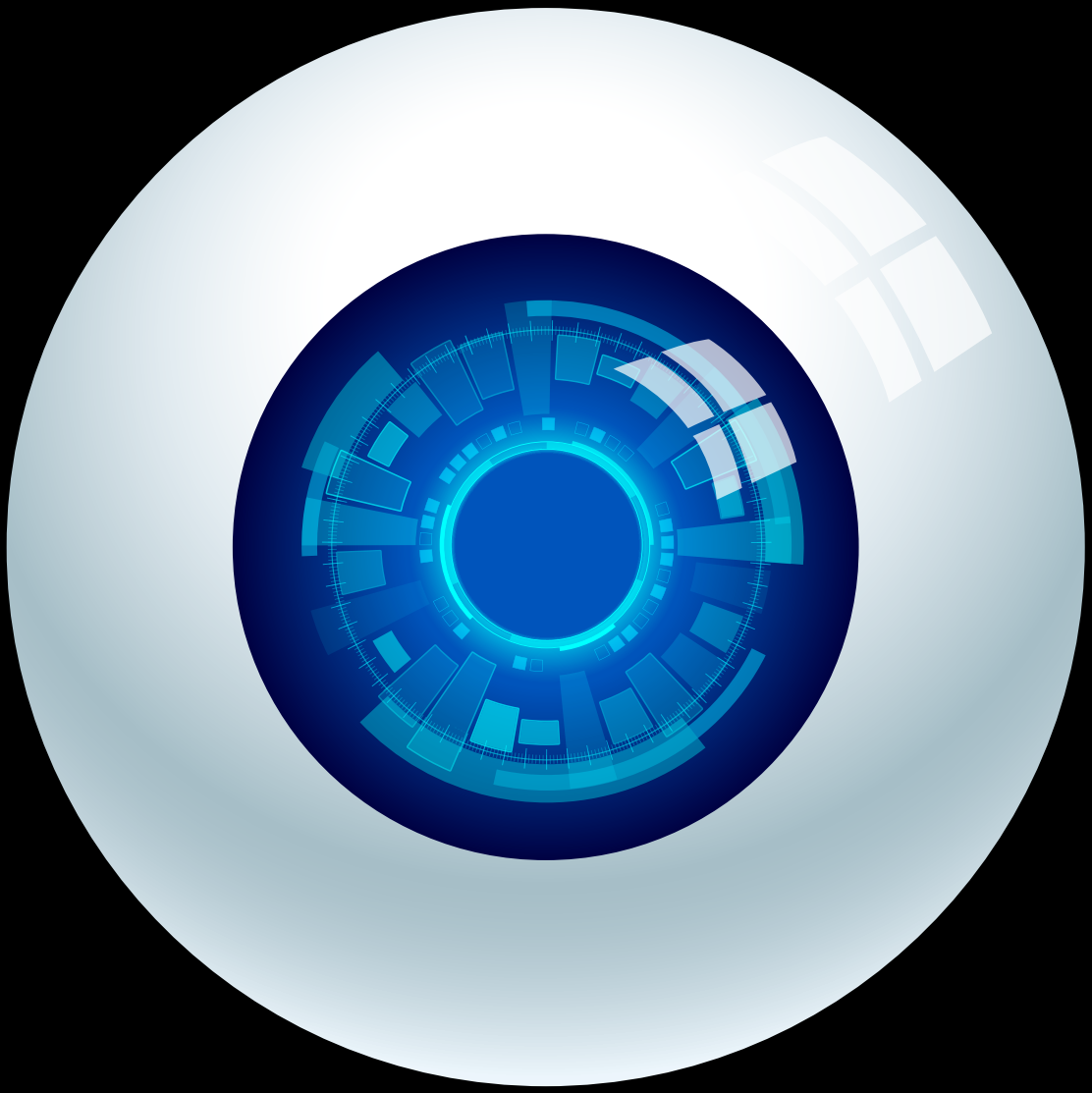
Deloitte.



Cyber Security Survey for Namibia

Keeping an eye on what matters

March 2018

Contents

It is with great pleasure that we present the findings of the first Deloitte Cyber Security Survey for Namibia. This survey covers both public and private entities and our aim is for this report to be a catalyst for contemplation, in-depth discussions and improvement of cyber security awareness and active cyber threat management in the country.

Foreword

In light of the continued efforts of the Namibian Government to formulate and promulgate an effective law that recognises and regulates electronic transactions and addresses the need to define and criminalise cyber crimes such as electronic harassment and theft of electronic details, cyber security is an emerging topic within the Namibian business environment. Added to this are the effects of globalisation and increased publication of exploitable vulnerabilities, which seem to have put Namibia on the map for cyber criminals.

This survey is the first of its kind in Namibia and collates and analyses data regarding the policies, procedures and practices followed by Namibian companies to manage and respond to cyber risk and potential cyber security attacks, as well as the impact this has on the company. This will assist users in assessing the general awareness and maturity of cyber security management within the following themes:

- Risk management;
- Skills and awareness;
- Monitoring and proactive incident management; and
- Financial metrics.

The survey was delivered via an electronic questionnaire and was directed at the person chiefly responsible for the oversight and strategic management of information security, such as:

- The Chief Information Officer;
- The Security Officer; or
- The Head of the IT department.

Given the qualitative and quantitative nature of the responses, we have taken care to ensure that information presented in our survey is anonymous and a fair reflection of the responses received.

Once again, we would like to extend our appreciation to the respondents for the time and enthusiasm devoted to providing comprehensive responses.

We believe that Namibia is a prime investment destination and provides excellent economic growth potential. Our hope is that this report will contribute to the adoption, implementation and application of strong policies, procedures and controls to mitigate and respond to the growing cyber security threat. We expect that this will lead to greater economic growth and stronger accountability and integration of IT functions with strategy and risk management functions.

Results

In this survey, we have relied upon the respondents' self-assessments. Their responses have been presented with no modification or adjustment in an attempt to preserve the integrity and anonymity of the responses. We have not verified the accuracy or completeness of the information provided by the respective respondents.

Overall, our respondents were moderately familiar with cyber security management techniques and generally exhibited a positive attitude towards pro-active risk management. However, the general sentiment amongst survey respondents was that Namibia in general is not a high-risk target for cyber crime. This is contrary to published data from internet security companies such as Symantec™, Verizon and the Ponemon Institute, which generally indicate a rise in activity globally as well as a rise in costs associated to successful breaches.

The results of the first Deloitte Cyber Security Survey for Namibia indicate that there is inconsistent appreciation and awareness of the risks and benefits of cyber security management in the Namibian market. We are pleased to note increased awareness of cyber security risks and increased commitment to appropriate responses in certain sectors, especially with regard to having proactive plans and controls in place. However, it is clear from responses in other areas and sectors that Namibia is still in the infancy of cyber security awareness and management.

The following are the high level findings of this survey:

- There is a lack of awareness of cyber risk;
- Accountability for cyber security is assigned, but not always to the correct level of personnel;
- There is a lack of high-level direction and governance for the management of information assets;
- Budgets for IT as a whole are comparable to global standards, but may be too low for the strategic development of information asset management;
- There is room for improvement on skills and training.

A number of Namibian industries are faced with the growing prevalence of Internet of Things and industrial control systems, which are generally maintained by parts of the business that do not necessarily have special training in information security and therefore do not always put adequate control measures in place. This causes these systems to become easy targets for malicious intent.

