Information Security & Risk Management:
Trustworthiness and Human Interaction

RCIS 2022 TUTORIAL 19/5/2022

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883188

Tutorial Programme

- Part 1
  - Introduction
  - Cybersecurity – the basics (interactive poll)
- Part 2
  - Human Interaction Flows and HORM Charts
  - System Security Modeller (SSM) and attack paths
- Part 3
  - ‘Hands-on’ with system modelling, risk assessment and risk mitigation
  - Wrap-up

- You will need a laptop for this session

LEARNING OBJECTIVES

By the end of this session you will have gained:

- General understanding of cybersystems, risk assessment and management, trustworthiness and the importance of humans in the system.
- Specific knowledge of attack paths in system models
- Specific knowledge of human interaction flows
- Hands-on experience of using a system modeller and human interaction flow charts

Who we are:

Dr Stephen Phillips
s.c.phillips@soton.ac.uk

Dr Nic Fair
n.s.fair@soton.ac.uk

Dr Gencer Erdogan
gencer.erdogan
@sintef.no

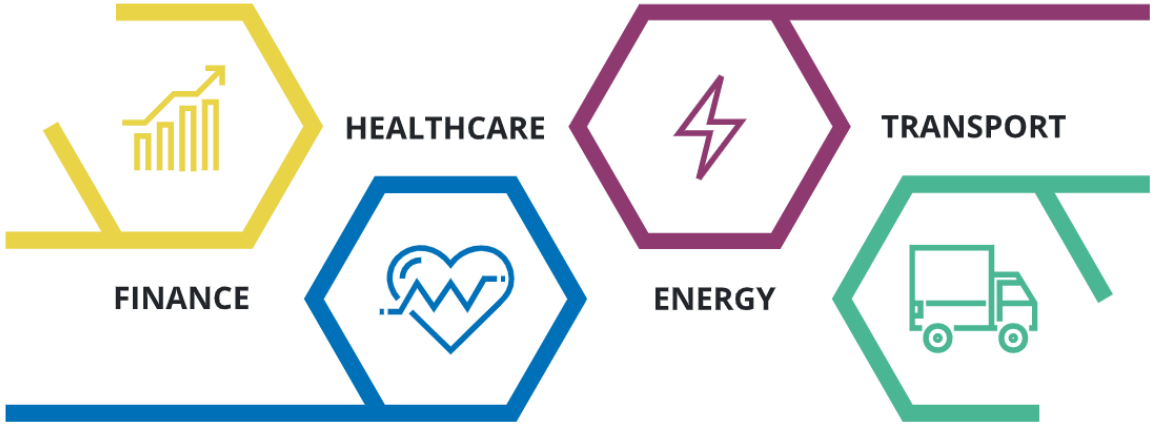
Mr Simeon Tverdal
simeon.tverdal
@sintef.no

CyberKit4SME

Democratizing a Cyber Security Toolkit for SMEs & MEs

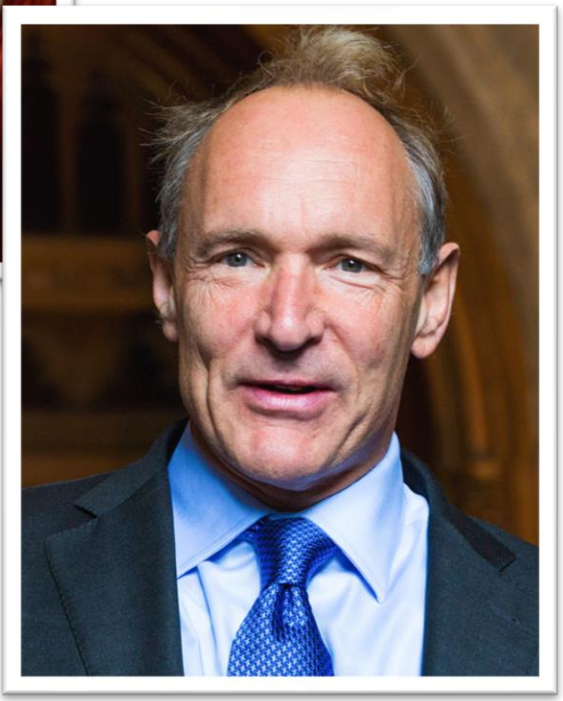
Helping SMEs and MEs analyse, forecast and manage cyber security and data protection risks.

https://cyberkit4sme.eu



Who are you?

- Have a short chat with your neighbours, explain:
- a little about you
- why you are interested in this workshop
- what you hope to get out of it
- what famous person (alive or not) you would like to have dinner with



Cybersecurity – the basics

PART 1 - RCIS 2022 TUTORIAL 19/5/2022

Question 1: Defining Cybersecurity

Cybersecurity is often confused with information security – which is mainly focussed only on data and prevention of criminal actions . But, *cybersecurity* includes all assets and entities (inc. people) as well as data within a cybersystem, and is focussed on threat reduction and mitigation as well as prevention.

- A cybersystem is a set of related entities that makes use of a cyberspace to form an integrated whole with a boundary to its surroundings.
- A cyberspace is a collection of interconnected computerized networks, including services, computer systems, embedded processors, and controllers, as well as information in storage or transit.
- A cyber-threat is a threat that exploits a cyberspace.
- Information security is the preservation of confidentiality, integrity, and availability of information.

Question 2:
Defining Cybersecurity Risk Assessment

Cybersecurity risk assessment is the process of identifying, estimating, analysing and evaluating cyber-risks.

(ISO 27005 formalises the steps as: Risk estimation, Risk analysis, Risk evaluation).

We can simplify this and say:

"By risk assessment we mean activities aiming to understand and document the risk picture for specific parts or aspects of a system or an organization.

The assessment includes the estimation of the risk level, as well as the identification of options for risk treatment.

The results serve as a decision basis for risk management, including the decision of which controls and measures to implement to mitigate risk". [1]

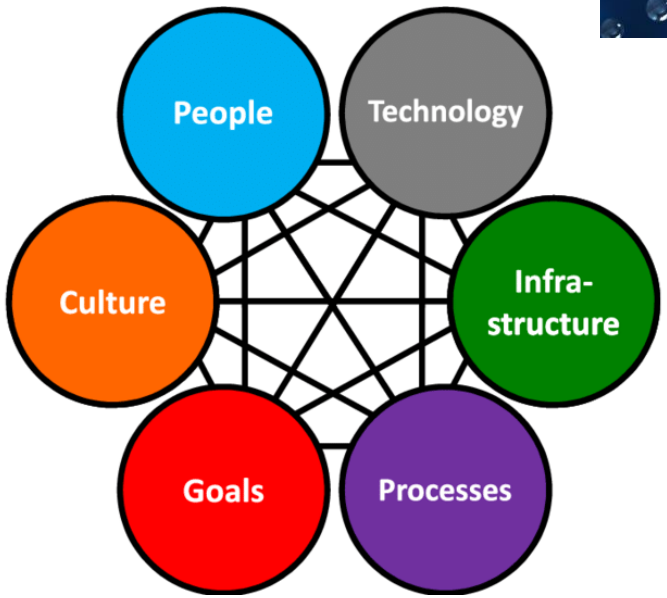
[1] Atle Refsdal, Bjørnar Solhaug, Ketil Stølen. Cyber-Risk Management. Springer, 2015.

Question 3:
What should be included in a Cybersecurity Risk Assessment

Many of the answers provided do not include HUMANS. Humans must be included in a cybersecurity risk assessment, because a cybersystem is in reality a **SOCIOTECHNICAL SYSTEM**

Sociotechnical systems ***"share an emphasis on interlinkages",*** in other words, they recognise the inseparability of all of the elements below (Geels, 2004; Borri & Grassini, 2014):

- material artefacts (technologies) and their use (societal functions)
- techniques & knowledge (development and diffusion of),
- networks of actors/people (including creators and users),
- institutions,
- socio-cultural norms,
- capital (financial, social, cultural…etc)
- standards, regulations & laws



Question 4:
Creating Trustworthy Cybersystems

There is no single correct answer here.

In fact, all these aspects are important in creating trustworthy cybersystems.

a. Transparency and explainability (of AI)
b. Accreditation (by a trusted third party)
c. Security (provable)
d. Simplicity, usability and functionality
e. Resilience (in face of disaster / war / pandemic)
f. Ethical, unbiased algorithms / system design
g. Accessibility and Inclusivity
h. Compliance with standards and regulations

Question 5:
Why humans matter in Cybersystems

There is no single correct answer here.

In fact, all these aspects are important in understanding the role of humans in a cybersystem.

a. Humans are normally the weakest link in a system
b. Technologies do not exist independently from their human designers, builders and users so can not be considered separately from humans (and societies)
c. Humans are unreliable, erratic, prone to mistakes, easily tricked, and often lack the necessary skills and literacies to make a system function optimally and safely
d. Human judgement is suspect and can be corrupted

Question 6:
System Modelling & Human Interaction Flows

By necessity, system models have to find the *balance between* enabling the modelling of a system in sufficient *detail*, while also supporting a level of *abstraction* (so that different systems can be modelled and analysed).

System models are *static in time* – a 'snapshot' of a system at a given moment.

A Human Interaction Flow also requires the same balance between detail and abstraction.

A Human Interaction Flow indicates the *'action-reaction'* or 'cause-effect' nature of human interactions over a period of time.

We are now going to explore Human Interaction Flows and System Modelling in more depth…

