A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises

Nicolas Huaman
CISPA Helmholtz Center for Information Security & Leibniz University Hannover

Bennet von Skarczinski
PwC Germany

Christian Stransky
Leibniz University Hannover

Dominik Wermke
CISPA Helmholtz Center for Information Security & Leibniz University Hannover

Yasemin Acar
Max Planck Institute for Security and Privacy & Leibniz University Hannover

Arne Dreißigacker
Criminological Research Institute of Lower Saxony

Sascha Fahl
CISPA Helmholtz Center for Information Security & Leibniz University Hannover

Cyber Attacks in Small- and Medium-sized Enterprises

- Cybercrime as a whole has been on the rise in recent years

- SMEs have become a major focus of these attacks
- Limited resources make them easier targets

Data about Cybercrime

Yearly reports concerning cybercrime exist

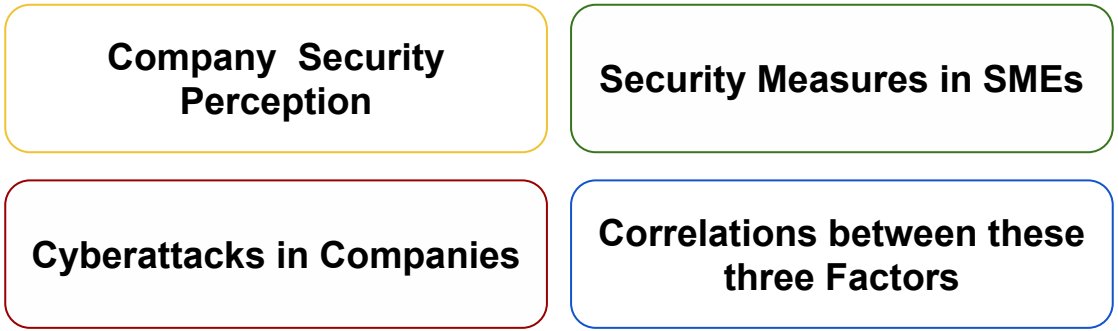
Focus:

- Cybercrime Measurement
- Security Recommendations

Research Questions

- *We want to look at potential influences for the risk of attack.*

Areas of focus:



Approach

Approach

- Conducted computer-assisted telephone interviews (CATI) with 5,000 SMEs in Germany

Category	Selection Criteria	Sample Size		Percent	
		Target	After Filtering	Dataset	Real World
10–49 employees	Proportional to the selection population by company size and industry; Industry by WZ08-Classification A to S†	1,000	1,190	23.8%	79.1%
50–99 employees		1,000	1,181	23.6%	10.5%
100–249 employees		1,000	1,120	22.4%	6.5%
250–499 employees	Best Effort Base by company size and industry; industry by WZ08-Classification A to S†	1,000	1,005	20.1%	2.2%
500+ employees		500+	504	10.1%	1.8%
Enterprises providing services of general interest [16]	Best Effort Base by industry; Selected industries (Subindustries of WZ08-D, E, H, J, K, L, O, P, Q)	500	*	*	*
Total			5,000	100%	100%

Interview Design

1. Design Phase
Literature review, six expert interviews and input from regional business advisory council.

2. Recruitment
Stratisfied random sampling (n=5000) by industry sector.

3. Piloting
Discussions with twelve security experts and five pilots

4. Training
Training sessions with the 141 telephone interviewers

5. Execution
5000 computer assisted telephone interviews (CATI); August 2018 to February 2019

6. Data Handling
Quality checks & anonymization by service provider; open coding & evaluation by authors

Survey

Main areas:

Company Perception

Risk Perception
Security Awareness

Security Measures

Firewalls, Antivirus
Employee Training
& more

Cybercrime Incidents

Phishing, DDoS
Ransomware
& more

Company Demographics

Budget, Size
Tech-employees
& more

Results

Demographics

	Ratio	Companies
Company Age > 10 Years	83.8%	4,192
Export Activity	39.9%	1,997
Interviewee position		
• Tech & Information Security	69.7%	3,484
• Management	23.4%	1,171
• More in paper...		
IT-Department Inhouse	85.2%	4,262
Information Security Staff Inhouse	73.6%	3,682

Regressions

To find correlations within the data, we conducted Regressions

General findings:

- Interviewee position bias
- Self reporting of incident counts likely of low quality

Table 4: Linear regressions for risk assessment.

