Executive course:

Cybersecurity for Board Members, Executives, and Managers

Strategic and operational cybersecurity for managers

"Cyber threats are one of the greatest business risks that we face. Therefore, it is crucial that our managers are equipped to understand and assess the threat landscape - and integrate cybersecurity into the overall strategy of their companies."

Nadeem Farooq, Deputy Director,
Danish Employers' Association for the Financial Sector

FA FINANSSEKTORENS ARBEJDSGIVERFORENING

Introduction

When you manage and run a business in one of the most digitized societies in the world, cybersecurity is a mandatory part of the company's risk management. Management has the overall responsibility for protecting the company's assets, and that task requires close collaboration with IT security professionals.

The Technical University of Denmark (DTU) has collaborated with the Financial Sector Employers' Association (FA) as a business partner on an initiative that addresses the increasing demand for competences in cybersecurity through ongoing development of continuing education.

This effort aimed to:

- Uncover competence needs as a prerequisite for being able to tailor relevant competence enhancement aimed at Board Members, Executives and Managers.
- Develop and implement effective, high-level skills based on needs identification and a technical basis in knowledge and experience from DTU, Cybersecurity Engineering,

DTU and FA are pleased to be able to present the result of the development work, namely two modules “Cybersecurity Essentials” and “Cyber-Risk Management, which separately or together strengthens the language and insight managers need to take responsibility for the company's activities in a proactive and well-informed manner.

Cybersecurity is in the hands of Board Members, Executives, and Managers

Critical task on the agenda

Where does your business stand if a cyber-attack cripples your digital systems? Today, cyber-attacks are among the most critical business risks companies face.

A cyber-attack can harm both earnings, customer relations and the company's reputation. Therefore, cybersecurity is moving up the agenda to involve not only security personnel but - and this is crucial - among boards and executives.

The question is how you, as a manager, can make balanced decisions that align with the company's interests and strategy.

Bridge a gap between cyber and business

A significant part of the day-to-day handling of cyber-risk management naturally falls to IT security professionals. However, risk management is at the core of every business decision, and as a result, cyber-risk management also requires leadership involvement. Unfortunately, the World Economic Forum's report 'Global Cybersecurity Outlook 2023' shows that the understanding between cyber leaders and business leaders still leaves much to be desired. How can a manager prioritize efforts and resources without insight into the possibilities - and the consequences?

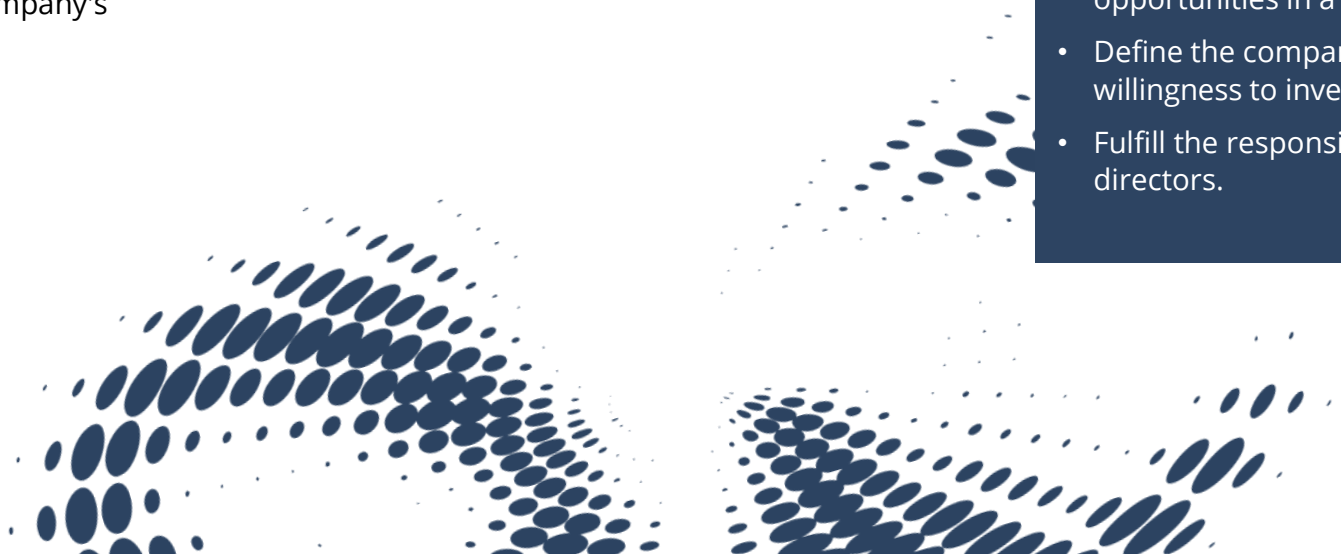
That is the gap that the courses in this presentation is designed to bridge. From a high-level technical point of view.

