SIT Learning

Cybersecurity: The Full Programme

Cybersecurity has many myths.

Perhaps some of the biggest ones are that cybersecurity is a technology problem, that dealing with it only requires technical proficiency, and it's enough for your IT staff to manage "the cyber".

The truth is that cybersecurity is the foundational enabler of business, and it has implications throughout your organization. Moreover, cybersecurity and resilience will only grow in importance as your organization advances on the digital transformation journey.

The best-performing enterprises and governments have grasped that cybersecurity is a strategic business enabler of every significant goal. You will learn to confidently navigate the digital realm to identify, create and seize new business opportunities.

On completion of this programme, you will:

- Develop a foundational knowledge of cyber risk
- Gain the universal frameworks to comprehend digital resilience and align security with key business goals
- Acquire the knowledge to ask the right questions about cyber risk management
- Acquire the ability to apply NIST CSF to scrutinize your organization's posture
- Gain strategic insight into the organizational considerations of leading cybersecurity strategies
- Grasp operational realities of implementing cybersecurity strategies within your organization
- The latest research, evidence, and best practices on an organization's cyber resilience - distilled for you

We invite you to discover more about this breakthrough programme.

Programme Structure

Day 1 – Cybersecurity as a Boardroom Level Conversation	Day 2 – Cybersecurity Measurement and Investment	Day 3 – Cybersecurity Management and Strategy
• Welcome and Introduction • Cybersecurity as a Key Element of Business Driver • Cybersecurity as a Competitive Advantage • Responsibility of Top Management Team for Cybersecurity • Assessing the Threat Landscape Risk Classification • Diagnostics, Assessment and Prioritization • Cybersecurity Requirements and Business Needs • Global Cybersecurity Trends and Agenda	• Assigning Responsibilities for Cybersecurity • Members of the Cybersecurity Eco-system • Cybersecurity Measurement and Reporting • Organizational Structures of Cybersecurity • Managing Investment in Cybersecurity • Cybersecurity Economics • Assessment of Financial Effects from Cybersecurity • Return on Security Investment (ROSI) • Planning Investments as part of Digital Transformation • Cybersecurity Insurance	• Choosing your Cybersecurity Building Blocks • Top Management View • Security by Design in Processes and Decisions • Mechanisms, Processes and Tools of Cybersecurity Management • Testing Methods • Managing a Major Cybersecurity Event • Cybersecurity for New Digital Technologies and Initiatives • Cybersecurity in M&A • Cyber Crisis Management and Business Continuity • Simulation Game

Day 1 – Cybersecurity as a Boardroom Level Conversation

Welcome and Introduction
The Academic Director of SIT Learning's Cyber Programme.

Cybersecurity as a Key Element of Business Driver
Business especially digital business relies on the internet. The internet, however is vulnerable. Information Security reduces the risk of data breaches and attacks on IT systems. It is about applying security controls to prevent unauthorized access to sensitive information, about preventing disruption of services such as denial-of-service attacks and minimizing the impact of insider attacks or physical outtages. It is about protecting your IT systems and networks from threats by outsiders and insiders.

Cybersecurity as a Competitive Advantage
Information Security can be a competitive advantage because it allows you to be better than your business competitors. If you and your competitors must meet certain security standards (like PCI, HIPAA or GDPR), and if you can do it more efficiently than your competition, your business gains competitive advantage. Additionally, that competitive advantage is further enhanced because a strong cybersecurity program encourages business innovation. You can satisfy customer needs without compromising the overall business or customer and user privacy. Creating trust with your customers can pay dividends. People are more likely to gravitate to businesses who demonstrate they are serious about data security and can protect privacy. Having confidence in your cybersecurity program can allow you to provide better services than your competitors, roll out advanced technologies more quickly and, when managed properly, can reduce overall security costs.

Responsibility of Top Management Team for Cybersecurity
Top management's involvement with the information security program includes ensuring that the intended outcomes of the information security program are achieved, which could include the following: Alignment with business strategy to meet the organization's strategic objectives. It also requires the empowerment of CISO and CIO with the right power to ensure the overall security. Oversight committees can help with some of these drivers but the responsibility is with the board as well.

Assessing the Threat Landscape Risk Classification
What existing and emerging threats affect our business? We must ground our security posture in facts. Contrary to common knowledge, substantial empirical evidence exists of the cyber-threat landscape, which should guide your strategies and risk management. You will learn the most current and important risks, threat actors, and economic incentives for their elimination and control. You will also learn the lifecycle of cyber-attacks - the general model to analyze cyber-attacks and improve your resilience. Moreover, you will be able to assess the likelihood and impact of cyber risks on your enterprise and find out how to move beyond a reactive risk avoidance posture. This allows you to ask the right questions when discussing different risk and threat classes and prioritise the cases.