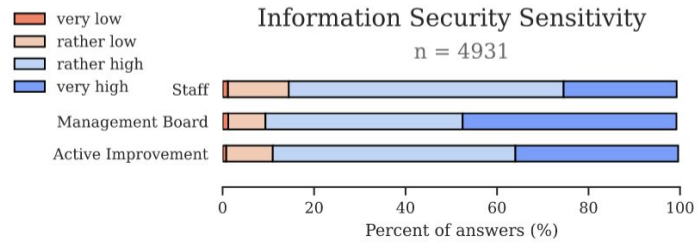
Assessment for mass attacks	**Coef.**	**C.I.**	***p*-value**
Interviewee Position			
Management	**0.13**	**[0.00, 0.25]**	**0.05***
Tech	**0.23**	**[0.12, 0.35]**	**<0.01***
Export Activity	**0.12**	**[0.04, 0.20]**	**<0.01***
Multiple National Branches	0.07	[-0.01, 0.15]	0.09
International Branches	**0.15**	**[0.03, 0.26]**	**0.01***
Information Security Sensitivity Employees	**-0.10**	**[-0.14, -0.06]**	**<0.01***
Per 1 Mio Annual Turnover	0.00	[-0.00, 0.00]	0.27
Employees (Per 100)	0.03	[-0.00, 0.06]	0.07
Assessment for targeted attacks	**Coef.**	**C.I.**	***p*-value**
Interviewee Position			
Management	-0.02	[-0.13, 0.08]	0.66
Tech	0.07	[-0.04, 0.17]	0.23
Data Protection Officer	**-0.11**	**[-0.22, -0.01]**	**0.04***
Other	**-0.13**	**[-0.26, -0.00]**	**0.05***
Export Activity	**0.14**	**[0.09, 0.20]**	**<0.01***
Multiple National Branches	**0.06**	**[0.00, 0.12]**	**0.03***
International Branches	**0.11**	**[0.03, 0.20]**	**<0.01***
Information Security Sensitivity Management	**-0.04**	**[-0.07, -0.02]**	**<0.01***
Per 1 Mio Annual Turnover	0.00	[-0.00, 0.00]	0.11
Employees Tech (Per 100)	0.00	[-0.00, 0.00]	0.09
Employees (Per 100)	**0.03**	**[0.01, 0.05]**	**<0.01***

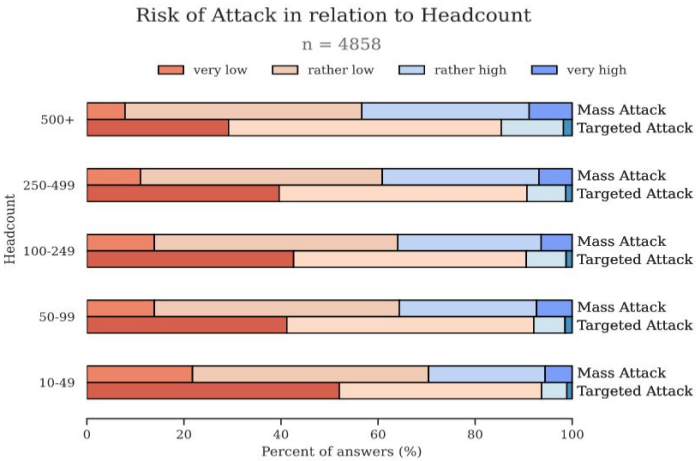
Company Security Awareness

Ratings:

- High self-reported security awareness
- Low estimation of attack risk
- Especially low risk of targeted attacks

➔ Misconceptions?





