Deloitte.

Cybersecurity:
The changing role of the Audit Committee and Internal Audit

#DistinctivelyRiskAdvisoryAfrica

1. Introduction

Among the most complex and rapidly evolving issues companies must contend with is cybersecurity. With the advent of mobile technology, cloud computing and social media, reports on major breaches of proprietary information and damage to organisational IT infrastructure have also become increasingly common, thus transforming the IT risk landscape at a rapid pace.

International media reports on high-profile retail breaches and the major discovery of the Heartbleed security vulnerability posing an extensive systemic challenge to the secure storage and transmission of information via the Internet have shone a spotlight on cybersecurity issues.

Consequently, this has kept cybersecurity a high priority on the agenda of Boards and Audit Committees.

- Organised crime is monetising the cyberspace, exploiting vulnerabilities in computer systems to compromise and remotely control computers, recording key strokes, monitoring screen displays and manipulating the computer user into divulging sensitive data.
- Cyberspace being borderless allows any attacker to route their assaults through multiple countries and jurisdictions, complicating investigation and law enforcement.
- Companies run the risk of losing substantial amounts of sensitive company information to malicious employees, who could also potentially remove it from company premises or introduce malicious software to corrupt company databases or sabotage network operations.
- Corporate espionage by companies is commonplace in cyberspace. Attacks often target sensitive intellectual property and there have been multiple instances of major firms with its security compromised over many months and losing substantial amounts of sensitive data during these attacks.
- Activism is also prevalent in cyberspace with sabotage and denial of service attacks growing progressively frequent. In the past, they would be attributed to 'hacktivist' groups such as Anonymous; but increasingly attacks point to political motivations.

Based on the Global Risk Landscape 2014 published by the World Economic Forum, cyber attacks are one of the risks with high impact as well as high likelihood. Refer to figure 1 below.

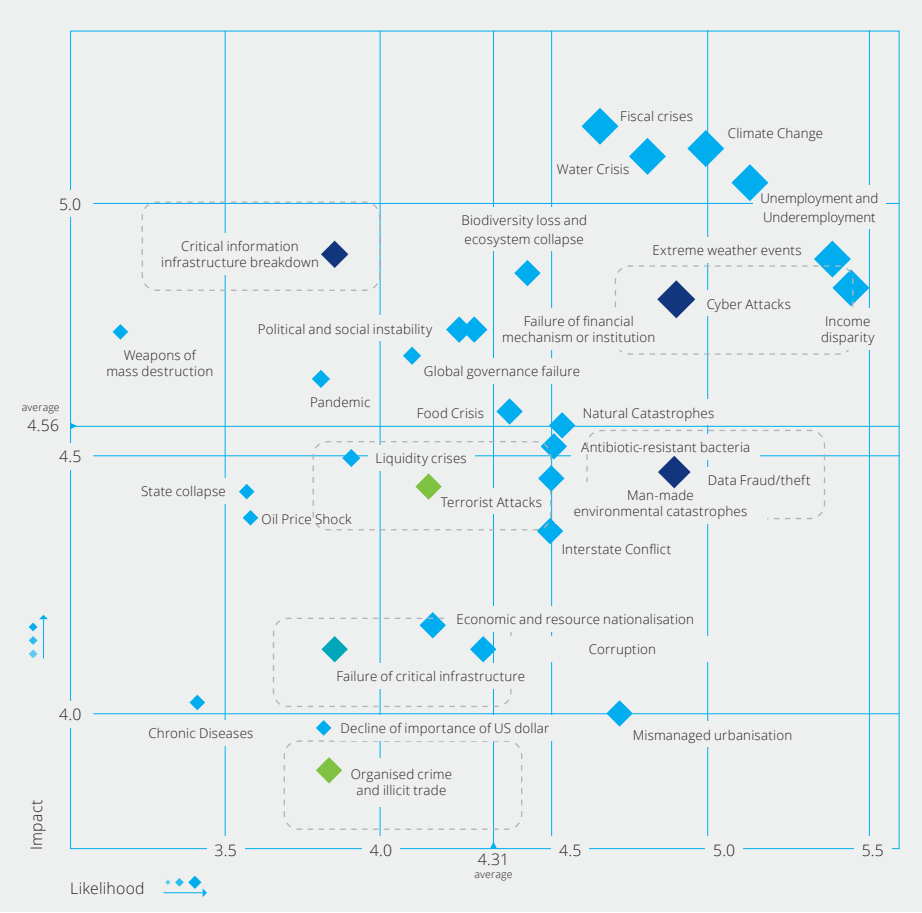


Figure 1. 2014 Global Risk Landscape (World Economic Forum)

