Social Engineering Academy

mobile business

Goethe Universität Frankfurt am Main

Human Factors in Security Management, Social Engineering & Privacy Enhancing Technologies

Dr. Sebastian Pape

Cyber Security for Europe

ARTHREAT ST

Motivation

- Interaction: humans and technology
- Many 'problems' technically solved
  - e.g. encryption
- But…
  - Users can also be attacked
    → can be weakest link
  - Best choice often not clear
    → decision support needed
  - Users do not use technology
    → technology acceptance
    needs to be considered

Agenda

- **Social Engineering**
  - Tool Support
  - Threat Elicitation
  - Awareness Training

- **Security Management**
  - Risk Assessment / Management
  - Decision Support

- **Privacy Enhancing Technologies**
  - Technology Acceptance
  - Economical Interests
  - Privacy by Design

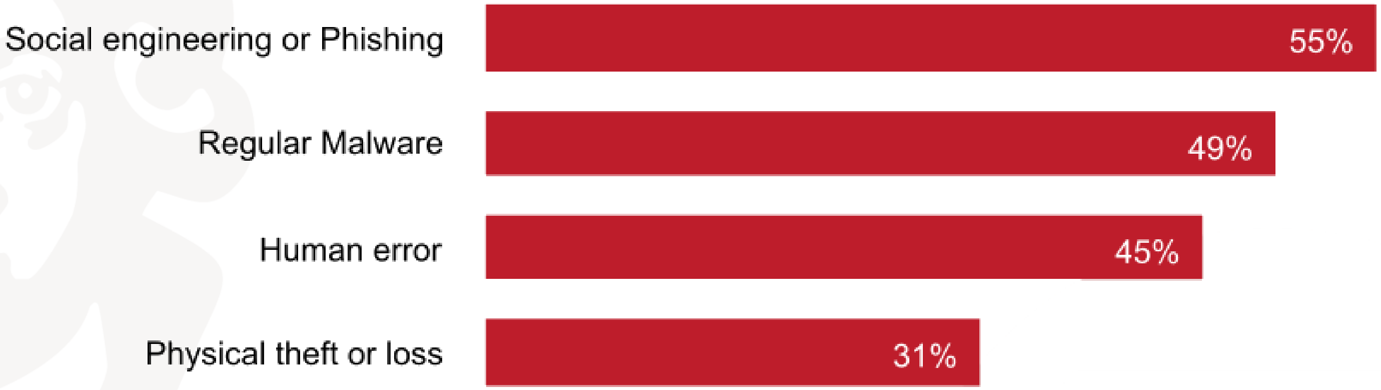
Social Engineering

Social Engineering

Social Engineering
The clever **manipulation** of the natural human tendency to trust!

Source: cybertec-security.com

Breach vectors leading to compromise:



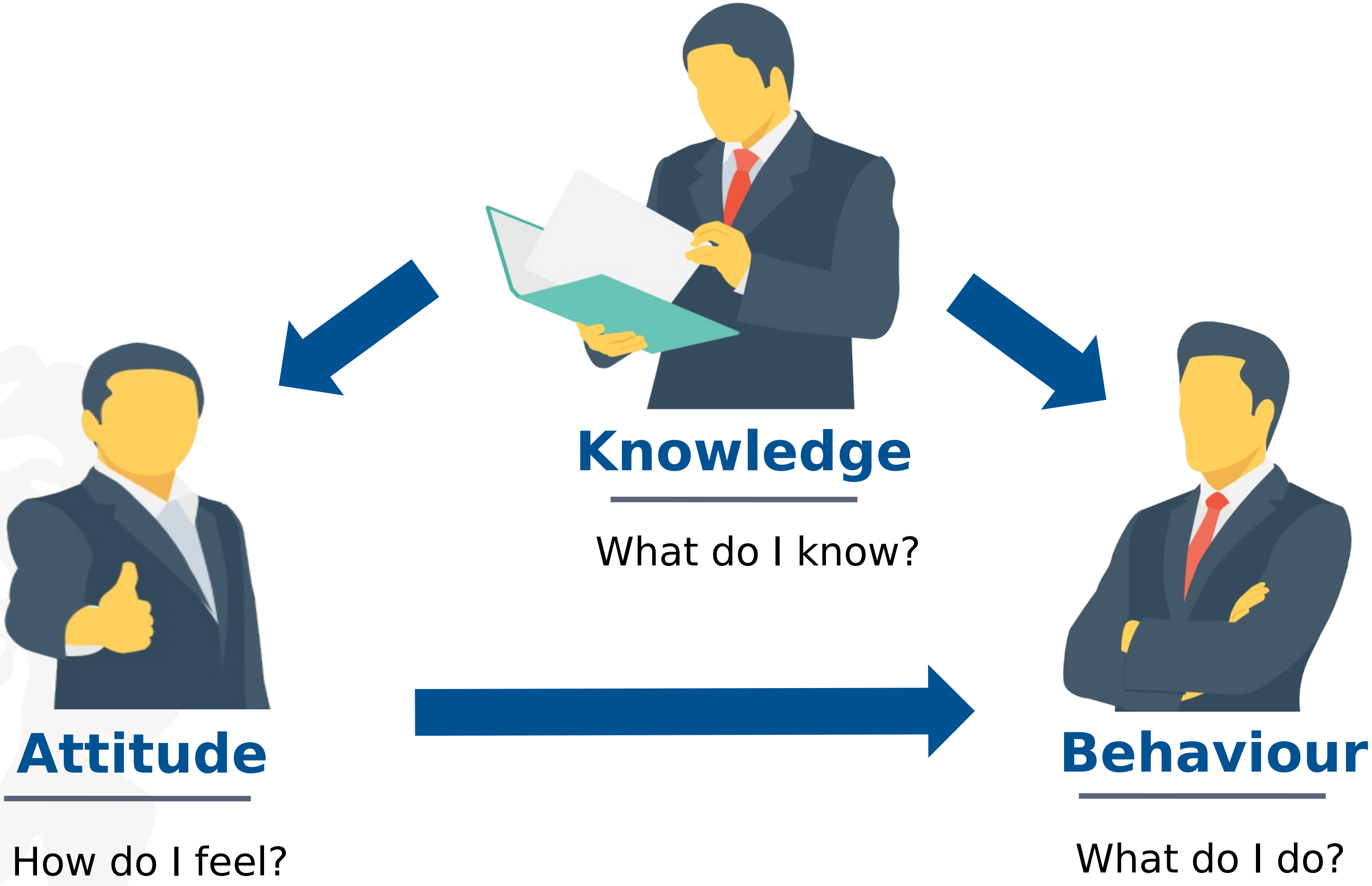
Source: PWC Information Security Breaches Survey 2017

Social Engineering Tools

- Most tools only for collecting information (1 exception)
- No support for defenders, e.g. for
  - Risk management
  - Creation of security policies
- Prediction
  - More data available
  - Use of artificial intelligence
    - e.g. synthesized speech

Beckers, K.; Schosser, D.; Pape, S. and Schaab, P.: A Structured Comparison of Social Engineering Intelligence Gathering Tools. In Trust, Privacy and Security in Digital Business - 14th International Conference, TrustBus 2017

Security Awareness



Knowledge

What do I know?

Attitude

How do I feel?

Behaviour

What do I do?

Peter Schaab, Kristian Beckers, and Sebastian Pape. Social engineering defence mechanisms and counteracting training strategies. Information and Computer Security, 25(2):206–222, 2017

Social Engineering Defense

Dimension		IT Defense Mechanism	Psychological Defense Mechanism
Knowledge	Attitude	Policy Compliance	---
		Security Awareness Program	Forewarning
		---	Persuasion Knowledge
		---	Attitude Bolstering
		---	Reality Check
	Behaviour	Audit	---
		---	Inoculation
		---	Decision Making

Peter Schaab, Kristian Beckers, and Sebastian Pape. Social engineering defence mechanisms and counteracting training strategies. Information and Computer Security, 25(2):206–222, 2017

Idea: Serious Games

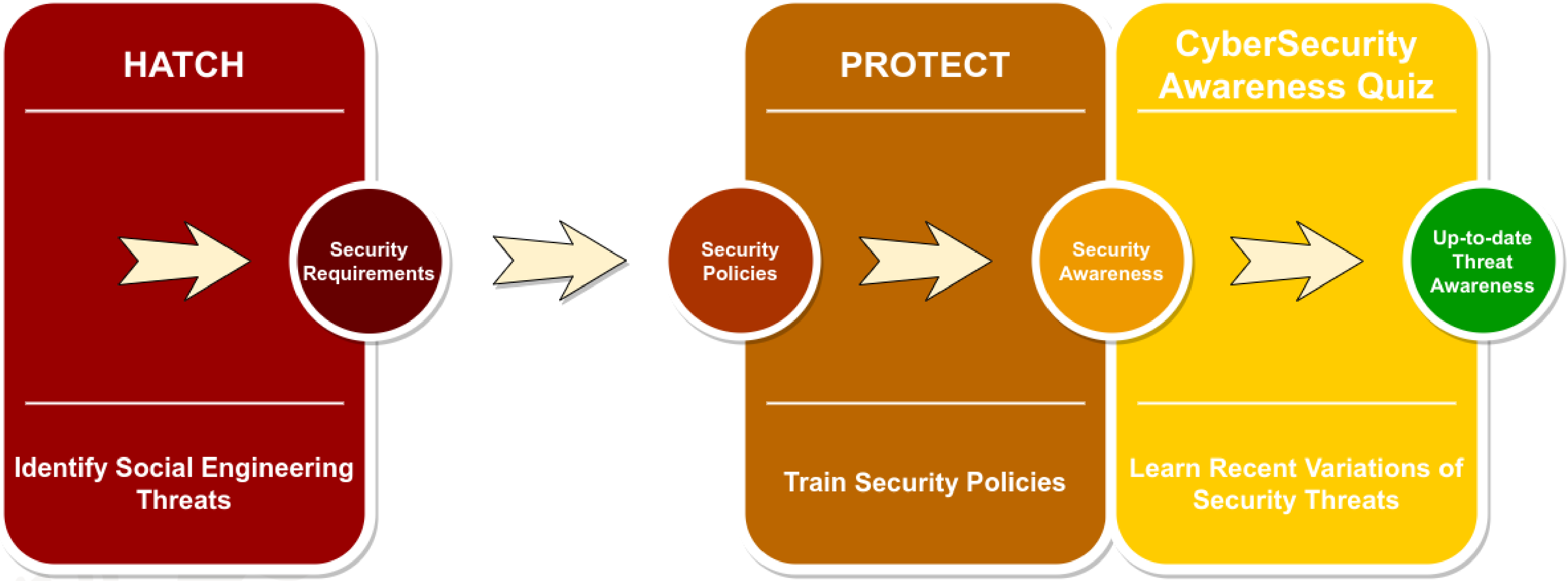
- Games can be fun
  → gets employees involved

- Games provide a realm
  → encourages employees to be creative

- Fictional situations are discussed in the game
  → no one is to blame

- Games are intended to be engaging and entertaining
  → which gets employees to play again and again

Serious Games



HATCH

Security Requirements

Identify Social Engineering Threats

PROTECT

Security Policies

Train Security Policies

CyberSecurity Awareness Quiz

Security Awareness

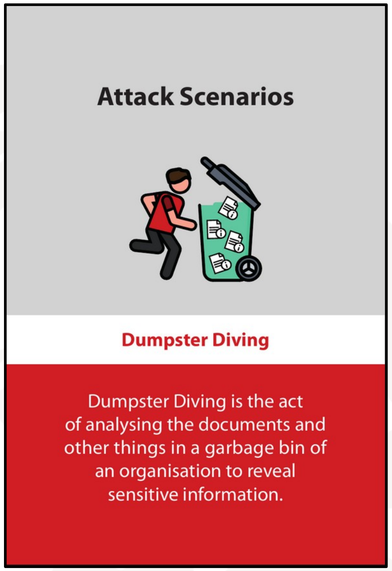
Up-to-date Threat Awareness

Learn Recent Variations of Security Threats

SOCIAL ENGINEERING ACADEMY

6. Deutscher IT-Sicherheitspreis 2016

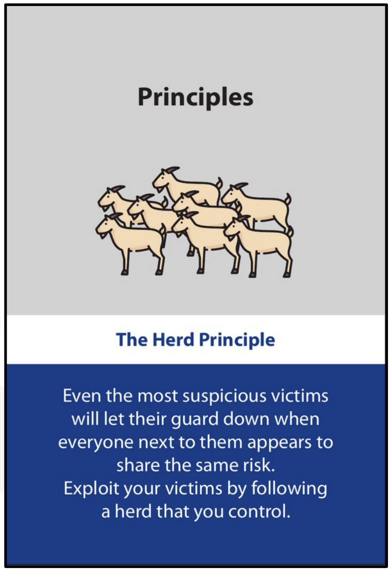
3. Preis



Attack Scenarios

Dumpster Diving

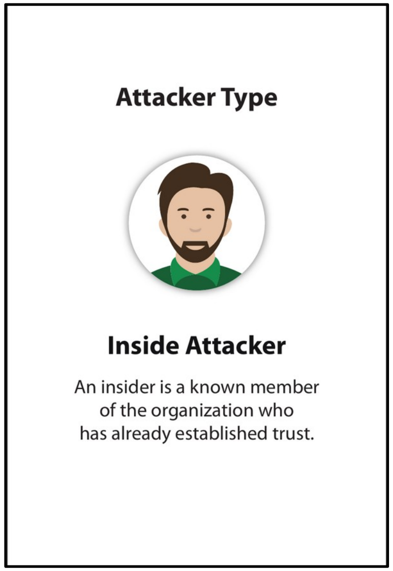
Dumpster Diving is the act
of analysing the documents and
other things in a garbage bin of
an organisation to reveal
sensitive information.



Principles

The Herd Principle

Even the most suspicious victims
will let their guard down when
everyone next to them appears to
share the same risk.
Exploit your victims by following
a herd that you control.



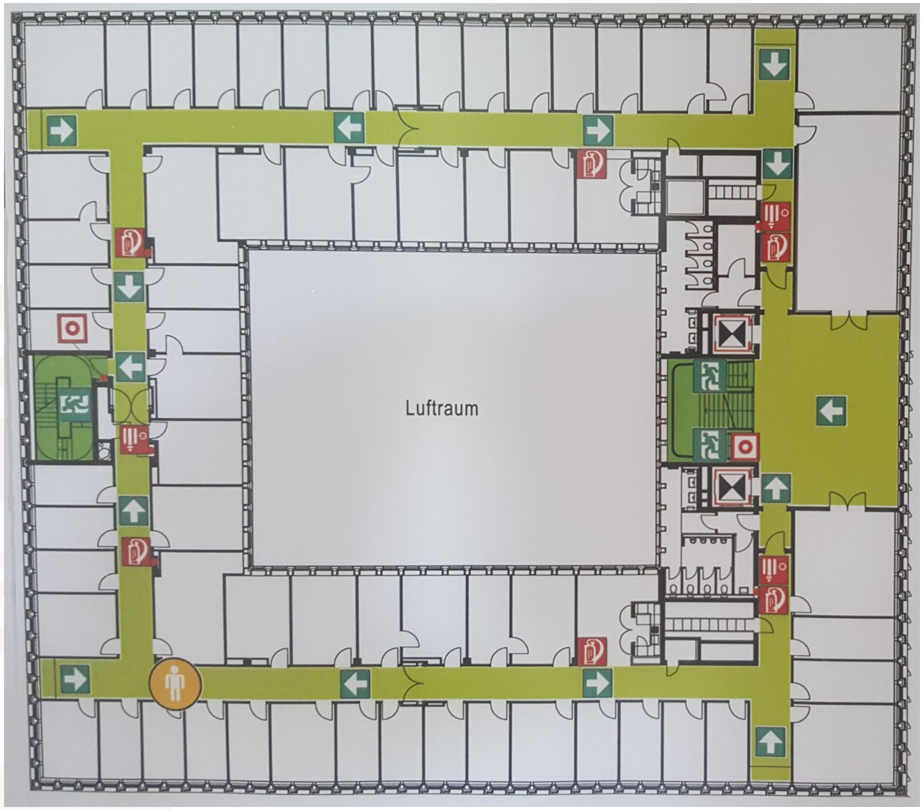
Attacker Type

Inside Attacker

An insider is a known member
of the organization who
has already established trust.