Diagnostics, Assessment and Prioritization
A successful data security risk assessment usually can be broken down into three steps: Identify what the risks are to your critical systems and sensitive data; identify and organize your data by the weight of the risk associated with it and take action to mitigate the risks. The NIST Cybersecurity Framework (NIST CSF) provides guidance on how to manage and reduce IT infrastructure security risk. The CSF is made up of standards, guidelines and practices that can be used to prevent, detect and respond to cyberattacks. Frameworks such as NIST, CIS and ISO can help companies to follow correct procedures. There are detailed sub categories such as control frameworks, program frameworks and risk frameworks.

Cybersecurity Requirements and Business Needs
The three requirements of cybersecurity are: confidentiality, integrity, and availability. The main business needs are: prevention of unauthorized access, counter threats, confidentiality, disruption, destruction and modification of business information.

Global Cybersecurity Trends and Agenda
Gartner identifies seven top trends for the next few years: Attacks on Surface Expansion, Identification of System Defence, Digital Supply Chain Risk, Vendor Consolidation, Cybersecurity Mesh, Distributed Decisions and Beyond Awareness. We discuss them all during this intervention.

Day 2 – Cybersecurity Measurement and Investment

Assigning Responsibilities for Cybersecurity

Who should be responsible for managing cybersecurity in an organization, and how to make the results of this work transparent? You will learn the SIX Principles for board governance of cyber-risk and discover tools and methodologies to assess the protection level of your organization. You will learn the difference between CSIRT and SOC, which approach is more suitable for which challenges, and discuss how to measure success and resilience over time. You will also discover how audits, pentests, and table-top exercises can and should be used to verify the IS setup of an organization.

Members of the Cybersecurity Eco-system

The IT ecosystem is defined by Forrester Research and others as "the network of organizations that drives the creation and delivery of information technology products and services" and includes customers, suppliers, and influencers (key stakeholders).

InfoSec Measurement and rRporting

Robust information security measurement and reporting provides information that is factually based and measures progress, effectiveness of a process while monitoring if outcomes are being achieved.

Organizational Structures of InfoSec

The IRC is the most important element of a security program's organizational structure. It is the structure that provides the security program cross-functional authority and visibility while simultaneously granting functional areas autonomy to carry out business functions in a way that makes the most sense.

Managing Investment in InfoSec

Economics of cybersecurity offers a rich toolbox to understand the all-important non-technical drivers of cyber risks. However, misaligned incentives, cognitive biases, and information asymmetries are among the profound challenges of this field, and no technology can overcome them. This session will enable you to navigate the complexities of identifying necessary cybersecurity capabilities, budgeting, and assessing RoI. You will learn how to measure and improve your investment in cybersecurity and what it means to spend more than your peers on cyber.

Cybersecurity Economics

The economics of information security addresses the economic aspects of privacy and computer security. Economics of information security includes models of the strictly rational "homo economicus" as well as behavioral economics.

Assessment of Financial Effects from Cybersecurity

Two aspects of stewardship that are of particular concern in cloud ecosystems:
Resilience: the capability of the system to recover from attacks that successfully compromise its declarative stewardship objectives (e.g., the confidentiality of a customer's PID is breached) or inhibit the effectiveness of its operational mechanisms to deliver its objectives (e.g., the loss of availability of authentication server); and **Adaptability**: the capability of the ecosystem to adapt to changes in its composition (infrastructure providers, service providers, consumers), in its required functionality, in its regulatory environment, and its threat environment. Adaptability is the key to sustainability.

Return on Security Investment

The ROSI calculation combines the quantitative risk assessment and the cost of implementing security counter measures for this risk. In the end, it compares the ALE with the expected loss saving.

Planning Investments as part of Digital Transformation

To plan investments, you will need to: define what digital transformation means for you, orient your strategy to a clear goal, recognise the role of data and prioritise flexibility.

InfoSec Insurance

InfoSec coverage is constantly developing solutions to protect your organization against a broad range of threats. We discuss the most popular methods such as risk transfer.

Day 3 – Cybersecurity Management and Strategy

Choosing your Cybersecurity Building Blocks

The large and elaborate market presents a bewildering barrage of solutions. Our expert instructors will lead you through the FUD to grasp the key points about the ubiquitous building blocks: FW, IPS, Backup & recovery, and Zero Trust. Moreover, you will gain the common language and framework that enables you to participate in critical discussions on cyber-risks (NIST CSF).