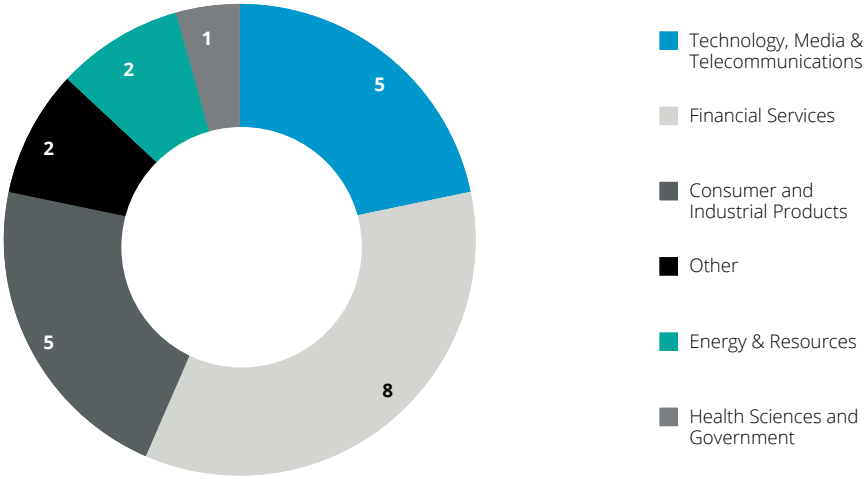
We would like to thank all the respondents to our survey for their time and efforts in providing us with valuable insight into the Namibian cyber security landscape. We trust that this report will contribute to the continued awareness of cyber security risk in Namibia.

General information

The following general information was noted from the participating entities.

Composition of respondents

Respondents by industry

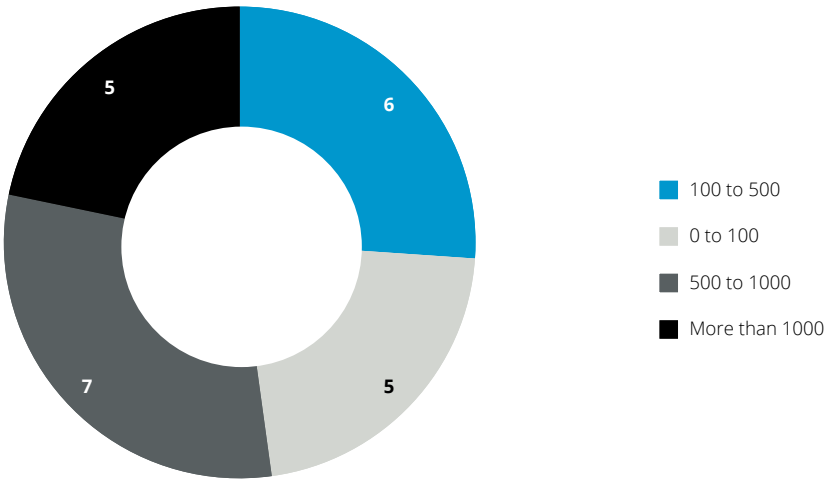


23 respondents across 6 industry categories participated

Size of respondents' staff complement:

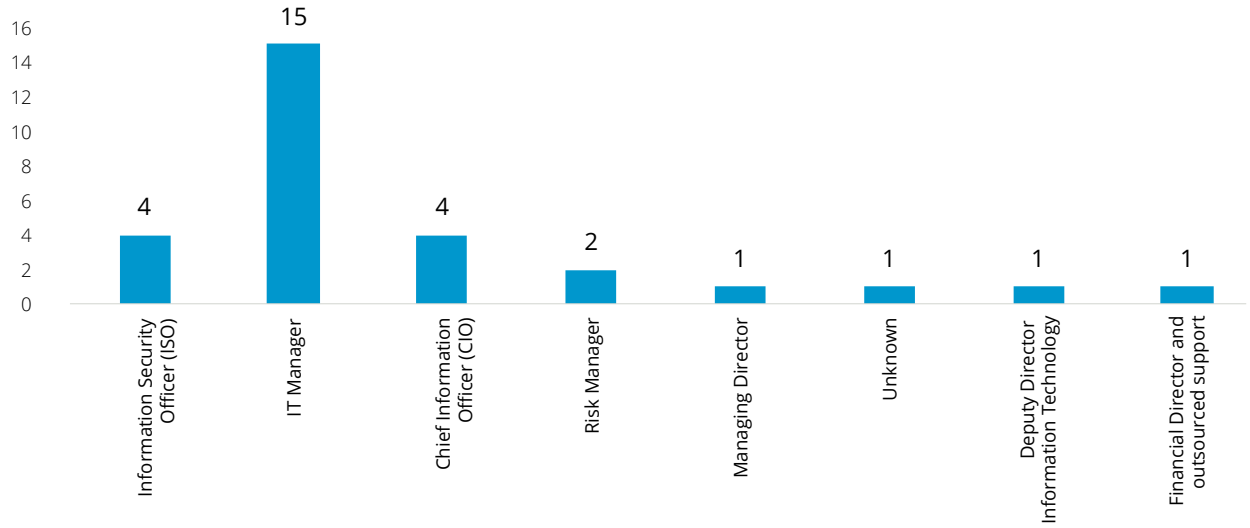
The respondents consisted of a roughly equal mix of small, medium large and very large entities, enabling us to obtain information likely to be of value to a wide segment of the Namibian economy.

Respondents by size



Responsibility for cyber security

Persons responsible for cyber risk

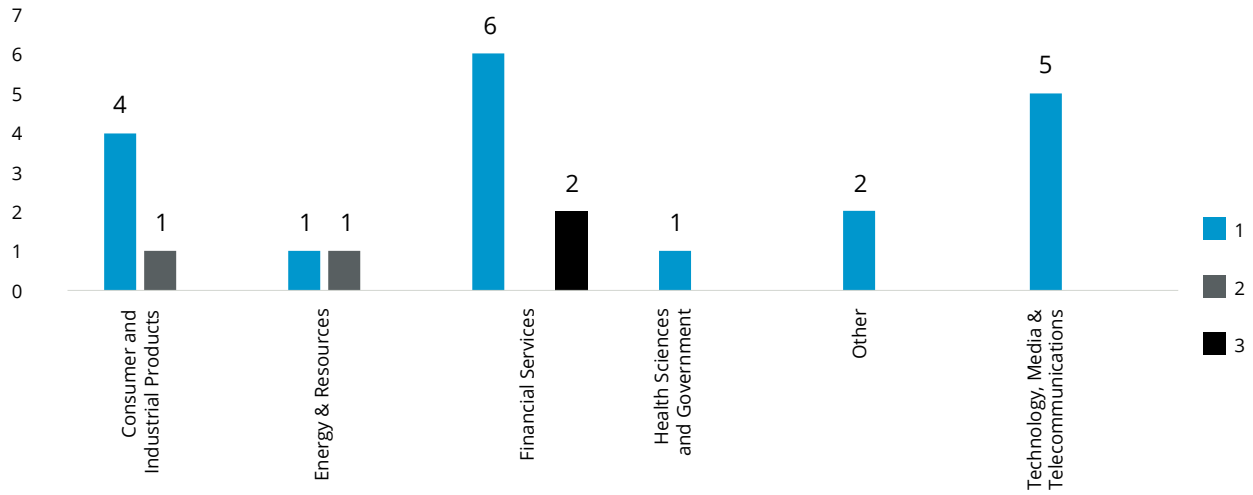


In most cases, the responsibility to monitor and manage cyber risk, cyber incidents and cyber security rests with the IT Manager, although we noted a number of entities made use of a dedicated Information Security Officer, Chief Information Officer or Risk Manager. ISACA, the Information Systems Audit 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. This is also in line with the requirements of the Namibian Code for corporate governance (NamCode) and King IV.