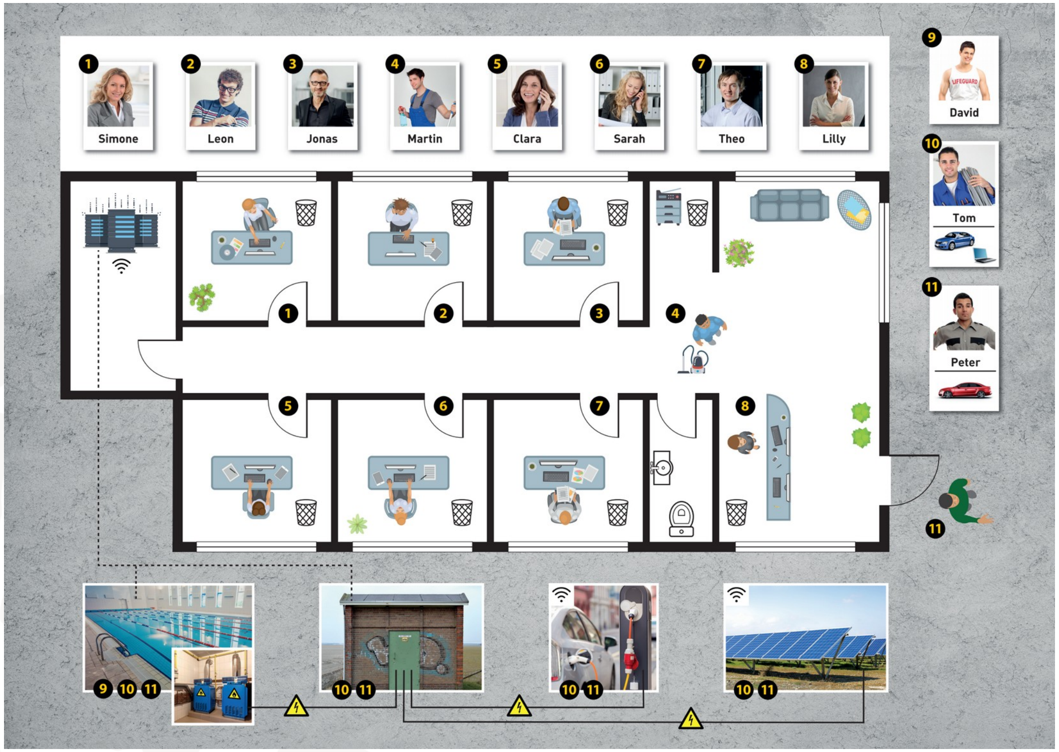
Design: Kristina Femmer

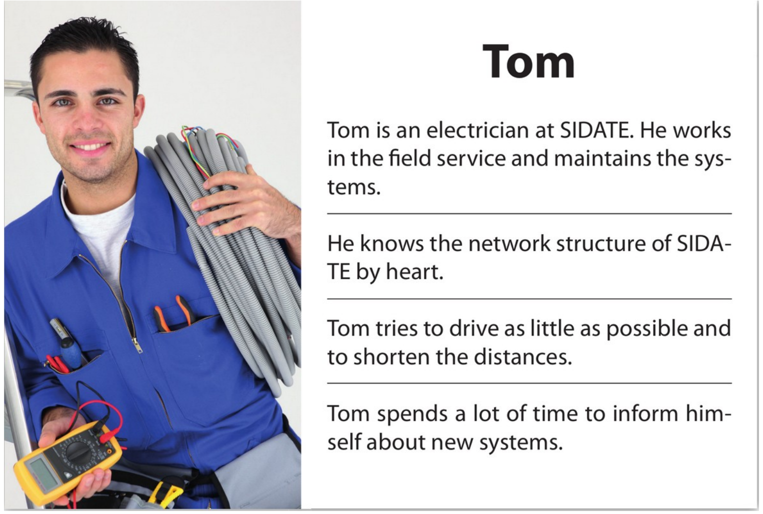
Real World: Threat Elicitation



Kristian Beckers and Sebastian Pape. A serious game for eliciting social engineering security requirements. In Proceedings of the 24th IEEE International Conference on Requirements Engineering, RE '16. IEEE Computer Society, 2016

Virtual Scenario: Training





Tom

Tom is an electrician at SIDATE. He works in the field service and maintains the systems.

He knows the network structure of SIDATE by heart.

Tom tries to drive as little as possible and to shorten the distances.

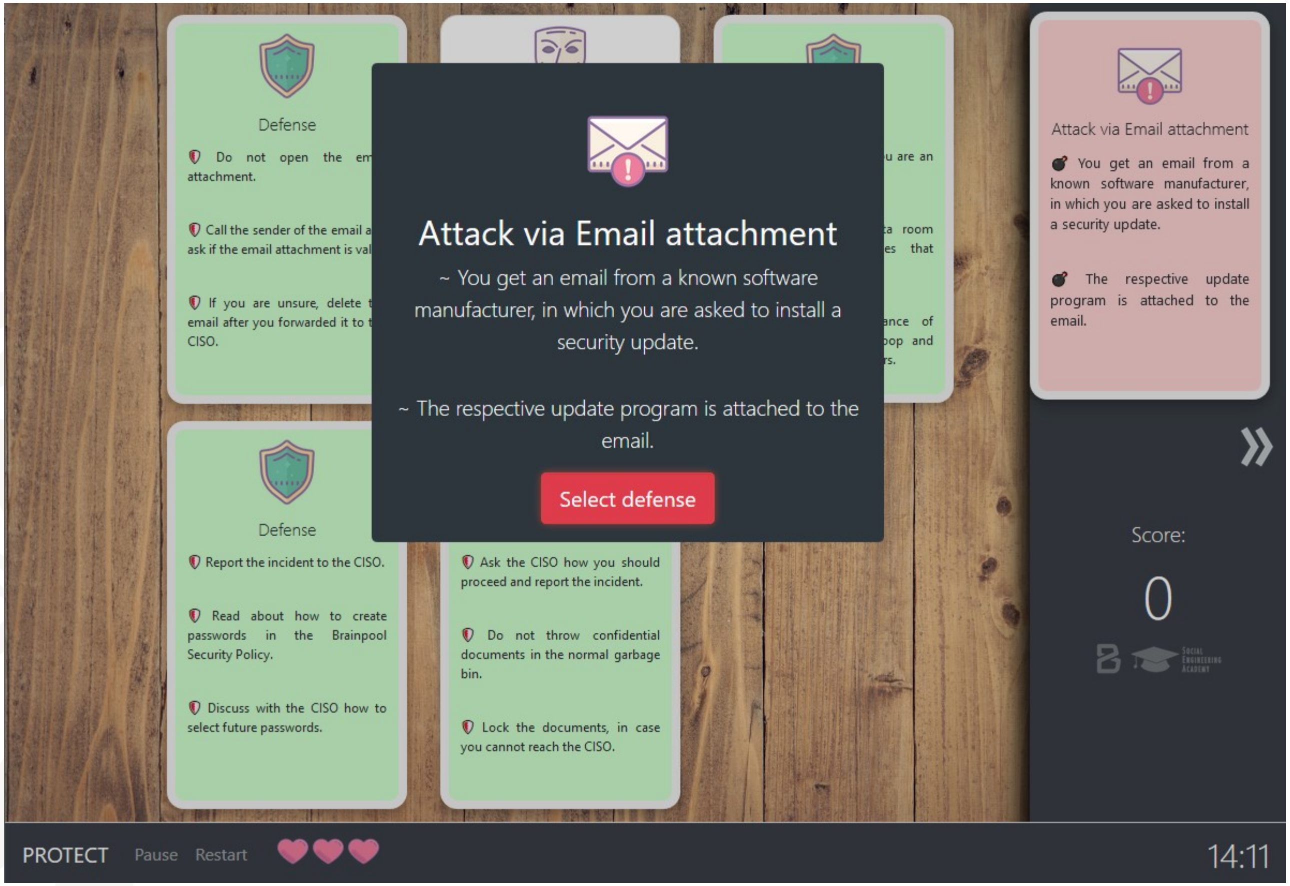
Tom spends a lot of time to inform himself about new systems.

Design: Kristina Femmer

Kristian Beckers, Sebastian Pape, and Veronika Fries. HATCH: Hack and trick capricious humans – a serious game on social engineering. In Proceedings of the 2016 British HCI Conference, Bournemouth, United Kingdom, July 11-15, 2016.

PROTECT

GOETHE UNIVERSITÄT FRANKFURT AM MAIN



Defense

Do not open the em attachment.

Call the sender of the email a ask if the email attachment is val

If you are unsure, delete t email after you forwarded it to t CISO.

u are an

a room es that

ance of pop and rs.

Attack via Email attachment

~ You get an email from a known software manufacturer, in which you are asked to install a security update.

~ The respective update program is attached to the email.

Select defense

Attack via Email attachment

You get an email from a known software manufacturer, in which you are asked to install a security update.

The respective update program is attached to the email.

Defense

Report the incident to the CISO.

Read about how to create passwords in the Brainpool Security Policy.

Discuss with the CISO how to select future passwords.

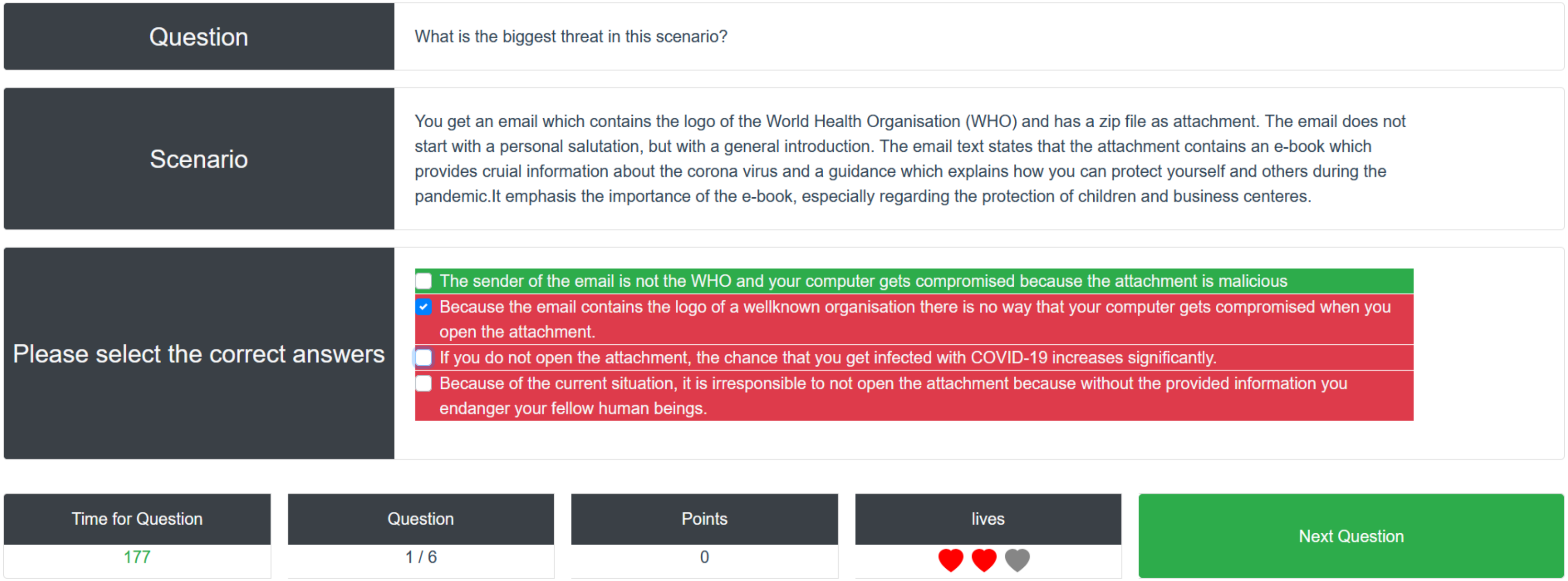
Ask the CISO how you should proceed and report the incident.

Do not throw confidential documents in the normal garbage bin.

Lock the documents, in case you cannot reach the CISO.

Ludger Goeke, Alejandro Quintanar, Kristian Beckers, and Sebastian Pape. PROTECT - an easy configurable serious game to train employees against social engineering attacks. In Computer Security - ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC, volume 11981 of Lecture Notes in Computer Science, 2019.

CyberSecurity Awareness Quiz



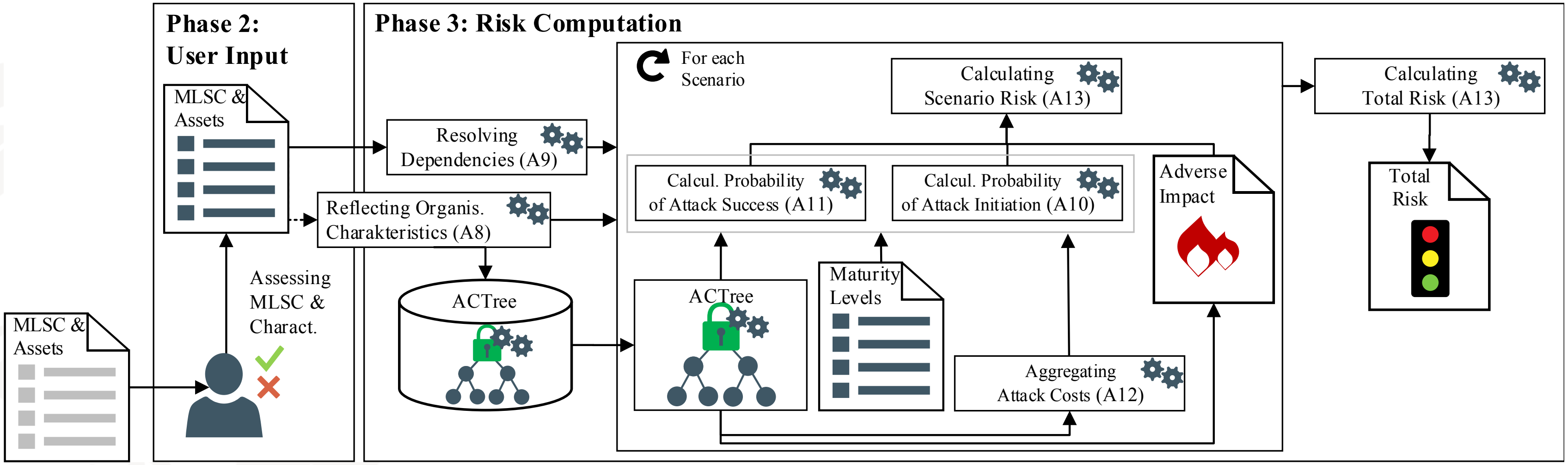
Question	What is the biggest threat in this scenario?
Scenario	You get an email which contains the logo of the World Health Organisation (WHO) and has a zip file as attachment. The email does not start with a personal salutation, but with a general introduction. The email text states that the attachment contains an e-book which provides cruial information about the corona virus and a guidance which explains how you can protect yourself and others during the pandemic.It emphasis the importance of the e-book, especially regarding the protection of children and business centeres.
Please select the correct answers	□ The sender of the email is not the WHO and your computer gets compromised because the attachment is malicious ☑ Because the email contains the logo of a wellknown organisation there is no way that your computer gets compromised when you open the attachment. □ If you do not open the attachment, the chance that you get infected with COVID-19 increases significantly. □ Because of the current situation, it is irresponsible to not open the attachment because without the provided information you endanger your fellow human beings.

Time for Question	Question	Points	lives
177	1 / 6	0	♥ ♥ ♡

Sebastian Pape, Ludger Goeke, Alejandro Quintanar, and Kristian Beckers. Conceptualization of a cybersecurity awareness quiz. In Computer Security - ESORICS 2020 International Workshops MSTEC, 2020.

Security Management

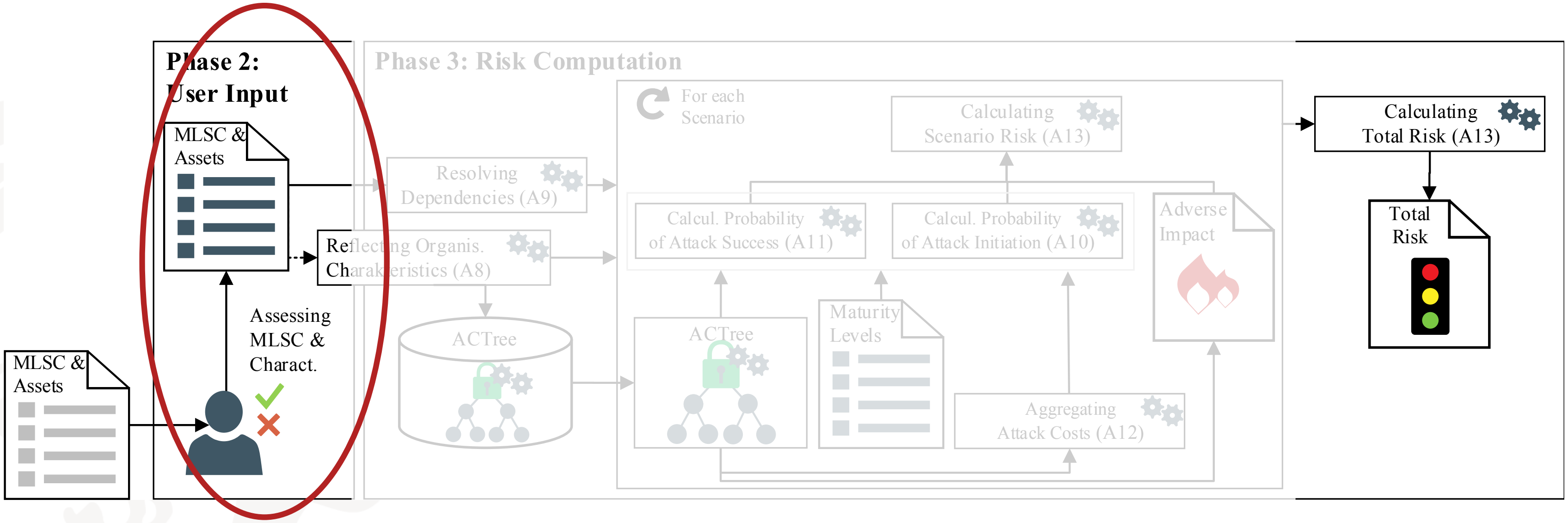
Riskmanagement



Christopher Schmitz and Sebastian Pape. Lisra: Lightweight security risk assessment for decision support in information security. Computers & Security, 90, 2020.