Human Factors & Attack Paths

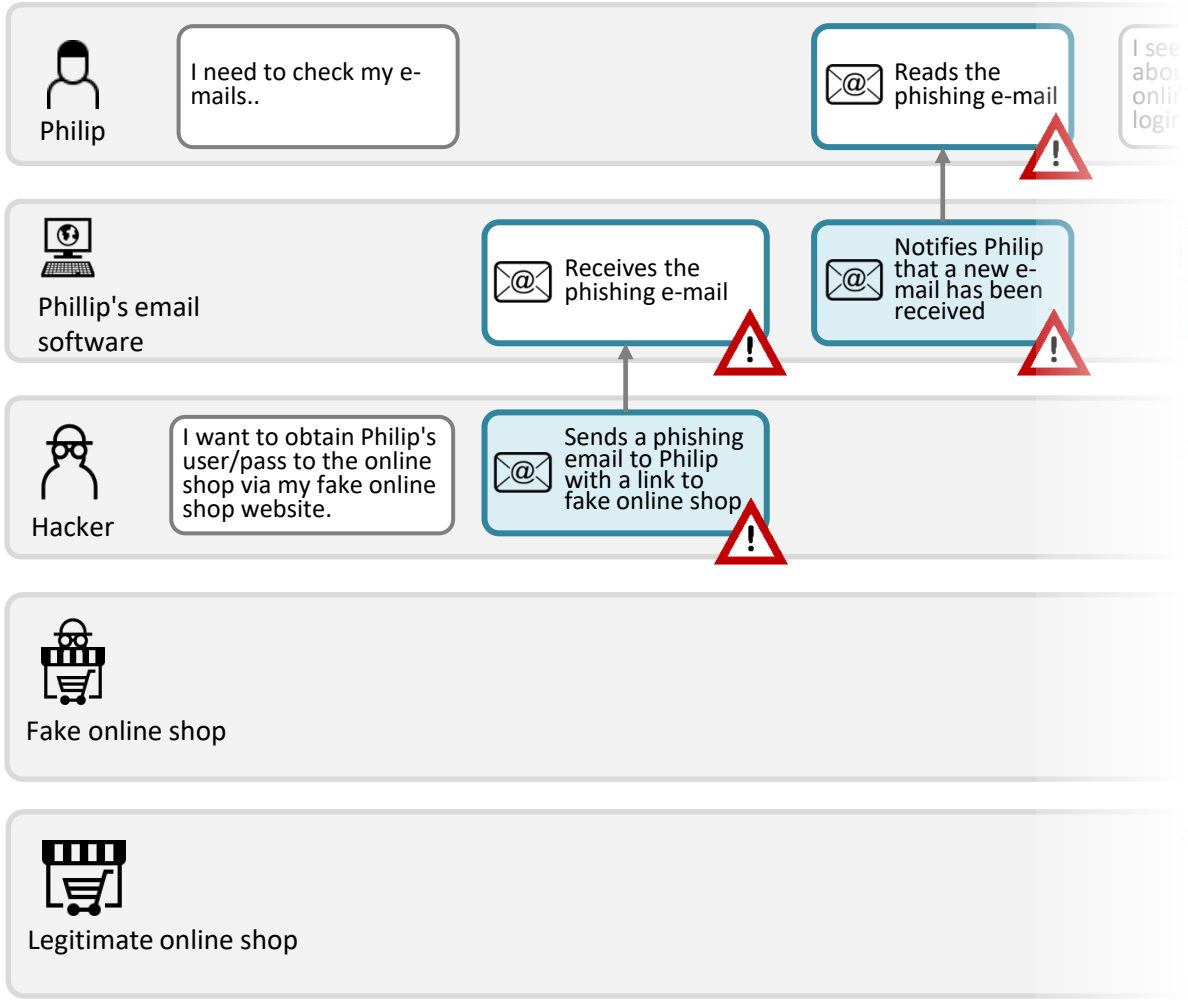
Threats to a System

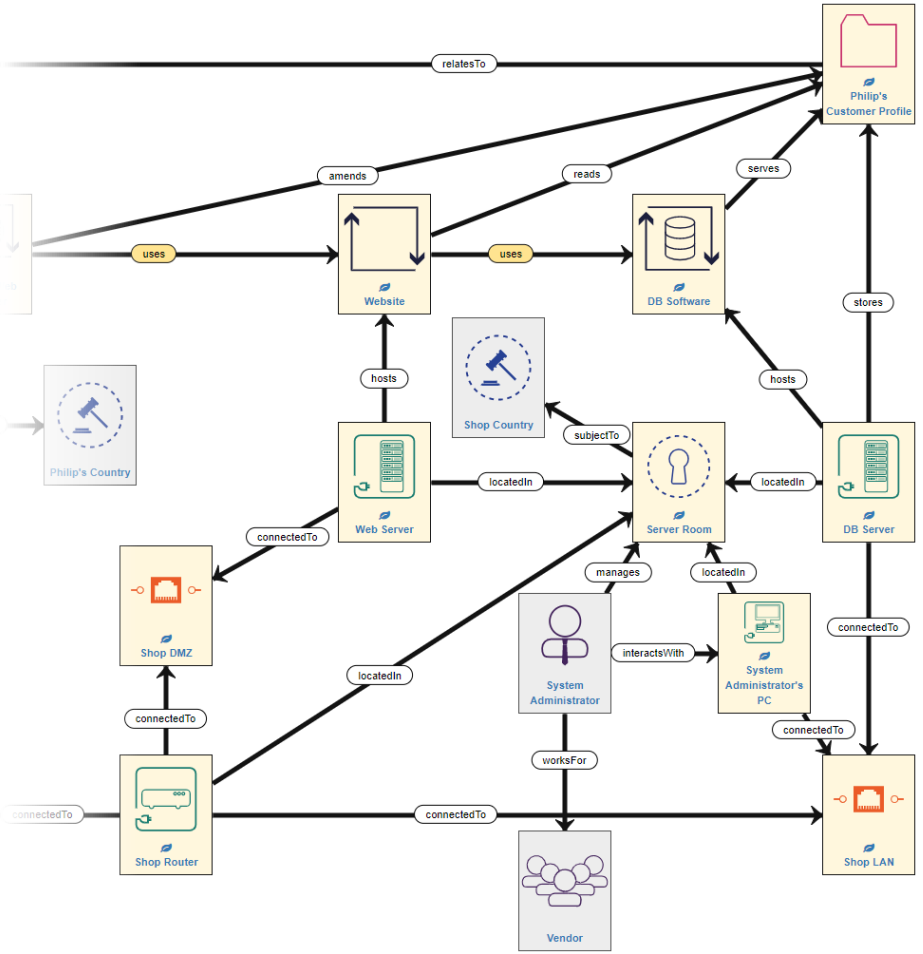
*"A threat has the potential to cause harm to assets such as information, processes and systems and therefore organizations. Threats may be of **natural or human** origin, and could be **accidental or deliberate**."*

--- ISO 27005

- Natural, accidental threats include:
  - Hardware failures
  - Software bugs
- Human threats include:
  - Deliberate: malicious actors
  - Accidental: people making mistakes
- We need to defend against all threats that may cause high risk consequences

Two Modelling Systems





Human Interaction Flows and HORM Charts

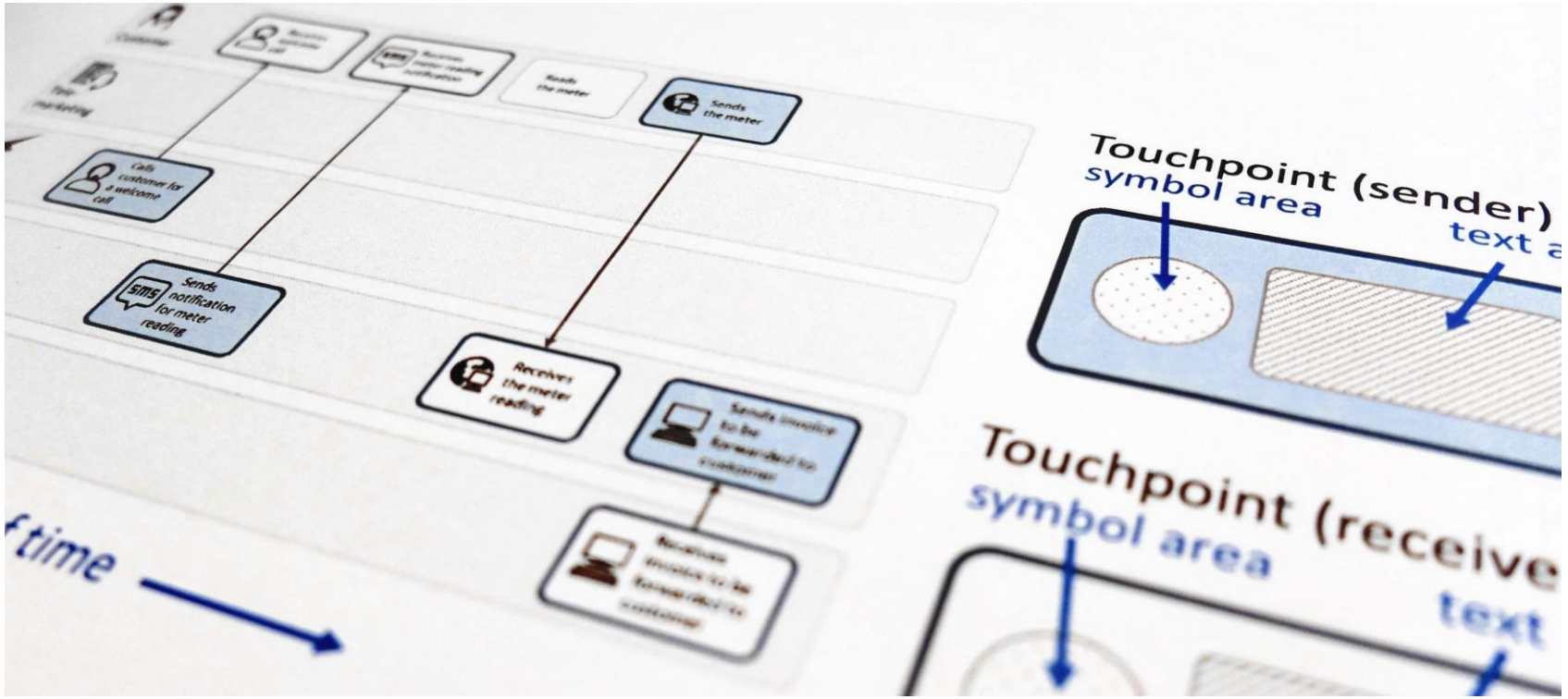
PART 2 - RCIS 2022 TUTORIAL 19/5/2022

Overview

- What is HORM?
  - A **H**uman and **O**rganizational **R**isk **M**odelling framework
  - Aim: to provide a comprehensible and easy to use framework for capturing risks ordinary people may be exposed to
- HORM consists of:
  - A modelling language based on Customer Journeys
  - A set of tools
  - A method
- An example phishing attack

