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

Daniel W. Woods, *University of Edinburgh;* Rainer Böhme, *University of Innsbruck;*
Josephine Wolff, *Tufts University;* Daniel Schwarcz, *University of Minnesota*

https://www.usenix.org/conference/usenixsecurity23/presentation/woods

This paper is included in the Proceedings of the
32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Open access to the Proceedings of the
32nd USENIX Security Symposium
is sponsored by USENIX.

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

Daniel W. Woods
University of Edinburgh

Rainer Böhme
University of Innsbruck

Josephine Wolff
Tufts University

Daniel Schwarcz
University of Minnesota

Abstract

Incident Response (IR) allows victim firms to detect, contain, and recover from security incidents. It should also help the wider community avoid similar attacks in the future. In pursuit of these goals, technical practitioners are increasingly influenced by stakeholders like cyber insurers and lawyers. This paper explores these impacts via a multi-stage, mixed methods research design that involved 69 expert interviews, data on commercial relationships, and an online validation workshop. The first stage of our study established 11 stylized facts that describe how cyber insurance sends work to a small numbers of IR firms, drives down the fee paid, and appoints lawyers to direct technical investigators. The second stage showed that lawyers when directing incident response often: introduce legalistic contractual and communication steps that slow-down incident response; advise IR practitioners not to write down remediation steps or to produce formal reports; and restrict access to any documents produced.

1 Introduction

The Computer Security Incident Handling Guide standardized in NIST-800-61 states that "learning and improving" is one of the most important but most frequently omitted parts of Incident Response (IR) [1, p. 38]. It recommends asking questions like: *What corrective actions can prevent similar incidents in the future?*; and *What additional tools or resources are needed to detect, analyze, and mitigate future incidents?* The answers to these questions should then be shared with the wider community [1, Sec. 4].

The academic literature suggests the security community fails at implementing these best practices [2]. Studies of firms have found "root causes are not alway identified" [3]. There is a "lack of incident information dissemination to all interested or involved parties" both within the firm [4, p. 651] and with external stakeholders [5–7]. Even when information is shared, it is often of questionable value [8–10]. A workshop convening participants across industry and academia reported that "the ultimate conclusion was that the IT industry does not have strong processes for extracting lessons learned and publishing them when incidents occur" [11].

This motivates understanding why real-world cyber incident response falls short of the normative guidance provided by NIST-800-61 [1]. For other security failures, misaligned economic incentives provide a better explanation than the underlying technical challenge, which is often solvable [12, 13]. This motivates empirical research into the economic structure surrounding incident response. Our study examines these economic incentives, as well as non-economic institutional factors, in the specific setting of cyber insurance.

Cyber insurance influences IR by paying for a range of services including forensic investigations, legal advice, and public relations [14, 15]. This matters because at least four million firms in the US are now cyber insurance policyholders as of 2020, double the number four years prior [16]. However, existing literature has not considered how insurers influence how IR is practiced. A 2020 cyber insurance SoK [17] highlights open research questions like: *how does insurance influence the choice of IR firm and the quality of service?*; and *how are lessons extracted from incidents and shared with relevant stakeholders?* Our study addresses these questions.

Contribution Stage 1 of our study found that cyber insurance pushes policyholders to work with a small number of in-network IR firms, drives down fees paid to those firms, and appoints breach attorneys to direct investigations and monitor quality. Insurers use market power to negotiate and organize affordable IR services thereby increasing access, possibly at the expense of quality. However, these economic considerations could not fully explain the centrality of lawyers to IR. This motivated Stage 2 exploring how breach attorneys influence technical investigations.

While breach attorneys' strategies in managing IR varied, a majority of participants discourage investigators from producing formal reports or putting remediation steps into writing. When reports are written, some lawyers review and suggest changes that reduce culpability for the victim firm, such as by

obfuscating root causes and corrective actions that could have prevented the incident (notably, NIST-800-61 recommends answering this question [1]). Lawyers typically advise against sharing written findings with insurers or regulators, not to mention the wider community. We argue that the attorneys' advice leads to *lessons lost* rather than *lessons learned*, all other things being equal.

Section 2 introduces concepts related to cyber insurance, IR and the law. Section 3 describes our research design. Sections 4 and 5 report results about cyber insurance and breach attorneys, respectively. Section 6 discusses potential technical, business, and policy solutions. Section 7 reflects on limitations. Section 8 concludes the paper.

2 Background

This section provides background on why insurers pay for technical and legal IR services. For a rough timeline, standalone cyber insurance has existed since around 2000 but only began growing rapidly in 2016 [16]. Technical incident response has existed since the 1980s [18]. Dating when breach attorneys emerged is hard, though cybersecurity regulation [19] and lawsuits [20] in the 2000s played a role.

Cyber Insurance Firms can purchase insurance against costs including data breach fines and damages, lost income resulting from network disruptions, ransomware payments, and—crucially for this study—post-breach services [21]. IR services reduce losses with benefit to both the policyholder and the insurer [22]. For example, appointing a breach attorney to advise on incident response may reduce the size of data breach damages or regulatory fines, which the insurer would otherwise have to pay.

Researchers argue that cyber insurance has had little effect on preventative measures [21, 23–25]. The literature is more positive about the social benefit of IR services associated with cyber insurance [15, 23]. However, it is unclear how insurers monitor IR quality or how they extract lessons from insurance claims [17]. Answering these questions requires turning to technical IR.

Technical Incident Response Digital Forensics and Incident Response (DFIR) is a multi-faceted technical process that includes: *(i)* preparing for; *(ii)* detecting; *(iii)* containing; *(iv)* recovering from; and *(v)* sharing lessons about security incidents [1]. Each task *(i–v)* touches on broad research topics that we cannot hope to survey. Detection is a standalone security topic in computer security [26–30]. Forensics techniques are tailored to specific systems like cloud environments [31], databases [32], multimedia data [33], digital cameras [34], and OS logs [35].

Regardless of how the initial steps *(i–iv)* are carried out, the final step creates a dilemma for victims of security incidents. Although technical best-practice recommends that investigators identify root-causes and measures that could have prevented the incident [1, Sec. 4.3.1], doing so may have negative consequences for the victim firm. For example, a root-cause like not updating software may be used in litigation against the firm who suffered an incident [36]. As a result, victims want to protect the confidentiality of digital forensics investigations.

Confidentiality Protections The naive solution is to prevent the report being shared outside the firm. However, litigants in the US legal system can use a process called *discovery* to compel entities to make documents available, such as forensic reports or any written communications with the investigator. To avoid this, the breached firm's attorneys sometimes claim DFIR reports are covered by *confidentiality protections*. We use this term throughout to describe attorney-client privilege and work-product immunity. Attorney-client privilege protects communications between lawyers and third-party consultants, such as cybersecurity firms, that attorneys rely upon to provide legal advice to a client. Work product immunity protects materials that attorneys or their consultants prepare in reasonable anticipation of litigation or for trial.

There is a complex body of case law describing under what circumstances documents and communications are covered by confidentiality protections [37–39]. Law firms argue that confidentiality protections extend to digital forensics investigations that are directed by an attorney [40]. Some legal experts have suggested that lawyers' efforts to maximize the chances that courts will accept such confidentiality protections may interfere with technical practitioners [37, 38]. This has not been empirically studied. In doing so, our study addresses a call for research into how lawyers influence cybersecurity [41].

