tnc23
DIGITAL GENERATIONS
TIRANA, ALBANIA | 5-9 JUNE 2023

Cyber Threats of Shadow IT in Dutch Higher Education and Research

Joost Gadellaa, SURF

TNC23; Tirana, Albania

Full thesis:

edu.nl/683h9

GÉANT
Co-funded by the European Union
SURF
Utrecht University

Context: IT in Higher Education Institutions (1/2)

“The least secure place in the universe?”
(Bongiovanni, 2019)

TECHNOLOGY NEWS FEBRUARY 5, 2020 / 5:22 PM / UPDATED 3 YEARS AGO

University of Maastricht says it paid hackers 200,000-euro ransom

By Reuters Staff 2 MIN READ

AMSTERDAM (Reuters) - The University of Maastricht on Wednesday disclosed that it had paid hackers a ransom of 30 bitcoin -- at the time worth 200,000 euros ($220,000) -- to unblock its computer systems, including email and computers, after an attack that unfolded on Dec. 24.

Ransomware attacks have become commonplace, with insurers raising cyber security premiums by as much as 25% after hacker targets in 2019 included companies, hospitals and airports.

University Vice President Nick Bos said the university had decided to pay the ransom after considering the alternatives, which would have included rebuilding its entire IT network from scratch.

Context: IT in Higher Education Institutions (2/2)

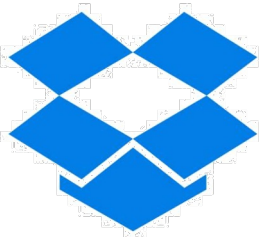
- In higher education institutions (HEIs), staff and students have freedom in arranging IT facilities.

- The sector has an open character:
  - Sharing of knowledge
  - Cooperation in research and education

- Balancing institution-wide IT solutions with the autonomy of departments and individuals

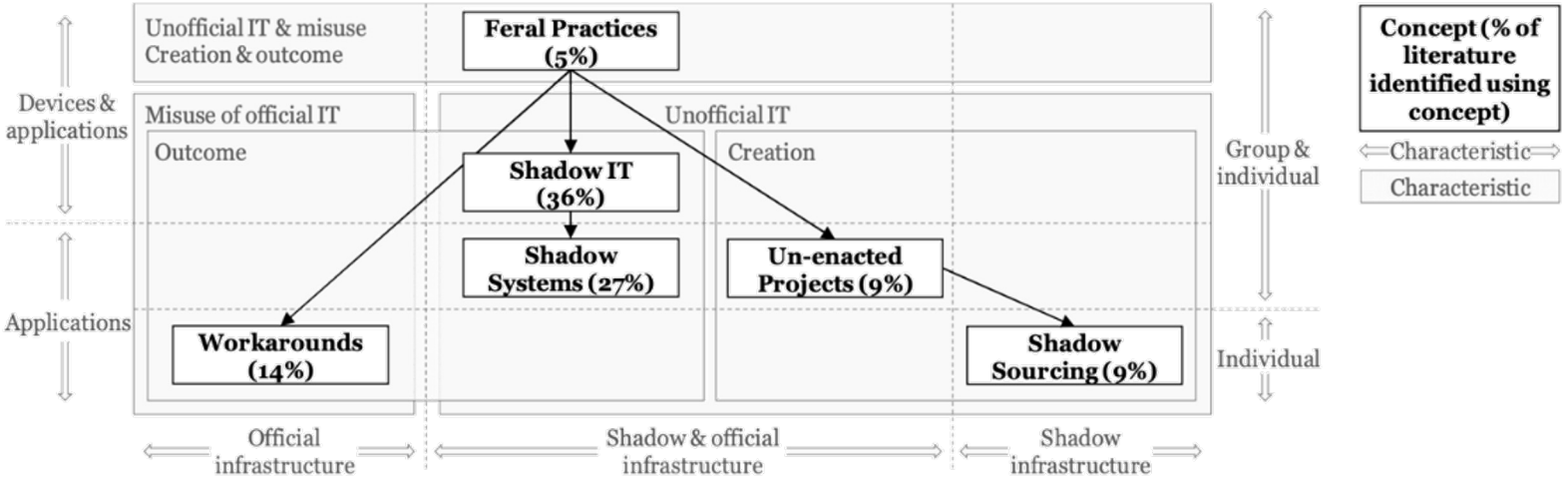
Shadow IT:

“hardware, software, or services built, introduced, and/or used for the job without explicit approval or even knowledge of the organization” (Haag & Eckhardt, 2017)



Tertiary Study on the Phenomenon of Shadow IT

- Development over time from Spreadsheets to Cloud
- Definitions get mixed, new terms are often coined
- The area matures with Kopper & Westner (2016)



Taxonomy of Shadow IT by Kopper & Westner (2016)

Mapping Study on Cybersecurity Consequences of Shadow IT

- Research does seldom cover practical or technical details

- Often on the governance level:
  - Lack of control
  - Not compliant
  - Blind spots

- No doubt about that shadow IT **can cause security problems**, but not worked out **why or how** exactly

Context: Governance of Shadow IT

- HEIs value an open IT environment; a total ban is not an option
- Identifying and managing *all* Shadow IT instances would be extremely difficult
- Instead, a risk-based approach is chosen; map out possible problems and perform targeted mitigations

Goal: To understand *how* the presence of shadow IT in HEIs can cause cybersecurity problems, as a first step for work on risk-based governance

MRQ: “What is the role of shadow IT in the cyber threat landscape of Dutch higher education institutions?”

MRQ: *"What is the role of shadow IT in the cyber threat landscape of Dutch higher education institutions?"*		Research Method(s)
SQ1:	"How is shadow IT defined and differentiated from similar concepts?"	Literature review, tertiary study
SQ2:	"What cyber threats are commonly associated with shadow IT?"	Literature review, mapping study
SQ3:	"What types of shadow IT are observed in Dutch higher education?"	Expert interviews
SQ4:	"Which cyber treats related to shadow IT are perceived by experts?"	Expert interviews
SQ5:	"Which recurring patterns can be identified in these occurences and cyber threats?"	Synthesis of SQ3 and SQ4

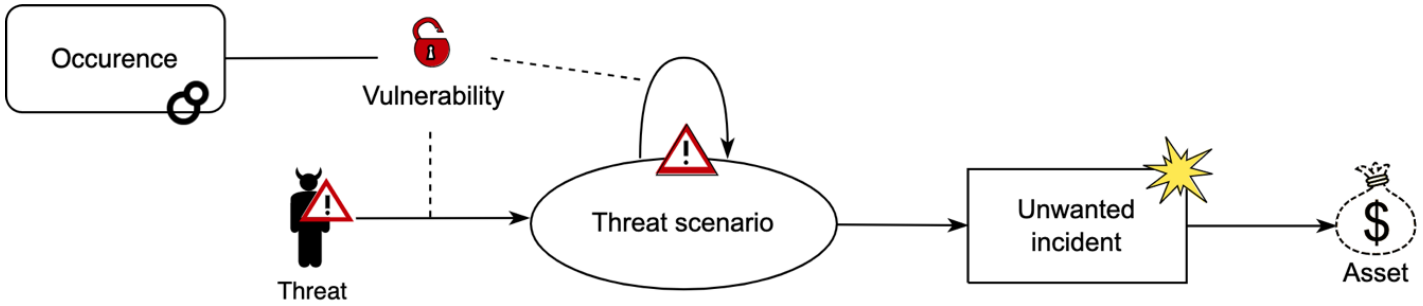
Data Analysis

Coding process:

- Open coding
- Axial coding with some emerging and some pre-defined semantic domains:

Codebook reliability:

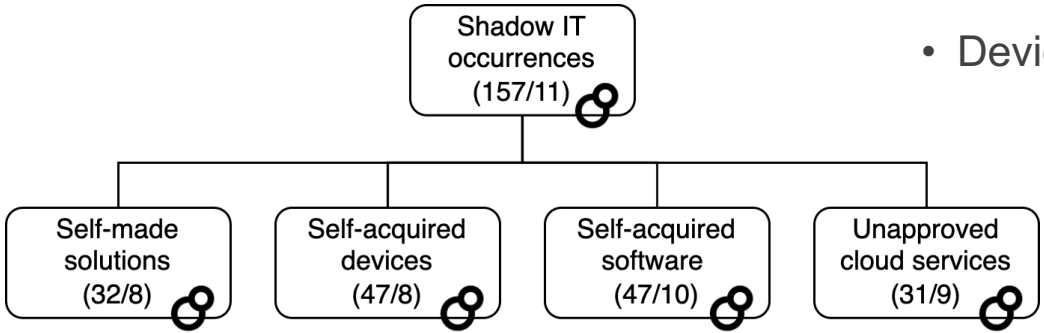
- 2 researchers coded 11 interviews
- Code saturation: 1,35% new codes after 10 interviews
- 104 codes, applied 726 times



