QUANTIFYING CYBER RISKS

MARIEKE KLAVER, PETER LANGENKAMP (TNO)
SANDER ZEIJLEMAKER (DISEM INSTITUTE)

INTRODUCTION

- Dr. Marieke Klaver
  - (PhD in mathematics)
  - Researcher at TNO
  - Focus areas: risk management, cyber security, critical infrastructures
- Dr. ir. Peter Langenkamp
  - (PhD in Physics)
  - Cyber Security Researcher, dept. Cyber Security and Robustness @ TNO
  - Focus: Risk analysis, secure multi-party computation, self-sovereign identity
- Sander Zeijlemaker RA RE MSc CISA CISM SCF
  - Managing Director @ Disem Institute
  - PhD researcher Radboud University (system dynamics and security economics)
  - Focus areas: cyber security, strategic assurance & optimalization, and executive coaching

CONTENTS

INTRODUCTION QUANTIFYING CYBER RISKS

QUANTIFYING CYBER RISKS
BACKGROUND

Research project by TNO and NCSC

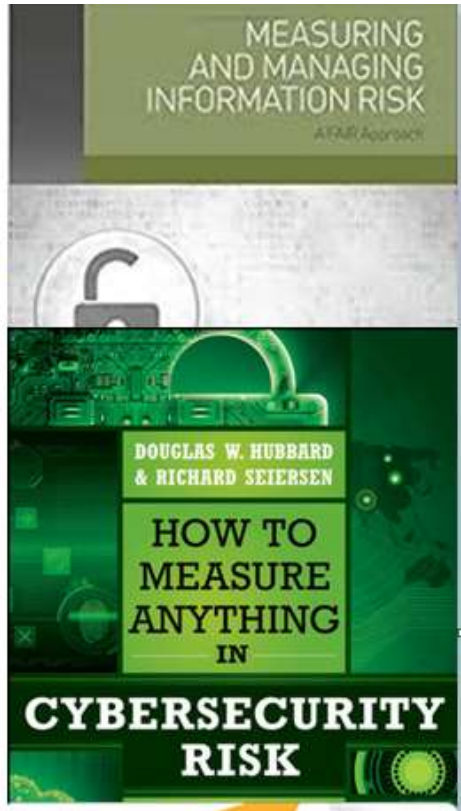
- Objective
  - To develop methods and tools for quantfying cyber risks
  - Based on case studies in critical sectors

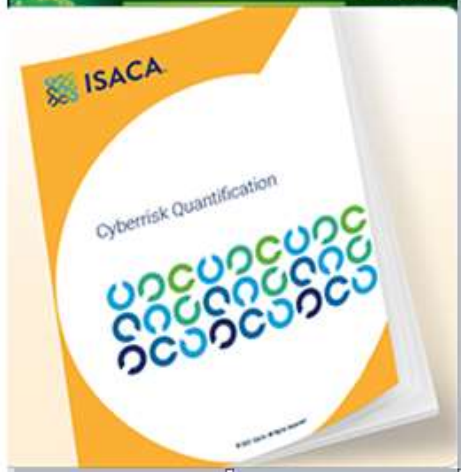
- Quantifying cyber risks helps to:
  - Provide a basis for cybersecurity investment decisions
  - Prioritize measures when resources are limited (distinctiveness)
  - Make cyber risks more comparable to other business risks
  - Facilitate information sharing on cyber risks
  - Assess how the effects of risks or measures propagate through the system (sensitivity analysis)
  - Potentially automate (parts of) analyses

DEVELOPMENTS QUANTIFYING CYBER RISKS

- Methods for quantifying cyber risk
  - Underpinning qualitative risk heat maps
  - Quantifying likelihood and impact
  - Several methods exist, however as of yet there is no commonly accepted standard available

- Supported by modelling approaches
  - Bayesian Belief Network
  - System Dynamics





APPROACH FOR USE CASES

- Developing a base model
  - Based on a methodology developed for and with the financial sector
  - Uses Bayesian Belief Network

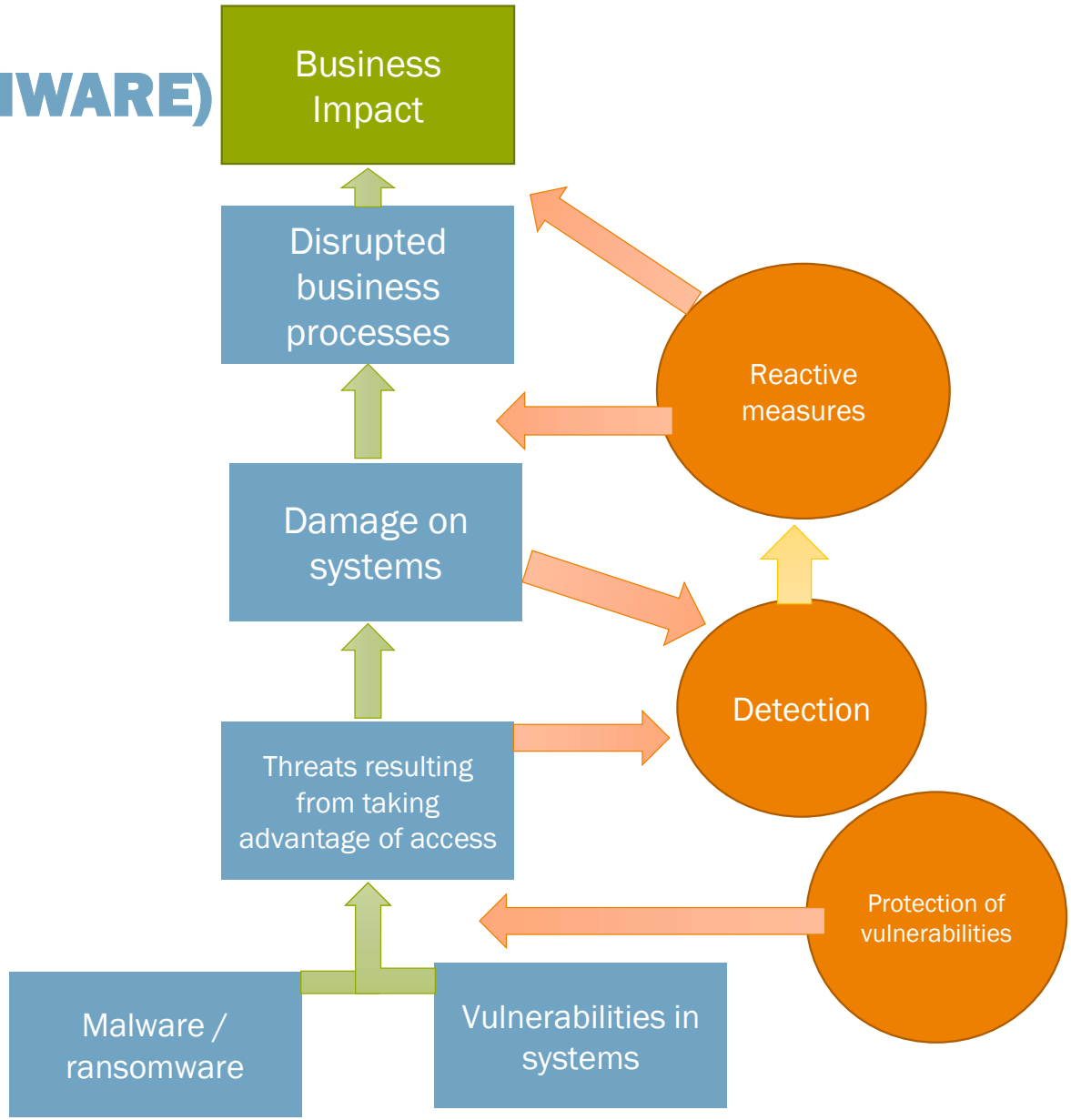
- Developing more detailed models in case studies
  - Preparation
    - Select threats which will be applied to your use case (dreigingsscenario's)
    - Gather information on the cases' organisation (business processes, architecture, measures)
  - Develop case specific model
  - Workshops
    - assess and extend case model
    - risk assessments
  - Present and discuss results with the case organisation

