INSTITUTE OF DIRECTORS
SOUTHERN AFRICA

AUDIT COMMITTEE FORUM™
POSITION PAPER 17

CYBERSECURITY: It's not just about technology

Issue Date: June 2017

acf.co.za

Audit Committee Forum™ is proudly Sponsored by KPMG

KPMG

The information contained in the position paper disseminated by the Audit Committee Forum™ is of a general nature and is not intended to address the circumstances of any particular individual or entity. The views and opinions of the forum do not necessarily represent the views and opinions of KPMG, the Institute of Directors and/or individual members. Although every endeavour is made to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No reliance should be placed on these position papers, nor should any action be taken without first obtaining appropriate professional advice. The Audit Committee Forum™ shall not be liable for any loss or damage, whether direct, indirect consequential or otherwise which may be suffered, arising from any cause in connection with anything done or not done pursuant to the information presented herein. Copyright by the Audit Committee Forum™, extracts of this paper may be reproduced with acknowledgement to the Audit committee Forum™.

These terms of reference have been drafted for the specific purposes of a public or state-owned company. In the case of other companies, the terms should be adjusted to reflect that the audit committee is a committee of the governing body and taking into account any other relevant legislation. We have also assumed with the drafting of this document that there is a separate risk committee.

The document goes into detail, but may be tailored and abbreviated to suit the entity's needs. The bold paragraphs are recommended, while the light paragraphs are optional.

Contents

Introduction

One of the greatest challenges facing governing bodies today is one that directors feel least prepared for: Cybersecurity.

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access.

Cybersecurity ranked as a top risk for governing bodies trailing only the economy and the regulatory environment. Governing bodies acknowledge cybersecurity as an urgent Global issue, but are failing to make the connection between the pervasiveness of cyber threats and their organisation's vulnerabilities.

With cybersecurity continually being focused on as a key risk area, governing bodies should review their specific approach to oversight of this risk and, where applicable, examine the role of the audit committee in coordinating with management and the entire governing body for assessing and responding to cybersecurity threats.

> "Cybersecurity ranked as a top risk for governing bodies trailing only the economy and the regulatory environment.

What is cybercrime and who is carrying it out?

Any compromise of network security, failure of IT continuity or loss of data integrity could result in legal liability, regulatory action, lost revenue or crisis containment costs as well as damaging an organisation's brand and reputation. Businesses must also be increasingly mindful of external stakeholders in the form of regulators and standard setting bodies and those who might incur financial harm as a result of cyber events occurring within the organisation's network.

The broad spectrum of cyber and information security risks which pose the potential for significant economic loss and reputational damage include:

- The theft, loss or unauthorised disclosure of personal, organisation information or client information, payment card information or other third party confidential information.
- Cyber-attacks and other events (ransomware) that result in denial of service, outages and disruption to critical software applications and networks.
- A changing regulatory environment with the Protection of Personal Information Act (PoPI), introducing penalties and the mandatory notification of affected data subjects following a breach.
- Unintentional electronic or print media infringements resulting in liability for defamation, plagiarism or infringement of copyright.

Business exposures resulting from cybercrime and the rapidly evolving regulatory environment may be classified into one of two categories;

- First party direct losses such as business interruption, extortion, loss of digital assets or fines and penalties or
- Third party liability losses such as information security breaches, denial of service or errors and omissions resulting in transmission of a virus.

Understanding the "actor', i.e. the person or organisation that is sponsoring or conducting the attacks, is essential for effective defense.

Actors can be divided into six categories:

- An individual hacker, generally acting alone and motivated by being able to show what he/she can do.
- Disgruntled employees focused on causing harm to the organisation.
- The activist, focused on raising the profile of an ideology or political viewpoint, often by creating fear and disruption.
- Organised crime focused solely on financial gain through a variety of mechanisms, from phishing to selling stolen organisation data.
- Governments, focused on improving their geopolitical position and/or commercial interests.
- Competitors seeking information, industrial espionage.