3 Methods

Stage 1 of our study had the exploratory research goal of describing the cyber insurance ecosystem. Rather than focus on the individual perspectives of stakeholders, we tried to uncover the structure of economic power. We adopted the convention of stylized facts from economics—statements that are essentially true but fail to explain certain particulars [43]. This allowed us to sketch broad economic structures without claiming perfect fidelity. To evaluate validity, we invited participants to falsify our stylized facts in an online workshop.

A number of puzzling findings related to breach attorneys could not be explained with economics. This motivated Stage 2 focusing on the advice offered by attorneys, in which two academics with law and policy expertise joined the project. As a result, our research design shifted towards the goal of describing the specifics of what lawyers advise and why. This was not well suited to deriving stylized facts because each lawyer had their own particular approach. The analysis in Stage 2 tried to capture these particularities. To account for the lawyers' preferences, we validated these findings by sharing written summaries instead of a workshop.

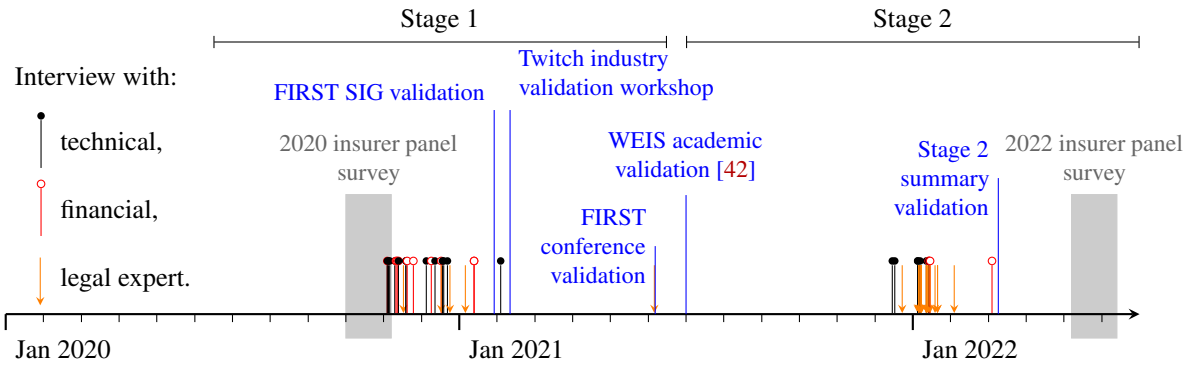

Figure 1: Timeline of the research project with alternating phases of fieldwork and validation exercises.

	Stage 1	Stage 2	Total
IR	13	7	20
Insurers	10	6	16
Lawyers	5	23	28
Misc	1	4	5
Total	29	40	69

Table 1: Our interview participants included technical IR practitioners, insurers (underwriters, claims managers, brokers), breach attorneys, and miscellaneous roles (recruiters, ISAC leaders and regulators).

Figure 1 summarizes our multi-stage, mixed methods exploratory study. The remainder of this section describes how we collected data across its two stages.

Recruitment Table 1 describes our interview composition across both stages. For Stage 1, recruitment consisted of a mixture of convenience sampling, an advert on a professional networking site, snowball sampling and cold-emails to employees at the IR firms we had not spoken to yet. For Stage 2, we also cold-emailed leaders of the data security and privacy practice groups at a list of the biggest law firms in the US. This helped us to understand whether legal advice generalized to law firms outside the cyber insurance ecosystem. We did not offer financial rewards for participation, and stopped recruiting when new interviews revealed little information.

We interviewed employees from 70% of the law firms and 65% of the IR firms identified as having more than two relationships with cyber insurers. To map these partnerships, we used lists of cyber insurance carriers as a seed sample[1]. We then searched each insurer's website for documents describing the cyber insurance products. In October 2020, we captured the business relationships of 24 cyber insurers advertising 480 partner IR firms of which 151 were unique. We replicated this analysis in April 2022.

Interview Process The interview guidelines (see Section A.1 and Section A.2) were drafted after pre-study discussions with a range of stakeholders, and after the case law analysis for Stage 2. The scripts were adapted for each profession (e.g. IR, insurer, legal and so on). Interviews were conducted by video call, lasting 30–60 minutes. We recorded and transcribed the audio if the participant provided written consent, and otherwise relied on a dedicated scribe.

Analysis For Stage 1, we followed an iterative process of: asking open questions; writing up a set of stylized facts that explained previous reports; and, asking follow-up questions to clarify whether these facts apply to other participants. We aimed for the highest level of generality that explained most of the participants' reports. For example, all insurers draft a list of approved IR providers but we failed to build a general account of the process by which firms were added to panels, which varied across insurers. Stage 1 proposed 12 stylized facts, of which 1 was rejected.

For Stage 2, the interviews were inductively coded to identify specific steps taken to protect confidentiality. This resulted in a list of concrete strategies like "share DFIR report with regulators". We then deductively read through each transcript to identify quotes that supported, contradicted or provided nuance about the concrete strategy. It was left blank if the participant's beliefs could not be confidently identified. The other researchers then reviewed these classifications. We present those strategies about which many participants expressed a belief.

Validation Our validity criterion was whether practitioners believed our descriptions of the ecosystem were accurate. The most structured validation channel was an online validation workshop, in which we presented the stylized facts and asked the audience to comment in the chat. The platform reports 61 unique viewers, 17 unique chatters, and 96 messages in chat.

[1] For example: https://www.reinsurancene.ws/top-20-us-cyber-insurance-companies/

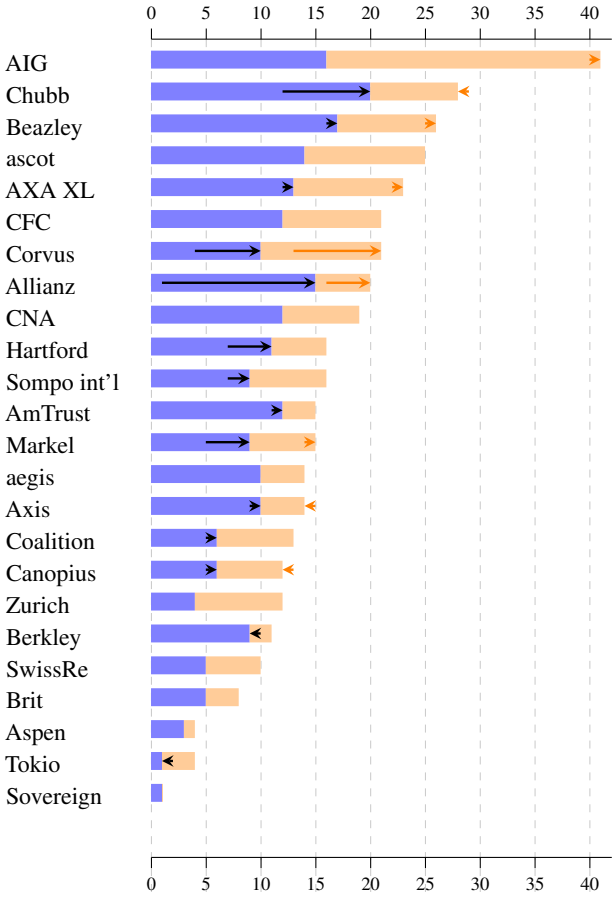

Figure 2: Number of IR (blue) and legal (orange) providers on insurers' panels in 2022 based on desk research. The arrows represent changes from 2020.

