universität innsbruck

Lessons Lost

Incident Response in the Age of Cyber Insurance and Breach Attorneys

Daniel W. Woods, Rainer Böhme, Josephine Wolff, Daniel Schwarcz

32nd USENIX Security Symposium · Anaheim, CA · 9 August 2023

Learning from Security Failures

“One of the most important parts of incident response [...]: learning and improving.”

NIST 800-61, p. 38

“Insurers accumulate data [...] which they mine to improve risk assessment and suggest best practice mitigation strategies to their clients.”

Anderson et al. 2008 (ENISA), p. 40

“The IT industry does not have strong processes for extracting lessons learned and publishing them when incidents occur.”

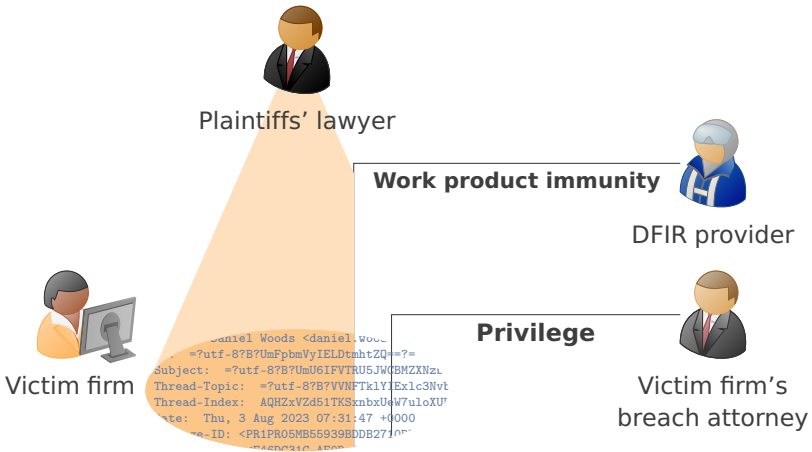
Knake, Shostack & Wheeler 2021 (Harvard Belfer Center)

Market Failure ?

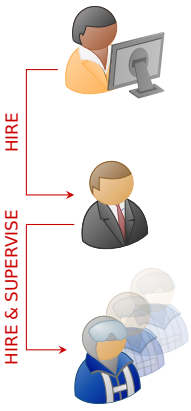
→ Insurers are not causing the issue. They are smart in dealing with the real problem.

DFIR: Digital Forensics / Incident Response

Discovery and Privilege



Consequences



Reasons to keep cybersecurity efforts confidential

- Limit litigation risk
- Negative publicity
- Regulatory actions

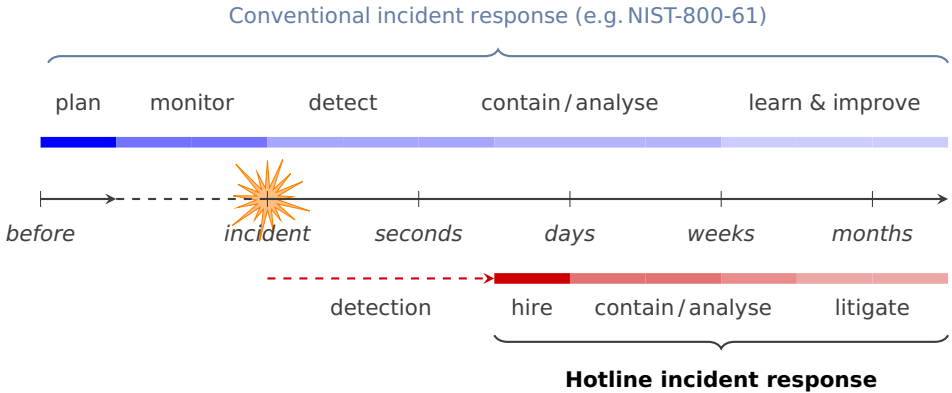
Measures taken

- Hire external counsel to coordinate all breach response
- “Hotline incident response”

Challenges for DFIR

- Onboard new provider during a crisis
- Mix of legal and non-legal goals
- Written reports: contents and distribution

Hotline Incident Response

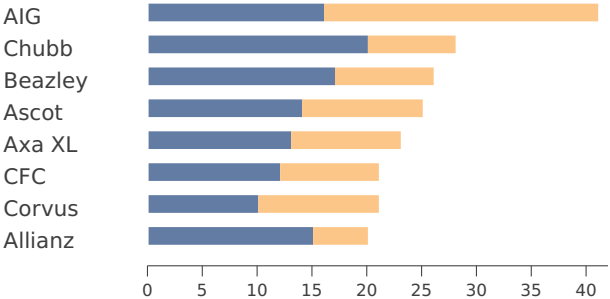


Woods, D. W. and Böhme, R. Incident Response as a Lawyers' Service. *IEEE Security & Privacy*, **20**, 2 (2022), 68–74.

Role of Insurers

Victim firms hire post-breach providers from a list (“panel”) specified in the policy.

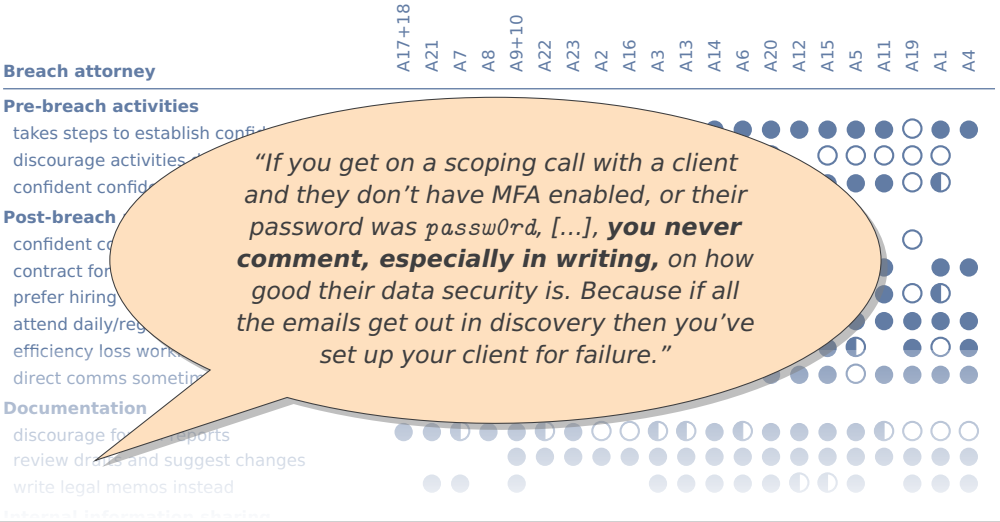
Number of DFIR and legal providers on insurers’ panels



→ Companies working together with pre-negotiated contracts can respond effectively.

