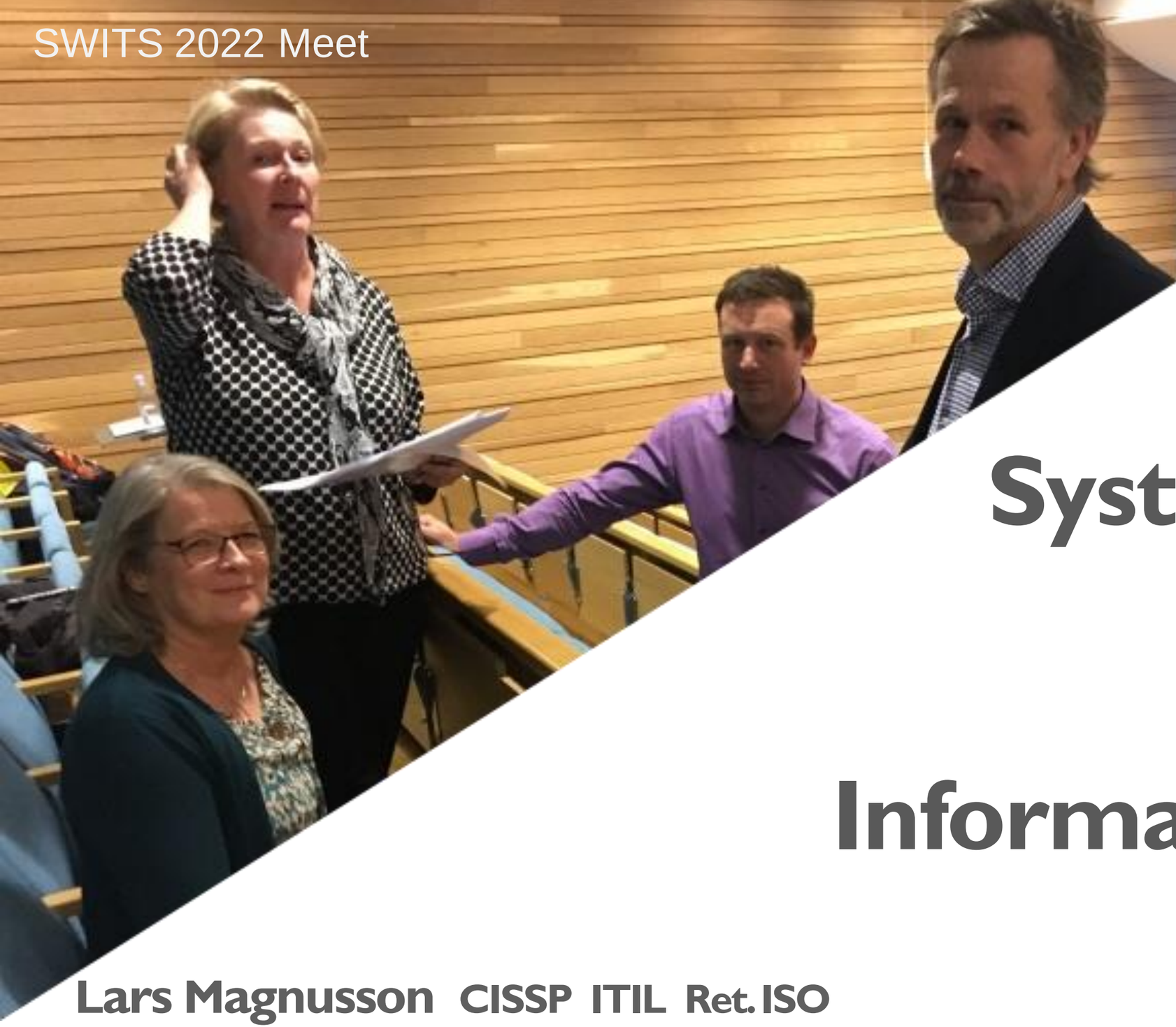


System thinking - how to beat basic flaws in Information Security

Lars Magnusson CISSP ITIL Ret. ISO

Lars.Magnusson@lnu.se

Linnéuniversitetet
Kalmar Växjö

Lars Magnusson

- Lars.Magnusson (at) Lnu.se

- *Doctoral student in Information Security at Linnaeus University since 2017*

- *Permanent Member - General Motors Information Security Core Team (2000 - 2009)*
- *Permanent Member - The Greenland Home Rule's IT Steering Board (1985-1987)*
- *Global Info Security Operations Manager - General Motors Corp (2007-2009)*
- *Info Security Officer - GM Europe (2005-2007) & Saab Automobile (2001-2011)*
- *Enterprise Security Architect - Tieto (2012-2018),*

- *Previously:*
- *CIO (Greenland Business School), TIO (PKA.dk), and Internet strategist (Saab Auto)*
- *Worked publicly, privately and in the financial sector in Sweden, Greenland, Denmark, UK and USA*

The *seven key audit flaws* of Info Security !!!

After studying 14 Federal Trade Commission and Security and Trade Commission Root Cause analysis, six EU GDPR Root Cause reports, and 20 Swedish Public Info Security IT Security audits, and with a previous amount of 25 audits (6 SOX, 5 normal IT Sec audits and rest customer/-vendor audits), all exhibited the same basic flaws, which in the 14 proved fatal for the succeeding hacker breaches. These *seven audit flaws*, most likely, due to existing evidence, is present at most of all organizations, are:

1. *Authorization of accounts, both user and system accounts*
2. *Authentication of accounts, active when they should be closed,*
3. *The 5 Audit W: "Who did what, when, where, and why?" - Lack of appropriate logging of what is happening.*
4. *Documentation decisions, system configurations, changes, and who decided what.*
5. *There were no readily error correction strategies, including documenting "Lessons Learned", i.e., repetitive errors.*
6. *Code audit, both own code as bought systems (lack of procurement demands), and*
7. *Lack of proper network segmentation, aka. "deny all, allow needed" or lack of Zero Trust networking.*

Info Security is more about bad governance than of technical flaws. We need to realize that practical all organizations do manage info security incorrectly, thus open up for breaches !

Then a Perfect Storm rising

The hackers used system thinking as a design concept in their attack …

Info Security need to do the same!

Lars.Magnusson@lnu.se

System thinking is hard …

Prof. Peter Ekman, MDU:

"Processes such as systems thinking are often difficult for researchers to accept due to. their complexity. But for many practitioners, such frameworks are completely natural, as you work with them on a daily basis".