Attacks by these different actors have a number of different characteristics, such as the type of target, the attack methods and scale of impact.

An interesting source of information is accessible at the following link[1] which provides the global origin, type and target of attacks.

[1] Norse – http://map.norsecorp.com/#/

Understanding the cyber risk

The amount of data continues to grow exponentially, as does the rate at which organisations share data through online networks. Billions of devices – tablets, smartphones, ATM machines, security installations, oil fields, environmental control systems, thermostats and much more – are all linked together, increasing inter-dependencies exponentially.

Organisations increasingly open their IT systems to a wide range of machines and lose direct control of data security. Furthermore, business continuity, both in society and within companies, is increasingly dependent on IT. Disruption to these core processes can have a major impact on service availability.

The two broad categories for cyber vulnerability are internal - disgruntled employees and external – cyber criminals.

Often internal people are a greater threat than outsiders. The people on the inside aren't more hostile, they just have more access. An insider could access private and/or sensitive information more easily than a cyber criminal.

Cyber criminals are driven by a wide range of motivations – from pure financial gain, to raising the profile of an ideology, to espionage or terrorism – individual hackers, activists, organised criminals and governments are attacking government and organisation networks with increasing volume and severity.

But while the cyber threat is very real and its impact can be debilitating, the media often sketches an alarmist picture of cybersecurity, creating a culture of disproportionate fear. Not all organisations are necessarily easy targets for cyber criminals. For example, a small or medium sized organisation has a very different risk profile than a multinational organisation.

What is true for any government or organisation is that cybercrime risks can be mitigated. Cyber criminals are not invincible geniuses, and while they can cause real damage to an organisation, steps can be taken to protect against them. It is not possible to achieve 100 percent security, but by treating cybersecurity as "business as usual" and balancing investment between risks and potential impacts, an organisation will be well prepared to combat cybercrime.

There is a plethora of data about various cyber threats, vulnerabilities, risks, trends that cover systems, malware, servers, data integrity, software patches, and cyber-attacks. To delve through all this data will prove to be overwhelming for executives. By developing pro-actively, a Key Risk Indicator (KRI) dashboard for cybersecurity, executives can keep current with and make decisions regarding their organisation's specific cyber security posture, the progress and status of mitigating plans and the latest cyber threats and their impact on the organisation, without having to delve into excessive amounts of data.

Typically, Key Risk Indicators (KRIs) are critical predictors of unfavourable events that can adversely impact an organisation. They monitor changes in the levels of risk exposure and contribute to the early warning signs that enable organisations to report risks, prevent crises and mitigate them in time.

Depending on the risk profile of an organisation, cyber KRIs may cover various cyber domains including incidents, patch management, encryption levels of all devices, malware breaches, third parties, privileged users, vulnerabilities, cyber training and awareness.

Organisations can reduce the risks to their business by building up capabilities in three critical areas – prevention, detection and response.*

Prevention

Prevention begins with governance and organisation. It is about installing fundamental measures, including placing responsibility for dealing with cybercrime within the organisation and developing an awareness and training for key staff.

Detection

Through monitoring of critical events and incidents, an organisation can strengthen its technological detection measures. Monitoring and data mining together form an excellent instrument to detect strange patterns in data traffic, to find the location on which the attacks focus and to observe system performance.

Response

Response refers to activating a well-rehearsed plan as soon as evidence of a possible attack occurs. During an attack, the organisation should be able to directly deactivate all technology affected. When developing a response and recovery plan, an organisation should perceive cyber security as a continuous process and not as a once-off solution.