78% of entities allocate responsibility for the monitoring and management of cyber risk at managerial level or below.

In 76% of all entities, a single person was reported to be responsible for the monitoring and management of cyber risk and incidents, with two respondents reporting as many as three different roles and individuals being involved in the management of cyber risk and incidents. While there are certainly a number of 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 on consistently.

Number of persons responsible for cyber risk by industry



Risk management

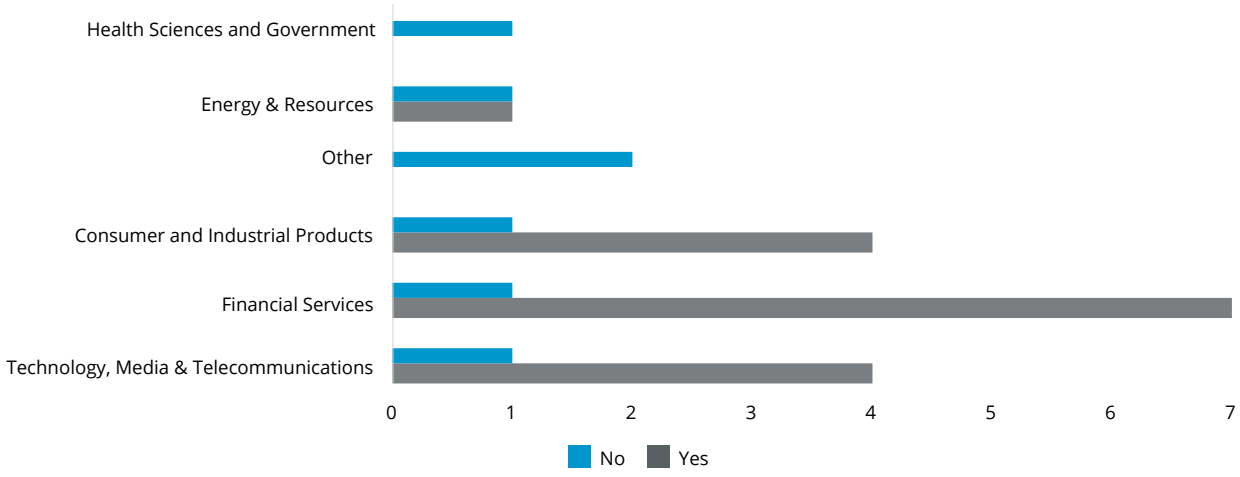
The risk management theme looks at the inclusion of cyber risk and business continuity management in the strategy and risk management of surveyed enterprises. It has been our experience in the past that entities are inclined to see the responsibility for cyber risk and business continuity to be mainly 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, as noted in the Guidance for Boards of Directors and Executive Management, 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 graph above.

Risk management includes the existence of a business continuity plan, which is an enterprise-wide contingency plan for a variety of likely scenarios, one aspect of which is an IT continuity or disaster recovery plan. By inference, a disaster recovery plan is only a small portion of the bigger whole of a business continuity plan and addresses the arguably most likely risk of IT system downtime.

70% of respondents felt that their organisation manages cyber risk actively, while respondents in regulated industries noted that regulators did not include cyber risk or business continuity as specific evaluation components in recent risk management audits.

This is expected, given the relatively recent development of cyber risk as a topic and a profession. However, global developments within this space, such as the General Data Protection Regulation (GDPR) of the European Union, which comes into effect 25 May 2018, may have a severe impact on local operations if Namibian entities are found to be in breach of global requirements.

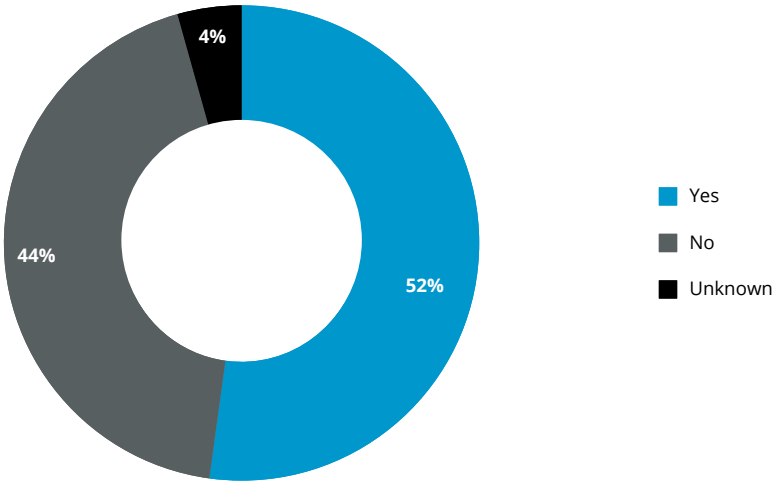
Active management of cyber risk by industry



70% manage cyber actively, but on 52% include a business continuity plan as part of this management

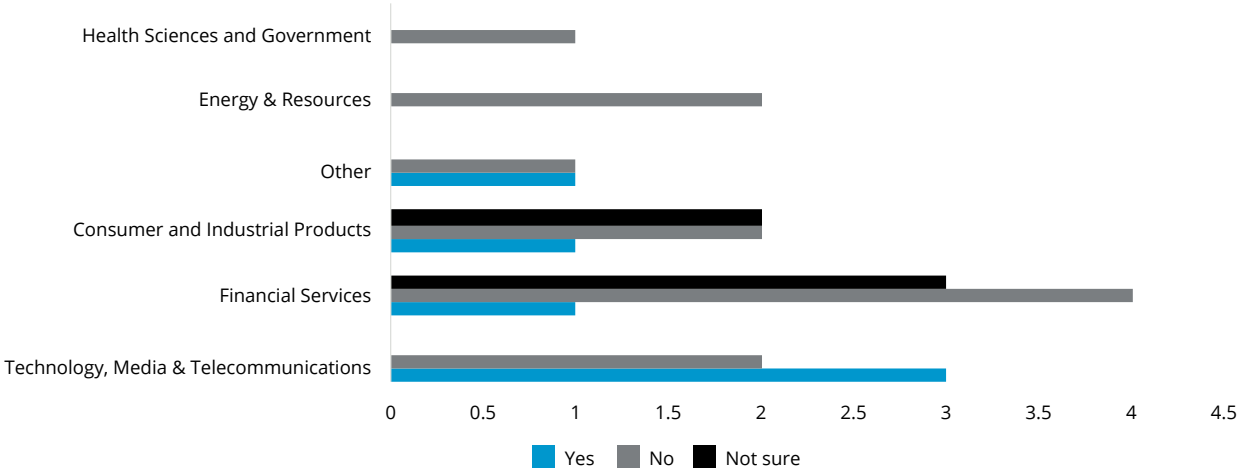
By contrast, only 52% of respondents had a documented and disseminated business continuity or disaster recovery plan, with 4% of respondents being unsure as to the status of any business continuity or disaster recovery plans. As a cyber incident may well cause system downtime, a well-documented business continuity plan or at an absolute minimum a disaster recovery plan is a critical component of cyber risk management.