Michael Schmid and Sebastian Pape. A structured comparison of the corporate information security. In ICT Systems Security and Privacy Protection - 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, pages 223–237, 2019.

Riskmanagement



Christopher Schmitz and Sebastian Pape. Lisra: Lightweight security risk assessment for decision support in information security. Computers & Security, 90, 2020.

Michael Schmid and Sebastian Pape. A structured comparison of the corporate information security. In ICT Systems Security and Privacy Protection - 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, pages 223–237, 2019.

Security Maturity Levels

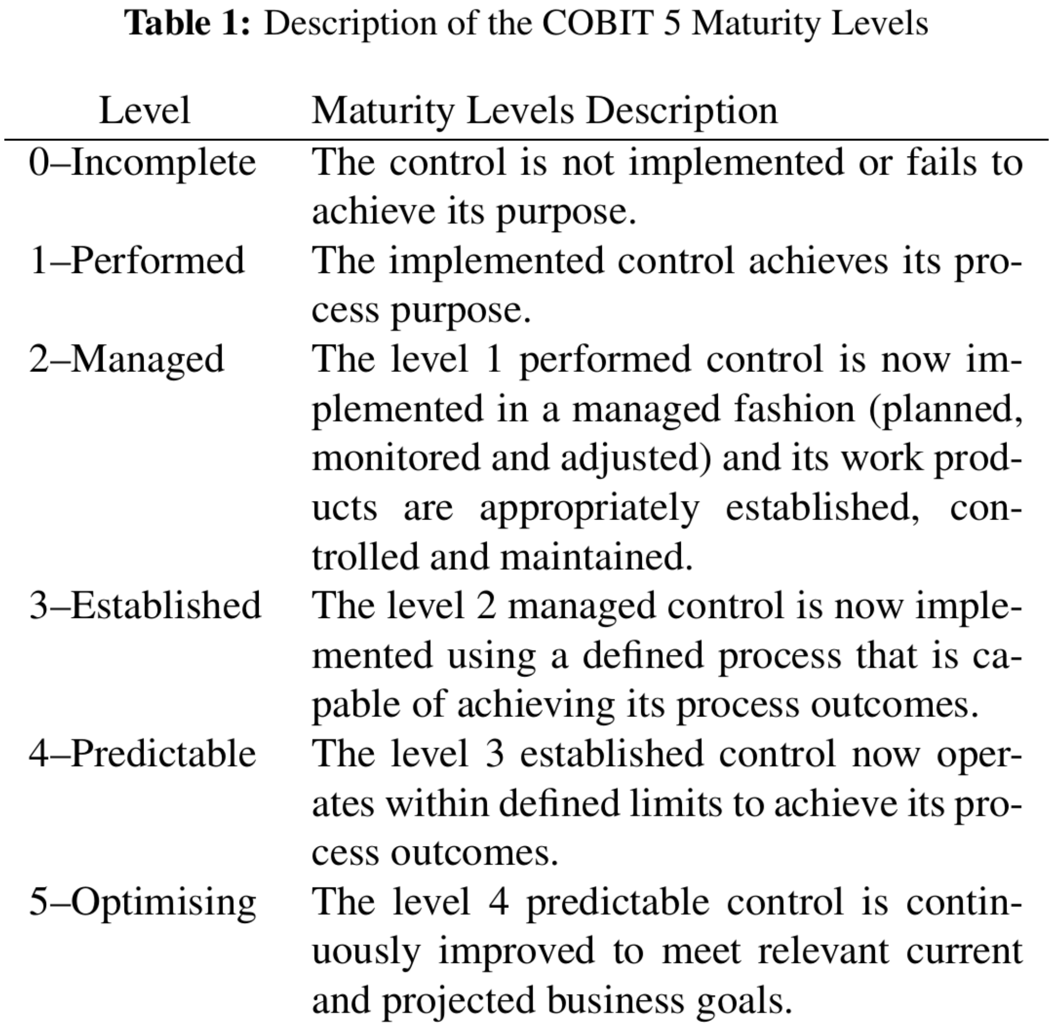
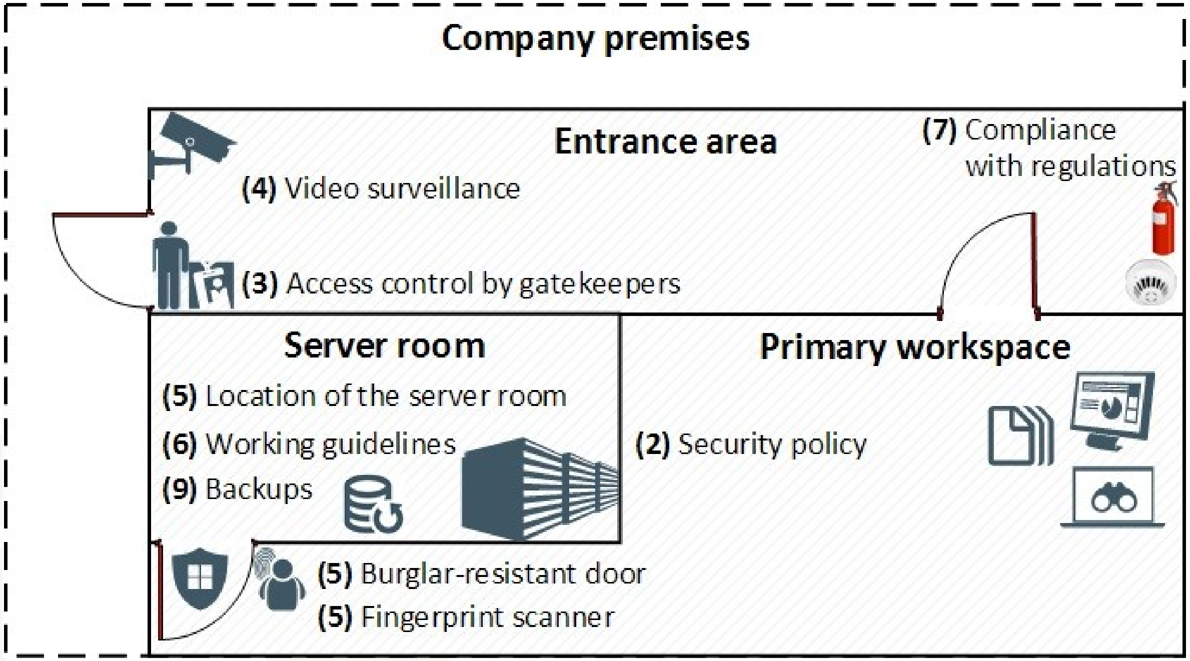


Table 1: Description of the COBIT 5 Maturity Levels

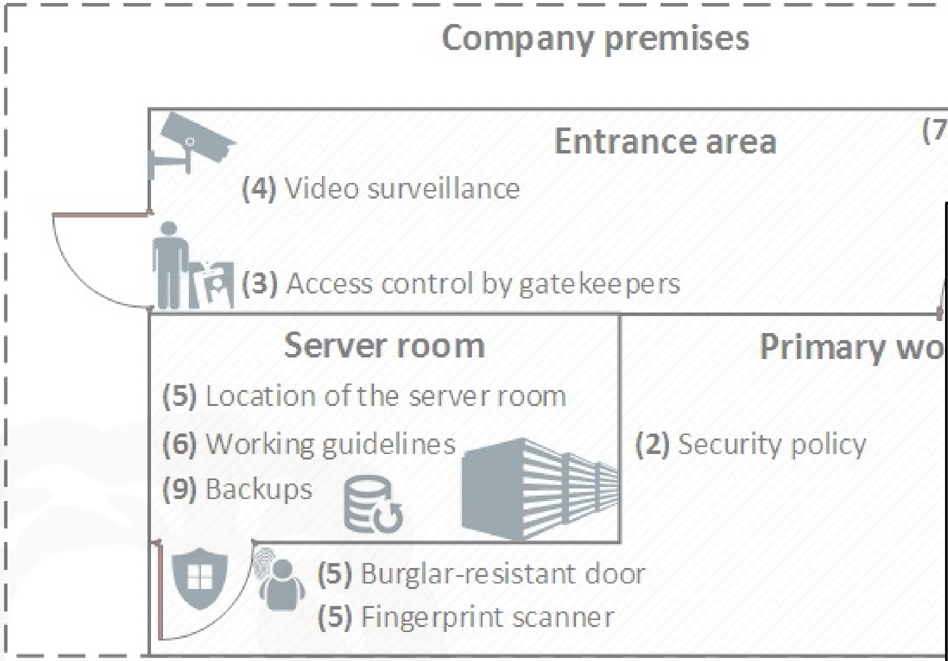
Level	Maturity Levels Description
0–Incomplete	The control is not implemented or fails to achieve its purpose.
1–Performed	The implemented control achieves its process purpose.
2–Managed	The level 1 performed control is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
3–Established	The level 2 managed control is now implemented using a defined process that is capable of achieving its process outcomes.
4–Predictable	The level 3 established control now operates within defined limits to achieve its process outcomes.
5–Optimising	The level 4 predictable control is continuously improved to meet relevant current and projected business goals.

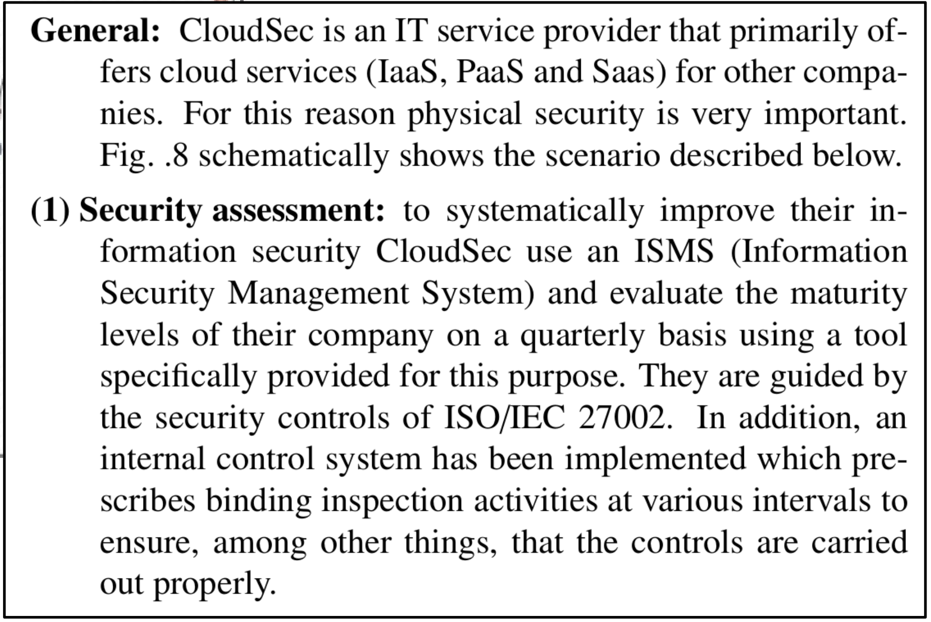
Controlled Experiment



Christopher Schmitz, Michael Schmid, David Harborth and Sebastian Pape: Maturity Level Assessments of Information Security Controls: An Empirical Analysis of Practitioners' Assessment Capabilities, Submitted to Computers & Security, Minor Revision

Controlled Experiment

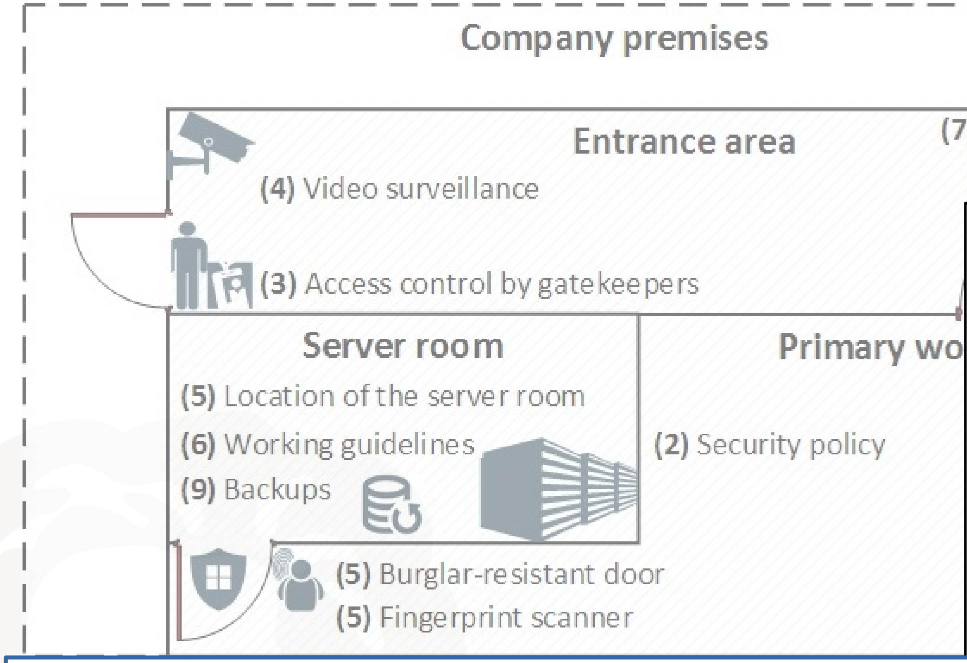


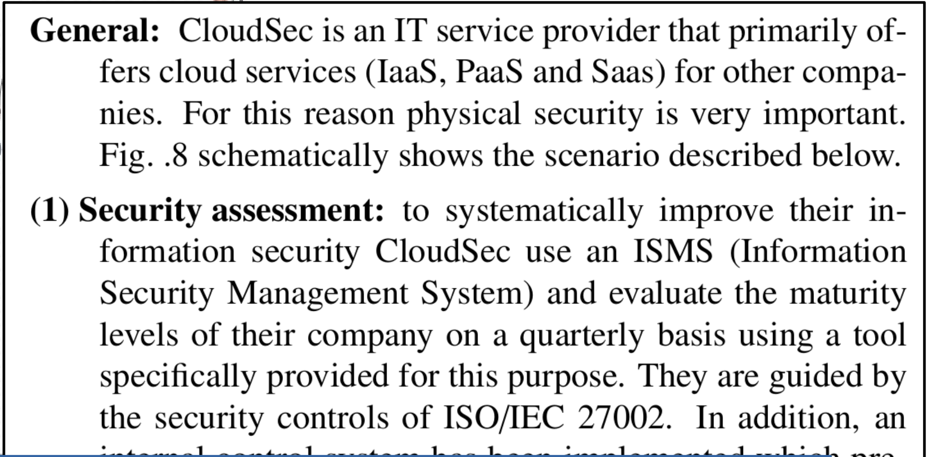


General: CloudSec is an IT service provider that primarily offers cloud services (IaaS, PaaS and Saas) for other companies. For this reason physical security is very important. Fig. .8 schematically shows the scenario described below.

(1) Security assessment: to systematically improve their information security CloudSec use an ISMS (Information Security Management System) and evaluate the maturity levels of their company on a quarterly basis using a tool specifically provided for this purpose. They are guided by the security controls of ISO/IEC 27002. In addition, an internal control system has been implemented which prescribes binding inspection activities at various intervals to ensure, among other things, that the controls are carried out properly.

