SecHUMAN
FORSCHUNGSKOLLEG
SICHERHEIT FÜR MENSCHEN IM CYBERSPACE

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

WHERE ARE WE ON CYBER?

A Qualitative Study On Boards' Cybersecurity Risk Decision Making

Jens Christian Opdenbusch
Ruhr University Bochum, Germany

Jonas Hielscher
Ruhr University Bochum, Germany

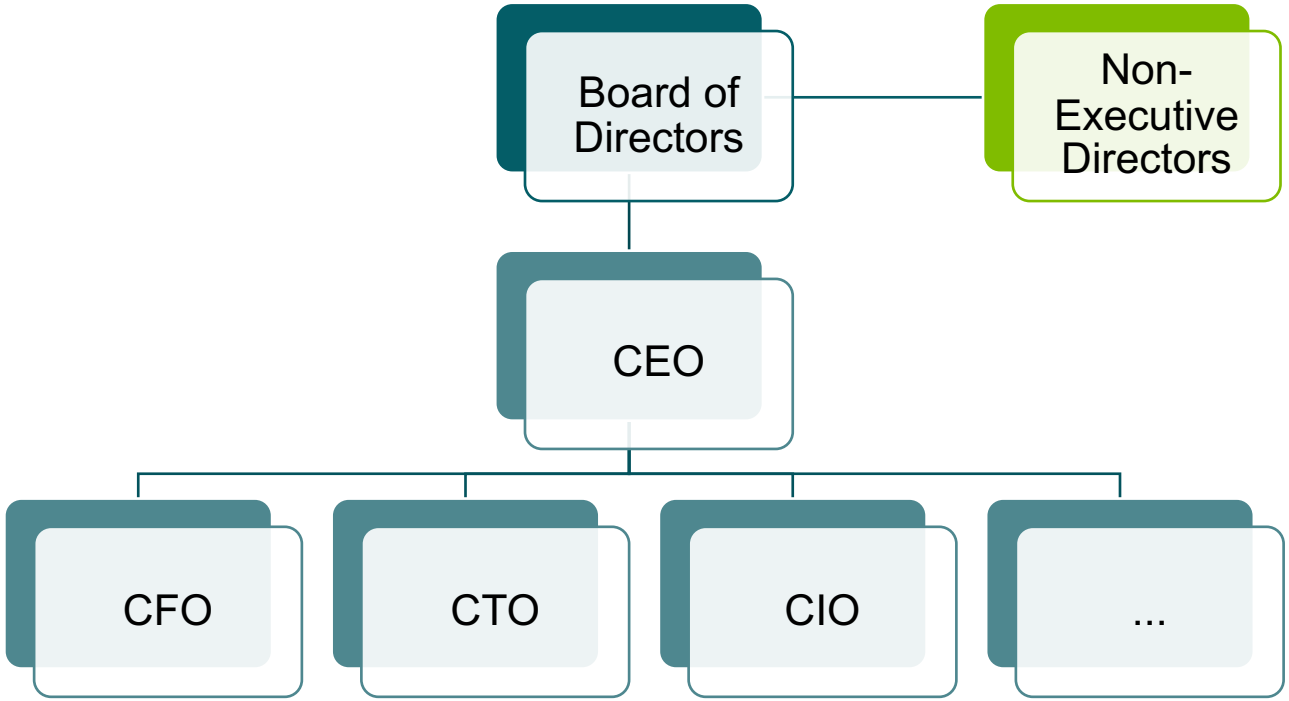
M. Angela Sasse
Ruhr University Bochum, Germany
University College London, UK

RUHR UNIVERSITÄT BOCHUM
RUB
Lloyd's Register
Gefördert durch
DFG Deutsche Forschungsgemeinschaft
National Cyber Security Centre
HG HORST GÖRTZ INSTITUT

ABOUT US

WHAT IS A BOARD

In the UK



WHY SHOULD WE LOOK AT BOARDS?