BUILDING BLOCKS (RANSOMWARE)

Building block 1: Data on the impact of cyber incidents

Building block 3: Measures and systems

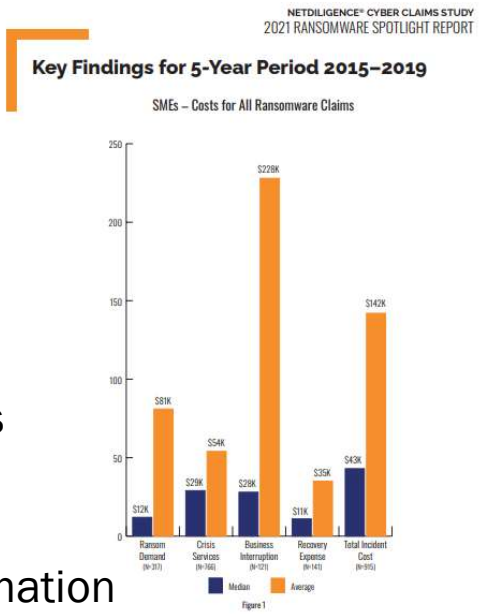
Building block 2: Data on likelihood and attack vectors



BUILDING BLOCK 1: IMPACT ON BUSINESS

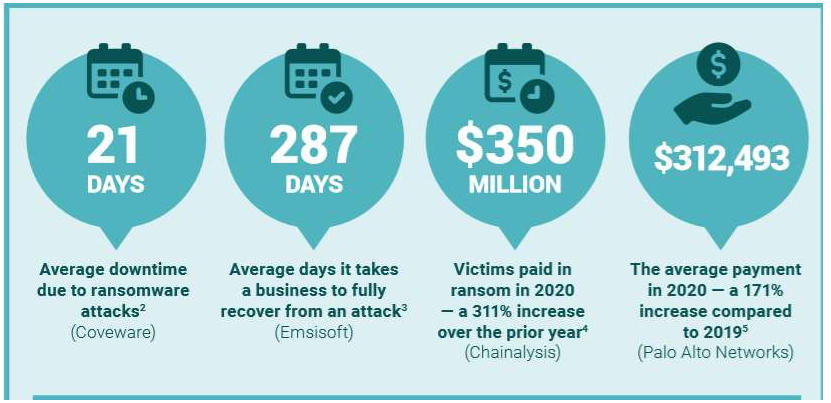
Different impact categories

- Financial
  - Crisis services
  - Operational costs (down-time)
  - Recovery services
  - Ransom paid
  - Costs of data breaches
  - …
- Reputation
- Safety
- Environment
- …



Data sources:

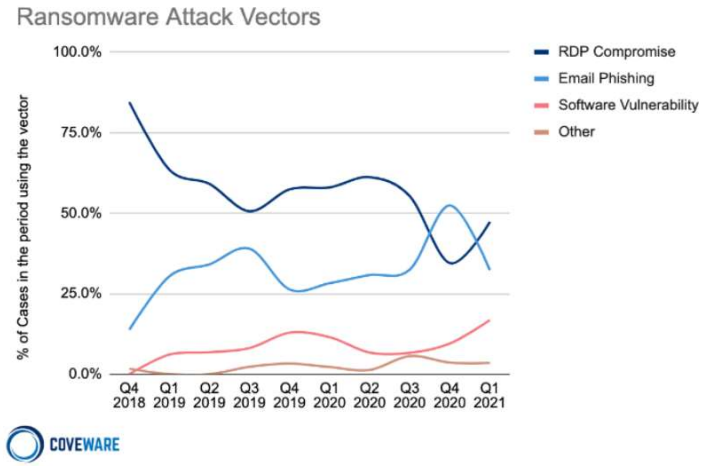
- Incident reports
- Insurance data
- Security companies
- Open sources
- Sensor data
- Sector based information



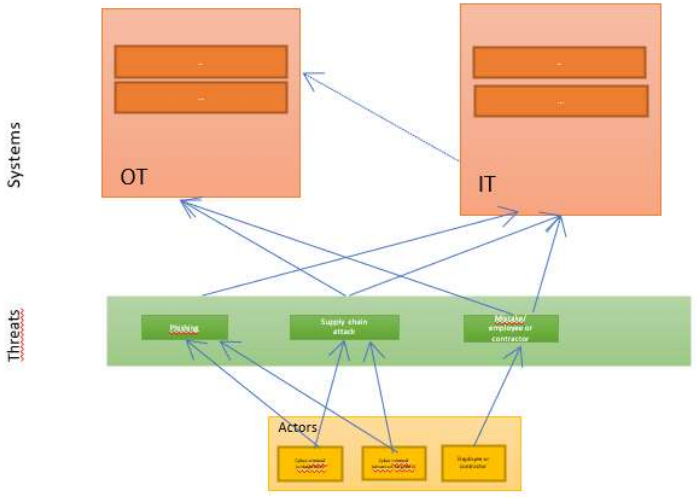
Gegevens VS 2020,
bron: taskforce ransomware

BUILDING BLOCKS 2: THREAT SCENARIO / 3: SYSTEMS

- Data on threats
  - Attack vectors
  - Data on frequency and trends



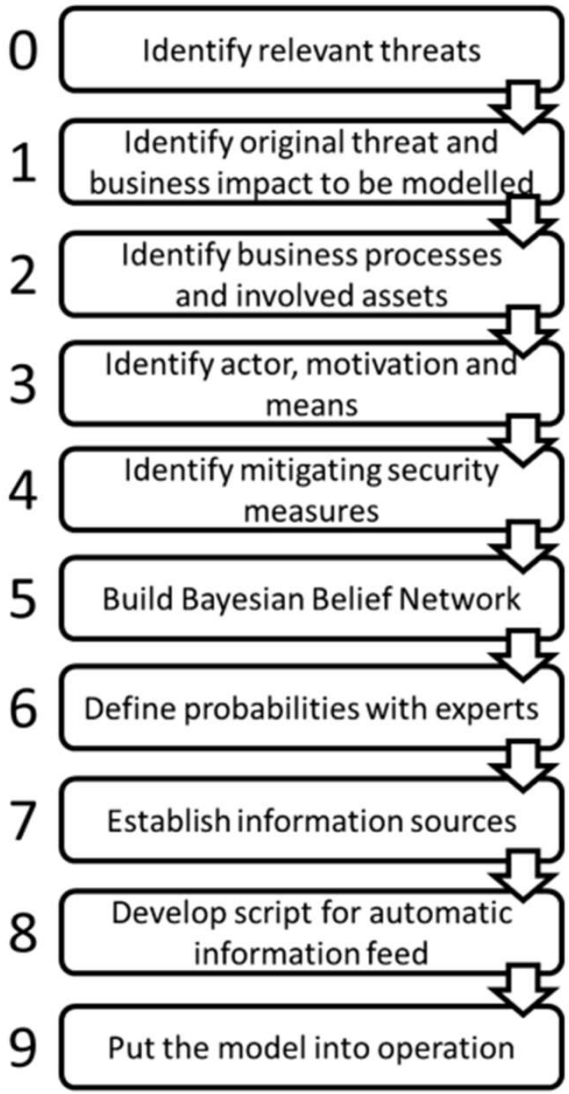
- Possible attack paths within an organisations own infrastructure
  - OT and IT networks and systems
  - (Digital) Architecture



