Shadow IT Mindsets of Corporate Employees

PhDs in Computer Security Workgroup meeting

Jan-Philip van Acken
j.vanacken@uu.nl

PhD student
Software Ecosystem Security group
Utrecht University

Image credits: David Revoy
See table on page 25 for attributions

2024-04-30

Universiteit Utrecht

Definitions

Definition

MINDSET:

- (mental) representation of concepts or ideas
- shorthand for reality ⟹ reducing complexity

Definition

SHADOW IT:

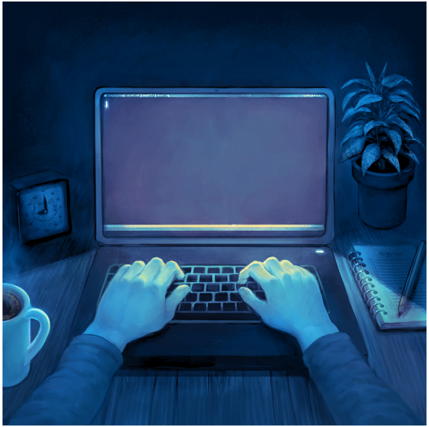
"hardware, software, or services built, introduced and/or used for the job without explicit approval or even knowledge of the organisation." [Haag and Eckhardt, 2017]

Shadow IT topology

Type	Description
Unapproved cloud services	Use of Internet-based Software and Software as a Service (SaaS) that are not approved or unknown by the IT department. (. . .)
Self-made solutions	Use of solutions developed by employees on the company's computers to perform their work tasks. For example, an Excel spreadsheet or an application developed by employees.
Self-installed applications	Use of software installed by employees to perform their work tasks on the company's computers. For example, downloading and installing software available free of charge on the internet.
Self-acquired devices	Use of devices owned by employees. These devices are purchased directly from retail rather than being ordered through the official catalog of the IT department. It includes the use of applications in the employee's personal devices at the workplace.

Shadow IT topology – [Mallmann et al., 2019]

Motivation



Shadow IT

- Not a new trend!
- Present in corporate settings as well as higher education [Gadellaa, 2023]

Shadow IT as a threat?!

Search & destroy approach $\Longrightarrow$ reduction of threats *for now*

Questions:

- Can we handle this differently?
- Should we handle this differently?

PhD School on Empirical Research Methods in Software Engineering and Informatic - **Cybersecurity Edition**

ERMSEI

When: May 13-17, 2024

Where: Utrecht

- deep dive into controlled experiments, qualitative methods, study design
- 2EC course, sponsored by SIKS & ACCCS
- possibility to work on your case/data!
- cosy class, max 25 participants
- instructors: Harald Störrle & Kate Labunets

PhD School ERMSEI - **Cybersecurity Edition**

Program & details

edu.nl/gnrnd

Sign-up

edu.nl/nhmcd

Related publication preview

Who is the IT Department Anyway: An Evaluative Case Study of Shadow IT Mindsets Among Corporate Employees *(under submission)*

(a) Jan van Acken

(b) Floris Jansen

(c) Slinger Jansen

(d) Kate Labunets

Focus: implications of shadow IT mental models for/in a large organization

Study context

- Dutch branch of a large professional services organisation, 5k+ employees
- Departments:
  - Client-facing, Support, IT, Management
- Ranks:
  - Junior, Senior, Manager, Senior Manager, Management
- Survey on shadow IT usage ($n = 450$)
- Follow-up interviews ($n = 32$)

Questioning shadow IT in companies:

Research Question I – SURVEY

How does SHADOW IT usage differ between DEPARTMENTS and RANKS?

Research Question II – INTERVIEW

How do employees perceive SHADOW IT and risks associated with its usage?

Research Question III – INTERVIEW

Which MINDSET motivates employees to opt for (or against) SHADOW IT usage in an organisational context?

