management roles and responsibilities assigned in the organisations surveyed were network security, business continuity/disaster recovery, and policy creation and maintenance.

More than half of the respondents are involved in incident management, data security, access control and Intrusion Detection System (IDS). (See Figure 9). Among the other management roles and responsibilities are Mobile Platform Security, Cloud Security, Insider Breach Monitoring, Physical Security, Crypto, Service Provider Security and End Point Security.

Overall, organisations are focusing heavily on the network and data security, as well as preventing threats through policy creation and risk management.

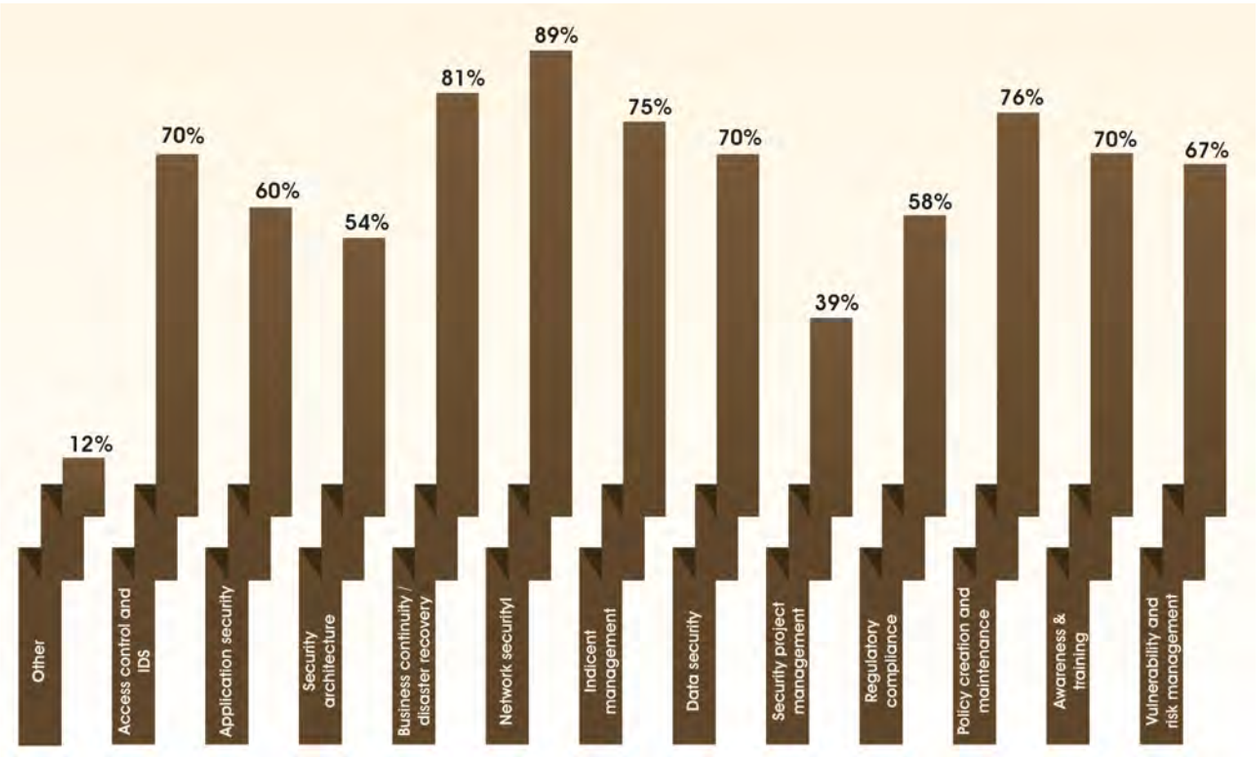


Figure 9: Management Roles and Responsibilities Assigned

6.2.4 Budget

The difficulty in justifying a cybersecurity budget is that it does not show a clear return on investment. However, a beach in cybersecurity could result in an organisation closing its doors or a major loss of confidence. That is why it is important to have adequate cybersecurity and to budget to protect the organisation.

The majority of respondents reported that their organisations do not have a separate budget for cybersecurity (67%); 10% were uncertain whether their organisation had a separate budget for cybersecurity. (See Figure 10).

Typically, separate budgets may not be allocated to cybersecurity, but may form part of an over-arching capability such as IT (as indicated in Section 6.2.5).

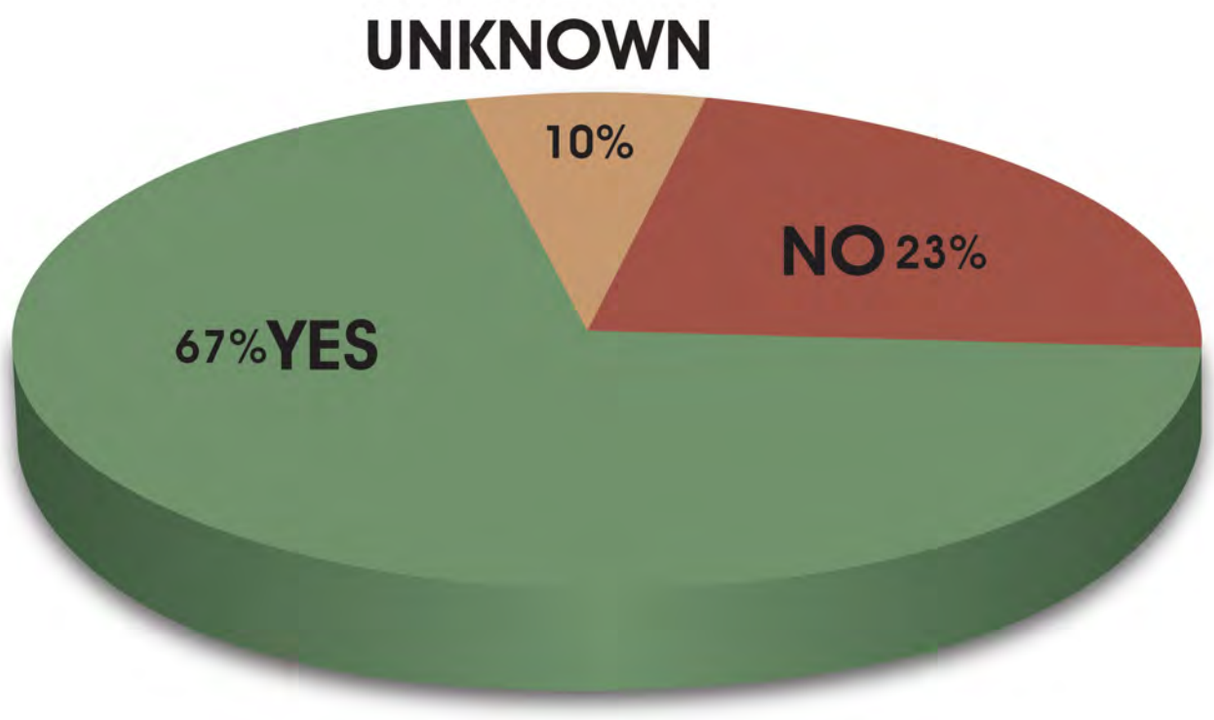


Figure 10: Cybersecurity Budget

6.2.5 Department in which Budget Forms Part

For the majority of respondents, the cybersecurity budget is part of the IT department (69%); 16% reported that there was no budget; 8% were uncertain of which department included the cybersecurity budget. 6% reported that their organisation had its own budget for cybersecurity. See Figure 11.

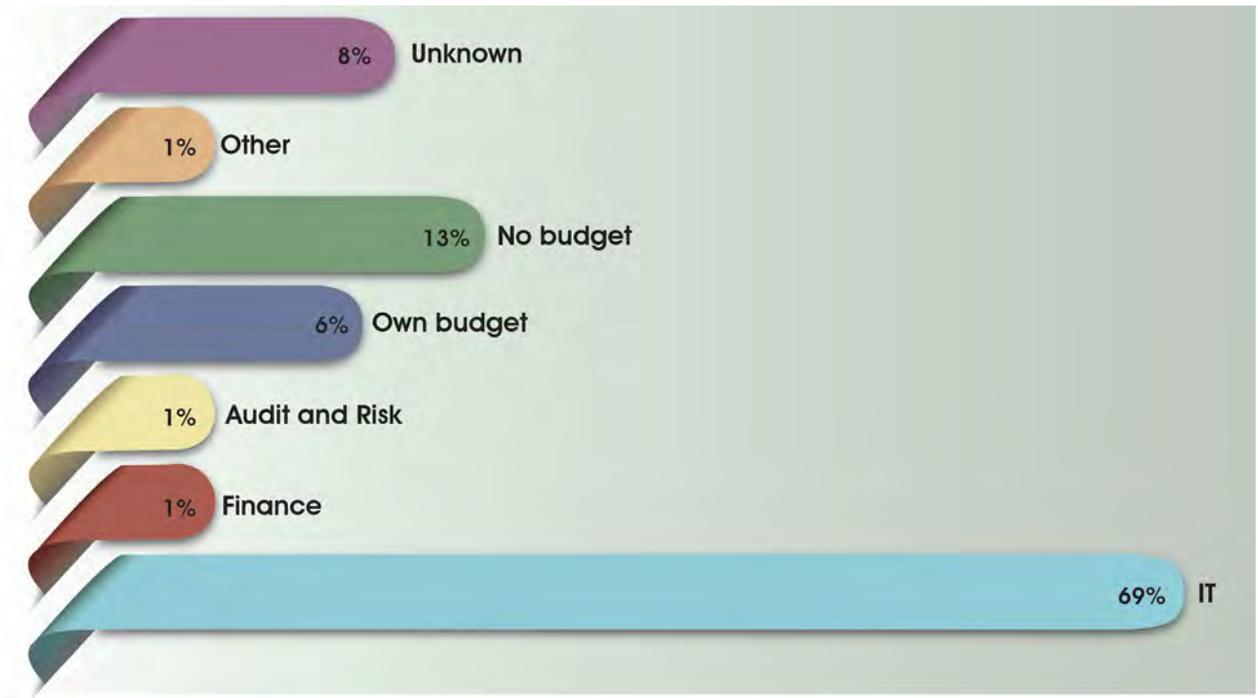


Figure 11: Department in which budget forms part

6.2.6 Cybersecurity Function Reporting

Ownership of cybersecurity has traditionally remained with the CIO of an organisation. However, with cybersecurity affecting the bottom line and business continuity, more organisations are seeing the need for cyber security to be reported at board level.

More than half the respondents answered CIO (52%) in response to the question on where the cybersecurity function reports within the organisation; 13% answered CEO; 13% said Other. See Figure 12.

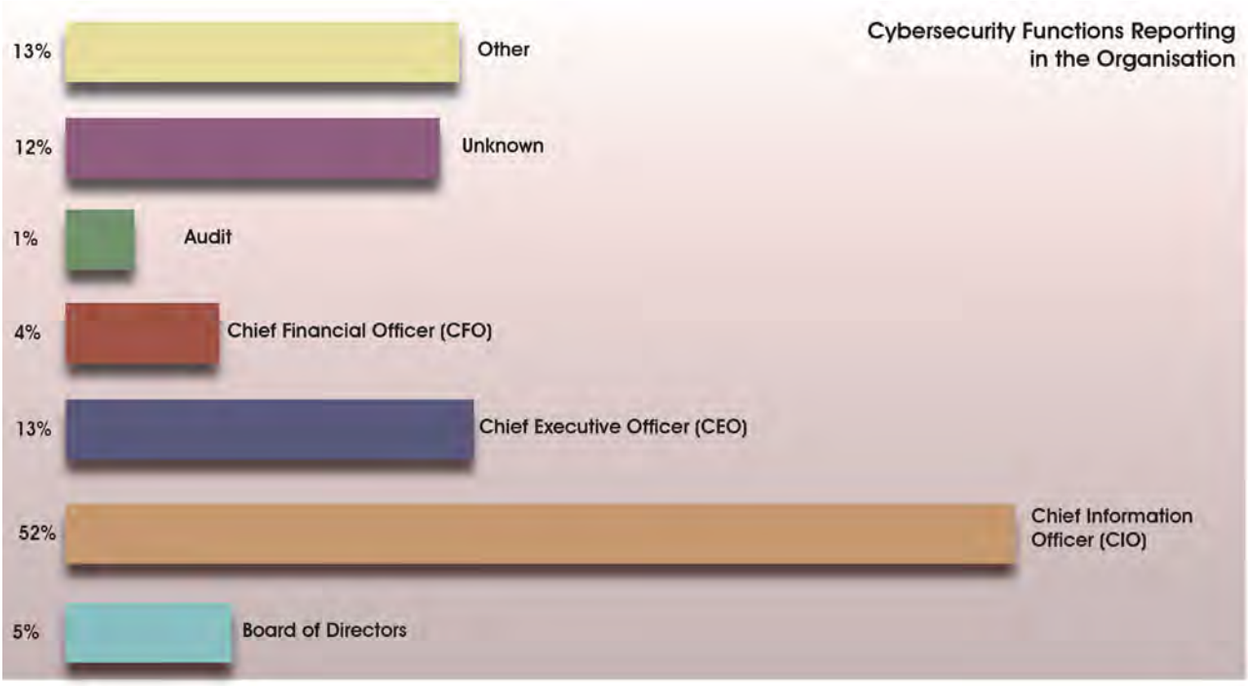


Figure 12: Cybersecurity Functions Reporting In the Organisation

6.3 STANDARDS

6.3.1 Organisational Alignment to Standards

The majority of respondents align to the ISO 27001 family of standards (61%). Other standards that are followed by more than one-third of respondents are NIST (36%) and SANS (31%). Some of the additional standards that organisations need to comply with are COBIT, Corporate Governance of ICT Policy Framework (CGICTPF) and Payment Card Industry (PCI). See Figure 13.

