



Utrecht
University

Unknown Unknowns: Cyber threats from Shadow IT in Education and Research

Joost Gadellaa, SURF

21 May 2024

| Introduction



Joost Gadellaa

(now) Technical Product Manager *Security & Privacy*

joost.gadellaa@surf.nl

[linkedin.com/in/joost836286/](https://www.linkedin.com/in/joost836286/)

- Technical Product Manager for SURFmailfilter, SURFcertificates, and Resilience Testing
- BSc in Economics, some Sociology, Psychology, Computer Science and an MSc in Business Informatics at Utrecht University
- Master's thesis on Shadow ICT in HEIs

| Context of a Higher Education Institution (HEI)

Open character

- Knowledge and data sharing
- Cooperation between institutions and with external parties
- Physically and digitally accessible

(Academic) Freedom

- BYOD and being able to work from home
- Autonomy in procurement, specialist equipment
- Independence (and stubbornness) is the norm

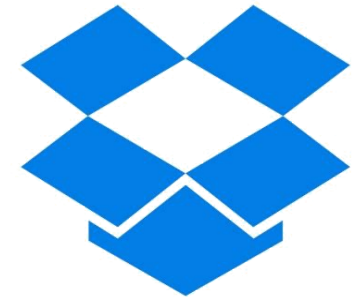
A search for balance between institution-wide IT solutions and the autonomy of departments and individuals



Shadow ICT:

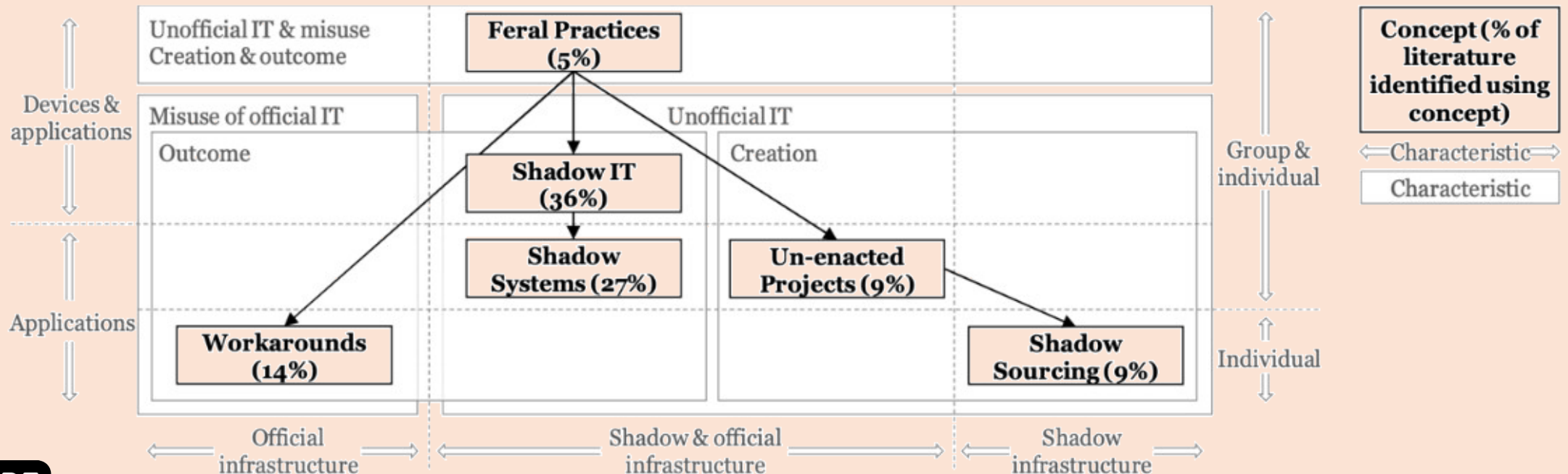


***"hardware, software or services built, introduced and/or used for work without approval or even knowledge of the (ICT) organisation"
(Haag & Eckhardt, 2017)***



Scientific research on Shadow ICT

- Develops from Spreadsheets to Cloud
- Definitions *all over the place* and always new
- A mature research area since Kopper & Westner (2016)



| Further in science:

Research is hardly concerned with the practical or technical aspect

Often at the *governance level*:

- Lack of control
- "Not compliant"
- Blind spots

No doubt *that* shadow IT can cause security problems, but rarely elaborated on *why* or *how* exactly



What should we do with it? What is needed for it?