HORM is based on CJML

CJML = Customer Journey Modelling Language



Customer journey

User journey

Employee journey

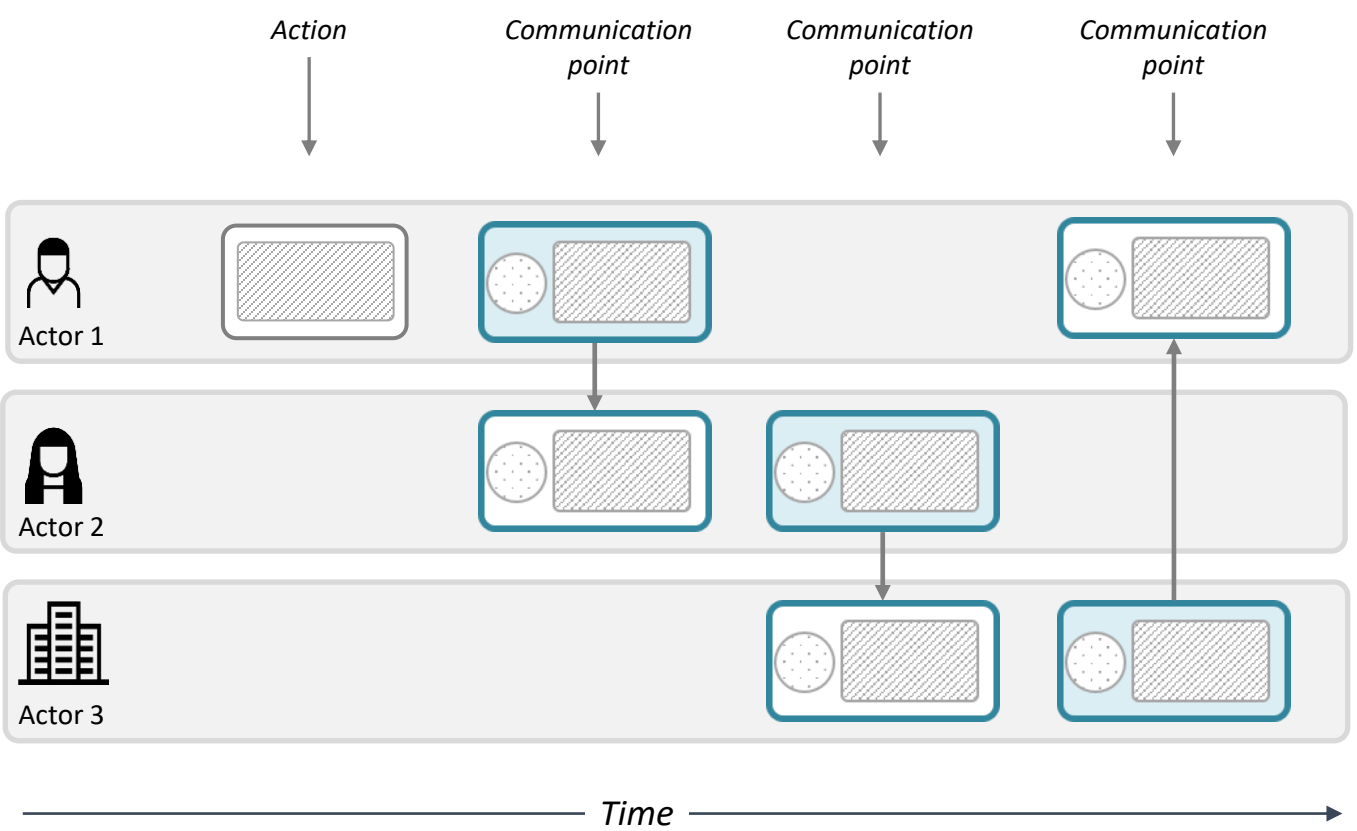
Patient journey

Citizen journey

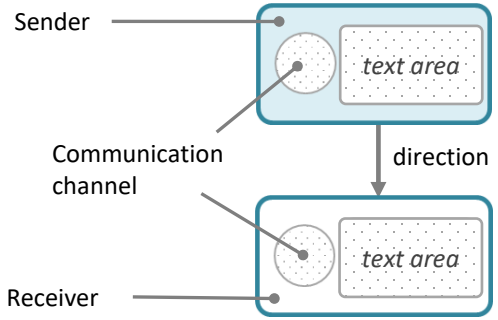
CJML is a visual language dedicated to modelling of customer journeys, human behaviour and digital service processes

Swimlane diagram – basic elements

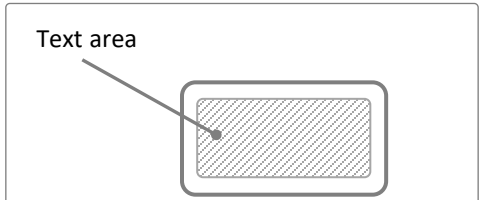
All the actors involved in the journey has a separate swimlane.



A communication point has a sender and a receiver that must be positioned in the corresponding swimlanes of the actors.



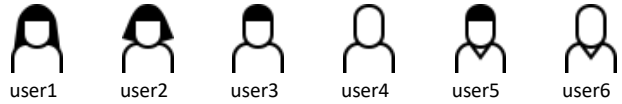
An action element is used for non-communicating events



Symbols

Actors

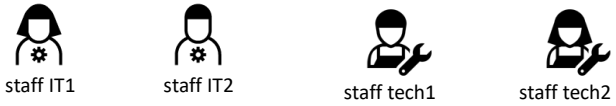
Users and customers



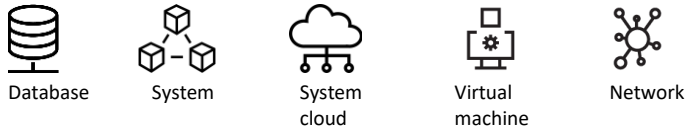
Service providers

Employee - general

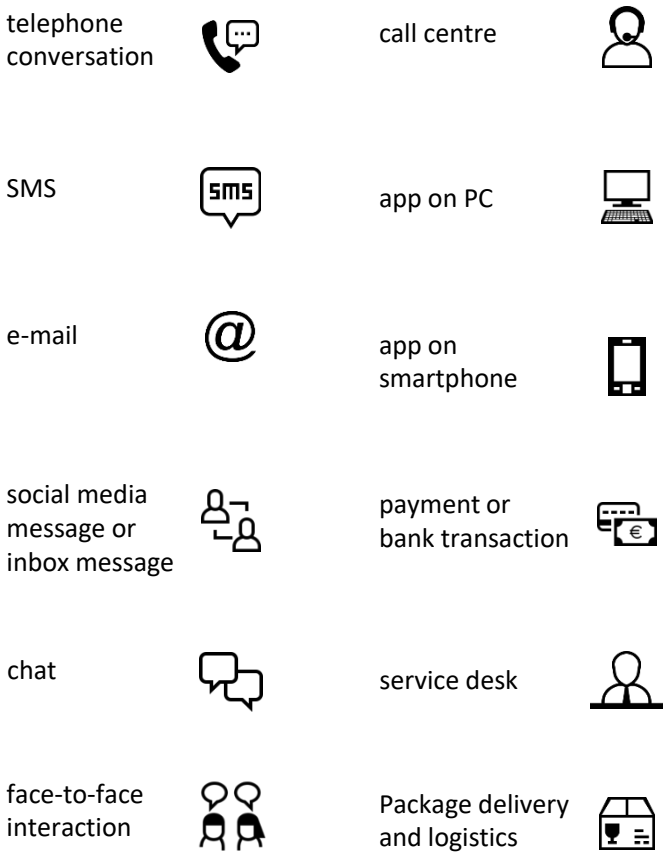
IT staff and technicians



Platforms and systems



Communication channels



Special symbols for cyber security

Cyber security experts

Attackers / malicious users

Special symbols

An example phishing attack

Philip is tricked to provide his login credentials to an online shop

- Philip often uses a popular online shop to purchase various goods.
- A hacker is aware that this online shop is very popular and decides to create a fake online shop that looks very similar to the original shop. However, when customers are asked to login via the fake online shop, the hacker logs their login credentials and simply provides an error message. This makes it look like there is something wrong with the webpage, in an attempt to make the user not think much of the failed attempt.
- The hacker needs to trick people to go to his webpage by convincing them that it is the original online shop webpage and ask them to log in. To accomplish this, the hacker constructs a very convincing email that asks the recipients to log in to the shop because of outstanding bills to pay. This is called a Phishing email.
- Finally, the hacker sends this phishing email to many random (email) recipients and waits for people to get tricked and provide their login credentials via the fake online shop.
- One of random victims is Philip, who believed that the email received is legitimate, He opens up the link provided in the phishing email and tries to login to the fake online shop. What happens instead, is that Philip is unknowingly providing his login credentials to the hacker.

Involved actors

Main actor

Philip

Other system actors

Phillip's email software

Legitimate online shop

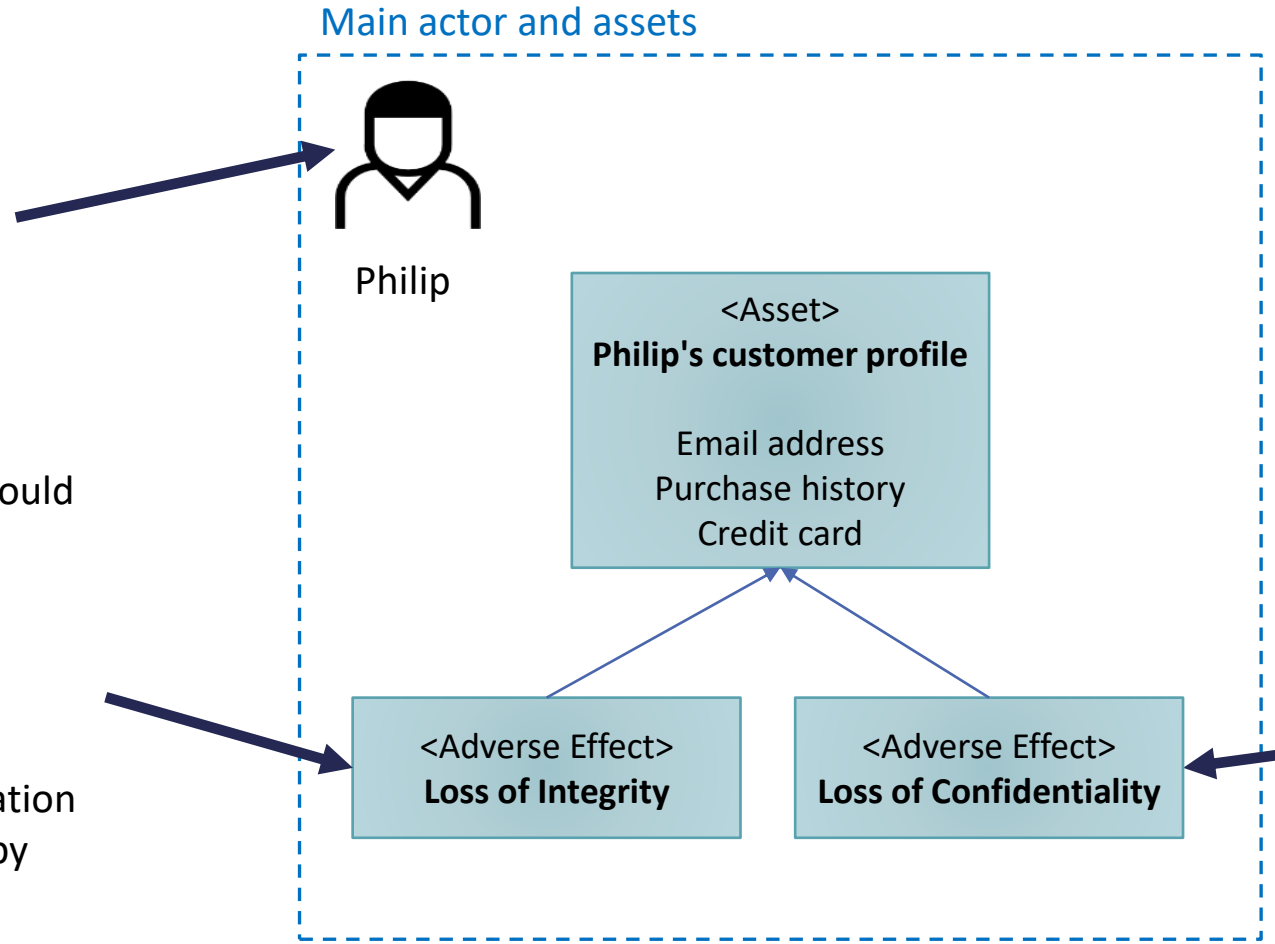
Malicious actors

Hacker

Fake online shop

Philip's assets

We want to assess the Phishing attack risk that Philip is exposed to



Another asset we would like to protect is the integrity of Philip's customer profile information