2. What is the role of Internal Audit and the Audit Committee?

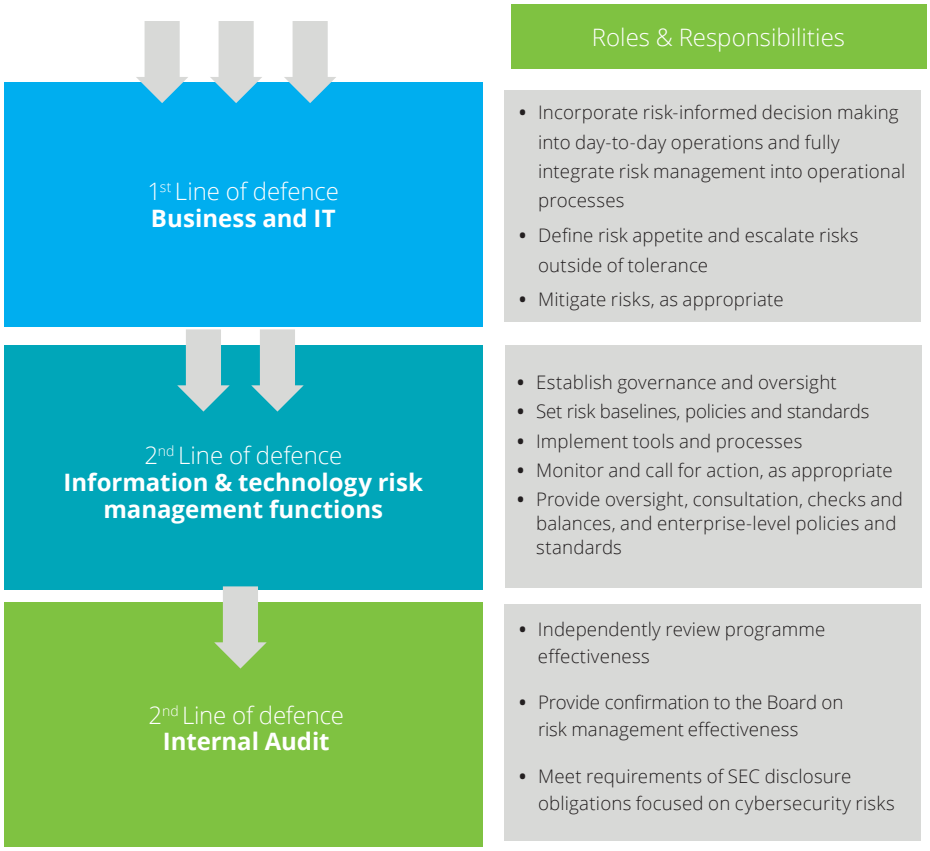
2.1 Three Lines of Defence Model

Effective risk management is the product of multiple layers of risk defence. Internal Audit should support the Board's need to understand the effectiveness of cybersecurity controls. Companies should institute and continually shore up three lines of defence:

1. **Management.** Companies that are good at managing information security risks typically assign responsibility for their security regimes to the highest levels of the company. Management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.
2. **Risk management and compliance functions.** Risk management functions facilitate and monitor the implementation of effective risk management practices by management and help risk owners in reporting adequate risk-related information up and down the company.
3. **Internal Audit.** The Internal Audit function provides objective assurance to the Board and executive management on how effectively the company assesses and manages its risks, including the manner in which the first and second lines of defence operate. It is imperative that this line of defence be at least as strong as the first two. Without a function that provides competent and objective assurance, a company faces real risks of its information privacy practices becoming inadequate or even obsolete. This is a role that Internal Audit is uniquely positioned to fill. But to do so, it must have the mandate and the resources to match.