The event was advertised on social media, allowing anyone to join. We believe the loss of control over who participates is compensated for by the open-science benefits. For example, the workshop recording provides a verifiable research artifact[2].

We did not conduct a validation workshop for Stage 2 because the lawyers indicated they would not join. Instead we sent a written summary of our findings and received feedback by email, which was better suited to their professional norms. To obtain further feedback, we presented Stage 1 results at the main DFIR practitioner conference (FIRST) and two specialist events. We presented the results from Stage 2 at two privacy and cybersecurity law events.

Ethics We obtained ethical approval for the interviews from the first author's institution, which included reviewing the study's information sheet, consent form, and interview scripts. To avoid damaging the participants' reputations, we anonymized names, job roles and firms. Workshop participants could choose a pseudonym and were aware the session was broadcast and would be later uploaded.

[2] https://www.twitch.tv/videos/908724413

4 How Insurance Shapes IR

We proposed 12 stylized facts and rejected 1, all can be found in the Appendix. These facts describe how insurers: influence which IR firms are hired (*S:1–3*); negotiate prices and contracts (*N:1–3*); monitor quality (*M:1–3*); and impact market structure (*C:1–3*).

Selection Upon detecting a cyber incident, policyholders are asked to call the insurer's *incident hotline* (*S:1*). The operator—typically a law firm (*S:3*)—advises the insured on which IR firms to hire. IR firms are selected from the insurer's *panel*, a list of pre-approved firms whose fees the insurer will pay (*S:1*). Figure 2 shows the composition of insurers' panels. All insurers maintained or expanded the number of IR firms between 2020 and 2022, while some reduced the number of law firms.

Firms commit to contractual terms in order to join the panel (*S:2*), which can be an involved process. One IR firm reported "exchanging documents for over a year" with an insurer before abandoning the process. Two IR firms reported that after becoming established in the insurance ecosystem, insurers started offering panel spots to them.

Although most policyholders follow the operator's recommendations about which firms to hire (*S:3*), insurers allow insureds to express preferences and even to hire off-panel firms. Off-panel firms must be added to the insurance policy at purchase time. The policyholder may have to pay additional costs if the off-panel firm is more expensive, which is often the case because insurers hold a strong negotiating position.

Negotiation To be added to an insurer's panel, IR firms typically commit to prices ahead of time (*N:1*), often below market rates. A discount of 30% is typical in our sample. Operators and IR firms work together sufficiently often that contract templates can be used. The contractual details to be negotiated in the aftermath of an incident are specifics like the number of sites/machines to be investigated (*N:1*).

In many cases, the IR firm is not hired by the victim firm but instead by a breach attorney on behalf of the victim (*N:2*), predominantly to protect the confidentiality of forensics findings. Legal risk also led IR firms to sub-contract ransomware tasks (*N:2*). One participant explained a regular arrangement in which an IR firm investigated ransomware incidents, outsourced the negotiation to another firm, and a third firm facilitated the payment.

Some IR firms earn extra income by up-selling mitigation measures (*N:3*). For example, many IR firms use end-point detection products to investigate incidents. Victim firms often pay out-of-pocket to keep the detection product long term. Some IR firms negotiated an arrangement with the vendor in which they received a sales fee when victims bought a subscription. We now turn to how contracts are monitored.

Monitoring Insurers tend not to micro-monitor each claim. IR quality is predominantly monitored by lawyers on a day-to-

Firm	Number of listings	
	2020	2022
Mullen Coughlin	19	20
BakerHostetler	14	15
McDonald Hopkins	12	14
Lewis Brisbois	12	13
Wilson Elser	8	7
Norton Rose Fulbright	6	6
Davis Wright Tremaine	5	5
Clark Hill	5	5
Marshall Dennehey	3	3
Holland & Knight	3	3
Fisher Broyles	2	3
Troutman Pepper	2	3

Table 2: Law firms who appeared on more than 2 cyber insurance panels in our desk research.

Firm	Number of listings	
	2020	2022
Crypsis (now Unit42)	18	15
Kivu	17	16
Charles River	16	17
Ankura	15	16
Kroll	14	17
Stroz Friedberg	13	16
CrowdStrike	10	13
FireEye/Mandiant	10	10
CyberScout	6	5
Arete	6	11
Verizon	5	6
Tracepoint	5	11
Cytelligence	3	3
Navigant	3	0
KPMG	3	6
BlueVoyant	3	4
RSM	3	4
Tetra Defense	2	3
Speartip	1	3

Table 3: Technical IR firms who appeared on more than 2 cyber insurance panels in our desk research.

day basis. Meanwhile, insurers rely on verbal reports (*M:2*). Both insurers and attorneys (in their role as operating the breach hotline) select IR firms based on past performance across multiple claims (*M:1*). IR firms who regularly won work from insurers struggled to answer the question *"What kind of disputes arise between insurer and service provider?"* The majority of disputes resulted from insureds hiring off-panel firms (*M:1*).

Lawyers also influenced how investigations are structured (*M:3*). For example, one IR practitioner reported that forensics firms share spreadsheets outlining how law firms and even individual lawyers want investigations to be presented. These two findings, along with *N:2*, revealed the centrality of breach attorneys, motivating Stage 2 of our study.

Market Structure The role of lawyers is particularly important given the concentrations of power within the ecosystem. A handful of IR firms hold the majority of panel listings (*C:1*). This market concentration is stronger for law firms than DFIR firms (compare Tables 2 and 3). Product-based IR firms who build/operate security products with relevance to the investigation were less common (*C:1*) than service-based IR firms.

Service-based firms are essentially consultancies with little intellectual property (relative to IR firms who also build security products). This helps explain why "there are always upstart forensic firms offering a lower price" (*C:3*). Often these firms are founded or run by employees of formerly dominant firms. Figure 5 (in the Appendix) identifies many such moves, whereas just one law firm was formed like this. This impacts the ability for technical IR firms to retain staff. A workshop participant claimed one firm "lost 46% of its talent [workforce] to competitors".

Stylized fact *C:2* claimed that "technical providers are often replaced mid-way through an investigation". We rejected it after it was contradicted by multiple workshop participants, for example:

- craifdmb4ever: "I think replacement of investigators is relatively rare."
- adhontwitch: "I also agree that its a very rare occurrence that someone gets replaced . . . "

Participants explained firms are instead punished by not receiving future work (similar to *M:1*).

Impact In trying to evaluate whether cyber insurance improved IR, our summary presented for validation suggested that insurers were driving down quality by pushing policyholders to hire from a small number of IR firms who were paid unsustainable fees. A participant provided an alternative interpretation:

> "Something missing from this conversation is how ensuring that everyone can work together is a HUGE benefit to breach response. Having a panel of companies that all work together with pre-negotiated contracts and pre-negotiated rates resolves the issues of compatibility and contract negotiation during a crisis."

