



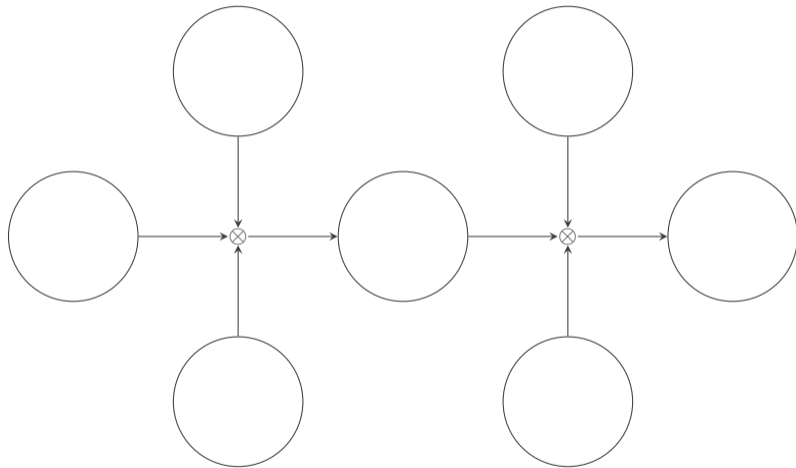
# Quantifying Cyber Risk

Workshop on Real-life Impacts of Security Vulnerabilities

Rainer Böhme

Collegium Helveticum · Zürich · 18 April 2024

# Preview



# Agenda

- 1. Systematic review of cyber risk quantification studies**
2. Towards a theory of security technology avoidance

# Naively Linking Security to Harm

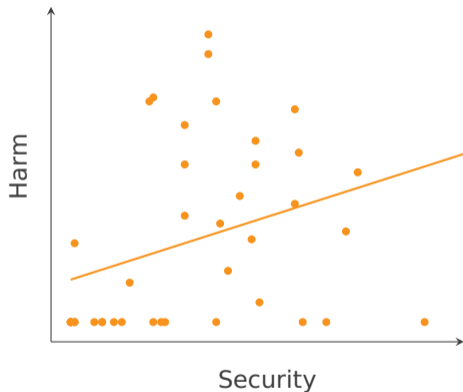
A fundamental law—more security, less harm ?



*“We find that investment in information technology (IT) security corresponds to a higher risk of data breach incidents within both a state and an industry.”*

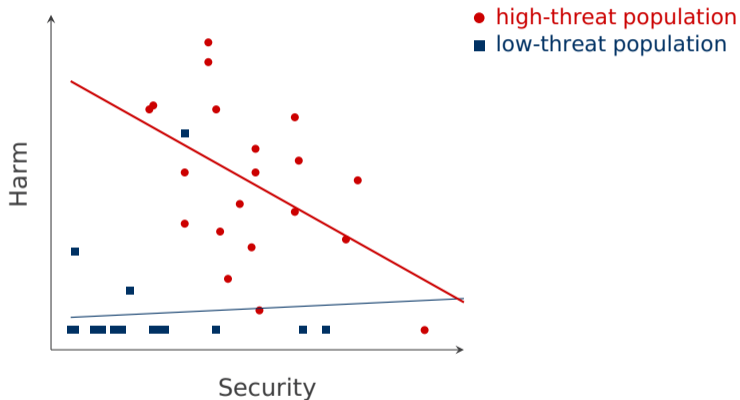
R. Sen and S. Borle. Estimating the contextual risk of data breach: An empirical approach.  
*Journal of Management Information Systems*, 32 (2):314–341, 2015.