Survey result: Usage percentage of *any* Shadow IT per scenario

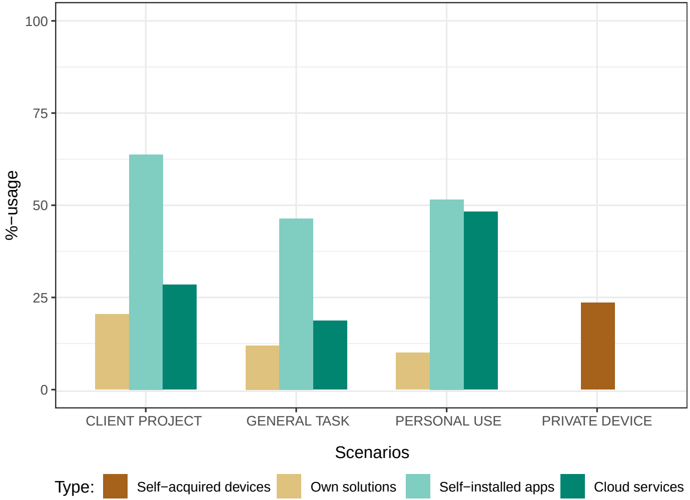


Figure: Rate of participants using at least one form of shadow IT. Grouped by scenarios, plus the rate of reported private device usage overall. (n=450)

Interview components:

	Jun.	*Sen.*	*Mngr*	*Sen. mngr*	*Mngmnt*	**Total**
Client-fac.	6	4	5	6	-	21
Support	1	2	3	1	-	7
Mngmnt	-	-	-	-	4	4
IT	0	0	0	0	-	0
Total	7	6	8	7	4	**32**

Topics covered

1. understanding of shadow IT
2. reasons for using shadow IT
3. perception of shadow IT usage implications
4. awareness of relevant org policies
5. how shadow IT is discussed amongst colleagues
6. how well-informed about shadow IT

General observations on what drives Shadow IT usage

- Approved solutions fail to meet functional needs
- Work requirement / client project demand
- Existing habits, convenience
- Overcoming *limitations* of current IT environment

The 10 mindsets elicited by Floris Jansen

Risk-Averse

1. Consequence Avoidance Orientation
2. Knowledge-Based Conservatism
3. Risk Transfer Mindset
4. Cautious-Seasoned Judgement

Risk-Taking

5. Common Sense Fallacy
6. Illusion of Self-Sufficiency
7. Misguided Sense of Protection
8. Performance-Driven Rule Bending
9. Longevity-Based Invincibility
10. Cost-Driven Compromise

Risk-Averse Mindsets 1-2

Consequence Avoidance Orientation

"Think about all the consequences. I think those hold the biggest risks. Which is also the reason I don't have anything external" –P19

Knowledge-Based Conservatism

"I am very aware of all sorts of risks. It is because of my role as [role]. So, therefore, I am aware of certain things that the average Joe here won't think of" –P7

Risk-Averse Mindsets 3-4

Risk Transfer Mindset

"I would try and let the client take responsibility for the risk. Because they are the ones asking for this tool.(. . .)" –P22

Cautious-Seasoned Judgement

"I have seen it all, but actually you should go through a data breach once just to see how bad it really is. After that, you'll think twice about your actions. You learn this through trial and error over the years" –P30

Risk-Taking Mindsets 5-6

Common Sense Fallacy

"Look, in our department, they just expect you to know this stuff. (. . .)" –P18

Illusion of Self-Sufficiency

"(. . .) we have everything taken care of" –P6

"(. . .) we have everything that we need" –P19

Risk-Taking Mindsets 7

Misguided Sense of Protection

“(. . .)I think they watch what you downloaded, and if it is not okay then maybe it will go through a system that detects this, or maybe there is a team that reads everything, and you then get a message to delete it from your machine” –P15

“And also you get a warning I think at [organisation] if you have something on your system which is not good [...]” –P5

Risk-Taking Mindsets 8

Performance-Driven Rule Bending

"I cannot explain to a client that certain tasks have not been completed. This means that sometimes employees enter a grey area, perhaps even cross it by doing what they shouldn't. " –P20