*Useful website to visit is - https://www.cyberaware.gov.uk/cyberessentials/

	Prevention	Detection	Response
Management and organisation	• Allocating cybercrime responsibilities.	• Ensuring a 24/7 stand-by (crisis) organisation.	• Using forensic analysis skills. • Maintaining a cybersecurity register.
Processes	• Cybercrime response tests (simulations). • Periodic scans and penetration tests. • Deep Dive testing. • Firewalls. • Keeping patches up to date. • Sharing of incident information by industry players.	• Procedures for follow-up of incidents to identify trends and track cyber threats.	• Cybercrime response plan.
Technology	• Ensuring adequate desktop security. • Ensuring network segmentation.	• Monitoring of the critical processes and information. • Implementing central monitoring of security incidents	• Deactivating or discontinuing IT services under attack.

The five most common cybersecurity mistakes

To many, cybersecurity is a bit of a mystery. This lack of understanding has created many misconceptions among management about how to approach cybersecurity. The following five cybersecurity mistakes occur regularly – often with drastic results.

Mistake 1

"We have to achieve 100 percent security"

Reality

100 Percent security is neither feasible nor the appropriate goal

Almost every airline organisation claims that flight safety is its highest priority while recognising that there is an inherent risk in flying. The same applies to cybersecurity. Whether it remains private or is made public, almost every large, well-known organisation will unfortunately experience information theft.

Developing the awareness that 100 percent protection against cybercrime is neither a feasible nor an appropriate goal is already an important step towards a more effective policy, because it allows management and the governing body to make decisions about the organisation's defensive posture. A good defensive posture is based on understanding the threat (i.e., the criminal) relative to organisational vulnerability (prevention), establishing mechanisms to detect an imminent or actual breach (detection) and establishing a capability that immediately deals with incidents (response) to minimise loss. Once the organisation has identified the risk of cybercrime, it should rank this information in terms of importance and focus its attention on this prioritisation with the appropriate time and effort.

In practice, the emphasis is often skewed towards prevention – the equivalent to building impenetrable walls to keep the intruders out. Once it is understood that perfect security is an illusion and that cybersecurity is "business as usual," then more emphasis must be placed on detection and response. After a cybercrime incident, which may vary from theft of information to a disruptive attack on core systems, an organisation must be able to minimise losses and resolve vulnerabilities.

Mistake 2

"When we invest in best-of-class technological tools, we are safe"

Reality

Effective cybersecurity is less dependent on technology than is thought

The world of cybersecurity is dominated by specialist suppliers that sell technological products, such as products that enable rapid detection of intruders. These tools are essential for basic security, and must be integrated into the technology architecture, but they are not the basis of a holistic and robust cybersecurity policy and strategy. The investment in technological tools should be the output, not the driver, of cybersecurity strategy. Good security starts with developing a robust cyber defence capability. Although this is generally led by the IT department, the knowledge and awareness of the end user is critical. The human factor is and remains, for both IT professionals and the end user, the weakest link in relation to security. Investment in the best tools will only deliver the return when people understand their responsibilities to keep their networks safe. Social engineering, in which hackers manipulate employees to gain access to systems, is still one of the main risks that organisations face.

Technology cannot help in this regard and it is essential that managers take ownership of dealing with this challenge. They have to show genuine interest and be willing to study how best to engage with the workforce to educate staff and build awareness of the threat from cyber attack. This is often about changing the culture such that employees are alert to the risks and are proactive in raising concerns with management.

Mistake 3

"Our weapons have to be better than those of the hackers"

Reality

The security policy should primarily be determined by the organisation's goals, not those of the attackers

The fight against cybercrime is an example of an unwinnable race.

The attackers keep developing new methods and technology and the defence is always one step behind. So is it useful to keep investing in increasingly sophisticated tools to prevent attack?

While it is important to keep up to date and to obtain insights into the intention of attackers and their methods, it is critical for management to adopt a flexible, proactive and strategic approach to cybersecurity. Given the immeasurable value of an organisation's information assets, and the severe implication of any loss on the core business, cybersecurity policies need to prioritise investment into critical asset protection, rather than simply the latest technology or system to detect every niche threat.

First and foremost, managers need to understand what kinds of attackers their business attracts and why.