The ISO 27001 family of standards consists of best practices and recommendations for information security management and risk management through security controls in an overall information security management system (ISMS). It is very wide in scope and covers various aspects, including confidentiality, privacy and technical aspects of cybersecurity. ISO 271001 is applicable to organisations of different sizes and domains. The standard was compiled by the International Organisation for Standardisation (ISO) and more specifically the ISO/IEC JTC1 (Joint Technical Committee) SC27 (Sub-committee 27).

The National Institute of Technology and Standards (NIST) is another popular set of standards to which many international companies aim to conform. It consists of a cybersecurity framework that was created in a collaborative effort between government and industry. This framework entails standard, guidelines and practices aimed at protecting critical infrastructure to manage cyber risk.

The SANS Institute also serves as a resource for the security community to aid with the development and implementation of security policies and guidelines for cybersecurity. SANS is well-known for its training capability, but also provides support for cybersecurity implementation and guidance.

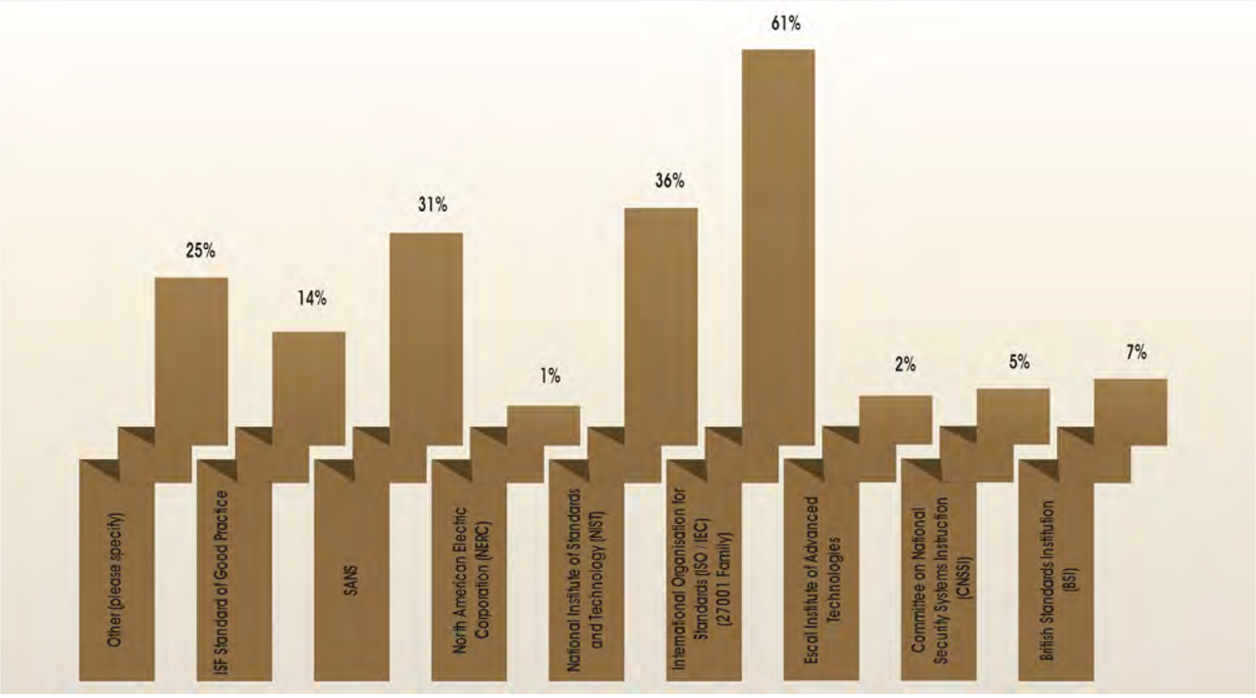


Figure 13: Alignment to Standards

6.4 Sector CSIRT Establishment

6.4.1 Membership to a Sector CSIRT

In the current digital world, it is becoming increasingly difficult to keep infrastructure and data secure. Attacks are becoming more prominent and most organisations have to develop strategies to deal with impending threats. System and network administrators may not always be able to deal with cyber threats and external help may aid in protecting business assets and systems. CSIRTs serve as a single point of contact for reporting incidents and helping to disseminate important incident-related information. Membership of a CSIRT means the organisation has access to a reliable team that can aid with quicker incident response and with mitigating emerging threats.

Of the organisations surveyed, 45% belong to a CSIRT. A substantial percentage of respondents (40%) did not belong to a CSIRT. (See Figure 14.) CSIRT membership provides a community of support for incident response and threat mitigation. The support, expertise and information that organisations receive provides great benefit from being a member of a CSIRT.

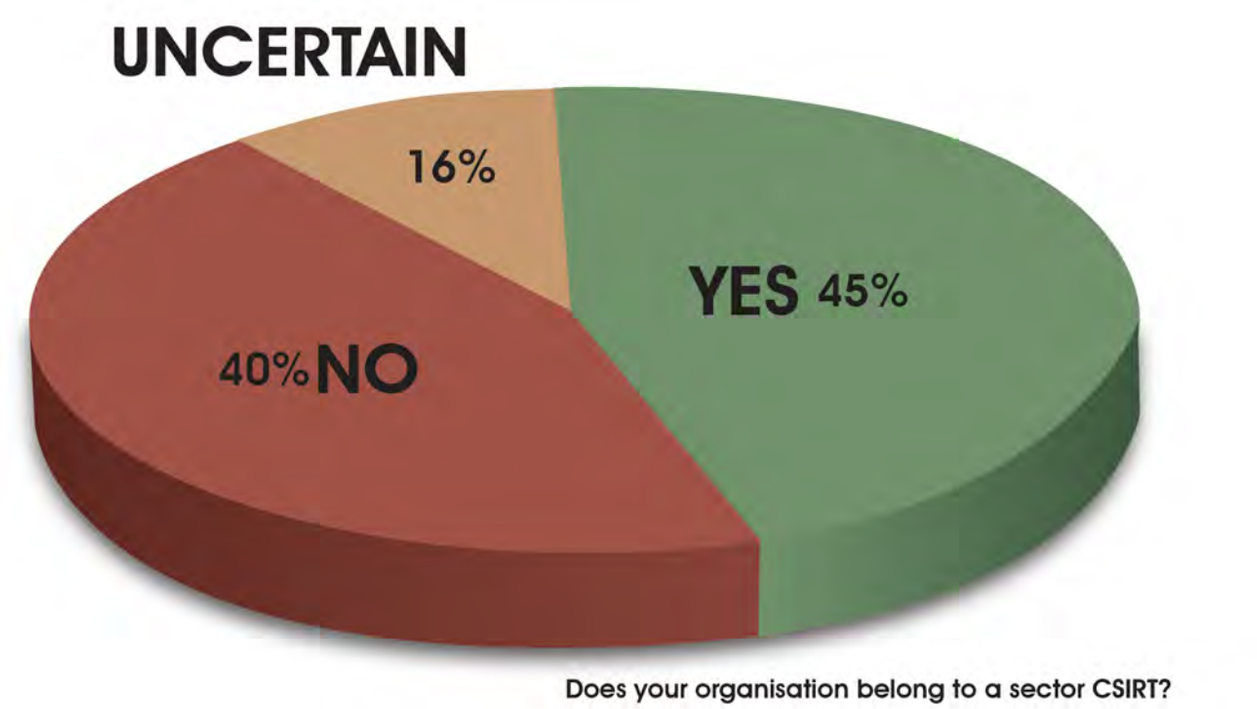


Figure 14: Membership to a Sector CSIRT

6.4.2 Reporting of Incidents to Sector CSIRT

22% of the respondant organisatons were obliged to report incidents. CSIRTs can help coordinate response efforts with similar institutions and also aid with intelligence gathering. Through CSIRTs, networking and sharing of incident information can help organisations to correct weaknesses.

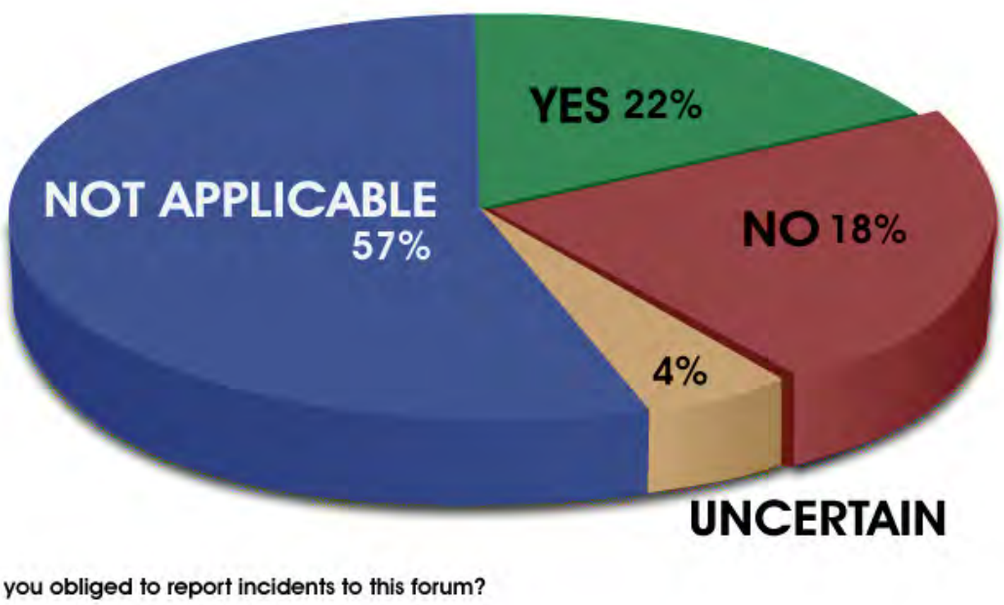


Figure 15: Reporting of Incidents to sector CSIRT

6.5 Awareness

6.5.1 Offer Cybersecurity Awareness Training

When it comes to the provision of cybersecurity awareness training: the majority of organisations (57%) responded yes; 29% were not certain whether their organisations offer cybersecurity awareness training. (See Figure 16.)

Systems, networks and devices all connect with each other and have become shared resources. It is also important that all employees use IT infrastructure safely and security systems to prevent falling victim to a scam. In order to promote good cyber behaviour, employees should be made aware of current and emerging threats, weaknesses and risks. Cyber security awareness can play an important role in informing and educating employees about cyber dangers.