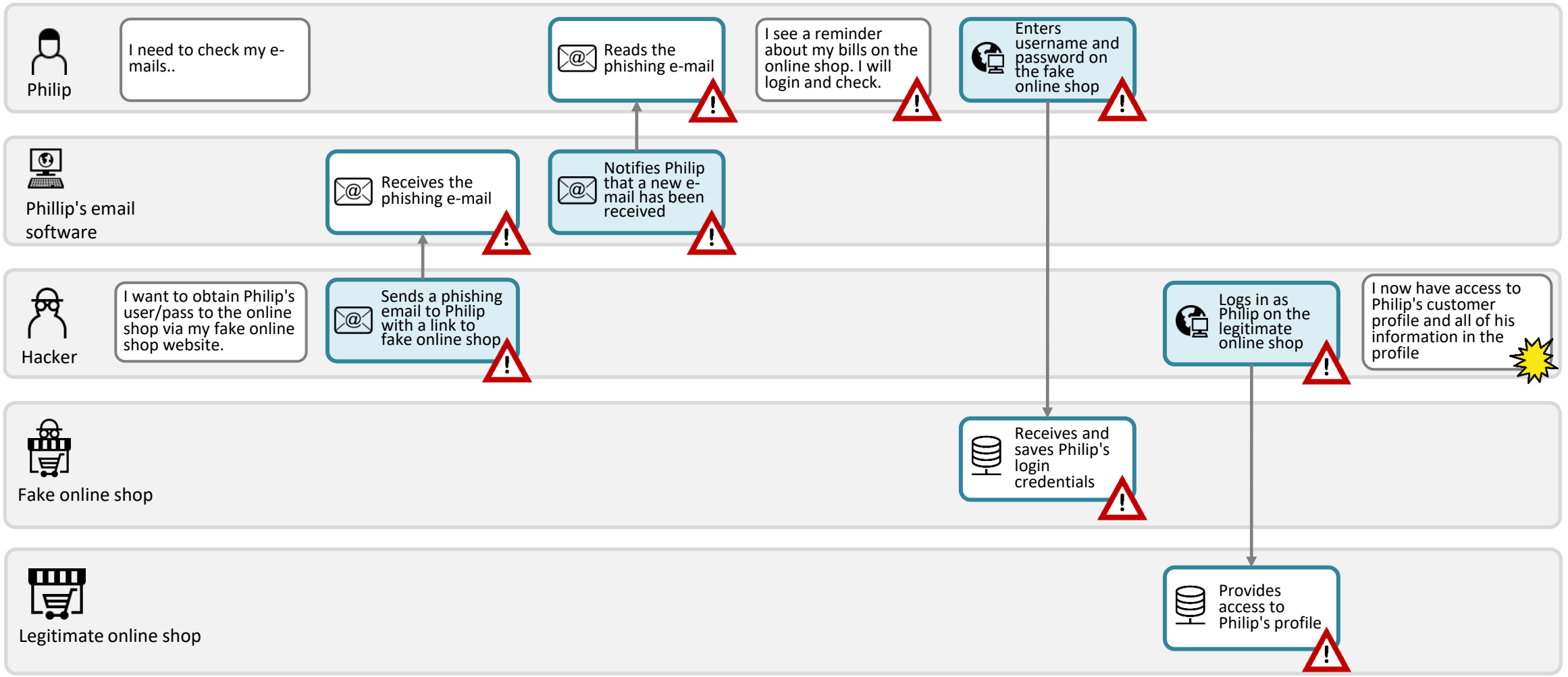
-Protect the information from being altered by unauthorized actors

We want to protect the confidentiality of Philip's customer profile on the online shop

-Protect the information from being accessed by unauthorized actors

Philip is exposed to a phishing attack

Philip's customer profile



System Security Modeller (SSM) and attack paths

PART 2 - RCIS 2022 TUTORIAL 19/5/2022

Open Source (soon!)

System Security Modeller

The SSM automates much of a cyber-security risk assessment. As well as looking for cyber threats it will also check for GDPR compliance.

It follows the process of **ISO 27005** and thereby supports **ISO 27001** compliance.

Value: Automation

Build a model of the assets and relations

Find the threats and their consequences

Both cyber-security and regulatory compliance

Calculate risks

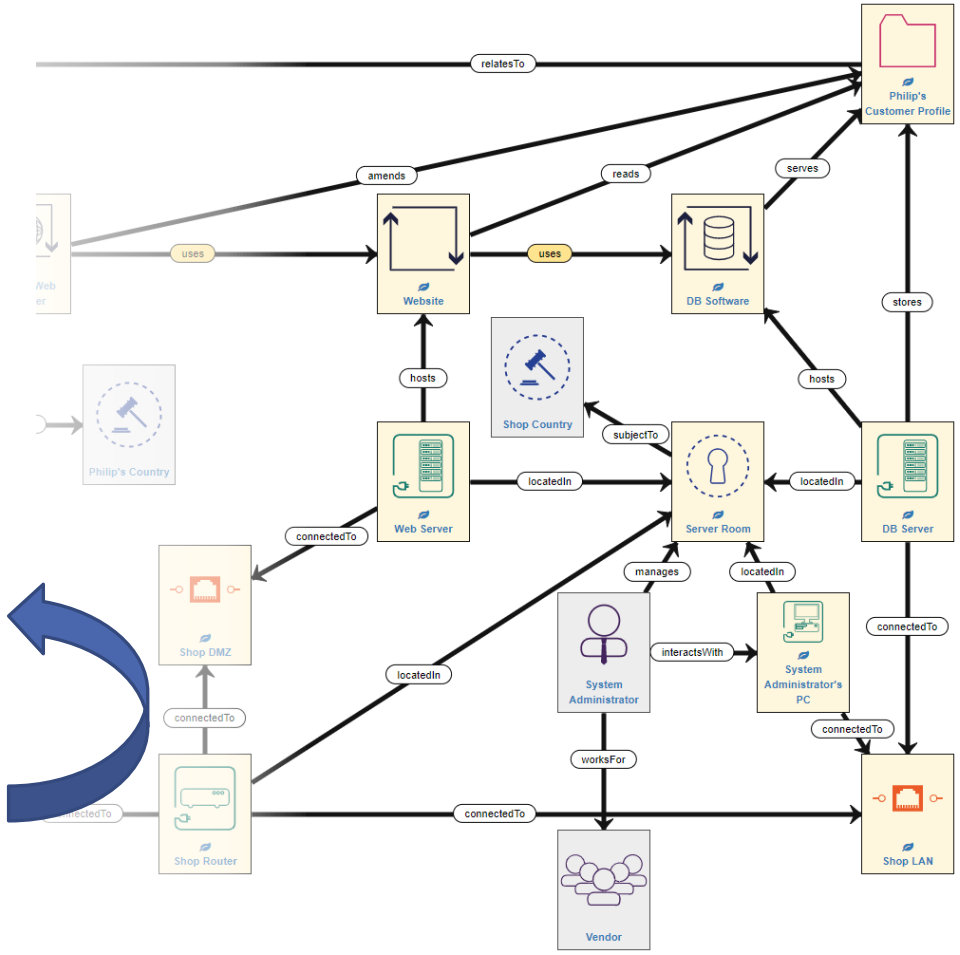
(Specified impact) × (Computed likelihood)

Select security controls from those proposed

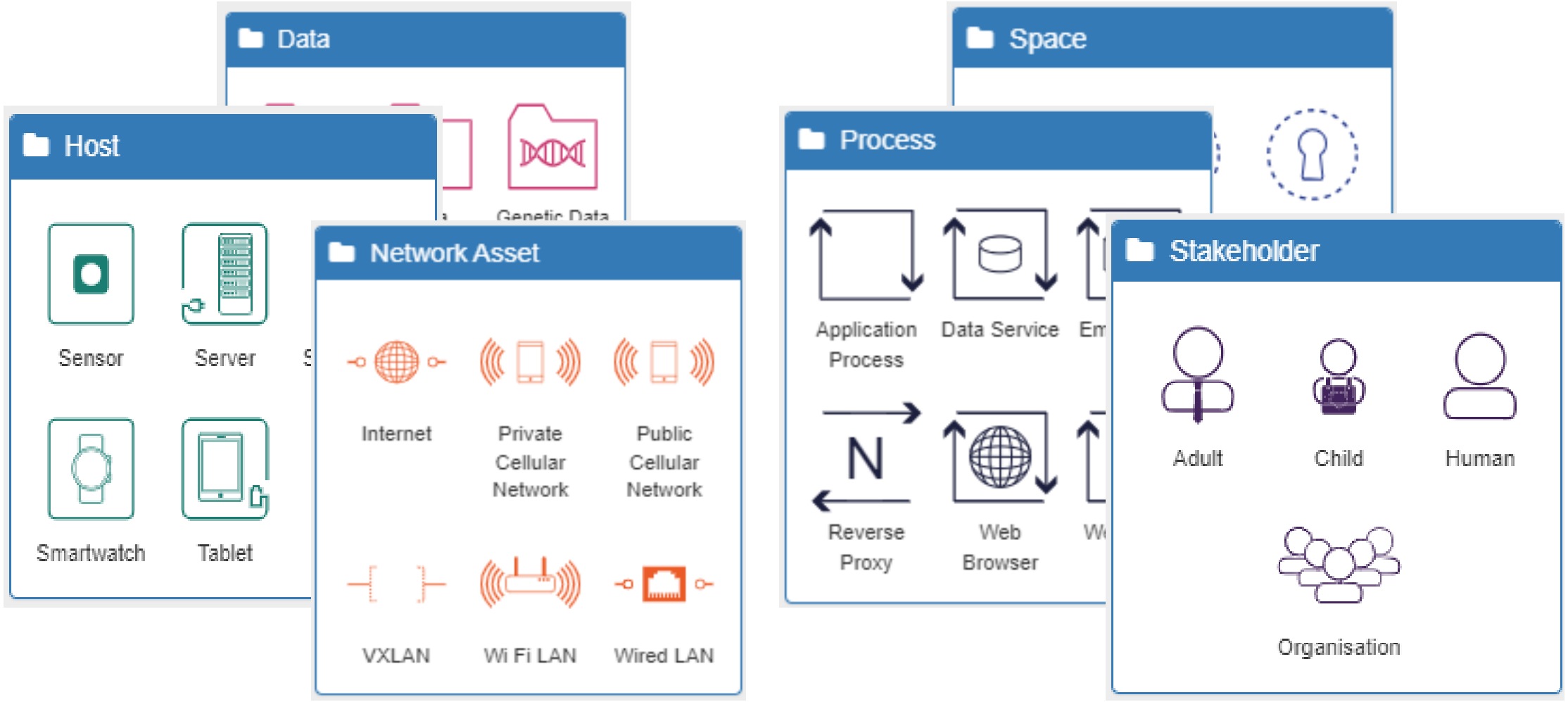
Security controls, policies, disable, re-design