Another workshop participant argued that:

> "Its driving a lot of good outcomes especially on the customer service part of things, which is more important in my view than a very elite technical team for most cyber claims."

Returning to our original question, it was not disputed that insurers had limited ability to monitor IR quality and extract lessons from incidents given they largely relied on oral reports provided by law firms (*M:2*). This was troubling given four firms hold 38% of the relationships with cyber insurers despite comprising 6% of the total law firms. The dominant law firm holds a relationship with 80% of the insurers identified in our desk research. This motivated Stage 2.

5 How Lawyers Shape IR

This section describes how lawyers advise clients. This covers the strategies that lawyers employ to protect confidentiality when overseeing incident investigations and the impacts these practices have on IR practitioners, breached firms, their insurers, and other third parties.

Pre-Breach Activities Although not strictly related to incident response, the majority of breach attorneys *took some steps to protect the confidentiality of pre-breach assessments and audits* (Row 1 of Table 4), even though several of them said such protections were unlikely to hold in court. Many lawyers said they would contract security firms for these services using boiler-plate language about how the activity (e.g. a risk assessment) was conducted to advise the lawyer on legal obligations. One lawyer said:

> "I warn clients that there's a good chance that privilege won't apply [to pre-breach activities] but I tell them there's a 100% chance privilege won't apply if you don't go through me. So often I will engage the teams that are doing . . . the pen testing and I had one recently where it was terrible and I just said to the forensics team, 'we don't want a final report, just keep this in draft form.' "

Other attorneys expressed concerns that the inability to provide strong confidentiality protections for pre-breach activities might at times deter companies from conducting such assessments, though most lawyers said the importance of cybersecurity protections usually outweighed such fears. One noted,

> "You never want to put in writing what the security system is like, but you also need candor to improve the system. And there is a risk that there won't be as much frank assessment, because that would turn into a roadmap for plaintiffs."

Broadly, this suggested that lawyers were usually not influencing the technical outcome of pre-breach risk assessments and audits, except in rare, extreme circumstances, and were instead typically making superficial tweaks to the work contract and reports.

Post-Breach Contracting To help protect confidentiality, all breach attorneys interviewed said they were involved in contracting with the forensics provider. Those contracts typically included clauses stating that the investigation was being conducted for the purpose of legal advice, and the attorney was a party in the contract sometimes even paying the IR firm directly (and later billing the client). If the forensics vendor was already providing pre-breach monitoring, the monitoring contract would be terminated and a new Statement of Work drafted in the event of an incident in most cases. A minority of breach attorneys said they believed a new firm should be hired entirely to provide the strongest possible claim for confidentiality and avoid any possible conflict of interest. Participants often referenced a recent legal ruling related to a breach of Capital One that suggested courts might regard continuity in DFIR providers before and after a breach as an indication that the DFIR firm was not hired specifically in anticipation of litigation. But one lawyer said that discontinuity in DFIR firms "can be counterproductive," a viewpoint echoed by a DFIR professional, who pointed out,

> "You don't want to spend time during incident response negotiating with the firm."

Communications After the contract was signed, all but one attorney maintained control via regular (e.g. daily) meetings to update on the progress of the investigation. This involved being on the call/in CC for any strategic aspects of the investigation but not for factual data collection and remediation efforts. Most attorneys accepted that routing communications through the attorney led to some efficiency loss, although a minority believed processes were sufficiently streamlined that this was not the case.

Most lawyers accepted that direct communication between vendor and client was necessary for technical tasks like gaining access to systems. Sometimes this freedom was extended to entire parts of the response, such as rebuilding networks and ransomware negotiation. One lawyer wanted to distance themselves from negotiating ransom demands because of OFAC sanctions. Another lawyer explained,

> "If the consultant is trying to get logs from IT people, we don't need to be on those calls, that's just logistical planning. Once conversations about where the firewalls were set up and how things were configured begin happening, we need to be involved in those conversations."

DFIR professionals also said they had learned to be careful about their communications based on instructions from lawyers overseeing their investigations. One DFIR professional said,

> "you never opine on whether [the client has] good or bad data security. If you get on a scoping call with a client and they don't have multifactor authentication enabled, or their password was passw0rd, you never chastise them, 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."

Documentation In terms of documenting findings, attorneys generally discouraged sending preliminary findings via emails or any medium that creates a written record. A handful of high-end lawyers expressed concern that the vendor's internal communications over platforms like Slack could be

discovered and used by litigants against the victim firm. The attorneys were divided on whether and under what circumstances a final report should be produced. A few lawyers noted that reports could be useful when demonstrating to regulators that the incident had been taken seriously. In most cases, however, lawyers advised against doing so because confidentiality protections may not apply. One lawyer said,

> "If I know there's likely to be litigation, we don't produce a report. People will go to the mat to get the report so it's much easier to just say 'I'm sorry, we don't have one.' "

Several lawyers faulted recent rulings that these reports were discoverable, as these court decisions discouraged writing reports. One attorney said,

> "I've started to advise against written reports. ... I'd say 75 percent of the time before [a ruling about a data breach report from] Capital One we had written reports, now in 75 percent plus we do not."

This trend away from written reports was also noted by DFIR professionals. One said,

> "It used to be that every time we responded to a breach, a client wanted a report at the end of it ... 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."

Another DFIR professional said there were three possible outcomes at the end of an investigation:

> "First, lawyers may ask only for evidence artifacts. Second, they may say 'thanks for investigations, you're done.' And the third option is they might ask for a formal report, which would include specific technical details that need to be conveyed about how to fix security issues. But a request for a formal report is made in less than 5 percent of cases, because in such a report we would have to document all the screw ups."

Many lawyers expressed concerns that reports could be incomprehensible to non-technical people or overly subjective, such as color-coding vulnerabilities in red or using terms like "a flagrant culture of non-compliance." However, speaking to forensics vendors revealed lawyers could also be unreasonable, such as one anecdote describing a long back and forth over whether the report could include the statement "the server was vulnerable". Such concerns motivated strategies like creating a bare-bones report, editing the vendor's report line-by-line over video call, or the attorney drafting a legal memo summarizing findings.

One major question was whether formal reports should include recommendations to improve the victim firm's security posture. Most lawyers preferred communicating recommendations orally or via PowerPoint because inclusion in the report provided a "road map to litigation" as they imply the incident would have been avoided had those measures been in place. One lawyer explained,

> "When I become concerned is when the forensics team is producing a paper trail. Because then plaintiff can say, 'your outside expert said you should do this, and you didn't, so you were negligent.' So I don't want that in writing."

Some lawyers said that including recommendations undermines the claim to confidentiality protections because it looks like the report was not prepared for a legal purpose. The majority of lawyers did not believe oral reports were less likely to be implemented, although a sizable minority contradicted this.

Information Sharing Most lawyers believed that sharing documents with third-parties (e.g. insurers, auditors and regulators) could undermine later claims of confidentiality. Instead, attorneys preferred to answer specific questions orally, especially for auditors. Insurers predominantly accepted this practice as in their best interest and did not request further information, with one of the largest US cyber insurers seeing a forensics report in less than 5% of claims. A passionate minority of underwriters believed this prevented insurers from learning lessons about which security controls were effective.