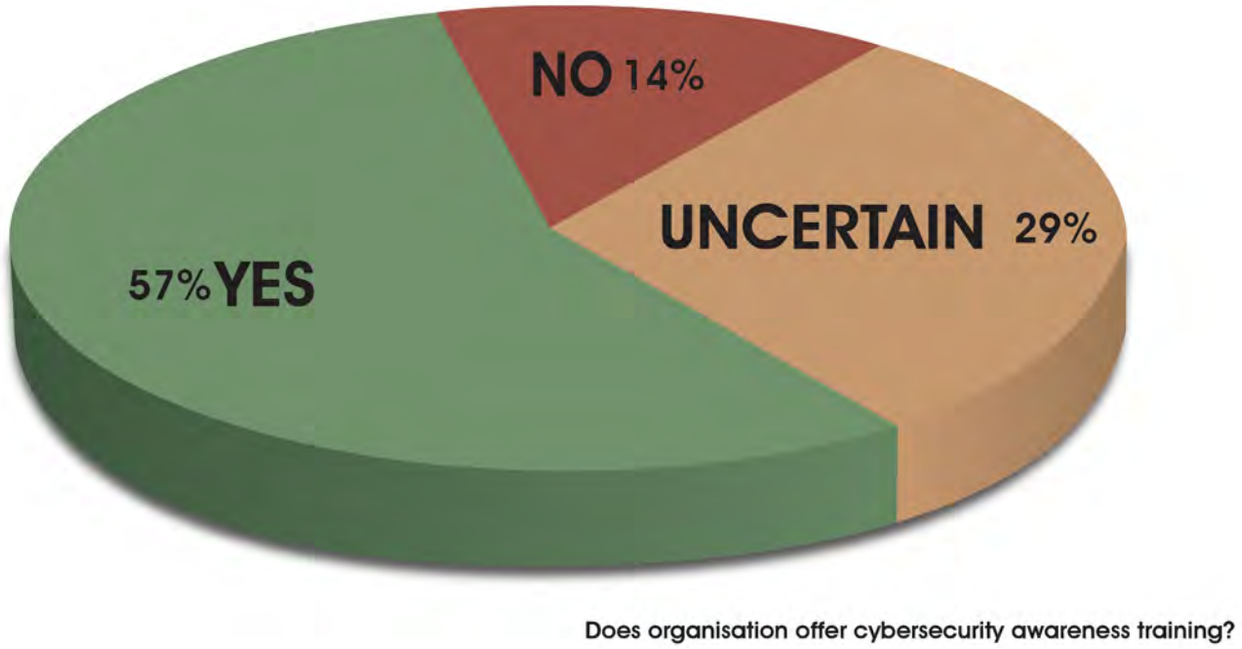


Figure 16: Offers Cybersecurity Awareness Training

6.5.2 Level of Security Awareness Training

When it comes to the level of security awareness training, the responses were widely spread: 27% of organisation offer beginner training; another 25% provide a hybrid mix of training; only 5% offer advanced training; 19% provide intermediate training. See Figure 17.

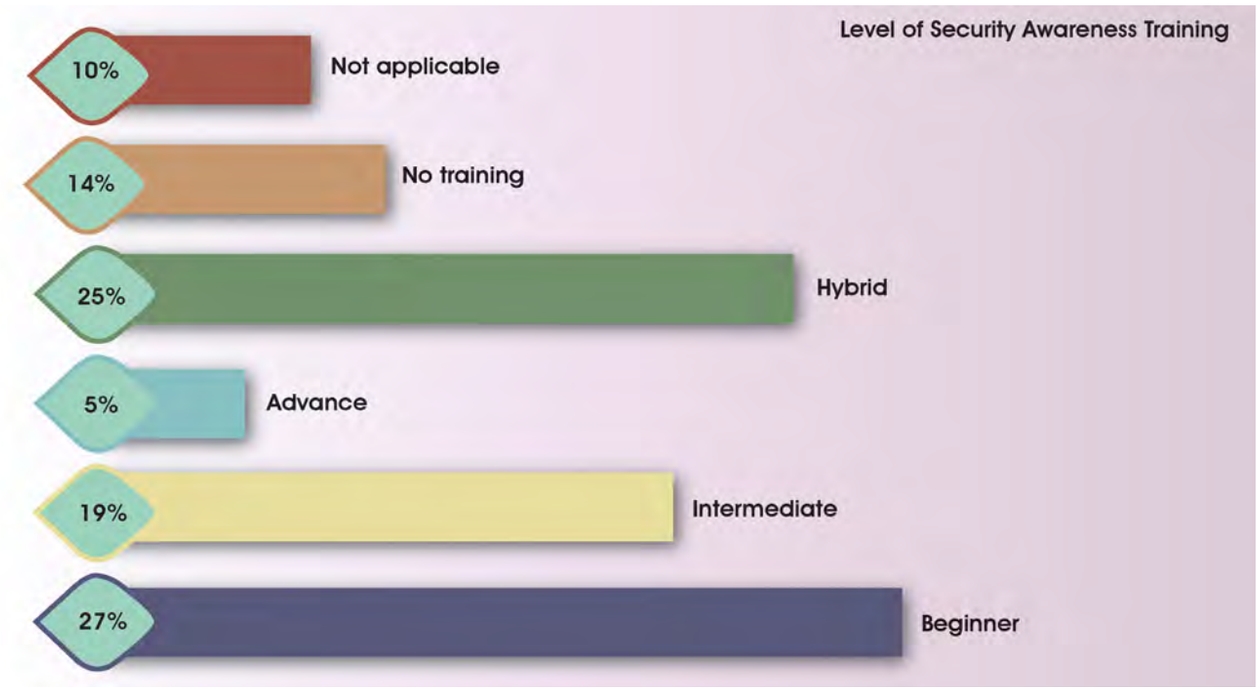


Figure 17: Level of Security Awareness Training

Once the foundation of cybersecurity awareness has been established with beginner training, employees can also benefit from more progressive training. A good mix of training that consists of beginner, intermediate and more advanced concepts will help employees learn the basics about cybersecurity, and also arm them with strong skills to help defend against more complex cyber-attacks.

6.5.3 Training Provider

For the majority of respondents (61%), the training provider was in-house. A small percentage of organisations use an external vendor (8%) or an affiliated organisation (4%). See Figure 18.

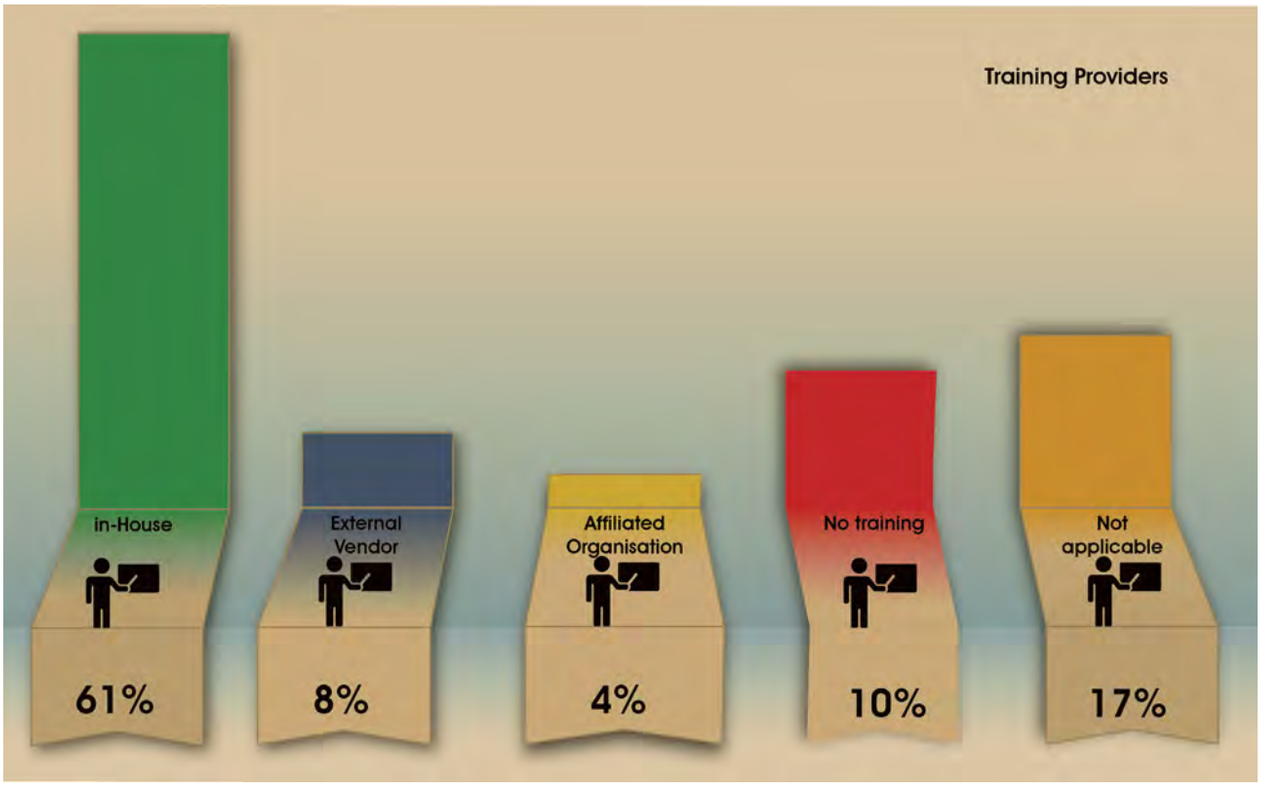


Figure 18: Training Providers

The selection of training providers may be affected by the budget. Using in-house training providers may be more cost-effective than sourcing an external vendor. The development of cyber awareness programmes will then have to be done by the in-house training partner.

6.5.4 Training Participants

On the issue of who attends cybersecurity awareness training, the responses were quite widely spread. Although 70% of core business staff in organisations attended cybersecurity awareness training, there is significant attendance by other groups of participants, e.g. support staff (69%), supervisors/functional managers (59%) and middle management (57%). See Figure 19.

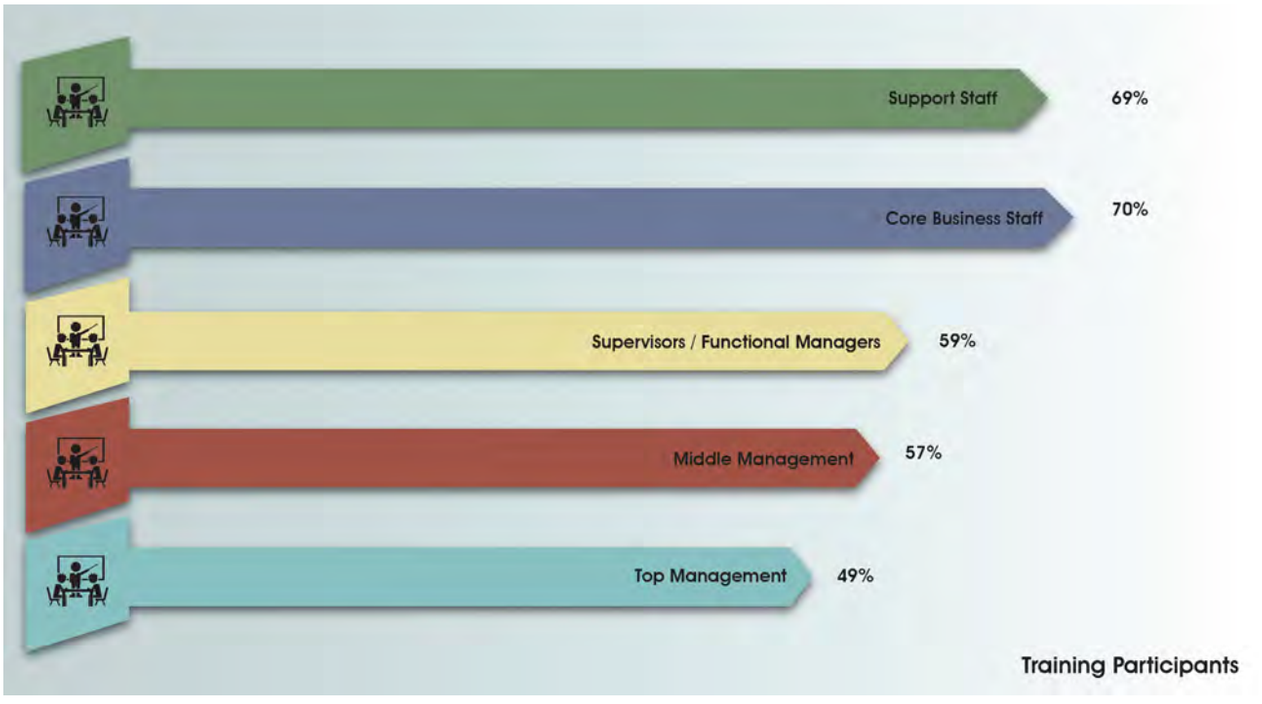


Figure 19: Cybersecurity Awareness Training Participants

6.5.5 Frequency of Cybersecurity Awareness Training

The most common frequency for cybersecurity awareness training was annually (28%) and quarterly (20%). Other responses were split between bi-annually (11%), never (13%) and unknown (28%). The responses were quite varied, with a fairly even split across the various frequencies. It is a challenge to balance the regularity of security awareness and reducing interest in attendees, as the impact is reduced when training is done too often. See Figure 20.