# Naive Regressions



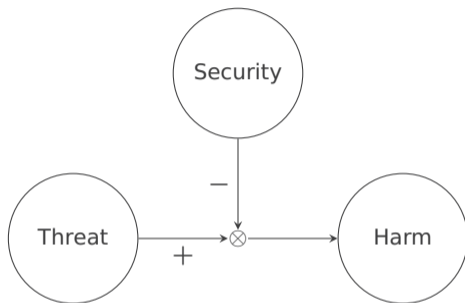
Artificial data from Woods & Böhme 2021

# Naive Regressions

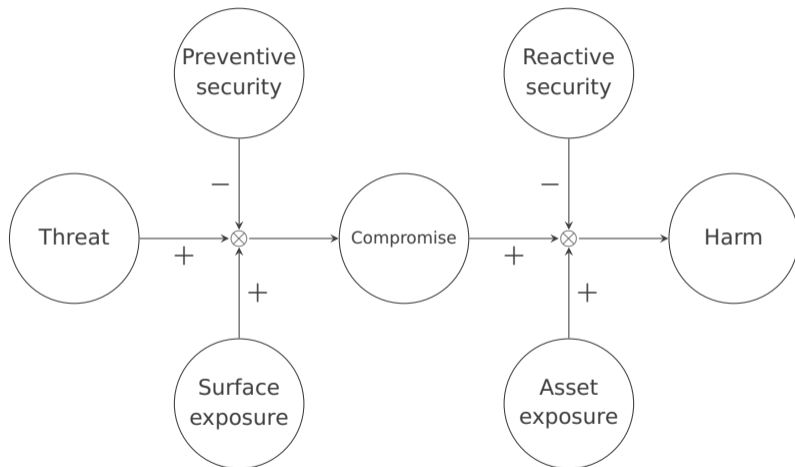


Artificial data from Woods & Böhme 2021

# How to Model Cyber Risk?



# Causal Model of Cyber Risk





# Description of Latent Factors

## **Threat**

The motivation, capability and activity of adversaries.

## **Surface exposure**

Factors increasing potential vectors of compromise.

## **Preventive security**

Interventions reducing the ease of compromise.

## **Compromise**

Violation of a victim security goal.

## **Asset exposure**

Factors increasing the value of what can be compromised.

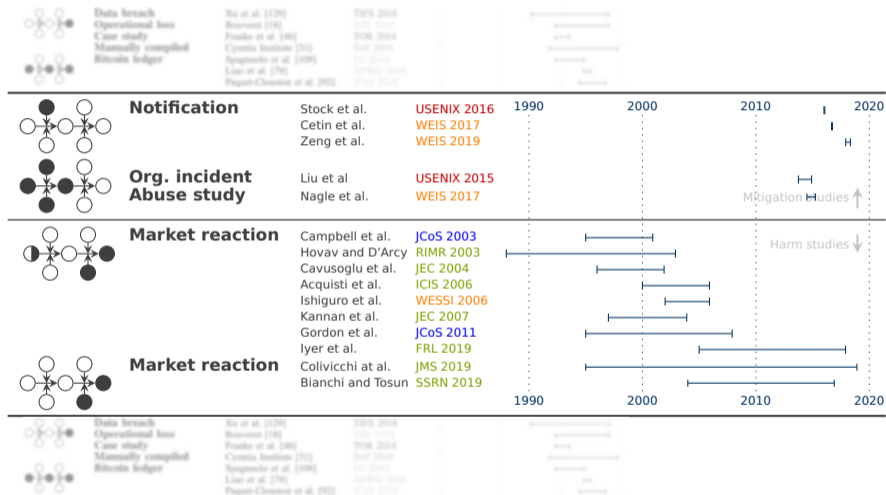
## **Reactive security**

Interventions reducing the impact of compromise.

## **Harm**

Negative consequences resulting from compromise.

# Classifying Studies

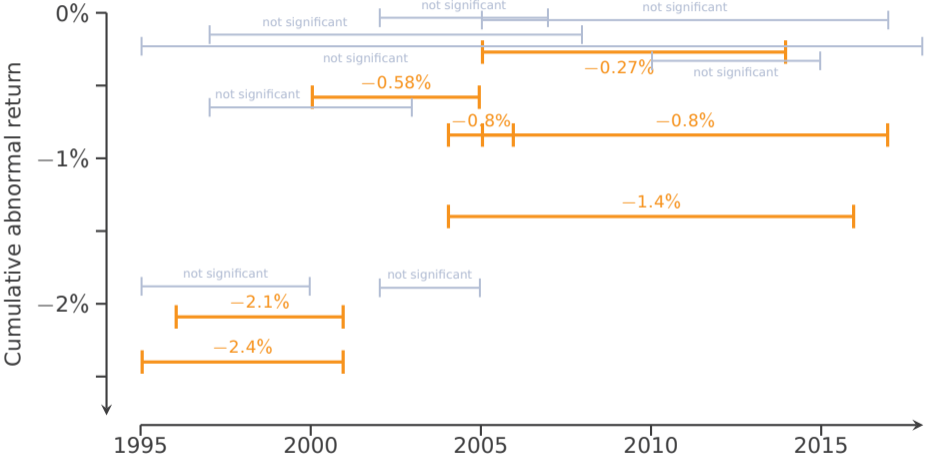


Extract from Table III in our SoK paper, which contains all classifications.