METHODOLOGY APPLIED WITH CASE STUDIES

INTRODUCTION QUANTIFYING METHODOLOGY

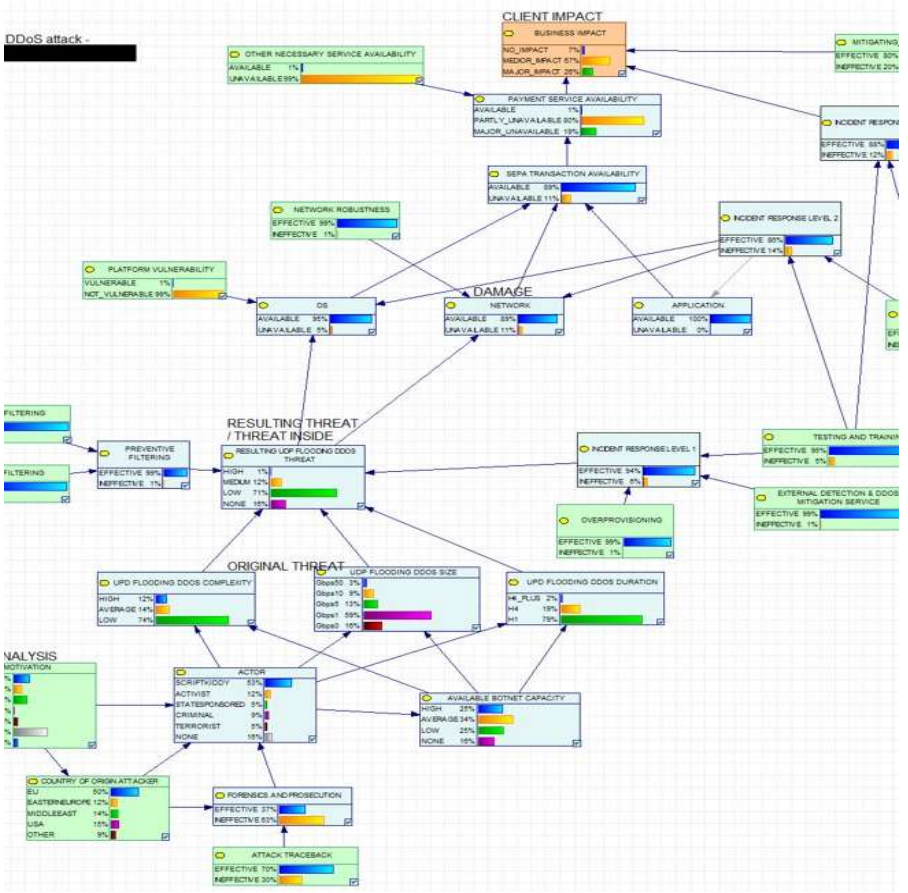
- In order to determine the quantitative risks in the case study, we applied a methodology which was developed in the Shared Research Programme Cybersecurity* a partnership between TNO, ABN AMRO, ING, Rabobank, de Volksbank and Achmea (see: https://www.tno.nl/srpcybersecurity).
  - Risk-based
  - Probabilistic model



*This research programme was the predecessor of the current Partnerchip for Cyber Security Innovation (PCSI, zie https://pcsi.nl/)

INTRODUCTION QUANTIFYING METHODOLOGY

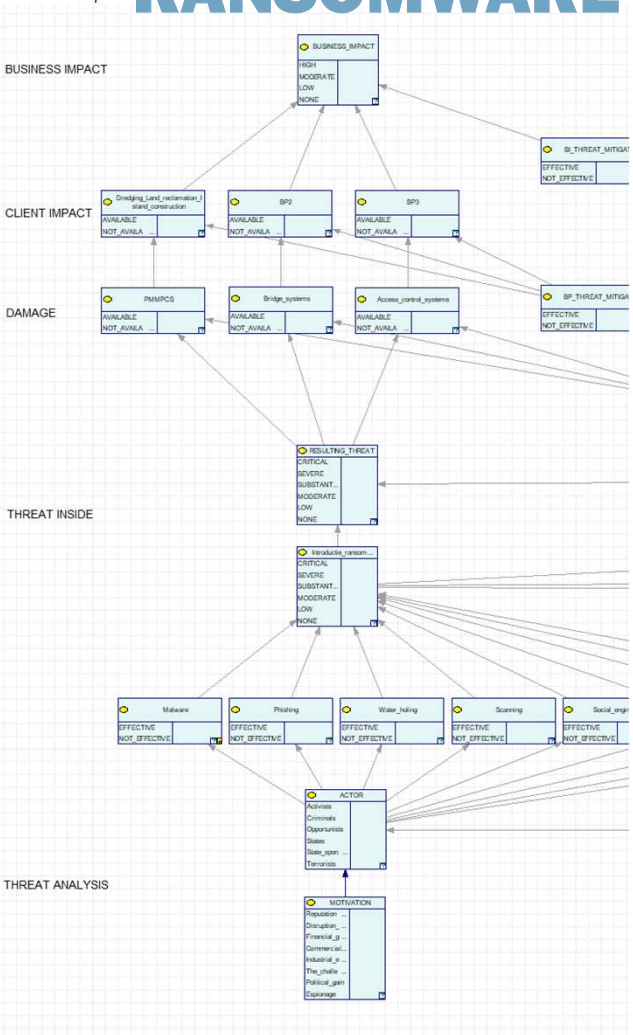
- In order to determine the quantitative risks in the case study, we applied a methodology which was developed in the Shared Research Programme Cybersecurity* a partnership between TNO, ABN AMRO, ING, Rabobank, de Volksbank and Achmea (see: https://www.tno.nl/srpcybersecurity).
  - Risk-based
  - Probabilistich model
- From input (green) to business impact (orange)