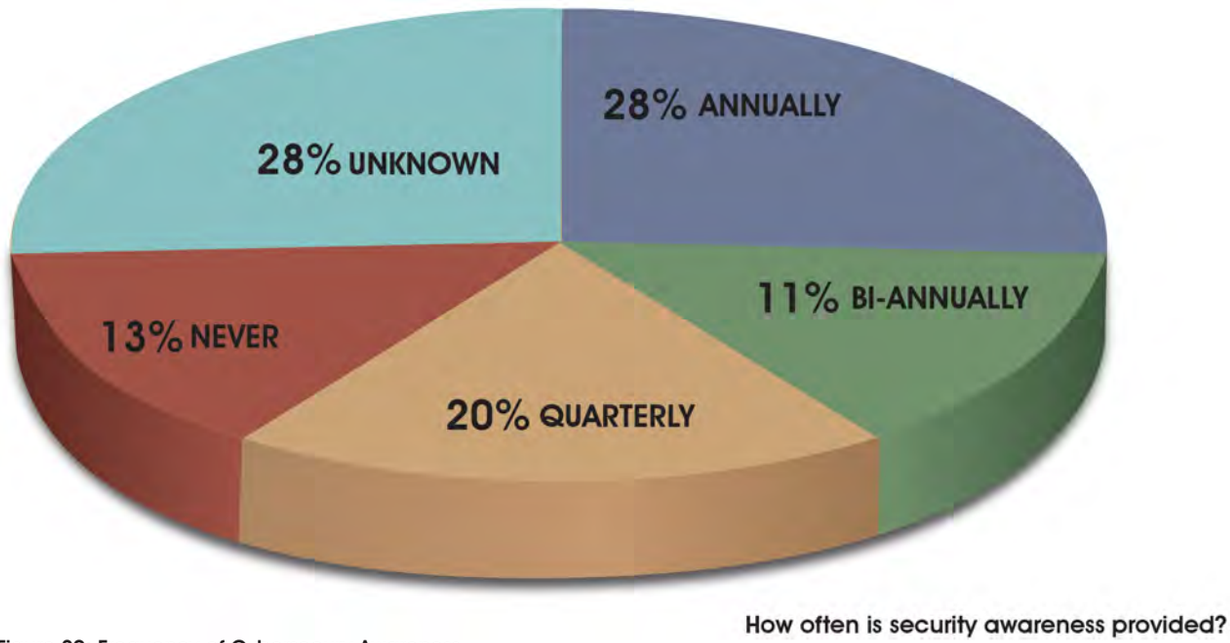


Figure 20: Frequency of Cybersecury Awareness

6.6 Vulnerabilities and Risk Assessment

6.6.1 Formal Identification of Critical Assets

The majority of organisations (69%) had identified critical assets. A small number of organisations had not identified critical assets (8%), and 23% were not sure whether their organisations had identified critical assets. See Figure 21.

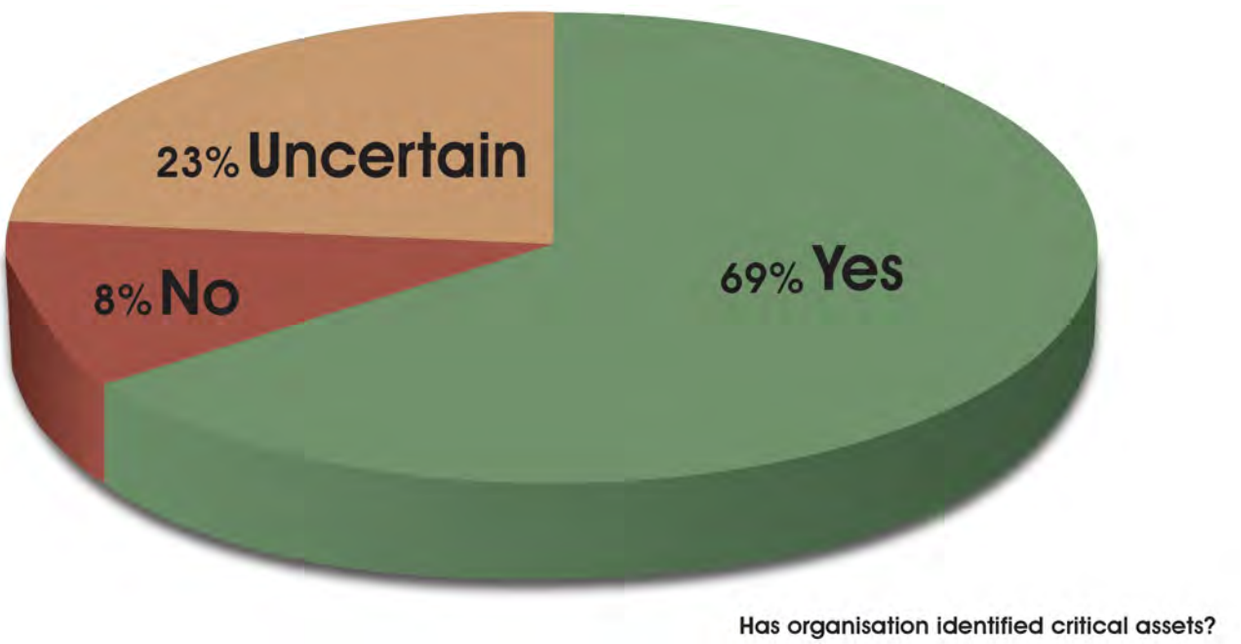


Figure 21: Formal identification of Critical Assets

Critical asset identification is necessary in order to ascertain which assets are vital for the functioning of the organisation. It can also aid with threat identification and risk mitigation. As part of a cybersecurity strategy or plan, it is important to understand what needs to be protected. Through the identification of critical assets, an organisation can determine the impact on its functionality should the confidentially, integrity or availability of these assets be affected.

6.6.2 Frequency of Risk Assessments

Risk assessment helps identify, analyse and evaluate risk by determining whether the implemented cyber security controls are appropriate in dealing with the risks. A risk assessment study can determine whether an organisation is wasting time, effort and resources, as there is little point in implementing security measures for risks that are highly unlikely to occur at an organisation. Through risk assessment, the organisation can prepare for the significant risks it faces.

Just over one-third of organisations (36%) are carrying out risk assessments annually. 20% of organisations are doing a risk assessment more than once a year. 14% are doing a risk assessment periodically, but not every year; another 14% are not sure of when a risk assessment is carried out. In 4% of organisations, a risk assessment is not formally done and 5% are assessing at other intervals (like monthly). See Figure 22.

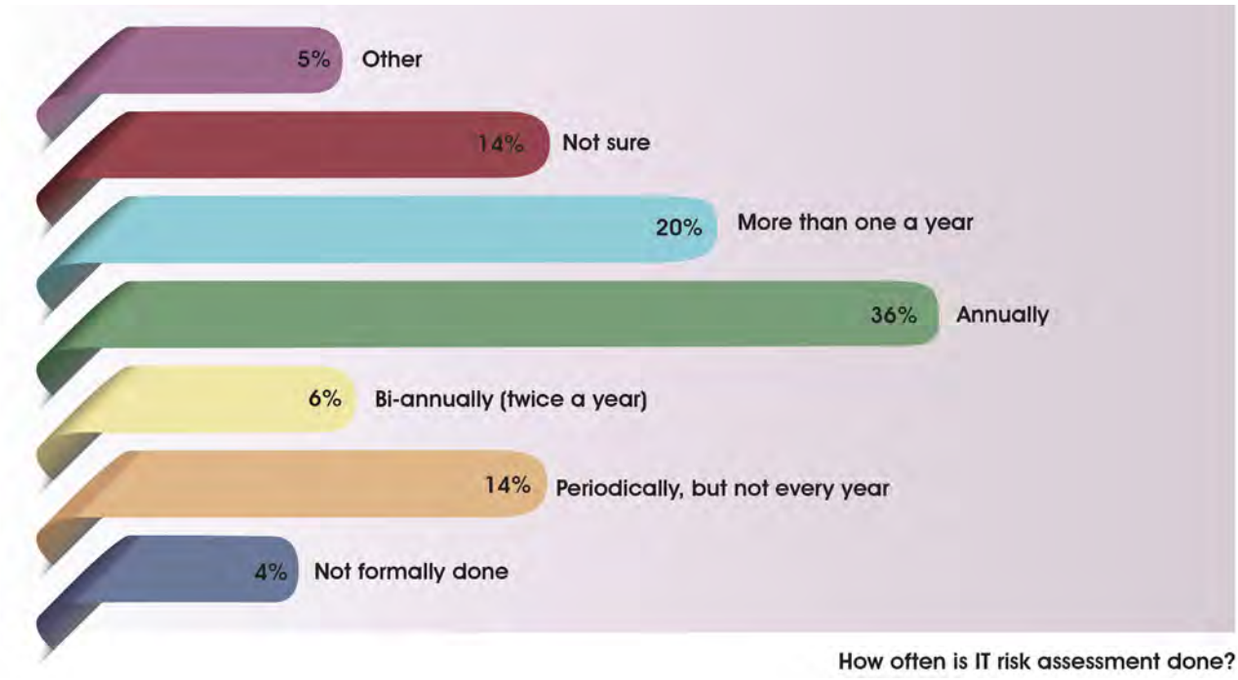


Figure 22: IT Risk Assessment Frequency

6.6.3 Actions in response to a risk assessment

Most organisations carried out policy updates (64%) or implemented new technologies (63%) in response to a risk assessment study. Another significant finding was that 49% of organisations implemented stronger education and awareness programmes in response to a risk assessment. Other action taken included the appointment of more security personnel (24%) and outsourcing of assistance (23%). See Figure 23.

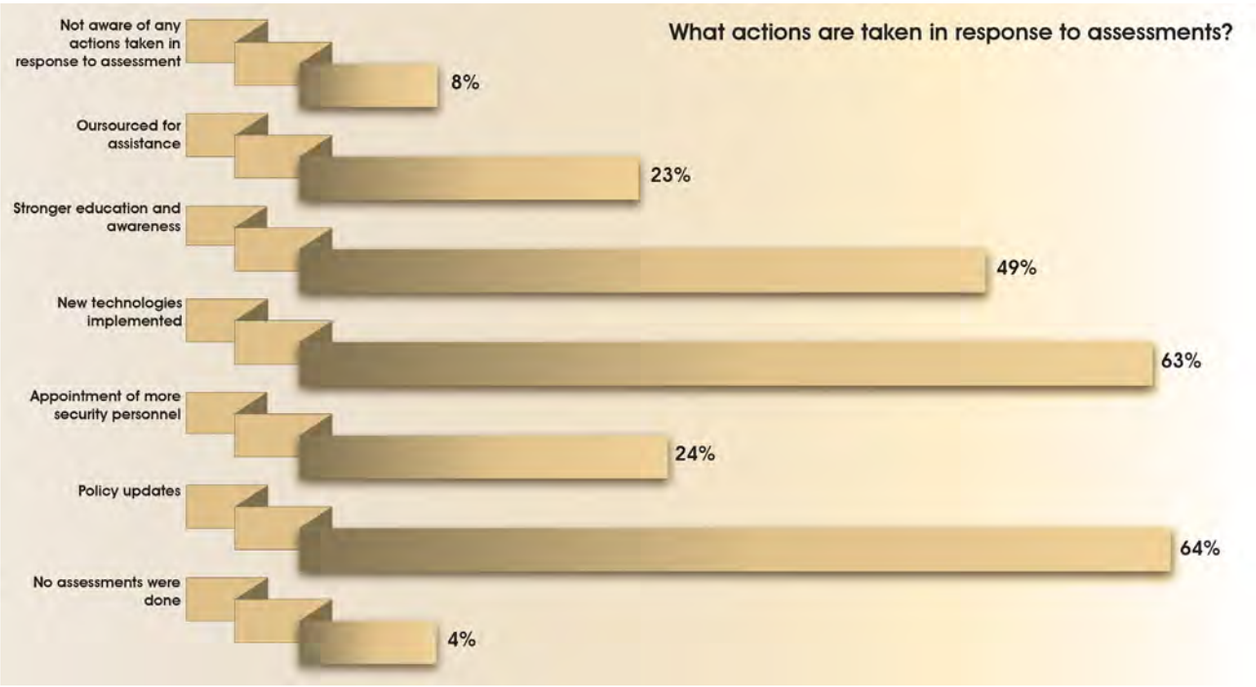


Figure 23: IT Risk Assessment Frequency

As part of the risk management process in an organisation, various defensive mechanisms can be put in place. In order to prevent certain risks from materialising, policy changes and awareness training can be implemented. This can help to prevent users from engaging in malicious action that may affect systems and networks. Technical controls can also be implemented in order to prevent certain attacks from occurring.