An organisation may perceive the value of its assets differently than a criminal. How willing are governing bodies and management to accept risks to certain assets over others? Which systems and people store the organisation's key assets, keeping in mind that business and technology have developed as chains and are therefore codependent on each other's security?

Mistake 4

"Cybersecurity compliance is all about effective monitoring"

Reality

The ability to learn is just as important as the ability to monitor

Reality shows that cybersecurity is very much driven by compliance. This is understandable, because many organisations have to accommodate a range of legislation and regulation. However, it is counterproductive to view compliance as the ultimate goal of a cybersecurity policy.

Only an organisation that is capable of understanding external developments and incident trends and using these insights to inform policy and strategy will be successful in combating cybercrime in the long term. Therefore, effective cybersecurity policy and strategy should be based on continuous learning and improvement.

Organisations need to understand how threats evolve and how to anticipate them. This approach is ultimately more cost-effective in the long term than developing ever-higher security "walls." This goes beyond the monitoring of infrastructure:

> *It is about smart analysis of external and internal patterns in order to understand the reality of the threat and the short-, medium- and long-term risk implications. This insight should enable organisations to make sensible security investment choices, including investing to save. Unfortunately, in practice, many organisations do not take a strategic approach and do not collect and use the internal data available to them.*

Organisations need to ensure that incidents are evaluated in such a way that lessons can be learned. In practice, however, actions are driven by real-time incidents and often are not recorded or evaluated. This destroys the ability of the organisation to learn and put better security arrangements in place in the future.

The same applies to monitoring attacks. In many cases, organisations have certain monitoring capabilities, but the findings are not shared with the wider organisation. No lessons, or insufficient lessons, are learned from the information received. Furthermore, monitoring needs to be underpinned by an intelligence requirement. Only once the organisation understands what it needs to monitor does monitoring become an effective tool to detect attacks.

Organisations need to develop an enterprise-wide method for assessing and reporting cybersecurity risks. This requires protocols to determine risk levels and escalations, and methods for equipping the governing body with insight into strategic cyber risks and the impacts on the core business.

Mistake 5

"We need to recruit the best professionals to defend ourselves from cybercrime"

Reality

Cybersecurity is not a department, but an attitude

Cybersecurity is often seen as the responsibility of a department of specialist professionals. This mindset may result in a false sense of security and lead to the wider organisation not taking responsibility.

The real challenge is to make cybersecurity a mainstream approach. The introduction of the Protection of Personal Information Act (PoPI) means that a breach and a loss of information becomes more critical than ever before. PoPI, which is aimed at giving effect to our constitutional right to privacy, was enacted on 26 November 2013 and introduced mandatory reporting and notification of data processing and breaches involving personal information. PoPI contains a number of liability provisions forcing organisations to take accountability for data integrity and the manner in which they gather, process and safeguard personal information.

A loss of personal information can have serious consequences for any organisation, ranging from penalties to civil action. This means that cybersecurity should become part of organisation policy, and in some cases linked to remuneration. It also means that cybersecurity should have a central place when developing new IT systems, and not, as is often the case, be given attention only at the end of such project.

The key is customisation

The risks of cybercrime for a small business compared to a large business, which is operating nationally and/or globally, are vastly different. The former may not have the resources or expertise to adequately detect or prevent cybercrime but the latter is a more attractive target to criminals: it may be more visible, more dependent on IT, and have far more valuable assets. It is clear that both businesses need to adopt a customised approach to cybersecurity, based on the character of the organisation, its risk appetite and the knowledge available. The table below sets out the appropriate and inappropriate responses to cybersecurity.