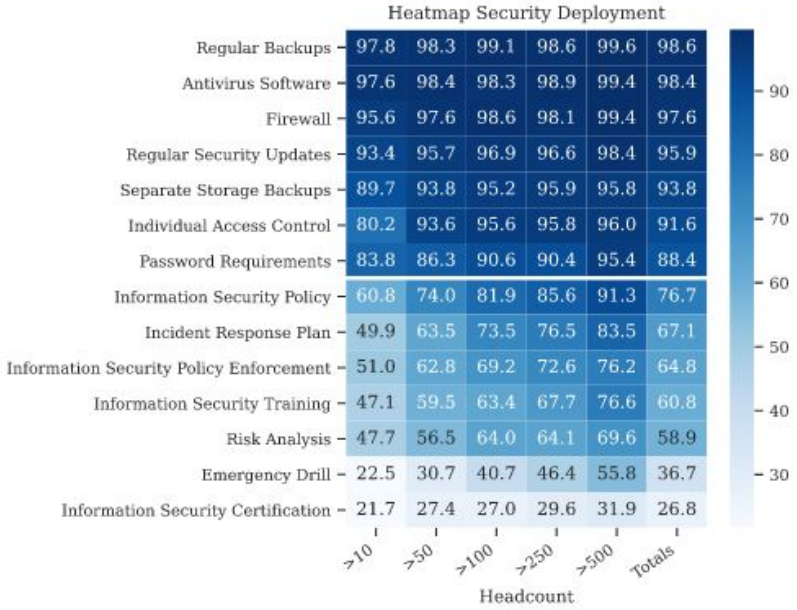
Security Measurements

Basic technical measures are available in all companies

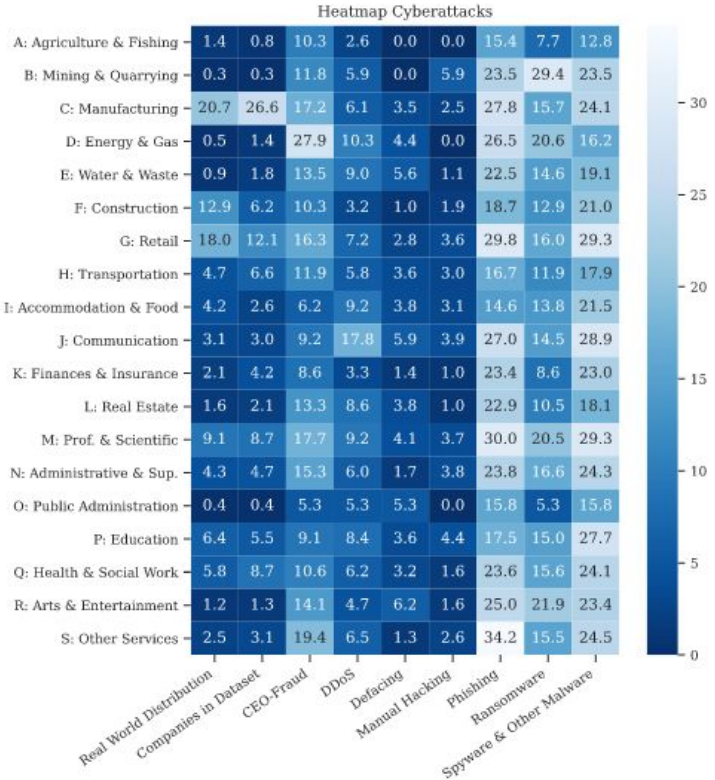
Limited distribution:

- Certification & Training
- Risk Analysis
- Emergency Drills

➔ Risk awareness and estimation is low



Cybercrime Incidence



Takeaways:

- Most common successful attack (within 12 months before the interview): Phishing
- Some industry sectors correlate with certain attack vectors
- Companies with higher coverage of measures also report higher incidence!
- More in the Paper...

Recommendations

Recommendations

- For Companies:
  - Investigate discrepancy between employee and management security awareness.
  - More in paper...

Recommendations

- For Legislators:
  - Industry sectors with higher legislative security requirements tend to report lower incidences.

➔ Security policies are important to control direction of company security

➔ More in paper...