Controlled Experiment

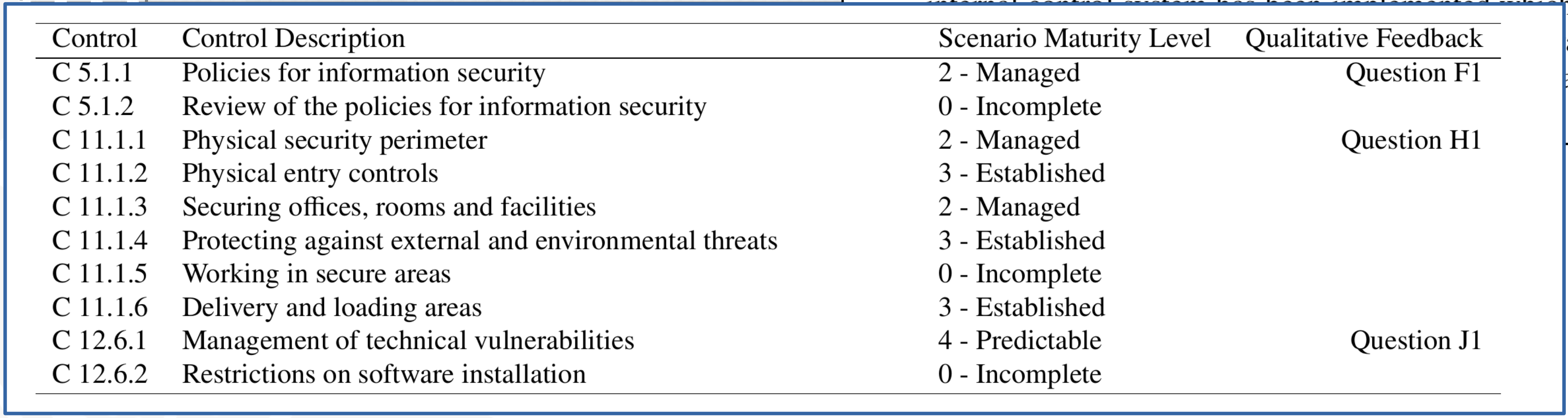



General: CloudSec is an IT service provider that primarily offers cloud services (IaaS, PaaS and Saas) for other companies. For this reason physical security is very important. Fig. .8 schematically shows the scenario described below.

(1) Security assessment: to systematically improve their information security CloudSec use an ISMS (Information Security Management System) and evaluate the maturity levels of their company on a quarterly basis using a tool specifically provided for this purpose. They are guided by the security controls of ISO/IEC 27002. In addition, an internal control system has been implemented which pre-

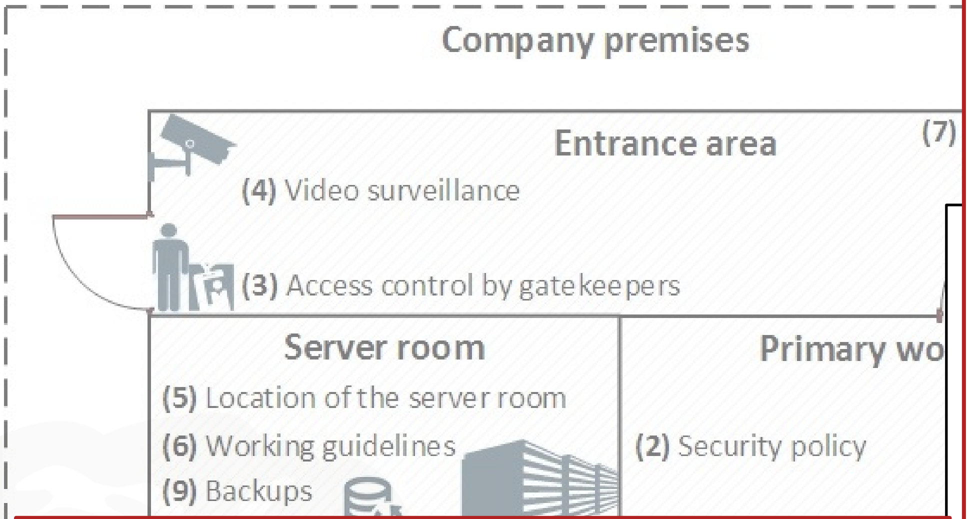
als to

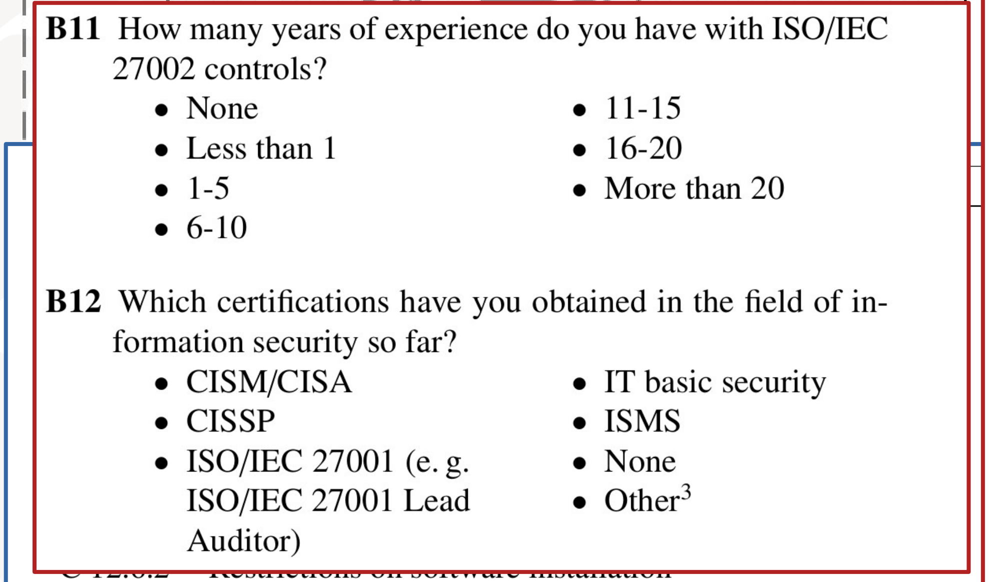
arried



Control	Control Description	Scenario Maturity Level	Qualitative Feedback
C 5.1.1	Policies for information security	2 - Managed	Question F1
C 5.1.2	Review of the policies for information security	0 - Incomplete	
C 11.1.1	Physical security perimeter	2 - Managed	Question H1
C 11.1.2	Physical entry controls	3 - Established	
C 11.1.3	Securing offices, rooms and facilities	2 - Managed	
C 11.1.4	Protecting against external and environmental threats	3 - Established	
C 11.1.5	Working in secure areas	0 - Incomplete	
C 11.1.6	Delivery and loading areas	3 - Established	
C 12.6.1	Management of technical vulnerabilities	4 - Predictable	Question J1
C 12.6.2	Restrictions on software installation	0 - Incomplete	

Controlled Experiment



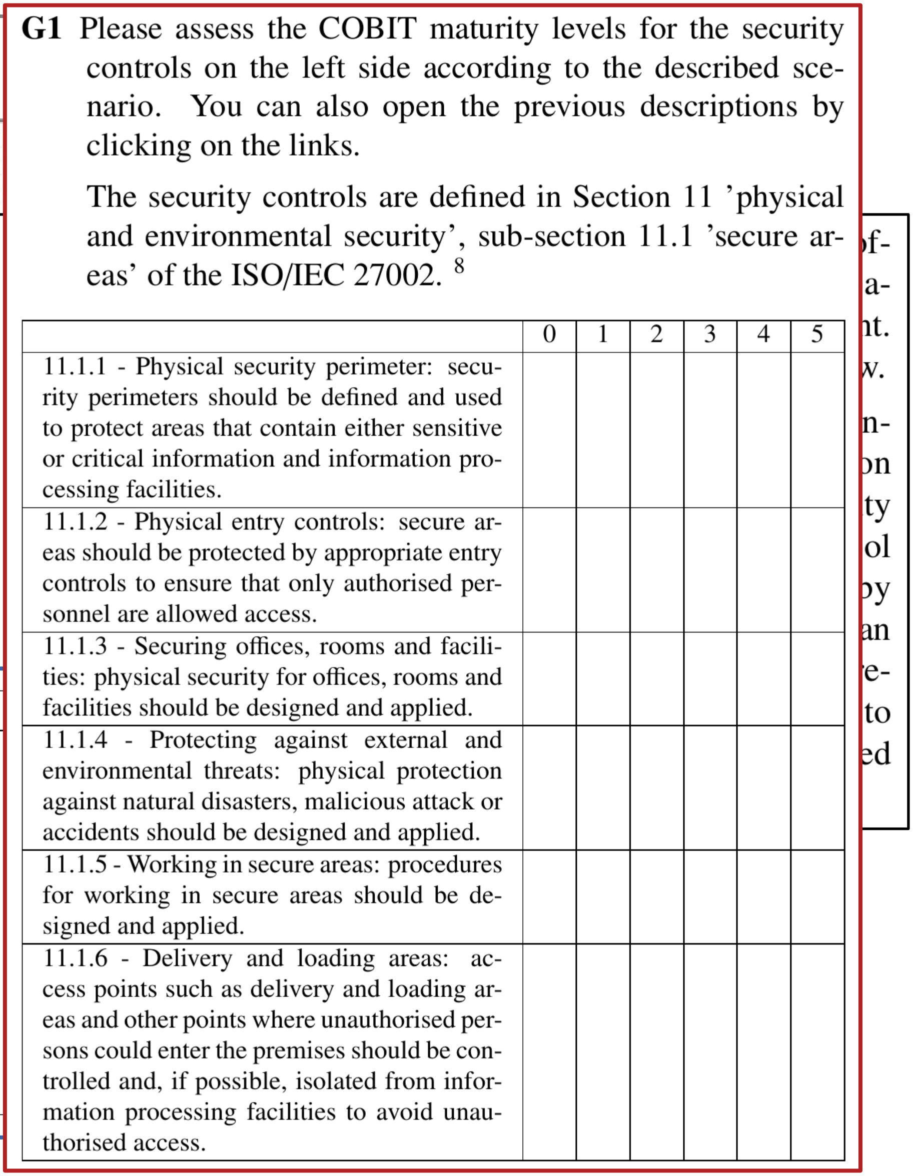


B11 How many years of experience do you have with ISO/IEC 27002 controls?

- None
- Less than 1
- 1-5
- 6-10
- 11-15
- 16-20
- More than 20

B12 Which certifications have you obtained in the field of information security so far?

- CISM/CISA
- CISSP
- ISO/IEC 27001 (e. g. ISO/IEC 27001 Lead Auditor)
- IT basic security
- ISMS
- None
- Other[3]



G1 Please assess the COBIT maturity levels for the security controls on the left side according to the described scenario. You can also open the previous descriptions by clicking on the links.

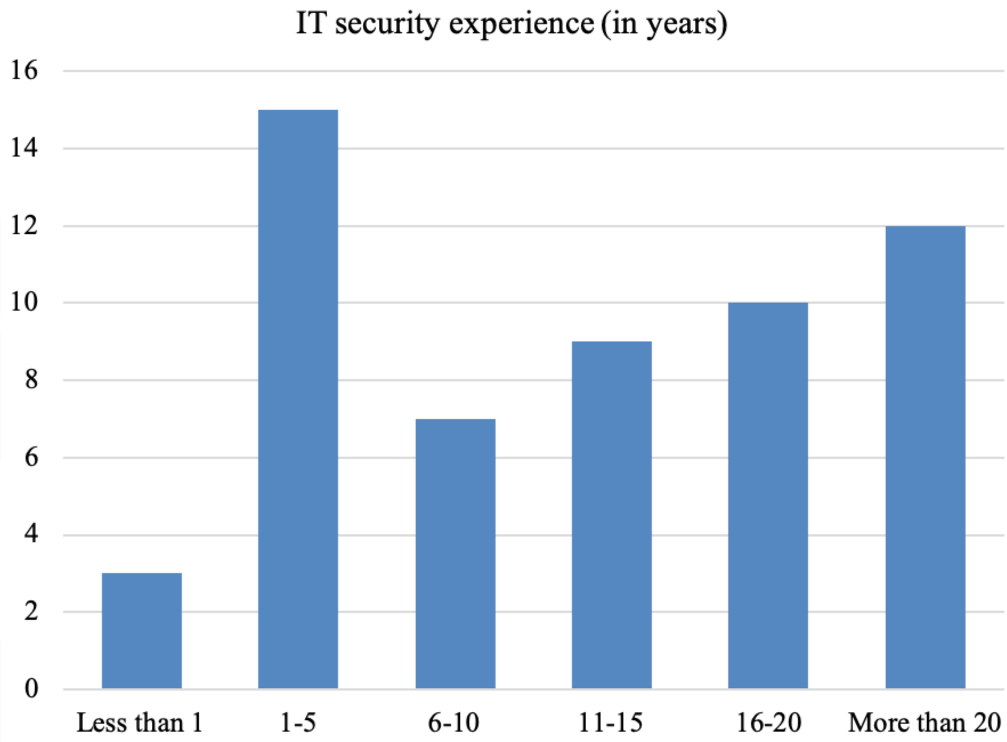
The security controls are defined in Section 11 'physical and environmental security', sub-section 11.1 'secure areas' of the ISO/IEC 27002. [8]

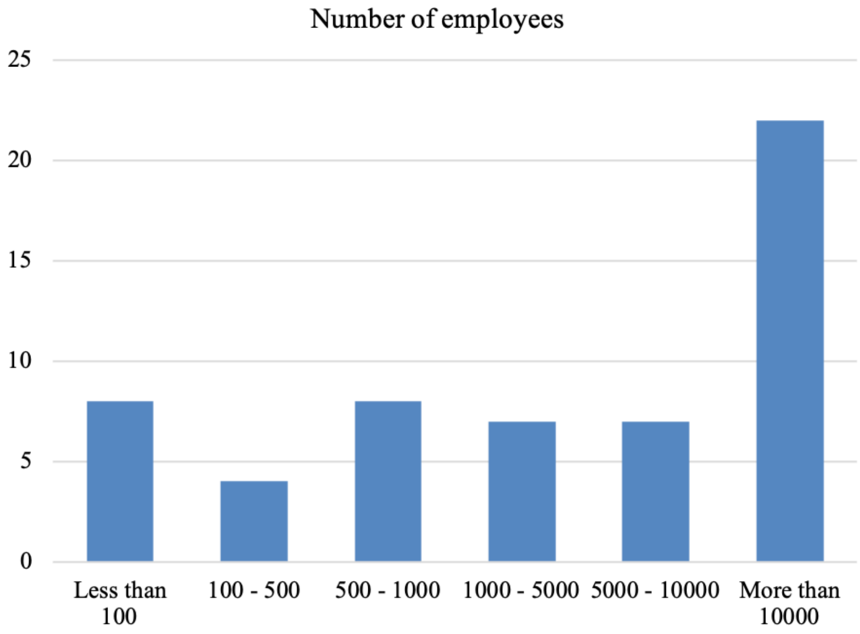
	0	1	2	3	4	5
11.1.1 - Physical security perimeter: security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.						
11.1.2 - Physical entry controls: secure areas should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.						
11.1.3 - Securing offices, rooms and facilities: physical security for offices, rooms and facilities should be designed and applied.						
11.1.4 - Protecting against external and environmental threats: physical protection against natural disasters, malicious attack or accidents should be designed and applied.						
11.1.5 - Working in secure areas: procedures for working in secure areas should be designed and applied.						
11.1.6 - Delivery and loading areas: access points such as delivery and loading areas and other points where unauthorised persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.						