Existence of final business continuity plans



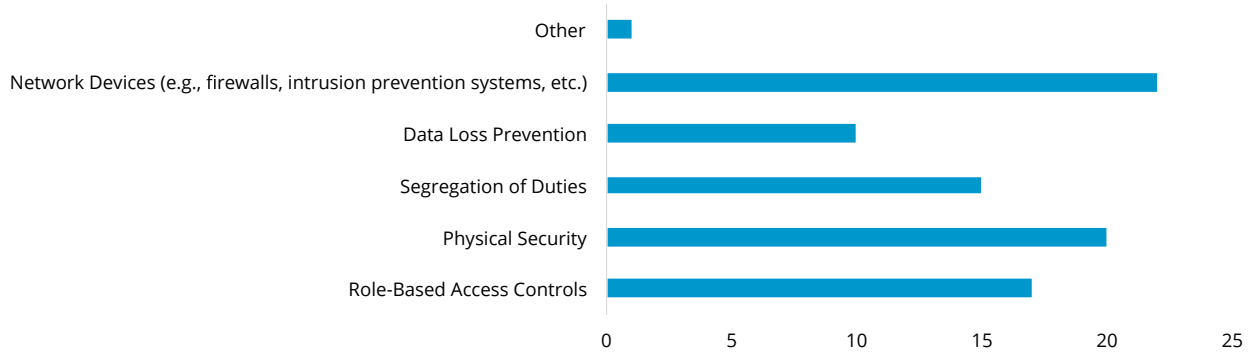
While cyber risk insurance coverage is a relatively new concept for Namibia, 22% of respondents indicated that their insurance covers cyber incidents, with another 26% being uncertain of the details of their insurance cover. In the absence of risk prevention methods or where such methods are considered cost-ineffective, insurance may be an appropriate risk management strategy. However, most insurers are likely to require certain risk prevention measures to be put in place. In the absence of precedents for Namibia, the likelihood of a successful claim against cyber risk insurance cannot be assessed appropriately.

Insurance on cyber risk



All entities surveyed applied at least one form of safeguard for their most sensitive information, with the most common form being some form of network device such as firewalls or intrusion prevention systems, with 26% of entities applying all five commonly recommended forms of safeguard and another 35% applying four out of five commonly applied safeguards.

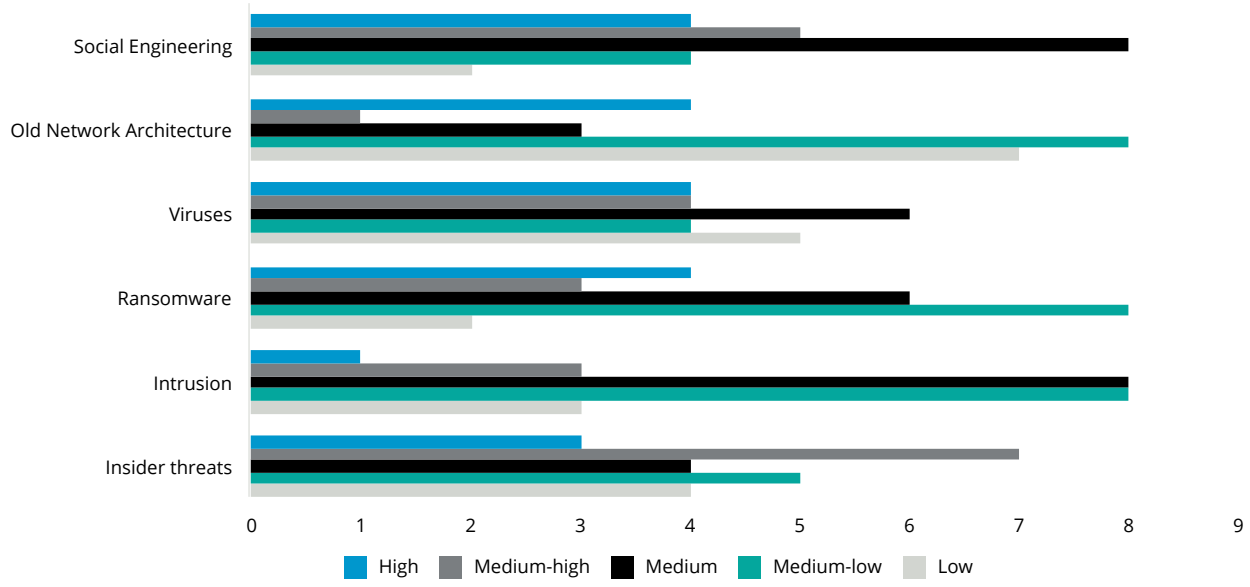
Safeguards applied



61% of entities apply at least four different types of safeguards and information security controls

In general, the majority of respondents assessed the likelihood and impact of cyber threats as low to medium, which is contrary to data in the Symantec™ Internet Security Threat Report (April 2017) that indicates an increased level and frequency of attacks globally. Some examples of recent cyber attacks range from the devastating such as the increased spate of ransomware such as WannaCry and Petya to the insidious, such as the hijacking of servers running Oracle (via a web server patch vulnerability) that were then used to mine cryptocurrency as recently as January 2018.

Assessment of threats



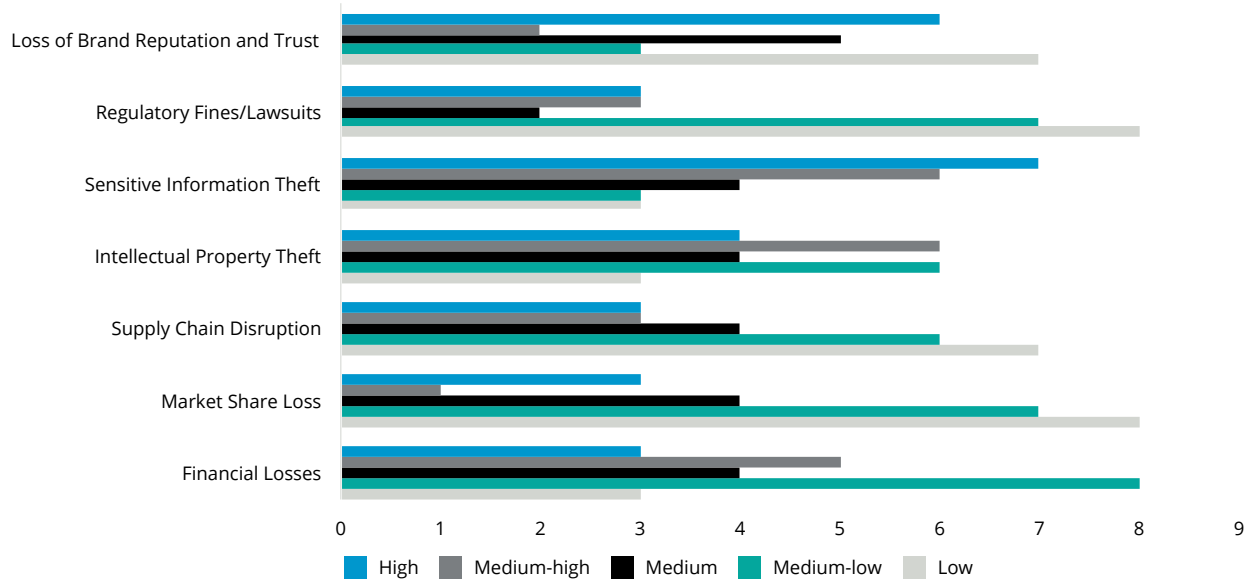
Entities surveyed generally seem to underestimate the likelihood of threats

Once a cyber attack has occurred, there are a number of risk exposures an entity may face. In general, these are:

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

Respondents rated loss of brand reputation and trust and the theft of sensitive information as the biggest threats to their entity and regulatory or legal implications, supply chain disruption and loss of market share as the lowest threats.