6.6.4 Challenges to Cybersecurity

The most significant challenges to successful operation of the cybersecurity function in an organisation are insufficient skilled people in relation to applying cybersecurity, as well as the lack of in-house skills. The remainder of responses was widely spread.

Skills shortages and a lack of core cybersecurity competencies are critical obstacles in managing cybersecurity effectively in an organisation. Cybersecurity professionals need to be trained and upskilled in order to deal with the growing requirement for specialists who can apply cybersecurity across an organisation.

In addition, the general staff population may be lacking in basic cyber awareness. This lack of cyber awareness contributes strongly to some of the issues organisations face with regard to cybersecurity. Phishing attacks, malware, social engineering and ransomware attacks can all be reduced if users are made aware of how these common attack vectors are distributed.

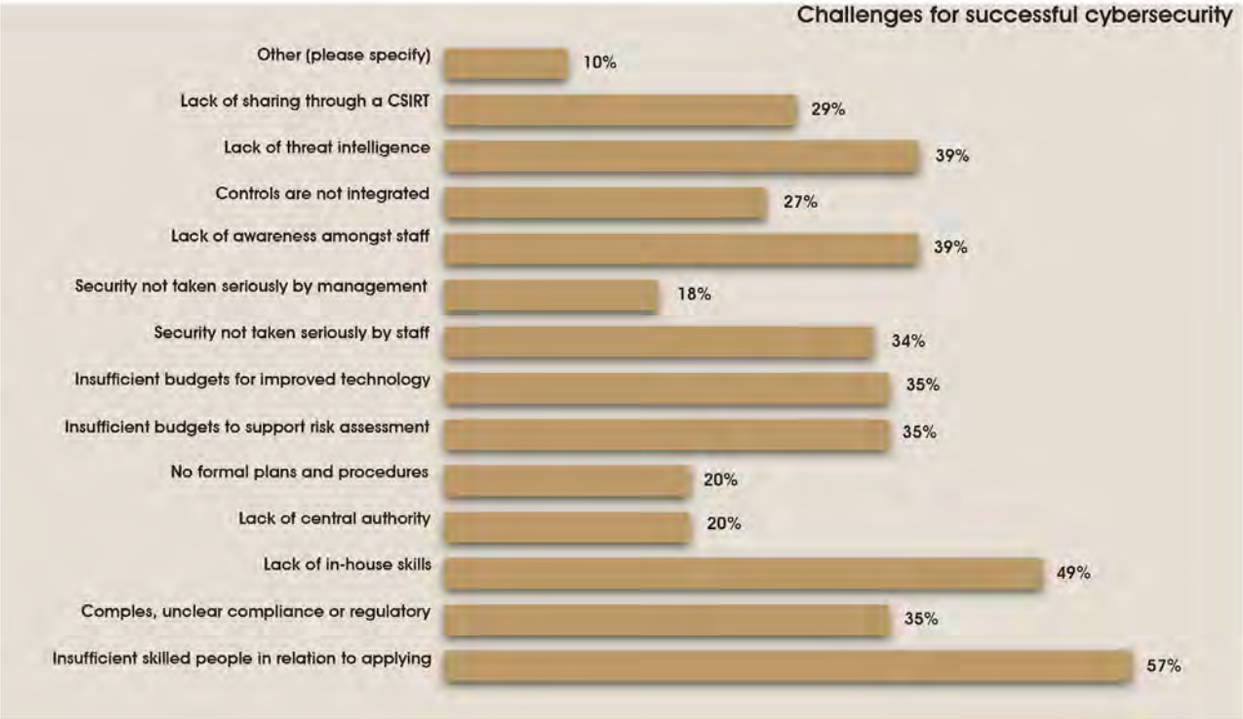


Figure 24: Challenges for Successful Cybersecurity

6.6.5 Top Threats

Respondents were asked to rate the top three threats facing their organisations. The results indicate that the top three threats facing organisations are: targeted malicious emails (64%), ransomware (57%) and theft of mobile devices and laptops (34%). 25% of organisations also listed Denial of Service Attacks as a top threat. See Figure 25.

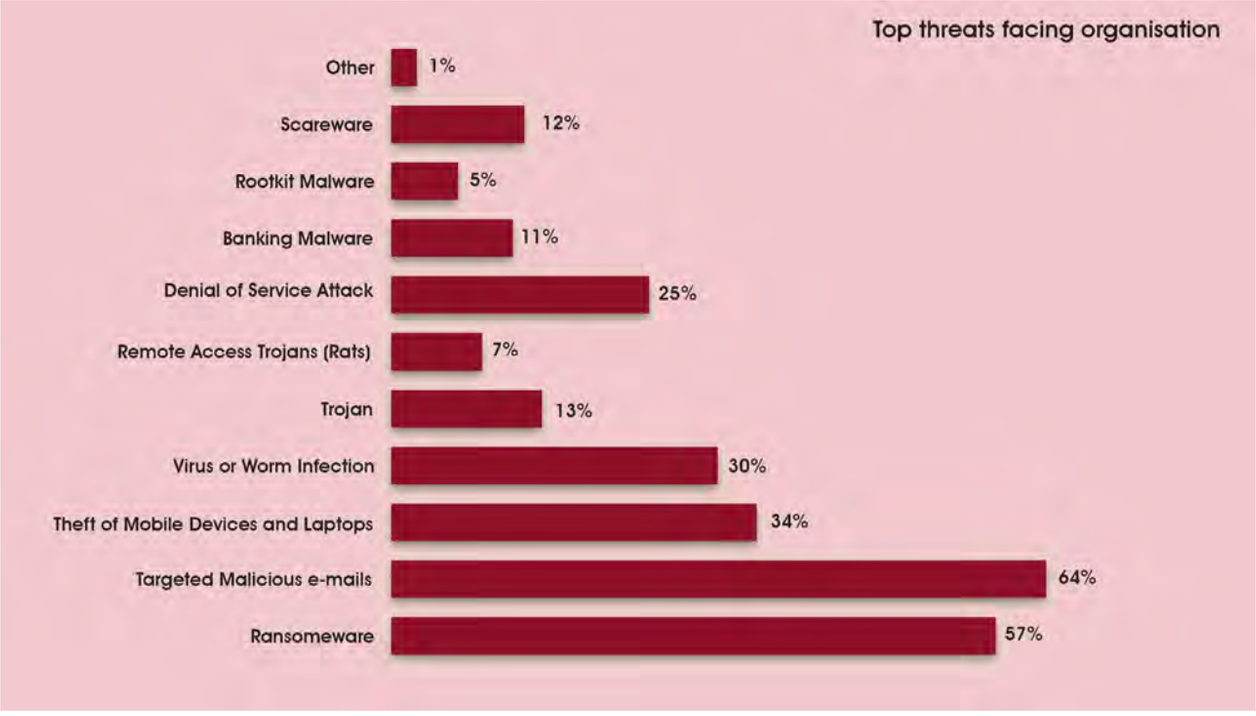


Figure 25: Top Threats Facing Organisations

With targeted malicious emails, users can be tricked into revealing sensitive information or clicking on malicious links that may infect machines. Attackers can gain access to an organisation's sensitive networks, data and resources through cleverly crafted emails that entice users to click on a link, which then activates malicious capabilities.

Another danger to systems and networks is ransomware in which data is encrypted and held hostage until a substantial financial sum is paid over. Data and systems can remain inaccessible until the fee is paid. Critical data could be affected.

These forms of computer network exploitation are concerning, as users can be tricked into performing actions that may reveal sensitive information or make critical data inaccessible. The organisation is at risk of inadvertent information disclosure or data theft.

Loss of information through theft of laptops and mobile devices is another area of concern. Data may not be properly protected through encryption and thus critical data may fall into the wrong hands. Physical safety is another area of cyber security that users need to be educated about. Basic tips about locking up devices in cabinets, not leaving them near windows in homes and cars, and encrypting data are all issues that need to be encouraged.

6.6.6 Threat Actors

For many organisations, employees (69%) and criminals from outside the organisation (64%) pose the biggest threat. Other actors that could pose a cybersecurity threat to organisations include contractors (41%), lone hackers (40%) and hacktivist groups (39%). See Figure 26.

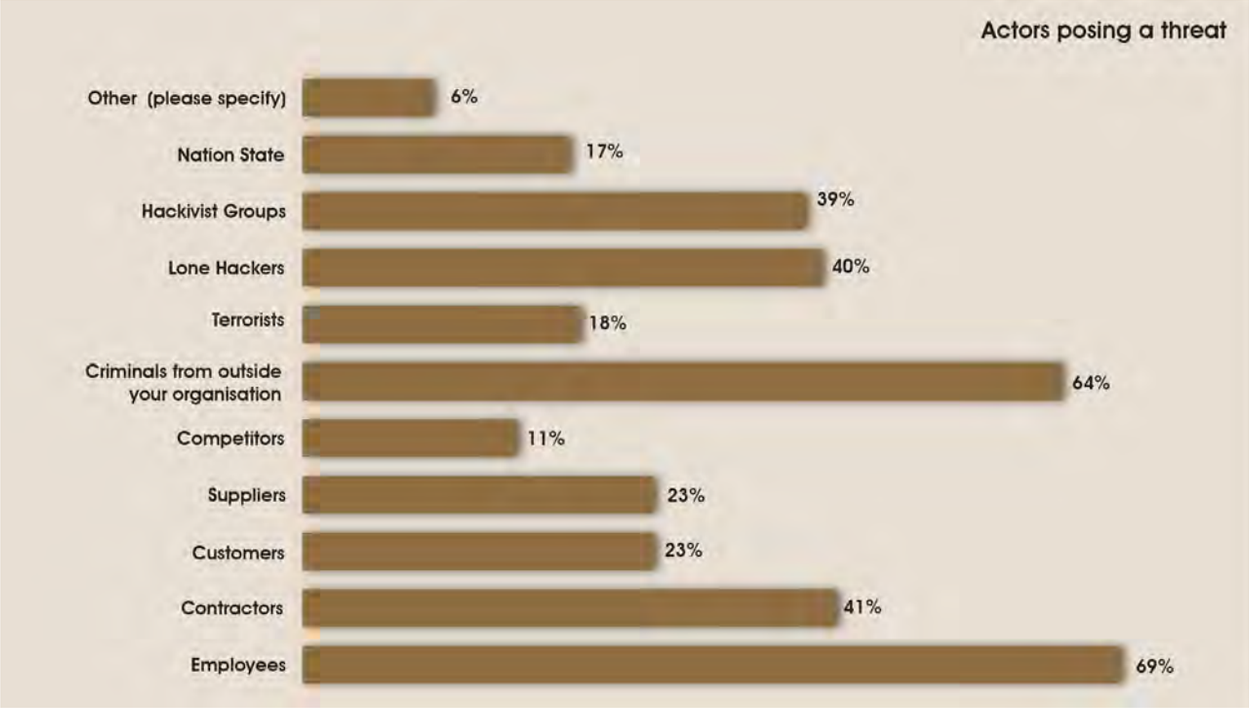


Figure 26: Actors Posting a Treat

Employees pose a bigger threat than criminals from outside the organisation. Insiders may try to abuse systems and information for fraudulent uses, theft and personal gain. Insiders have the advantage of being in close proximity to the systems and data and may not need to hack into an organisation's network. Organisations may find it harder to protect their systems as insiders already have legitimate access to the organisation's information and assets.