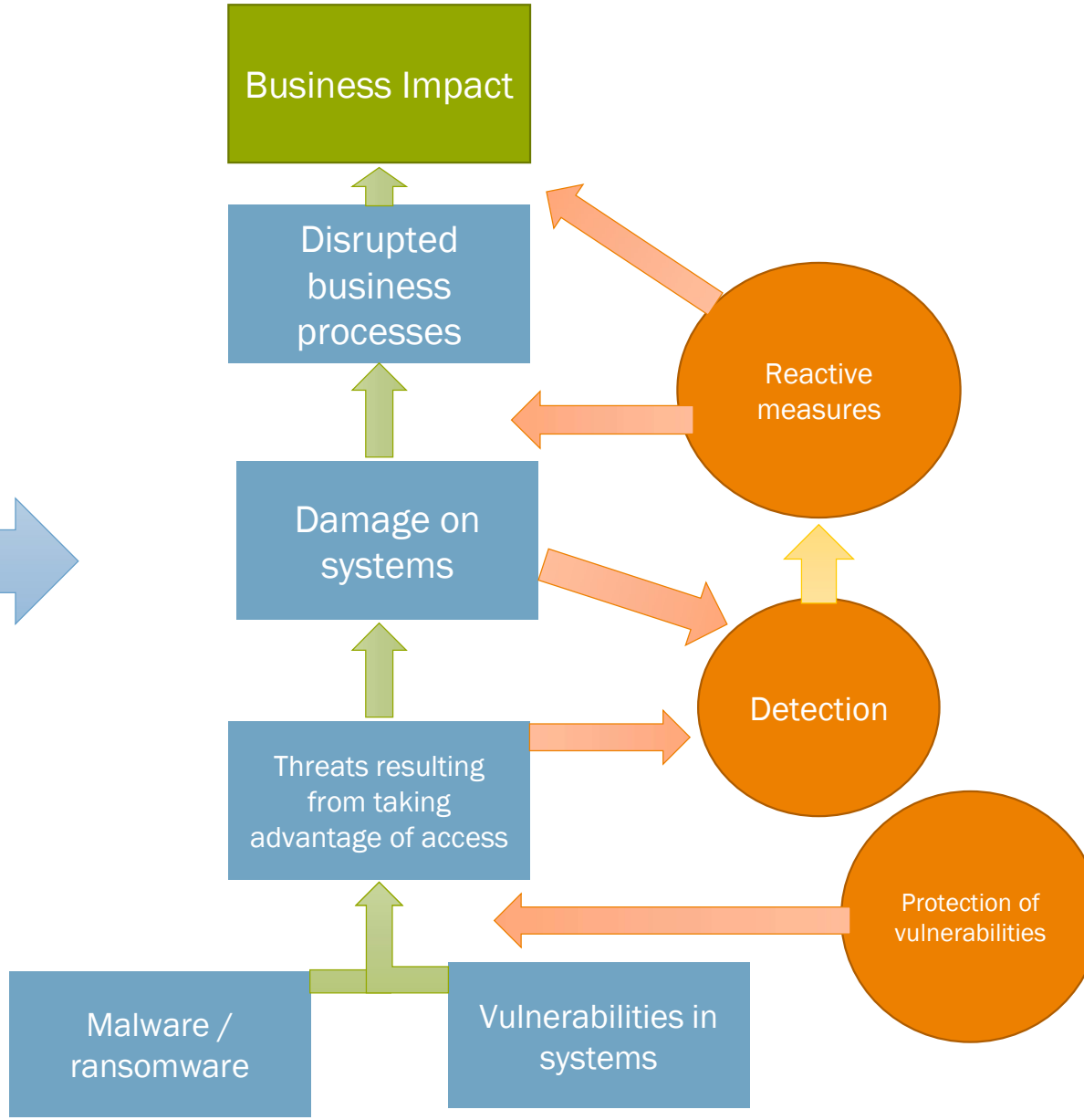
0 Identify relevant threats
1 Identify original threat and business impact to be modelled
2 Identify business processes and involved assets
3 Identify actor, motivation and means
4 Identify mitigating security measures
5 Build Bayesian Belief Network
6 Define probabilities with experts
7 Establish information sources
8 Develop script for automatic information feed
9 Put the model into operation

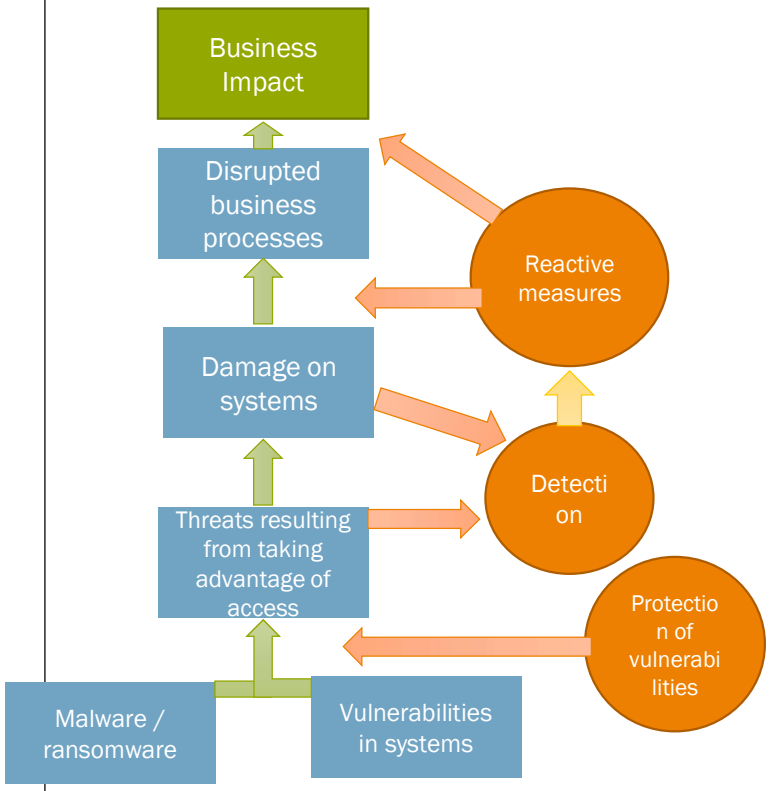
*This research programme was the predecessor of the current Partnerchip for Cyber Security Innovation (PCSI, zie https://pcsi.nl/)

