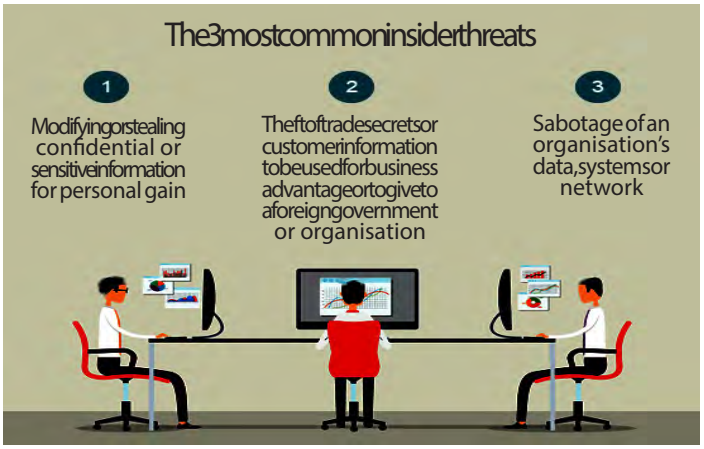
INFORMATION TECHNOLOGY (IT) SECURITY GOVERNANCE AND THE INTERNAL AUDITOR'S ROLE

CPA Abdhallah Mambo Dallu, Internal Auditor, Umma University

Introduction

The threat to technology-based information assets is higher now than it has been in the past. As technology has advanced, so too have the tools and methods employed by those who seek to gain unauthorised access to data or disrupt business processes. Attacks on any organisation are inevitable.

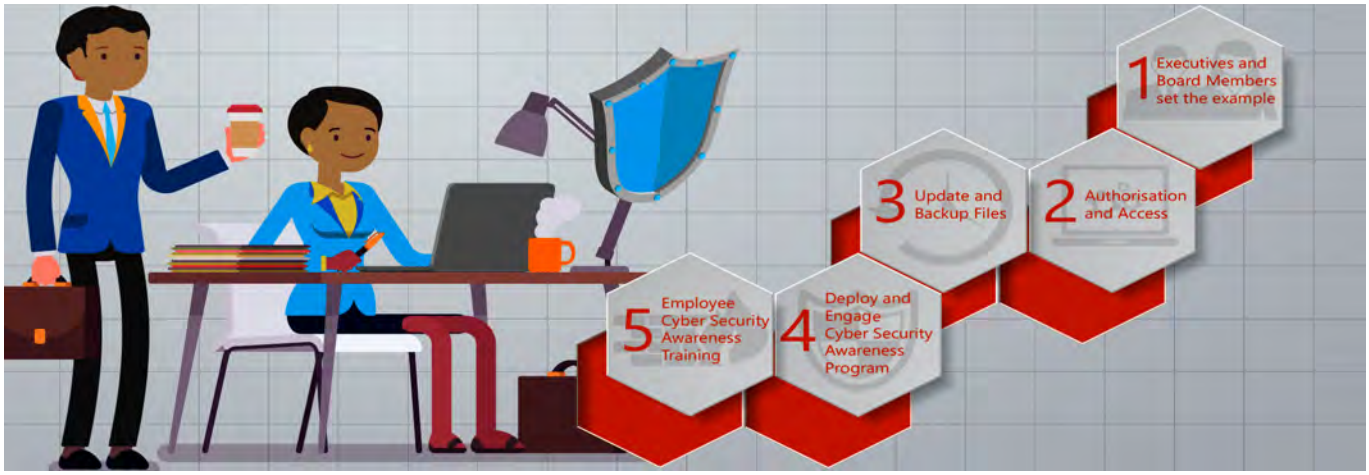


But the sophistication and persistence of those attacks depend on the attractiveness of that organisation as a target, primarily its role and assets. Today, threats originating from misguided individuals have been replaced by highly skilled international organised crime groups or foreign nation states that have the skills, personnel and tools to conduct sophisticated covert cyber espionage attacks.

In today's era of lightning-quick social media sharing, brand protection has become even more important for technology, media and communications (TMC) companies. In the face of social media and mobile applications use by customers and employees and the relentless tide of cyber threats, including growing public disclosures of data leaks and breaches, many TMC companies are beginning to re-evaluate how they interact with other organisations and how they safeguard against breaches. Without question, loss or theft of any type of high-value data can have lasting, negative effects on an organisation from both operational and brand perspectives. Everything negative that happens to a company and becomes public can damage its brand and cyber breaches and loss of internet protocol are some of the fastest ways for this damage to occur.

5 steps to increase a company's cyber security awareness

Below is a list of 5 steps an organisation can take towards better cybersecurity practices and increased awareness. It is important to keep in mind that cyber security is an ongoing process that starts with awareness.