Appropriate Response	Inappropriate Responses
The directors know which assets to protect and have set up the appropriate measures within the organisation.	The directors take measures without a having a clear idea of the assets of the organisation which are essential to protect.
The directors perceive theft as a risk in the organisation and know that, realistically, it is not possible to prepare for 100 percent security.	The directors see cybercrime as unusual and strive to achieve 100 percent security within the organisation.
The directors have focused on measures that prevent a person from gaining access to and taking the organisation's valuable assets.	The directors have focused on measures that prevent a person from gaining access to the organisation's valuable assets but the directors have not considered taking measures that prevent a person from taking the organisation's valuable assets.
The directors do not let security suppliers spook them and make their own purchasing decisions.	The director's security policy depends on the tools available in the marketplace, without knowing exactly what they need.
When something goes wrong or almost goes wrong, the directors take this as a learning experience.	When something goes wrong or almost goes wrong, the directors panic.
The directors ensure that employees are trained on how to reduce the risk of theft and communicate effectively when they make mistakes.	The directors view cybersecurity as mainly a matter for specialist professionals and don't burden the rest of the organisation with it.
The directors invest in tools because it will assist the continuity of the organisation.	The directors invest in tools because it is mandatory and because the media reports on incidents every day.

The six dimensions of cyber maturity

As management, it is essential to know whether the organisation has an adequate approach to cybersecurity.

Leadership and governance

Is the governing body demonstrating due diligence, ownership and effective management of cyber risk?

Human factors

What is the level and integration of a security culture that empowers and ensures the right people, skills, culture and knowledge?

Information risk management

How robust is the approach to achieve comprehensive and effective risk management of information throughout the organisation and its delivery and supply partners?

Business continuity

Has management made preparations for a security event and the ability to prevent or minimise the impact through successful crisis and stakeholder management?

Operations and technology

What is the level of control measures implemented to address identified risks and minimise the impact of compromise?

Legal and compliance

Is the organisation complying with relevant local and international legislative requirements and governance codes?

The following sources provide guidance in relation to cybersecurity:

- Organisation for Economic Co-operation and Development (OECD).[2]
- King IV.[3]
- Cybercrimes and Cybersecurity Bill.[4]

Addressing all six of these key dimensions can lead to a holistic cybersecurity model, providing the following advantages to the organisation:

- Minimising the risk of an attack on an organisation by an outside cyber criminal, as well as limiting the impact of successful attacks.
- Better information on cybercrime trends and incidents to facilitate decision making.
- Clearer communication on the theme of cybersecurity, enabling everyone to know his or her responsibilities and what needs to be done when an incident has occurred or is suspected.
- Improved reputation, as an organisation that is well prepared and has given careful consideration to its cybersecurity is better placed to reassure its stakeholders.
- Increased knowledge of competence in relation to cybersecurity.
- Benchmarking the organisation in relation to peers in the area of cybersecurity.

[2] OECD - http://www.oecd.org/general/searchresults/?q=cyber security&cx=012432601748511391518:xzeadub0b0a&cof=FORID:11&ie=UTF-8

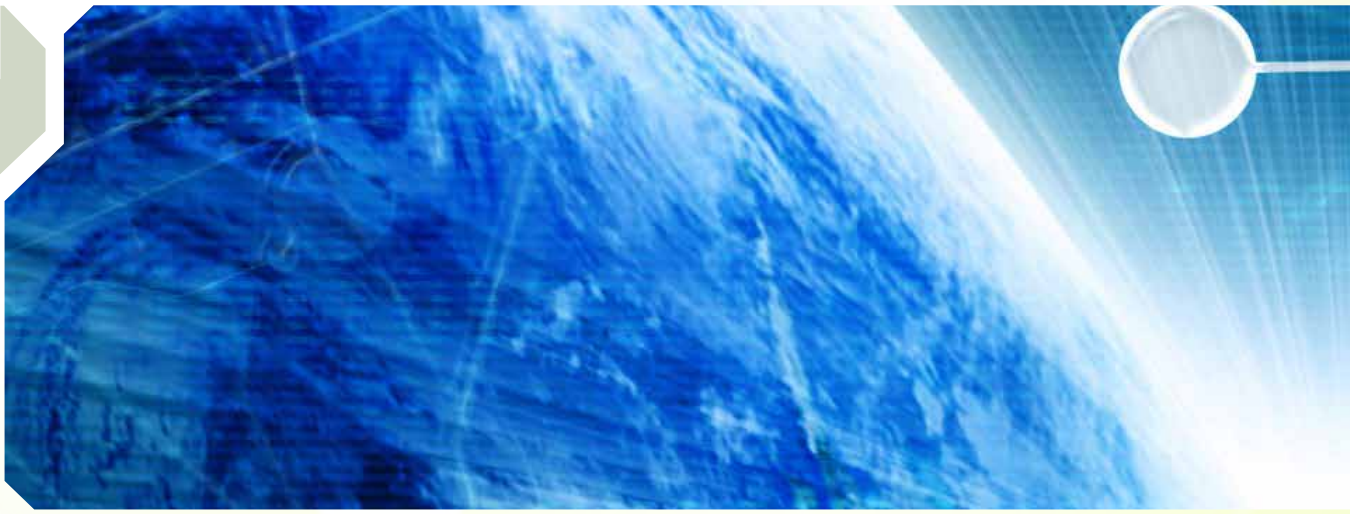
[3] King IV – Principle 12: The governing body should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives; practice 13d