Data source: authors’ desk research, 2022; excerpt of Fig. 2 in our paper.

Qualitative Data

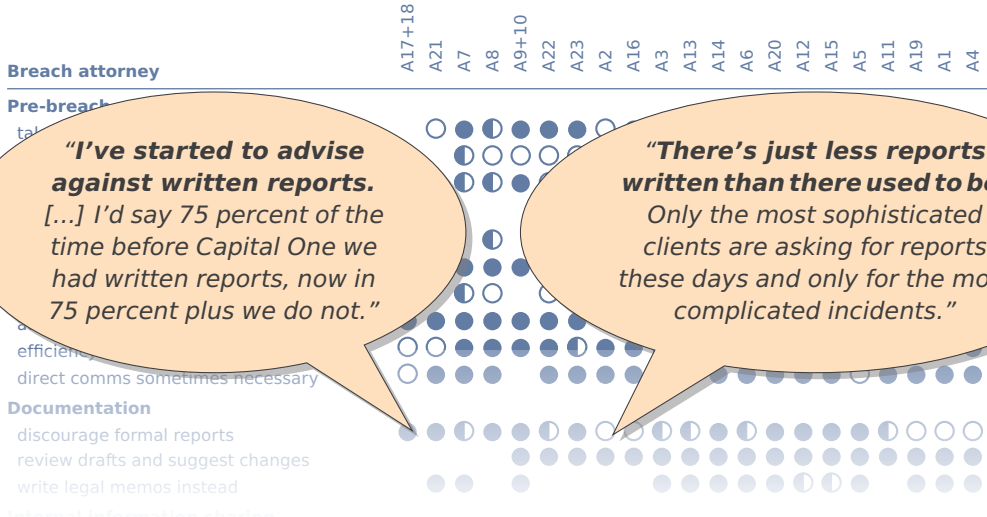


Turning Point: Capital One

- Early-adopter of public cloud strategy in the highly regulated financial industry
- Major breach in 2019, exposes 30 GB of credit application data
- Technical: SSRF + AWS EC2 weakness + ability to decrypt encrypted data
- Legal: court ruled that **incident report is discoverable** because it was driven by business rather than legal considerations.

Khan, S., Kabanov, I., Hua, Y. and Madnick, S. E. A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. *ACM Transactions on Privacy and Security*, **26**, 1 (2023), 3:1–3:29.

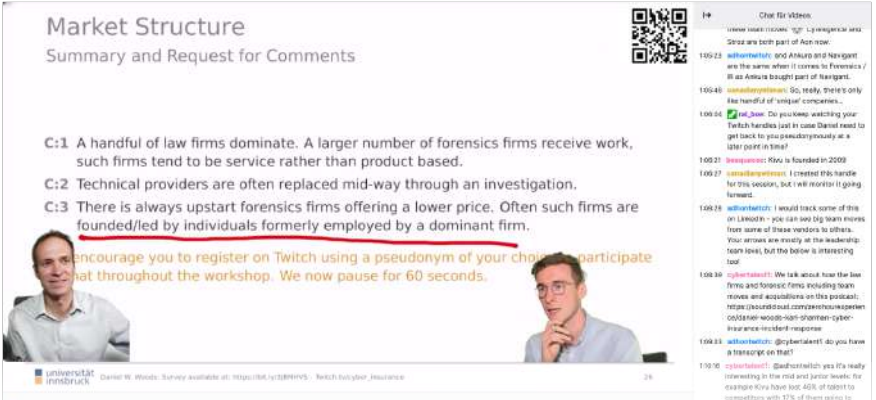
Qualitative Data (cont'd)



Upshot

- Insurance improved IR planning, especially for SMEs.
- Technical best practices collide with the litigation system.
- Attorneys are not adversaries:
  the net impact of lawyer-led IR is hard to evaluate.
- However, lawyer-led IR introduces barriers to how firms (and the wider community) learn from security failures.
- Potential solutions are future work — see paper for avenues.

Notes on Methodology



- Multi-stage, multi-method inspired by **grounded theory** (“everything is data”)
- ∼**70 expert interviews** covering the DFIR and breach attorney markets
- Twitch validation session with Chatham House rules during the pandemic

universität innsbruck

Thank You

Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys

Daniel W. Woods, Rainer Böhme, Josephine Wolff, Daniel Schwarcz

32nd USENIX Security Symposium · Anaheim, CA · 9 August 2023

Acknowledgments

First and foremost, we thank the participants for volunteering their time to advance the project. We are grateful to Lukas Walter and Kaylyn Stanek for providing superb research assistance and to Patrik Keller and Alexander Schlögl for moderating the validation workshop. The four WEIS reviewers, five USENIX reviewers, Shauhin Talesh, and Jono Spring all provided detailed and insightful comments on versions of this paper. We also received useful feedback from FIRST's Cyber Insurance Special Interest Group and Annual Meeting, the University of Cambridge's Security Seminar Series, the Privacy Law Scholars Conference, and the Cybersecurity Law and Policy Scholars Conference. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 894799.

Path Dependencies

Should insurers update procedures introduced to contain damage after data breaches?

	Major driver of cyber claims	
	Personal data breach early 2000s–2017	Ransomware since 2018
Litigation risk	high	low
Legal costs	high	low

Wolff, J. and Lehr, B. Roles for Policymakers in Emerging Cyber insurance Industry Partnerships. In *TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy*. 2018.

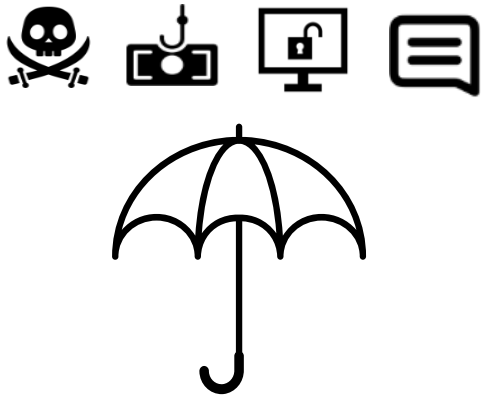
THE UNIVERSITY of EDINBURGH

universität innsbruck

KING'S College LONDON

"Why would money protect me from cyber bullying?"