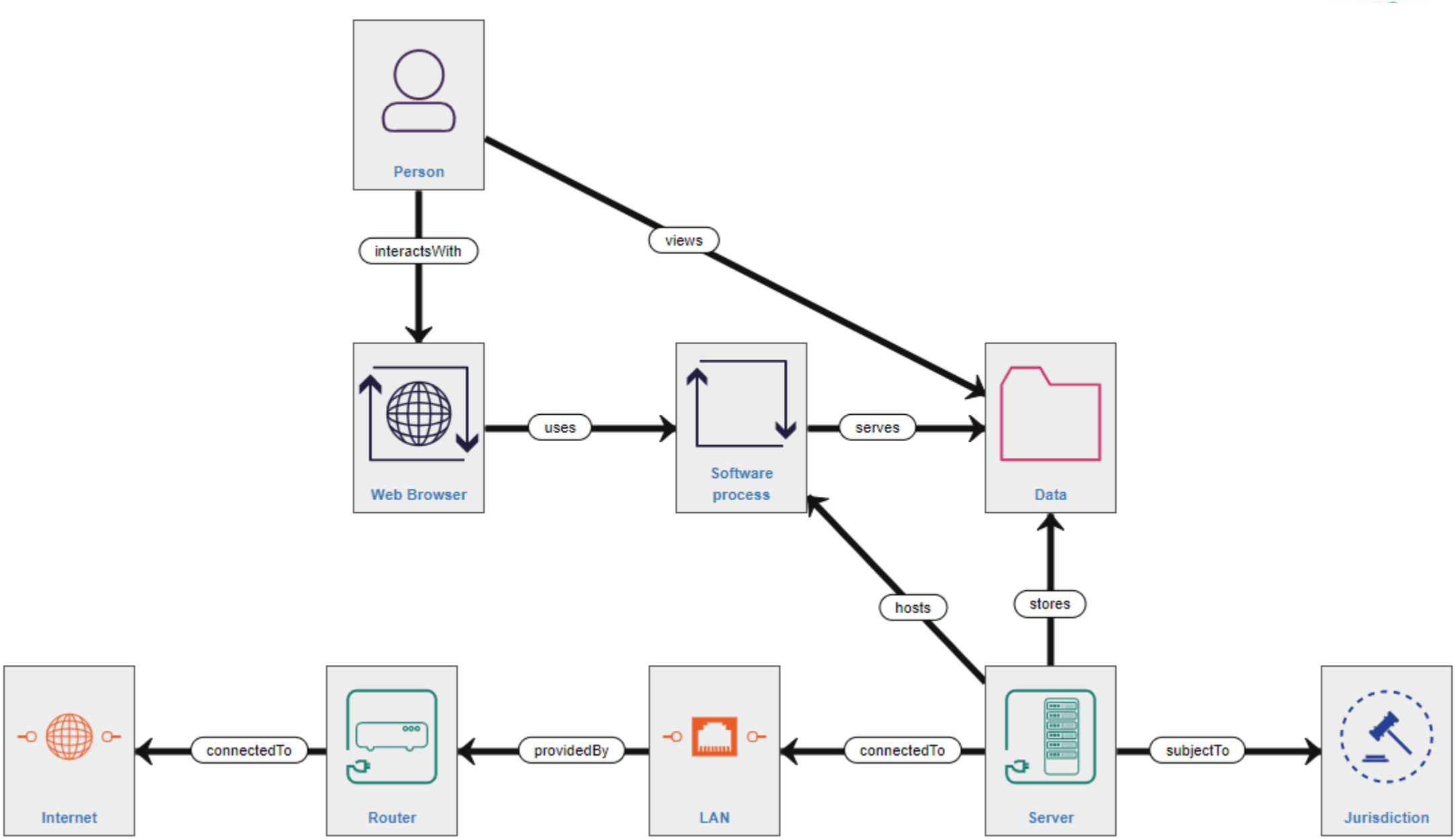
Output results

Integrating with other systems



Assets and Relations





Threats

*"A threat has the potential to cause harm to assets such as information, processes and systems and therefore organizations. Threats may be of **natural or human** origin, and could be **accidental or deliberate**."*

--- ISO 27005

- Threats potentially cause "**consequences**" or "**adverse effects**" at assets.
- The SSM has a knowledgebase of generic, fine-grained threats (and security controls).
- **Primary threats**: often the result of a malicious or external action but can be inherent in the system
  - made more likely by loss of trustworthiness (see next slide)
- **Secondary threats**: caused automatically as a result of another adverse effect
  - e.g. If a server crashes then any software process on the server will also crash

Trustworthiness of Assets

"How likely an asset will avoid or resist being involved in a threat"

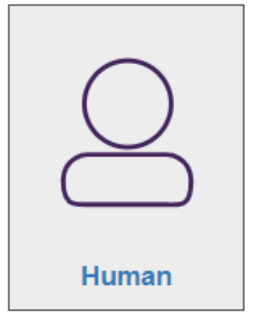
--- not in any standard!

Trustworthiness of *Human* ?

Attribute at Asset	Assumed	Calculated
Astuteness	Medium	Medium
Availability	Very High	Very High
Benevolence	Very High	Very High
Reliable	Very High	Very High
Timeliness	Very High	Very High

Ability to spot e.g. a phishing attack

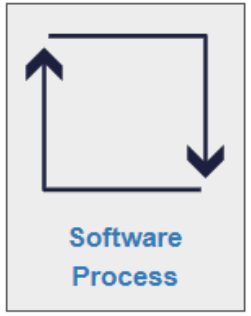
Low benevolence == "malicious"



Trustworthiness of Assets

Free from software vulnerabilities that may be discovered by hackers

Free from bugs that would cause it to crash without provocation



Trustworthiness of *Software Process*

Attribute at Asset	Assumed	Calculated
Availability	Very High	Very High
ExtrinsicTW	Medium	Medium
Health	Very High	Very High
IntrinsicTW	Very High	Very High
Reliable	Very High	Very High
Timeliness	Very High	Very High
TrojanTW	Very High	Very High
UserTW	Very High	Very High

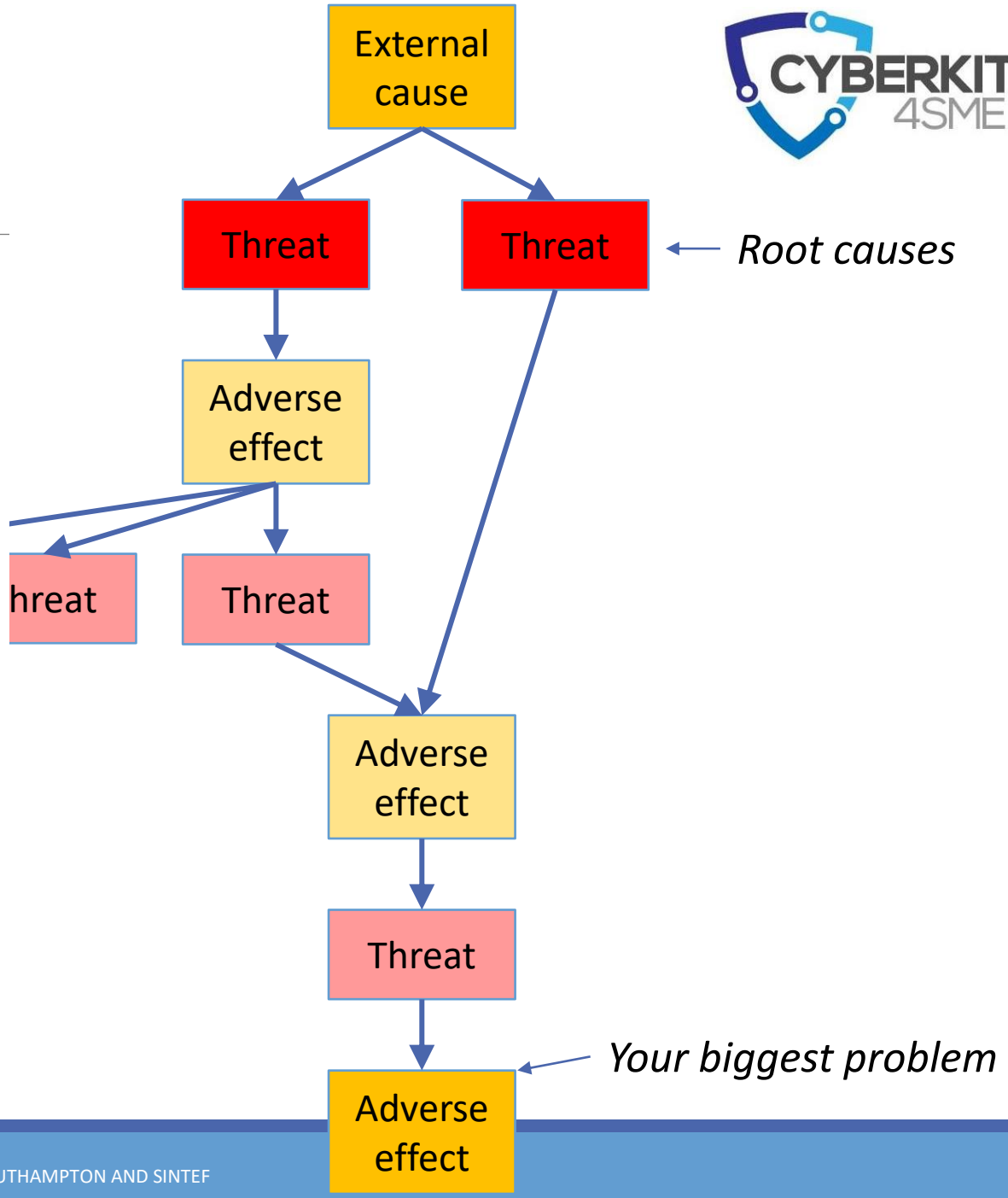
Risk, Impact, Likelihood

Specified **Impact**	Calculated **Likelihood**				
	Very Low	Low	Medium	High	Very High
Very Low	Very Low	Very Low	Very Low	Low	Low
Low	Very Low	Very Low	Low	Low	Medium
Medium	Very Low	Low	Medium	High	High
High	Low	Medium	High	Very High	Very High
Very High	Low	Medium	High	Very High	Very High