Risk exposure on occurence of cyber attack



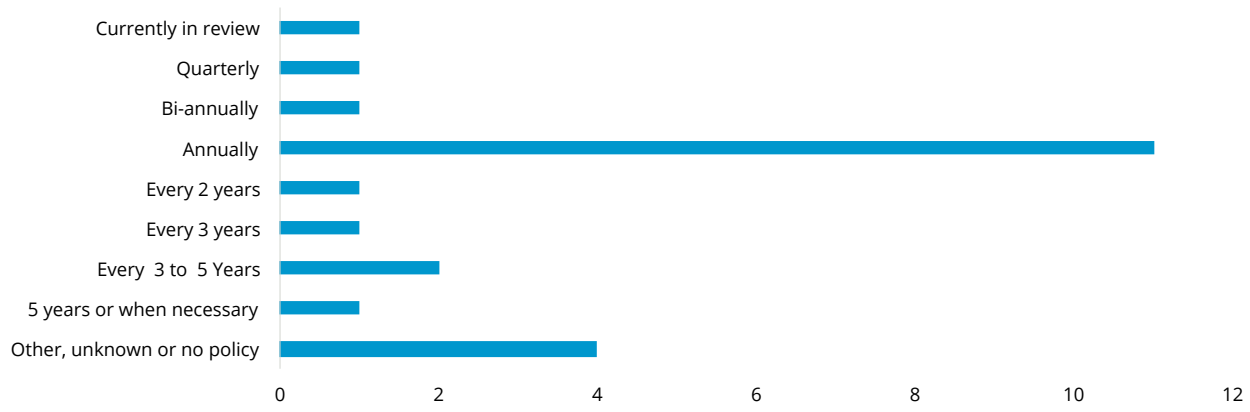
Loss of brand reputation and trust and theft of sensitive information were ranked as the highest concerns to entities

Most respondents reported having an information security policy but only one respondent had a documented cyber incident response plan. About half of all respondents indicated also having a separately defined information security plan or strategy and a data classification policy.

Implementation of plans and policies

Reviews of the above documents are performed annually in 48% of cases, with 13% of entities performing reviews more frequently.

Review frequency of information security documents



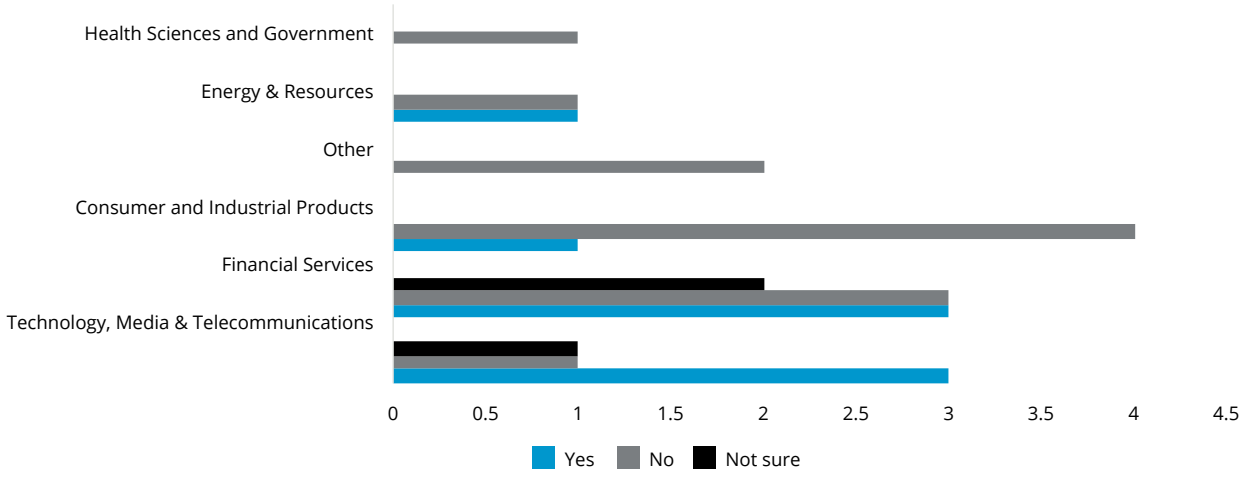
61% review information security related policies at least annually

Skills and awareness

Only 35% of respondents felt that their organisation had adequate skills and capacity within the organisation to deal with information security activities and risks. Responses seem to indicate a bias of skilled personnel to seek out positions within the Financial Services and Telecommunications industries respectively.

35% of respondents did not conduct training on information security at all. 40% of the entities who responded "no" or "not sure" regarding skills and capacity above did not conduct any training on information security. 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*, 2017, 80% of hacking-related breaches leveraged weak password culture (e.g. sharing of passwords, lack of complexity), and 95% of successful phishing attacks led to the installation of malicious software.

Evaluation of skills and capacity in information security

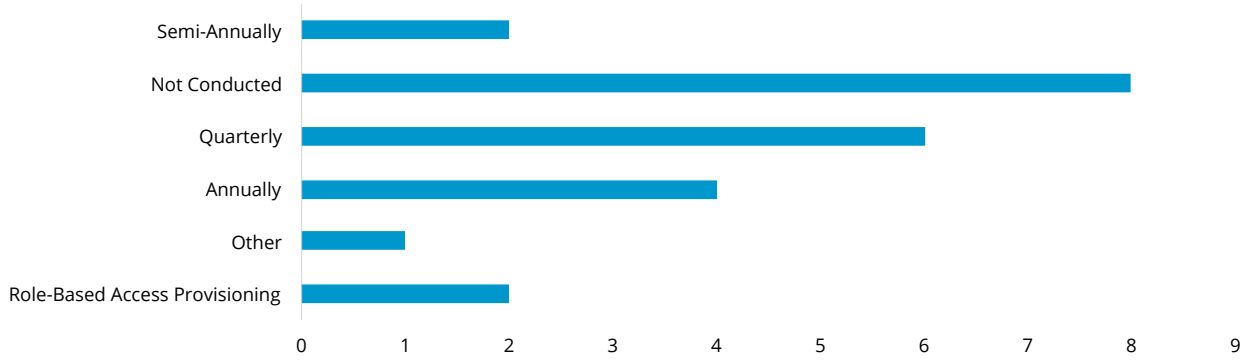


65% of entities feel insufficient skills exist in within their entity

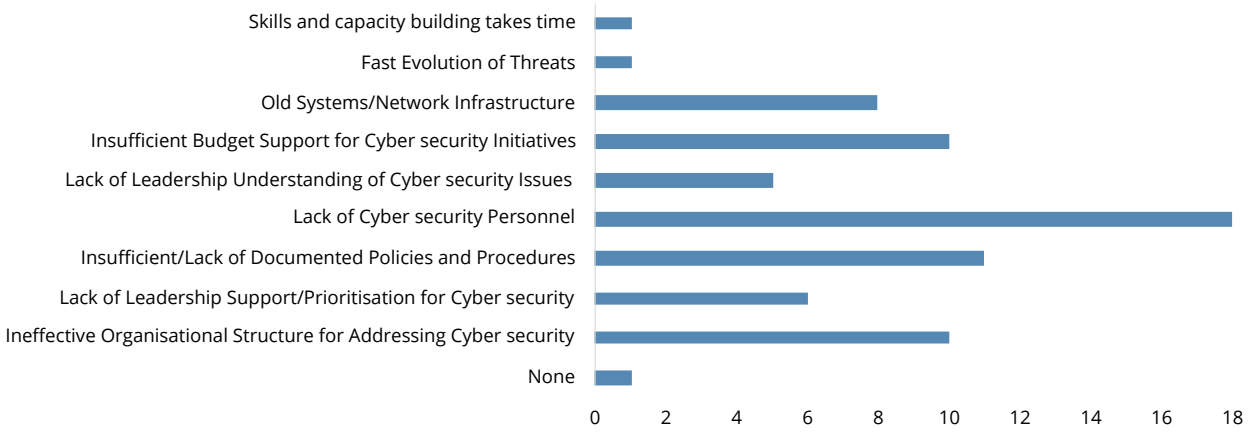
35% of entities did not conduct user training on information security at all