[4] Cybercrime and Cybersecurity Bill – http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf

Appendix 1

Questions to ask to assess "Cyber Literacy"

1. What do the directors consider as the most valuable assets? How does the organisation's IT system interact with those assets? Do the directors believe they can ever fully protect those assets?
2. Do the directors think there is adequate protection in place if someone wanted to get at or damage the corporate "crown jewels"? What would it take for the directors to feel comfortable that those assets were protected?
3. Do the directors believe they are investing enough so that the corporate operating and network systems are not easy targets to a determined hacker?
4. Do the directors believe they are considering the cybersecurity aspects of the major business decisions, such as mergers and acquisitions, partnerships, new product launches, etc., in a timely fashion?
5. Do the directors know who is in charge? Do they have the right talent and clear lines of accountability/responsibility for cybersecurity?
6. Does the organisation participate in any of the public or private sector ecosystem-wide cybersecurity and information-sharing organisation's?
7. Is the organisation adequately monitoring current and potential future cybersecurity-related legislation and regulation?
8. Does the organisation have insurance that covers cyber events, and details of what exactly is covered?
9. Does the organisation have adequate insurance for its directors' and public officers' exposure?
10. What are the benefits beyond risk transfer of carrying cyber insurance?



Appendix 2

Questions about cybersecurity

Situational awareness

1. Were the directors told of cyber-attacks that have already occurred and how severe they were?
2. What are the organisation's cybersecurity risks, and how is the organisation managing these risks?
3. How will the directors know if the organisation has been hacked or breached, and have the directors satisfied themselves that the processes and systems in place will ensure swift communication to them of any incidents?
4. Who are the organisation's likely adversaries?
5. In management's opinion, what is the biggest vulnerability in the organisation's technology systems and information controls?
6. If an adversary wanted to damage the organisation, how would they go about it?
7. Have the directors assessed the inside threat to the organisation?
8. Have the directors performed a penetration test or external assessment? What were the key findings, and how are the directors addressing them? What is the organisation's cyber security maturity level?
9. Does the organisation's internal or external auditor consider, review and report any deficiencies in IT systems? If so, where?

Corporate strategy and operations

1. What are leading practices for cybersecurity, and where do the organisation's practices differ?
2. Do the directors have an appropriately differentiated strategy for general cybersecurity and for protecting the organisation's mission-critical assets?
3. Do the directors have an enterprise-wide, independently budgeted cyber-risk management team? Is the budget adequate?
4. Do the directors have a systematic framework in place to address cybersecurity to assure adequate cyber hygiene?
5. Where do management and the organisation's IT team disagree on cybersecurity?
6. Do the organisation's outsourced service providers and contractors have cyber controls and policies in place and are they clearly monitored? Do those policies align with the organisation's expectations?
7. Does the organisation have cyber insurance? If so, is it adequate?
8. Is there an ongoing, organisation-wide awareness and training program established around cybersecurity?
9. What is the organisation's strategy to address cloud, Bring Your Own Device (BYOD), and supply chain threats?
10. How are the directors addressing the security vulnerabilities of an increasingly mobile workforce?