Future Work

- Misconceptions in risk awareness and how to approach security should be investigated.
- In-depth investigation of the correlations we found regarding security measures and incidence reporting.
- Future work needs to consider: The interviewee position had a significant influence on almost all areas!

Key Takeaway

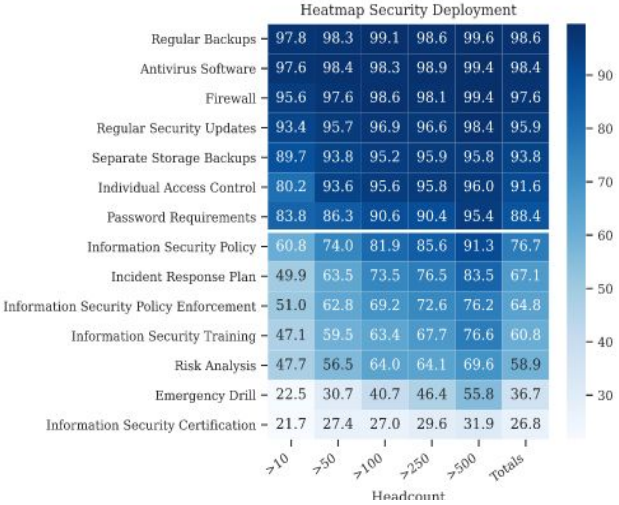
- Information Security has arrived in companies!
  - Security in practice might be flawed however
  - Factor “Human” is still not appropriately considered!

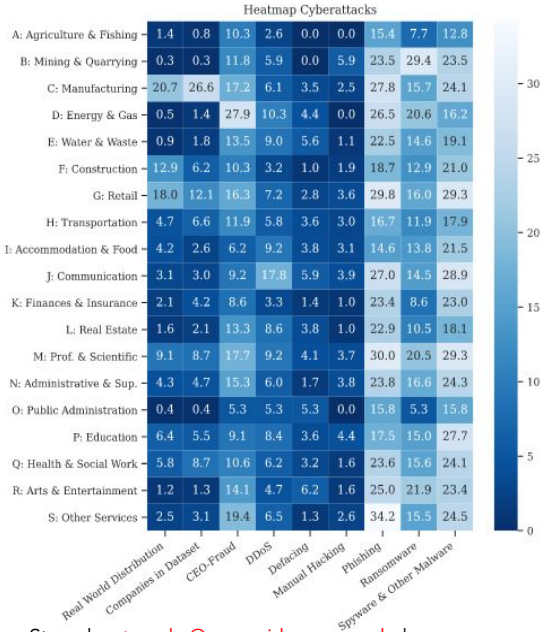
Conclusion

Interviewed 5000 company representatives:

- Created an overview of cybercrime effects in germany
- Found interesting tendencies to follow
- Found a few important indicators for self-reporting quality (e.g. interviewee position)

Category	Selection Criteria	Sample Size		Percent	
		Target	After Filtering	Dataset	Real World
10–49 employees 50–99 employees 100–249 employees	Proportional to the selection population by company size and industry; Industry by WZ08-Classification A to S†	1,000 1,000 1,000	1,190 1,181 1,120	23.8% 23.6% 22.4%	79.1% 10.5% 6.5%
250–499 employees 500+ employees	Best Effort Base by company size and industry; industry by WZ08-Classification A to S†	1,000 500+	1,005 504	20.1% 10.1%	2.2% 1.8%
Enterprises providing services of general interest [16]	Best Effort Base by industry; Selected industries (Subindustries of WZ08-D, E, H, J, K, L, O, P, Q)	500	*	*	*
Total			5,000	100%	100%





Nicolas Huaman huaman@sec.uni-hannover.de | Bennet von Skarczinski bennet.simon.von.skarczinski@pwc.com | Christian Stransky stransky@sec.uni-hannover.de | Dominik Wermke wermke@sec.uni-hannover.de | Yasemin Acar yasemin.acar@mpi-sp.org | Arne Dreißigacker arne.dreissigacker@kfn.de | Sascha Fahl sascha.fahl@cispa.de

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY KFN