96% of respondents have experienced at least one common challenge in addressing cyber risk appropriately, with the majority (78%) being concerned about the lack of trained cyber security personnel. 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). Offerings for these certifications are available online and exams can be written at a certified venue in Namibia.

Frequency of training on information security

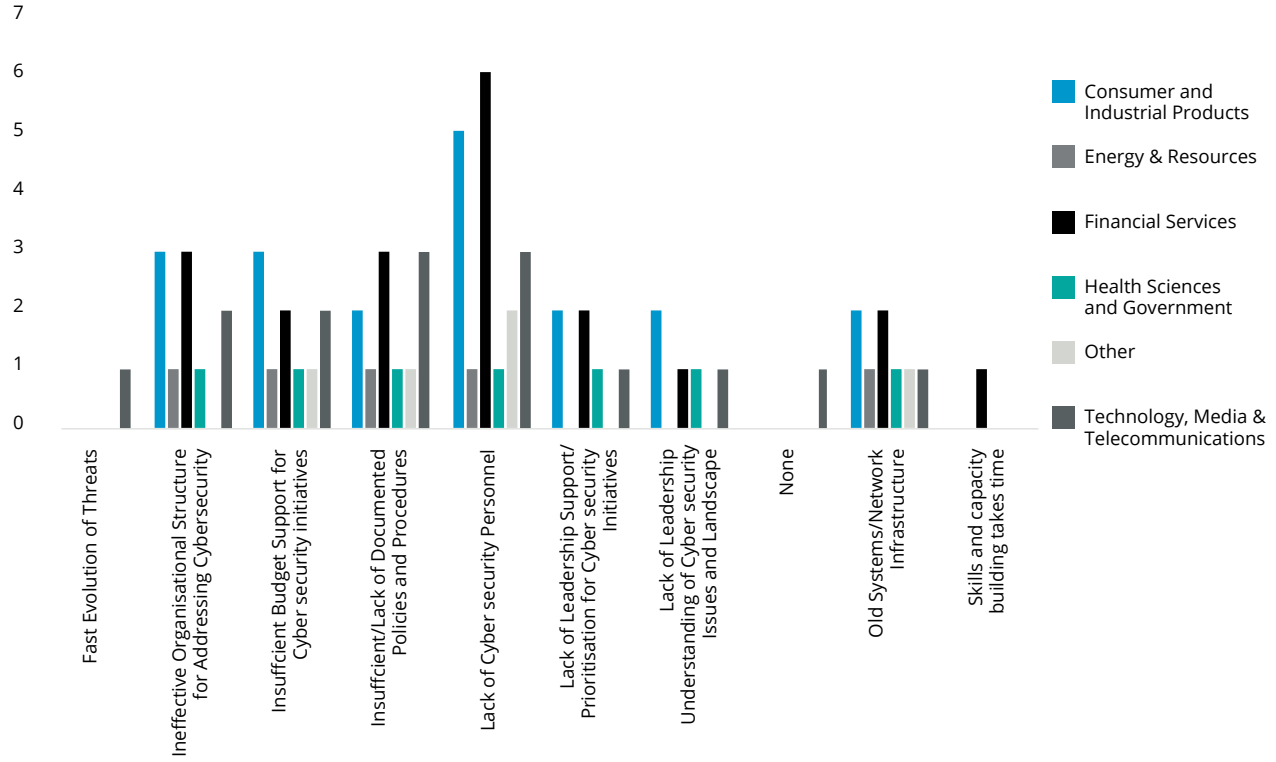


Common cyber challenges experienced



Interestingly, the perception of challenges experienced by industry does not directly correlate to the industries' perception of the adequacy of currently available skills and staff, indicating that information security professionals tend to gravitate towards certain industries, although we are not in a position to make a determination on the root cause of this.

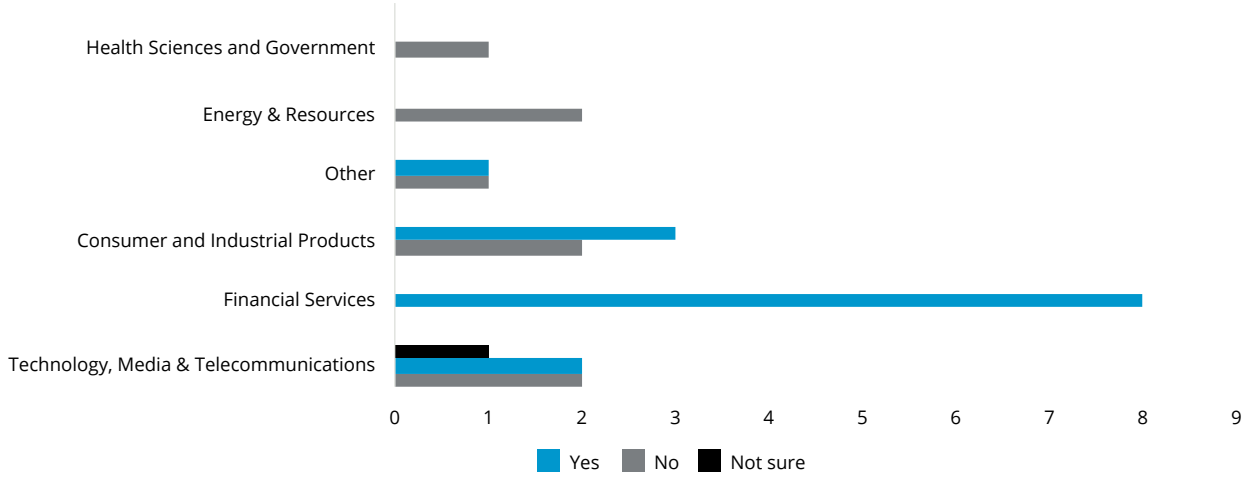
Cyber Challenges by industry



Monitoring and proactive incident management

39% of respondents have never performed or are not aware of the performance of a vulnerability assessment, penetration test or a review of software source code. Financial services 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 v3.2) to which most financial services would have to comply as a result of offering card services.