Incident responses

1. How will management respond to a cyber-attack? Is there a validated corporate incident response plan? Under what circumstances will law enforcement and other relevant government entities be notified?
2. For significant breaches, is the communication adequate as information is obtained regarding the nature and type of breach, the data impacted, and ramifications to the organisation and the response plan?
3. Do the directors have an adequate understanding of the organisation's cyber-preparedness and response plan in order to exercise proper oversight of management's actions?
4. What constitutes a material cybersecurity breach? Does the organisation have a vocabulary describing the level, likelihood and impact of potential breaches? How will material or significant events be disclosed to investors?

Appendix 3

Is the organisation ready for action?

Cybersecurity must be on the agenda. Stakeholders expect the audit committee to pay sufficient attention to this problem.

How big is the risk for the organisation and the organisations which we do business with?

- How attractive is the organisation to potential cyber criminals?
- How dependent is the organisation on the services of partners, suppliers and other organisations, and how integrated are their corresponding cyber security processes?
- Does the audit committee know which processes and/or systems represent the greatest assets from a cybersecurity perspective?
- Has the audit committee considered the risk tolerance of the organisation in relation to these processes and/or systems since there is no such thing as 100 percent security?
- Do the organisation's business partners have the same risk appetite and cybersecurity measures as the organisation?
- Has the audit committee considered its oversight responsibilities regarding the business case for the organisation's cybersecurity investments?

Do governance processes and the organisational culture enable effective risk management?

- Does the audit committee understand how the culture of the organisation contributes to (or hampers) good cybersecurity?
- When was the last time the governing body communicated to the audit committee the importance and processes in place with regard to cybersecurity?
- Has the audit committee satisfied itself that management has an appropriate plan of action to respond to a cybercrime event or breach and how this plan has been communicated throughout the organisation?
- Has the audit committee considered its oversight responsibility for the organisation's cybersecurity policy?

How large should the cybersecurity budget be and how should it be spent?

Depending on the cyber risk profile of the organisation, there should be an appropriate amount set aside for cybersecurity measures. Currently, a significant part of such budgets is often spent on implementing technological solutions and solving problems from the past.

The key questions that need to be answered are:

- Has an appropriate amount of the total IT budget been set aside for cybersecurity?
- How much of the cybersecurity budget is spent on solving past problems?
- How much is spent on structural investments in better security systems?
- How much is spent on systems and tools?
- How much is spent on ensuring proper communication throughout the organisation?
- How much is spent on awareness and culture change?
- Does the audit committee have access to a cybersecurity specialist?