Meta model of Semantic Domains based on CORAS (Lund et al., 2011)

Occurrences

- Divided into a topology of shadow IT, adapted from Mallmann et al. (2019)
- Everything exists, highly different between institutions

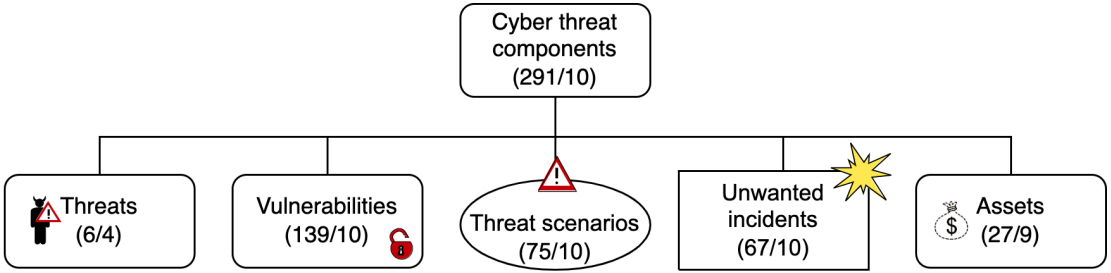


- Software is top-of-mind
- Especially cloud services can be very small or very large
- Self-developed applications in research are unique
- Devices add variety

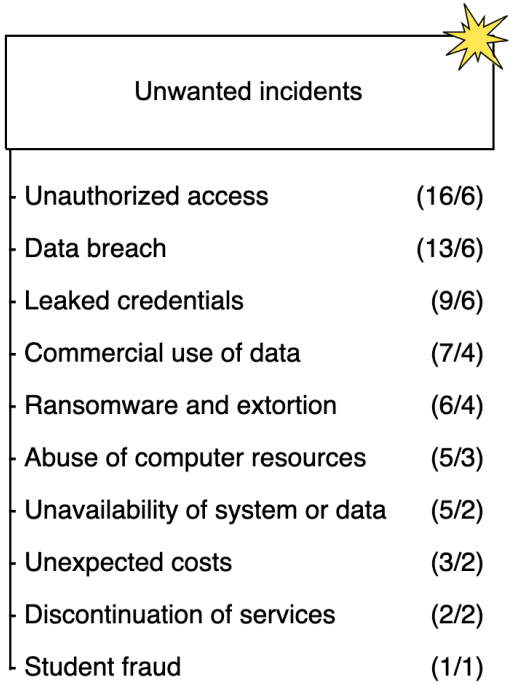
Overview of Shadow IT occurrence categories

Threat Components

- Captured with the lens of CORAS (Lund et al., 2011) to operationalize ‘cyber threat’
- Experts focused on vulnerabilities, scenarios and incidents; rest is left implicit