"The main issue with that is that the show must go on" –P20

Risk-Taking Mindsets 9-10

Longevity-Based Invincibility

"We've used it for so long without any issues (. . .) sometime a while ago it was introduced and it has stayed up until now (. . .) over time it has grown to what it is now for us." –P12

Cost-Driven Compromise

"I wonder about, for example [tool], since we used it because it provides a free package. One might wonder how good that is (. . .)" –P5

What to do about Shadow IT? 1/2

- Transparent communication
  - safe space for employees to communicate their tech needs
- Targeted Shadow IT awareness training
  - tailor training to the need of roles, departments, mindsets
- Shadow IT protocols
  - how to navigate *rule bending* situations

What to do about Shadow IT? 2/2

- Track long-term instances
    - Once found: try uncovering the reasons for adoption!
- Make security policies visible
    - targeting people influenced by mindsets like COMMON SENSE FALLACY and/or MISGUIDED SENSE OF PROTECTION
- Accommodate employees' perspective and needs
    - usable software, usable security, useful training

Future work

What's on your mind concerning mindsets?

Current set of mindsets are not validated yet, some seem close to established BIASES.

Is the set EXHAUSTIVE?

Can we use established models from the SECURITY BEHAVIOUR field to validate?

What about STABILITY OVER TIME?

How can we model INTERACTION between mindsets?

That's all for now

Questions welcome

If you want to stay in touch:

Get in touch for an authors copy!
Especially get in touch with ideas for model validation or enrichment!
Did we miss anything?

Mail:
j.vanacken@uu.nl
Mastodon:
@jpvanacken@social.edu.nl
@jpvanacken@scholar.social

Sources

- Submission based on the Master thesis of Floris Jansen
- Slide content inspired by the “Enhancing Information Security” slide deck by Kate Labunets from the 2023 Meetup “Resilience against ransomware”
- Content furthermore based on the “Cybersecurity Mental Models and Shadow IT Mindsets” slide deck by Jan van Acken from the 2023/24 edition of the Utrecht University course “Software Ecosystem Security”
- Slide themed after the LaTeX template from the UU NLP group, cf. github.com/Yupei-Du/uunlp-group-meeting/tree/main/UU_unofficial_LaTeX_template

Image sources

Slide	Reference
4	“The mediocre programmer” by David Revoy - CC-BY 4.0
7	authors’ personal files
8	“F5 CHATONS” by David Revoy, Framasoft.org - CC-BY 4.0
14	“Ninja Carrot” by David Revoy - CC-BY 4.0
15	“Powerful” by David Revoy - CC-BY 4.0
16	“Contribateliers” by David Revoy, Framasoft.org - CC-BY 4.0
18	“Peertube Plugin” by David Revoy, Framasoft.org - CC-BY 4.0
19	“This is not fine” by David Revoy, CC-BY 4.0
23	“Des Livres En Commun” by David Revoy, Framasoft.org - CC-BY 4.0

Bibliography

Gadellaa, J. (2023).
Cyber Threats of Shadow IT in Dutch Higher Education and Research.
https://studenttheses.uu.nl/handle/20.500.12932/45731.

Haag, S. and Eckhardt, A. (2017).
Shadow IT.
BUS INF SYST ENG, 59(6):469–473.

Kopper, A. and Westner, M. (2016).
Towards A Taxonomy for Shadow IT.
Americas Conference on Information Systems.

Mallmann, G. L., de Vargas Pinto, A., and Maçada, A. C. G. (2019).
Shedding Light on Shadow IT: Definition, Related Concepts, and Consequences.
In *Information Systems for Industry 4.0*, Lecturenotes in information systems and organisation, pages 63–79. Springer International Publishing.