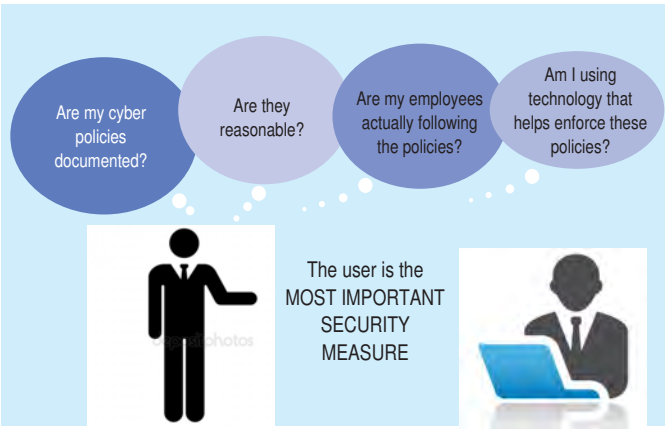
What is cyber security?

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attacks, damage or unauthorised access. The term "cyber security" refers to business function and technology tools used to protect information assets. Data is increasingly digitised and the internet is being used to save, access and retrieve vital information. Protecting this information is no longer a priority but has become a necessity for most companies and government agencies around the world.

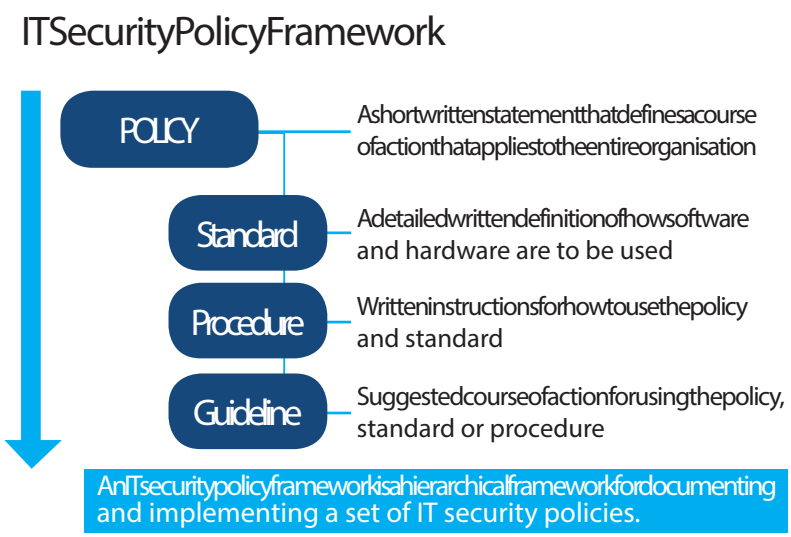
Reliance on security technology

We live in a world driven by technology. It is not uncommon for companies to first turn to technical security solutions without addressing how those solutions are going to be implemented, maintained and managed on a day-to-day basis. Too often we see organisations implement technical security safeguards, such as firewalls or intrusion detection, but fail to implement proper security policies or procedures. As a result weak practices persist that undermine security and expose assets to significant risk. The following are just a few examples of such practices:

- Non-existent security policies or procedures.
- Outdated and/or ignored security policies, where they do exist.
- Poor awareness of security practices at all levels.
- Lack of effective network zoning, or compliance thereof.
- Inadequate hardening and patching.
- Poor access control practices such as uncontrolled group passwords, shared accounts, proliferated privileges, shared root access, absence of an authorisation process (except at a low operational level).
- Lack of security compliance audits and reviews.
- Absence of an authority figure for decisions affecting the security and integrity of infrastructure and information assets.

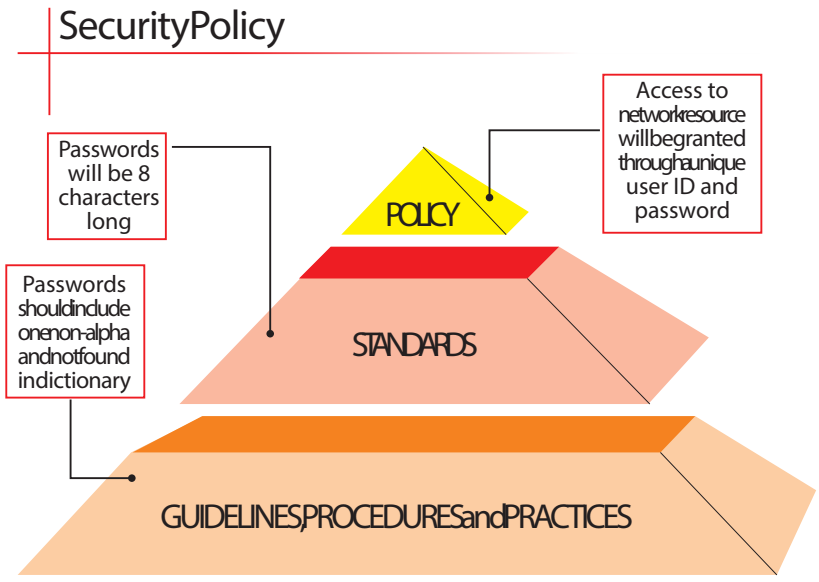


A cyber security policy is a formal set of rules by which those people who are given access to company technology and information assets must abide. The cyber security policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.