FOCUS CASE STUDIES: RANSOMWARE

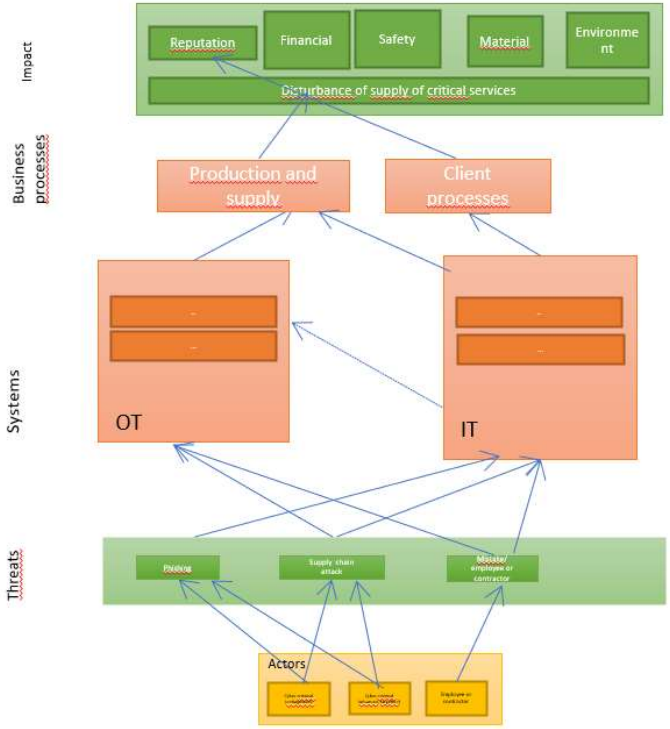


Interpretation model for our use case



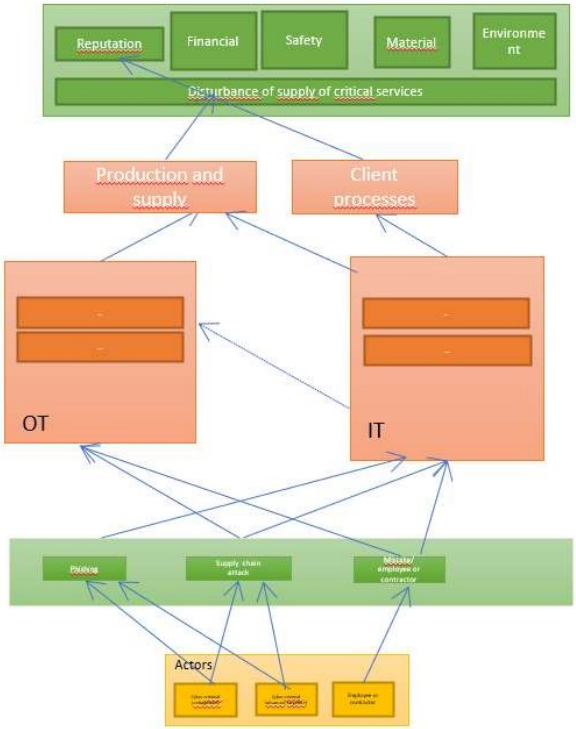


Together with experts, we refine the model

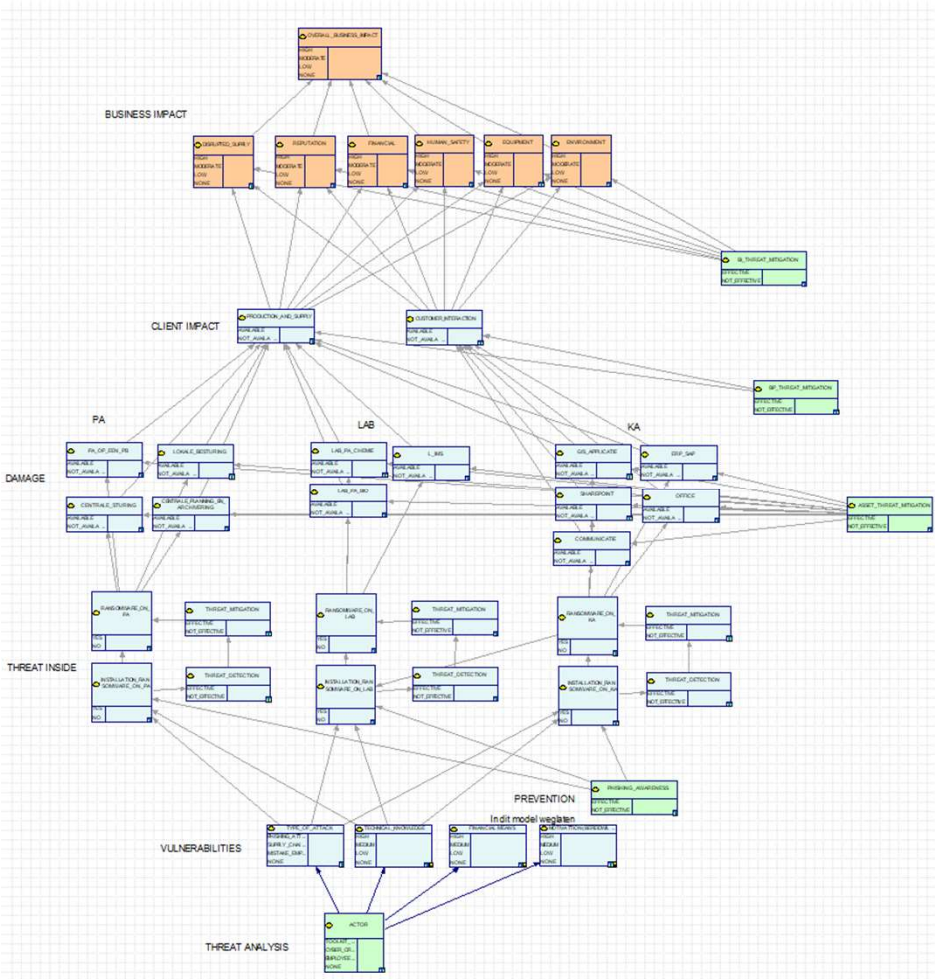


RESULTING MODEL

RESULT OF CASE STUDY: RANSOMWARE MODEL



Turn the model into a Bayesian Belief Network

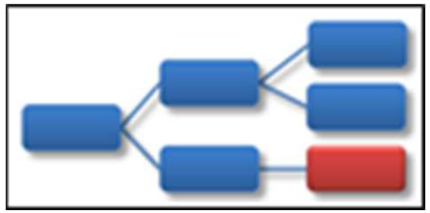


TYPES OF VARIABLES IN THE MODEL
INPUT, ANALYSIS, GOAL

- Input
  - In the model, these variables don’t have ‘parents’
  - Parameters have to be filled out by the user

- Analysis
  - Have both 'parent’ and 'child' variables
  - ‘Probability table’ determines relation from input ‘parent(s)’ to output 'child'

- Goal
  - Terminus of the model, de variable that you want to determine (e.g. Impact)
  - ‘Probability table’ determines influence of 'parent' variabele(s)



EXAMPLE INPUT VARIABELE
PHISHING AWARENESS

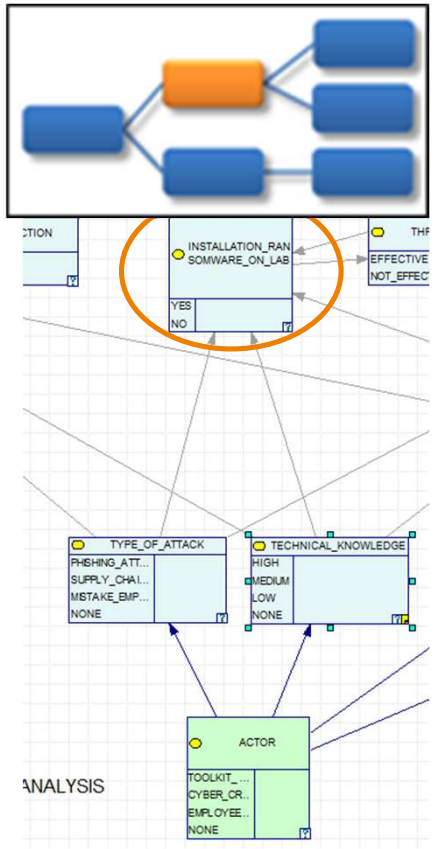
- What is the likelyhood of an employee not falling for a phishing scam

Phishing awareness	Probability
Effective	30 %
Not_effective	70 %

EXAMPLE ANALYSIS VARIABELE
INSTALLATION OF RANSOMWARE

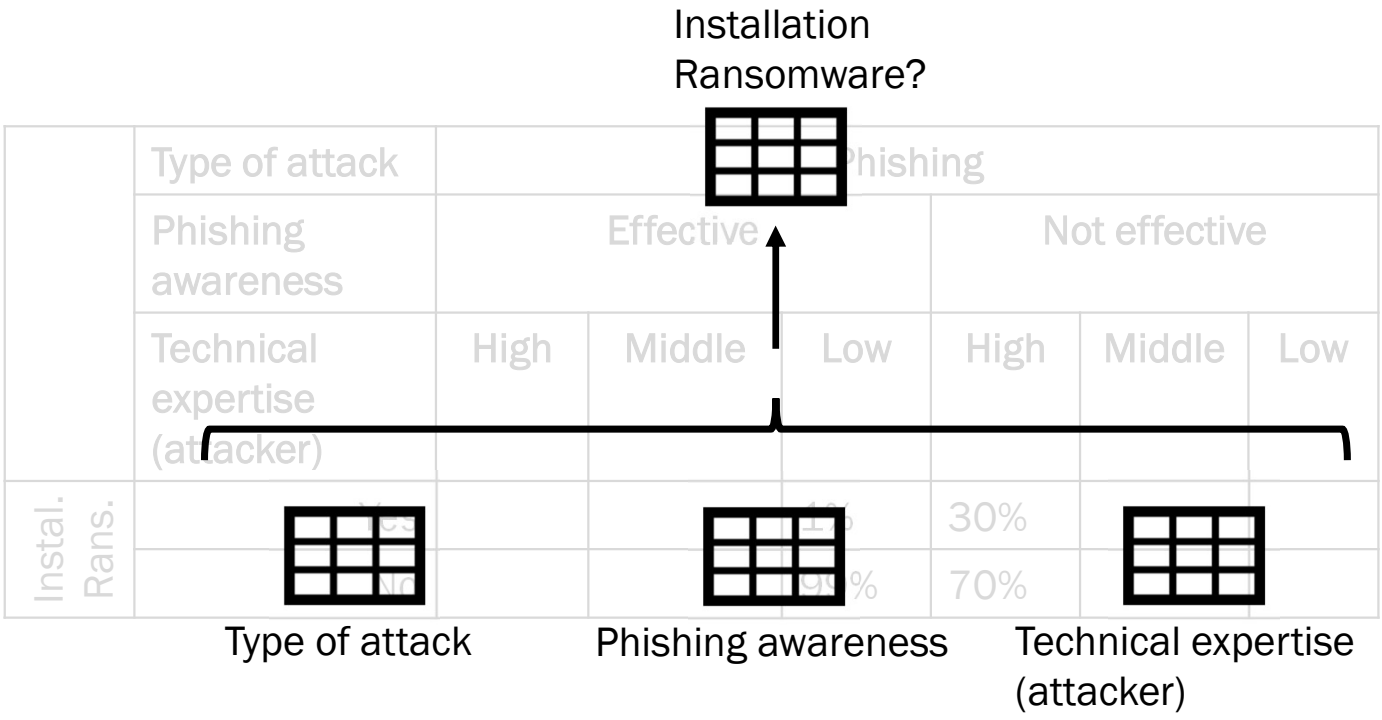
- Given a specific type of attack, what is the probability of the successful installation of ransomware?