The three lines of defence illustrated below are not unique to data privacy and security, but should be in place and operating at a robust level to deal with any critical risk to the company. For most companies , information security and privacy are critical risks because of its potential to cause financial and reputational damage.

Given recent high profile cyber attacks and data losses, and the expectations of the SEC and other regulators, it is critical for Internal Audit to understand cyber risks and be well prepared to address the questions and concerns expressed by the Audit Committee and Board.



2.2 Organisational Roles and Responsibilities for Cybersecurity

Audit Committee and Board of Directors– Overseeing a successful cybersecurity programme requires frequent and proactive engagement from the Board of directors and Audit Committee. The Audit Committee, in its capacity of overseeing risk management activities and monitoring management's policies and procedures, plays a significant strategic role in coordinating cyber risk initiatives and policies and confirming their efficacy. These responsibilities include setting expectations and accountability for management, as well as assessing the adequacy of resources, funding and focus for cybersecurity activities. The Audit Committee chair can be a particularly effective liaison with other groups in enforcing and communicating expectations regarding security and risk mitigation.

Boards are devoting increased attention and resources to responding to cybersecurity issues. Whether or not there is a dedicated risk committee on the Board, it is important to confirm that there are directors with knowledge and skills in security, IT governance and cyber risk. Given the Audit Committee's responsibility for risk oversight, it can be advantageous to recruit committee members with cybersecurity experience so that informed decisions are made about the sufficiency of the efforts overseen.

Management – All members of management should be fully aware of the company wide cyber strategy which should include plan of action and who will occupy key roles in the event of an attack or threat. Most companies have a senior management position related to information security in place so that there is a clear voice directing cyber threat prevention, remediation and recovery plans, related educational activities and the development of frameworks for effective reporting.

This position is sometimes held by a Chief Information Officer (CIO), or a Chief Security Officer (CSO) who is also responsible for physical security, but some companies may have a dedicated Chief Information Security Officer (CISO) who focuses solely on cyber threats. These executives will sometimes report directly to the Board, but in all cases, they can be an effective liaison with whom the Audit Committee and Board can communicate regarding risks and the response to attacks.

Internal Audit –The Audit Committee should confirm that the Internal Audit function regularly reviews controls pertaining to cybersecurity, is up-to-date on the latest developments and includes related issues prominently and regularly on its agenda.

External Auditor –The external auditor can often be a valuable source of information on cybersecurity issues. Many firms have practices focused on evaluating and strengthening security controls and implementing programmes for enterprise risk management. They are also qualified to provide perspectives gained through working with a wide variety of companies in diverse industries.

External Specialists – It can be helpful to seek the input of external specialists in assessing cybersecurity.

Companies can conduct annual external reviews of security and privacy programmes, including incident response, breach notification, disaster recovery and crisis communication plans. Such efforts can be commissioned and reviewed by the Board's risk committee or another designated committee to confirm that identified gaps or weaknesses are addressed.

Third-party security assessments can also provide benchmarking relative to other companies of similar size or in the same industry.

2.3 The Audit Committee's role in cybersecurity

The extent of the Audit Committee's involvement in cybersecurity issues varies significantly by company and industry. In some companies, cybersecurity risk is tasked directly to the Audit Committee, while in others, there is a separate risk committee.

Companies for which technology forms the backbone of their business often have a dedicated cyber risk committee that focuses exclusively on cybersecurity.

Regardless of the formal structure adopted, the rapid pace of technology and data growth and the attendant risks highlighted by recent security breaches demonstrate an increasing importance in understanding cybersecurity as a substantive, enterprise-wide business risk.

Audit Committees should be aware of cybersecurity trends, regulatory developments and major threats to the company, as the risks associated with intrusions can be severe and pose systemic economic and business consequences that can significantly affect shareholders.

