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

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security
Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

SECURITY ECONOMICS AND THE INTERNAL MARKET

Ross Anderson
Rainer Böhme
Richard Clayton
Tyler Moore

THE CYBER PROJECT

Learning from Cyber Incidents

Adapting Aviation Safety Models to Cybersecurity

Report on the Interdisciplinary Workshop on the Development of a National Capacity for the Investigation of Cyber Incidents

Rob Knake
Adam Shostack
Tarah Wheeler

HARVARD Kennedy School
BELFER CENTER for Science and International Affairs

PAPER
NOVEMBER 2021

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

NIST 800-61, p. 38

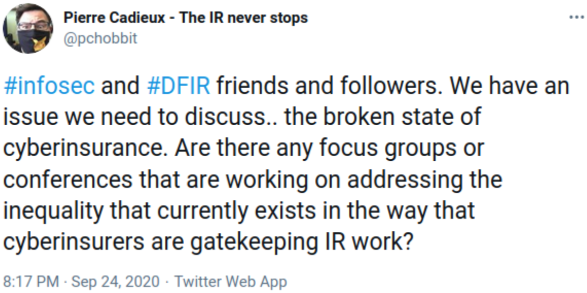
“Insurers accumulate data […] which they mine to improve risk assessment and suggest best practice mitigation strategies to their clients.”

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 ?



Pierre Cadieux - The IR never stops
@pchobbit

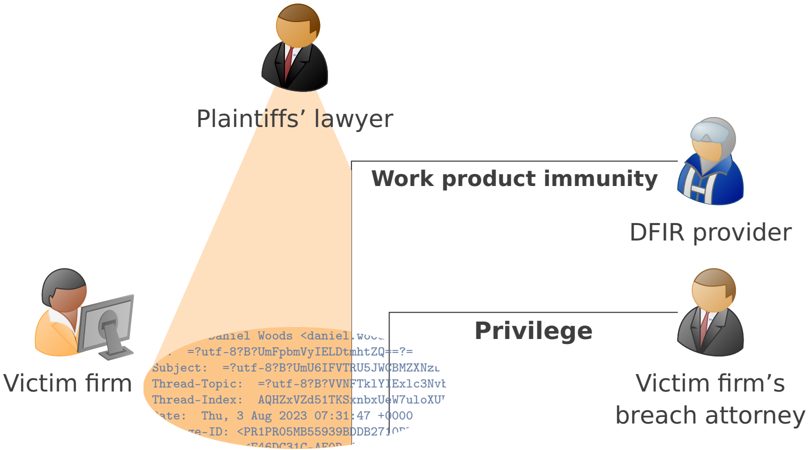
#infosec and #DFIR friends and followers. We have an issue we need to discuss.. the broken state of cyberinsurance. Are there any focus groups or conferences that are working on addressing the inequality that currently exists in the way that cyberinsurers are gatekeeping IR work?

8:17 PM · Sep 24, 2020 · Twitter Web App

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

DFIR: Digital Forensics / Incident Response

Discovery and Privilege



Plaintiffs’ lawyer

Work product immunity

DFIR provider

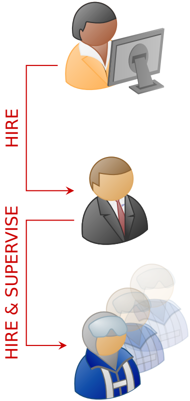
Privilege

Victim firm

Victim firm’s
breach attorney

```
  Daniel Woods <daniel.woo
:  =?utf-8?B?UmFpbmVyIELDtmhtZQ==?=
Subject:  =?utf-8?B?UmU6IFVTRU5JWCBMZXNz
Thread-Topic:  =?utf-8?B?VVNFTklYIExlc3Nv
Thread-Index:  AQHZxVZd51TKSxnbxUeW7uloXU
ate:  Thu, 3 Aug 2023 07:31:47 +0000
  ge-ID: <PR1PR05MB55939BDDB2710
       <E46DC31C-AF0D
```