Performance of vulnerability assessment, penetration testing or software code review

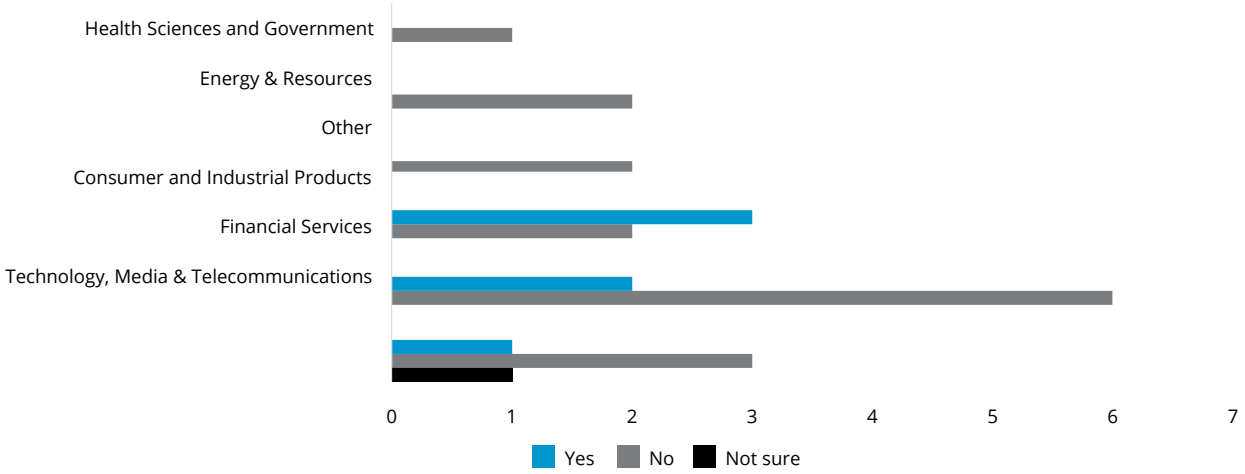


39% of entities have never performed a vulnerability assessment penetration testing or software code review to determine potential exposure

Only 26% of respondents have indicated being aware of a cyber incident within their entity and have experienced interruptions due to such an incident, despite Symantec's reports of rising, successful attacks. According to Symantec, "Services" was the most targeted industry in 2016 with 452 successful breaches, followed by the financial services sector with 226 breaches.

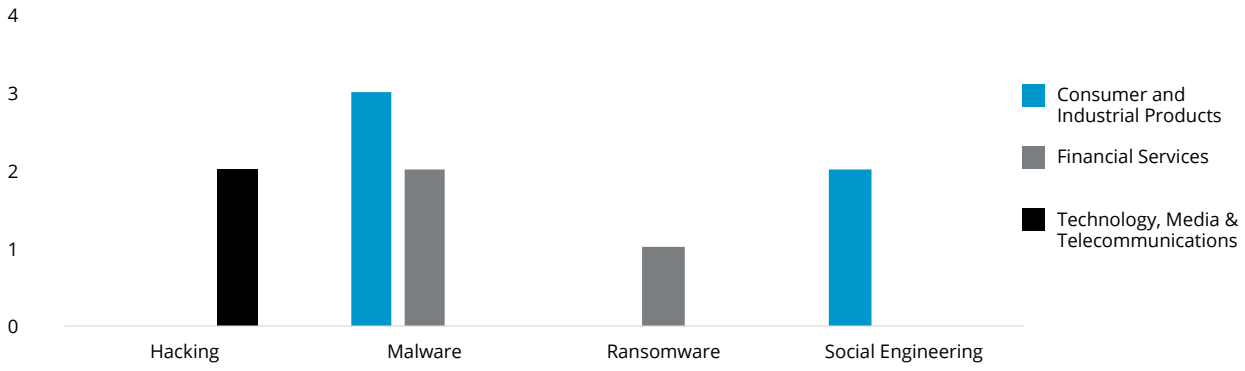
The Ponemon Institute's *2017 Cost of Data Breach Study* puts the average total cost of incidents with fewer than 10 000 compromised records at USD 1.9 million and at USD 6.3 million for incidents with more than 50 000 compromised records, which highlights the potentially devastating effect even a "minor" incident can have on an entity. Furthermore, the Ponemon study noted that regulated industries such as healthcare, education and financial services experience an increased cost proportionately to other industries and that malicious or criminal attacks were the root cause of breaches in 47% of cases, followed by human error in 28% of cases and system errors in 25% of cases.

Interruptions due to cyber incidents



Of the above respondents, the largest proportion (83%) experienced malware attacks with 67% having experienced two or more forms of cyber incidents before. This is in line with above metrics on information security training and much higher than reported in the Verizon Data Breach Investigations Report, 2017, which states the installation of malicious software occurs in about 51 % of breaches. Interesting to note is also that targeted industries, or at least industries aware of being targeted, are focussed on industries of national importance, given that without payment services or telecommunications, other industries are unlikely to be able to operate. Likewise, given the small concentration of consumer and industrial product companies in Namibia, attacks on these entities may have a ripple effect on the ability of consumers or other entities to survive.

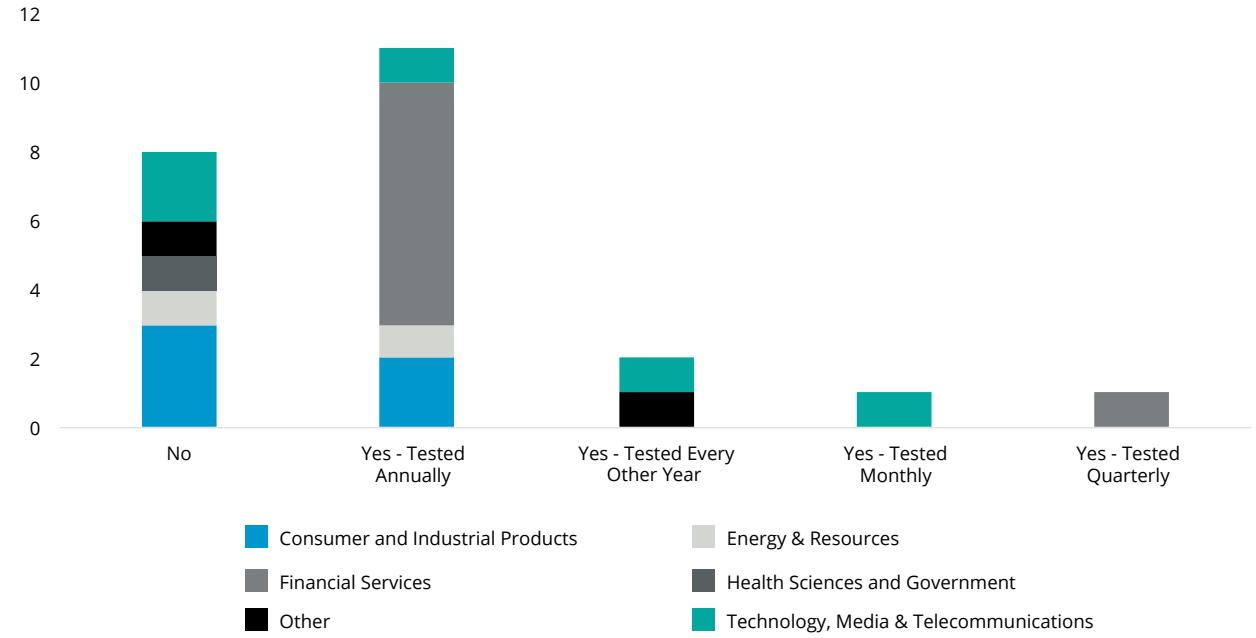
Types of cyber incidents experienced



In line with insufficient skills and lack of training, malware is the biggest source of attack for entities

65% of respondents test their business continuity plans; with 48% testing at least annually, in line with best practice.

