Cybersecurity Leadership Masterclass
Duration: Two-days

The pervasive nature of cyberspace, the Internet and ICT systems brings substantial benefits, particularly in developing countries. Integrating ICTs into daily life has propelled the growth of the information society and digital economy. Critical services like water and electricity, along with most businesses, organizations, and individuals, now rely on ICTs. These technologies and new network-based services provide significant advantages, especially for developing nations. Applications such as e-government, e-commerce, e-education, e-health, and e-environment are essential for development, efficiently delivering a wide range of basic services.

However, these systems are inherently vulnerable to new and serious threats, attracting geopolitical adversaries and criminals. Although technology enhances variety and convenience in our lives, it also increases opportunities for cybercriminals. Both international and domestic cybercriminals view businesses and private individuals as prime targets for various cybercrimes. This 'digital paradox' implies that while governments and organizations can now provide more services rapidly, cybercrime has emerged as a significant opposing force, limiting this potential.

Cybersecurity is no longer a niche concern confined to IT departments; it is a strategic imperative that affects all aspects of governance and service delivery. The threats we face are multifaceted and increasingly sophisticated. Cybercriminals, hacktivists, nation-state actors, and insider threats continually develop new techniques to exploit vulnerabilities, disrupt services, and steal sensitive information. These actors employ a wide array of tactics, from phishing and ransomware to advanced persistent threats and zero-day exploits, posing significant risks to our national security and public safety. Cybersecurity has thus become a critical pillar of national security, economic stability, and public trust.

In addition, the relentless pace of technological advancement brings unprecedented opportunities but also exposes us to sophisticated and ever-evolving cyber threats. This complex global problem requires rapid responses from organisations to ensure the confidentiality, integrity and the availability of data assets controlled by the organisation. Organisations therefore need a proactive, holistic and flexible leadership approach.

The cybersecurity discipline includes technologies, policies, procedures, practices and culture designed to secure the organisation and the information it controls. Given the real-world security challenges in South Africa and across the African continent, data protection, privacy and cybersecurity legislative frameworks are under development requiring cybersecurity governance compliance. The CISO and CIO will therefore require a higher level of knowledge of the broader cybersecurity domain.

The **Cybersecurity Leadership Masterclass** is designed as an interdisciplinary course, focusing on emerging legislative and regulatory frameworks, security technologies, national strategies, standards, and organisational frameworks. The course incorporates elements relevant to creating a culture of cybersecurity awareness and resilience. The course also focuses on developing relevant strategic responses to the security challenges posed to the digital communications ecosystem.

Course Outcomes

The Masterclass is specifically designed to provide the building blocks for the foundational analytical skills for the CISO. It aims to advance the knowledge of organisations in general, and of IT security professionals and aspiring CISOs in particular, with respect to building successful cybersecurity leadership, in the face of increasingly sophisticated attacks.

Participants also need to be aware of the larger obligations placed on organisations by the unfolding Cybersecurity legislative frameworks, and also of regional and international fora for co-operation, in order to counter the transnational nature of Cyberattacks

Participants will interact with other cybersecurity practitioners and leaders and debate critical issues relating to the cyber domain and emerging technology domains, gaining valuable lessons and insights. On successful completion of the Masterclass, participants will be able to:

- Analyse the complex nature of the cybersecurity domain and the interdependencies between cybersecurity and traditional information security.
- Categorise the range of threats and threat actors facing organizations, institutions, and nation-states.
- Identify the effects of cyber-attacks on organizations and various levels of defence required to ensure the integrity of organizations, their data, and reputations.
- Formulate a foundational cybersecurity strategy by critically analysing the current organizational environment.
- Demonstrate the value of the various cybersecurity roles and responsibilities and the benefits to institutional governance.
- Critically evaluate the technology options available to defend the organization and consider solutions for ensuring the integrity of systems.

Audience

This program aims to advance the knowledge of senior officials and managers, IT security professionals, in particular, to build successful cybersecurity leadership, in the face of increasingly sophisticated attacks.

Course Outline

This 2-day Masterclass covers a comprehensive set of topics over four modules. In preparation for the program participants will need to familiarise themselves with the content and will be provided with an extensive reading list. A Certificate of Attendance will be issued on completion of the program