6.7 Incident Management and Business Continuity

6.7.1 Ability to respond to incidents

Incident response refers to an organisation's ability to deal with a situation in which company infrastructure and technology is being attacked and requires action to limit the damage, costs and effects of the incident. Preparation, planning and testing form part of incident response capability.

Organisations need to ensure that they plan and prepare for a serious incident or disaster, to ensure they are able to restore systems to an operational state within a reasonable amount of time. Recovery and restoration of critical systems forms an essential component of business continuity plans. Contingency planning ensures that an organisation can effectively cope with major incidents or disasters, whether they are foreseen or not. Business continuity may also include some risk management, governance and compliance aspects. Through risk assessment, organisations can formerly identify potential interruptions to operations and plan for contingency measures. A business continuity plan may incorporate essential business processes and details of systems that are operationally required.

The majority of respondents (64%) indicated that their organisations would be able to respond to threats. 23% were uncertain about their organisation's ability to respond to threats. See Figure 27.

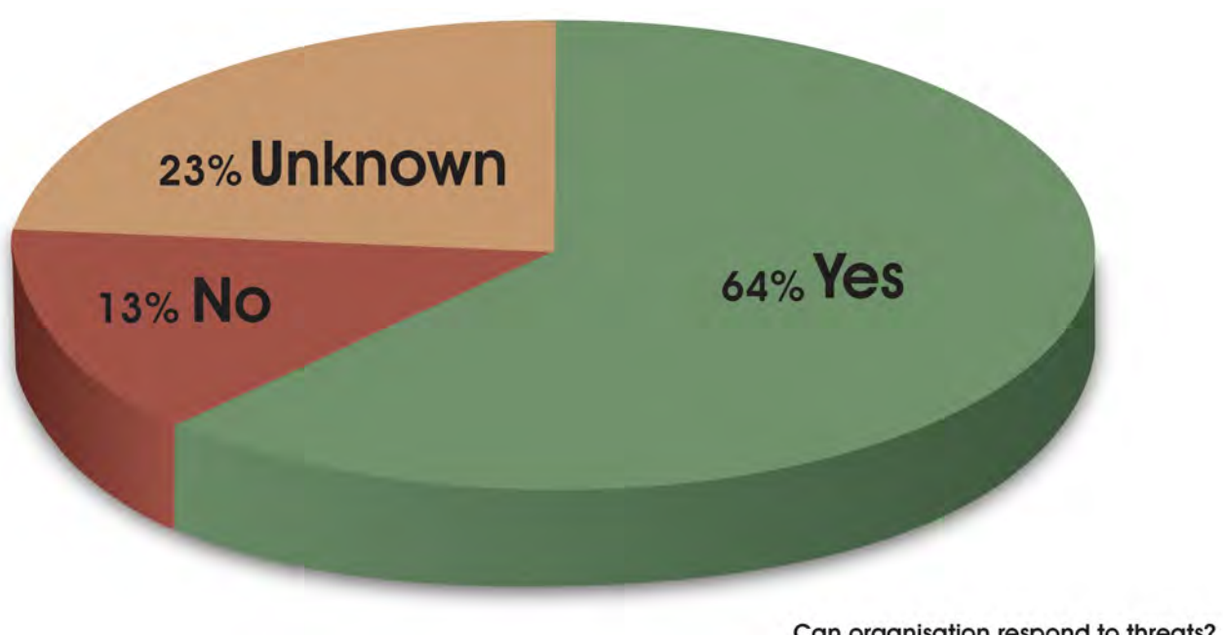


Figure 27: Organisations capability to respond to Threats

6.7.2 Frequency of Incident Response Testing

24% of organisations test their incident response annually. 25% never test their incident response capability and 24% are unsure of the frequency of testing. See Figure 28.

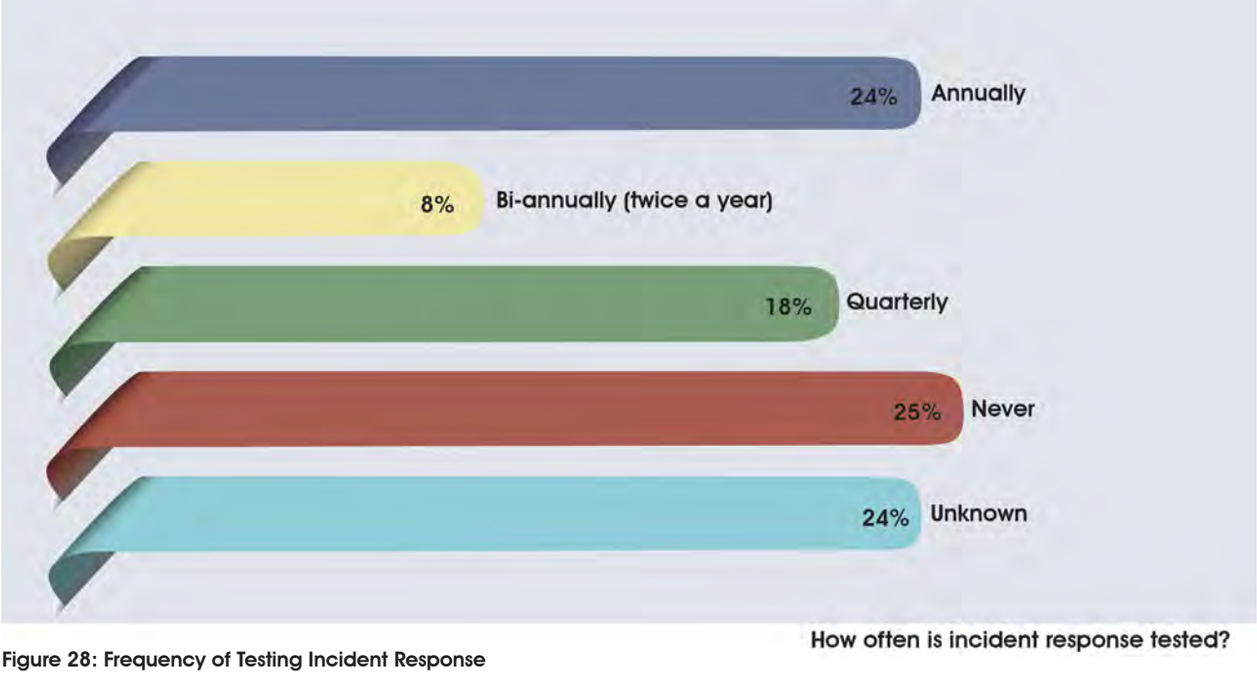


Figure 28: Frequency of Testing Incident Response

An organisation may be faced with many incidents that affect the confidentiality, integrity or availability of systems, technology and infrastructure. To cater for impending events, an organisation needs to test its incident response capability, in order to identify gaps, test skills and processes, and determine how the organisation can best deal with a downtime incident. System recovery, restoration and minimisation of damage form a key part of incident response and the ability to carry out these critical functions should be tested regularly.

6.7.3 Response to Past Incidents

More than half of the organisations surveyed responded that they were always able to respond successfully to past incidents. 27% responded that they were sometimes able to respond successfully to past incidents; 18% were not sure; 5% were never able to respond successfully to past incidents. See Figure 29.

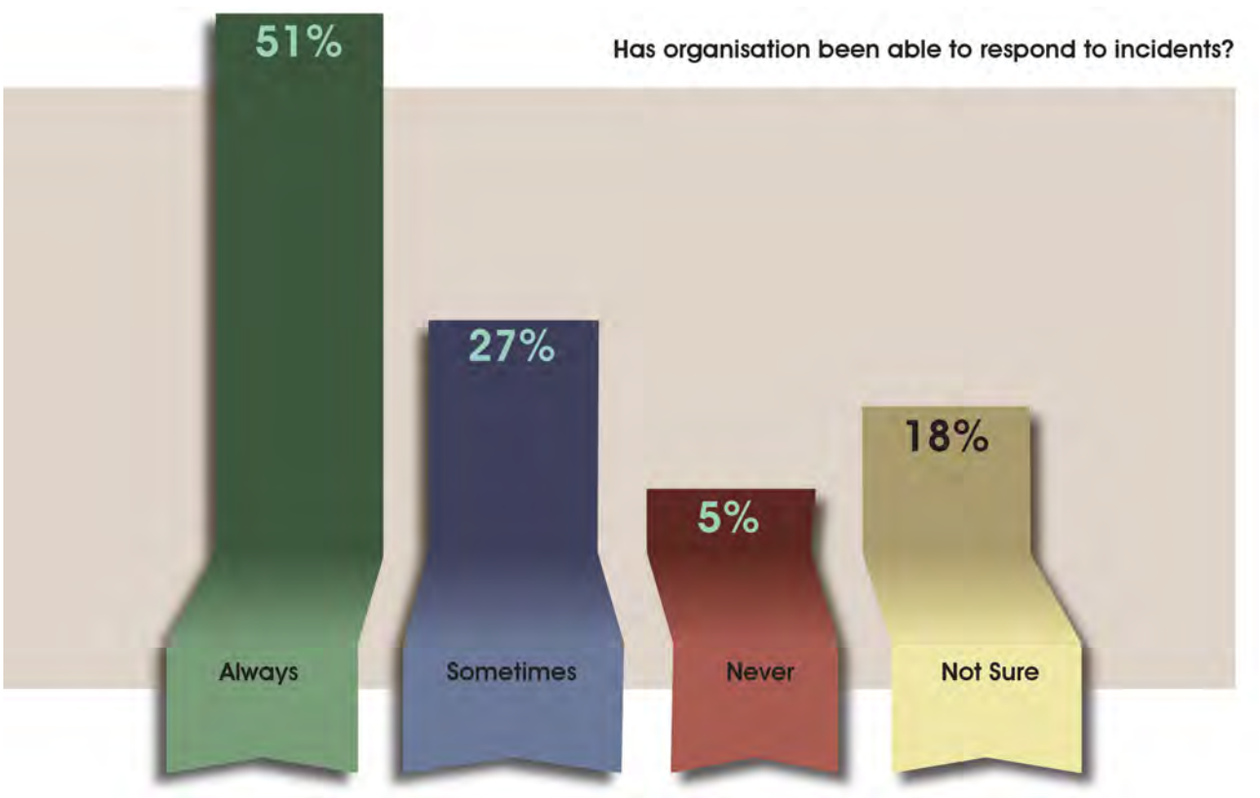


Figure 29: Responding to incidents

Incident handling tries to ensure that a cyber incident is contained, and it can mean the difference between complete recovery and total disaster. Organisations may be able to respond to incidents, but how the incident is handled may determine whether the organisation can recover and restore systems with minimal disruption and effect on the organisation.

6.7.4 Continuation after Cybersecurity Incident

42% responded positively that their organisations would be able to carry on with business as usual, or resume operations without heavy losses when faced with a cybersecurity incident. 51% were uncertain whether their organisations would be able to carry on with business as usual and resume operations without heavy losses. (See Figure 30.)