Strategies around sharing information with regulators varied. One respondent explained that information was always shared over the phone, noting that working relationships had been established across the volume of incidents the respondent's firm works every year. Other attorneys believed that producing and sharing a forensics report helped to convince the regulator that the firm was taking the incident seriously, which was especially important for regulators with broad authority over the firm. Regulators themselves seemed largely resigned to their inability to access these reports. One explained,

> "We sort of half-heartedly ask on these calls—and most of the time I don't—is there a report? But it's evolved to a point where most of the time they're not writing a report, and that's a shame."

Impact There was variation in the extent to which all stakeholders—lawyers, forensics investigators, and insurers—identified costs in pursuing confidentiality protections. Some said they thought there was no impact on the investigation either in terms of speed or efficacy. Many stakeholders said that funneling all communications through the lawyers, refusing to issue final written reports with recommendations, and declining to share information about the incident with third parties could significantly erode long-term learning from incidents.

Table 4: Strategies employed by each breach attorney (A1–A23) that we interviewed.

Breach attorney	A17+18	A21	A7	A8	A9+10	A22	A23	A2	A16	A3	A13	A14	A6	A20	A12	A15	A5	A11	A19	A1	A4
Pre-breach activities																					
takes steps to establish confidentiality		○	●	◐	●	●	●	○	●	◐	●	●	●	●	●	●	●	●	○	●	●
discourage activities due to confidentiality	◐		◐	○	○	○	○	○	○	○	○	○	◐	○		○	○	○	○	○	
confident confidentiality protected			◐	◐	●	○	◐	○	●	◐	●	◐	◐	◐	◐	●	●	●	○	◐	
Post-breach response																					
confident confidentiality protected				◐		●	○		◐				●	◐	◐	◐			○		
contract forensics firm	●	●	●	●	●		●	●	◐	●	●	◐	●	●	●	●	●	●		●	●
prefer hiring new firm	●		◐	○		○		○	○	●		○	○	◐	○	●	◐	●	○	◐	
attend daily/regular updates	●	●	●	●	●	●	●	●	○	●	●	◐	●	●	●	●	●	●	●	●	●
efficiency loss working through law firm	○	○	●	●	●	●	◐	●	●	○		○		●	●	●	◐		●	○	●
direct comms sometimes necessary	○	●	●	●		●	●	●	●	●		●	●	●	●	●	○	●	●	●	●
Documentation																					
discourage formal reports	●	●	◐	●	●	◐	●	○	○	◐	◐	●	◐	●	●	●	●	◐	○	○	○
review drafts and suggest changes					●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
write legal memos instead		●	●		●					●	●	●	●	●	◐	◐	●		●	●	●
Internal information sharing																					
limit sharing of report within firm	●		●			●				●	●	●		○		●				◐	●
restrict involvement of IT staff	●		●	●		○	●			●	●	◐					○	○			
discourage recommendations in report		●	●	●		●	○	○		●	●	●	●	○	○	●	●	●	●	●	●
recommendations primarily orally		●	●		●			○		●	○			○	◐	○	●	●	●	●	◐
above means implementation unlikely	○	●	●	●			○	●		○	◐			●	○	○	○	○	○	○	○
External information sharing																					
share report with insurers	○	◐	○	○		○	●	○	●	◐	●	○	○	○	○	○	○	○	○	●	○
share report with auditors			○			○		○				○			○	○	○	○		○	○
share report with regulators	○	◐	○	◐	◐	○	○	◐	●	○	◐	○	○		◐	○	○	○	◐	○	○
do insurers request detailed info	○	○	●	○			○		○		◐	○	◐	◐		○	●	◐	○	●	●
sharing report waives AC privilege			●	◐			○		○	○	◐	◐		◐	◐	●		◐	●	○	●
oral comms with insurer	●	●	●	●		○					○	●	●	●	●	●	●	●		○	●
oral comms with regulator	●		●	●	○	○		○	○	●	●	●	◐		●	●	●	●	●	○	○

●/○ = participant supported/contradicted the statement in the first column, ◐ = the participant described nuance (e.g. "it depends on…"), and no symbol if we were not confident of the participant's belief upon reviewing the transcript. A9+10 and A17+18 were joint interviews. The column order is generated from a dendrogram to cluster similar response patterns.

Some respondents believed contracting with a new firm was inefficient because the existing firm has familiarity with and access to the client's network, while others suggested retaining the firm that provided security services prior to the breach created a conflict of interest. Attorneys defending this practice argued the inefficiency was off-set by the experience and understanding built by working with favored IR firms on many incidents.

The problems associated with documentation were again contested. The lack of a written record made reconstructing attacks difficult after time had passed, such as when investigators make inquiries months and even years later. There was widespread disagreement about whether the lack of written remediation advice prevented victims improving their security posture. Technical vendors believed written reports helped security departments advocate for more resources and track progress. One IR professional said,

> "There's a lot of information you can convey verbally but when you have larger companies with bigger teams [sending a written report] gives such a better understanding of the weaknesses in their systems."

Another pointed out,

> "IT directors can strategically use forensics reports to win internal resources. But this doesn't happen and can't happen if I just deliver it to counsel."

This was contradicted by lawyers who believed such findings could be adequately communicated in a separate report or even orally. It was also noted that forensics vendor's remediation advice tended to be obvious, not tailored to the client or consist of up-selling the vendor's products and services in some cases.

6 Discussion

Section 6.1 discusses the influences on IR that emerge from our study. Section 6.2 then discusses solutions at the technical, business and policy level.

6.1 How is IR Impacted

Insurance To evaluate whether cyber insurance improves IR, we must ask how hotline operators assign IR firms to incidents and compare that to a hypothetical baseline in which cyber insurance was not purchased. Insurers coordinating IR is most beneficial for under-resourced firms with no IR plan. Even firms who would otherwise have a plan may appreciate the insurer's influence. Insurers benefit from a stronger negotiating position and the ability to observe the IR firms' performance across multiple claims. Furthermore, the insurer's influence is optional given insurers will pay for off-panel firms if this request is made pre-incident. Thus, it appears cyber insurance has improved IR planning. For a historical analogy, insurers created the first fire service in London, which later became a public service [44].

Lawyerization Some legal strategies identified in Table 4 have a superficial impact on outcomes, such as whether the law firm is party to the contract with the IR firm. Other strategies introduce real costs, such as time delays and financial cost when lawyers join calls to create the impression they are directing the investigation. However, the net impact of lawyer-led IR is difficult to evaluate given lawyers also bring benefits in terms of advising on notification requirements [45], managing reputation [46], project management and more. We instead focus on the question of how lawyers influence the learning process.

Lawyer-led IR has all the same problems the technical community faces in extracting lessons from incidents [1, 47], plus additional constraints about what can be put into writing and shared. This advice limits information flows, even within the firm. In extreme cases, attorneys may distort the documentary record to reduce litigation risk, as evidenced by one participant having to fight to describe a server as vulnerable. Such strategies introduce additional barriers to how firms learn from security failures, not to mention how the wider community learns, that would not exist if lawyers were not directing IR.