Engaging in regular dialogue with technology-focused company leaders will help the committee better understand where attention should be concentrated. Some questions for Audit Committees to consider asking management regarding cybersecurity are:

- What is the overall company-wide cyber strategy and plan for protecting assets?
- How robust are the company's incident response and communication plans?
- What are the company's critical assets and associated risks to be secured?
- How are vulnerabilities identified?
- How are risks disclosed?
- How are critical infrastructure and regulatory requirements met?
- What controls are in place to monitor cloud and supplier networks, as well as software running on company devices, such as mobile devices?
- What digital information is leaving the company, where is it going and how is it tracked?
- Do we have trained and experienced staff who can forecast cyber risks?
- Is it known who is logging into the company's network, from where and if the information they are accessing is appropriate to their role?

2.4 Transforming Cyber Defences

Within the broader context of responsibility for risk oversight, Audit Committees are responsible for the oversight of financial reporting and disclosure and more recently cybersecurity.

Cybersecurity is a business issue as it exceeds the boundaries of IT and cyber risk needs to be managed with as much discipline as financial risk.

Both the technical nature of the threat and amount of attention cyber risk demands calls for primary Audit Committee involvement. Yet companies have acknowledged a lack of expertise on cybersecurity issues. As a result, audit committees are seeking not only education for themselves, but also an elevation of the discussion amid C-level executives.

These efforts include increasing engagement with the CIO and CISO, drawing on the expertise of the IT partner from the external audit firm, encouraging CIOs and CISOs to participate in peer-group information sharing and challenging management to produce metrics that the Audit Committee can use to evaluate cybersecurity effectiveness.

A comprehensive cybersecurity strategy and plan also requires appropriate culture and tone at the top.

These encompass an awareness of the importance of security extending from the C-suite to the professionals in each function, since breaches can occur at any level and in any department.

The CEO should make it clear that cybersecurity is a major corporate priority and should communicate that he or she is fully on Board with enforcing compliance with policies and supporting efforts to strengthen infrastructure and combat threats.

"A company's cybersecurity programme can be difficult to evaluate because Audit Committees do not know the key success factors and its indicators to measure it."

Several practices that companies are employing to enhance the Audit Committee's oversight of cybersecurity risk, leverage the recent broader strategic focus of the CISO and CIO roles:

a. **Increasing interaction with the IT department**
CIO and CISO should attend Audit Committee meetings and take the Audit Committee through one "deep dive" education session on cybersecurity issues. The Audit Committee should also continue engaging with the CIO and CISO.

b. **Sharing information with industry counterparts**
CIOs and CISOs benefit from sharing information with their industry counterparts about cyber attack patterns and cyber defence strategies. For instance, providing first-hand experience of a cyber attack to industry peers would better inform and prepare them for the prevention of similar attacks and in the process isolate a high-impact and high-likelihood risk from crippling a company.

c. **Technology experts joining the Board.**
The lack of technology expertise is an issue that has to be recognised in Boards today. With the average age of Board members exceeding 50, there is often a lack of understanding of context as a CIO is briefing the Board. It is, therefore, beneficial for the Board to have a member with significant technology experience.

d. **Engaging the expertise of the external audit firm**
External auditors employ a variety of professionals that include cybersecurity experts. They are a great resource for providing an honest perspective on the company – the knowledge of the management team and how the company is benchmarked. Some companies engage external audit firms to be "ethical hackers" without the knowledge of the CIO and/or CISO, while others choose to notify these executives ahead of time.

e. **Deploying Internal Audit**
Internal Audit plays a central role in helping the Audit Committee oversee cybersecurity. The regular assess- ments conducted by Internal Audit play an important part in providing the Audit Committee with a comprehensive appraisal of the company's strengths and weaknesses. Internal Audit should also be able to develop a road map for the future dealing with various cyber-risk issues and scenarios.

f. **Evaluating the company's cybersecurity programmes.**
A company's cybersecurity programme can be difficult to evaluate because Audit Committees do not know the key success factors and its indicators to measure it. The most important indicator is the amount of time that elapses between the hacker's penetration and the company's detection. Detection and response time are among the most important metrics that the company should track to ensure progression and effectiveness of the techniques being employed.