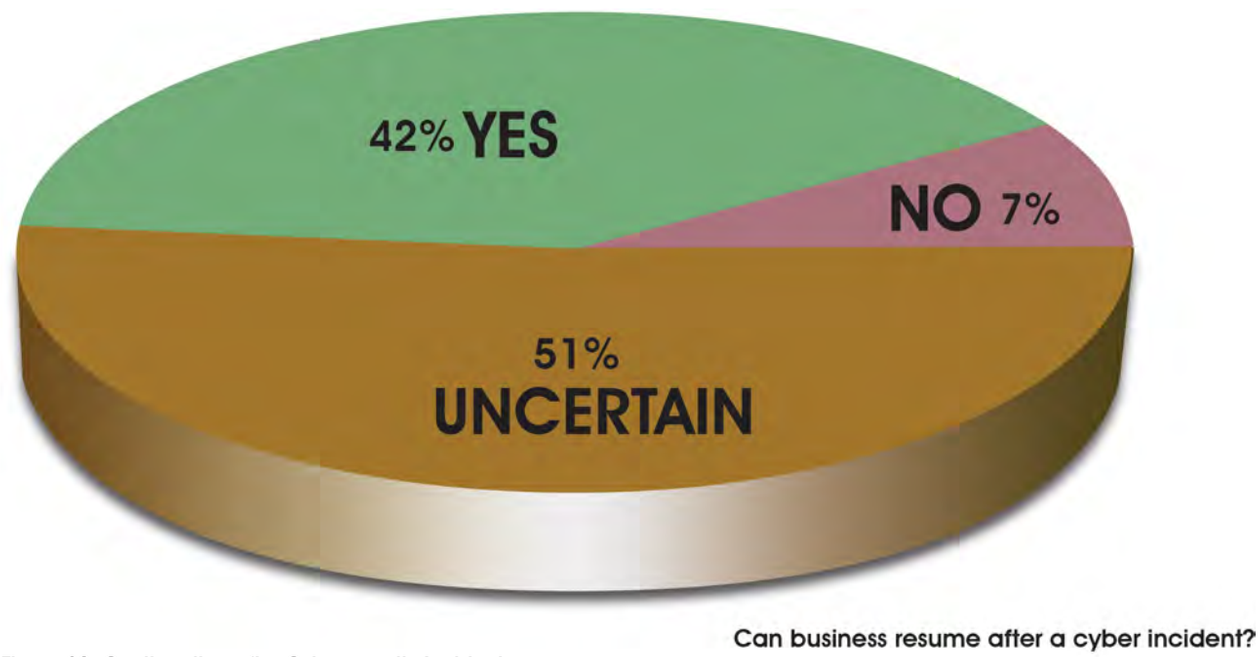


Figure 30: Continuation after Cybersecurity Incident

The majority of organisations were unable to assess whether they could continue with business and resume operations without heavy losses. This indicates that many organisations may not have a strong incident handling ability and require stronger planning and testing in order to minimize the threat of system downtime and losses.

6.7.5 Increase in Cybersecurity Incidents

Notably, 42% of respondents indicated that the total number of cybersecurity incidents faced by an organisation had not increased in the current calendar year, when compared to the previous calendar year. (See Figure 31). It is a positive trend if cyber incidents are reducing, and shows that controls and measures may be helping to curb an increase in attacks.

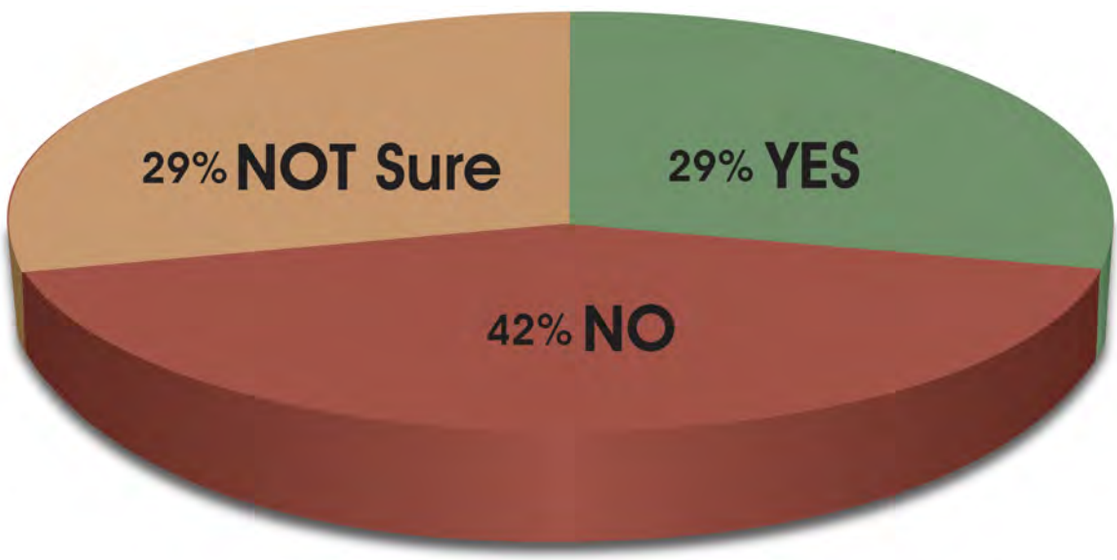


Figure 31: Increase in Cybersecurity Incidents

6.7.6 Type of Cybersecurity Incidents

Organisations reported that the types of incidents have changed compared to previous years (42%). (See Figure 32.) This indicates that organisations will need to prepare, adapt and respond to changing incident types and that they cannot just rely on tried and tested methods used to deal with current attacks.

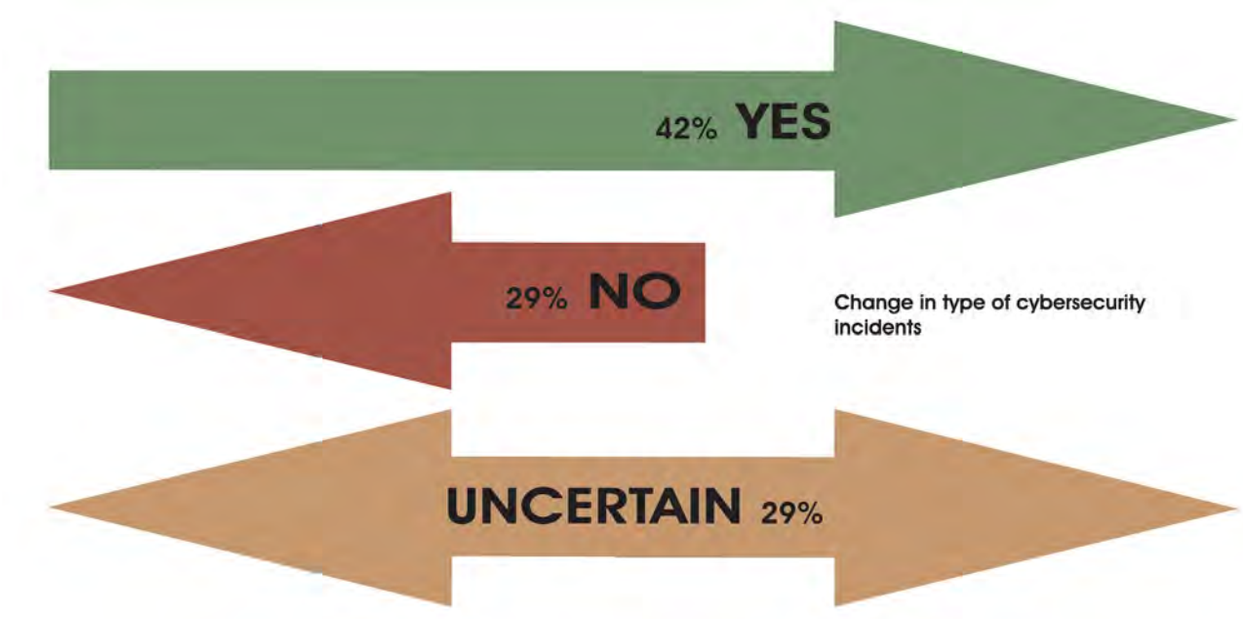


Figure 32: Cybersecurity incidence trends

6.7.7 Threat Intelligence Capability

Threat intelligence can provide useful capability in trying to manage the increase in cyber-attacks, by collating data to gain new insight and identify trends. Threat intelligence can contribute to the development of detective and reactive action, by investigating the source, motivation and capability of the perpetrator. 25% of surveyed respondents indicated they had a threat intelligence capability; another 20% indicated this is in development. This shows that the large majority of organisations have recognised that threat intelligence is a growing requirement. (See Figure 33).

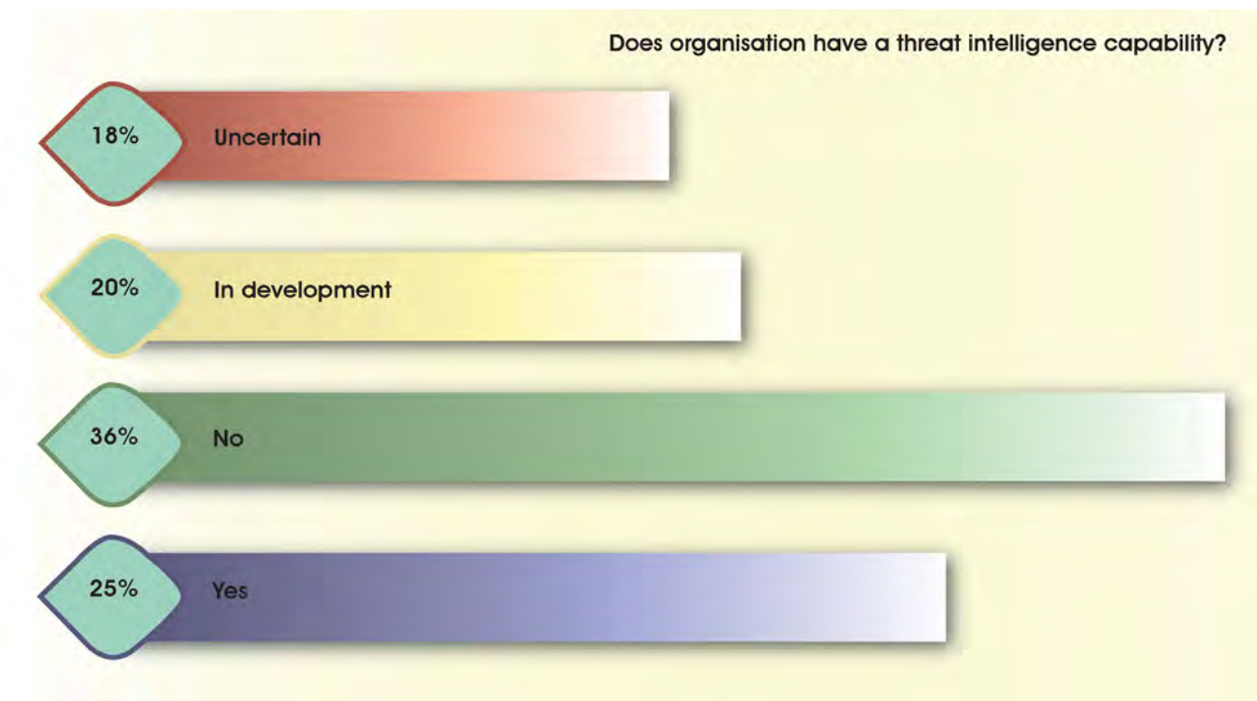


Figure 33: Threat intelligence capability

7

Critical Findings

1

IMPLEMENT CYBERSECURITY PLAN/STRATEGY

Organisations in South Africa need to implement their cybersecurity strategy/plan to ensure resilience of the underlying foundation and to help minimise cyber security threats. Without a sound cybersecurity plan/ strategy, the direction and main security approach of an organisation will be lacking. Once a strategy has been discussed, plans should be put into place for implementation within a set time frame. If a strategy/ plan is not implemented, the organisation may fall behind with best practices and current evolving threats.

2

INCREASE CYBER SECURITY AWARENESS TRAINING

In South Africa, there is a strong requirement to increase the level of security awareness of various technology users and ICT security practitioners. This will help ensure that more users are knowledgeable in different areas and levels of cybersecurity. ICT security risks can be minimised if more users are knowledgeable about best practices and essential precautions. Many staff members lack basic cybersecurity awareness. While beginner training is useful for entry level workers, more advanced, intermediate and hybrid training should also be provided to help educate users about pertinent cyber risks and threats.

3

TRAIN AND UPSCALE CYBERSECURITY EXPERTS

Many organisations are faced with the challenge of insufficient skills experts who can apply cybersecurity. In-house skills and lack of cyber knowledge all contribute to this growing issue. Organisations now need to grow the skill levels of employees and develop cybersecurity knowledge through training and certifications. The cybersecurity competencies of cyber security experts and security practitioners need to be improved in order to ensure adoption of key security practices.

4

RISK ASSESSMENTS EXECUTION

In South Africa, risk assessments need to be carried out on a more regular basis to ensure that key risks are identified and mitigated. If organisations do not regularly carry out risk assessments, they could potentially be faced with a crisis with no form of disaster recovery of business continuity plan. Risk assessments can help prepare an organisation for adverse events in order to ensure continuation of operations and minimal disruptions.

