



Get to grips with cyber security:  
*Decision making and communication*



DISEM INSTITUTE  
&  
OVERTUIGCOACH

# Proposition by Disem Institute and Overtuigcoach

*Disem Institute* was founded in 2021 and stands for Dynamics in Information Security, Economics and Management. Disem Institute is specialised in analysing complex, dynamic, strategic issues and making them understandable, and excels in the field of cyber security. We offer innovative and new strategic assurance and consultancy services and specialised training courses.

*Overtuigcoach* is founded by Arthur Noordhuis and is specialised in opinion forming and persuasiveness. Arthur has been active for over 20 years as a trainer in business, government and politics. He wrote the bestseller book on management *Debatteren om te winnen*. As trainer and coach, Arthur helps people improve their verbal skills and achieve their goals using good communication.

Organisations weigh up cyber security matters against other business matters

People are often not aware how their cyber security decisions influence the organisation in the short and long term

The training 'Get to grips with cyber security' by the Disem Institute and Overtuigcoach offers a solution to this problem

# Getting to grips with and keeping a grip on cyber security are a challenge

*56% of experienced (senior) managers and security professionals make suboptimal decisions (Zeijlemaker 2019\*, 2022\*\* in press).*

*These suboptimal decisions lead to an increase of up to 200% in structural cost base (Zeijlemaker 2019\*, 2022\*\* in press).*

So, you want to get to grips with cyber security?

How do you deal with the dynamics? How do you think about it, work with it, communicate about it?

- 1 Are your warnings concerning cyber security risks not being heard?
- 2 Should cyber security move up the agenda?
- 3 Is there a lack of cyber security awareness among your colleagues?

This training course combines the latest scientific research and focusses on improving policy making and communication. This training teaches how to deal with complex cyber security matters in a practical way - how to think about it, work with it, and communicate about it.

**Target group:**

Professionals, trainers, high potentials, consultants, managers, policymakers and others who work in cyber security and IT.

\* Zeijlemaker, S., Rouwette, E.A.J.A. & Cunico, G. (2019). Results from the cyber-security game: decision makers may have difficulties in appreciating dynamic complex systems. In Proceedings on the 37th International Conference of the System Dynamics Society, Albuquerque, New Mexico, USA

\*\* Zeijlemaker, S. (2022). Unravelling the dynamic complexity of cyber-security: Towards identifying core systemic structures driving cyber-security investment decision-making (PhD Thesis).

# Understanding and effective communication are decisive

*Looking is one thing, seeing is another.  
Seeing is a lot more difficult, but helps  
you understand. In order to make good  
decisions you need to understand.*

## Understanding the complexity and communicating effectively are key

In this day and age, far-reaching digitalization leads to a deeper intertwining of the cyber security within the organisation and between organisations. Cyber security therefore affects the employees, the processes, the technology and management. Cyber security responsibility is often divided among different people and departments, which makes policymaking slow and complex. This way, incorrect risk estimations and considerations can lead to significant, additional costs in order to correct and repair. And in some situations even to a considerable threat to the organisation's continuity.

The reciprocal, complex dynamic relation between the behaviour of the attacker and the defence of the organisation, its business operations and IT, finances and risk management plays a decisive role. Well known and common principles of management and prioritization can, in terms of cyber security, often be counter-intuitive. But how do you explain this well to managers and colleagues who have different priorities? How do you convince them of this new way of thinking? That's why this training doesn't only discuss the insights, but we also practise communication techniques.

# A dynamic perspective strengthens the existing decision making processes

*Cyber security is considerably influenced by its dynamic nature: evolving attack tactics, changing organisations, limits to staff and budget, sudden changes in priorities.*

*How you deal with the dynamics of cyber security ultimately determines how successful the safety strategy is.*

## Forecasting and taking into account errors and vulnerabilities

The famous footballer Johan Cruijf once said: "Before I make a mistake, I don't make it." In this training in cyber risk management we take things a step further. With the unique and innovative insights from the scientific method of system dynamics, we demonstrate when mistakes will probably be made, with consequences to staff, the organisation, and its stakeholders. The biggest challenge is to make sure colleagues within the organisation become familiar with these insights and this way of thinking by using effective communication techniques.

It is precisely this combination of insights with realistic exercises that make this training so effective.

## What makes this training so unique, fun and educational?

By using famous data breach cases, we gain insight and experience that can be directly applied to one's own business. What can we learn from one of the biggest international hacks? What went wrong where, when and how? And how could it have been prevented with better insights, decision making and communication? What were the underlying dynamics?

Could you have prevented the hack for example by communicating differently? We reflect on the learnt lessons and teach effective communication techniques such as framing, storytelling and the yes set technique.

# Day 1: Cyber Security Strategy

Time	Day 1	Cyber security strategy: Plan, measures & decisions
9:30	Introduction	
9:45	Insights in strategic cyber security decision making.	
10:00	How do I persuade a moderately interested management board? Break the communication wall.	
10:45	Break	
11:00	Common structural fallacies when prioritizing cyber security matters .	
11:30	How do I persuade an impatient management board? Persuasive speaking and the yes set technique.	
12:15	Lunch	
13:15	Defining game changers in cyber security.	
14:00	How do I convince better with a different use of voice and body language (part 1)?	
14:45	Break	
15:00	Short and long term consequences of cyber security (part 1).	
15:45	How do I convince better with a different use of voice and body language (part 2)?	
16:30	Conclusion.	
17:00	End	

# Dag 2: Cyber Risk Management

Time	Day 2	Cyber risk management: Priorities & decision
9:30	Introduction	
9:45	Insight in the true nature of cyber risk management.	
10:00	How do I emphasize the right parts in my conversation? The power of framing.	
10:45	Break	
11:00	The flip side of chance and impact.	
11:30	How do I move a discussion to the right level? The correct use of reframing.	
12:15	Lunch	
13:15	The consequences of a layered defence.	
14:00	How do I recognize fallacies?	
14:45	Break	
15:00	Short and long term consequences of cyber security (part 2).	
15:45	Conducting a dialogue.	
16:30	Conclusion.	
17:00	End	



# The trainers

## Sander Zeijlemaker RA RE MSC CISA CISM SCF



Sander Zeijlemaker is director of the Disem Institute. As a strategist, consultant and author, he focusses on the forecasting of complex, strategic decisions. He's had a career in business operations, IT, finances and security solutions. For many years, he has created and led a strategic simulation lab to analyse a wide variety of dynamic, complex, strategic security issues and he was business controller of the global security function.

He has had great success in using a specialised approach based on the scientific method of system dynamics in order to enable managers to plan more effectively, to involve their organisations and to forecast the results of their decisions.

As president of the global special interest group of security, stability and resilience of the System Dynamics Society, Sander mobilises and connects a group of professors, professionals and students in this area.

## Arthur Noordhuis



Arthur Noordhuis has been active for over 20 years in business, politics, NGOs and government. He has taught managers, legislative lawyers, inspectors, accountants, politicians, tax advisors, lawyers and public prosecutors, among others, how to get stronger verbally and he has enabled them to achieve their goals using good communication. Arthur regularly works with colleagues from the Dutch Debate Institute (Nederlands Debat Instituut). Together they have made several educational videos. Over the past years, Arthur has enjoyed training thousands of students.





*Disem Institute is specialised in analysing complex, dynamic and strategic management issues and excels in the field of cyber security. Disem Institute offers the means to see and follow how strategic decisions will develop in the future. Our scientific approach shows the effectiveness of a strategy before managers make big investments.*



**DISEM INSTITUTE**