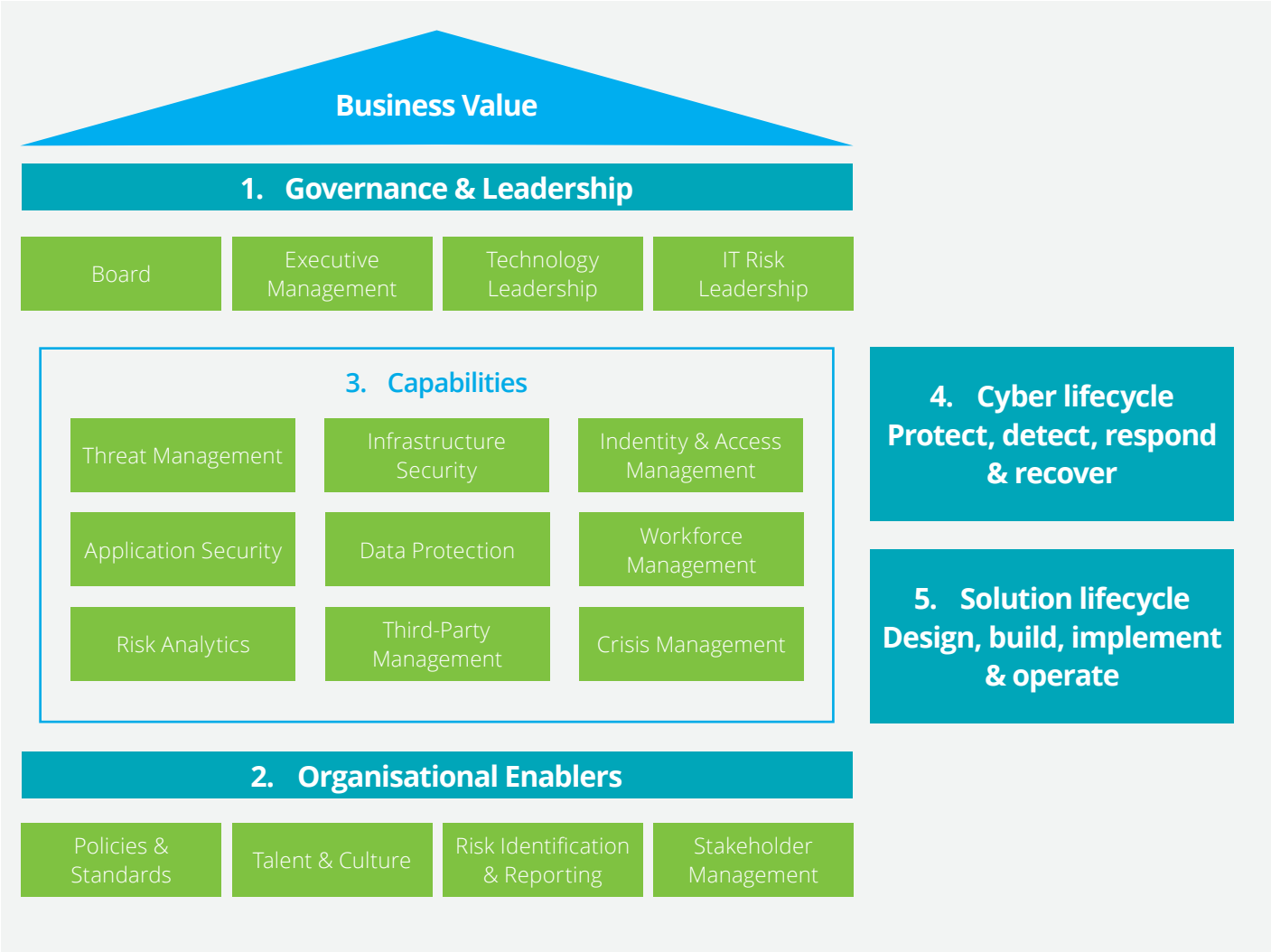
3. Framework for Cyber Risk Management

The Cyber Risk Management Framework can help focus the conversation on the Audit Committee, other members of the Board and senior management on what cybersecurity strategy and plans are in place and its possible gaps. This can potentially bridge the gap between the seemingly technical world of cybersecurity and how it translates into the governance decisions that Boards and senior executives make. It also encourages dialogue between companies in similar industries which have a shared interest in identifying and addressing vulnerabilities.