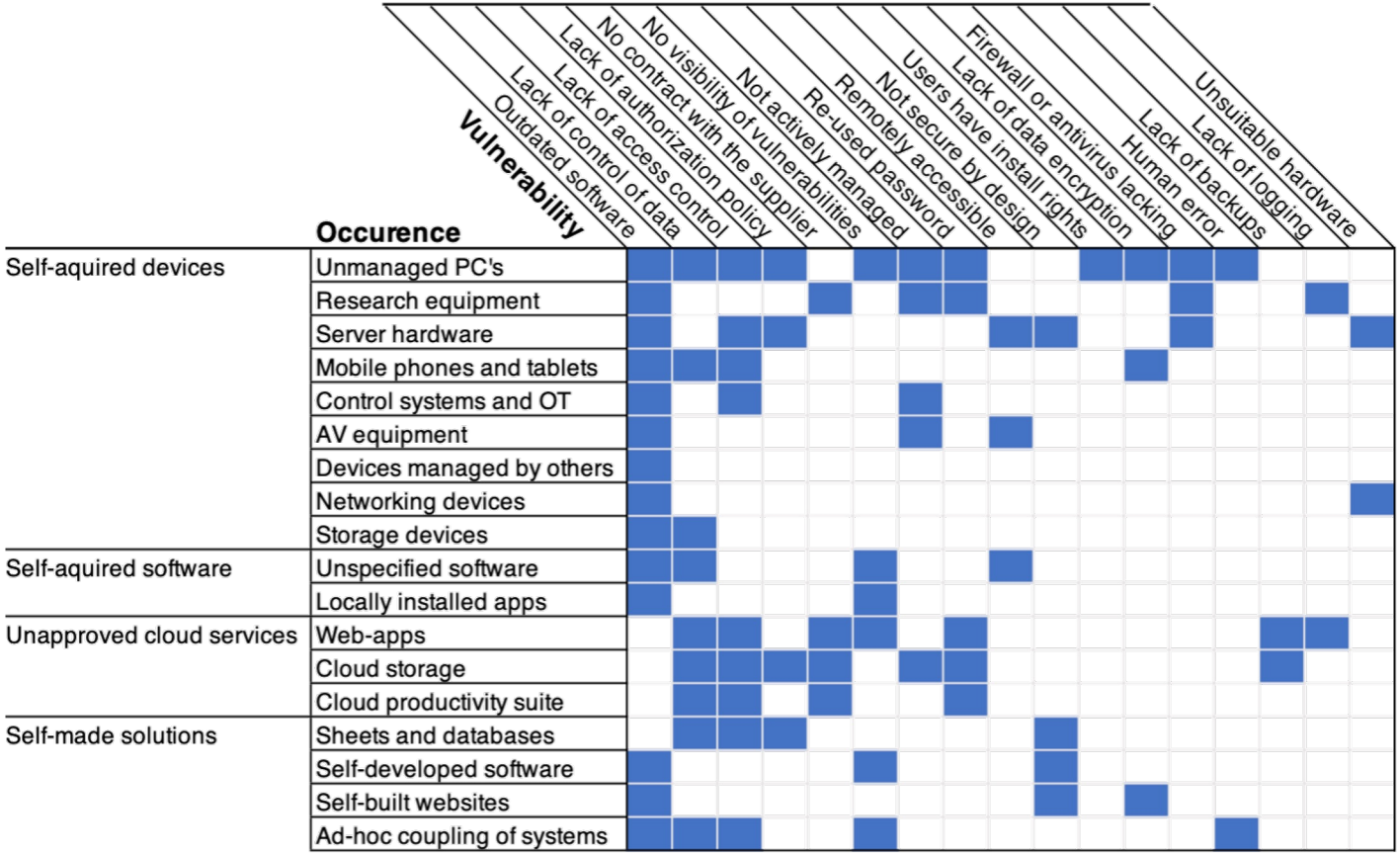


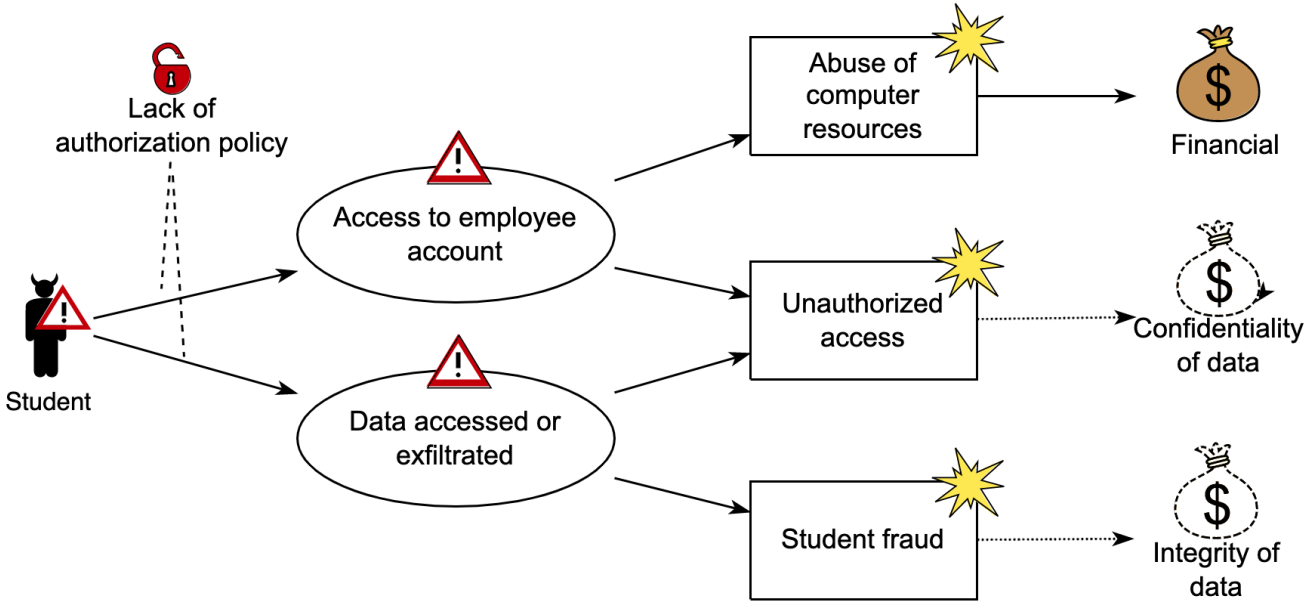
Overview of Threat Component categories

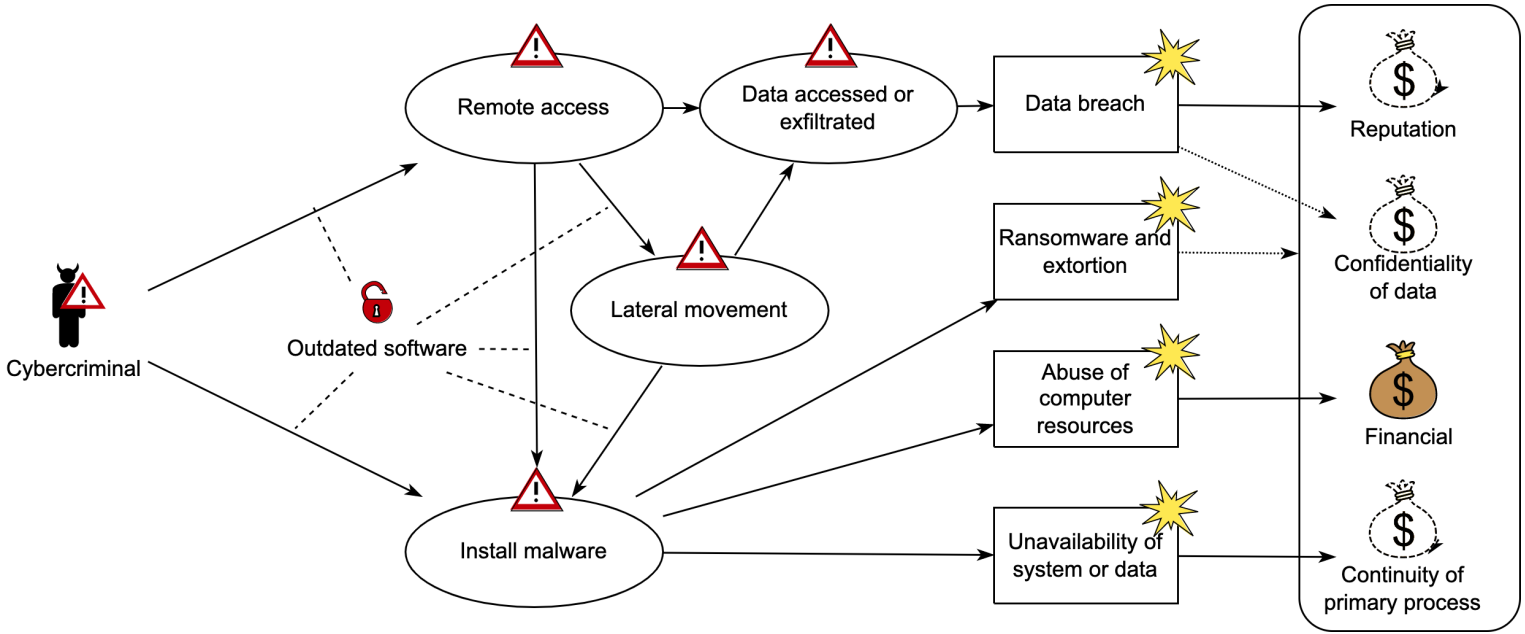


Linking them!

- Also served as input to prioritize the modelling of attack paths




Lack of
authorization policy
Student
Access to employee
account
Data accessed or
exfiltrated
Abuse of
computer
resources
Unauthorized
access
Student fraud
Financial
Confidentiality
of data
Integrity of
data


Remote access
Data accessed or exfiltrated
Data breach
Reputation
Ransomware and extortion
Confidentiality of data
Lateral movement
Cybercriminal
Outdated software
Abuse of computer resources
Financial
Install malware
Unavailability of system or data
Continuity of primary process

Takeaways from the Modelling of Attack Paths

- Three main cases:
  1) The ‘classic’ network infiltration scenario (a ‘Maastricht’)
  2) Lack of control of data causing unintended harm
  3) Misconfigurations causing problems between users
- The detailed modelling allowed for linking to solutions
- Many scenario’s could be linked to solutions. Problems dependend on the institutions’ measures already in place

Limitations

- Modeling remains an exercise in semantics and ontology
- Complete overview of occurrences and threats, but not of the links between them
- ‘How often named’ is an indicator for importance
- Results on prevention, detection and mitigation were not anticipated

Conclusions

MRQ: “What is the role of shadow IT in the cyber threat landscape of Dutch higher education institutions?”