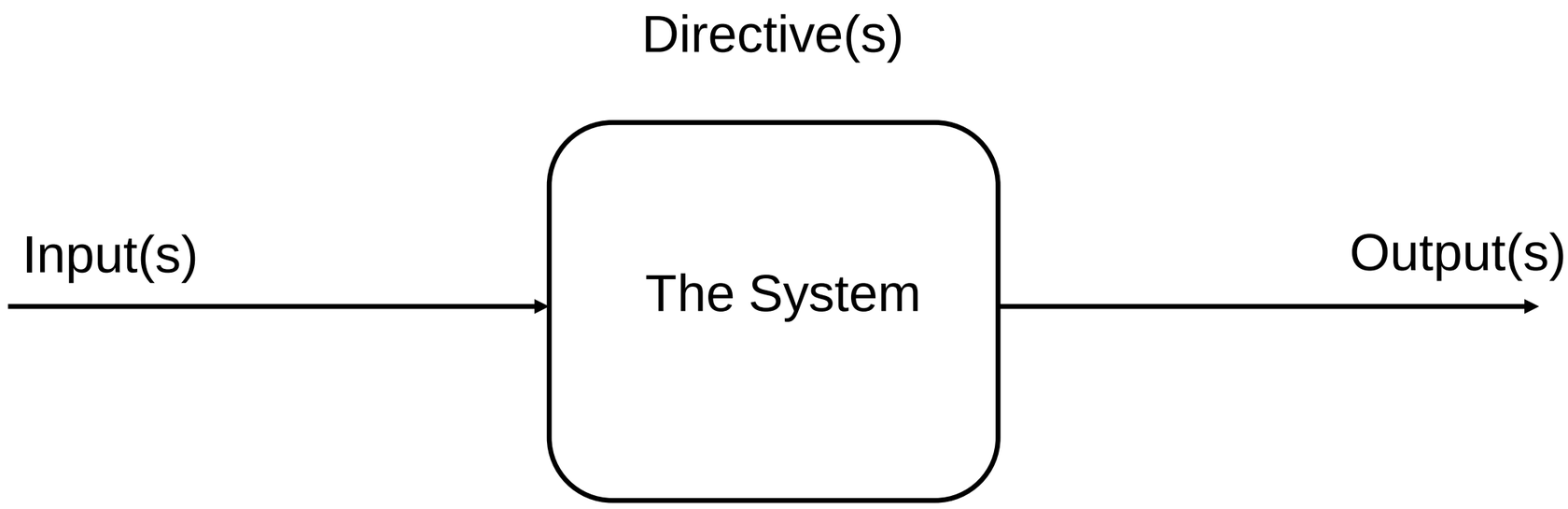
Prof. Ricardo Valeri, Univ. of Arizona:

"System thinking is not natural; some individuals can never learn system thinking. At the same time, our schools, especially universities, are bad at teaching systems thinking. Systems thinking is basically an experimental knowledge ".

Thus, many researchers avoid systems thinking and work with simplifications.

System Thinking as normally envisioned in ICT

The normal view of systems is as a singular black box entity, balanced by its inputs, outputs, and processing directives:

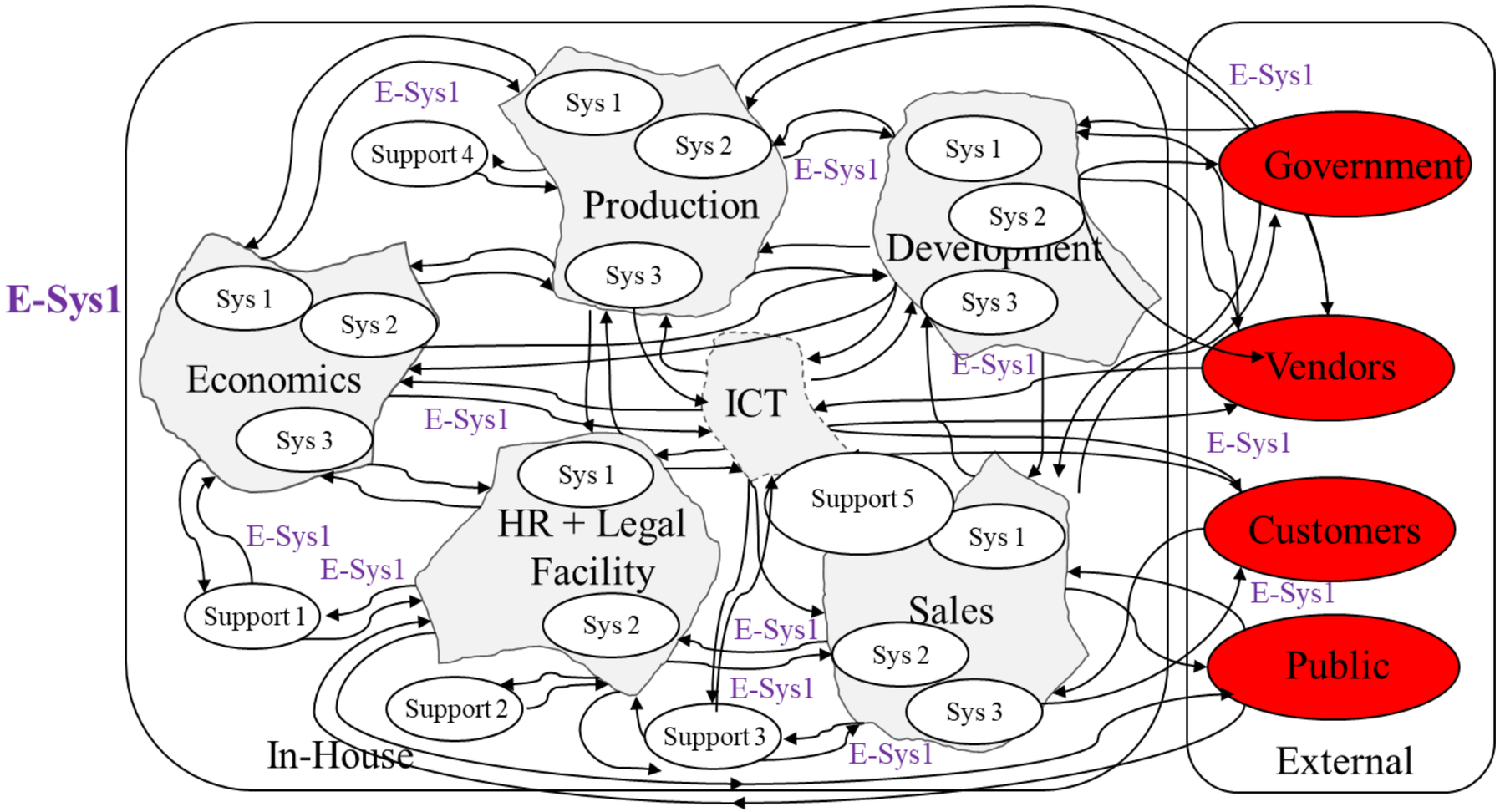


Complexity only within input, output, and processing directives …

Lars.Magnusson@lnu.se

Systems in Real Life – a practical perspective

A multitude of interconnected entities, often badly documented and poorly understood, not well coordinated, but systems still imperative for each others:



Lars.Magnusson@lnu.se

System thinking - how?

- Everything around us exists in some kind of system

To understand the world we act in, we must know how the parts relate

- We have systems on macro level – the observable universe
  - We have systems on galaxy level
    - Or the solar system – our home
      - We have geological, physical, and chemistry systems
      - Or systems on micro level, biology - Gaia

All of these govern how our perspective looks like, physically, biologically, chemically, technically and their relations.

But how do we learn how system works?

By observing the holistics view, system is not simplified units, it is about the enterprise perspective.

The problem: Closed systems always suffer from atrophy!

Everything around us is part of some kind of system, scientific, technical, economics and social. That is why systems thinking is needed… Why?

All these systems relate somewhere to the other systems, they belong together.

Most researchers tend to reduce complexity by working with simplified models. Problem is, you often sort out everything you see as insignificant, but later which can prove critical.

If we filter data due to the model we choose, how sure can we be that we are not creating a "black swan"?

Furthermore, filtered data means we make approximations, which can lead us astray. We think we see reality, but as Plato said about the man in the cave:

"*He sees pictures moving over the inner wall of the cave, but what is those? Just the shadow of the real individuals passing outside, between the cave opening and a fire outside". Which we see as chimeras ".*

The challenge !

- We are governed by multiple, coherent systems, no matter what we do.
  - As declared, humans have a weakness in thinking systemically (experimentally shown)
    - It's about breaking out of the "box", thinking holistically
      - To approximate to relevant boundaries (data) – guessing the swans
    - To identify key relationships that must be included
      - To realize that we must work with complexity
        - To be able to work broadly, across several disciplines
          - To be a bit of Renaissance people / generalists

As Ekman and Valeri pointed out,
to work more experimentally.