Starting point:

- HEIs value an open ICT environment; simply banning it is not pragmatic
- Institutions have departments and independent researchers; identifying and managing everything is not realistic

Risk-based approach: identify problems and implement targeted measures



Aim: To understand *how* the presence of shadow ict in HEIs can cause cybersecurity problems, as a first step for risk-based policy.



MRQ: "What is the role of shadow ict in the cyber threat landscape of Dutch higher education institutions?"

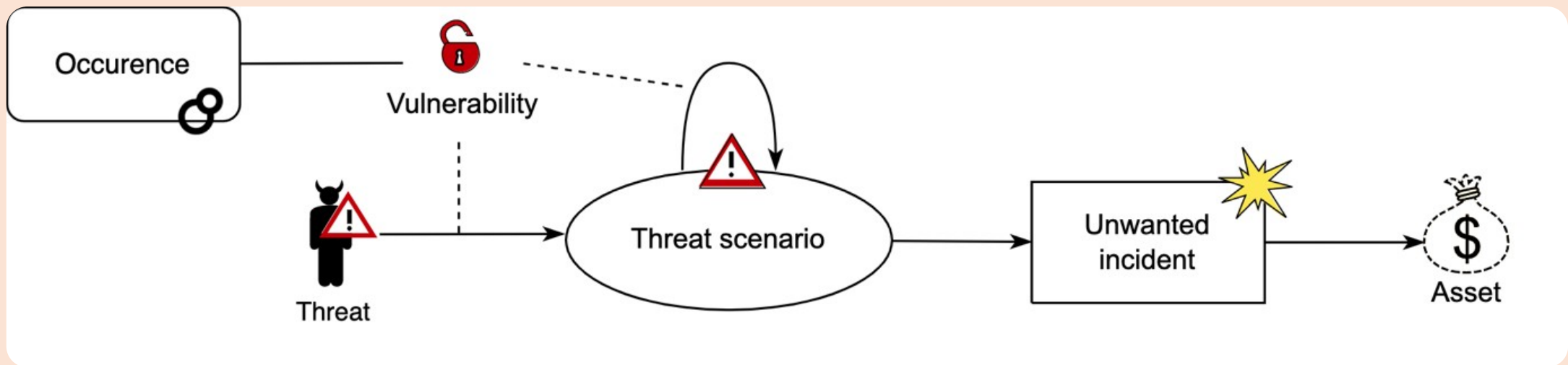
| Data collection

Analysis of qualitative data:

- Open coding
- Axial coding with emergent and predefined semantic domains:

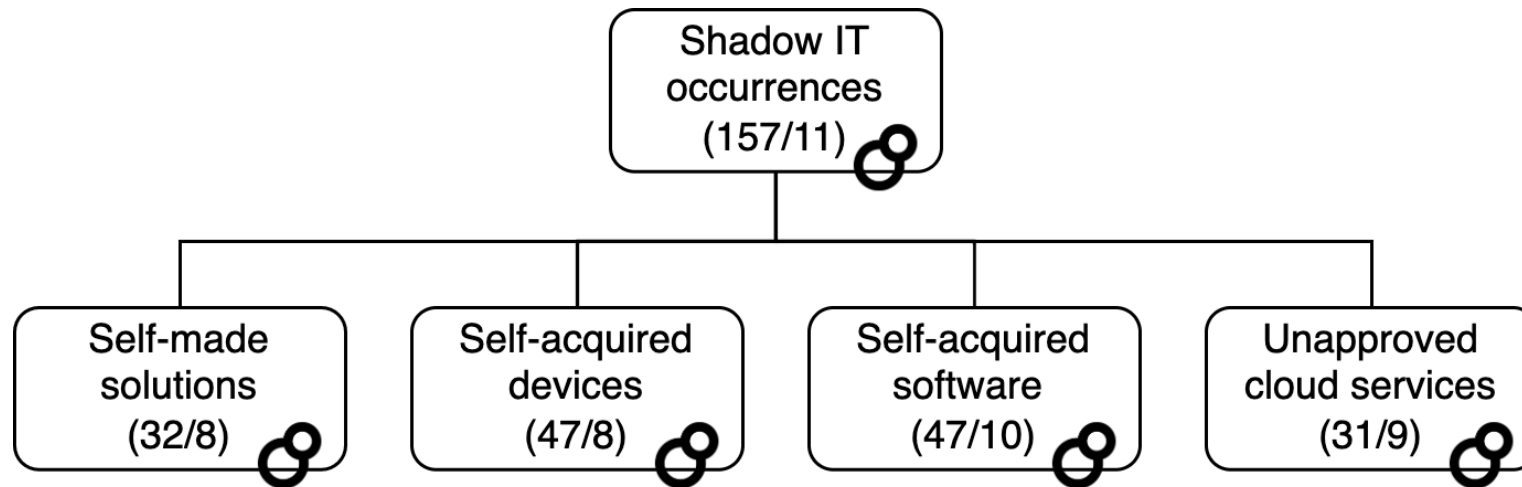
Codebook reliability:

- 2 researchers coded 11 interviews
- Saturation: 1.35% new codes after 10 interviews
- 104 codes, 726 times applied



Presence of Shadow ICT


- Subdivided with a topology based on Mallmann et al. (2019)
- Everything exists, varying greatly between institutions
- Software is *top-of-mind*
- Cloud services range from small to very large
- Unique to research: self-developed software

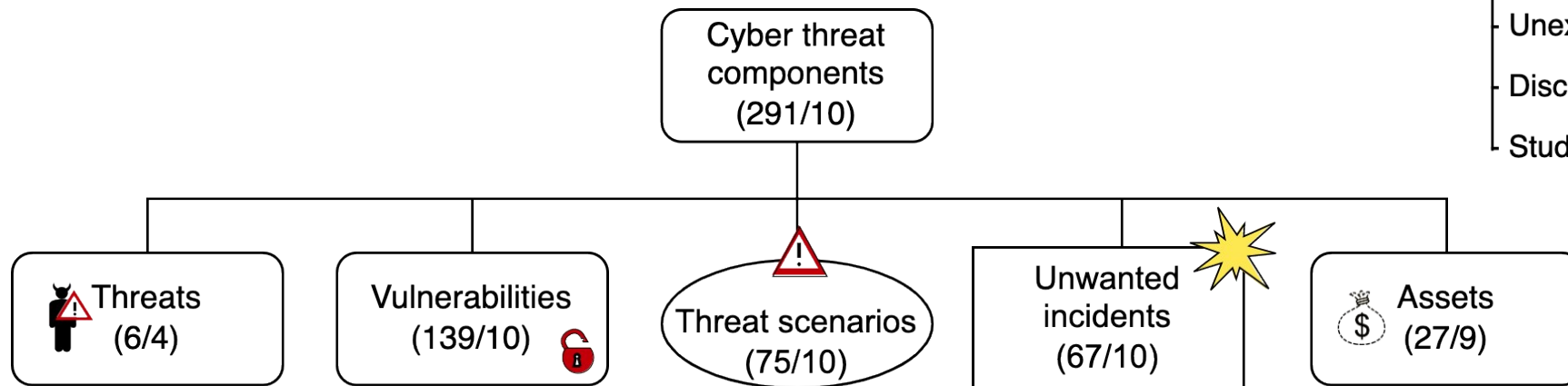


create variety

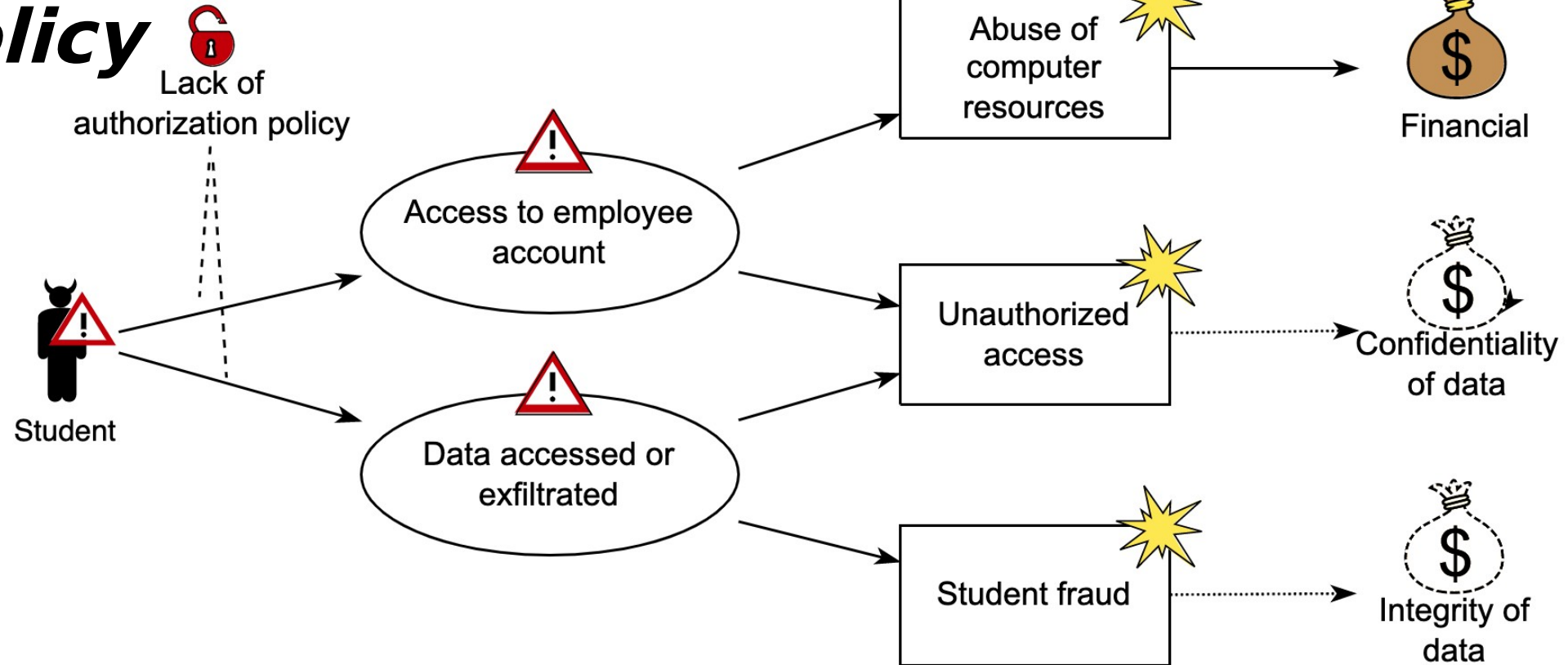
Threat components of shadow ICT