Make a difference through culture

In the daily life of most companies, the weak link is not technology but culture: Managers and employees often fail to differentiate between the many types of cyber threats or their severity in their current context. This makes it too easy for cybercriminals to succeed, which is why the program (e.g., the module “Cybersecurity Essentials”) also focuses on the human factor: how to create a culture where secure habits are part of the users' daily routine.

Management needs cyber expertise to:

- Protect assets, business processes and customers.
- Generate growth and exploit the business opportunities in a digitized context.
- Define the company's risk profile and willingness to invest.
- Fulfill the responsibilities of the board of directors.



A flexible course with two modules

Cybersecurity for Board Members, Executives, and Managers consists of two modules, which you can either take together or separately, depending on your needs. The lectures are conducted in English.

Module 1: Cybersecurity Essentials
When the management needs to discuss cybersecurity on a qualified basis, it requires language insight and technical understanding that gets through to and challenge those responsible for cybersecurity in the company.

This is why Module 1 focuses on establishing a fundamental insight into the field:

- Introduction and Security Trends. Including cybersecurity, typical threats and attack vectors and various approaches to cybersecurity.
- General Security Concepts. Including fundamental concepts, different aspects and principles of cybersecurity.
- The Role of People in Security (Social Engineering). Including potential risk behaviour, secure habits and efforts to build a healthy security culture.
- Types of Attacks and Malware. Including symptoms and relevant defences and guidelines.
- Identification and Authentication. Including the role of passwords and how they can be attacked and strengthened.

Professor Nicola Dragoni
PhD, Deputy Director, Professor in Secure Pervasive Computing, Head of Section Cybersecurity Engineering, Head of DIGISEC - DTU Centre for Digital Security

Module 2: Cyber-risk Management
In a connected world, 100% cyber security is both impossible and priceless. So which efforts should the company prioritize - and where is the balance between risks on the one hand and the price of security on the other?

In Module 2, we create the link between business and cyber security, and we go in depth on areas such as:

- The conceptual framework. A structured approach to cyber risk management.
- The context. The factors the company must consider and include in its work with cyber risk management.
- Assessment of threat scenarios and risks. How to proceed and direct to make the most of available resources.
- Balanced decision-making given relevant findings. Options for treatment and control.
- Communication to inform and engage relevant parties.

Professor Ketil Stølen
PhD in Computer Science, Project leader, Lecturer, Writer and Advisor

You will not become a technical expert. You will become capable of making well-informed decisions.

Choose the path that suits your needs

You can take the two course modules either separately or together. Here is our recommendation.

Your role	Recommendation
Manager without cybersecurity background	Module 1: Cybersecurity Essentials
Cybersecurity employee, including managers and board members, with expertise comparable to Module 1	Module 2: Cyber-risk Management
Manager or board member with no cyber-security expertise who needs an insight into cybersecurity management	Module 1: Cybersecurity Essentials followed by Module 2: Cyber-risk Management

Contact us if you are unsure which module to select based on your background and responsibilities.

Module 1: Cybersecurity essentials enables you to:

Understand and guard against the most common cyber threats.

- Be empowered with cybersecurity knowledge, skills, and mindset
- Comprehend the changing cyber threat landscape.
- Establish a culture of resilience and enhance long-term success in an increasingly digitized world.

Module 2: Cyber-risk management enables you to:

Align cybersecurity with business objectives.