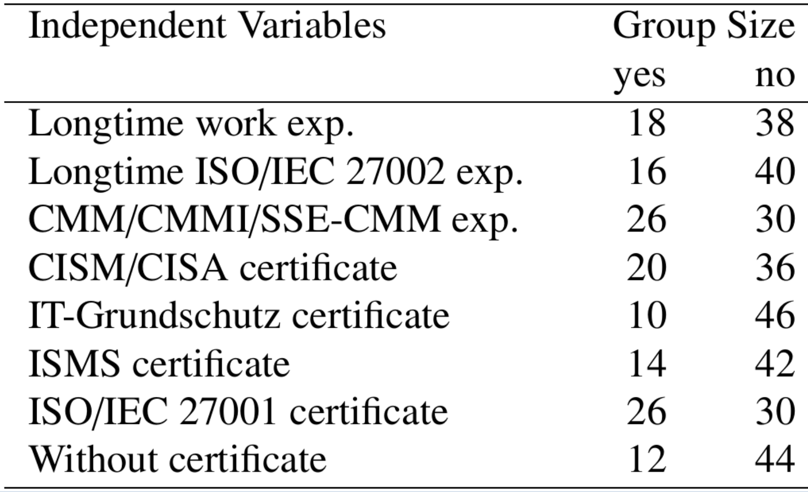
Methodology

- Survey (N=56)
  - Scenario
  - Demographics
  - Assessments
  - Justification (Activities to reach next level)
  - Challenges / Difficulties / Confidence
- Interviews (N=7, 20-30min)
  - Agreement
  - Assessment of Challenge
  - Possible Assistance for Task
- Quantitative & Qualitative Evaluation

Participants (N=56)

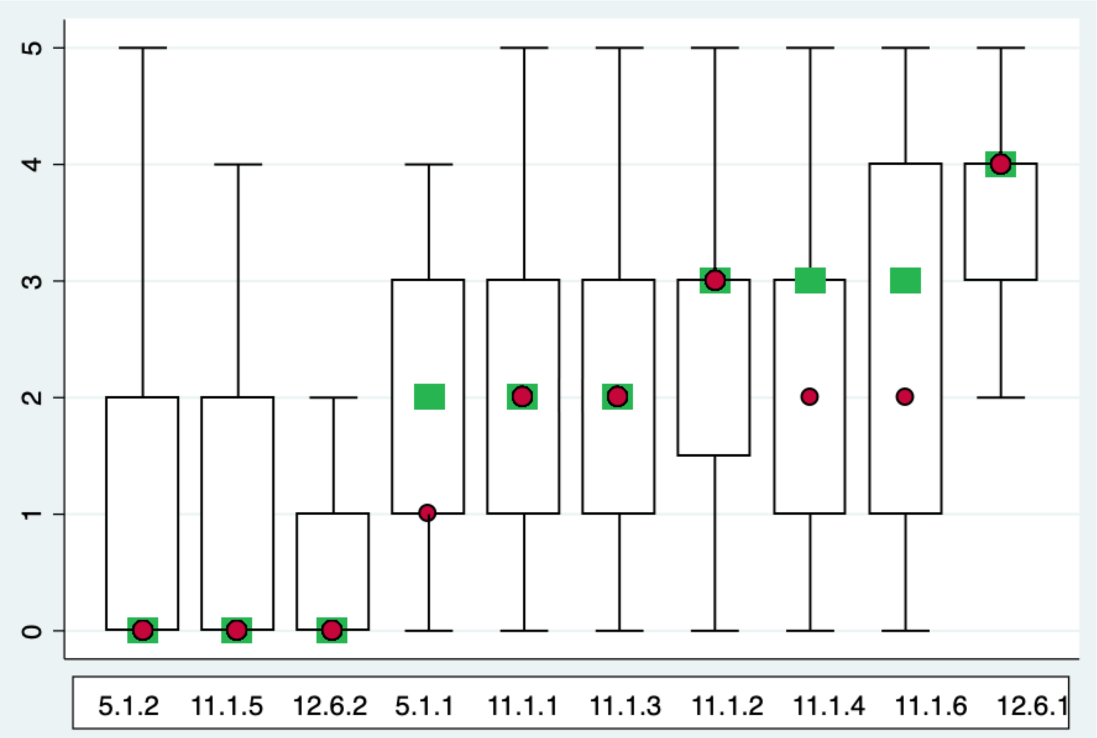


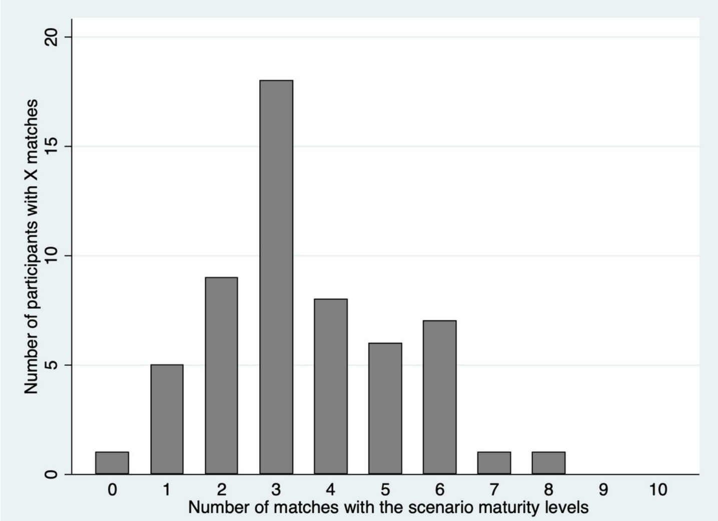




Independent Variables	Group Size	
	yes	no
Longtime work exp.	18	38
Longtime ISO/IEC 27002 exp.	16	40
CMM/CMMI/SSE-CMM exp.	26	30
CISM/CISA certificate	20	36
IT-Grundschutz certificate	10	46
ISMS certificate	14	42
ISO/IEC 27001 certificate	26	30
Without certificate	12	44

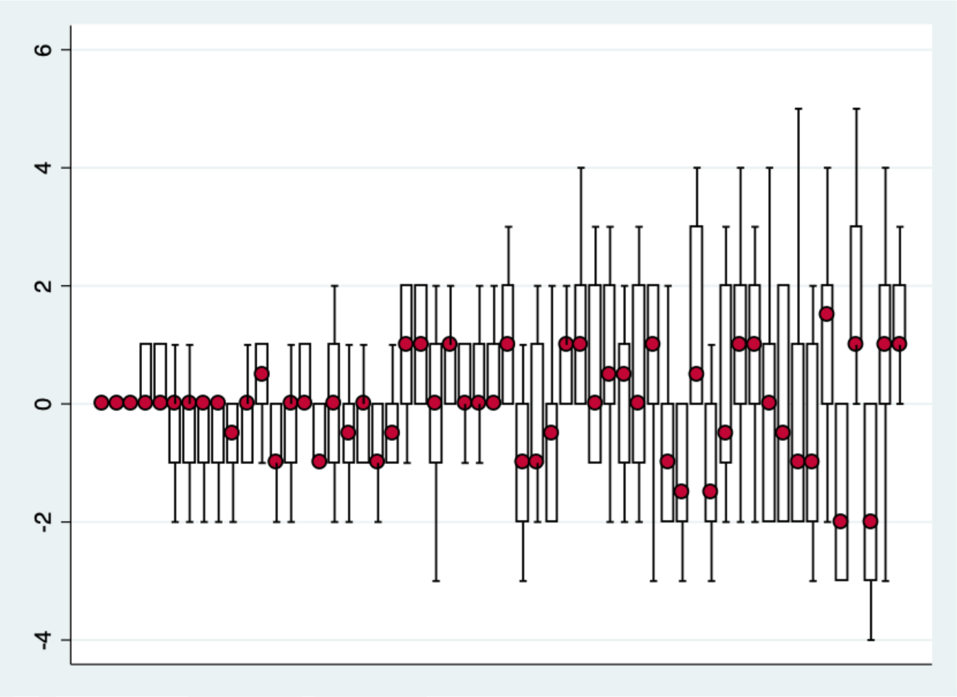
Results I





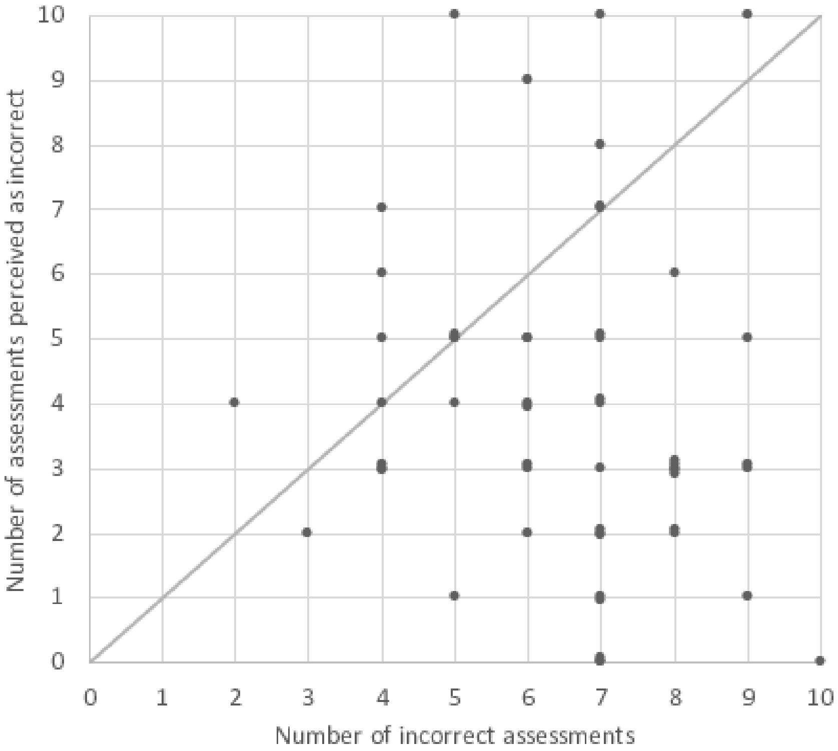
Control	Control Description	Scenario Maturity Level	Qualitative Feedback
C 5.1.1	Policies for information security	2 - Managed	Question F1
C 5.1.2	Review of the policies for information security	0 - Incomplete	
C 11.1.1	Physical security perimeter	2 - Managed	Question H1
C 11.1.2	Physical entry controls	3 - Established	
C 11.1.3	Securing offices, rooms and facilities	2 - Managed	
C 11.1.4	Protecting against external and environmental threats	3 - Established	
C 11.1.5	Working in secure areas	0 - Incomplete	
C 11.1.6	Delivery and loading areas	3 - Established	
C 12.6.1	Management of technical vulnerabilities	4 - Predictable	Question J1
C 12.6.2	Restrictions on software installation	0 - Incomplete	

Results II



Section K: Confidence

K1 In total, you have assessed the maturity levels for ten security controls. For how many of them have you been uncertain?



Results III

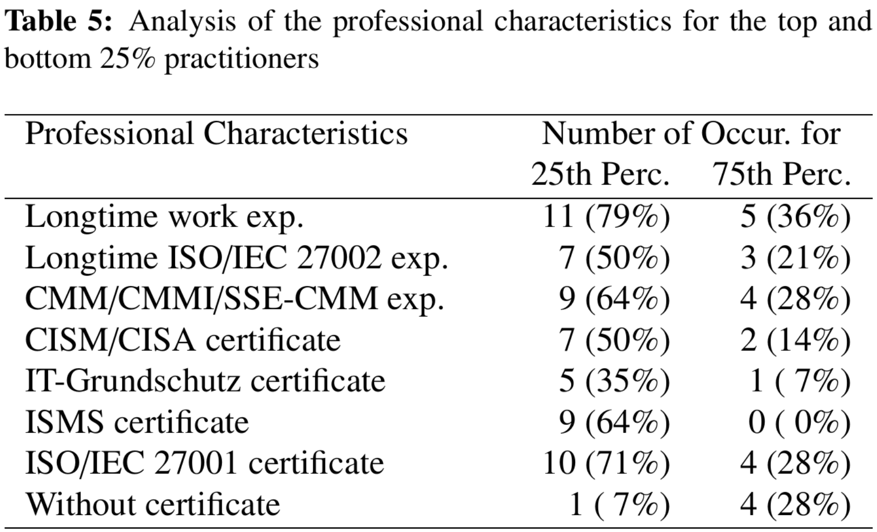


Table 5: Analysis of the professional characteristics for the top and bottom 25% practitioners

Professional Characteristics	Number of Occur. for 25th Perc.	75th Perc.
Longtime work exp.	11 (79%)	5 (36%)
Longtime ISO/IEC 27002 exp.	7 (50%)	3 (21%)
CMM/CMMI/SSE-CMM exp.	9 (64%)	4 (28%)
CISM/CISA certificate	7 (50%)	2 (14%)
IT-Grundschutz certificate	5 (35%)	1 (7%)
ISMS certificate	9 (64%)	0 (0%)
ISO/IEC 27001 certificate	10 (71%)	4 (28%)
Without certificate	1 (7%)	4 (28%)

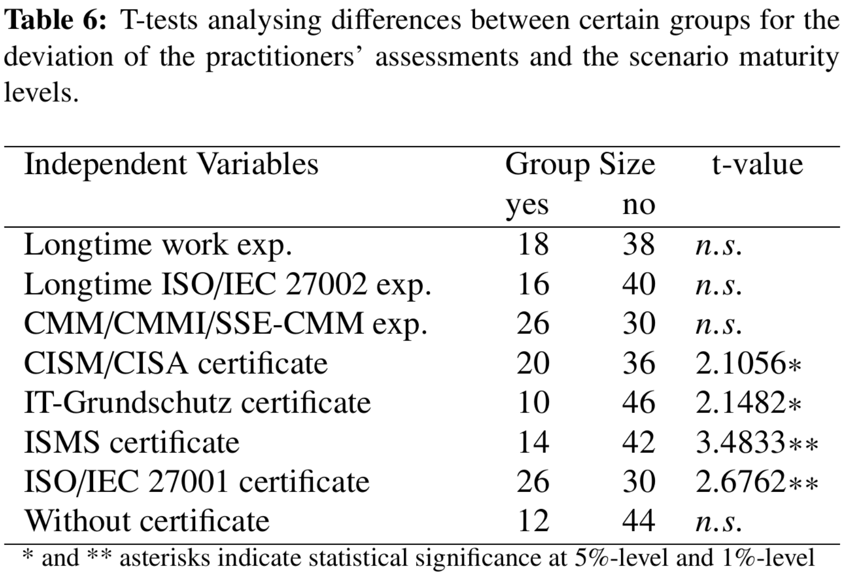


Table 6: T-tests analysing differences between certain groups for the deviation of the practitioners' assessments and the scenario maturity levels.

Independent Variables	Group Size yes	no	t-value
Longtime work exp.	18	38	*n.s.*
Longtime ISO/IEC 27002 exp.	16	40	*n.s.*
CMM/CMMI/SSE-CMM exp.	26	30	*n.s.*
CISM/CISA certificate	20	36	2.1056*
IT-Grundschutz certificate	10	46	2.1482*
ISMS certificate	14	42	3.4833**
ISO/IEC 27001 certificate	26	30	2.6762**
Without certificate	12	44	*n.s.*

* and ** asterisks indicate statistical significance at 5%-level and 1%-level

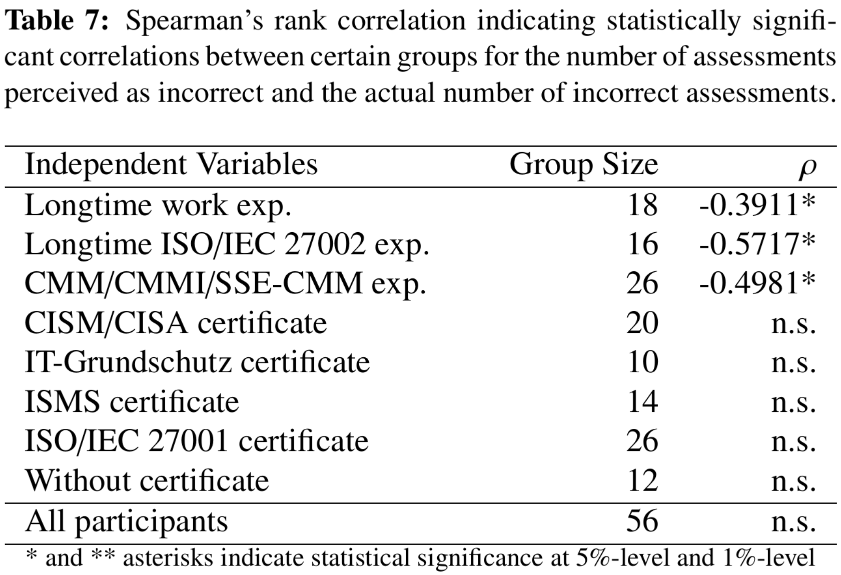


Table 7: Spearman's rank correlation indicating statistically significant correlations between certain groups for the number of assessments perceived as incorrect and the actual number of incorrect assessments.

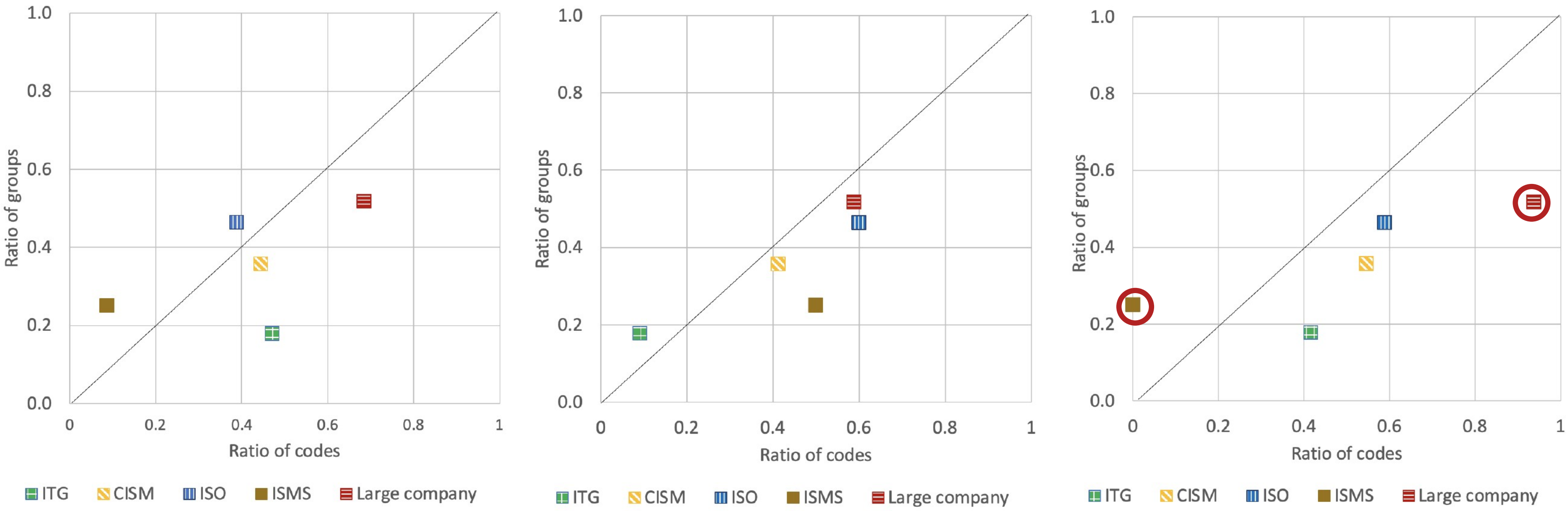
Independent Variables	Group Size	ρ
Longtime work exp.	18	-0.3911*
Longtime ISO/IEC 27002 exp.	16	-0.5717*
CMM/CMMI/SSE-CMM exp.	26	-0.4981*
CISM/CISA certificate	20	n.s.
IT-Grundschutz certificate	10	n.s.
ISMS certificate	14	n.s.
ISO/IEC 27001 certificate	26	n.s.
Without certificate	12	n.s.
All participants	56	n.s.