- Captured using the lens of CORAS (Lund et al., 2011) to operationalise 'cyber threat'.
- Participants focus on vulnerabilities, scenarios and incidents; everything else remains implicit

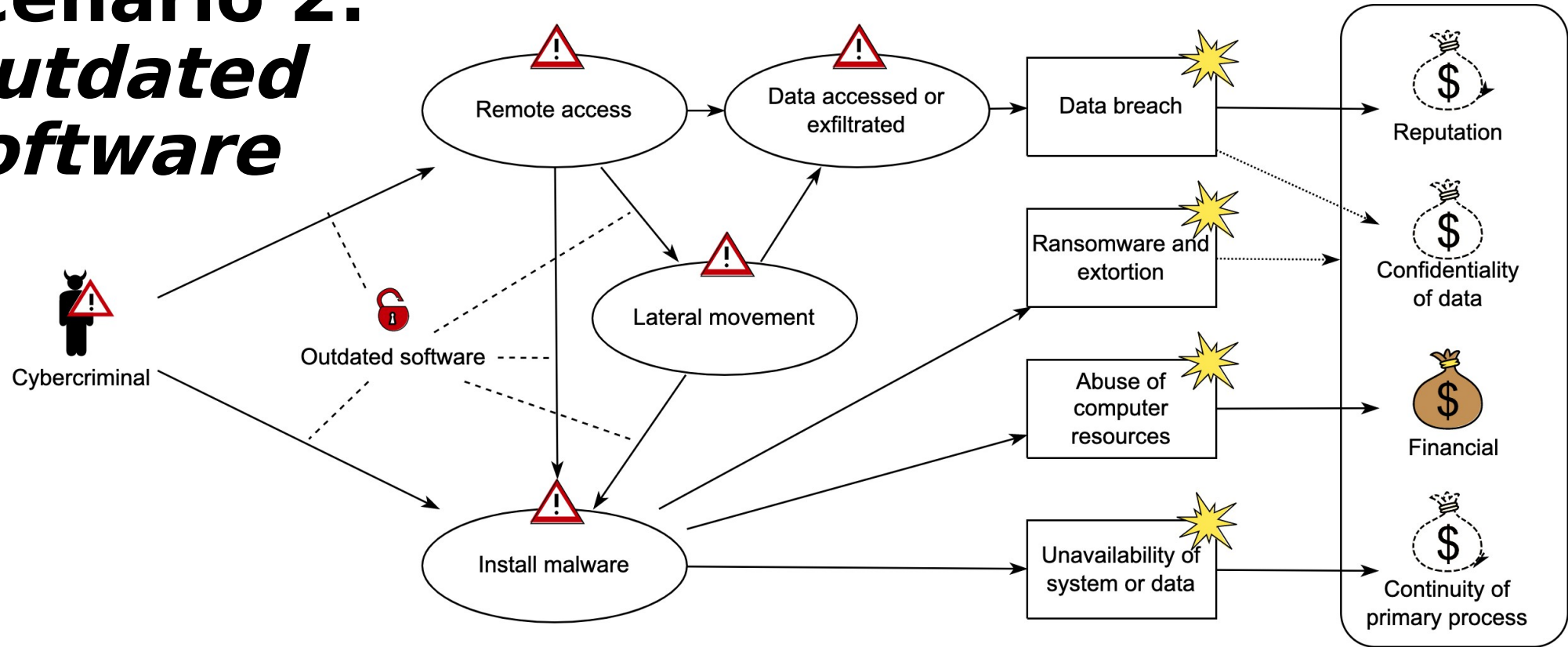
Unwanted incidents 	
Unauthorized access	(16/6)
Data breach	(13/6)
Leaked credentials	(9/6)
Commercial use of data	(7/4)
Ransomware and extortion	(6/4)
Abuse of computer resources	(5/3)
Unavailability of system or data	(5/2)
Unexpected costs	(3/2)
Discontinuation of services	(2/2)
Student fraud	(1/1)