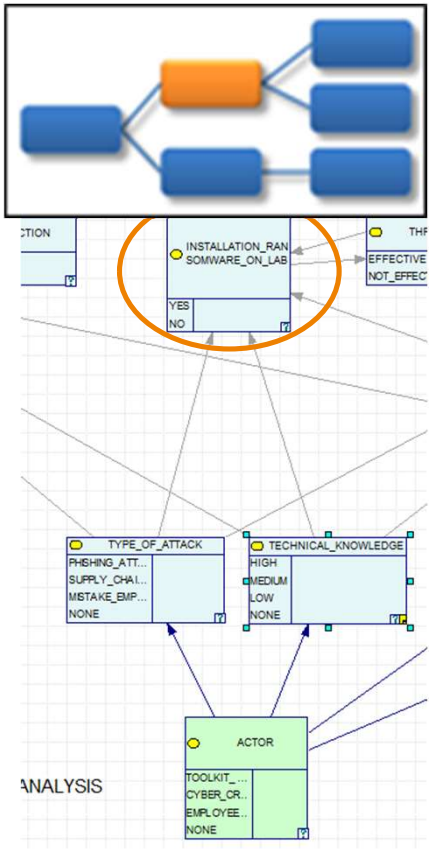
	Type of attack	Phishing					
	Phishing awareness	Effective			Not effective		
	Technical expertise (attacker)	High	Middle	Low	High	Middle	Low
Instal. Rans.	Yes			1%	30%		
	No			99%	70%		



EXAMPLE ANALYSIS VARIABELE
INSTALLATION OF RANSOMWARE

- Given a specific type of attack, what is the probability of the successful installation of ransomware?





OUTPUT

The acquired model can be used in multiple ways!

- Determine the probability distribution of one or more goal nodes
  - Straightforward calculation of probable states based on input
- Given the actual end state, what was the likely input state?
  - In case of a certain actual impact, what was the likely attack path? (actor, type of attack, …)
- Sensitivity analysis
  - What if…?
  - Is it worthwhile to invest in certain measures? Or do they barely have any effect?
  - Is it crucial to understand parts of the model in more detail? Or do they have limited bearing on the output?

HANDLING DYNANICS IN CYBER RISK

DISEM INSTITUTE

A system dynamics approach

System Behaviour Paradigm

The *observed behaviour* of any eco-system is a function of the operational *structure* that drives it *(Paich 2009):*

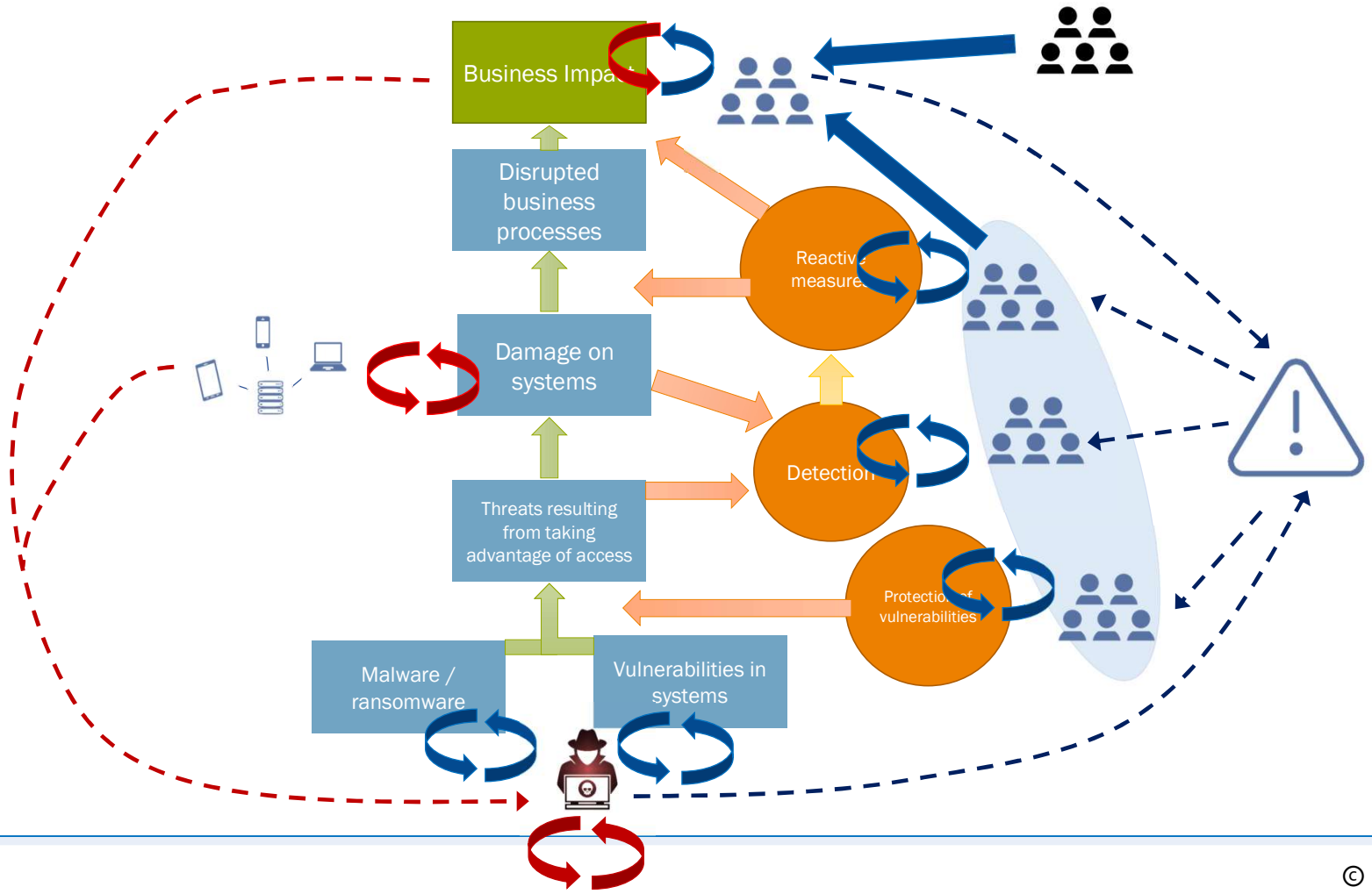
- *What eco-system structure (feedback, accumulation and time delays) drives its outcome of interest (behavior over time)?*
- *How can we influence this structure (what policies) ?*

Security strategies and programs are significantly affected by *the dynamic nature of cyber risk*.