Appendix

Shadow IT and related but different concepts

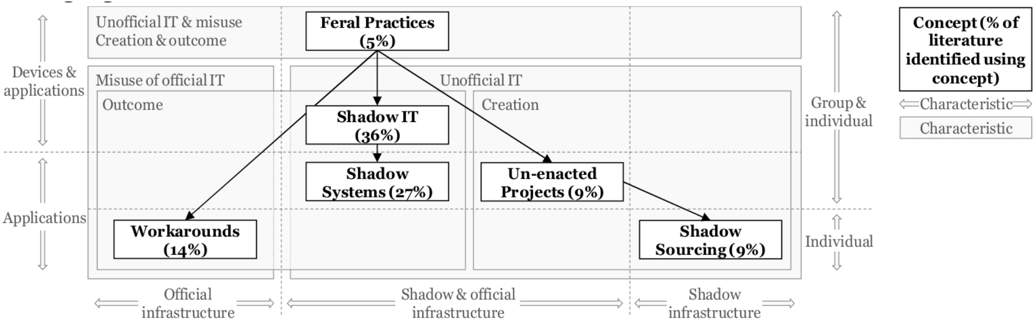
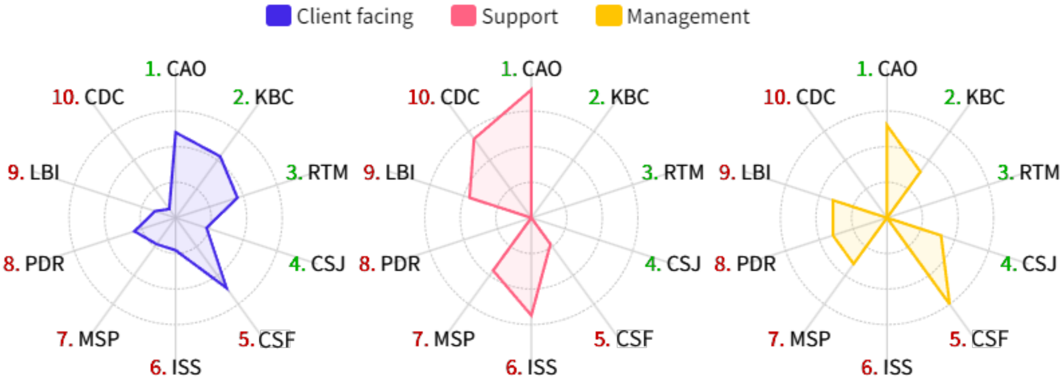
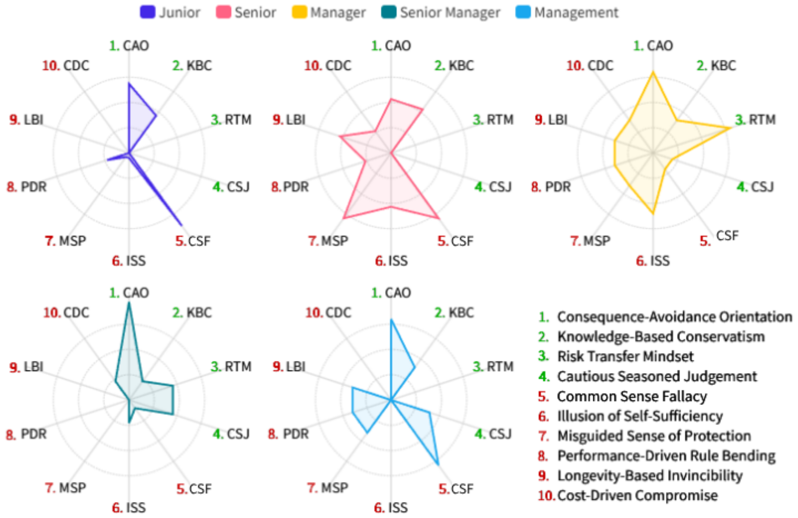


Figure source: [Kopper and Westner, 2016]

Mental models by department



Mental models by rank



1. Consequence-Avoidance Orientation
2. Knowledge-Based Conservatism
3. Risk Transfer Mindset
4. Cautious Seasoned Judgement
5. Common Sense Fallacy
6. Illusion of Self-Sufficiency
7. Misguided Sense of Protection
8. Performance-Driven Rule Bending
9. Longevity-Based Invincibility
10. Cost-Driven Compromise