- Integrate cybersecurity considerations into business planning, decision-making processes, and risk management frameworks.
- Effectively assess and mitigate risks.
- Have constructive discussions with key IT security staff to ensure that cyber risk is being appropriately managed.

What threats do you see?

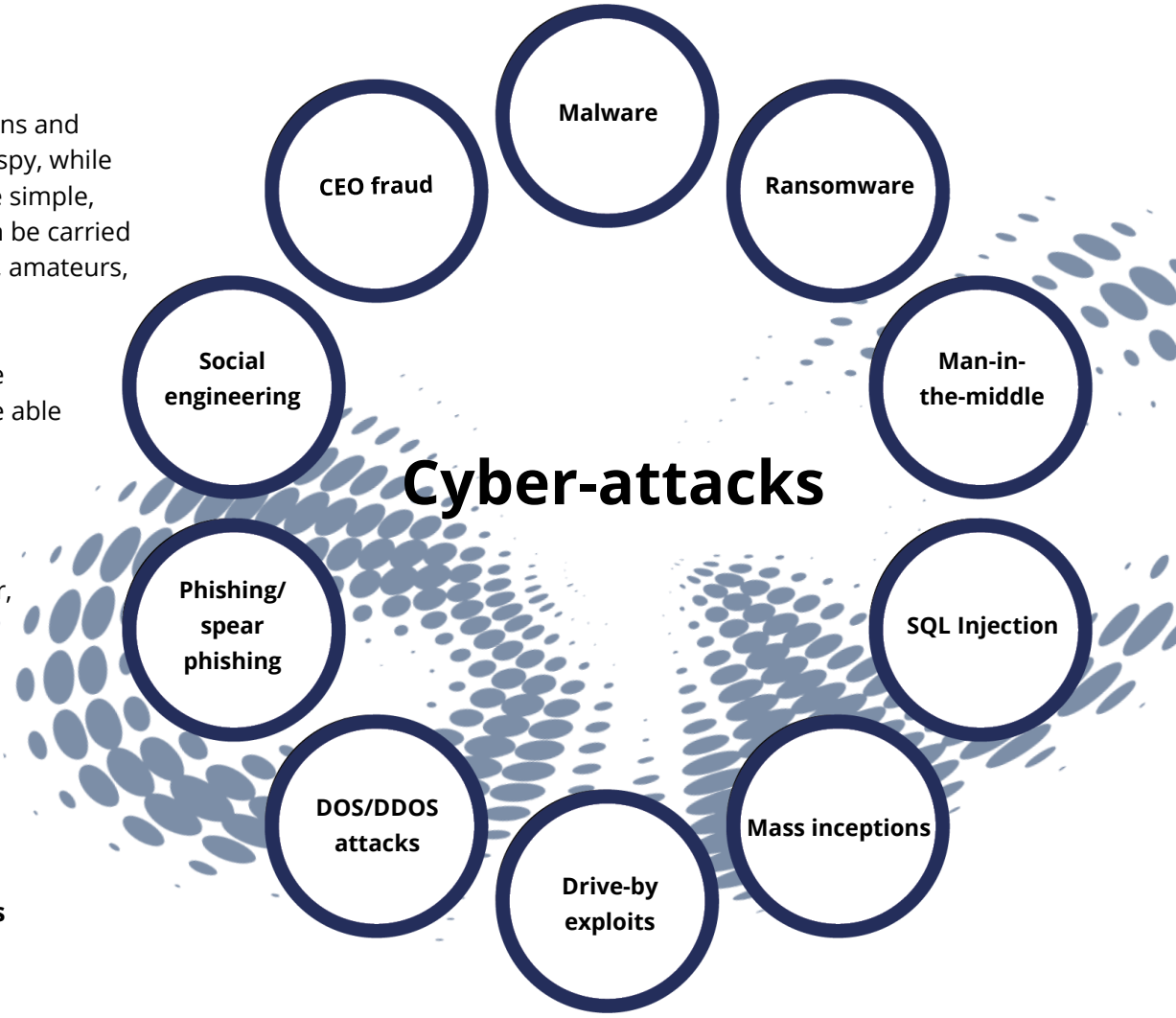
The concept of cyber threats encompasses a wide range of different attacks with various objectives. In order to work on a cyber-security strategy, you need insight to assess what is particularly vulnerable to your company and discuss which efforts should therefore be prioritised.