# Approaches Taken by Harm Studies

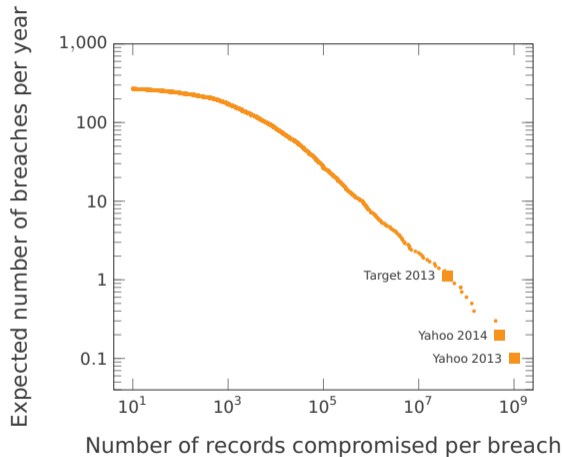
Unit of analysis	# of studies	Econ loss	Sample size	Earliest study	Earliest sample
<b>Public reports</b>					
Data breach	9	X	600–6160	2008	2000
Operational loss	3	✓	341–1579	2015	< 2003
Cyber incident	1	✓	2216	2016	2005
<b>Private reports</b>					
Internal incident	2	X	1800–23000	2010	1996
Insurance claim	1	X	70	2019	2015
Crime reports	1	✓	7925	2020	2017
Firm survey response	3	✓	664–4209	2012	2012
Individual survey response	5	✓	1500–64287	2014	2010s
<b>Externally observed</b>					
Legal case	2	X	19–230	2011	1999
Legal case	1	✓	118	2017	2010
Bitcoin transaction	3	✓	10m	2014	2009
Criminal forum post	2	✓	13m	2007	2006
Insurance prices	1	✓	6828	2019	2007
Stock market reaction	19	✓	43–542	2003	1988
<b>System-wide harm</b>					
Multi-party incident	1	✓	800	2019	2008

# Meta Review of Stock Market Reactions

















Simplified version of Figure 4 in our SoK paper. Statistically significant at the 0.05 level.

# Published Data Breaches 2007–2016



Data source: Privacy Rights Clearinghouse, own analysis following the method in Wheatley et al. 2016

# Contradictory Data Breach Studies

Reference	# obs	Years	Breach frequency	Breach size
Curtin et al. (2008)	899	2005–07		?
Maillart et al. (2010)	956	2000–08		
Edwards et al. (2016)	2253	2005–15		
Wheatley et al. (2016)	5365	2007–15		
Eling et al. (2017)	2266	2005–15		
Xu et al. (2018)	600	2005–17		
Wheatley et al. (2019)	1713	2005–17		
Carfora et al. (2019)	5724	2005–17		?

Simplified version of Table II in our SoK paper.

# Agenda

1. Systematic review of cyber risk quantification studies
2. **Towards a theory of security technology avoidance**

# Asokan's Conjecture

Widespread *negative perception* from *well-publicized vulnerabilities* causes *opportunity costs*.

These costs come in at least two forms:

- 1. Industry may prematurely pull technologies from deployment;*
  - 2. Students and early-career researchers may shy away from technology that was subject to claimed total breaks;*
- because they perceive it as too risky.*

<https://medium.com/@asokan.public/workshop-real-life-impacts-of-cyber-security-vulnerabilities-846f0fda62d2>  
(accessed 17 April 2024; abridged from the original)



# Confirming Observations

## SoK: Privacy-Enhancing Technologies in Finance

Carsten Baum 

Technical University of Denmark, Lyngby, Denmark

James Hsin-yu Chiang 

Aarhus University, Denmark

Bernardo David 

IT University of Copenhagen, Denmark

Tore Kasper Frederiksen 

Zans, Paris, France

### Abstract

Recent years have seen the emergence of practical advanced cryptographic tools that not only protect data privacy and authenticity, but also allow for jointly processing data from different institutions without sacrificing privacy. The ability to do so has enabled implementations of a number of traditional and decentralized financial applications that would have required sacrificing privacy or trusting a third party. The main catalyst of this revolution was the advent of decentralized cryptocurrencies that see public ledgers to register financial transactions, which must be verifiable by any third party, while keeping sensitive data private. Zero Knowledge (ZK) proofs rose to prominence as a solution to this challenge, allowing for the owner of sensitive data (e.g. the identities of users involved in an operation) to convince a third party verifier that a certain operation has been correctly executed without revealing said data. It quickly became clear that performing arbitrary computation on private data from multiple sources by means of secure Multiparty Computation (MPC) and related techniques allows for more powerful financial applications, also in traditional finance.