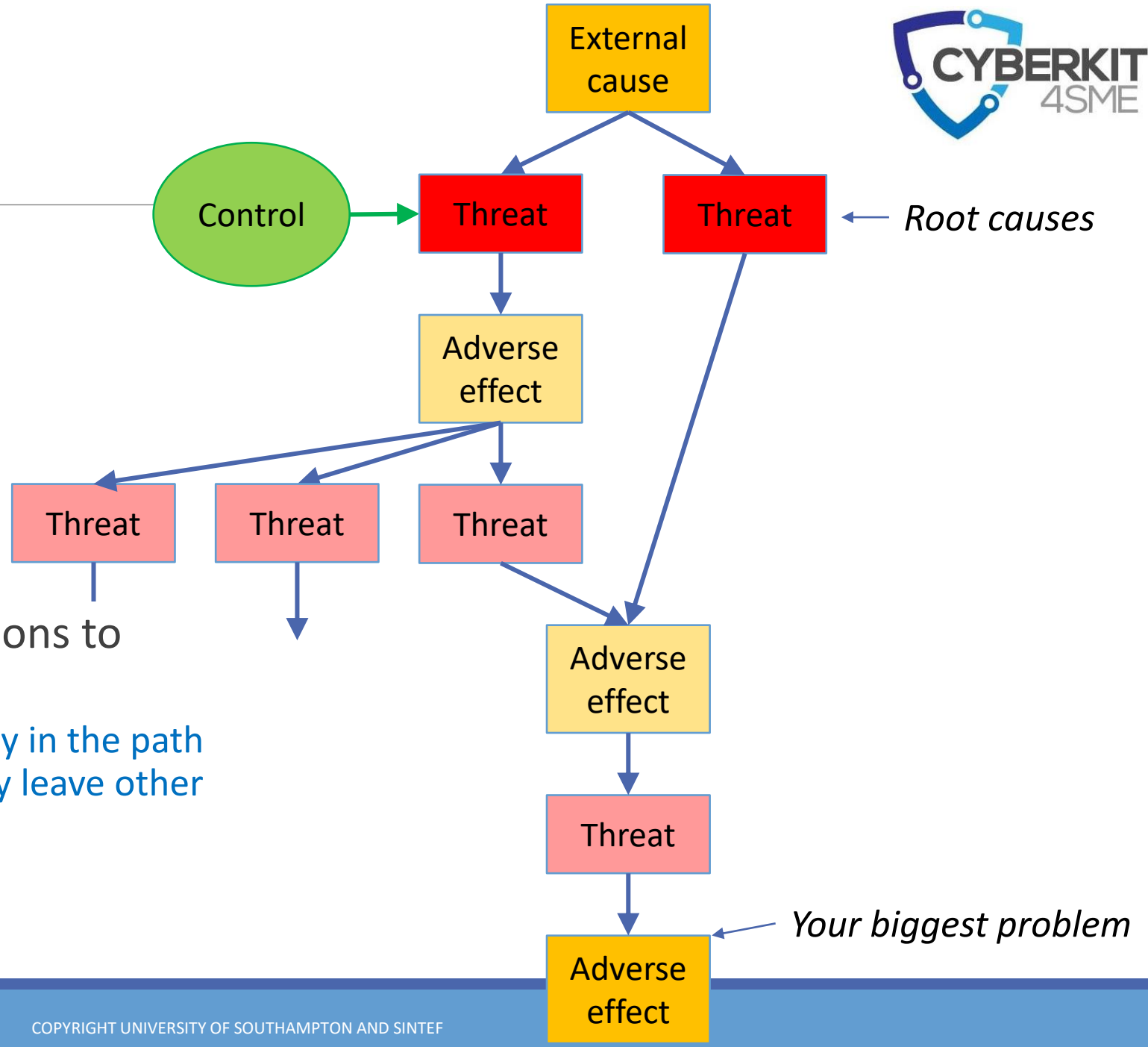
- Calculated **risk** = (specified business **impact**) x (calculated **likelihood**)
- The **impact** of an adverse effect varies according to the asset:
  - Loss of confidentiality of customer profile data => high impact
  - Loss of confidentiality of data on a public website => very low impact
- **Likelihoods** are calculated from the configured asset trustworthiness, the adverse effects of threats, and the presence of security controls
- Sometimes we say A "**causes**" B: we mean A is the reason B is as likely as it is

Attack Paths

- The SSM's analysis shows the highest risk adverse effects: your biggest issues
  - E.g. loss of confidentiality in customer profile data
- As an analyst you want to know what has caused this risk (to be so likely) and therefore how to mitigate it
- There are often many options to mitigate a threat

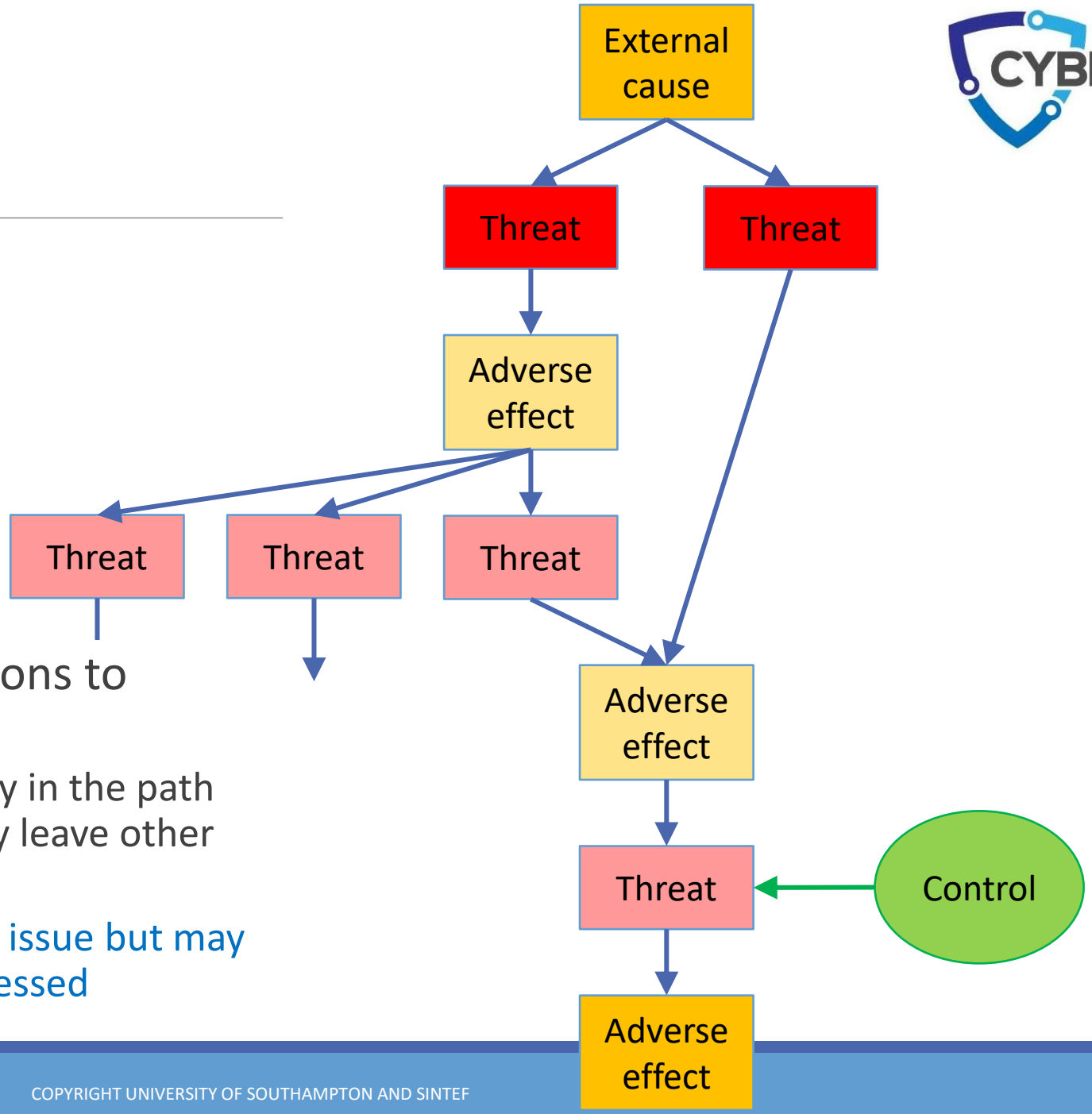


Attack Paths



- There are often many options to mitigate a threat
  - Putting a security control early in the path mitigates many paths but may leave other options for the attacker

Attack Paths



- There are often many options to mitigate a threat
  - Putting a security control early in the path mitigates many paths but may leave other options for the attacker
  - Putting it late will fix that one issue but may leave other problems unaddressed

Getting ‘hands-on’ with modelling, risk assessment and mitigation

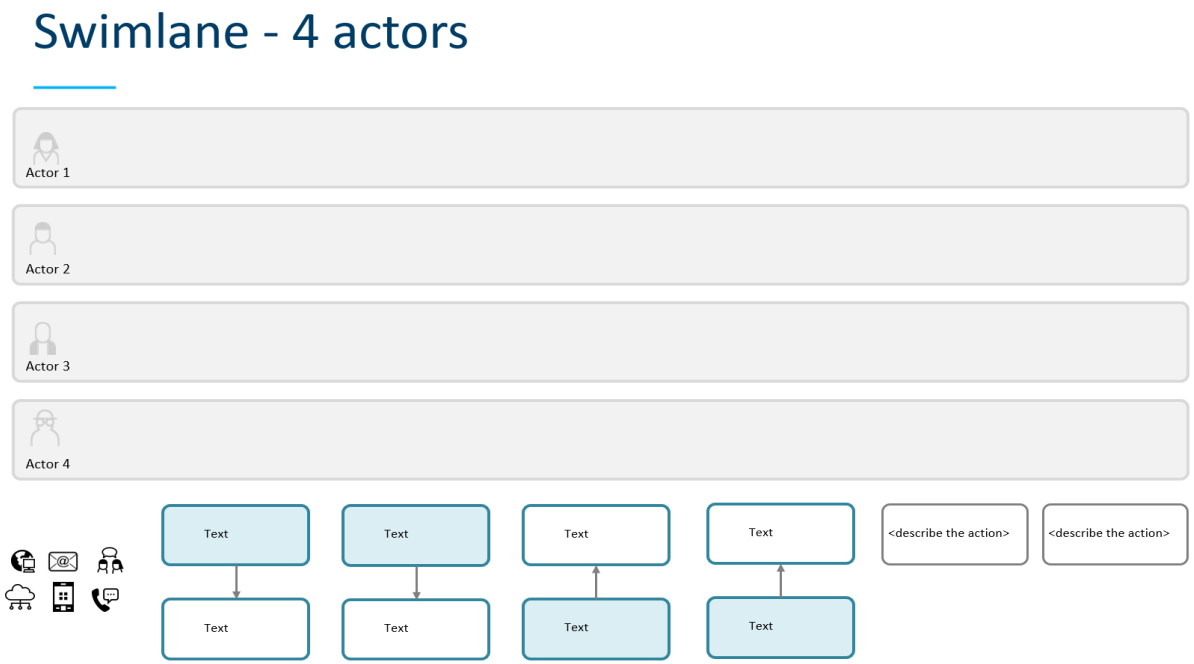
PART 3 - RCIS 2022 TUTORIAL 19/5/2022

The HORM tools

- Three main tools
  - PowerPoint diagrams
  - Online diagramming tool
  - Web application
- Several supplemental tools
  - Diagram generator
  - HORM game
- The main tools allow for creating complete diagrams from scratch as well as editing existing diagrams, while the supplemental tools are intended mainly as learning aides.