5

IMPROVE BUSINESS CONTINUITY / DISASTER RECOVERY CAPABILITY

Organisations may not be able to recover from a cyber incident and resume operations once more. More detailed business continuity/disaster recovery plans need to be developed and tested to ensure that company downtime is minimised should disaster strike. It is imperative that organisations assign responsibilities and develop processes in order to deal with a crisis.

8 Conclusion

In order for South African organisations to stay ahead of the threat curve, research, investment and skills development in certain key areas are vital. Awareness, risk assessment, implementation of cyber security plans/strategies, infrastructure and technologies are all areas which enhance the ability to contain cyber threats. Currently, South African organisations are placing emphasis on the most discernible measures in order to reduce cyber threats.

However, in the evolving threat landscape, more advanced skills like threat intelligence will help play a role in combatting threats. The implementation of standards and membership to sector CSIRTs could also help contribute to the improved governance of cybersecurity.

One of the biggest challenges facing organisation is insufficient skilled people in the industry. Training, expertise development and awareness in order to upskill members will all be required in order to tackle this challenge. Training and growing of cyber security experts can help secure critical infrastructure and protect organisations. South Africa, like the rest of the world continues to be confronted with cyber threats. Through various cyber defence plans, strategies and technologies, organisations strive to enhance their cyber resilience and establish a first line form of protection.

Bibliography

9

1. Shackleford D. December 2016. SANS 2016 Security Analytics Survey, SANS Institute.
2. African Cyber Security Report 2016. 2016. SERIANU and USIU Centre for Informatics Research and Innovation (CIRI)
3. Acampora J. 2015. How to Analyze Survey Data in Excel, https://www.excelcampus.com/pivot-tables/analyze-survey-data-in-excel/. Accessed 2017/09/10.
4. Florentine S. 2016. Why you need a CSO/CISO. Available at https://www.cio.com/article/3048074/careers-staffing/why-you-need-a-cso-ciso.html. Accessed 2017/10/10.
5. IT Governance. 2017. Cyber Security Risk Assessments. Available at https://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security. Accessed 2017/10/10.
6. Ruefle M. 2017. Critical Asset Identification (Part 1 of 20: CERT Best Practices to Mitigate Insider Threats Series). Available at https://insights.sei.cmu.edu/insider-threat/2017/04/critical-asset-identification-part-1-of-20-cert-best-practices-to-mitigate-insider-threats-series.html. Accessed 2017/10/11.
7. Kip R. 2015. Are Targeted Malicious Email (TME) and spear phishing emails, the same in Advanced Persistent Threat attack? Available at https://www.quora.com/Are-Targeted-Malicious-Email-TME-and-spear-phishing-emails-the-same-in-Advanced-Persistent-Threat-attack. Accessed 2017/10/13.

APPENDIX A

Data collection protocol and Research Methodology

During the initial phase of the study, the survey was designed and questions compiled that would form part of the survey. This went through several iterations of editing, changing and compiling the final set of survey questions. Other cybersecurity surveys and reports were consulted to guide the process. The final set of questions was sent for statistical checking, in order to assess the survey. Inputs were received from a trained statistician and the final set of questions agreed upon. This final set of questions formed the survey. The survey was then posted online and invited participants could then complete it. Once the data was captured, the results were analysed and captured in this report.

DTPS, together with the CSIR, developed a 31-question (10-15 minute) web-based survey. The survey was captured using a free open-source tool (FourEyes) in a web-based platform. Most survey questions included a "don't know" or "uncertain" choice, to cater for respondents who could only answer questions within their domain of expertise.

Letters were sent out from DTPS requesting participants' assistance in completing the survey. This would assist in data collection of this kind for the first time in South Africa. Prospective respondents were then sent the survey link and requested to complete the survey on behalf of their organisation. Organisations that could be classified under the target sectors were invited to participate in the survey. The survey was run between 18/01/2017 and 05/09/2017. Throughout the duration of the survey being open on FourEyes, the target organisations were reminded about completing the survey.

APPENDIX B

SECTOR-CSIRTS

A Computer Security Incident Response Team is an organisation that receives reports of security breaches, conducts analyses of the reports and responds to the senders. CSIRT services are usually performed for a defined constituency. The National Cybersecurity Policy Framework (NCPF) emphasises the need to establish sector-based capacity in order to improve the threat posture of the country. This sector-base capacity is in the guise of sector Computer Security Incident Response Teams (CSIRTs).

PAYMENTS ASSOCIATION OF SOUTH AFRICA (PASA)

PASA's formation emanated from international efforts to address risks associated with payment systems, and South Africa's reintegration into the world economy in the early 1990s. In 1994, the banking industry requested the South African Reserve Bank to take the lead in the modernisation process of the domestic payment system. A strategy was the establishment of a payment system management body and PASA was formally established on 26 September 1996.

PASA is the Payment System Management Body recognised by the South African Reserve Bank, in terms of the National Payment System Act of 1998, as revised and amended in 2004, to organise, manage and regulate the participation of its Members in the payment system. PASA exists to facilitate the circulation of money in the interest of economic development of South Africa.

PASA's mission is to manage and develop the NPS and facilitate integration with international payments. PASA aspires to be acknowledged as world class, in assisting in the evolution and oversight of the payments industry.

http://www.pasa.org.za/

ASSOCIATION OF SAVINGS AND INVESTMENTS SOUTH AFRICA (ASISA)

The Association for Savings and Investment South Africa (ASISA) represents the majority of the country's asset managers, collective investment scheme management companies, linked investment service providers, multi-managers and life insurance companies.

ASISA's members are considered the custodian of the bulk of the nation's savings and investments and are among the country's biggest contributors to the national GDP.

https://www.asisa.org.za/

ASISA enables this industry to speak with one voice and represents the unified goal of ensuring that the South African savings and investment industry remains relevant and sustainable into the future in the interest not only of ASISA and its members, but also the country and its citizens.

ASISA will work towards promoting a culture of savings and investment in South Africa by playing a significant role in the development of the social, economic and regulatory framework in which our members operate, thereby assisting members to serve their customers better.

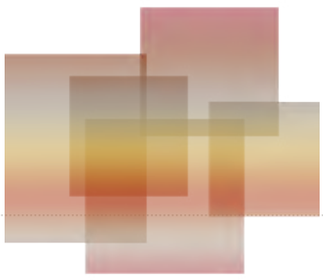
ASISA-CSIRT co-ordinates response to cyber and information security incidents experienced by ASISA-members. It also provides cyber threat related information to members, to reduce the risk of cyber security incidents to their individual businesses. The ASISA-CSIRT also facilitates skills development interventions to increase the competence levels of incident response teams at member companies.

The ASISA-CSIRT represent members at an industry level in interactions with the SA Government and Regulators on issues relating to cyber security.

Fast Moving Consumer Goods CSIRT

In view of the growing global threat of cyber security attacks and the potential negative (and disastrous) consequences for business, civil society and government, the Consumer Goods Council of South Africa (CGCSA) is in the process of establishing a sector-specific CSIRT which is focused on the fast-moving consumer goods (FMCG) sector.

The intention is to establish the necessary awareness, communication, protocols and support mechanisms for FMCG companies and stakeholders across the manufacturing, logistics and wholesale/retail industries. This is undertaken to preserve the security of assets and infrastructure of companies operating within the FMCG sector, and supports the



national efforts aimed at protecting the country against cybersecurity threats, guided by the National Cybersecurity Policy Framework.

This FMCG CSIRT, which is in the early stages of development, will respond to the specific requirements of the FMCG sector, and build synergies with other similar CSIRTs at the national level (established through the Department of Telecommunications and Postal Services, DTPS) and in other sectors (such as banking, etc.).

The FMCG CSIRT is entering into a phase of dialogue with the CGCSA membership base, and has already initiated a cybersecurity readiness survey in partnership with the DTPS. Insights gained will influence the structure and priorities of the FMCG CSIRT.

Given the structure and size of the FMCG industry, the nature of external cyber threats and the relative preparedness of the companies in the sector, it seems likely that the FMCG CSIRT may well include elements of proactive liaison and communication across member companies and between these and other stakeholders, as well as the provision of operational support to companies (including, for example, threat alerting services, incidence response support and awareness initiatives).

The rapid growth of the cybersecurity threat globally, and the systematic increase in the number and sophistication of cyber-attacks on companies and individuals, makes this one of the high priority initiatives for the FMCG sector, and the CGCSA. The importance of education and awareness cannot be understated, and forms an integral part of the sectors efforts to mitigate this threat to the sector, and will consequently feature highly in the future.

Internet Service Providers' Association: (ISPA)

CSIRT.net.za is an initiative of the South African Internet Service Providers' Association (ISPA), an Industry Representative Body recognised in terms of the Electronic Communications and Transactions Act, 25 of 2002. It is an Internet industry sector CSIRT which aims to provide information on security vulnerabilities related to South Africa IP address space to Internet Service Providers (ISPs) in the country.

The target constituency is the Internet services sector and operators of Internet infrastructure in South Africa. Although many of these organisations are already members of ISPA, participation in CSIRT.net.za is open to any organisation providing Internet services.

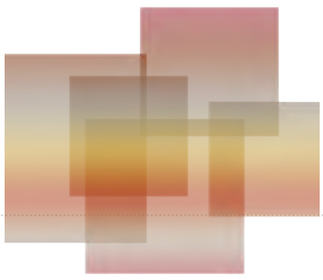
CSIRT.net.za provides a co-ordinating and advisory role and does not directly handle security incidents. Members of CSIRT.net.za are welcome to contact the CSIRT team for security advice at any time (including during an incident), and a response will be provided on a best effort basis. The CSIRT's primary role is to collect available information on security issues relating to South African IP address ranges and make this available to ISPs based on the ASNs associated with their networks.

https://www.CSIRT.net.za

South African Banking Risk Information Centre (SABRIC)

The South African Banking Risk Information Centre (SABRIC) is a Non Profit Company formed by the Banks and Cash in transit companies to combat organised bank-related crimes. SABRIC aims to be Africa's trusted financial crime risk information centre leveraging on strategic partnerships. Cybercrime was identified as a global transnational threat which led to the interbank decision to establish a banking industry CSIRT at SABRIC, in 2010.

The decision to establish an industry CSIRT was motivated by the following factors, amongst others:



- shared expertise and skills among banks will lead to a higher probability of identifying threats earlier and facilitate more effective responses;
- shared knowledge and experience will contribute to improved preventative measures at member banks;
- international threat intelligence does not cover all local threats thus generating and sharing localised intelligence, will improve the industry's detection and mitigation activities;
- collaboration as an industry was deemed to be an important step in the right direction to support the National Cybersecurity Policy Framework and ultimately the objectives of the Cybercrime and cybersecurity Bill.

SABRIC member banks agreed that the CSIRT should be a collaboration CSIRT with dedicated fulltime resources hosted at SABRIC. The CSIRT has been in existence for 7 years and currently has 19 member banks. SABRIC led interbank cybersecurity initiatives to improve cyber resilience in the industry, are facilitated by the Banking industry CSIRT which also supports Government's cybersecurity initiatives and works closely with the Cybersecurity Hub of the DTPS as well as law enforcement.

https://www.sabric.co.za/

10 Abbreviations

CSIRT	Computer Security Incident Response Team
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technologies
CRO	Chief Risk Officer
CTO	Chief Technology Officer
CSIR	Council for Scientific and Industrial Research
ICT	Information Communication Technology
ISO	International Organization for Standardization
NCPF	National Cybersecurity Policy Framework
NIST	National Institute of Standards and Technology

List of Contributors 11

We wish to thank the following persons for the valued contribution to the the compilation of this report:

1. **Dr Namosha Veerasamy**: Council for Scientific and Industrial Research (CSIR)
2. **Ms Thulani Mashiane:** Council for Scientific and Industrial Research (CSIR)
3. **Dr Jabu Mtsweni:** Council for Scientific and Industrial Research (CSIR)

Notes

Cybersecurity Readiness

2017

The Department of Telecommunications and Postal Services

Postal Address
Private Bag X860, Pretoria, 0001

Physical Address
iParioli Office Park, 1166 Park Street, Hatfield, Pretoria, 0001

Contact Information
Tel: +27 12 427 8000 - Fax: +27 12 427 8110
www.dtps.gov.za