A mixed-methods study of personal cyber insurance



Rachiyta Jain, Temima Hrle, Margherita Marinetti, Adam Jenkins, Rainer Böhme, and **Daniel W. Woods***

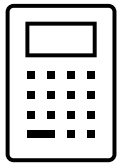
***Email:** daniel.woods@ed.ac.uk

Why is cyber insurance worth thinking about?

1. We cannot **protect users** from digital harm via technical measures alone

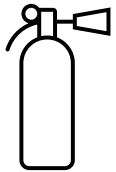
Why is cyber insurance worth thinking about?

1. We cannot **protect users** from digital harm via technical measures alone
2. Insurers have a unique perspective, creating many **innovative risk solutions**



invented actuarial science in ~1693

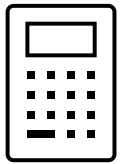
10 insurers create London's first fire brigade in 1833



policies often require customers to adopt safety measures

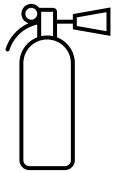
Why is cyber insurance worth thinking about?

1. We cannot **protect users** from digital harm via technical measures alone
2. Insurers have a unique perspective, creating many **innovative risk solutions**



invented actuarial science in ~1693

10 insurers create London's first fire brigade in 1833



policies often require customers to adopt safety measures

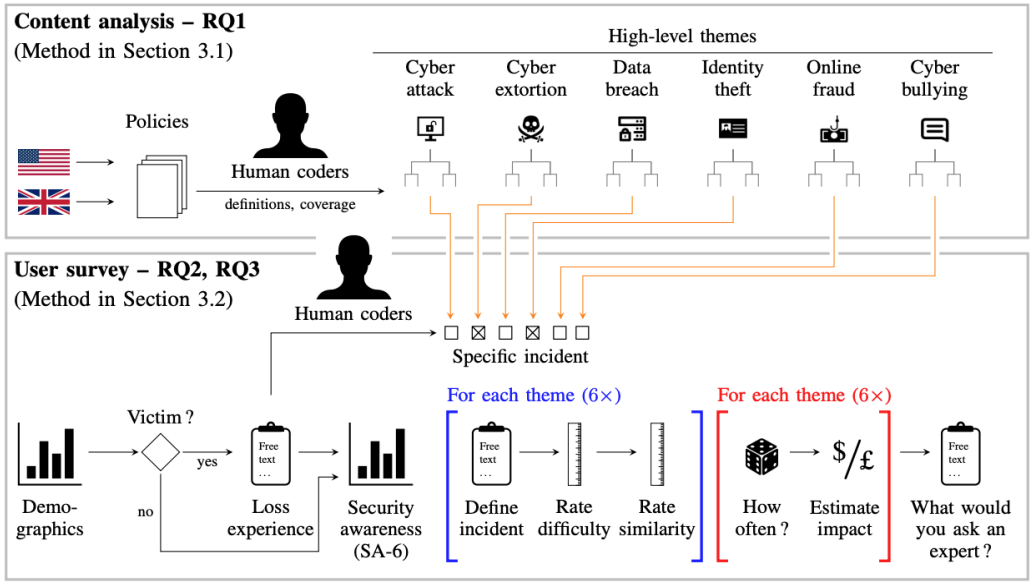
3. An industry that essentially sells promises **needs oversight**

A mixed methods study of personal cyber insurance

Stage 1

Analyzed insurance policies to identify which incidents are covered (RQ1)

- 2 qualified lawyers
- 21 from US and 3 from UK



A mixed methods study of personal cyber insurance

Stage 1

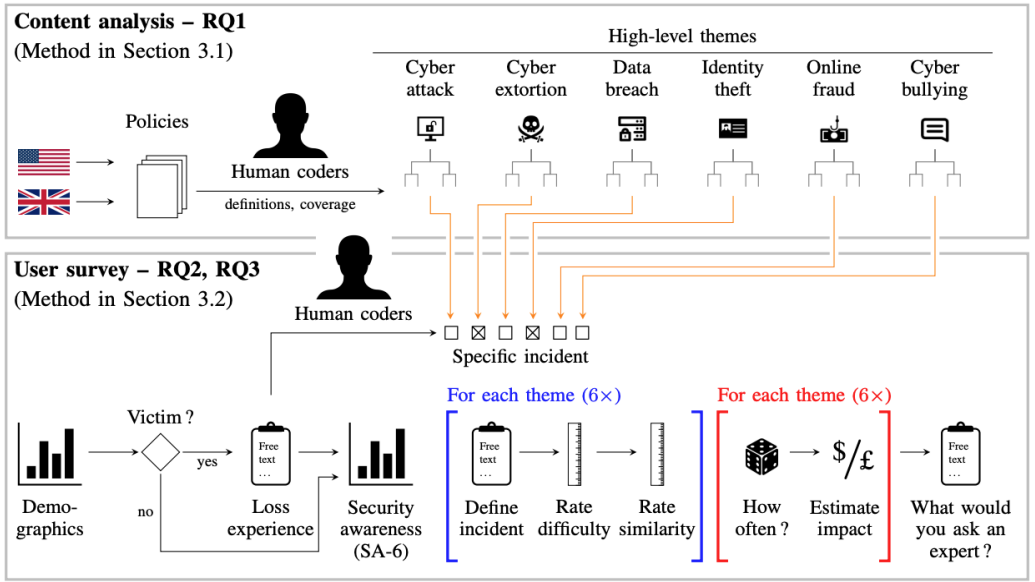
Analyzed insurance policies to identify which incidents are covered (RQ1)

- 2 qualified lawyers
- 21 from US and 3 from UK

Stage 2

User survey explored risk perceptions (RQ2) and coverage uncertainties (RQ3)

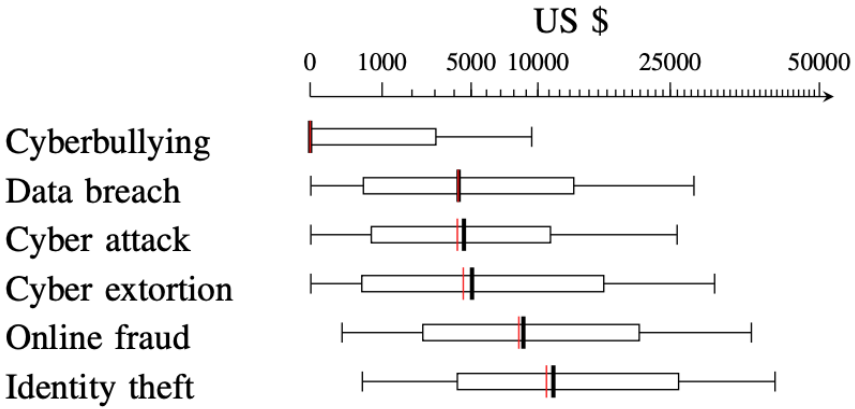
- recruited via Prolific
- even US/UK split (n = 585)