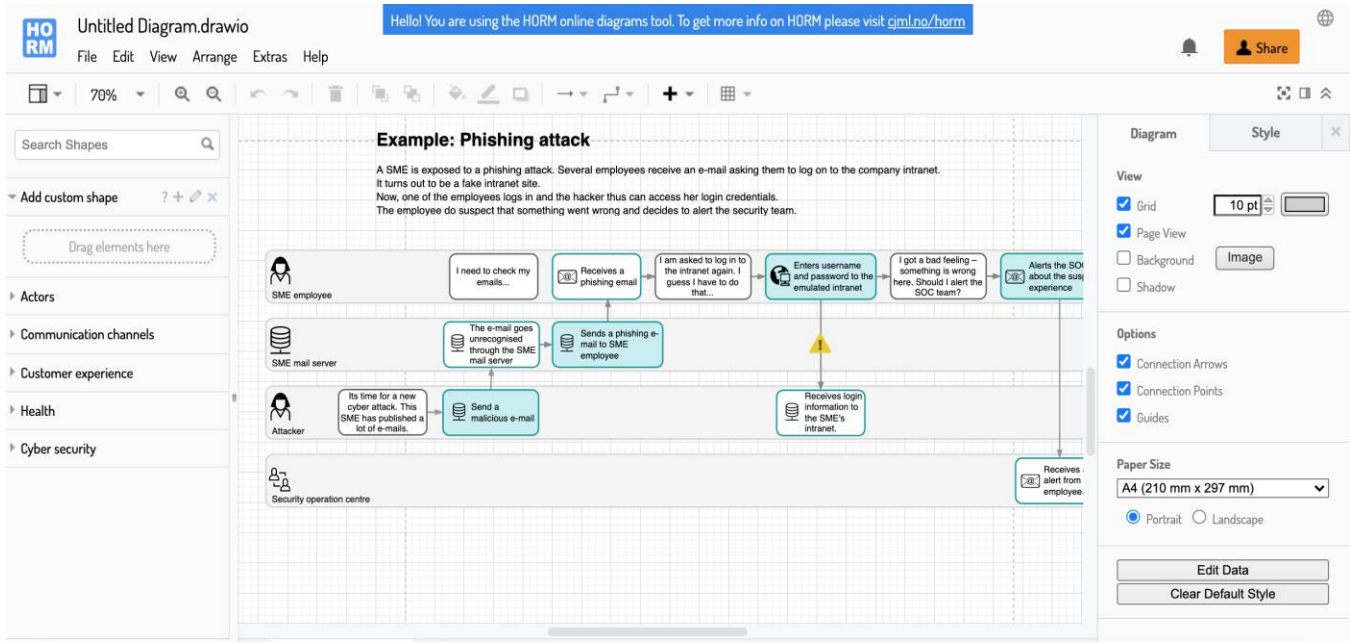
PowerPoint diagrams

- A set of templates and icons that facilitate creating HORM and CJML diagrams in PowerPoint.
- Includes all elements and icons in addition to an overview of diagram types as well as the required background for creating CJML and HORM diagrams.



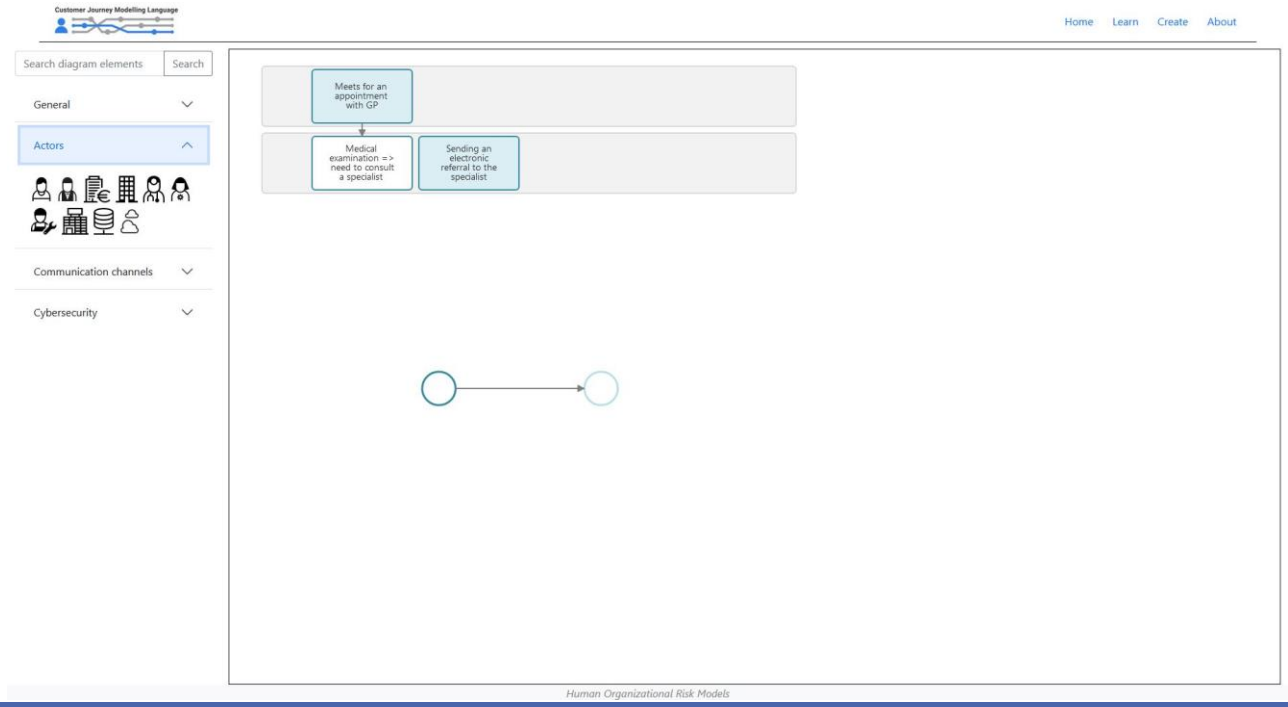
Online Diagramming tool

- A complete diagramming tool based on diagrams.net
- Drag and drop elements from a menu onto the canvas
- Export/import diagrams in various formats



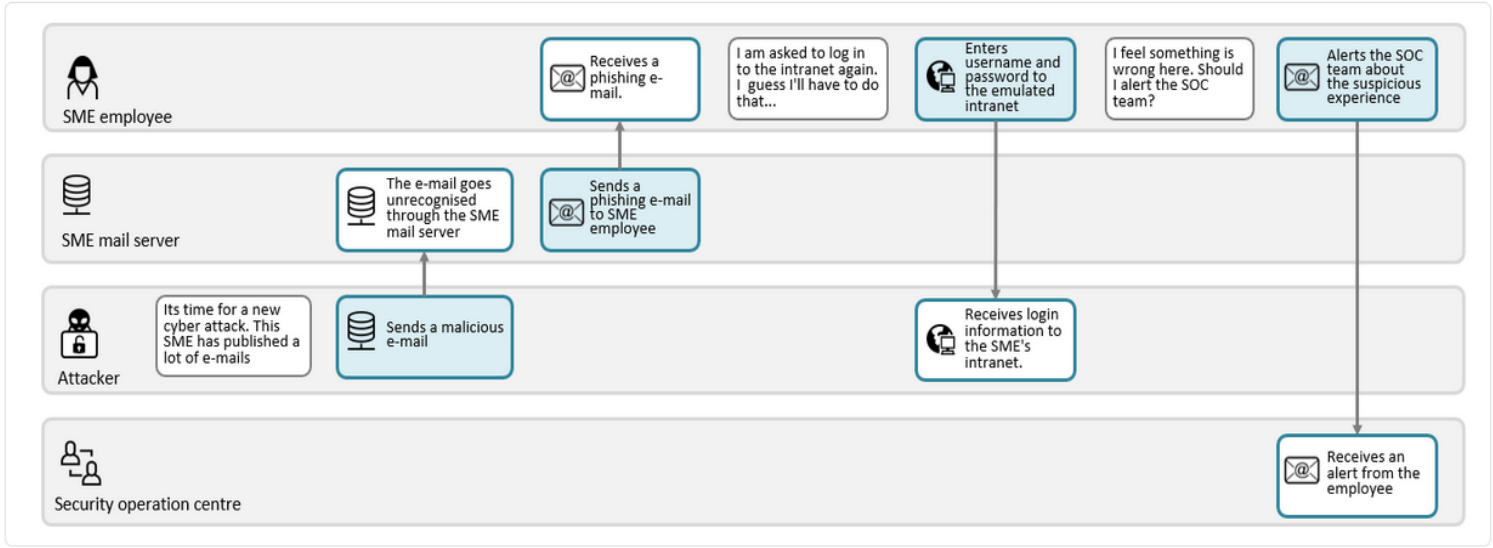
Web application

- Built from scratch with jointjs to support CJML and HORM specific semantics
- Transfer from swimlane to single journey diagrams and vice versa.
- Streamlines the diagramming process by guiding the user during the initial stages.
- Intends to interact with other relevant tools by means of diagram export.



Scenario generator

- Allows for creating swimlane diagrams by providing text input.
- Less flexible than the main tools, but guides the user through the process of creating a diagram from scratch.
  - Provide relevant actors
  - List touchpoints representing actions and communication
- Outputs a static diagram



HORM Minigame

- A minigame designed to
- Arrange the communicat rrect actors.

Information Security & Risk Management: Trustworthiness and Human Interaction

Introduction

In the first part of the tutorial you will be asked to vote anonymously using a Vevox Poll.

Human and Organizational Risk Modelling framework

The Human and Organizational Risk Modelling framework aims at providing a comprehensible and easy to use framework for capturing risks ordinary people may be exposed to. The HORM framework webpage is currently under construction, but continuously updated. You may find the framework on the following URL: https://cjml.no/horm/

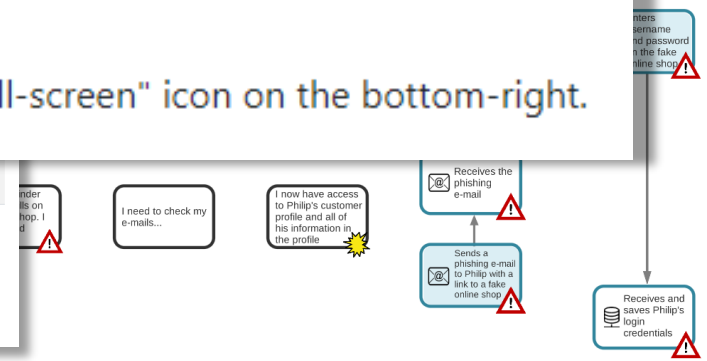
For the hands-on session, we would like you to play a jigsaw puzzle game which will teach you how to create a HORM model based on a Phishing example.

To access the game, please go to: https://cjml.no/gamify/Phishing/ Remember to click on the "full-screen" icon on the bottom-right.

Server 5	Model 17	Model 18	Model 19	Model 20

The model has some basic security controls activated, but the risk to the confidentiality and integrity of "Philip's customer profile" is Very High.