In this SoK, we categorize the main traditional and decentralized financial applications that can benefit from state-of-the-art Privacy-Enhancing Technologies (PETs) and identify design patterns commonly used when applying PETs in the context of these applications. In particular, we consider the following classes of applications: 1. Money Management, KYC & AML, 2. Markets & Settlement, 3. Legal and 4. Digital Asset Custody. We examine how ZK proofs, MPC and related PETs have been used to tackle the main security challenges in each of these applications. Moreover, we provide an assessment of the technological readiness of each PET in the context of different financial applications according to the availability of: theoretical feasibility results, preliminary benchmarks (in scientific papers) or benchmarks achieving real-world performance (in commercially deployed solutions). Finally, we propose future applications of PETs as Finnish solutions to currently unsolved issues. While we systematic financial applications of PETs at large, we focus mainly on those applications that require privacy preserving computation on data from multiple parties.

2012 ACM Subject Classification Security and privacy → Cryptography

Keywords and phrases DeFi, Anti-money laundering, MPC, FHE, identity management, PETs

Digital Object Identifier 10.4230/LIPDS-AFT.2021.12

Related Version Full Version: <https://arxiv.org/abs/1907.02021v2>

Funding Carsten Baum: Part of the work was carried out while the author was visiting Copenhagen University and supported by Partisia. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of Partisia. James Hsin-yu Chiang: This work was supported by a DTU Caspar scholarship.

Bernardo David: The project was supported by the Independent Research Fund Denmark (IRFD) grants number 9048-00009 (DTA-C), 9033-00070 (FUTIA) and 0003-00070, and by EDRAC. Tore Kasper Frederiksen: This work was carried out while working at Protocol Labs and the Alexandria Institute (supported by Copenhagen FinTech as part of so part of the "National Platform of Strength programmes for Finance & Fintech" funded by the Danish Ministry of Higher Education and Science).

© Carsten Baum, James Hsin-yu Chiang, Bernardo David, and Tore Kasper Frederiksen.

 Licensed under Creative Commons License (CC BY 4.0)

https://creativecommons.org/licenses/by/4.0/

https://doi.org/10.4230/LIPDS-AFT.2021.12.30

 Lecture Notes in Computer Science, Springer, 2021

**A note on Trusted Execution Environments.** Trusted Execution Environments (TEE) such as Intel's SGX are special modes of modern processors. A processor in its trusted execution setting guarantees that programs and their data are shielded from every other program running on the computer - even the operating system or any user having full access. A secure TEE allows to build many of the aforementioned PETs such as ZK proofs, PSI, MPC etc. "cheaply" and without additional cryptographic tools. In practice, SGX and similar technologies from other vendors<sup>5</sup> are regularly broken and do not offer the protection that they claim. We therefore do not consider it as a PET in this document.

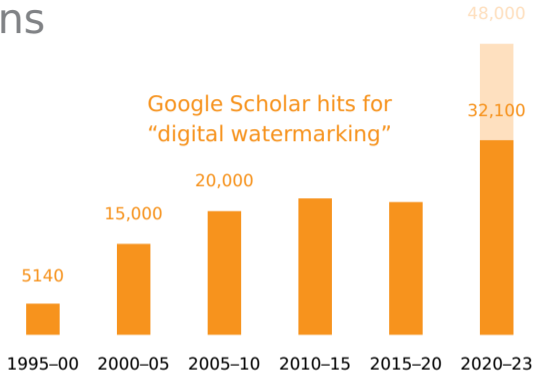
# Contradicting Observations

## Attacks on Copyright Marking Systems

Fabien A.P. Petitcolas \*, Ross J. Anderson, and Markus G. Kuhn\*\*

University of Cambridge, Computer Laboratory  
Pembroke Street, Cambridge CB2 3QG, UK  
{fapp2, rja14, mgk25}@cl.cam.ac.uk  
<http://www.cl.cam.ac.uk/Research/Security/>

**Abstract.** In the last few years, a large number of schemes have been proposed for hiding copyright marks and other information in digital pictures, video, audio and other multimedia objects. We describe some contenders that have appeared in the research literature and in the field; we then present a number of attacks that enable the information hidden by them to be removed or otherwise rendered unusable.