Cyber insurance covers a range of digital incidents (RQ1)

	Security & Privacy			Scams		Social media
						
Incident (Theme)	Cyber attack	Cyber extortion	Data breach	Identity theft	Online fraud	Cyber-bullying
Policies with coverage	100%	100%	63%	92%	100%	54%

Fraud and ID theft estimated to be costliest losses (RQ2)



→ See our paper for multi-variate analysis and frequency estimates

Exploring uncertainty about coverage (RQ3)

In your own words, please explain what is meant by "cyberbullying"?

How easy was the above description to write?

- Very easy
- Easy
- Neither easy nor challenging
- Challenging
- Very challenging

Insurance companies provide policies that describe what is and is not covered by the purchased insurance. The quote below is how one such policy defines the term "cyberbullying."

> Cyberbullying means two or more similar or related acts of harassment, intimidation, defamation, invasion of privacy, threats of violence or other similar acts. These related acts must be perpetrated, wholly or partially, using computers, cell phones, tablets or any similar device.

Does the definition match your understanding of the crime?

- Extremely similar
- Moderately similar
- Slightly similar
- Somewhat similar
- Not at all similar

Exploring uncertainty about coverage (RQ3)

In your own words, please explain what is meant by "cyberbullying"?

How easy was the above description to write?

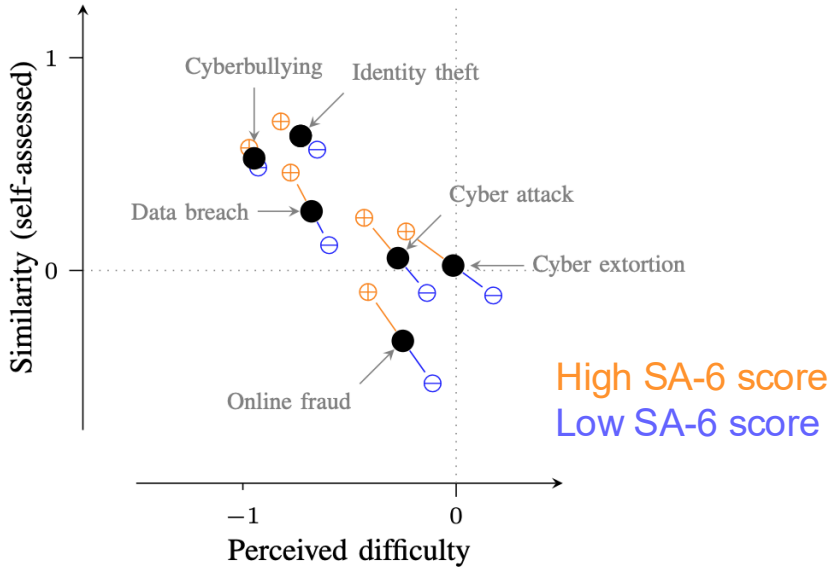
- Very easy
- Easy
- Neither easy nor challenging
- Challenging
- Very challenging

Insurance companies provide policies that describe what is and is not covered by the purchased insurance. The quote below is how one such policy defines the term "cyberbullying."

> Cyberbullying means two or more similar or related acts of harassment, intimidation, defamation, invasion of privacy, threats of violence or other similar acts. These related acts must be perpetrated, wholly or partially, using computers, cell phones, tablets or any similar device.

Does the definition match your understanding of the crime?

- Extremely similar
- Moderately similar
- Slightly similar
- Somewhat similar
- Not at all similar



Why would money protect me from cyber bullying?

Insurers don't indemnify emotional harm, they pay for crisis response:

- Lawyer fees to issue take down requests
- Counselling to address harm from incident
- Paying for child or elder care
- Cost of relocating home or school

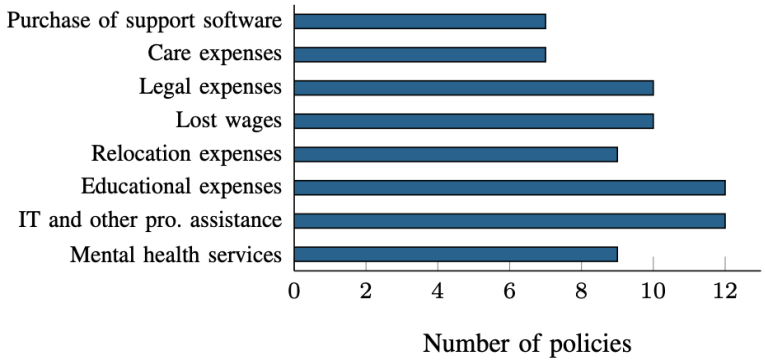


Figure 3. Specific costs covered related to Cyberbullying.

Why would money protect me from cyber bullying?

Insurers don't indemnify emotional harm, they pay for crisis response:

- Lawyer fees to issue take down requests
- Counselling to address harm from incident
- Paying for child or elder care
- Cost of relocating home or school

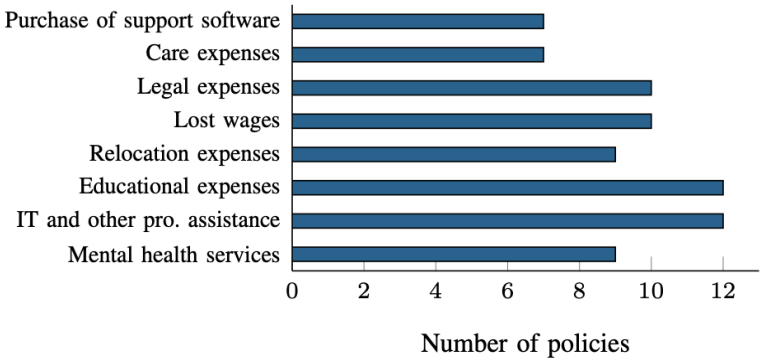


Figure 3. Specific costs covered related to Cyberbullying.