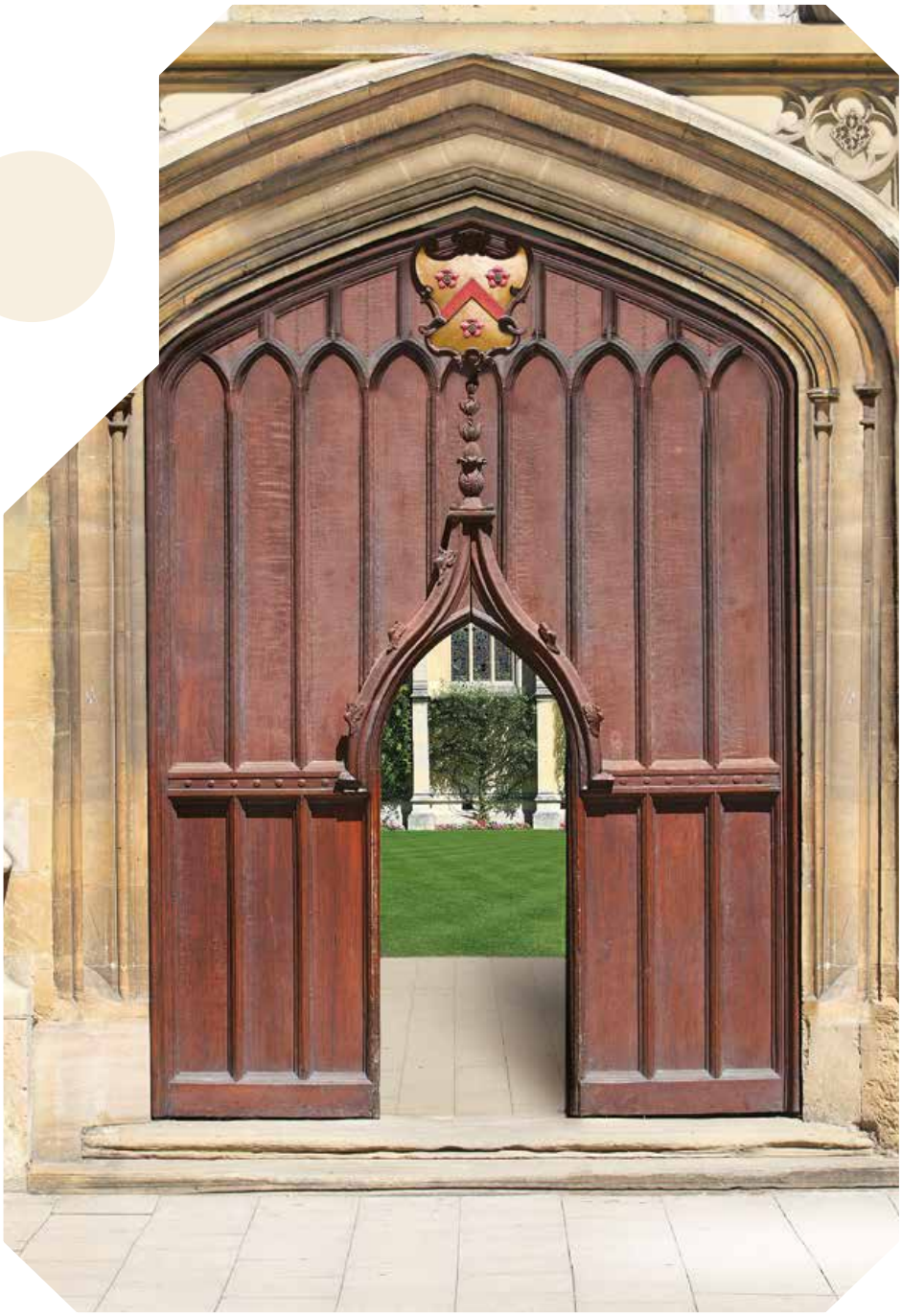
Appendix 4

Cyber Insurance

Information security risks have left many traditional forms of insurance unable to adequately respond to these exposures. An optimised insurance programme combined with specific cyber insurance can fill many of the gaps in traditional insurance and provide direct loss and liability protection for risks created by the use of technology and information in day-to-day operations.

While cyber risk insurance is a relatively new concept in the South African market, there are a number of Insurers writing this class of insurance and it is a rapidly developing segment. As the local market capacity for this class of insurance increases and companies begin to incorporate a cyber-element to their insurance portfolios rates may be expected, to become more competitive in the short to medium term.

Pricing is linked to risk exposure and takes into account the number and type of data records stored or processed, the system security measures in force by way of firewalls, anti-virus, password controls and data encryption and controls implemented to restrict physical access. Insurers will also take into account the organisation's Business Continuity Plans when assessing the risk.



Contact us

KPMG Department of Professional Practice

Thingle Pather
Director
M: +27 (0)83 704 0064
E: thingle.pather@kpmg.co.za

Samantha Habib
Manager
M: +27 (0)82 718 9166
E: samantha.habib@kpmg.co.za

acf.co.za