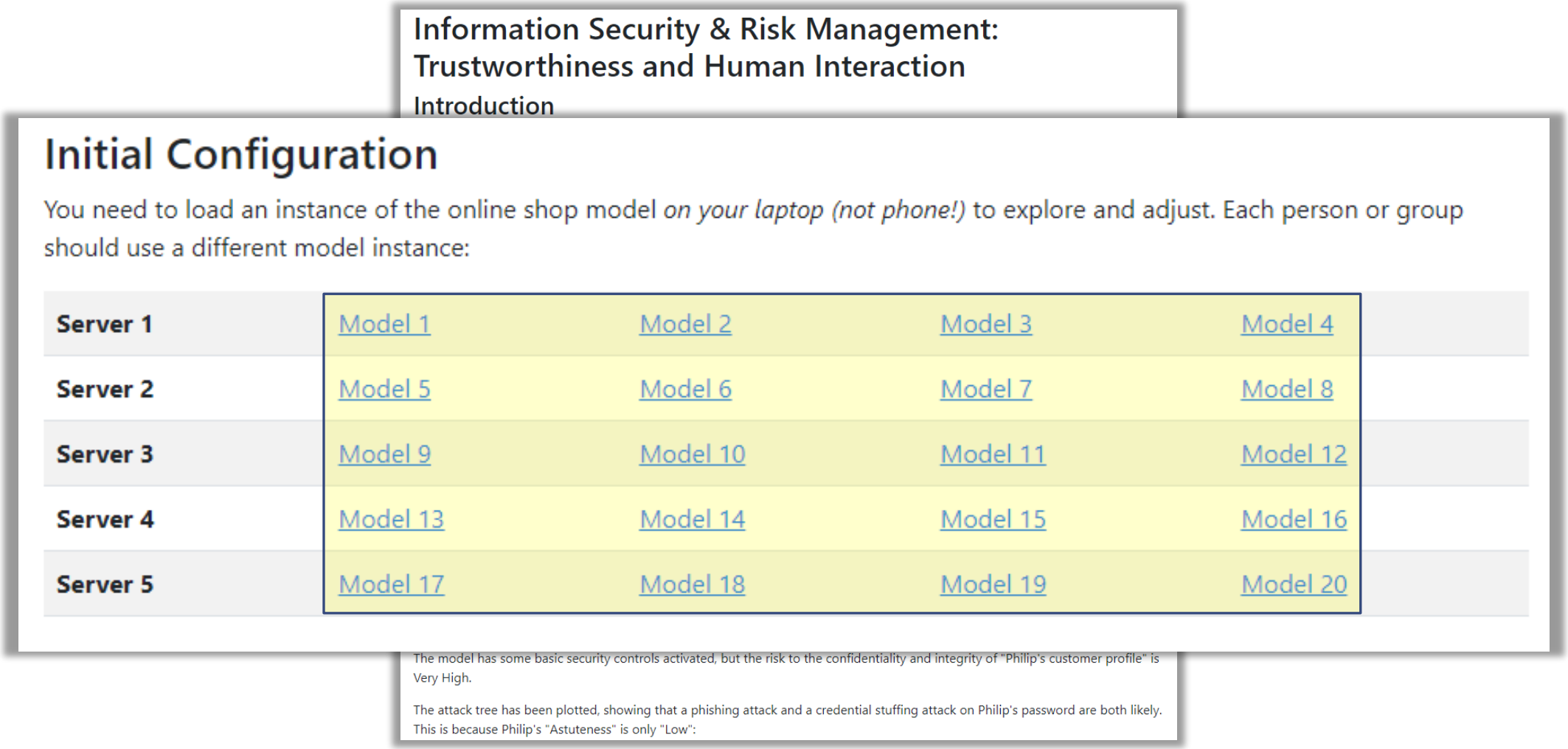
The attack tree has been plotted, showing that a phishing attack and a credential stuffing attack on Philip's password are both likely. This is because Philip's "Astuteness" is only "Low":



System Security Modeller

- We are going to look at a model of an online shop.
- We will use the SSM to explore the model, looking at the risks and adding security controls.
- To help understand what security controls to put where there are some attack path pictures already generated as PDFs.
- The SSM user interface is complex so we'll go through the first example together.

Load Your Model



Information Security & Risk Management: Trustworthiness and Human Interaction

Introduction

Initial Configuration

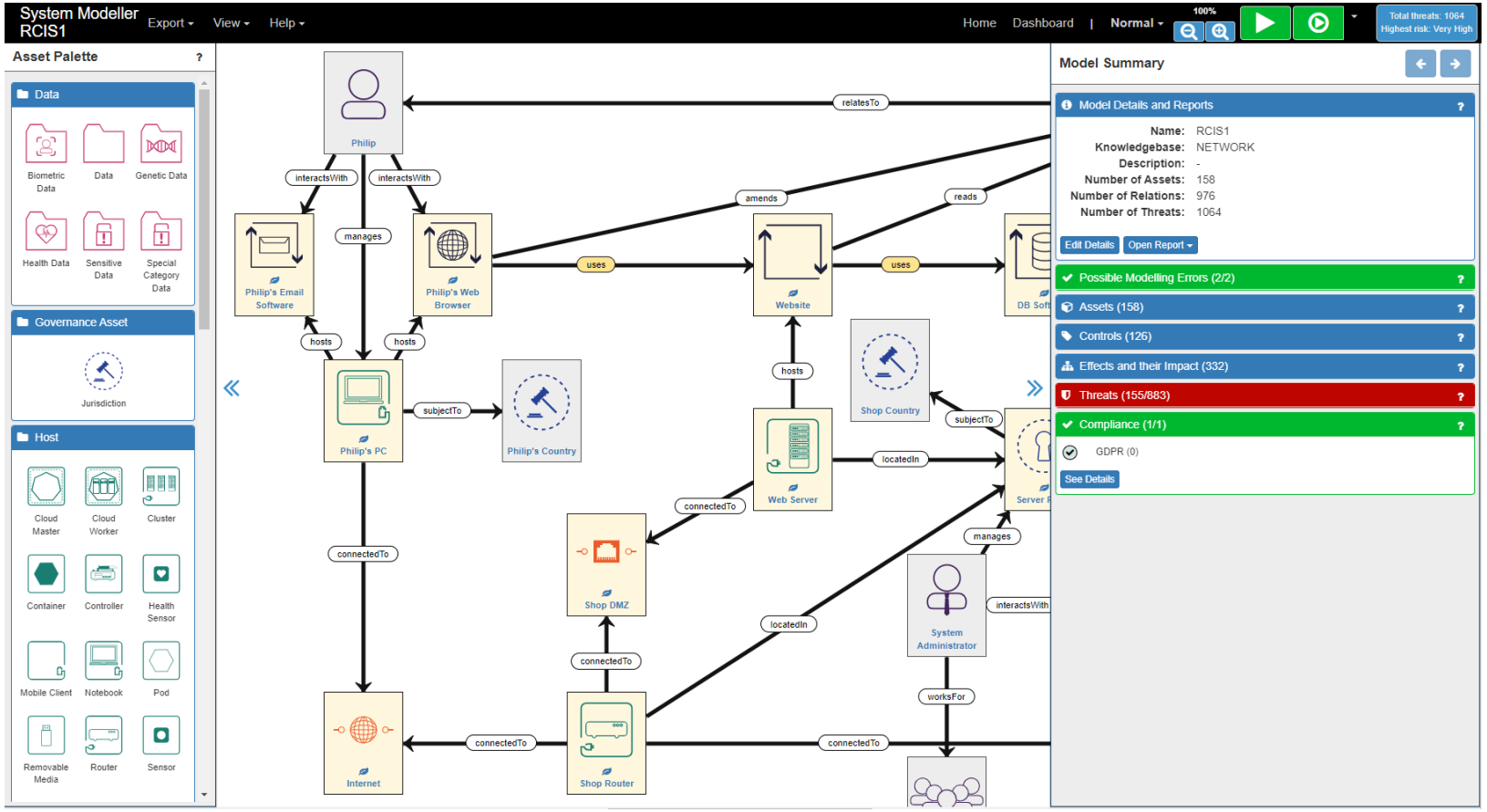
You need to load an instance of the online shop model *on your laptop (not phone!)* to explore and adjust. Each person or group should use a different model instance:

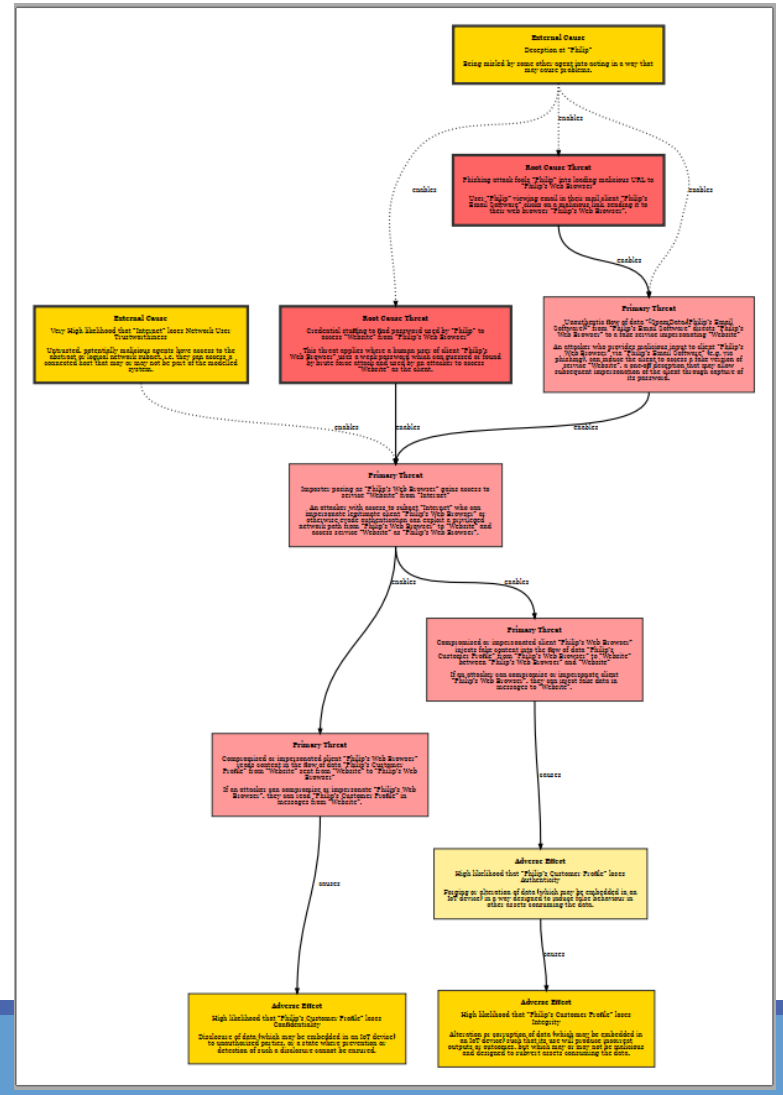
Server 1	Model 1	Model 2	Model 3	Model 4
Server 2	Model 5	Model 6	Model 7	Model 8
Server 3	Model 9	Model 10	Model 11	Model 12
Server 4	Model 13	Model 14	Model 15	Model 16
Server 5	Model 17	Model 18	Model 19	Model 20

The model has some basic security controls activated, but the risk to the confidentiality and integrity of "Philip's customer profile" is Very High.

The attack tree has been plotted, showing that a phishing attack and a credential stuffing attack on Philip's password are both likely. This is because Philip's "Astuteness" is only "Low":

We use SSM and Attack Paths together





Session takeaways and concluding thoughts

RCIS 2022 TUTORIAL 19/5/2022

Session Close

TAKEAWAYS:

1. Cybersystems are sociotechnical
2. Humans must be included in any risk assessment
3. Human behaviour mitigation strategies are very important

CONCLUSION:

1. Trustworthy cybersystems are founded on a complex mix of:
   - Provably effective security (based on comprehensive risk assessment and mitigation that includes humans and human behaviour),
   - Transparency & Explainability of system models and human behaviour (attack paths and interaction flows),
   - Ethical design (including accessibility, inclusivity, equality, simplicity, sustainability and resilience),
   - Compliance with rules & regulations

Information Security & Risk Management:
Trustworthiness and Human Interaction

RCIS 2022 TUTORIAL 19/5/2022 – THANK YOU FOR ATTENDING

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883188