The complex landscape
Cyberattacks are driven by different intentions and methods. Some attacks aim to steal data or spy, while others aim to steal money. Some attacks are simple, while others are advanced. Cyberattacks can be carried out by organized criminals, sovereign states, amateurs, internal employees and competitors.

A successful attack can ultimately cripple the company. Therefore, it is crucial that you are able to assess your vulnerability - and allocate resources to the right countermeasures.

The most prevalent cyber threats today are phishing emails and CEO fraud. However, your company's risk exposure depends both on the industry, the company's most valuable assets and its vulnerabilities, and therefore, it should be assessed individually.

It is estimated that 9 out of 10 companies have already been hacked.



Bridging the gap between business and cybersecurity

On one side, management holds the responsibility for risk management and understands that cyber threats are serious for the business. On the other side, IT security specialists know the technological aspects. The cybersecurity strategy can be a bridge between these two actors.

The strategy sets the framework
A cybersecurity strategy is the framework that ensures all aspects of security are included in the company's ongoing cyber-risk management. The strategy should enable the company to implement the basic functions of a cybersecurity framework: the ability to identify, protect, detect and respond to cybersecurity incidents - as well as the ability to restore affected systems and assets.

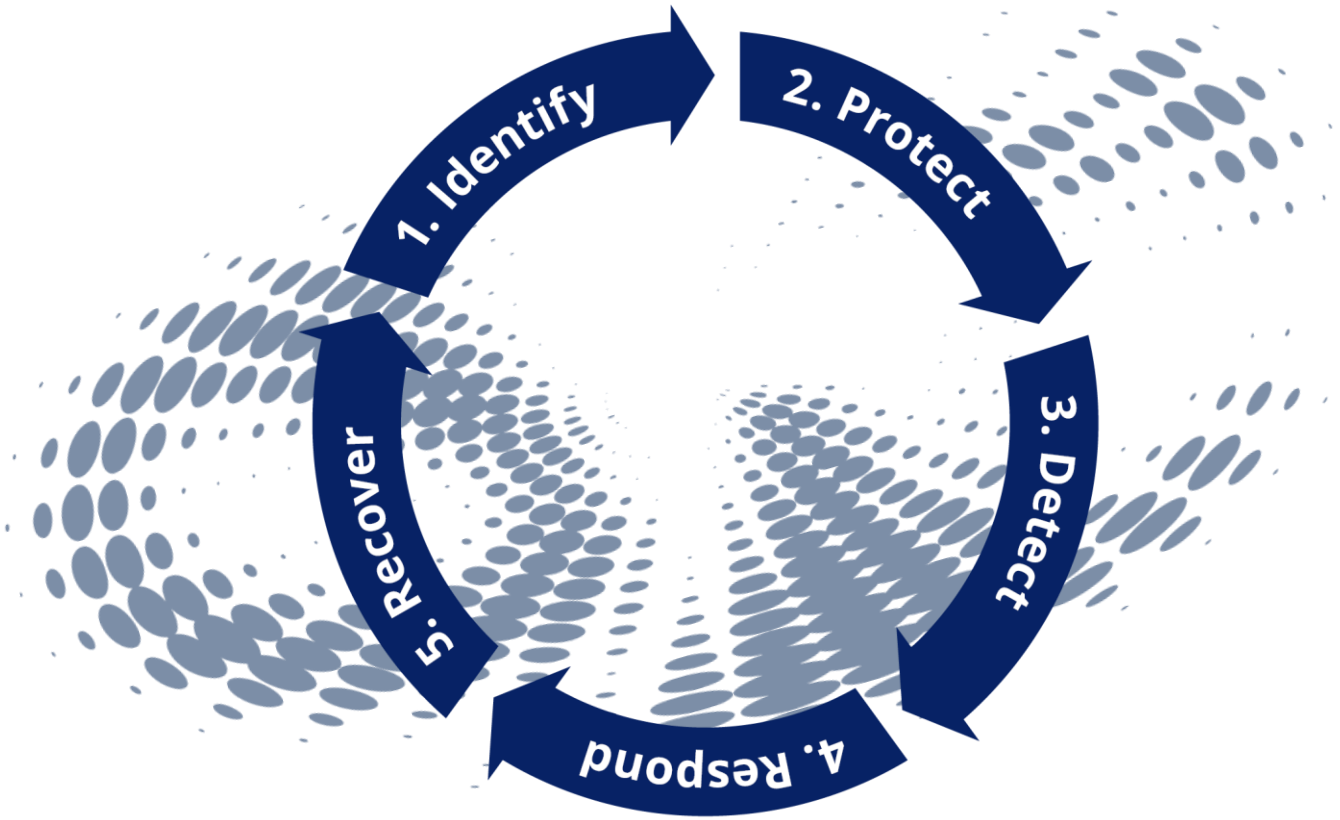
The strategy also addresses all aspects of security - from governance and management to tools, processes, people and IT. Therefore, it should naturally be high on any management's agenda.