Some policies can have multiple guidelines, which are recommendations as to how the policies can be implemented. Finally, information security management, administrators and engineers create procedures from the standards and guidelines that follow the policies.

The end result is an enterprise that feels secure because it has invested in security solutions, but has so many inherent vulnerabilities that little meaningful security protection is achieved. In this case, a dangerous sense of false confidence exists, but the organisation remains extremely vulnerable to attacks, with intruders exploiting those weak practices to circumvent technical security solutions and gain control of systems. This is not theoretical; it is a common scenario that has been observed as a root cause in many well publicised and successful attacks on major corporations and government agencies.



The role of IT security governance

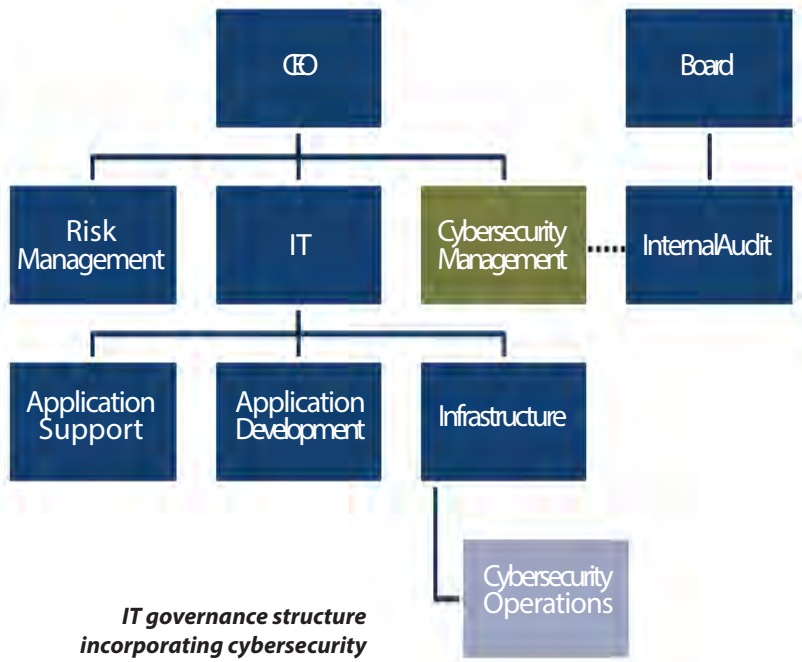
Security governance is the glue that binds together all the core elements of cyber defense and effective risk management. Without it, dangers persist and the resulting compromise of assets is inevitable. Moreover, senior leadership is unaware of their organisation's risk exposure, for which they will ultimately be held accountable.

Security cannot exist in a vacuum and must be part of a larger risk management strategy, driven by the organisation's business goals, objectives and values. Organisations must be aware of their risk tolerance threshold, or "level of acceptable risk." This threshold may vary by asset grouping. For example, an organisation may tolerate a certain amount of risk when the impact is considered low, but may be very risk averse regarding anything that might adversely impact its reputation.

Governance is the mechanism by which those risk-related values are reflected in direction and judgement that shape business plans, information architecture, security policies and procedures, as well as operational practices. However, providing direction without having any means to ensure that it is followed is meaningless. Thus, compliance is the critical feedback loop in security governance. It ensures that everyone is working according to plan, as a team, to deliver business activities and ensure the protection of assets within the context of risk management and security strategy and direction. Where that is not possible, it ensures that variances that result in risk exposures are made known at the leadership level, so that they can either decide to accept these risks, or provide mitigating direction and the resources necessary to address them.

Executive responsibility for IT security governance

In the past, security was often left to managers and administrators at the technical and operational levels. However, as both technology and the nature of threats

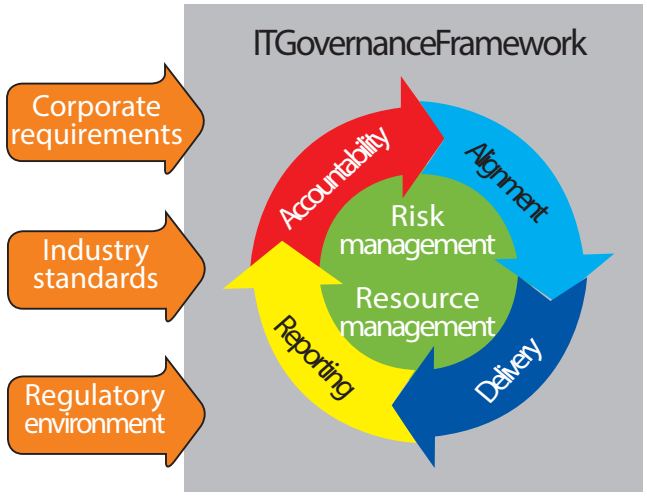


IT governance structure incorporating cybersecurity

have increased in scale and complexity, the ultimate responsibility for protecting an organisation's mission and assets is now being been laid at the doorstep of senior management.