The framework's core consists of five functions :

1. Governance and leadership,
2. Organisational enablers,
3. Capabilities,
4. Cyber lifecycle and
5. Solution lifecycle

These provide a high-level, strategic view of a company's management of cybersecurity risks and examine existing cybersecurity practices, guidelines and standards.



Cybersecurity strategy and plans should take into account the past, present and future with regard to cyber risks. Consideration should be given to the percentage of the available budget required for prevention efforts, immediate response to attacks and resiliency exercises.

Throughout the past decade, most companies' cybersecurity programmes have focused on strengthening prevention capabilities based on established information assurance strategy: defence in-depth. This approach advocates a multi-layered approach to deploying security controls with the intent of providing redundancy in the event that a security control fails or a vulnerability is successfully exploited in one of the layers.

To be effective and well balanced, a cyber defence must have three key characteristics: secure, vigilant and resilient.

1. **Secure:** Being secure means focusing protection around the risk-sensitive assets at the heart of a company's mission.
2. **Vigilant:** Being vigilant means establishing threat awareness throughout the company and developing the capacity to detect patterns of behaviour that may indicate, or even predict, compromise of critical assets.
3. **Resilient:** Being resilient means having the capacity to rapidly contain the damage and mobilise the diverse resources needed to minimise impact – including direct costs and business disruption, as well as reputation and brand damage.

In summary, the model below has 3 objectives – secure, vigilant and resilient – woven together with 5 design principles of:

a. Incorporating security in the core design

b. Applying threat intelligence in the core design

c. Sharing of intel and information among security practitioners

d. Automating processes to address the scarcity of skilled resources

e. Enabling the power of combating crime together

Once the cyber risks have been identified, the 3 objectives within the cybersecurity plan can be used to map the programme and governance to mitigate or address those risks.

3.1 Cyber Risk Appetite and Tolerance

Risk appetite and tolerance must be a high priority on the Board agenda. It is a core consideration in an enterprise risk management approach. Risk appetite can be defined as 'the amount and type of risk that a company is willing to take in order to meet its strategic objectives.'

Every company possess different risk appetites depending on their sector, culture and objectives. A range of appetites exist for a diverse portfolio of risks, which may change over time according to the risk portfolio.

While risk appetite is interpreted differently, there is a general consensus that effective communication of an appropriate risk appetite statement can help companies achieve their goals and sustain their operations.

Management should develop an understanding of cyber criminals, their objectives and how attacks might happen. The following questions can be used to develop an understanding:

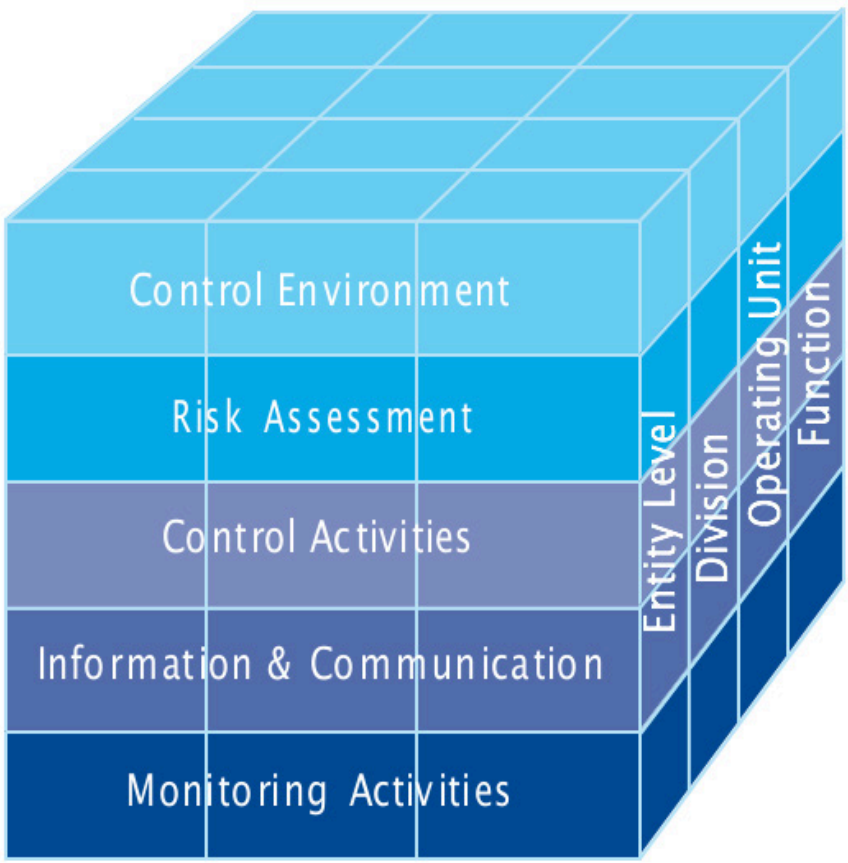
1. Who might attack?
2. What are they after and what business risks do we need to mitigate?
3. What is the intruder's arsenal?

3.2 A representative Internal Audit Plan to address cyber risk

It is imperative that Internal Audit takes a leading role in determining whether a systematic and disciplined approach exists to evaluate and strengthen the effectiveness of cyber risk management. It should also determine if appropriate cybersecurity capabilities (people, process and technology) are in place to protect against cyber threats.

In developing the Internal Audit plan for cybersecurity, the COSO Framework should be used as the framework for guiding the Internal Audit's approach. Managing cyber risk through a COSO lens enables the Board and senior executives to better communicate their business objectives, their definition of critical information systems and related risk tolerance levels. This enables others within the company, including IT personnel, to perform a detailed cyber risk analysis by evaluating the information systems that are most likely to be targeted by attackers, likely methods of attack and points of intended exploitation. In turn, appropriate control activities can be established to address such risks. Through the COSO cube, companies may view their cyber risk profile through the components of internal control to manage cyber risks in a secure, vigilant, resilient manner. For example

Figure 2 – The COSO Cube



a. **Control Environment** — Does the Board understand the company's cyber risk profile and are they informed of how the company is managing the evolving cyber risks management faces?

b. **Risk Assessment** — Has the company and its critical stakeholders evaluated its operations, reporting and compliance objectives and gathered information to understand how cyber risk could impact such objectives?

c. **Control Activities** — Has the company developed control activities, including general control activities over technology that enable the company to manage cyber risk within the acceptable level of tolerance to the company? Have such control activities been deployed through formalised policies and procedures?

d. **Information and Communication** — Has the company identified information requirements to manage internal control over cyber risk? Has the company defined internal and external communication channels and protocols that support the functioning of internal control? How will the company respond to, manage and communicate a cyber risk event?

e. **Monitoring Activities** — How will the company select, develop and perform evaluations to ascertain the design and operating effectiveness of internal controls that address cyber risks? When deficiencies are identified, how are these deficiencies communicated and prioritised for corrective action? What is the company doing to monitor their cyber risk profile?

A cybersecurity assessment can drive a risk-based IT Internal Audit plan and audit frequency should correspond to the level of risk identified and applicable regulatory requirements/expectations.

The following table illustrates the detailed cyber risk programme and governance derived from the three key characteristics (secure, vigilant and resilient) linked to the Internal Audit plan each year to address the cyber risks. Another approach is to allow some coverage of each area (Secure, Vigilant and Resilient) in each year.

