KPMG

Cyber Academy

EXPAND YOUR HORIZONS

Cyber Security

It is no longer news that we are in the digital age; advancement in digital technology is enabling business innovations and agility across the world.

The business ecosystem is rapidly evolving in response to the convergence of digital. However, the digital evolution has introduced a new dimension to enterprise risk: *The Cyber Risk*. However, cyber risk is not conventional, neither are the threat actors.

Many businesses often find that it is not the technology that led to a security incident. It is the fact that employees were not trained or made aware of the need to protect their company's data and how to do it. High profile cases of data loss and increasing cyber attacks are making it more important than ever to get the basics right.

Many organisations often race to implement new technologies in an effort to solve a basic business problem but leave their people out of the loop. Once people understand the importance of controls and have the power to act, they can transform from being a risk to the first line of defence. KPMG's Cyber Academy has been created as a leading-edge centre for bespoke cyber learning. The academy offers a blended framework of e-learning, virtual classrooms and workshop-based face-to-face training.

The challenge for organisations is that cyber threats are increasingly complex, cross-border in nature, fast moving and difficult to keep pace with. Moreover, most issues playing out in public often don't reflect what people see day to day.

We can help you define the security role profiles for your organisation as well as build cyber competence across various levels. We can do this by reviewing your processes to direct and guide people on what cyber competency development .

WHAT'S ON YOUR MIND?

How do I ensure that my employees have sufficient guidance to help protect themselves and the organisation?

How do I make people aware of the *dos* and *don'ts* of Information Security? How do I identify the skills gaps in my people and ensure the required skill sets are obtained?

Can I demonstrate to regulators, stakeholders, shareholders, customers, business partners and auditors that sufficient knowledge, training and awareness have been delivered?

How KPMG can help you turn risk to advantage?

1 AWARENESS PROGRAMMES

We can help you deliver awareness training and communication throughout your business by delivering distinctive, tailored and measurable Information Security Training and Awareness campaigns.

2 TECHNICAL TRAINING

We can provide a tailored technical cyber security curriculum to support your IT/ IS staff development. Training can include core areas such as the ISO27001 Information Security Management System. We also deliver specialist training in specific areas such as *Threat Management, Vulnerability Management, Identity and Access Management, Privacy, Security Testing, Monitoring and Analytics*. We can assist with the needed capacity development of IT people who wish to transition to Information Security, and apply best practices to deliver the different elements of the cyber security framework.

3 CAPABILITY FRAMEWORK

We can help you assess the level of skills and capabilities you require to run an effective information security function. We do this by first building your current state and then build a suite of assessment tools based on established, refreshed competencies and additional requirements for roles – wrapped in what we define as a Cyber Capability Framework. The tools will enable assessment of the skill levels within teams and organisations, the subsequent gap analysis, and the development of recommendations to close these gaps.

Targeted Training

Audience classification for learning interventions

Our Offering

C-suite	A phased approach to give board members and top management a clear insight to understand cyber risk and what it means for their organisation. To support boards and top management in answering key questions and defining the organisation's future stance in dealing with emerging threats.
Cyber Specialists	Next are your information security professionals. Cyber defence, vulnerability managers, pen testers, risk, controls and compliance teams. The training is specialised and targeted to expertise in these roles.
IT Professionals	Following the specialists are key IT roles. People who have a huge impact on security but are not necessarily career security professionals. Training is varied and needs to be embedded at a specialised level.
End Users	Finally, we have those who use the systems but are not accountable for security. Training is focused on influencing behaviour and increasing awareness around the value of, and threats to an individual's and organisation's information.

Potential benefits to you

- Reduced risk of data loss or security incident through employee negligence or error.
- Improved culture and behaviours with employees more proactively engaging with the security team.
- Knowledge of industry good practice approaches in delivering highly successful training and awareness programmes, so that you have the confidence that everyone with access to systems and data is being trained in the most important areas.

How we have helped others

Top players in the FS & Insurance Industry in various Cyber Threat and Vulnerability Management courses.

We have delivered customized training courses in the following areas:

- ✓ The Evolving Threat Landscape
- ✓ Threats Identification and Classification
- ✓ Vulnerability Assessment and Classification
- ✓ Introduction to Vulnerability Scanning (Practical labs)
- ✓ Vulnerability Scanning (using Nessus, Qualys/Burp Suite, etc)
- ✓ Vulnerability Exploitation (using Metasploit)
- ✓ Vulnerability Remediation/Infrastructure Hardening (Network, Operating System, databases and web applications)
- ✓ Integrating Threat and Vulnerability Management with Enterprise Risk Management and other existing processes
- ✓ Etc.

We have also helped organizations with general awareness and technical sessions on regulatory standards such as PCI DSS, ISO 27001 (ISMS) and ISO 22301 (BCMS).

We believe cyber security should be about what you can do – not what you can't. And if adequately managed, cyber risk should be an enabler of digital innovation.

Why KPMG?

INDEPENDENT

KPMG member firms technical strategies and recommendations are based on what is fit and appropriate for your business.

COLLABORATIVE

KPMG brings together leading organisations to discuss emerging issues and the solutions which work in an ever-increasing cyber threat landscape.

TRUSTED

KPMG professionals have the qualifications and hands-on experience from several cyber security engagements for leading organisations.

GLOBAL, LOCAL

We have over 2,000 security practitioners globally, giving member firms the ability to orchestrate and deliver to consistently high standards worldwide.

Contact us

Joseph Tegbe
Partner and Head , Technology Advisory
KPMG in Nigeria
T: +234 803 402 0989
E: joseph.tegbe@ng.kpmg.com

John Anyanwu
Associate Director, Technology Advisory
KPMG in Nigeria
T: +234 803 975 4061
E: john.anyanwu@ng.kpmg.com

Samuel Asiyanbola
Manager, Technology Advisory
KPMG in Nigeria
T:+234 802 501 3893
E: Samuel.asinyanbola@ng.kpmg.com

Kpmg.com/ng/socialmedia