Example scenario 1: *Lack of authorisation policy*



Example scenario 2: *Outdated software*



What stood out?

Three key case studies:

- The classic network infiltration scenario (a 'Maastricht')
- Lack of control over data causes unintended harm
- Misconfigurations causing problems between users

For each institution, the type of problems was strongly related to the measures already implemented

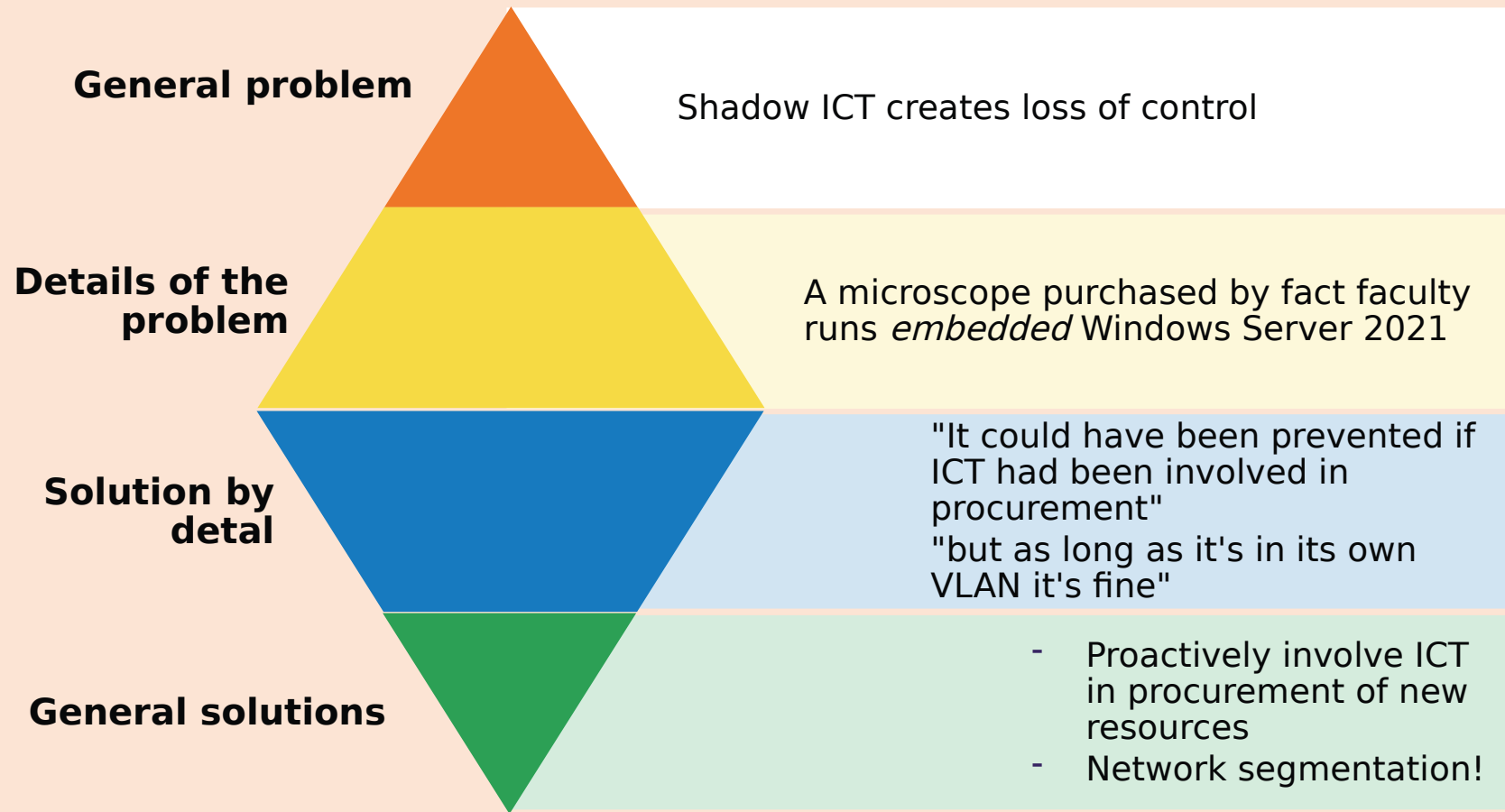


Conclusion(?)

MRQ: "What is the role of shadow ict in the cyber threat landscape of Dutch higher education institutions?"

- Shadow ICT is an inherent part of HEIs IT environments
- Three main scenarios summarise the potential problems
- The role of shadow IT in the cyber threat landscape can be quite manageable if it is assumed and taken into account

| Problem -> Observations -> Conclusions



Shadow ICT problems can be:

Prevented with training, policies and usable official solutions tailored to user needs

Detected with monitoring and scanning, and by keeping users on managed devices for as long as possible

Limited by commonly known technical measures:

- Multi-factor authentication
- Network segmentation
- Mobile device management
- Well-thought-out password policy
- Endpoint security
- ...

Shadow ICT issues can be **prevented**:

*"And we are also pushing [departments] to play a role in this with [IT] coaches and small teams that also start thinking within such a [department] about: yes, **what do we need? What will we have to deal with in the future?** What are our teaching staff working on? What IT support do they have? That starts slowly, starts to grow and, yes, starts to work. I think that becomes the best solution or the biggest solution for shadow IT: to **just have that conversation** [...] so that people can put their wants and needs somewhere."*