6.2 Potential Solutions

We survey various proposals, which should be evaluated in more depth in future work.

IR Cost-saving Insurers negotiating lower fees for DFIR work creates a need for more efficient investigations. Investigators can improve tooling, such as via automation [48, 49]. Similarly, vendors can make APIs available to IR teams. For example, an undocumented Windows Exchange API was used to investigate compromises of email inboxes until Microsoft removed access [40]. Such APIs can, however, erode user privacy, which motivates research into privacy preserving solutions.

Increasing the supply and skills of IR practitioners would also reduce costs. This could be done via workforce development, such as training and/or formal education. One could also argue that insurers limit the supply of IR practitioners by only working with on-panel firms. It could be broadened by covering the cost of investigators with up-to-date professional certifications regardless of whether their firm was approved. However, this is possibly naive in the short term given research reveals a lack of IR quality assurance mechanisms [50] or best practice [51, 52].

Extracting Lessons Many actors could take responsibility for learning from cybersecurity incidents. Insurers could sim-

ply ask IR firms to begin documenting and sharing findings for low-profile incidents that are unlikely to be litigated. After all, empirical studies have shown that few cyber incidents result in litigation [53], and many of those are settled before entering the discovery phase (when confidentiality protections become relevant). IR reports may help insurers extract lessons by linking insurance claims back to (the absence of) security controls. This would allow insurers to begin improving ex-ante cybersecurity, which they have failed to do so far [24, 25].

This trade-off between lessons learned and litigation risk could be eased if policymakers created confidentiality protections specifically tailored to cybersecurity investigations [37, 39]. This would allow IR firms to document findings and share with relevant parties without the associated documentation being used by litigants. Unfortunately this would also limit the ability of consumers and shareholders to seek damages from firms who mismanaged personal data [54]. To correct for this, policy-makers could force victim firms to prioritize lessons learned by creating an affirmative obligation to collect, document, and share specific evidence. This highlights the challenge that policy-makers face in finding a balance between confidentiality protections that enable improved IR and holding firms accountable for security failures.

So far, we assumed the burden of knowledge extraction lies within the private sector. Given the benefits accrue to the public, arguably knowledge generation should be publicly funded. Governments could fund investigations into cybersecurity failures, much like how the US National Transportation Safety Board investigates civil transportation accidents and issues safety recommendations [11].

Summary Solutions are available to insurers and victim firms, such as using better forensic tooling, broadening panels, and demanding the production of forensics reports. However, it seems unlikely these incremental solutions will solve the long-standing problem of extracting lessons from cyber incidents [1, 11]. Doing so requires resources at a different scale. Governments can change the legal regime upon which legal strategies are based, or provide government funded investigations insulated from concerns around litigation. The software and cloud vendors who design and operate vast swathes of corporate IT infrastructure are also responsible. They have access to the data to understand causes of failure, and can then apply these lessons when building the next-generation of corporate IT infrastructure.

7 Limitations

Our approach adopts some aspects of grounded theory [55]: (i) focusing on the day-to-day processes of research participants; (ii) minimal prior theory; (iii) iterative stages of data collection and analysis; and (iv) embracing the idea that *everything is data*. However, we diverge from mainstream grounded theory by aiming to derive a functional description and evaluating this via practitioner feedback.

Validity Asking practitioners who observe these services on a day-to-day basis to validate research findings comes with risks. A lack of falsification does not necessarily represent positive confirmation of the results—findings cannot be contradicted if they are incomprehensible or do not reach enough/the right practitioners. It is therefore encouraging that we avoided two failure modes; (i) no refutation at all (a sign findings are not clear enough to contradict), and (ii) constant refutation. The validation workshop feedback led us to reject one stylized fact (*C:2*) and develop a more nuanced interpretation of the descriptive findings—we directly quoted this input in the results section.

In general, we focused on descriptions of insurer processes and legal strategies (the stylized facts and Table 4). Although we did ask participants about the impact on cybersecurity outcomes, we only presented the findings as perspectives. We were not confident that participants could reliably isolate causal effects on system-level outcomes, in part because participants are self-interested in not blaming their profession for negative outcomes. Future work could investigate this empirically by measuring how legal strategies impact quantitative metrics like the time to contain incidents.

Bias Our desk research is exposed to inaccuracies given websites are infrequently updated and that some insurers did not publish approved IR firms on their website. Our recruitment strategy was also vulnerable to sample/non-response bias given many practitioners did not hear about our study/opted against participating. In retrospect, we should have tracked how many invites to interview were sent by email/LinkedIn so that we could calculate the response rate. A substitute recruitment metric is the coverage of major DFIR and law firms (65%/70%) in the cyber insurance ecosystem.

Generalizability We believe Stage 1 describes most of the US cyber insurance ecosystem. Not only did we speak to the majority of IR firms in the ecosystem, but we asked participants about their experience dealing with other stakeholders. This is beneficial because one IR practitioner may work for multiple insurers, including those we did not interview.

We believe Stage 2 describes the range of advice being offered by US-based lawyers. Even those lawyers we interviewed who operate independently of insurers offer similar advice and reference the same case law (e.g. Capital One). Anecdotal data from outside the US suggest that lawyers are less central to incident response, but still present.

8 Conclusion

The exploratory stage of our study showed that the insurance industry created emergency phone lines that policyholders can call upon detecting a cyber incident. The operator, typically

a law firm, advises on which incident response firms to hire. Contractual terms like the hourly rate are pre-negotiated by the insurer, and the insurer withdraws future work if service quality is perceived to have fallen. While some participants worried insurers' cost-cutting was lowering the quality of IR, there are benefits in terms of broadening access to IR for under-resourced firms, and giving a small number of firms experience working together.

However, it became clear that insurers could not extract lessons from claims given they largely received oral reports about incidents. This motivated the second stage of our study that focused on the stakeholders who direct and monitor investigations on a day-to-day basis, namely breach attorneys. Attorneys often advise against writing a report, review the contents and suggest changes or even draft legal memos that summarize the forensics findings. Remediation steps are rarely included in the report, although they might be communicated in other channels. Many attorneys advise against sharing documents with third-parties because doing so could be a waiver of confidentiality protections. Together these impacts suggest that the advice of breach attorneys leads to *lessons lost* rather than *lessons learned*.

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 article. 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.

References

[1] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. Computer security incident handling guide. *NIST Special Publication*, 800(61):1–147, 2012.

[2] Rick Van der Kleij, Geert Kleinhuis, and Heather Young. Computer security incident response team effectiveness: a needs assessment. *Frontiers in Psychology*, 8:2179, 2017.

[3] Martin Gilje Jaatun, Eirik Albrechtsen, Maria B Line, Inger Anne Tøndel, and Odd Helge Longva. A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, 2(1-2):26–37, 2009.

[4] Atif Ahmad, Justin Hadgkiss, and Anthonie B Ruighaver. Incident response teams–challenges in supporting the organisational security function. *Computers & Security*, 31(5):643–652, 2012.