Motivation

Boards have an oversight role, including cybersecurity risk

[1][2][3]

Non-Executive Directors are tasked with maximizing shareholder value

Cybersecurity can harm stock price because cybersecurity disclosures harm stock price

[4]

[1] R. A. Rothrock, J. Kaplan, and F. Van Der Oord, “The board’s role in managing cybersecurity risks,” MIT Sloan Management Review, vol. 59, no. 2, pp. 12–15, 2018.
[2] SEC, “Federal Register Commission Statement and Guidance on Public Company Cybersecurity Disclosures,” 2018.
[3] S. Schinagl and A. Shahim, “What do we know about information security governance? “from the basement to the boardroom”: towards digital security governance,” Information & Computer Security, vol. 28, no. 2, pp. 261–292, 2020.
[4] Wu, Huaping, Ming Ma, and Jidong Zhang. "Impact of Cybersecurity Disclosure Frequency on Stock Price Crash Risk." *Journal of Corporate Accounting & Finance* (2024).

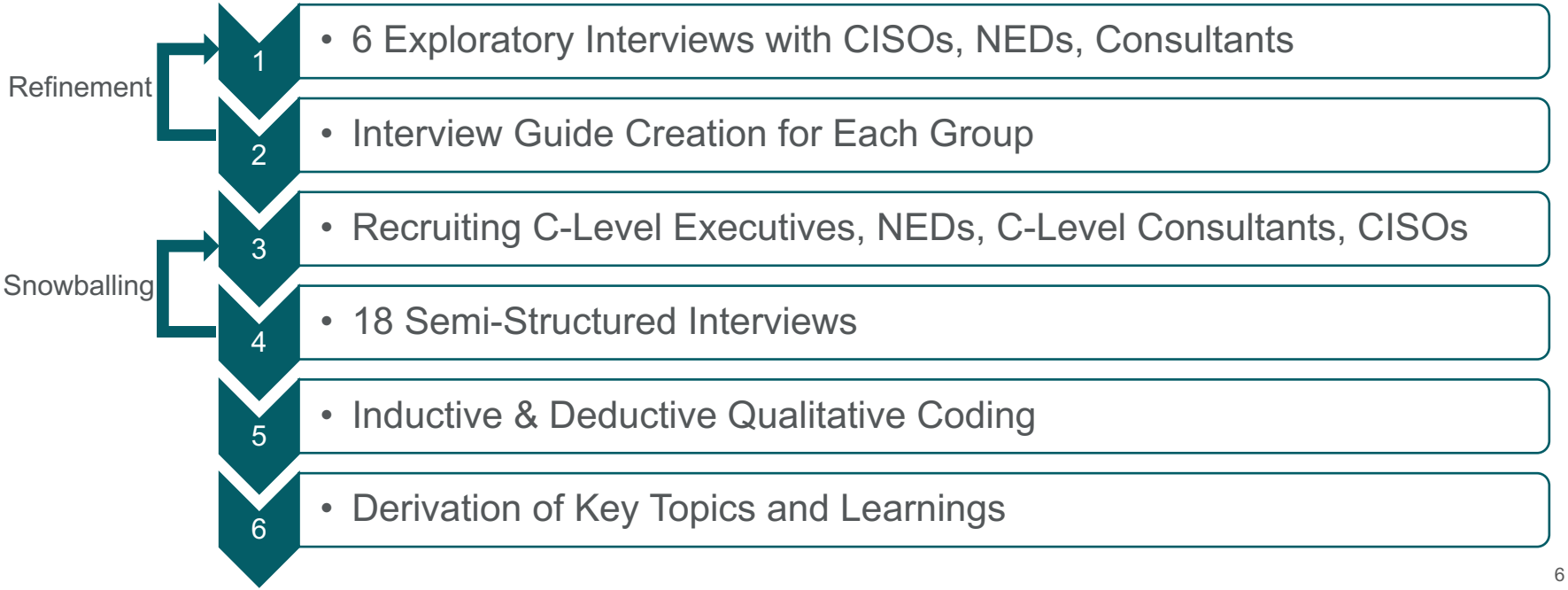
WHAT DID WE RESEARCH?