It is interesting to note a potential divide in the perspectives of CEOs and line managers. While we have seen senior management in organisations insist on the creation of security policies and procedures in response to the industry recognition of increased threat and the importance of security best practices, we have also seen instances where adequate policies and procedures exist, but have not been implemented consistently (or at all) at the operational level.

The end result is that senior leaders are confident that their responsibility for diligence has been satisfied and



that risks are being managed effectively. Yet the reverse is often true, and they are unaware that their organisation remains extremely vulnerable through endemic failures in the governance process. Ultimately, critical risks persist, where senior management may have been uninformed, but is still held accountable. This false sense of security is extremely dangerous for an organisation and results in an uncontrolled state of risk and liability.

To meet modern security challenges, organisations must consistently apply effective risk management practices at all levels. Risks must be made visible to senior management. These executives must play a key role in either accepting those risks or directing activities and enabling resources to mitigate them to acceptable levels from a business, legal, legislative and regulatory standpoint. To do that, senior management must have visibility regarding responsibility and accountability in each instance.

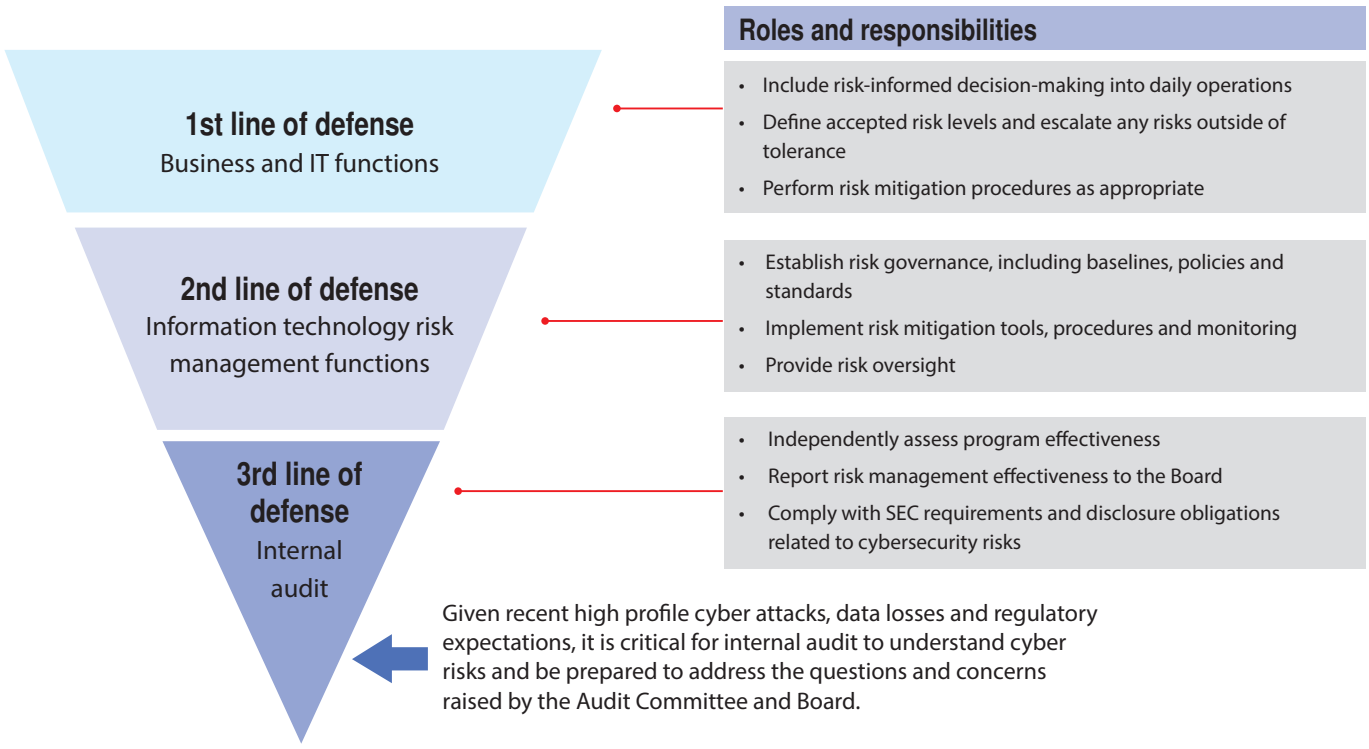
Defining internal audit's role in cyber security

Effective risk management is the product of multiple layers of risk defense (See diagram overleaf). Internal audit should support the board in understanding the effectiveness of cyber security controls.