[5] Atif Ahmad, Sean B Maynard, and Graeme Shanks. A case analysis of information systems and security incident responses. *International Journal of Information Management*, 35(6):717–723, 2015.

[6] Stefan Laube and Rainer Böhme. Strategic aspects of cyber risk information sharing. *ACM Computing Surveys*, 50(5):1–36, 2017.

[7] Adam Zibak and Andrew Simpson. Cyber threat information sharing: Perceived benefits and barriers. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pages 1–9, 2019.

[8] Vector Guo Li, Matthew Dunn, Paul Pearce, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. Reading the tea leaves: A comparative analysis of threat intelligence. In *Proc. of the 28th USENIX Security Symposium*, pages 851–867, 2019.

[9] Xander Bouwman, Harm Griffioen, Jelle Egbers, Christian Doerr, Bram Klievink, and Michel van Eeten. A different cup of TI? the added value of commercial threat intelligence. In *Proc. of the 30th USENIX Security Symposium*, pages 433–450, 2020.

[10] Xander Bouwman, Victor Le Pochat, Pawel Foremski, Tom Van Goethem, Carlos H Gañán, Giovane Moura, Samaneh Tajalizadehkhoob, Wouter Joosen, and Michel van Eeten. Helping hands: Measuring the impact of a large threat intelligence sharing community. In *Proc. of the 31st USENIX Security Symposium*, pages 1149–1165, 2022.

[11] Rob Knake, Adam Shostack, and Tarah Wheeler. Learning from cyber incidents: Adapting aviation safety models to cybersecurity. *Harvard Belfer Center*, 2021.

[12] Ross Anderson. Why information security is hard—An economic perspective. In *Proc. of the Computer Security Applications Conf.*, pages 358–365. IEEE, 2001.

[13] Ross Anderson and Tyler Moore. The economics of information security. *Science*, 314(5799):610–613, 2006.

[14] Josephine Wolff and William Lehr. Roles for policy-makers in emerging cyber insurance industry partnerships. 46th Research Conference on Communication, Information and Internet Policy, 2018.

[15] Shauhin A Talesh. Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry*, 43(2):417–440, 2018.

[16] National Association of Insurance Commissioners Staff. Report on the cybersecurity insurance market. https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf, 2021. Accessed: 2022-03-11.

[17] Savino Dambra, Leyla Bilge, and Davide Balzarotti. SoK: Cyber insurance—Technical challenges and a system security roadmap. In *Proc. of the Symp. on Security and Privacy*, pages 293–309. IEEE, 2020.

[18] John Douglas Howard. *An analysis of security incidents on the internet 1989-1995*. Carnegie Mellon University, 1997.

[19] Stefan Laube and Rainer Böhme. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, 2(1):29–41, 2016.

[20] Sasha Romanosky, David Hoffman, and Alessandro Acquisti. Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, 11(1):74–104, 2014.

[21] Sasha Romanosky, Andreas Kuehn, Lillian Ablon, and Therese Jones. Content analysis of cyber insurance policies: How do carriers price cyber risk? *J. of Cybersecurity*, 5(1), 2019.

[22] Ulrik Franke. The cyber insurance market in Sweden. *Computers & Security*, 68:130–144, 2017.

[23] Daniel W Woods and Tyler Moore. Does insurance have a future in governing cybersecurity? *IEEE Security & Privacy*, 18(1):21–27, 2020.

[24] Jamie MacColl, Jason RC Nurse, and James Sullivan. Cyber insurance and the cyber security challenge. *Royal United Services Institute Occasional Paper Series*, 2021. [Online; accessed 19-Sep-2022].

[25] Josephine Wolff. *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*. MIT Press, 2022.

[26] Manuel Egele, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. Compa: Detecting compromised accounts on social networks. In *NDSS*, 2013.

[27] Ulrik Franke and Joel Brynielsson. Cyber situational awareness–a systematic review of the literature. *Computers & Security*, 46:18–31, 2014.

[28] Pedro Garcia-Teodoro, Jesus Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, 28(1-2):18–28, 2009.

[29] Grant Ho, Aashish Sharma, Mobin Javed, Vern Paxson, and David Wagner. Detecting credential spearphishing in enterprise settings. In *Proc. of the 26th USENIX Security Symposium*, pages 469–485, 2017.

[30] Amin Kharaz, Sajjad Arshad, Collin Mulliner, William Robertson, and Engin Kirda. UNVEIL: A large-scale, automated approach to detecting ransomware. In *Proc. of the 25th USENIX Security Symposium*, pages 757–772, 2016.

[31] Sameera Almulla, Youssef Iraqi, and Andrew Jones. A state-of-the-art review of cloud forensics. *Journal of Digital Forensics, Security and Law*, 9(4):2, 2014.

[32] Rupali Chopade and Vinod Keshaorao Pachghare. Ten years of critical review on database forensics research. *Digital Investigation*, 29:180–197, 2019.

[33] Rainer Poisel and Simon Tjoa. Forensics investigations of multimedia data: A review of the state-of-the-art. In *6th International Conference on IT Security Incident Management and IT Forensics*, pages 48–61. IEEE, 2011.

[34] Tran Van Lanh, Kai-Sen Chong, Sabu Emmanuel, and Mohan S Kankanhalli. A survey on digital camera image forensic methods. In *2007 IEEE International Conference on Multimedia and Expo*, pages 16–19. IEEE, 2007.

[35] Hudan Studiawan, Ferdous Sohel, and Christian Payne. A survey on forensic investigation of operating system logs. *Digital Investigation*, 29:1–20, 2019.

[36] Josephine Wolff. *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*. MIT Press, 2018.

[37] Jeff Kosseff. The cybersecurity privilege. *Journal of Law and Policy for the Information Society*, 12(2):261–303, 2015.

[38] Chinomnso John Okebie. Legal professional privilege and cybersecurity breach in context: A comparative law analysis. *Queen Mary Law Research Paper*, (350), 2021.

[39] Daniel Schwarcz, Josephine Wolff, and Daniel W Woods. How privilege undermines cybersecurity. *Harvard Journal of Law & Technology*, 2023 (forthcoming).

[40] Daniel W. Woods and Rainer Böhme. Incident response as a lawyers' service. *IEEE Security & Privacy*, 20(02):68–74, 2022.

[41] Daniel W Woods and Aaron Ceross. Blessed are the lawyers, for they shall inherit cybersecurity. In *New Security Paradigms Workshop*, pages 1–12, 2021.

[42] Daniel W. Woods and Rainer Böhme. How cyber insurance shapes incident response: A mixed methods study. In *Workshop on the Economics of Information Security*, 2021.

[43] Nicholas Kaldor. A model of economic growth. *The Economic Journal*, 67(268):591–624, 1957.

[44] Jennifer Anne Carlson. The economics of fire protection: From the great fire of London to rural/metro 1. *Economic Affairs*, 25(3):39–44, 2005.

[45] Yixin Zou, Shawn Danino, Kaiwen Sun, and Florian Schaub. You 'might' be affected: An empirical analysis of readability and usability issues in data breach notifications. In *CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2019.

[46] Sarah Bana, Erik Brynjolfsson, Wang Jin, Sebastian Steffen, and Xiupeng Wang. Cybersecurity hiring in response to data breaches. *Available at SSRN 3806060*, 2021.