Insurers creating the digital fire service?

Insurers create London's first fire brigade in 1833

Open questions about personal cyber insurance

Market Evolution

- Will it become a mainstream product?
  - Just 1.6% of users have cyber coverage
  - 8.5% are aware of the product
- Specialist product or absorbed by home insurance
- Coverage innovations to meet emerging harms
- Is pricing adequate, competitive, and non-discriminatory?
- ...

Open questions about personal cyber insurance

Market Evolution

- Will it become a mainstream product?
  - Just 1.6% of users have cyber coverage
  - 8.5% are aware of the product
  - Specialist product vs absorbed by home insurance
- How will it evolve to address emerging harms?
- Regulatory questions
  - Is pricing adequate, competitive, and non-discriminatory?
  - Are claims reliably paid?
- …

Impact on Security, Privacy and Safety

- Will insurers incentivize risk reduction or incentivize complacency?
  - Risk assessment
  - Exclusions
  - Subsidized tools
  - …
- How will insurers organize crisis response?
- …

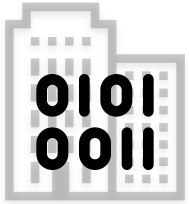
A History of Cyber Risk Transfer

Daniel W Woods and Josephine Wolff

Workshop on the Economics of Information Security
Dallas, USA
9th April 2024

Tufts UNIVERSITY
THE UNIVERSITY of EDINBURGH

Who pays after a cyber incident?



Tech Vendors

InfoSec Vendors

Firms

Capital Markets

Reinsurers

Insurers

Transfer to Tech Firms

Tech Vendors

InfoSec Vendors

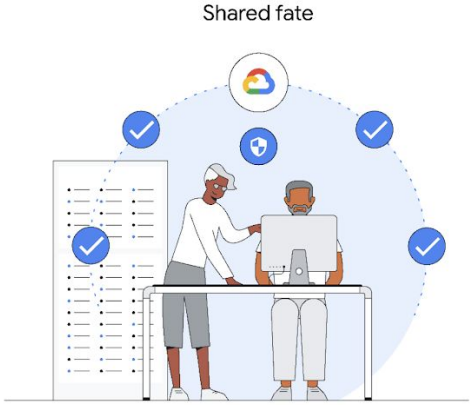
Firms

The cloud vendor story

— In 2022, cloud vendors announce risk transfer partnerships
    — Google argue shared responsibility is broken

— Solution to the principal-agent problem

Sounds delightful but…



The cloud vendor story

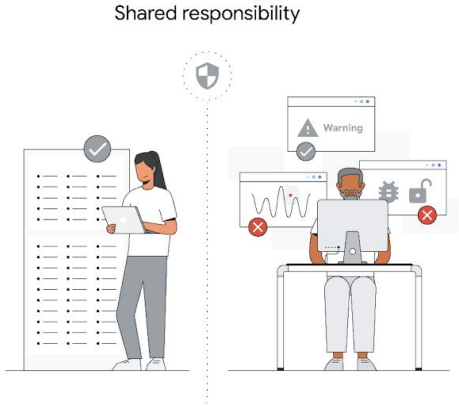
— In 2022, cloud vendors announce risk transfer partnerships
    — Google argue shared responsibility is broken

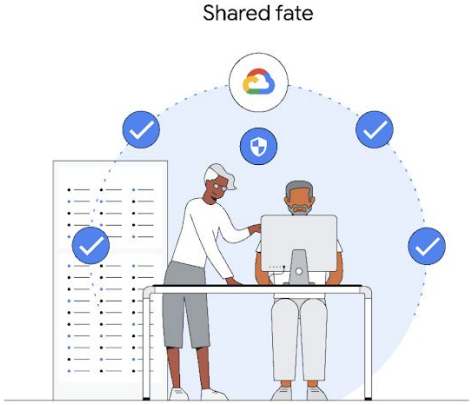
— Solution to the principal-agent problem

Sounds delightful but…

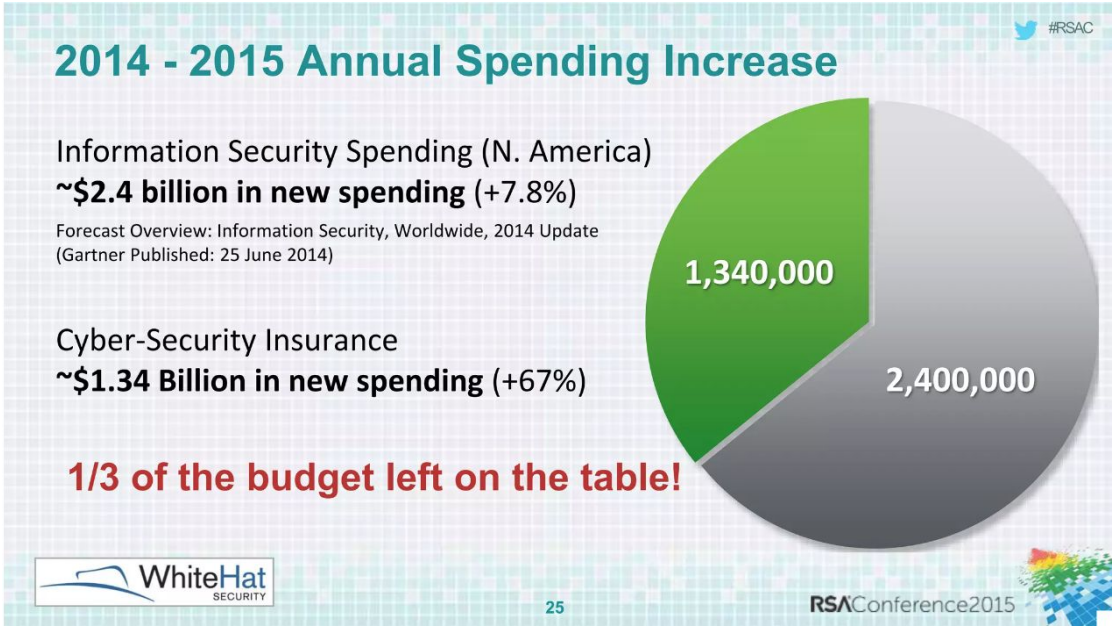
— Existing partnerships don’t transfer risk to vendors’ balance sheets

— Instead a cyber insurance referral
    — APIs provide insight into cloud security
    — supposedly allowing insurers to offer broader coverage