Our Research Questions

I) How does cybersecurity risk decision-making of boards work?	We want to understand the information flow toward the board, the type and content of their decisions, and how they are executed.
II) How do other Stakeholders influence those decisions?	We want to understand how CISOs, executives, regulators, investors, and others influence cybersecurity risk decision-making.

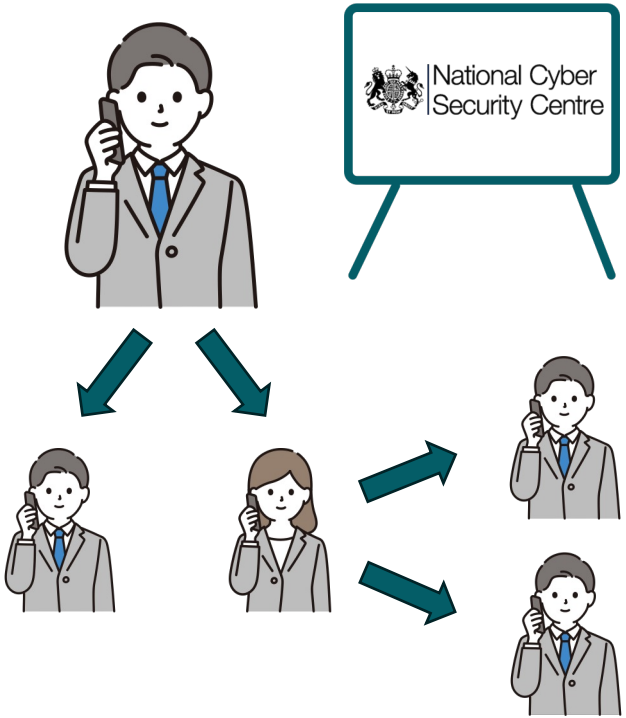
HOW DID WE DO THAT?

Methodology



WHO PARTICIPATED?

Recruitment

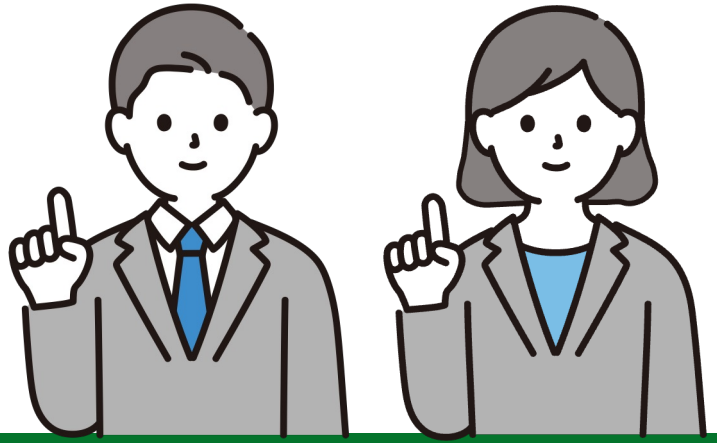


Gender		#	%
Male		16	*89%*
Female		2	*11%*
Job Title			
Executive		6	*33%*
Non-Executive (NED)		4	*22%*
CISO		5	*28%*
Consultant		3	*17%*
Industry			
Banking		5	*28%*
Telecommunication		4	*22%*
Logistics		3	*17%*
Consulting		3	*17%*
Energy		1	*6%*
Technology		1	*6%*
Public sector		1	*6%*
Number of Employees			
Max	260,000	*Average*	88,900
Min	5,000	*Median*	94,000
Interview Duration [min]			
Max	62	*Average*	48
Min	37	*Median*	49

ASKING THE RIGHT QUESTIONS?