	2015	2016	2017
Secure	**Cybersecurity risk and compliance management** • Compliance monitoring • Issue and corrective action planning • Regulatory and exam management • Risk and compliance assessment and management • Integrated requirements and control framework	**Secure development life cycle** • Secure build and testing • Secure coding guidelines • Application role design/access • Security design/architecture • Security/risk requirements	**Security programme and talent management** • Security direction and strategy • Security budget and finance management • Policy and standards management • Exception management • Talent strategy
	• Evaluation and selection • Contrast and service initiation • Ongoing monitoring • Service termination	• Information and asset classification, and inventory • Information records management • Physical and environment security controls • Physical media handling	• Account provisioning • Privileged user management • Access certification • Access management and governance

Vigilant	**Threat and vulnerability management**
	• Incident response and forensics
	• Application security testing
	• Threat modelling and intelligence
	• Security event monitoring and logging
	• Penetration testing
	• Vulnerability management
		Data management and protection
		• Data classification and inventory
		• Breach notification and management
		• Data loss prevention
		• Data security strategy
		• Data encryption and obfuscation
		• Records and mobile device management
			Risk analytics
			• Information gathering and analysis around:
			  ◦ User, account, entity
			  ◦ Events/incidents
			  ◦ Fraud and anti-money laundering
			  ◦ Operational loss

Resilient	**Crisis management and resiliency** • Recover strategy, plans and procedures • Testing and exercising • Business impact analysis • Business continuity planning • Disaster recovery planning	**Security operations** • Change management • Configuration management • Network defence • Security operations management • Security architecture	**Security awareness and training** • Security training • Security awareness • Third-party responsibilities
	SOX (financially relevant systems only)	**Penetration and vulnerability testing**	**BCP/DRP testing**

4. Looking Ahead

As recently as five years ago, it was rare for a Board of directors to be closely involved in managing cybersecurity risks, but rapid advancements in technology, coupled with a corresponding increase in the sophistication of cyber criminals and cyber legislation, have made it essential for the Board and Audit Committee to be informed and proactive. New technologies continue to shape the physical and virtual borders of companies, which must frequently review and quickly adapt policies to address emerging issues.

Cybersecurity specialists are developing increasingly sophisticated approaches for preventing, detecting and responding to security breaches, but no single solution can address all the evolving challenges associated with cyber threats. It remains important to apply prudent and adaptable controls to respond to changes in the threat landscape and to have strong response and resiliency plans in place in the event of an attack.

Increasingly, cybersecurity is becoming a top-of-mind issue for most CEOs and Boards and they are becoming more pre-emptive in evaluating cybersecurity risk exposure as an enterprise-wide risk-management issue, not limiting it to an IT concern.

For more information please contact:

Southern Africa

Navin Sing
Managing Director:
Risk Advisory Africa
Mobile: +27 83 304 4225
Email:navising@deloitte.co.za

Derek Schraader
Risk Advisory Africa Leader:
Cyber Risk Services
Mobile: +27 79 499 9046
Email:dschraader@deloitte.co.za

Dean Chivers
Risk Advisory Africa Leader:
Governance, Regulatory & Risk
Mobile: +27 82 415 8253
Email: dechivers@deloitte.co.zaza

Rushdi Solomons
Risk Advisory Africa Leader:
Internal Audit
Mobile: +27 74 141 4444
Email: rsolomons@deloitte.co.za

Central Africa

Tricha Simon
Risk Advisory Regional Leader:
Central Africa
Mobile: +263 772 234 932
Email:tricsimon@deloitte.com

Rodney Dean
Director: Risk Advisory Central Africa
Mobile: +263 772 263 016
Email:rdean@deloitte.co.zw

West Africa

Anthony Olukoju
Risk Advisory Regional Leader:
West Africa
Mobile: +234 805 209 0501
Email:aolukoju@deloitte.com.ng

Temitope Aladenusi
Director: Risk Advisory West Africa
Mobile: +234 805 901 6630
Email:taladenusi@deloitte.com.ng

East Africa

Julie Nyangaya
Risk Advisory Regional Leader:
East Africa
Mobile: +254 720 111 888
Email:jnyangaya@deloitte.co.ke

William Oelofse
Director: Risk Advisory East Africa
Mobile: +254 71 785 0555
Email:woelofse@deloitte.com

Deloitte.

Designed and produced by Creative Services at Deloitte, Johannesburg. (000000/Ame)