Top Management View of InfoSec

The role of the top management is crucial in making sure that information security policy is developed and enforced in their agencies or organizations. If not supported from the top, the implementation of an information security measures will definitely fail.

Security by Design in Processes and Decisions

Security by design is an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as continuous testing, authentication safeguards and adherence to best programming practices. The security by design model contrasts with less rigorous approaches including security through obscurity, security through minority and security through obsolescence.

Mechanisms, Processes and Tools of Cybersecurity Management

Security mechanisms deal with the hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. Processes move through phases building and strengthen themselvesalong the way. Although the Information Security process has many strategies and activities, we can group them all into three distinct phases - prevention, detection, and response.

Testing Methods

There are five main testing methods: Network Scanning, Vulnerability Scanning, Ethical Hacking, Password Cracking and Penetration Testing. An overview will be provided highlighting the benefits and limitations of the different types.

Managing a Major Cybersecurity Event

What actions can and should be taken as you learn that a significant breach is in progress? In this session, you will learn how management needs to act through the crisis and how to boost resilience even after a breach occurs. You will gain realistic direct experience from interactive incident response TTX / Simulation with proven methods to minimize damages from cyber-incidents. This session will also guide you through creating a tailored incident response plan. Moreover, you get a Cyber Incident Response Playbook which boosts your effectiveness in building digital resilience.

Cybersecurity for New Digital Technologies and Initiatives

InfoSec is rapidly becoming crucial in the rapidly developing Internet of Things environment, in which almost any conceivable device, object or entity can be given a unique identifier and networked to make them addressable over the Internet. One of the major challenges of IoT security is the fact that security has not traditionally been considered in product design for networking appliances and objects that have not traditionally been networked.

Cybersecurity in M&A

M&A decision-makers must fully understand the potential risks a data breach would pose to critical business assets and functions, from intellectual property (IP) and operations to customer information and credit card data. Ignoring these cybersecurity risks in M&A can leave a buyer exposed to a range of risks, including diminished revenues, profits, market value, market share and brand reputation.

Cyber Crisis Management and Business Continuity

A business continuity plan is a thorough emergency document that outlines how a company will continue to function during and after a disaster or other unplanned disruption. Today, a large section of a business continuity plan focuses on cyber security risks and data loss, but that is not enough.

Cyber Crisis Simulation Game

In this game, all your knowledge from the program will be put to the test. You will also develop your own Capstone project that will allow you to implement your learning in your own organization.

Speaker Biographies

Dr. Lior Tabansky

Head of Research Development for Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University

Dr. Lior Tabansky earned a PhD in Political Science, an MA in Security Studies and BA in Political Science – all from Tel Aviv University.

Lior's doctoral dissertation "Explaining National Cyber Insecurity: A New Strategic Defense Adaptation Analytical Framework" (Tel Aviv University, School of Government and Politics, 2018) builds upon Defense Adaptation and Military Innovation theoretical framework to explain why even the most advanced nations remain exposed to destructive cyberattacks on strategic homeland targets by foreign states.

"Cybersecurity in Israel," 's 2015 book co-authored with Professor Maj.-Gen. Isaac Ben-Israel, is the first comprehensive "insider" account of decades of Israeli policy and operations. Moreover, the authors develop an original analysis of the roles grand strategy and innovation play in cybersecurity.

Lior Tabansky conducted research at the Institute for National Security Studies (INSS) think-tank in Tel Aviv, where he authored and published the inaugural Israeli cybersecurity scholarship in 2011-2013.

In parallel with academic work, Lior has built a record of accomplishment in tackling complex policy problems through strategic advisory in Asia and Europe.

Candid Wüest

Vice President of Cyber Protection Research at Acronis

Candid Wüest is the VP of Cyber Protection Research at Acronis, the Swiss-Singaporean cyber protection company, where he researches on new threat trends and comprehensive protection methods.

Wüest has extensive experience in the field of IT security accumulated during the past 20 years. Prior to joining Acronis, he was the lead Threat Researcher at the global Symantec Security Response team and, prior to that role, analyzed computer viruses for the Symantec Anti-Malware Lab in Dublin. Wüest has also held key positions with the Global Security Analyzing Lab of IBM Research in Rüschlikon. Wüest holds a Master in Computer Science degree from the Swiss Federal Institute of Technology (ETH).

Wüest is a security advisor for the Swiss federal government on cyber protection of critical infrastructure, a member of the Defcon Switzerland Board and organizer of the Area41 Conference. He's won multiple industry awards, holds several security patents, and has authored numerous books, white papers, threat reports, and articles. As a result of his cutting-edge work, Wüest is a respected security conference speaker.