* and ** asterisks indicate statistical significance at 5%-level and 1%-level

Results IV

Total numbers:

24 24 18



(a) Code ’control misinterpreted’

(b) Code ’scenario misinterpreted’

(c) Code ’security measure exaggerated’

Figure 7: Distribution of codes for certain groups

Results V

- Reasons for Exaggerated Measures
  - Individual background (regulated sectors)
  - No economic considerations
- Challenges
  - Scope for interpretation
  - Differentation between maturity levels
  - Control dependencies
  - Mapping controls to processes
  - Lack of skills
- Difficulties
  - Internal / external assessments
  - Not all controls represent processes
  - Transition between maturity levels

- Support
  - Discussion in teams
  - Examples
  - Trainings
  - Catalogue of measures

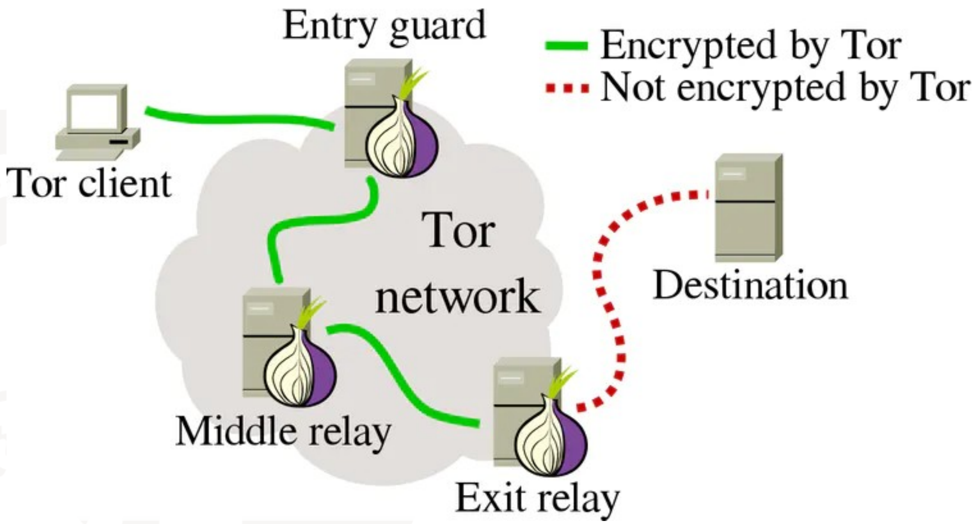
Summary

- Participants struggled with the assessments
  - Scenario vs. own company
  - Economic considerations
  - Wiggle room
- Assessors with certificate performed better
- Practitioners overconfident

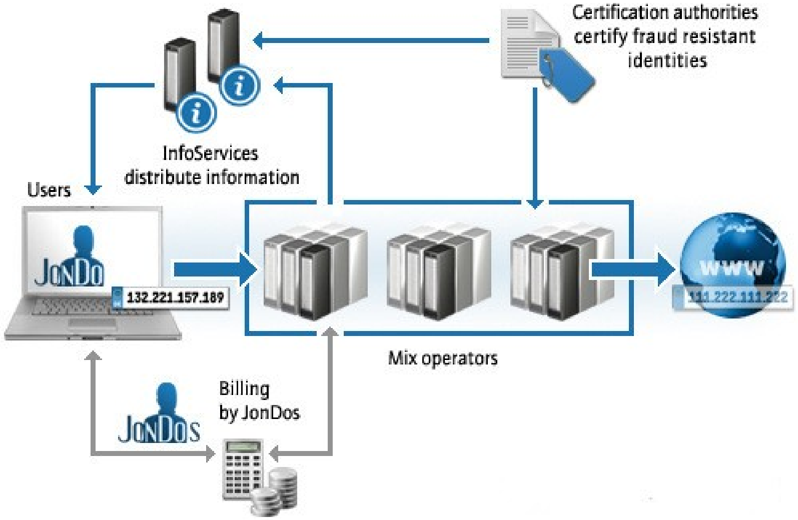
- Limitations
  - Scenario
  - Subset of controls
  - Self-selection bias

Privacy Enhancing Technologies

Anonymity Networks



Source: Econotimes.com


Certification authorities certify fraud resistant identities
InfoServices distribute information
Users
JonDo
132.221.157.189
www
111.222.111.222
Mix operators
Billing by JonDos
JonDos

Source: JonDonym

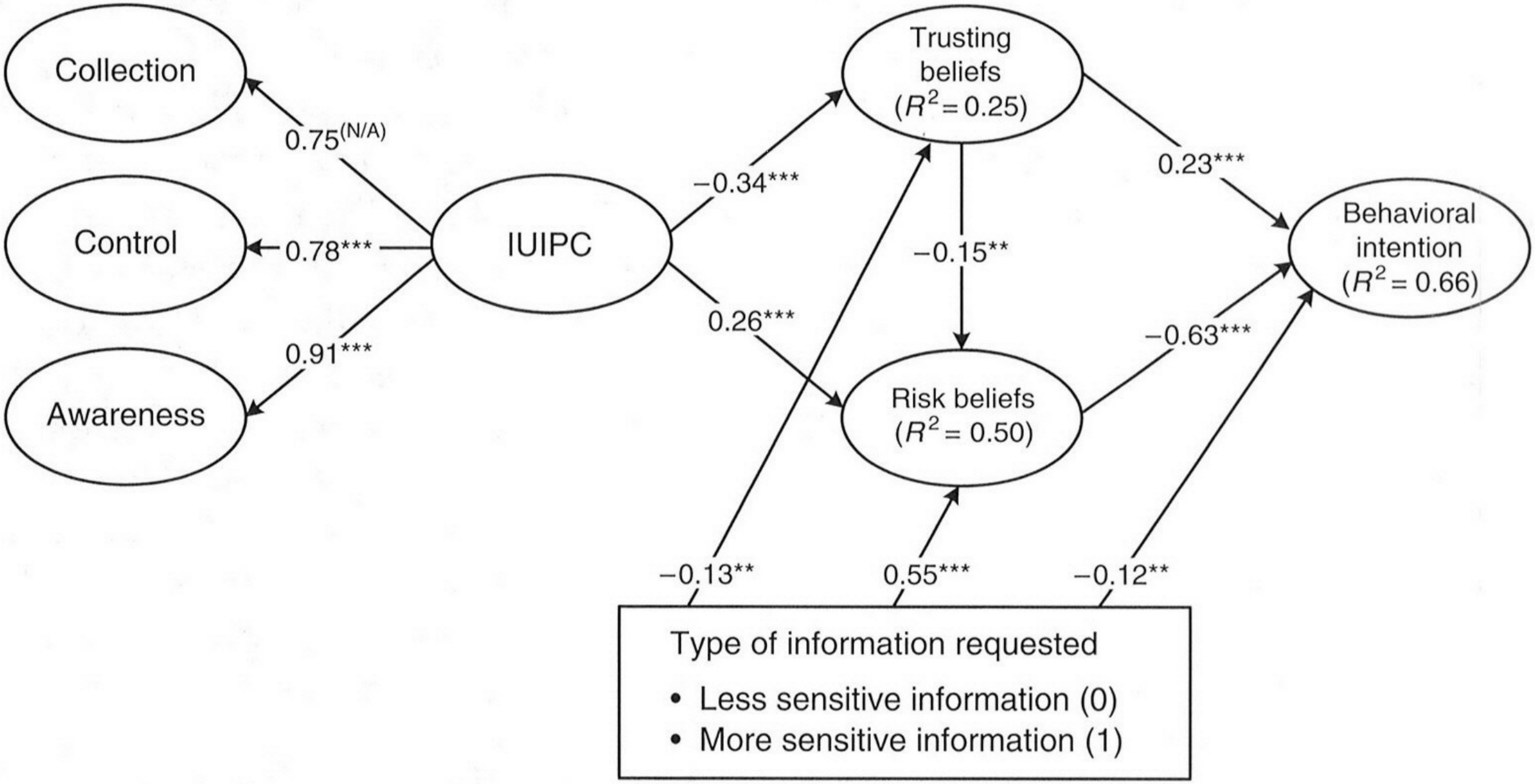
- Investigate users intention to use Tor / Jondonym
- Compare differences

Methodology

- Constructs adapted from existing literature:
  - technology acceptance factors (Venkatesh and Davis 2000, Venkatesh et al. 2012)
  - trust (Pavlou 2003)
  - perceived anonymity (Benenson et al. 2015)
- German and English-speaking users of JonDonym and Tor acquired
  - during the rollout of a new browser and on the official homepage (Jondonym)
  - via the Tor mailing list (+ diverse other channels to reach Tor users)
- Constructs translated into German with two certified translators
- Active users (N=141 for JonDonym + 124 for Tor)

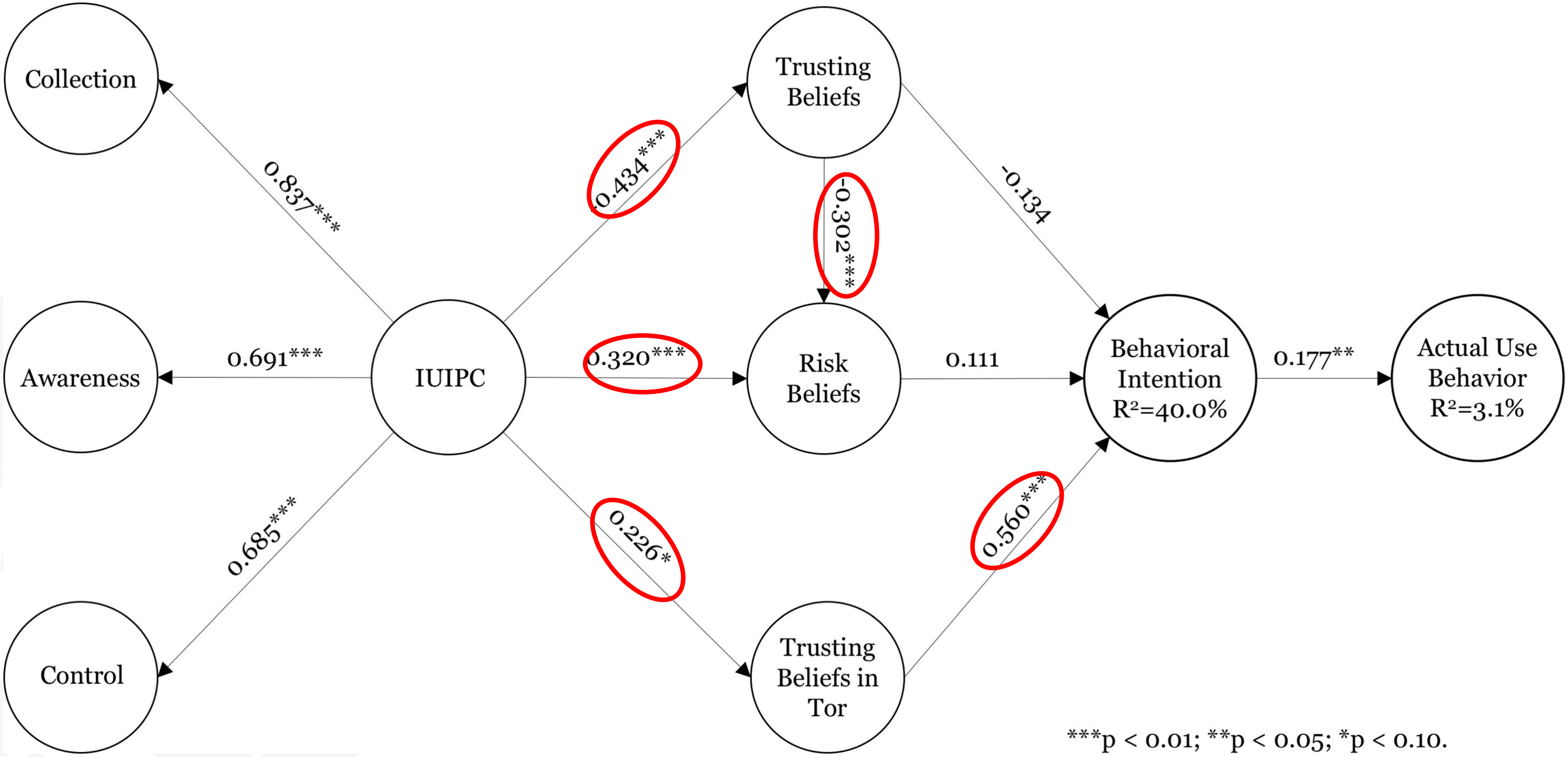
- Partial least squares structural equation modelling (PLS-SEM) with SmartPLS 3.2.7 (Ringle et al. 2015)
- Coding of answers by two coders

Internet Users‘ Information Privacy Concerns (IUIPC)


Collection
Control
Awareness
0.75(N/A)
0.78***
0.91***
IUIPC
−0.34***
0.26***
Trusting beliefs ($R^2 = 0.25$)
Risk beliefs ($R^2 = 0.50$)
−0.15**
0.23***
−0.63***
Behavioral intention ($R^2 = 0.66$)
−0.13**
0.55***
−0.12**
Type of information requested
• Less sensitive information (0)
• More sensitive information (1)

Malhotra, Kim & Agarwal: Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model, Information Systems Research 15(4), 2004

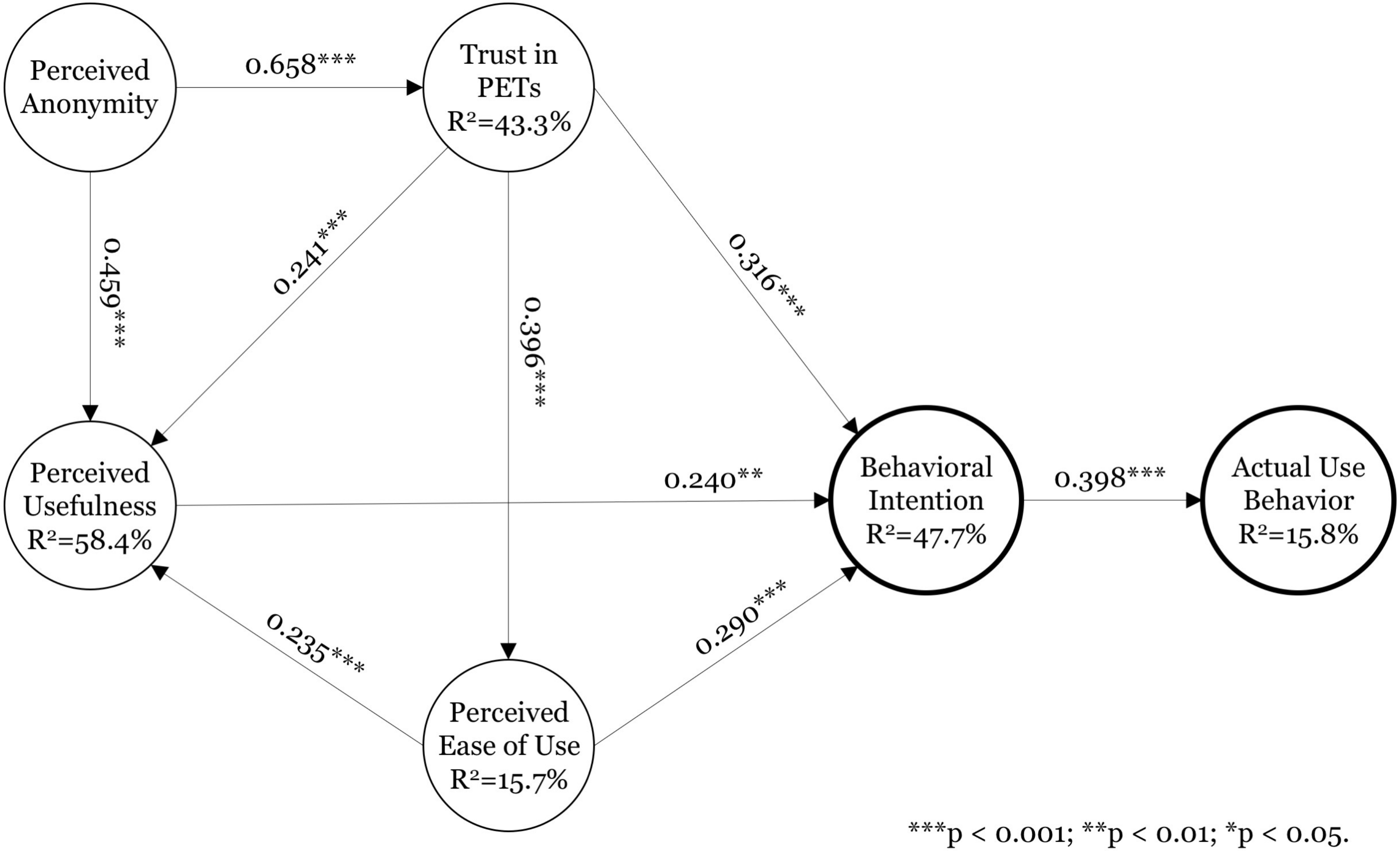
IUIPC: Tor (Jondonym)



***p < 0.01; **p < 0.05; *p < 0.10.

David Harborth and Sebastian Pape. How privacy concerns and trust and risk beliefs influence users' intentions to use privacy-enhancing technologies – the case of tor. In 52nd Hawaii International Conference on System Sciences (HICSS) 2019, 2019.