These three lines of defense for cyber security risks can be used as the primary means to demonstrate and structure roles, responsibilities and accountabilities for decision-making, risks and controls to achieve effective governance risk management and assurance.

Business operations perform day-to-day risk management activities such as risk identification and risk assessment of IT risk. They provide risk responses by defining and implementing controls to mitigate key IT risks and reporting on progress. An established risk and control environment helps accomplish this.

Risk management is the process of drafting and implementing policies and procedures, ensuring that existing procedures are kept up to date, responding to new strategic priorities and risks, monitoring to ensure compliance with the updated policies and



providing surveillance over the effectiveness of the compliance controls embedded in the business.

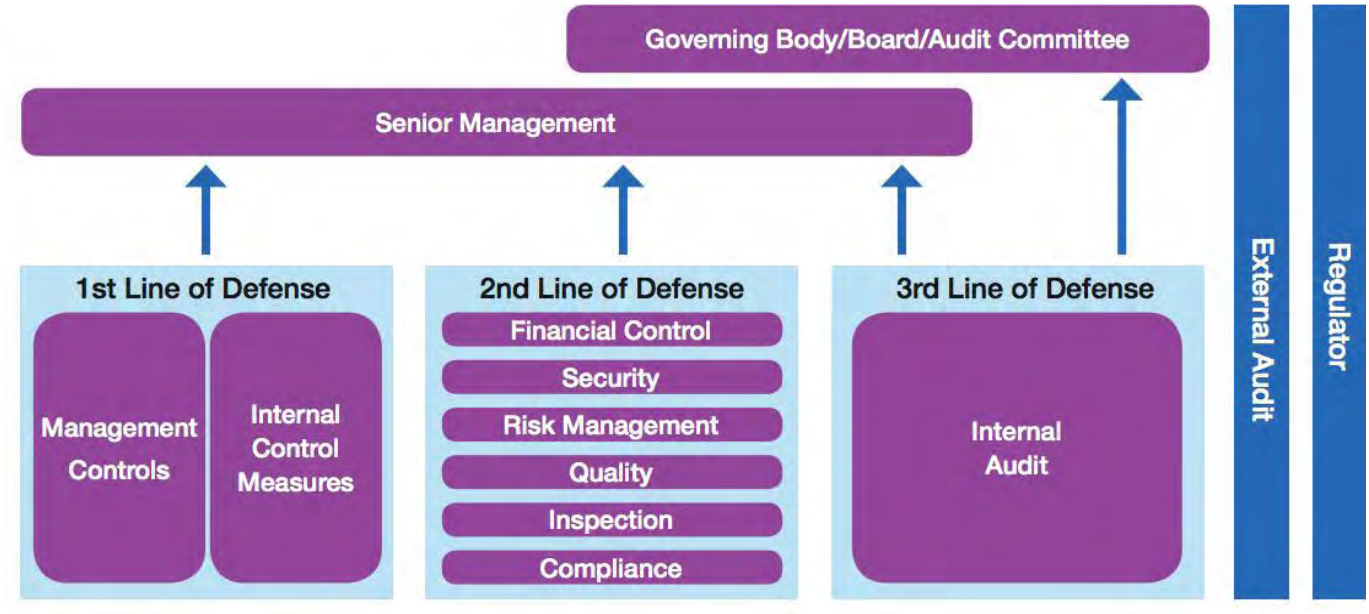
As the 3rd line of defense, what steps can internal audit take?

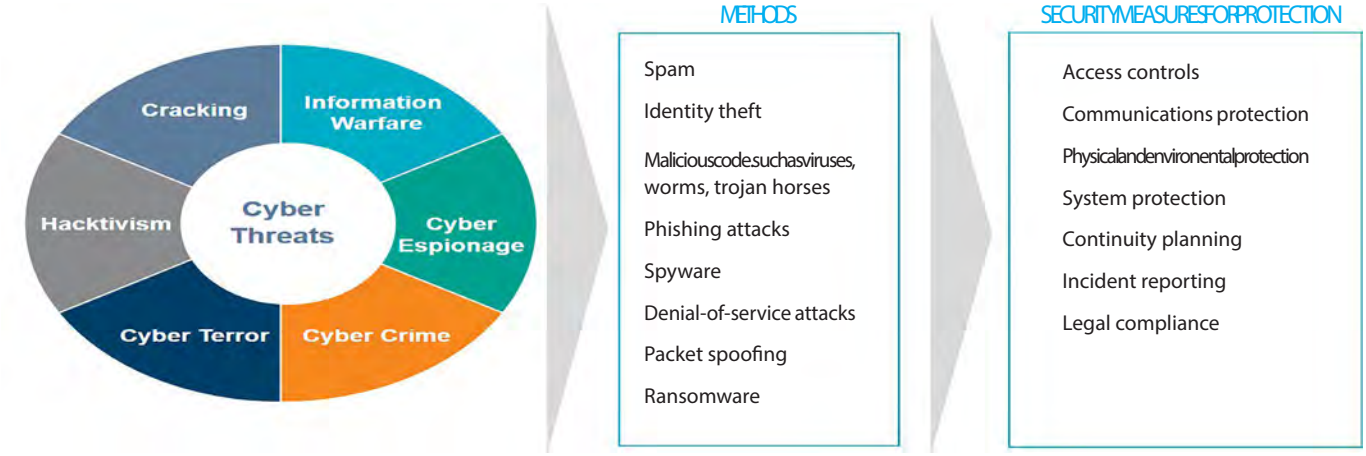
1) Work with management and the board of directors to develop a cyber-security strategy and policy.