Results (1/6)

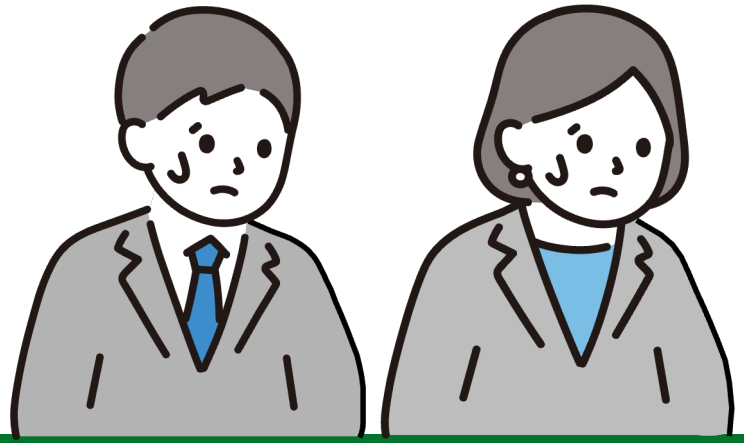
*“They want to know that I have got enough investment, which they always ask me around, **’Are we giving you enough money?’**.” – [CISO3]*



ASKING THE RIGHT QUESTIONS?

Results (1/6)

*"They're perhaps just sometimes **scared that it's technology**. I can't understand it, you know, **it's a dark art, it's a bunch of chaps in hoodies.**" – [Executive 6]*



ROLE OF REGULATION

Results (2/6)

*"**Regulation elevates the profile with boards**, and I think that is healthy because else it could get pushed down and you might lose traction." – [CISO3].*

*"I do think **[the cybersecurity agency] could do a lot more in sharing what they know.**" – [CISO3].*

DIFFERENT RISK PERCEPTIONS

Results (3/6)

*"If you have a **board conversation where someone is talking about what antivirus tool** they are using, **you have got a problem**." – [Executive 3]*

vs.

TRANSLATING CYBERSECURITY RISKS

Results (4/6)

*"What I do is **I prepare the material for the CFO to present to the board**. And that is another challenge, is that **the CFO is not, is not an IT person**. So I need to give him the material and he is the one communicating to the board. […] **I think it works really well** because he understands and **he manages to put that in the bigger perspective and translate** that, **removing the IT, geeky world and concept out of it**" – [CISO1]*

TRADITIONAL RISK MANAGEMENT VS CYBERSECURITY RISKS

Results (5/6)

*"The ability to measure is something the financial services world is very comfortable with, and **cyber and many operational risks do not easily fit into that framework**." – [NED3].*

INVESTORS DEMAND FOR CYBERSECURITY

Results (6/6)

*"I sit through quarterly investor presentations, and **I have never heard a question about it**. Which is surprising, now you mention it." – [NED2].*

*"I mean **I would be amazed if any investor ever asked questions about cybersecurity** because, you know, it is one of many, many things that a company manages." – [NED3].*

*"Well the first question is **would a serious investor even think of asking that question**?"– [NED4].*

WHAT CAN WE DO BETTER?

Discussion

Bridging the gap between CISOs' and NEDs' Language

Short Term: Executive translating

Build Subcommittees designated to discuss and translate cybersecurity risks

CISOs, Executive, NED attending

WHAT'S NEXT?

Future Work

Study Cybersecurity at Boards

- Highest Level in Organizations
- Hard to recruit
  - Leveraging State (Cybersecurity) Agencies

Leveraging Risk Management

- Build on the maturity of other fields
- Research applicability to cybersecurity
  - We found some evidence that market and credit risk might be a fit.

Q&A!

CASA
Cyber Security in the Age of Large-Scale Adversaries

Jonas Hielscher
jonas.hielscher@ruhr-uni-bochum.de
Chair for Human Centred Security
Ruhr University Bochum - Germany

Jens Christian Opdenbusch
jens.opdenbusch@ruhr-uni-bochum.de
Chair for Human Centred Security
Ruhr University Bochum - Germany

Prof. M. Angela Sasse
martina.sasse@ruhr-uni-bochum.de
Chair for Human Centred Security
Ruhr University Bochum – Germany
University College London - UK

The project was funded by the UK NCSC and Lloyds Register Foundation, as well as the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972, and also by the PhD School "SecHuman – Security for Humans in Cyberspace" by the federal state of NRW, Germany.