*"I do notice that in the past we had a lot more shadow IT. It used to be very easy for a user to walk to [an electronics shop] and buy [a NAS] system and put it under their desk. [...] At some point, we adopted the policy of: yes, **we can manage that kind of thing too**. We're not going to be difficult about that. [...] If you want, we also manage your [storage] [...]. But prefer not to do it next time."*

*"That is also why **we have deployed large-scale centralised storage** in different flavours. Very good ones with redundancy, backup, protection against ransomware and things like that. A very cheap one, which is cheaper than any commercial provider."*

Shadow ICT issues can be **detected**:

*"Yes, and **we scan the network regularly**, so if we come across things like [compromised devices], then.... Look, sometimes a new device like that comes in, gets connected quickly, without requesting a separate connection for it, for example. You come across things like that. [...] We use **intrusion detection, and protection system** on our network. And that has stopped a lot of attacks in the years we've been using it. So in that respect, I am less afraid than at an average other institution."*

*"**If you lose your managed laptop, you can sleep easy.** If you lose your [unmanaged laptop], unfortunately you have to fix it yourself. We are trying to change that with different programmes, such as **mobile device management**. But you notice, because those devices are actually owned by the [department], you get resistance to that kind of effort."*

Keeping users on managed devices and networks for as long as possible!

Shadow ICT problems can be **limited:**

- Open door, but in practice problems depend on the measures taken
- Many incidents could have been prevented if cyber hygiene was in order
- Help users with:
- Data classification, least privilege
- *Security awareness* and culture





Utrecht
University

Unknown Unknowns: Cyber threats from Shadow ICT in Education and Research

Joost Gadellaa, SURF

21 May 2024

Full thesis:



edu.nl/683h9