2) Identify and act on opportunities to improve the organisation's ability to identify, assess and mitigate cyber security risk to an acceptable level.

3) Recognise that cyber security risk is not only external; assess and mitigate potential threats that could result from the actions of an employee or business partner.

4) Leverage relationships with the audit committee and board to heighten awareness and knowledge on cyber threats, and ensure that the board remains highly engaged with cyber security matters and up to date on the changing nature of cyber security risk.





5) Ensure that cyber security risk is integrated formally into the audit plan.

6) Develop and keep current an understanding of how emerging technologies and trends are affecting the company and its cyber security risk profile.

7) Evaluate the organisation's cyber security program against the NIST Cyber Security Framework, recognising that because the framework does not reach down to the control level, the cyber security program may require additional evaluations of ISO 27001 and 27002.

8) Seek out opportunities to communicate to management that, with regard to cyber security, the strongest preventive capability requires a combination of human and technology security; a complementary blend of education, awareness, vigilance and technology tools.

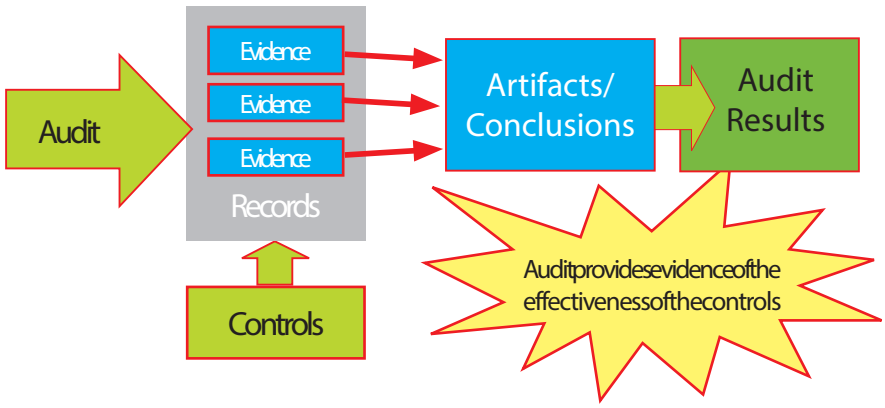
9) Emphasise that cyber security monitoring and cyber incident response should be a top management priority; a clear escalation protocol can help make the case for; and sustain, this priority.

10) Address any IT/audit staffing and resource shortages as well as a lack of supporting technology/tools, either of which can impede efforts to manage cyber security risk.