Examples are:

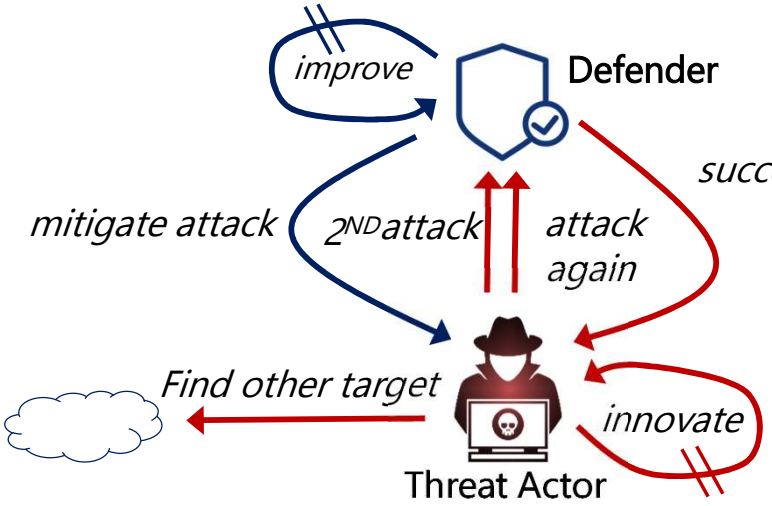
- Evolving attacker tactics
- Changing organizational characteristics
- Limits to resource availability
- Emerging impact of incident response and recovery
- Etc.

Dynamics: attacker - defender interaction & response



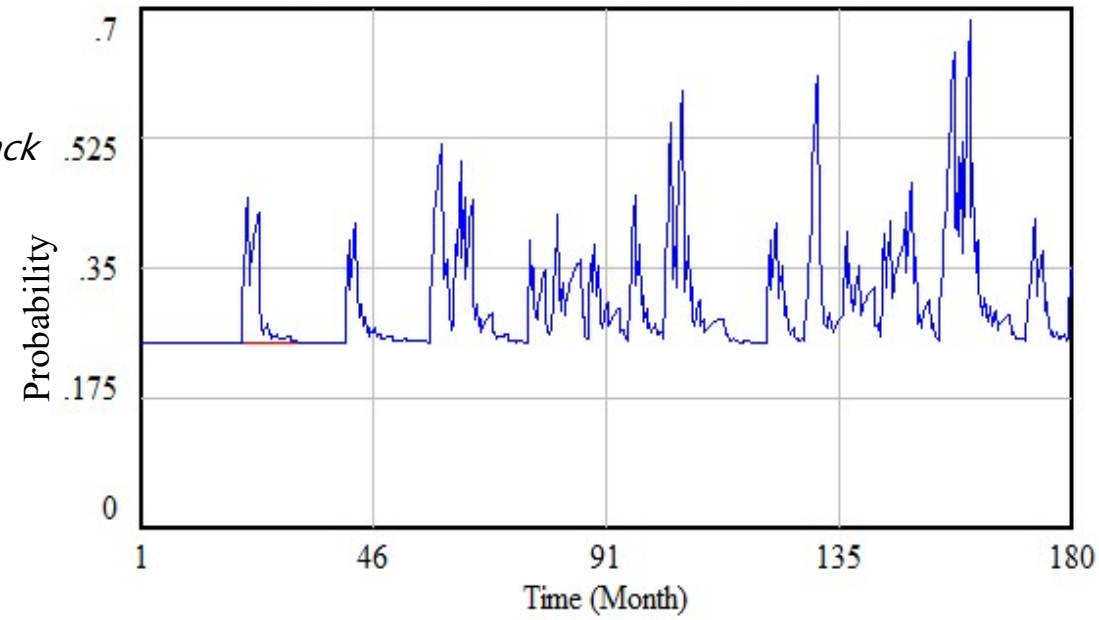
Example: attacker's behavior: structure and behavior