The infosec vendor story



Jeremiah Grossman announces at Black Hat 2014 that his Software Auditing firm **will pay up to $250k** in breach related costs to any customer that is hacked

Warranties proliferate from 2021 onwards

ID	Vendor	Type	Year	Limit*
W1a [9]	WhiteHatSecurity	Security audit	2014	$250k
W1b [9]	WhiteHatSecurity	Security audit	2015	$500k
W2 [57]	SentinelOne	End-point	2016	$1m
W3 [58]	MyDigitalShield	Network	2016	$50k
W4 [59]	Cymmetria	Deception	2016	$1m
W5 [62]	AsTech	Security audit	2017	$5m
W6 [63]	CrowdStrike	End-point	2018	$1m
W7 [64]	Cybereason	End-point	2020	$1m
W8 [65]	ThreatAdvice	MSP	2020	$250k
W9 [14]	Deep Instinct	End-point	2021	$3m
W10a [66]	Rubrik	Back-up	2021	$5m
W11 [67]	Arctic Wolf	MSP	2021	$1m
W12 [68]	Sophos	End-point	2022	$1m
W13 [69]	Kroll	End-point	2022	$1m
W14 [70]	Defendify	End-point	2022	$1m
W15 [71]	Dell	Back-up	2022	$10m
W10b [72]	Rubrik	Back-up	2023	$10m
W16 [73]	Veeam	Back-up	2023	$5m
W17 [74]	Barracuda	XDR	2023	?
W18 [75]	PCH Technologies	MSP	2023	?
W19 [76]	Adlumin	End-point	2023	$500k
W20 [77]	CloudCover	Network (Cloud)	2023	$1m
W21 [78]	LionGard	MSP	2023	?

— Theoretical solution to the principal-agent problem

— In practice, coverage only when solution is perfectly configured and monitored

— Vendors actively endorse a patchwork of warranties across “endpoint security, firewalls, email security and web security”

Daniel W. Woods and Tyler Moore. "Cyber warranties: market fix or marketing trick?." *Communications of the ACM* 63, no. 4 (2020): 104-107.

History of Cyber (Re)Insurance

Four themes

1. **Coverage**
2. Solvency
3. Information Collection
4. Incentives

Capital Markets

Reinsurers

Firms

Insurers

How to decide whether and how much to pay out?

Parametric

- Whether to pay based on external trigger
- How much to pay is predetermined
- Cloud outage the only successful product

Indemnity

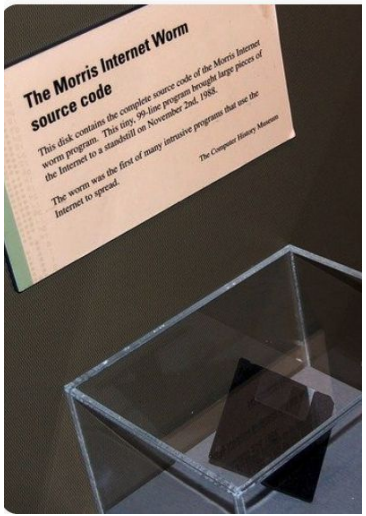
- Whether to pay based on legal definition
- How much to pay based on loss in a specific incident
- Vast vast majority of the $15bn cyber (re)insurance market

Cyber Incident means any actual or reasonably suspected:

A. **Computer Malicious Act, Human Error, Programming Error**, failure of **Network Security**, or **Unauthorised Use or Access** or any other threat or action against a **Covered Computer System**, including those threats or actions done in the commission of a **Cyber Extortion Event**;

B. **Privacy and Network Security Wrongful Act**; or

Cyber~~security~~ insurance



Security failure ✔

September 14, 1996

New York's Panix Service Is Crippled by Hacker Attack

By ROBERT E. CALEM

Denial of service ✔

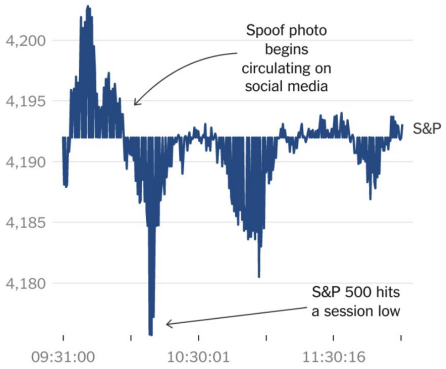
December 8, 2023, 9:30 AM GMT

Court Challenges to Web Tracking Tools Raise Crucial Questions

Luke Sosnicki
Thompson Coburn

Web tracking ✔

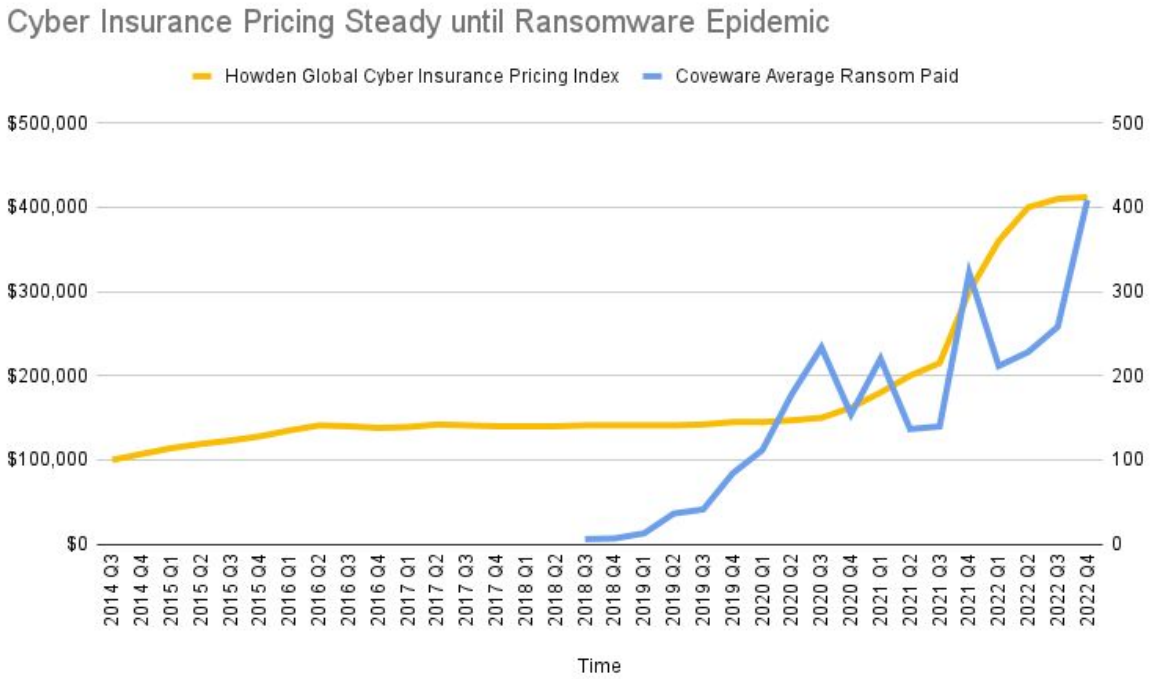
Publishing liability ✔



Source: Sentieo/AlphaSense • By The New York Times

Media manipulation❓

Indemnity insurance leads to a ransomware surprise



The History of Cyber (Re)Insurance

4 themes:

1. Coverage
2. Solvency
3. **Information Collection**
4. Incentives

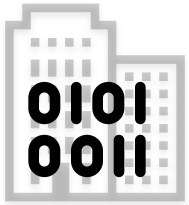
Capital Markets

Reinsurers

Firms

Insurers

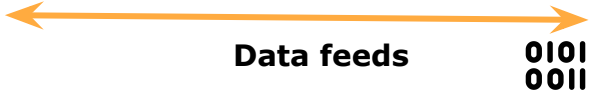
What information is collected?

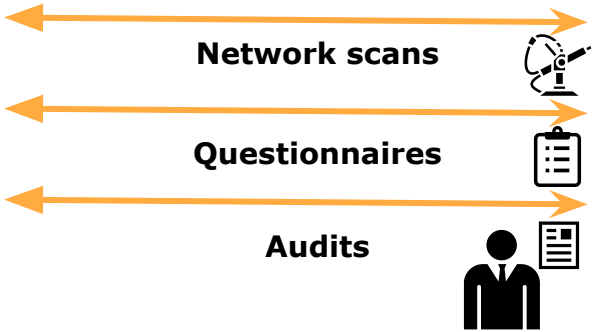


Tech Vendor

InfoSec Vendor

Firm



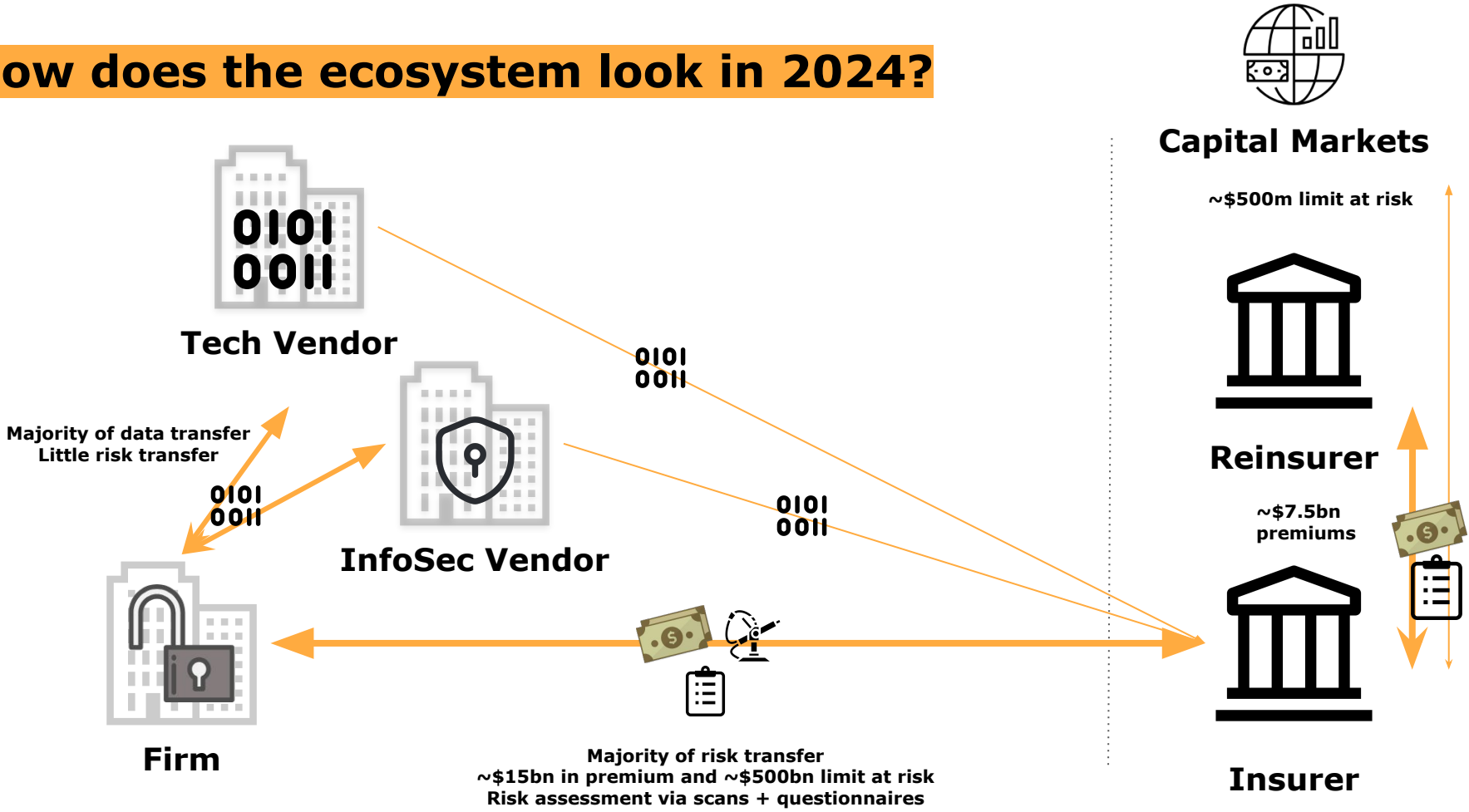


Capital Markets

Reinsurer

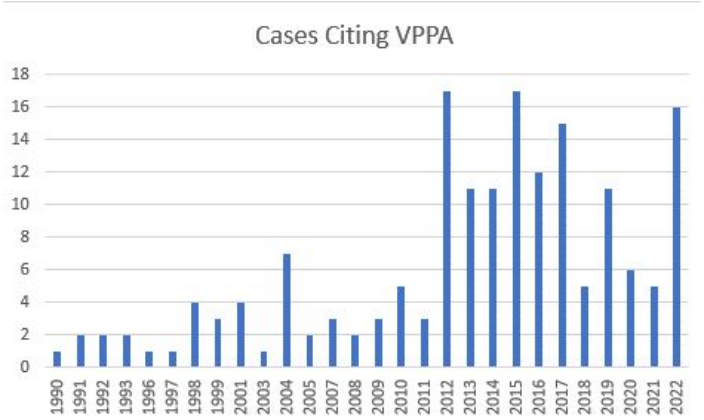
Insurer

How does the ecosystem look in 2024?