Consequences



Reasons to keep cybersecurity efforts confidential

- Limit litigation risk
- Negative publicity
- Regulatory actions

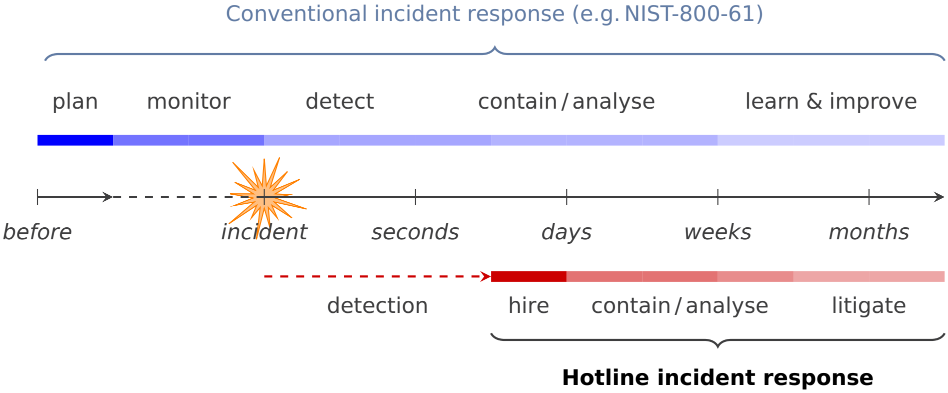
Measures taken

- 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

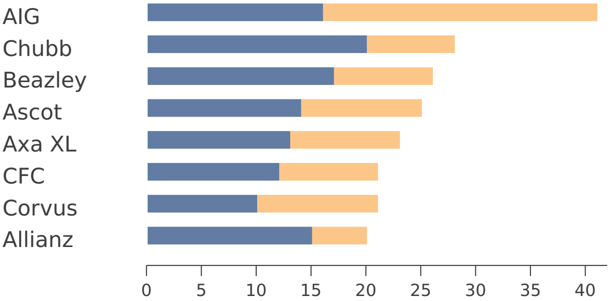


Woods, D. W. and Böhme, R. Incident Response as a Lawyers' Service. *IEEE Security & Privacy*, **20**, 2 (2022), 68–74.

Role of Insurers

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

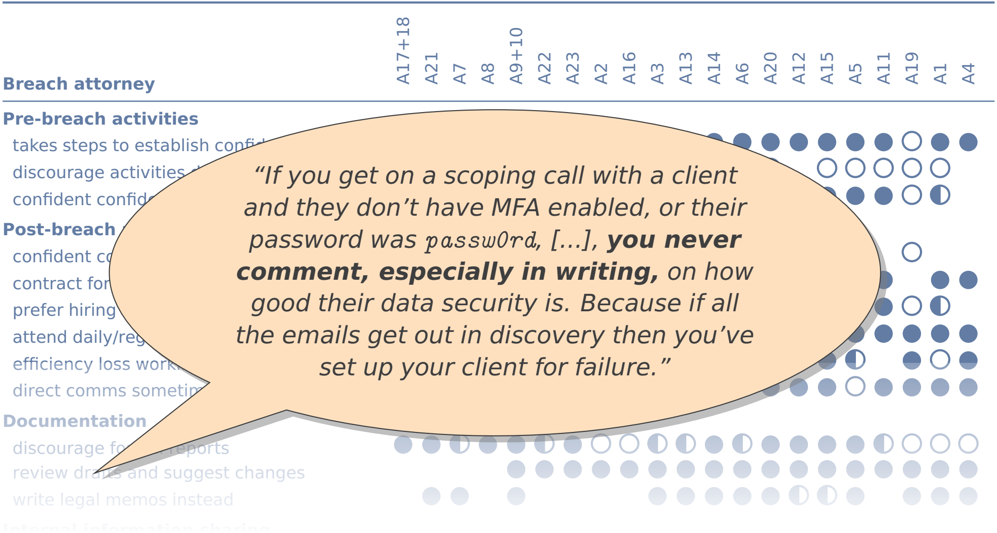
Number of 🟦 DFIR and 🟧 legal providers on insurers’ panels



→ 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



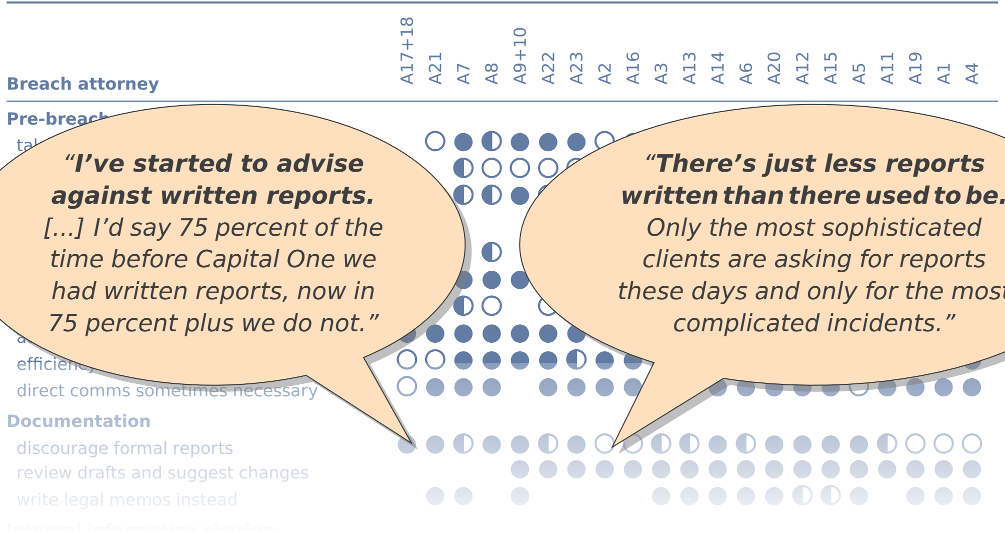
“If you get on a scoping call with a client and they don’t have MFA enabled, or their password was `passw0rd`*, […],* ***you never comment, especially in writing,*** *on how good their data security is. Because if all the emails get out in discovery then you’ve set up your client for failure.”*