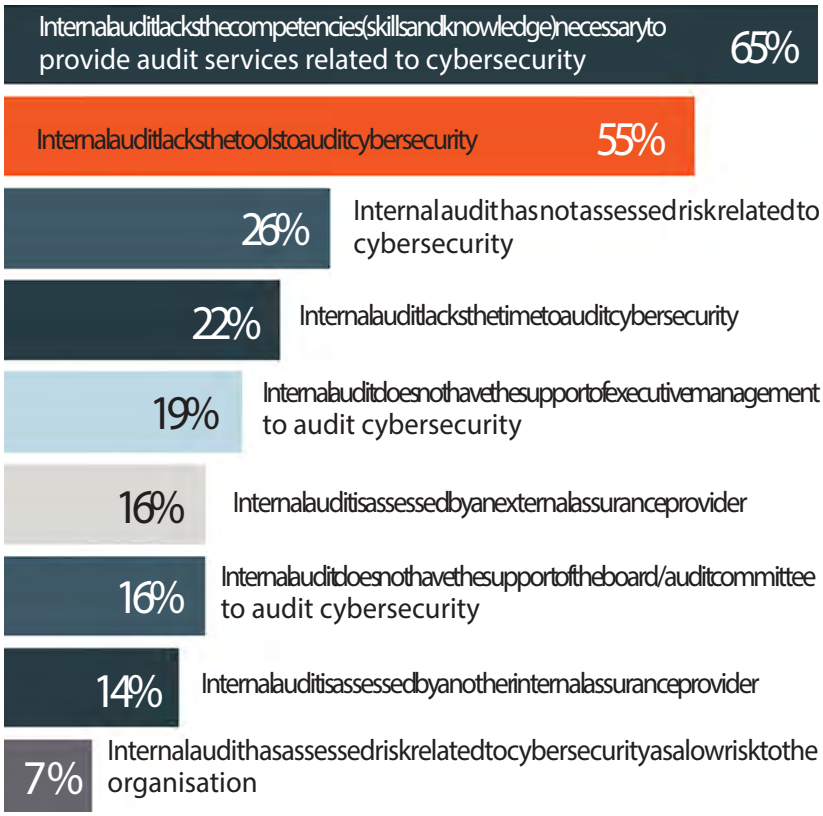
Internal audit focus areas

Organisations must constantly monitor cyber security practices, policies and plans. This is where internal audit plays a crucial role. Once cyber security plans are created, organisations should enlist internal audit to do what it does best – test for effectiveness and efficiency of controls and protocols and provide the board and management with assurance about those protections. There are four areas where internal audit focuses on cyber security:

1) Provide assurance over readiness and response. According to The IIA Audit Executive Center's 2016 North American Pulse of Internal Audit report, just one in four respondents who reported having a business-continuity plan said it provided "clear, specific procedures for responding to a cyber-attack." What's more, 17 percent reported their plans had no such procedures at all. This is the kind of data that should keep the C-suite and board up at night.



Reasons why internal audit departments do not audit cybersecurity



Source Global Perspectives and Insights

Internal audit can help organisations review and test cyber security, business-continuity and disaster-recovery plans. The potential for reputational harm that poorly managed business disruptions create is significant, and it is far better to find faults through mock exercises than in a real-life scenario.

2) Communicate to the board and executive management the level of risk to the organisation and efforts to address such risks. Understanding how much of a risk cyber-attacks pose and what is being done to mitigate them is essential to managing the risk.

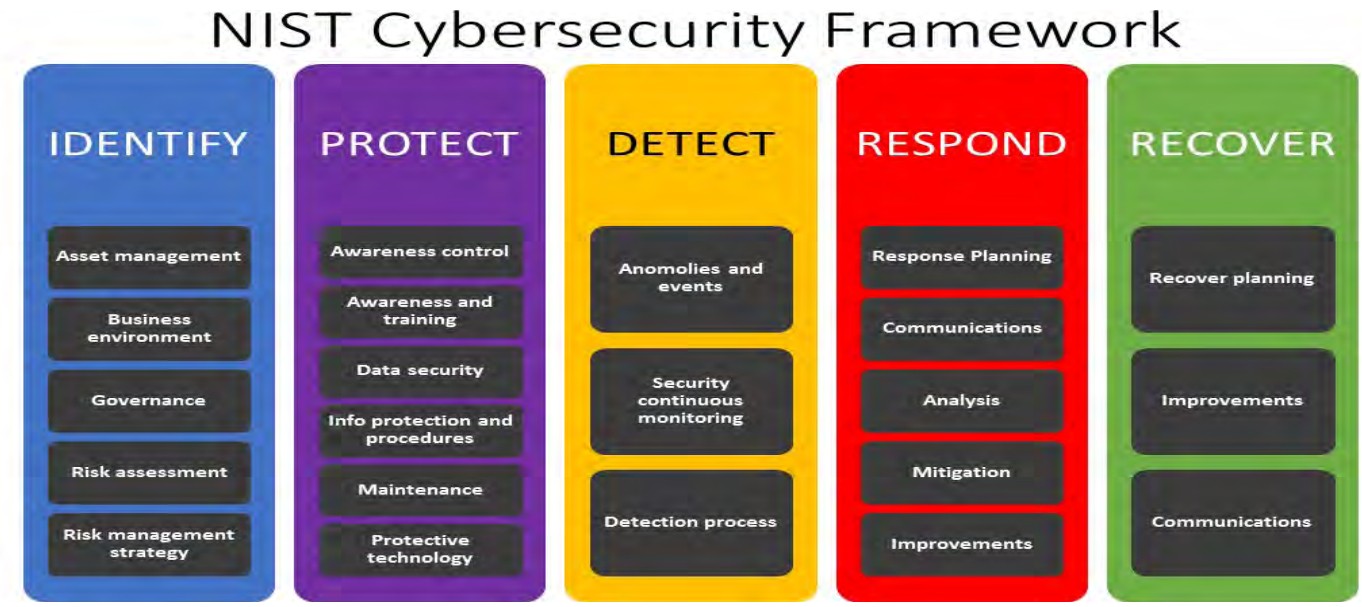
3) Work collaboratively with IT and other parties to build effective defenses and responses. Cyber risk is a business risk, not just an IT risk. Too often, it is magnified, modified and mystified by being supported solely by IT systems. Building strong, collaborative relationships between internal audit and IT will help ensure mitigation efforts and responses are effective.

4) Ensure communication and coordination. This may be the most valuable benefit internal audit can offer. Because a well-resourced and effective internal audit function has a broad perspective about organisational risks, it is in an ideal position to promote communication and coordination about cyber risks across the organisation.