- Shadow IT is an inherent part of HEIs IT environment
- Three main scenarios
- The role of shadow IT in the cyber threat landscape can be very manageable when assumed and accounted for

Shadow IT *problems* can be

- **Prevented** with guidance, policy and usable official solutions that are aligned to user needs
- **Detected** with monitoring and scanning, and by keeping users on managed devices for as long as possible
- **Mitigated** by many already known technical measures
  - Multi-factor authentication
  - Zero-trust network architecture
  - Mobile device management
  - Proper password policies
  - Endpoint detection and response
  - …

Shadow IT *problems* can be Prevented

“And we are also pushing [departments] to play a role in this with [IT] coaches and little teams that will also think within such a [department] about: yes, ***what do we need? What will we face in the future?*** *What is our teaching staff working on? What IT support do they have? That starts slowly, starts growing and, yeah, starts to work. I think that will become the best solution or the biggest solution for shadow IT: to just* ***have that conversation*** *[...] so that people can voice their desires and needs somewhere.”*

"I do notice that in the past, we had a lot more shadow IT. See, it used to be very easy for a user to walk to [an electronics store] and buy [a network attached storage] system and put it under their desk. [...] ***At one point we adopted the policy of: yes, we can also manage that kind of thing.*** *We are not going to get fussy about that. [...] If you want, we also manage your [storage] [...]. But next time, preferably don't do it.”*

“That is also why ***we have deployed large-scale central storage in various flavors****. Very good ones with redundancy, backup, ransomware protection, and things like that. A very cheap one, which is* ***cheaper than any commercial provider****.”*

Shadow IT *problems* 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, is quickly connected, without them requesting a separate connection for it, for example. You come across things like that. [...] We use a security system, **intrusion detection, and protection system on our network**. And it has been able to stop quite a few attacks over the years we have been using it. So in that respect, I am less afraid than at an average other institution."*

*"**If you lose your managed laptop, then you can sleep easy**. If you lose your [unmanaged laptop], then sorry, you have to solve it yourself. We are trying to change that with different programs, so **mobile device management** for example. But you notice, that because those devices are actually owned by the [department], you do get resistance to those kinds of efforts."*

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

Shadow IT *problems* can be Mitigated

- Basic security measures (source: english.ncsc.nl)
- Problems depend on these measures

- Help them with:
  - Data classification, least privilege
  - Security awareness and culture

Shadow IT *problems* can be

- **Prevented** with guidance, policy and usable official solutions that are aligned to user needs
- **Detected** with monitoring and scanning, and by keeping users on managed devices for as long as possible
- **Mitigated** by many already known technical measures
  - Multi-factor authentication
  - Zero-trust network architecture
  - Mobile device management
  - Proper password policies
  - Endpoint detection and response
  - …

tnc23
DIGITAL GENERATIONS
TIRANA, ALBANIA | 5-9 JUNE 2023

Thank you

Any questions?

joost.gadellaa@surf.nl

Full thesis:

edu.nl/683h9

GÉANT
Co-funded by the European Union
SURF
Utrecht University

References

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & Security, 86, 350–357.

Kopper, A., & Westner, M. (2016). Towards a Taxonomy for Shadow IT. AMCIS 2016 Proceedings. Americas Conference on Information Systems.

Lund, M. S., Solhaug, B., & Stølen, K. (2011). Model-Driven Risk Analysis. Springer Berlin Heidelberg.

Mallmann, G. L., de Vargas Pinto, A., & Maçada, A. C. G. (2019). Shedding Light on Shadow IT: Definition, Related Concepts, and Consequences. Lecture Notes in Information Systems and Organisation, 31, 63–79.

Cyber Threats of Shadow IT in Dutch Higher Education and Research

Joost Gadellaa, SURF

TNC23; Tirana, Albania

GÉANT
Co-funded by the European Union
SURF
Utrecht University