Addressing the misperception

'People think that cybersecurity is something that's highly technical. Yes, some roles require deep technical expertise, but cybersecurity is a vast domain and making an organization cyber-resilient also requires generalist roles that need a broader skillset.'

Bobby Ford, Chief Security Officer, Hewlett Packard Enterprises.

ADVANCED PROGRAM CYBER SECURITY & GOVERNANCE

The cybersecurity field is one of the fastest-growing, in-demand and cross-sectoral fields. Cybersecurity workforce demand is very high and it is difficult to hire competent professionals. The agile and changing cyber environment sets high requirements for workforce awareness, competence, and skillsets. Educating students is not sufficient, we need to re-train and upskill current workforce with *professional training*. Given the global nature of the challenge, no single actor alone can find the solution. It requires collaboration across the public and private sectors. The *Advanced Program Cyber Security and Governance* covers a wide range of cybersecurity knowledge areas needed for the workforce to conduct their day-to-day activities and tasks. The uniqueness of the program is that it combines the best practices of academia, the public sector and industry to meet the needs of professional life through a truly practitioner's approach.

Background

According to the *WEF Future of Jobs 2023 report*, cybersecurity is among the top strategic skills for the workforce. Yet, there is a shortage of 3.4 million cybersecurity experts to support today's global economy. This number is only expected to grow as the impact of emerging technologies is felt across organizations. Despite efforts to close the workforce gap, the *(ISC)² Cybersecurity workforce study 2022* shows that though the number of cybersecurity professionals in EMEA grew with almost 12%, the cybersecurity workforce gap has grown more than twice as much as the workforce itself.

Due to the workforce shortage, retaining cyber talent proves difficult. Pressure and burnout are frequently listed as reasons why cybersecurity professionals leave their jobs. Educating students is not sufficient, we need to re-train and upskill current workforce with *professional training*. Tilburg University is setting up a comprehensive *cyber education program* to address the cybersecurity workforce gap. Important component of this educational program is this professional learning course developed by Tilburg Institute for Law, Technology and Society (Tilt) in cooperation with TIAS School for Business & Society.

Scope

- Multi-disciplinary course covering the full-spectrum of cyber security principles and management, cyber security tools and technologies, law and cyber governance, and cyber preparedness and response
- Five course days. Each course day is divided into 2 teaching sessions and one practical exercise or case study
- Each day a corporate CISO is co-host ensuring teaching is grounded in practice.

Target participants

People working in public and private organizations responsible for decisions as to cyber security, cyber risk management, cyber governance, or cyber incident preparedness and response, regardless of their discipline (cyber security, IT incident management, legal, crisis management)

Entry-level

The course does not require a specific technical background, but is aimed at participants with managerial responsibilities (so above operations level).

PROGRAM & DATES

Module 1 : Thursday 12th October 2023

CYBERSECURITY AS A STRATEGIC ENTERPRISE-WIDE RISK

- Identify the complexities and interdependencies in cyber space
- Cyber threats today and tomorrow
- The 'economics' of cyber security, bounty programs etc.
- Evolution of third-party cyber security services
- Evolution of security roles and responsibilities
- Risk assessment: risk as a combination of threat, vulnerability & impact
- Identifying key assets and possible impact
- Supply chain risks
- Threat Intelligence
- Practical risk assessment exercise

Module 2: Friday 13th October 2023

LEGAL RESPONSIBILITIES AND LESSONS LEARNED

- The developing global legal landscape governing corporate responsibility for cyber security
- Deep dive: the EU legal framework: NIS 1 + 2, DORA, Cybersecurity Act, the draft Cyber Resilience Act
- Regulatory burden and how to mitigate without compromising on security
- The clash between cyber security + privacy: the reality
- Lessons learned from assisting multinationals in their global cyber incident response
- Global reporting and notification requirements relating to data breaches, cyber incidents, ransomware attacks and payments
- Managing legal aspects of cyber incidents

Module 3: Thursday 26th October 2023

BUILDING A CYBER RESILIENT ORGANIZATION

- Security frameworks and mappings
- The pro's and con's of standardization – where diversity brings security
- Implementing cyber risk management cycle
- Top 10 controls in practice
- Zero trust: opportunities and challenges
- Human + behavioral factors
- Pro's and cons of a multi-vendor strategy
- Visibility in a multi-cloud
- Case study: how to design an optimal cyber governance and distribution of duties and responsibilities

Module 4: Friday 27th October 2023

MONITOR, MEASURE AND REPORT

- Monitor, measure and report
- Monitoring relevant threats and adapt mitigations: threat-informed defense
- Cyber oversight by the Board: with a no-nonsense approach
- Cyber board reporting metrics that make sense
- Insights from research
- Case study: optimizing the cyber governance

Module 5: Thursday 9th November 2023

CYBER INCIDENT PREPAREDNESS & RESPONSE

- Core elements of an Incident Response Plan
- Best practices incident preparedness & management
- Recognize the common pitfalls
- Ransomware: the 'No-IT' scenario
- Third party experts and their services
- Ripple effects
- The legal dimension
- Table-top exercise

Academic directors

- Prof. Lokke Moerel, Professor of Global ICT Law, Morrison & Foerster
- Freddy Dezeure, MSc, former head of CERT-EU.

Contributions from: NCSC, DNB, TU Delft, Fox-IT, Microsoft, and the CISOs of ASML, Philips and Signify

Dates: 12 -13 October, 26-27 October, 9 November 2023

Location: Tilburg University Campus (Warandelaan 2)

Price: € 3.800,- including coffee, tea, drinks, lunch and entrance to virtual campus.

Registration: For more information and registration contact Melanie Back (m.back@tias.edu)

Tilt Tilburg Institute for Law, Technology, and Society

TIAS SCHOOL FOR BUSINESS AND SOCIETY

TILBURG UNIVERSITY