Turf battles over who "owns" the cyber security risk are counterproductive and weaken the

Action items for Risk and Internal Audit

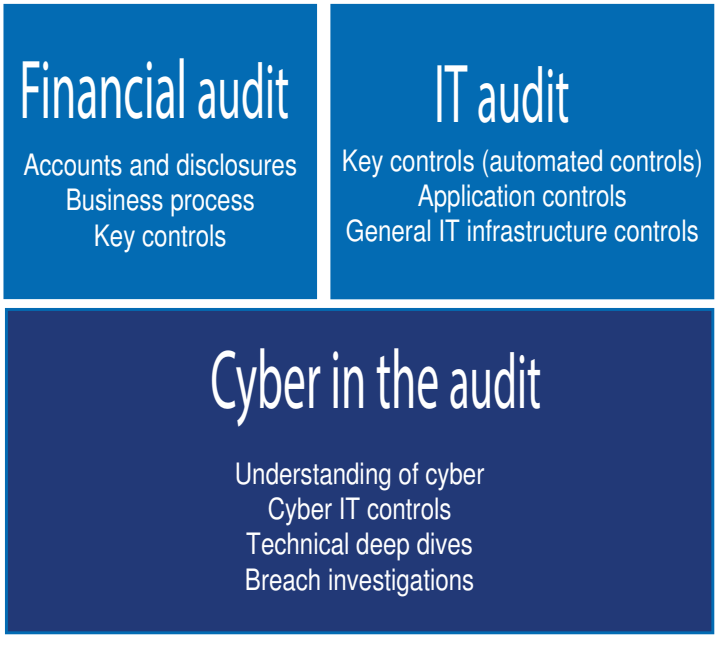
Given internal audit's key role in effective cyber-security, there are ten actions that IA can take



organisation's cyber security efforts. A unified effort where roles are clearly defined creates the best conditions for deterring cyber-attacks, executing business-continuity plans when cyber breaches occur and building cyber-resilient organisations.

Building effective cyber-resilience plans

Despite its complexity and formidable challenge, effective cyber security is within the reach of most organisations. By using the "Four Rs" – resist, react, recover and re-evaluate – organisations can build effective cyber-resilience plans.



(a) Resist

The recent WannaCry cyber-attack provided a shocking wakeup call that even the most basic phishing attacks still can have devastating impacts. The ransom ware virus, which claimed more than 200,000 victims in 150 countries, could have been successfully rebuffed with basic cyber security measures.

- Instruct employees on defensive cyber etiquette, and enlist internal audit to test for compliance.
- Take advantage of available frameworks and guidance, such as NIST's Framework for Improving Critical Infrastructure Cyber security or the Nymity Privacy Management Accountability Framework.
- Understand the process and importance of software and data updates, and enlist internal audit to test for compliance.
- Test IT controls regularly.

(b) React

When a cyber-breach occurs, a crisis-management plan is an essential component of effective business-continuity management.

- Immediately assess the scope of the breach and method for addressing it.
- Ensure that each part of the organisation understands and carries out its role in crisis-management and business-continuity plans.
- Communicate with transparency and with a single voice.

- Internal audit should monitor and assess the response.

(c) Recover

Strong business-continuity planning and proper execution of those plans can help an organisation quickly recover from a cyber-breach.

- Identify necessary steps to safely and quickly restore business operations.
- Ensure frequent internal communications throughout the recovery.

(d) Re-evaluate

Analysis of processes, procedures and their execution is essential once the crisis has passed and operations are restored and secure.

- Look for ways to improve the crisis response.
- Determine training/retraining needs.
- Consider what role, if any, corporate culture played in contributing to the breach.
- Review data and security privacy policies.
- Consider what role, if any, third-party risks played in contributing to the breach.

Successful cyber security requires a unified and coordinated effort. Management and boards can manage the effort effectively if they understand the scope of the challenge, commit the necessary resources to develop and execute an informed strategy, support internal audit's independent oversight and review and nurture open communications and cooperation among the key players.

Conclusion

Most people think that IT Security and Internal Audit are two different fields within the solid structure of a company, so they aren't related and work in a totally different mechanism. However, it turns out that internal audit can actually play an important part in strengthening cyber security and the accountant doesn't need to understand the whole technical terms at all.

With the increasing threats in cyber security and more breaches within the past years to not only international companies but the local companies as well, the internal audit department must start to see the possible opportunities of how their expertise can be used in the company's risk management and assessment. When the auditor understands the whole concept of the business, the objectives, the strategies, the information the company produces, and what matters the most for them, the auditor can help in strengthening the most important aspects and elements of the structure, resulting in better and stronger cyber security.

Internal audit needs to "rebrand" itself as a strategic partner that delivers more value than what stakeholders would traditionally expect, particularly in emerging risk areas like technology advancements, cybersecurity and privacy threats and more.

David Toh
PwC Singapore's Internal Audit Leader