

EXECUTIVES AND DECISION MAKERS – STRATEGY & POLICY FORMULATION

- **Module Title:**

Executives & Decision Makers – Cyber Strategy & Policy Formulation Session 1

- **Description:**

This introduction to the cyber threat domain covers the threat types, how organisations are structured for cyber security leadership and the causes of cyber breaches within both commercial and governmental entities. It demonstrates the actual modes of execution of attacks by mal actors in terms of their notification, communication and contextual negotiations. The session closes with insight into the anticipated cyber-attack trends that need to be accounted for during a cyber risk assessment as new and emergent technologies are adopted for attacks.

- **Learning outcomes:**

Participants will gain an understanding of the general context within which cyber gangs operate and how they act during a period of attack and what can be expected of those interfacing with them post-breach. They will be aware of the most common forms of attack, as well as how mal actors develop new, or repurpose old attack techniques. The causes of cloud breaches and third-party contributing factors will also be comprehended.

- **Lecture title:**

The Cyber Threat Environment

- **Lecture description:**

This session introduces the participants to the operating environment all organisations now function within and how existing technologies, as well as AI and large language model use creates new attack forms, along with new threat vectors. Common tools utilized by mal actors are disclosed. Regulatory shifts that must also be complied with are covered, ensuring awareness of the multi-faceted approach to cyber risk management and technology risk control.

- **Module Title:**

Executives & Decision Makers – Cyber Strategy & Policy Formulation – Session 2

EXECUTIVES AND DECISION MAKERS – STRATEGY & POLICY FORMULATION

- **Description:**

This session highlights the multiple impacts arising from a successful cyber breach. It demonstrates, with examples, of how mal actors manipulate markets, behaviours and the threat of financial penalties for regulatory non-compliance. Commercial and governmental examples of the types and extent of cyber threat impacts from a financial perspective are provided. Physical security, vendor and third-party risks are explained, along with cascading impacts and the increasing targeting of critical infrastructure by mal actors is disclosed.

- **Learning outcomes:**

Participants will gain an understanding of the on and off-balance sheet impacts arising from cyber breaches. Data protection and privacy laws and how they lay an increasing role in the formulation of cyber security policies will be understood. Vendor risks, allied to AI, physical security and contractor, as well as insider risks will be more readily identified in order to be accounted for within cyber risk assessments. Comprehension of why peering and benchmarking can cause cyber security weaknesses in quantification will be attained.

- **Lecture title:**

Cyber Threats and Their Impacts

- **Lecture description:**

This session introduces the participants to the wide-range of negative impacts arising from cyber threats; from direct legal responsibility, to financial impacts. The easily missed elements that should be contained within vendor selection due diligence is described. Examples of how AI and large language models create new forms of cyber risks are provided, allied to how mal actors repurpose legitimate tools.

- **Module Title:**

Executives & Decision Makers – Cyber Strategy & Policy Formulation – Session 3

- **Description:**

This session introduces a number of concepts that many are unaware of when creating relevant strategies and policies covering the cyber threat environment within which all entities function. Those with leadership and senior managerial responsibilities are mandated by their

EXECUTIVES AND DECISION MAKERS – STRATEGY & POLICY FORMULATION

role to develop the risk appetite that then determines the overall cyber and information technology risk management of all organisations. The session therefore encompasses as many crucial elements required for the task by those tasked with determining which paths must be reviewed and critically assessed to control cyber risks, whilst simultaneously complying with multiple laws.

- **Learning outcomes:**

Participants will gain an understanding of the two fundamentally different cyber and technology risk management approaches. A full comprehension of the various freely available frameworks and standards that underpin cyber threat control will be attained. Risk mapping at the highest level, allied with data availability for formulating appropriate cyber strategies and policies will be attained. Understanding what mitigation options are available to all entities is provided to enable senior stakeholders to determine relevance within the entity's functional environment. Why and how new hierarchical management structures need to be formulated to account for new and emergent technologies will be learned.

- **Lecture title:**

De-Risking Cyber

- **Lecture description:**

The session focusses on three major components of cyber risk controls; mapping, standards (and frameworks), and mitigation options. The globally significant standards and approaches, allied with freely available resources for cyber risk management is disclosed. AI and large language model risks are covered, together with risk transfer as a cyber threat impact mitigation option. New governance and management structures are disclosed in order to account for AI, large language model and quantum computing use.

- **Module Title:**

Executives & Decision Makers – Cyber Strategy & Policy Formulation – Session 4

- **Description:**

This session attempts to unravel the multiple threads linking AI, large language models and quantum computing to the cyber threat landscape into the near-to-long term periods.

EXECUTIVES AND DECISION MAKERS – STRATEGY & POLICY FORMULATION

Examples of the multi-faceted impact of AI on the legal, compliance, threat and intellectual property domains is disclosed. How new laws, treaties and technical alliances are being formed through their interrelatedness and dependencies is discussed. Privacy, data usage, legality of use, liability and market impacts are covered.

- **Learning outcomes:**

Participants will gain an understanding of the overall new and emergent (those suddenly appearing) and how these may impact into the short/medium and longer terms in order to comprehend the elements required for future cyber resilience building and the resources required. The geopolitical environment and how it is shaping policy in relation to new laws, liability and the potential future cyber threat landscape will be comprehended. Insight into the interplay between foes and defenders utilising new and emergent technologies will be attained.

- **Lecture title:**

AI & What the Future May Bring

- **Lecture description:**

This session provides insight into the current AI trends in terms of the direction of travel of hardware versus software; laws versus data availability and use; the major players within the AI segment, as well as how the overall operational environment is shifting as a result of AI and quantum computational capabilities impacting upon cyber resilience on a global scale. The geopolitical landscape, globally significant joint ventures and the regulatory domains impacting upon how AI is/could/may be impacted is also described.