TAM: Tor / Jondonym


Perceived Anonymity
0.658***
Trust in PETs R²=43.3%
0.459***
0.241***
0.396***
0.316***
Perceived Usefulness R²=58.4%
0.240**
Behavioral Intention R²=47.7%
0.398***
Actual Use Behavior R²=15.8%
0.235***
0.290***
Perceived Ease of Use R²=15.7%
***p < 0.001; **p < 0.01; *p < 0.05.

David Harborth, Sebastian Pape, and Kai Rannenberg. Explaining the technology use behavior of privacyenhancing technologies: The case of tor and jondonym. Proceedings on Privacy Enhancing Technologies (PoPETs), 2020(2):111–128, 2020.

TAM: Tor / Jondonym - Diffs

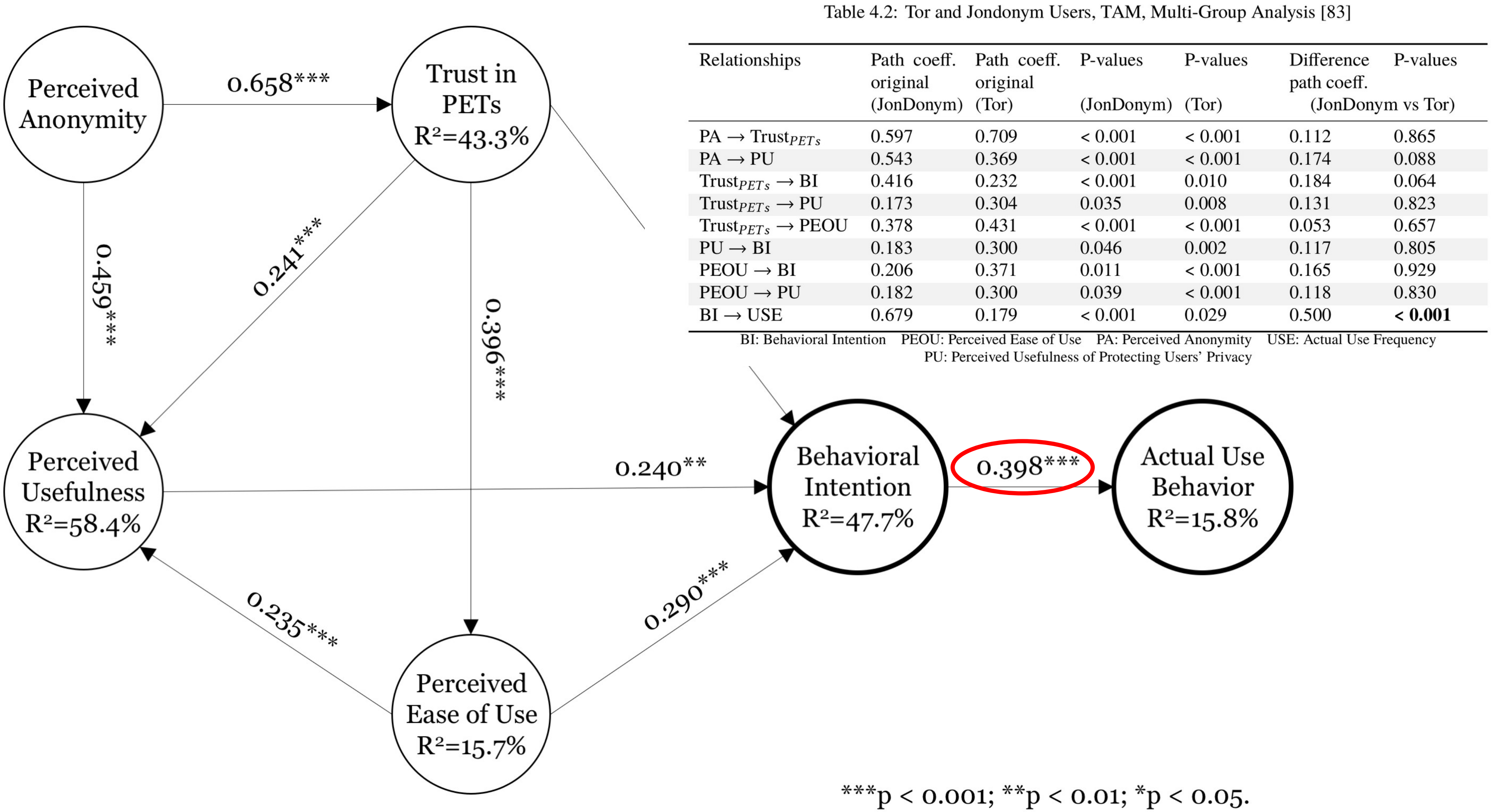

Perceived Anonymity
0.658***
Trust in PETs R²=43.3%
0.459***
0.241***
0.396***
Perceived Usefulness R²=58.4%
0.240**
Behavioral Intention R²=47.7%
0.398***
Actual Use Behavior R²=15.8%
0.235***
0.290***
Perceived Ease of Use R²=15.7%

Table 4.2: Tor and Jondonym Users, TAM, Multi-Group Analysis [83]

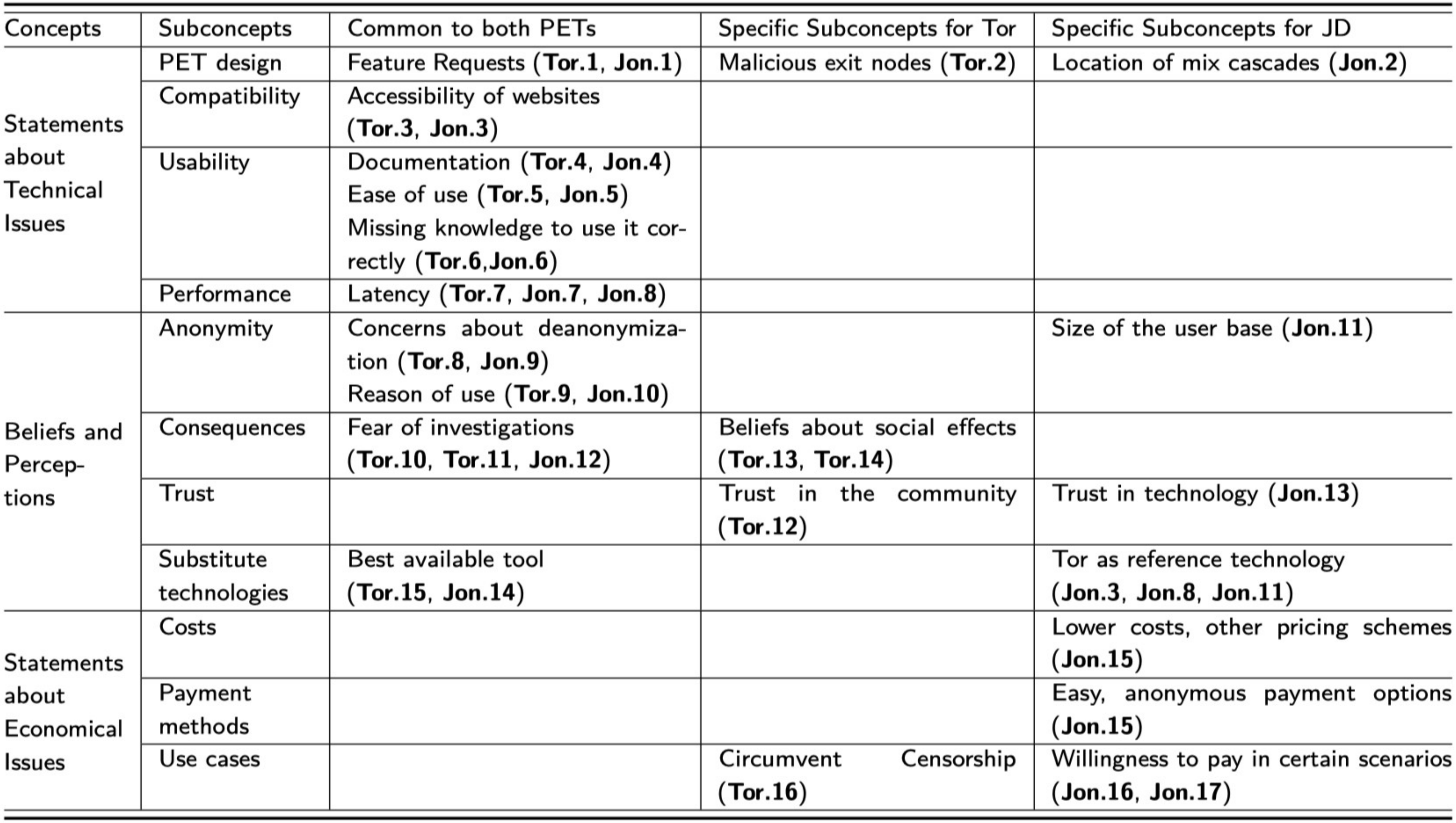
Relationships	Path coeff. original (JonDonym)	Path coeff. original (Tor)	P-values (JonDonym)	P-values (Tor)	Difference path coeff. (JonDonym vs Tor)	P-values
PA → Trust$_{PETs}$	0.597	0.709	< 0.001	< 0.001	0.112	0.865
PA → PU	0.543	0.369	< 0.001	< 0.001	0.174	0.088
Trust$_{PETs}$ → BI	0.416	0.232	< 0.001	0.010	0.184	0.064
Trust$_{PETs}$ → PU	0.173	0.304	0.035	0.008	0.131	0.823
Trust$_{PETs}$ → PEOU	0.378	0.431	< 0.001	< 0.001	0.053	0.657
PU → BI	0.183	0.300	0.046	0.002	0.117	0.805
PEOU → BI	0.206	0.371	0.011	< 0.001	0.165	0.929
PEOU → PU	0.182	0.300	0.039	< 0.001	0.118	0.830
BI → USE	0.679	0.179	< 0.001	0.029	0.500	**< 0.001**

BI: Behavioral Intention PEOU: Perceived Ease of Use PA: Perceived Anonymity USE: Actual Use Frequency
PU: Perceived Usefulness of Protecting Users' Privacy

***p < 0.001; **p < 0.01; *p < 0.05.

David Harborth, Sebastian Pape, and Kai Rannenberg. Explaining the technology use behavior of privacyenhancing technologies: The case of tor and jondonym. Proceedings on Privacy Enhancing Technologies (PoPETs), 2020(2):111–128, 2020.

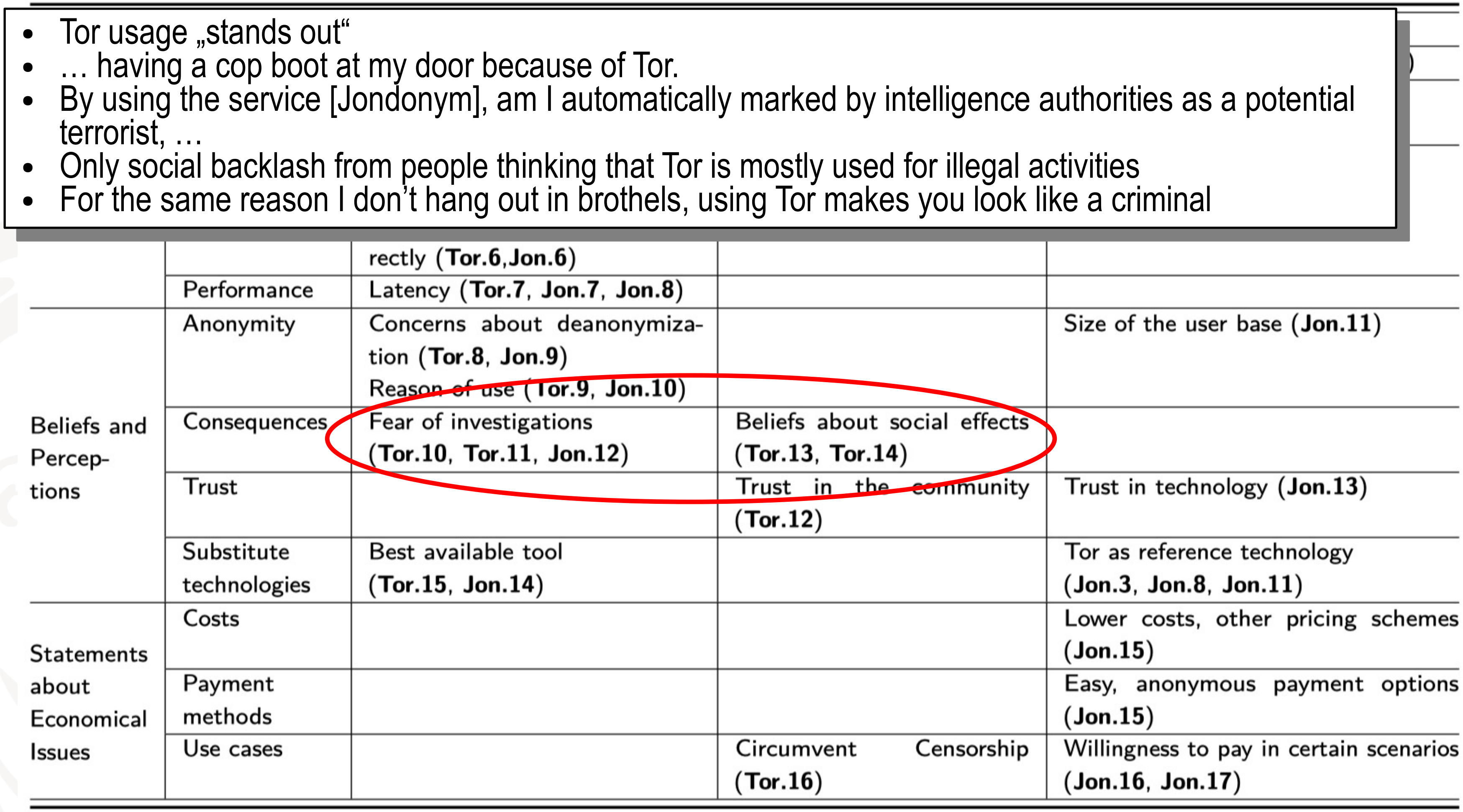
Qualitative Results – Concepts



Concepts	Subconcepts	Common to both PETs	Specific Subconcepts for Tor	Specific Subconcepts for JD
Statements about Technical Issues	PET design	Feature Requests (**Tor.1**, **Jon.1**)	Malicious exit nodes (**Tor.2**)	Location of mix cascades (**Jon.2**)
	Compatibility	Accessibility of websites (**Tor.3**, **Jon.3**)		
	Usability	Documentation (**Tor.4**, **Jon.4**) Ease of use (**Tor.5**, **Jon.5**) Missing knowledge to use it correctly (**Tor.6**,**Jon.6**)		
	Performance	Latency (**Tor.7**, **Jon.7**, **Jon.8**)		
Beliefs and Perceptions	Anonymity	Concerns about deanonymization (**Tor.8**, **Jon.9**) Reason of use (**Tor.9**, **Jon.10**)		Size of the user base (**Jon.11**)
	Consequences	Fear of investigations (**Tor.10**, **Tor.11**, **Jon.12**)	Beliefs about social effects (**Tor.13**, **Tor.14**)	
	Trust		Trust in the community (**Tor.12**)	Trust in technology (**Jon.13**)
	Substitute technologies	Best available tool (**Tor.15**, **Jon.14**)		Tor as reference technology (**Jon.3**, **Jon.8**, **Jon.11**)
Statements about Economical Issues	Costs			Lower costs, other pricing schemes (**Jon.15**)
	Payment methods			Easy, anonymous payment options (**Jon.15**)
	Use cases		Circumvent Censorship (**Tor.16**)	Willingness to pay in certain scenarios (**Jon.16**, **Jon.17**)