Structure

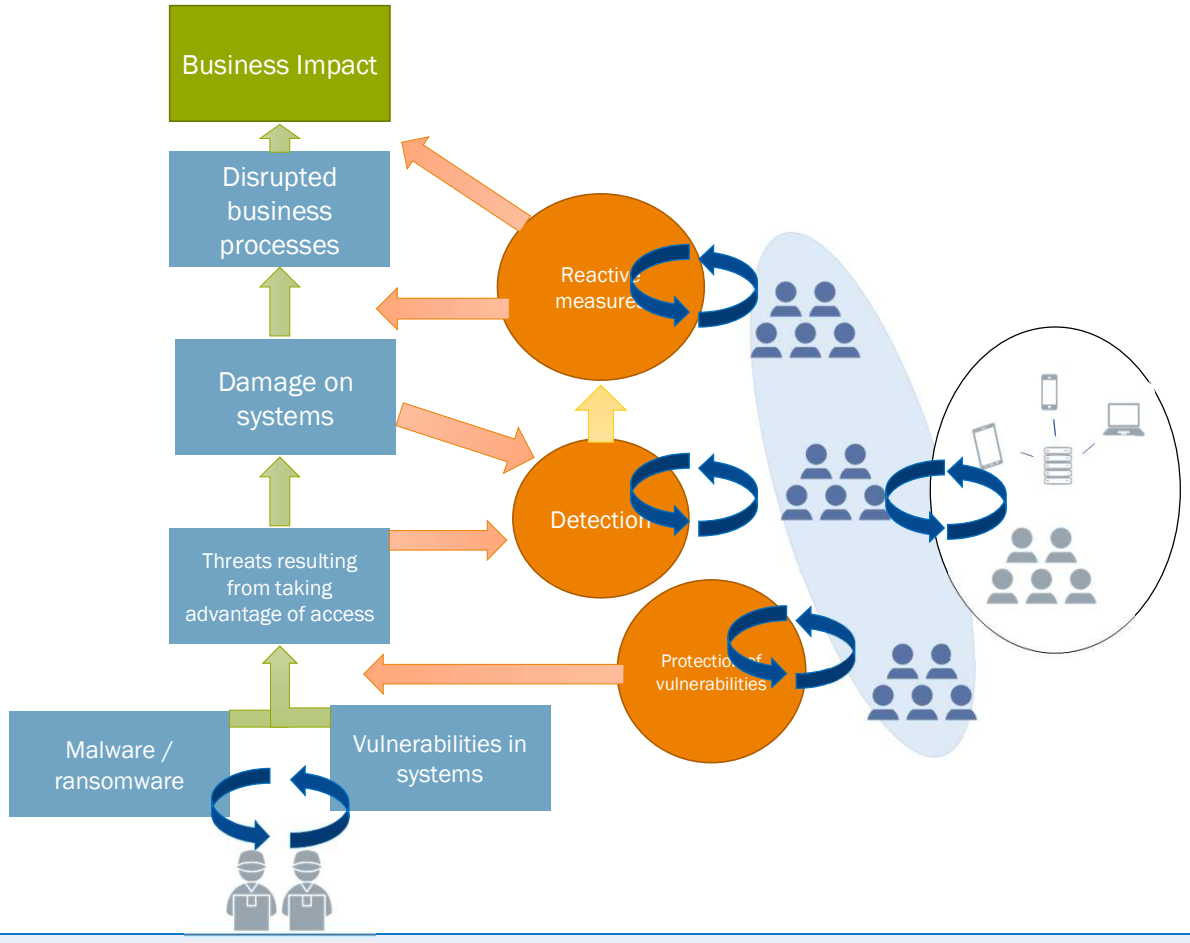


Behavior

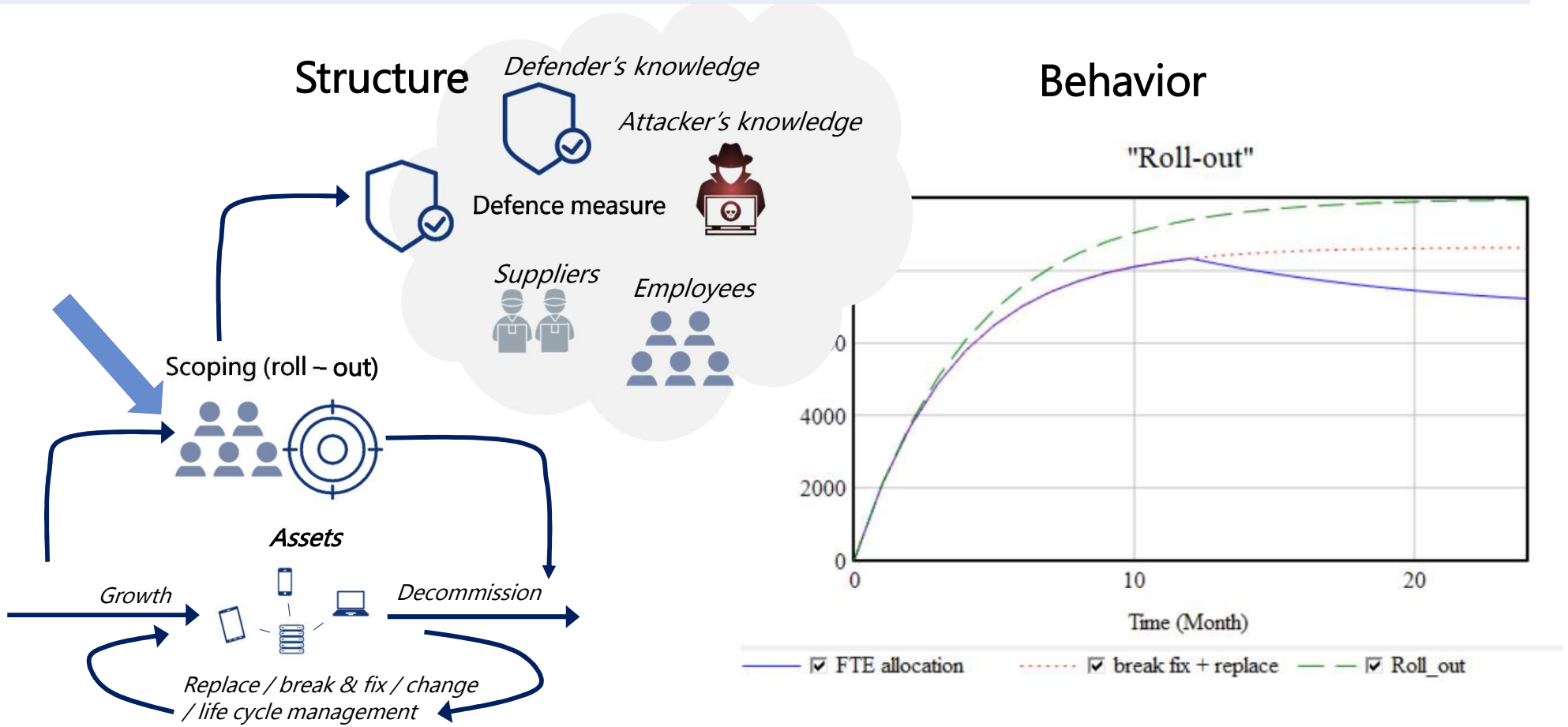
DDOS attack probability graph



Dynamics: changing organization: suppliers, asset base, insiders



Example: security capability roll-out: structure and behavior



(Zeijlemaker 2016)

Why using a system dynamics approach?

Ultimately these dynamic effect *determine the success* security strategies and programs.

An system dynamics approach *accounts for these effects* by:

1) Providing explainable and understandable insights in the structures that causes these dynamics
2) Compute and simulate realistic future performance of relevant performance indicators while using these structures
3) Identifying relevant organizational levers that can influence these dynamics

CONCLUSIONS

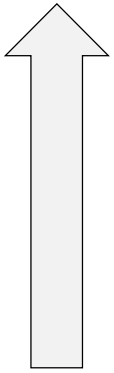
The contribution of cyber risk quantification

- Substantiate and rationalize cyber risks.
- Enable decision makers to prioritize cyber risks amongst other risks.
- Give credence to cyber-security strategy and program.

Cyber risk quantification: Bayesian Belief Networks (BBN) and System Dynamics (SD) complement and reinforce each other

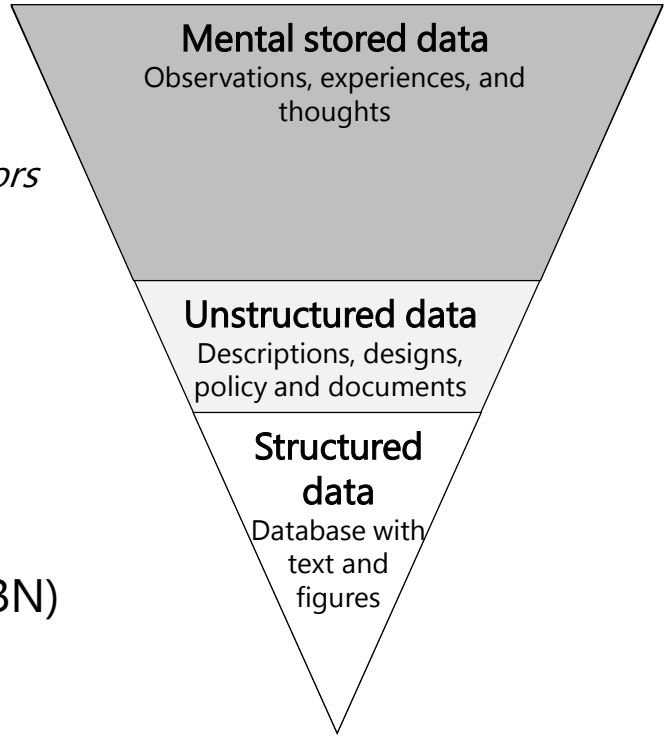
System Dynamics (SD)

- *Long term outlook*
- *Behavior of performance indicators*



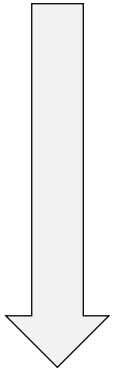
Bayesian Belief Networks (BBN)

- *Address uncertainty*
- *Near real-time*



System Dynamics (SD)

- *Use knowledge about structure*
- *Generate relevant data*



Bayesian Belief Networks (BBN)

- *Sensitivity analysis*
- *Probability state and probable attack paths*

NEXT STEPS

Research project NCSC and TNO

- Finalise and describe approach and models
- Explore inclusion of models and tools in processes NCSC
- Stimulate data collection process


TNO innovation for life
© DISEM INSTITUTE
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid
THANK YOU