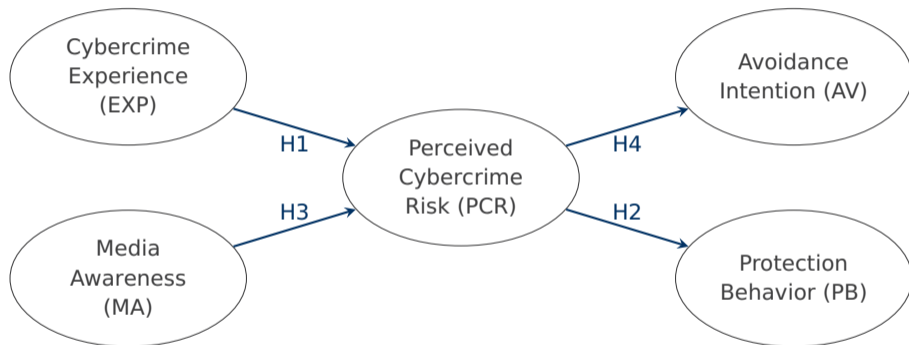
*IH'99 could be called the “Workshop on Watermarking Resistant to Lossy Compression.” We know fairly well how to achieve this, but have no idea how to achieve real security against well targeted attacks on watermarks. Industry’s hope of copy protection by watermarking either needs a real scientific breakthrough or a more realistic perspective.*

Andreas Pfitzmann

Information Hiding 1998 (top) and 1999 (bottom); abridged from the original. Own estimates using Google Scholar ranges.

# Towards Security Technology Avoidance

**Idea:** transfer a theory of consumer behavior to security expert behavior



**Riek, M.,** Abramova, S., and Böhme, R. Analyzing Persistent Impact of Cybercrime on the Societal Level: Evidence for Individual Security Behavior. In *Proceedings of the Thirty Eighth International Conference on Information Systems (ICIS)*. Seoul, 2017.

**Riek, M.,** Böhme, R., and Moore, T. Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, 13, 2 (2016), 261–273.

# Concluding Remarks

## State of the art

- Studies disagree on the harm resulting from cyber incidents.
- Studies inconsistently establish the effect size and even causal direction of security.
- Indicators of exposure tend to explain more variance than indicators of security.

## Lessons for this seminar

- Despite 20+ years of effort, it remains hard to link vulnerabilities to harm.
- The opportunity cost of **security technology avoidance** may exceed the harm caused by occasional breaches.
- Negative language (“broken”, if a distinguisher exists), amplified by popular media and opinionated experts, may cause undue security technology avoidance.
- Frameworks exists that can be adapted to support these conjectures with evidence.



# Merci

to the organizers for the invitation and to the audience for their attention

[rainer.boehme@uibk.ac.at](mailto:rainer.boehme@uibk.ac.at)

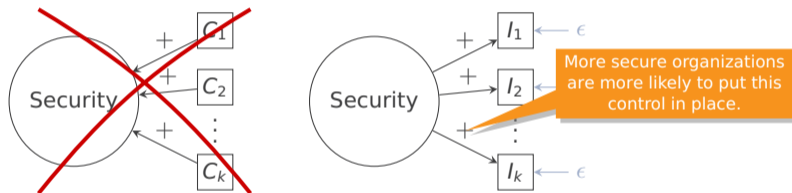
Part of this material is based on joint work with Svetlana Abramova, Markus Riek, and Daniel W. Woods.

# References

1. Woods, D. W., and Böhme, R.  
**Systematization of Knowledge: Quantifying Cyber Risk.**  
*IEEE Symposium on Security and Privacy*, (May 2021), 909–926.
2. Böhme, R., Laube, S., and Riek, M.  
**A Fundamental Approach to Cyber Risk Analysis.**  
*Variance*, 12, 2 (2019), 161–185.
3. Anderson, R., Barton, C., Böhme, R., et al.  
**Measuring the Changing Cost of Cybercrime.**  
*Workshop on the Economics of Information Security (WEIS)*, Harvard, 2019.
4. Tajalizadehkhoob, S., van Goethem, T., Korczykński, M., et al.  
**Herding Vulnerable Cats: A Statistical Approach to Disentangle Joint Responsibility for Web Security in Shared Hosting.**  
*ACM Conference on Computer and Communication Security*, Dallas, Texas, 2017.
5. Laube, S., and Böhme, R.  
**Strategic Aspects of Cyber Risk Information Sharing.**  
*ACM Computing Surveys*, 50, 5 (2017), 77:1–77:36.

# Measuring Latent Variables via Reflexive Indicators

Observing all security controls that collectively determine the security level is infeasible.



We can infer the latent security level using multiple controls as reflexive indicators.

# Review