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)

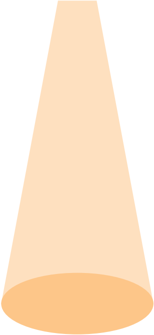


“I’ve started to advise against written reports. *[…] I’d say 75 percent of the time before Capital One we had written reports, now in 75 percent plus we do not.”*

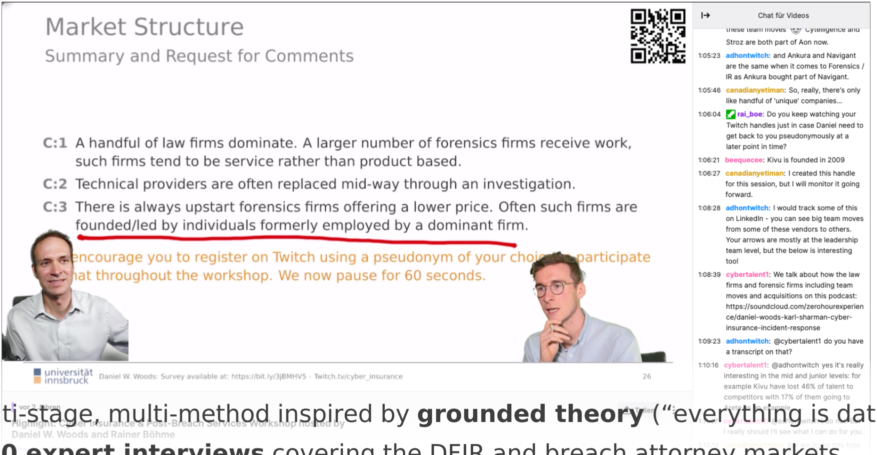
“There’s just less reports written than there used to be. *Only the most sophisticated clients are asking for reports these days and only for the most complicated incidents.”*

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



Market Structure

Summary and Request for Comments

C:1 A handful of law firms dominate. A larger number of forensics firms receive work, such firms tend to be service rather than product based.

C:2 Technical providers are often replaced mid-way through an investigation.

C:3 There is always upstart forensics firms offering a lower price. Often such firms are founded/led by individuals formerly employed by a dominant firm.

encourage you to register on Twitch using a pseudonym of your choi participate
hat throughout the workshop. We now pause for 60 seconds.

universität innsbruck Daniel W. Woods: Survey available at: https://bit.ly/3jBMHV5 · Twitch.tv/cyber_insurance 26

vor 2 Jahren

Highlight: Cyber Insurance & Post-Breach Services Workshop hosted by Daniel W. Woods and Rainer Böhme

Chat für Videos

these team moves 🙂 Cytelligence and Stroz are both part of Aon now.

1:05:23 adhontwitch: and Ankura and Navigant are the same when it comes to Forensics / IR as Ankura bought part of Navigant.

1:05:46 canadianyetiman: So, really, there's only like handful of 'unique' companies...

1:06:04 rai_boe: Do you keep watching your Twitch handles just in case Daniel need to get back to you pseudonymously at a later point in time?

1:06:21 beequecee: Kivu is founded in 2009

1:06:27 canadianyetiman: I created this handle for this session, but I will monitor it going forward.

1:08:28 adhontwitch: I would track some of this on LinkedIn - you can see big team moves from some of these vendors to others. Your arrows are mostly at the leadership team level, but the below is interesting too!

1:08:39 cybertalent1: We talk about how the law firms and forensic firms including team moves and acquisitions on this podcast: https://soundcloud.com/zerohourexperience/daniel-woods-karl-sharman-cyber-insurance-incident-response

1:09:23 adhontwitch: @cybertalent1 do you have a transcript on that?

1:10:16 cybertalent1: @adhontwitch yes it's really interesting in the mid and junior levels: for example Kivu have lost 46% of talent to competitors with 17% of them going to Arete as an example

1:11:07 cybertalent1: @adhontwitch I do not! But I really should I'll see what I can do for you.

1:13:14 canadianyetiman: Are we doing this type

- 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

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.