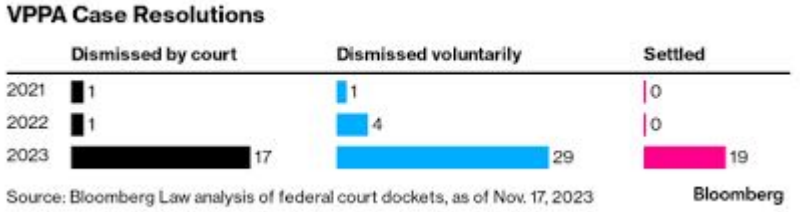


Indemnity insurance leads to a web privacy surprise?

Video Privacy Protection Act (1988)



Source: Husch Blackwell



Broad indemnity triggers in everything

Reinsurance

- Mostly structured as proportional co-pay
  - aka quota share
- This means reinsurance inherits the indemnity triggers

Limits insurers' upside and reinsurer's downside relative to sophisticated structures

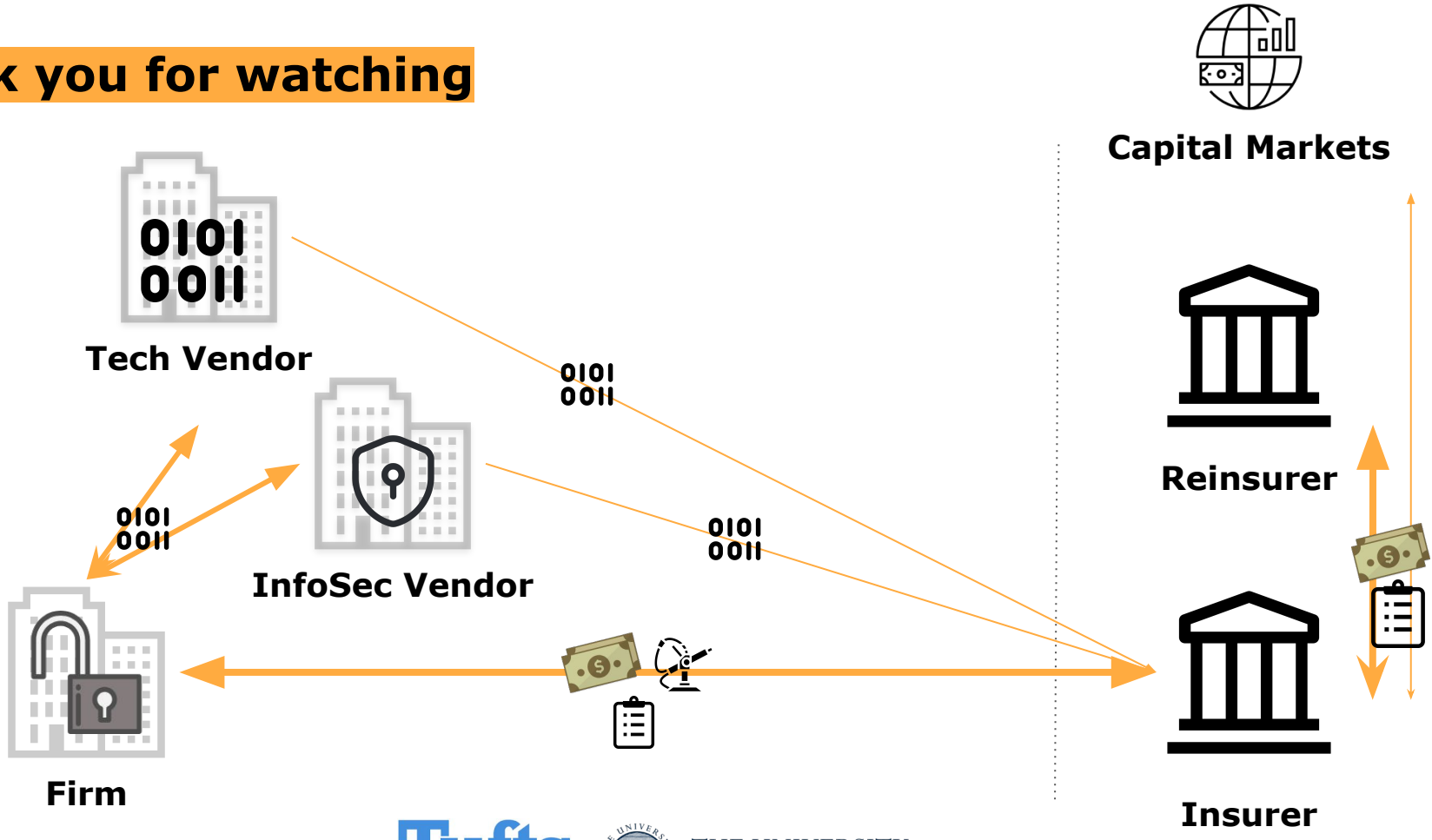
- Half of all premiums flow to reinsurers
- Anecdotal reports of high market concentration within cyber reinsurance

Capital Markets

Cedant	Trigger	Type	Size	Date
Beazley	Indemnity	Private Cat Bond	$45m	Jan 2023
HannoverRe	Indemnity	Quota share retrocession	$100m	Jan 2023
Beazley	Indemnity	Private Cat Bond	$20m	May 2023
Beazley	Indemnity	Private Cat Bond	$16.5m	Sep 2023
AXIS Capital	Indemnity	Cat Bond (144A)	$75m	Nov 2023
Beazley	Indemnity	Cat Bond (144A)	$130m	Dec 2023
SwissRe	Indemnity*	Cat Bond (144A)	$50m	Dec 2023
Chubb	Indemnity	Cat Bond (144A)	$100m	Dec 2023

- Reinsurance capacity crunch pushes insurers to tap investors
- No parametrics triggers

Thank you for watching



Tufts UNIVERSITY

THE UNIVERSITY of EDINBURGH