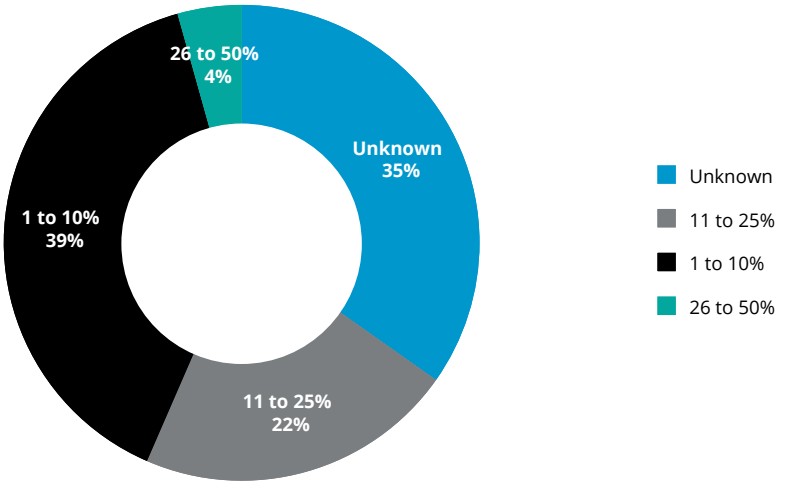
Testing of business continuity plans



Financial metrics

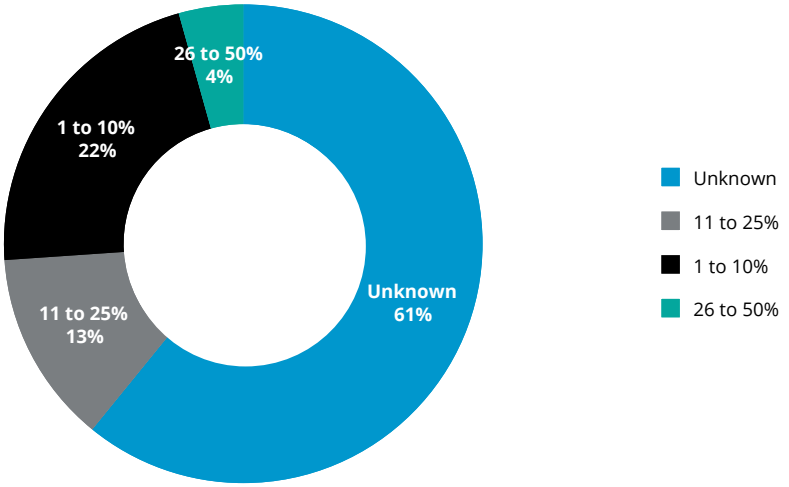
Budgetary spend on cyber security has a direct correlation to risk exposure and helps in understanding the relative level of investment to support the security of the total IT environment from an overall operational point of view. As per the Gartner report on key IT metrics for 2017, the average spend on IT security as a percentage of total expenditure amounts to 5.9%. Based on this, Namibian entities appear to be aligned to global metrics. This number may however be too low given the general drive towards development of IT infrastructure and general immaturity of IT security. A large proportion (35%) of respondents were not sure that cyber security management forms part of overall operating cost considerations.

Percentage of operating costs dedicated to cyber security management



The business continuity plan should take cyber risk into consideration and therefore the business continuity budget would ordinarily make provision for such costs, however in 61% of cases, cyber security and incident response management does not seem to be included as a cost consideration.

Percentage of Business Continuity Budget set aside for cyber security



Cyber security and business continuity does not form part of the IT operational budget in the majority of cases

Background and definitions

In general, the topics of cyber security, information security and IT governance are used in a loosely interchangeable fashion, resulting in significant confusion amongst participants in discussions. In order to clarify the topic, we refer to the definitions as contained in the Namibian Code of Corporate Governance (NamCode), which we have used in the sense provided throughout this report:

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 – Is 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.

Classified information systems – Refers to a system of people, data records and activities that process the data and information in a company, and it includes the company's manual and automated processes. In a narrow sense, the term information system (or computer-based information system) refers to the specific application software that is used to store data records in a computer system and automates some of the information-processing activities of the company.

Cloud-computing – Is a style of computing in which dynamically scalable and often virtualised resources are provided as a service over the Internet.

Information governance – Is an emerging discipline with an evolving definition. The discipline embodies a convergence of data quality, data management, business process management, and risk management surrounding the handling of data in a company. Also defined as data governance.

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.

Security incident management programme – Security incident management programme is the monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events. It defines and implements a process that a company may adopt to promote its own welfare and the security of the public.

Standards and guidelines

A significant portion of our survey focussed on the respondents' ability to provide adequate direction and management of the related cyber risks, which depend heavily on clearly defined roles and responsibilities. Chapter 5 of the NamCode provides for the following high-level responsibilities related to the governance of information technology:

1. The board should be responsible for information technology (IT) governance;
2. IT should be aligned with the performance and sustainability objectives of the company;
3. The board should delegate to management the responsibility for the implementation of an IT governance framework;
4. The board should monitor and evaluate significant IT investments and expenditure;
5. IT should form an integral part of the company's risk management;
6. The board should ensure that information assets are managed effectively; and
7. A risk committee and audit committee should assist the board in carrying out its IT responsibilities.

King IV goes a step further than the NamCode in allocating responsibility in this area of entity operations by recognising that there is a distinct difference between "Information" and "Technology" and defines these concepts as follows, respectively:

1. Information includes all data, records and knowledge in electronic or any other format, which form part of the intellectual capital used, transformed or produced by the organisation.
2. Technology comprises the infrastructure, devices, systems and software that generate, use or carry information and enable transactions.

Accordingly, the responsibility for information management and risk assessment should be carefully and clearly defined to manage the overlap between the various activities performed by each role within an entity, and an overall responsible party should be designated who is in a position to understand, communicate and manage all parties' interests.

In addition to the above codes of corporate governance, COBIT 5, ITIL, PCI DSS 3.2 and ISO 27001 all provide further guidance on a more managerial level on the considerations and controls that should be put in place. COBIT 5, in particular, focusses on connecting and aligning the governance of IT to the overall strategy and direction of the enterprise, while ITIL, PCI DSS 3.2 and ISO 27001 focus on adequate control structures. All standards acknowledge and manage the people element of information technology and recognise that information security hinges on appropriate behaviours by employees, customers and suppliers with access to company information assets.

Contacts

Melanie Harrison
Director
Risk Advisory
Tel: 061 285 5003
Email: melharrison@deloitte.co.za

Nicoline Badenhorst
Manager
Risk Advisory
Tel: 061 285 5056
Email: nbadenhorst@deloitte.co.za

Bibliography

1. IT Governance Institute: Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition; copyright 2006
2. Symantec™: Internet Security Threat Report April 2017
3. Linda Hall, Eric Stegman, Shreya Futela, Disha Gupta: Gartner IT Key Metrics Data 2017: Key IT Security Measures: Current Year, Published: 12 December 2016
4. Verizon: 2017 Data Breach Investigations Report (Executive Summary)
5. Ponemon Institute LLC: 2017 Cost of Data Breach Study - Global Overview, June 2017
6. The Namibian Stock Exchange (NSX) and the Institute of Directors in Southern Africa (IoDSA): NamCode, the Corporate Governance Code for Namibia
7. Institute of Directors Southern Africa: King IV Report on Corporate Governance for South Africa 2016

Deloitte.

Designed and produced by Creative Services at Deloitte, Johannesburg. (00000/chr)