Qualitative Results – Concepts

- Tor usage „stands out“
- … having a cop boot at my door because of Tor.
- By using the service [Jondonym], am I automatically marked by intelligence authorities as a potential terrorist, …
- Only social backlash from people thinking that Tor is mostly used for illegal activities
- For the same reason I don’t hang out in brothels, using Tor makes you look like a criminal



		rectly (**Tor.6**,**Jon.6**)		
	Performance	Latency (**Tor.7**, **Jon.7**, **Jon.8**)		
Beliefs and Perceptions	Anonymity	Concerns about deanonymization (**Tor.8**, **Jon.9**) Reason of use (**Tor.9**, **Jon.10**)		Size of the user base (**Jon.11**)
	Consequences	Fear of investigations (**Tor.10**, **Tor.11**, **Jon.12**)	Beliefs about social effects (**Tor.13**, **Tor.14**)	
	Trust		Trust in the community (**Tor.12**)	Trust in technology (**Jon.13**)
	Substitute technologies	Best available tool (**Tor.15**, **Jon.14**)		Tor as reference technology (**Jon.3**, **Jon.8**, **Jon.11**)
Statements about Economical Issues	Costs			Lower costs, other pricing schemes (**Jon.15**)
	Payment methods			Easy, anonymous payment options (**Jon.15**)
	Use cases		Circumvent Censorship (**Tor.16**)	Willingness to pay in certain scenarios (**Jon.16**, **Jon.17**)

PET Economics

$$WTP/WTD_i = \beta_0 + \beta_1 \cdot RP_i + \beta_2 \cdot VIC_i + \beta_3 \cdot TRUST_i + \beta_4 \cdot TRUST_{PET,i} + \beta_5 \cdot TOR/JD_i + \epsilon_i$$

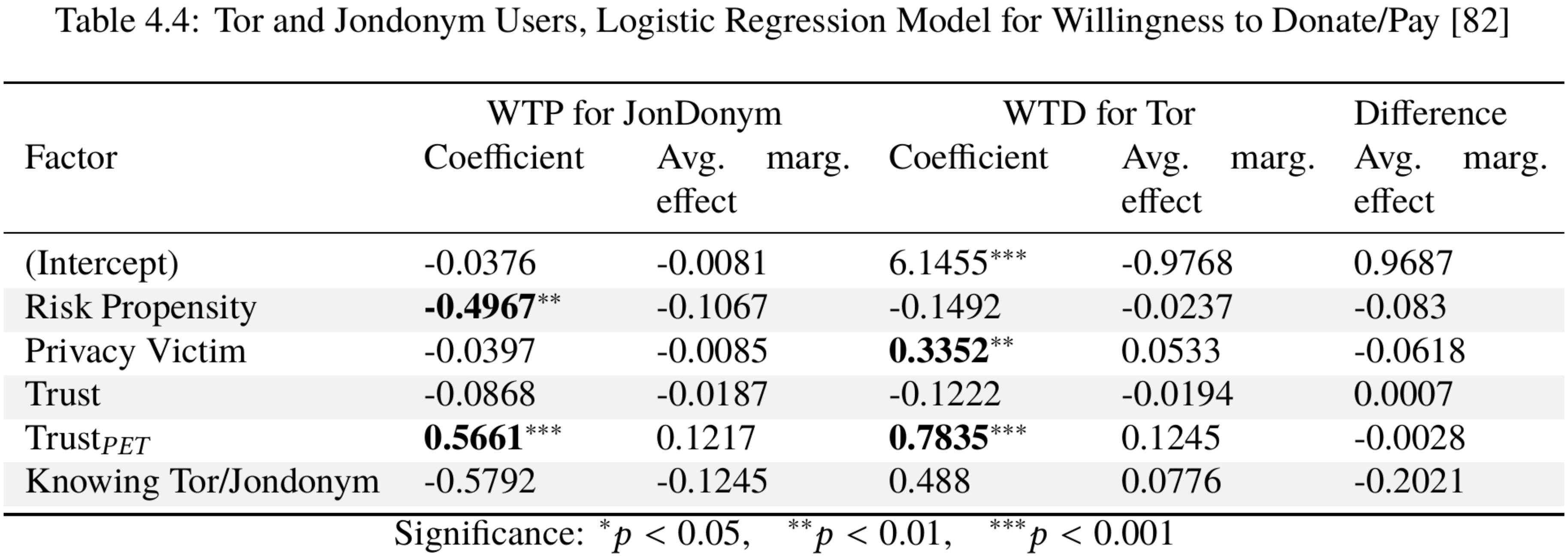


Table 4.4: Tor and Jondonym Users, Logistic Regression Model for Willingness to Donate/Pay [82]

	WTP for JonDonym		WTD for Tor		Difference
Factor	Coefficient	Avg. marg. effect	Coefficient	Avg. marg. effect	Avg. marg. effect
(Intercept)	-0.0376	-0.0081	6.1455***	-0.9768	0.9687
Risk Propensity	**-0.4967****	-0.1067	-0.1492	-0.0237	-0.083
Privacy Victim	-0.0397	-0.0085	**0.3352****	0.0533	-0.0618
Trust	-0.0868	-0.0187	-0.1222	-0.0194	0.0007
Trust$_{PET}$	**0.5661*****	0.1217	**0.7835*****	0.1245	-0.0028
Knowing Tor/Jondonym	-0.5792	-0.1245	0.488	0.0776	-0.2021

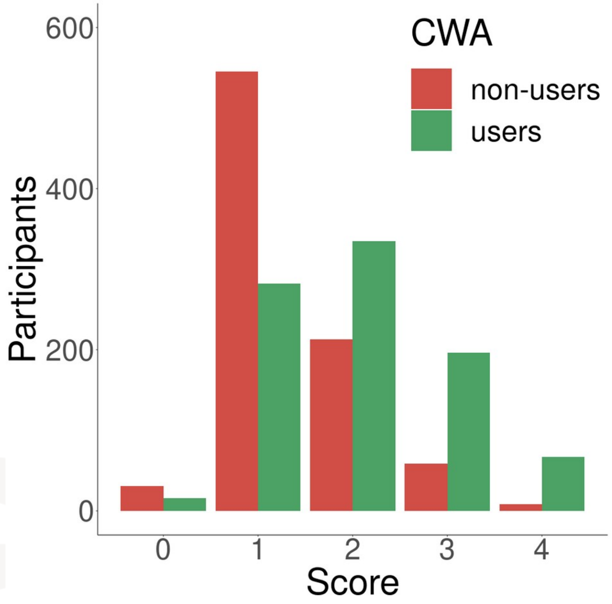
Significance: $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$

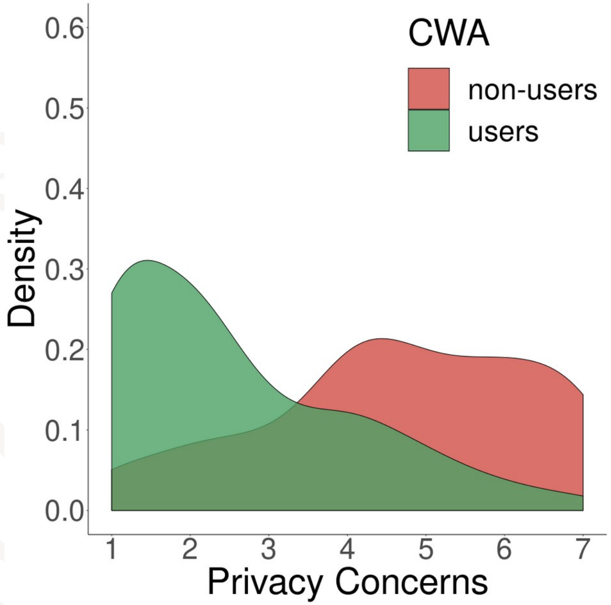
David Harborth, Xinyuan Cai, and Sebastian Pape. Why do people pay for privacy? In ICT Systems Security and Privacy Protection - 34th IFIP TC 11 International Conference, SEC 2019.

Conclusion

- Trust
  - Acceptance of PETs
  - Social engineering attacks
- Economics
  - PETs
  - Security Management
- Regulations
  - Can foster adoption
  - Can hinder provision

Study about Corona Warn-App





Sebastian Pape, David Harborth, Jacob Leon Kröger: Privacy Concerns Go Hand in Hand with Lack of Knowledge: The Case of the German Corona-Warn-App, Submitted to IFIP SEC 2021

Sensor-based Inference Attacks on Wearables

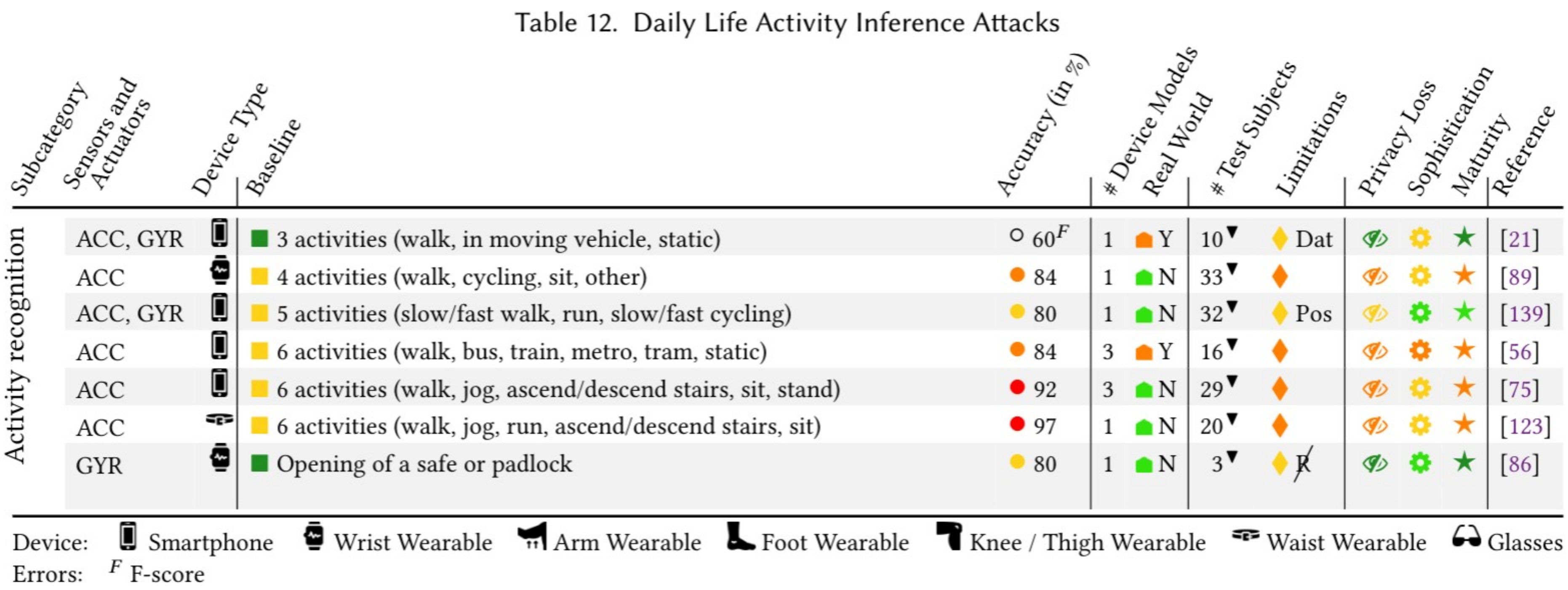


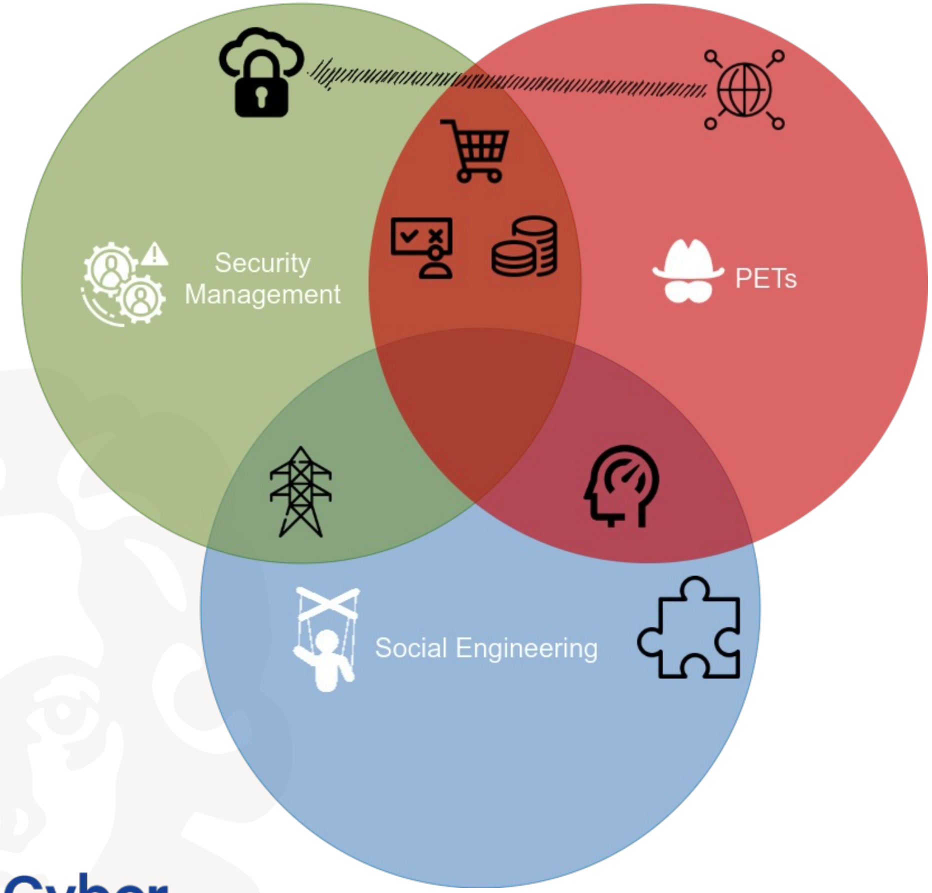
Table 12. Daily Life Activity Inference Attacks

Subcategory	Sensors and Actuators	Device Type	Baseline	Accuracy (in %)	# Device Models	Real World	# Test Subjects	Limitations	Privacy Loss	Sophistication	Maturity	Reference
Activity recognition	ACC, GYR	📱	🟩 3 activities (walk, in moving vehicle, static)	○ 60^F	1	⌂ Y	10▼	◆ Dat	👁	⚙	★	[21]
	ACC	⌚	🟨 4 activities (walk, cycling, sit, other)	🟠 84	1	⌂ N	33▼	◆	👁	⚙	★	[89]
	ACC, GYR	📱	🟨 5 activities (slow/fast walk, run, slow/fast cycling)	🟡 80	1	⌂ N	32▼	◆ Pos	👁	⚙	★	[139]
	ACC	📱	🟨 6 activities (walk, bus, train, metro, tram, static)	🟠 84	3	⌂ Y	16▼	◆	👁	⚙	★	[56]
	ACC	📱	🟨 6 activities (walk, jog, ascend/descend stairs, sit, stand)	🔴 92	3	⌂ N	29▼	◆	👁	⚙	★	[75]
	ACC	⌚	🟨 6 activities (walk, jog, run, ascend/descend stairs, sit)	🔴 97	1	⌂ N	20▼	◆	👁	⚙	★	[123]
	GYR	⌚	🟩 Opening of a safe or padlock	🟡 80	1	⌂ N	3▼	◆ ~~R~~	👁	⚙	★	[86]

Device: 📱 Smartphone ⌚ Wrist Wearable Arm Wearable Foot Wearable Knee / Thigh Wearable Waist Wearable 👓 Glasses
Errors: ^{F} F-score

Sebastian Pape, Vanessa Bracamonte, Jacob Leon Kröger, Welderufael Tesfay, Majid Hatamian, Shinsaku Kiyomoto, Kai Rannenberg: A Framework for Privacy Risk Analysis of Sensor-Based Inference Attacks onSmartphones and IoT Wearables, Submitted to TOPS

Contact



Sebastian Pape

sebastian.pape@m-chair.de