Transform knowledge to a cybersecure business
With the two courses presented, Board Members, Executives and Managers are well equipped to make decisions related to a cybersecurity strategy.

.

Objectives of a cybersecurity strategy

1. **Identify** assets, vulnerabilities, threats etc.
2. **Protect** the company by appropriate measures.
3. **Detect** if or when a cybersecurity attack occurs.
4. **Respond** to a detected cybersecurity incident.
5. **Recover** capabilities and services affected.



A fraud use case

A charity organization only became aware there was an incident when their bank contacted them querying a change in a supplier's bank details.

Their CISO explained, “We checked the Finance Manager’s email account and discovered that a rule had been set up to divert any email containing the words ‘payment’, ‘invoice’, overdue’ bank details’ etc. to the Really Simple Syndication (RSS) feeds folder. At this point, the fraudster doctored the body of the email and the invoice attachment with the fraudulent bank details. It was believable as the main body of the email had clearly come from a known supplier as it was answering questions that only they could have known. At this point we had narrowly missed making a payment to a fraudulent bank account.”

Another supplier emailed a week later to chase payment of an invoice which the organization thought they had paid. On checking the payment details they discovered the payee’s account details were different to those on the invoice.

“Looking back, the Finance Manager had noticed that people were saying that they had sent her an email, but they were taking a day or two to come through, but it was just thought to be a lag with the system. This will be a red flag for us going forward.”

Immediate Action Taken

- Finance Manager called the bank and alerted them to the fraud
- CISO reported it to Action Fraud to obtain a crime reference number
- CISO reported it to The Charity Commission as a serious incident

Lessons learned/further actions

- CIOSO updated their processes and procedures
    - weekly checks on email accounts to ensure no rules have been set
    - check email ‘safe senders’ list to make sure it is authentic
    - check the location of any logins to Microsoft 365 to ensure no activity on the account
    - check RSS Feed folder for rogue emails
    - bank details for new and updated suppliers to be verified by a phone call
- If making a payment online and bank details don’t match, phone and check with the payee that the details are correct
- Implemented multi-factor authentication for logging into Microsoft 365

Cybersecurity for Board Members, Executives, and Managers - registration and contact

See further details about the course at:

https://lifelonglearning.dtu.dk/en/compute/single-course/cybersecurityessentials/

https://lifelonglearning.dtu.dk/en/compute/course/cyber-risk-management/

Cybersecurity Essentials
Start: 22 November 2023
Location: DTU Kgs. Lyngby
Language: English
Price: 12.500

Reg. deadline: 10 November 2023

Cyber-risk Management
Start: 5 December 2023
Location: DTU Kgs. Lyngby
Language: English
Price: 12.500

Reg. deadline: 25 November 2023

Contact
If you have questions about the course, you can contact:

Nicola Dragoni
Professor, Head of Section
DTU Compute
+45 45 25 37 31
ndra@dtu.dk

Camilla Gudrun Poulsen
Senior Officer
DTU Compute
+45 31 26 75 86
cagupo@dtu.dk

DTU

FA FINANSSEKTORENS ARBEJDSGIVERFORENING