[47] Inger Anne Tøndel, Maria B Line, and Martin Gilje Jaatun. Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45:42–57, 2014.

[48] Golden G Richard III and Vassil Roussev. Next-generation digital forensics. *Communications of the ACM*, 49(2):76–80, 2006.

[49] Eva A Vincze. Challenges in digital forensics. *Police Practice and Research*, 17(2):183–194, 2016.

[50] Helen Page, Graeme Horsman, Anna Sarna, and Julienne Foster. A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn? *Science & Justice*, 59(1):83–92, 2019.

[51] Sydney Liles, Marcus Rogers, and Marianne Hoebich. A survey of the legal issues facing digital forensic experts. In *IFIP International Conference on Digital Forensics*, pages 267–276. Springer, 2009.

[52] Vikram S Harichandran, Frank Breitinger, Ibrahim Baggili, and Andrew Marrington. A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security*, 57:1–13, 2016.

[53] Sasha Romanosky. Examining the costs and causes of cyber incidents. *J. of Cybersecurity*, 2(2):121–135, 2016.

[54] Daniel J Solove and Woodrow Hartzog. *Breached!: Why Data Security Law Fails and How to Improve it*. Oxford University Press, 2022.

[55] Barney G Glaser and Anselm L Strauss. *The discovery of grounded theory: Strategies for qualitative research*. Routledge, 1967.

A Interview Guidelines

We prepared the following set of questions before the interviews began. We did not ask a question if the participant had already provided that information when answering another question. In both stages, interview scripts were tweaked for specific stakeholders. For example, an IR firm would be asked to "talk me through a typical or specific example of a negotiation with an insurer", whereas an insurer firm would be asked to "talk me through a typical or specific example of a negotiation with an IR firm".

A.1 Stage 1

General

- Could you describe your professional background.
- What kind of services do you provide?
- How do you interact with insurers, brokers or breach coaches in your role?
- How many members in your team? Experience?

Search

- Who has influence in deciding which service provider is chosen?
- Rank the influence of insurers, brokers, breach coaches and the client in choosing the IR firms
- What percentage of your relationships involved the insurer making first contact?
- Can you quote prices before understanding the incident? (e.g hourly rate or fixed price)
- Under what circumstances would you share quotes?

Negotiation

- Talk me through a typical or specific example of a negotiation with a service selector.
- How would you go about evaluating a service provider's quality?
- Do service providers negotiate with insurers/breach coaches/clients? Along which lines?
- What kind of agreements are there between insurer and service provider?
- Who decides what level of investigation takes place, how much time etc.
- How do the services in insurer agreements compare to clients you find independently?
- Are the insurers' prices negotiable?
- How often is it renegotiated?

Monitoring

- What happens to the forensic report?
- Who monitors service quality?
- What kind of disputes arise between insurer and service provider?
- How are they resolved?

High-level

- Do you anticipate any trends?
- Do you see any dysfunctional aspects of the IR services ecosystem?
- Could IR services be automated?
- What is the role of triage in IR response? Who decides how resources get assigned to each incident?

A.2 Stage 2

General

- What is your role in incident response?
- How long have you been working in cyber incident response?
- What kind of clients does your firm work for? Is your firm typical of the industry?

Specifics of Client–Attorney Privilege
For lawyers:

- To what extent do concerns about protecting client confidentiality impact how you operate incident response and direct others involved in the process, like digital forensic experts?
- How much confidence do you have that placing lawyers in charge of incident response will indeed preserve confidentiality through doctrines like A/C privilege and work product?

For non-lawyers:

- Under what circumstances are you aware of CA privilege or work doctrine concerns?
- What practical steps do you or your colleagues take to uphold either privilege?

Pre-Breach Monitoring

- How do confidentiality concerns impact ex-ante monitoring?
- Have you ever seen evidence that firms may be reluctant to actively monitor or for breaches or take other proactive measures because any materials generated by that process would not be shielded from discovery?

Contracting

- How do confidentiality concerns impact the decision of which IR firms to hire?
- Do they impact any details about the contract?
- Discontinuity in hiring?

Investigation

- How do confidentiality concerns impact what you investigate? What you document?
- Have you ever told or been told not to produce a post-incident report because of confidentiality concerns?

Information Sharing

- If findings and recommendations cannot be shared through a formal report how are they shared? Powerpoint? Oral discussions?
- How do confidentiality concerns impact the decision to share this information?
- If formal post-incident response are now shared with insurers, what information is shared with them?
- How do confidentiality concerns impact post-incident remediation?
- What kind of/how often do incident response clients subsequently purchase further products or services?

High-Level (if time allows)

- Are there any problems in the ecosystem as you see them? Any misaligned incentives or conflicts of interest?
- Do you observe any trends in the ecosystem?

B Supplemental Material

B.1 Stylized Facts

Stylized Facts related to Search

S:1 Insurers build a panel of firms whose services the policy will indemnify, and the hot line operator triages by recommending specific providers.

S:2 Shortlisting for the panel is selective and the provider must commit to certain terms.

S:3 Most firms follow the recommendation of the hot line operator, who tends to be an external law firm in the US.

Stylized Facts related to Negotiation

N:1 Insurers negotiate hourly rate/fixed pricing while building the panel, policyholders provide information about their environment (e.g. number of sites or machines), and hot line operators advise on the scope of work. This results in a statement of work, which must be approved by the insurer or a delegated authority.

N:2 Often insureds contract with external counsel, who then hire firms on the insured's behalf. Technical work may be further sub-contracted.

N:3 Insureds negotiate additional services that are not covered by cyber insurance. Monitoring tools installed as part of the investigation are often retained by the insured at their own cost.

Stylized Facts related to Monitoring

M:1 IR firms avoid disputes in order to receive future work from insurers and external counsel. There are few disputes when on-panel firms are used.

M:2 Insurers rely on external counsel to monitor providers on a day-to-day basis. The insurer mainly receives informal/verbal reports.

M:3 Forensics reports are not standardized. Investigations are structured according to the law firm.

Stylized Facts related to Market Structure

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. *(rejected)*

C:3 There are always upstart forensics firms offering a lower price. Often such firms are founded/led by the former employees of dominant firms.

B.2 Supplemental Figures

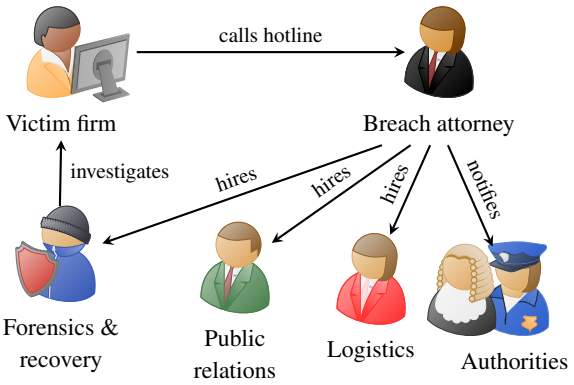

Figure 3: Policyholders call insurer's incident hotline, which is operated by a breach attorney who directs subsequent investigation. Figure adapted from [42].

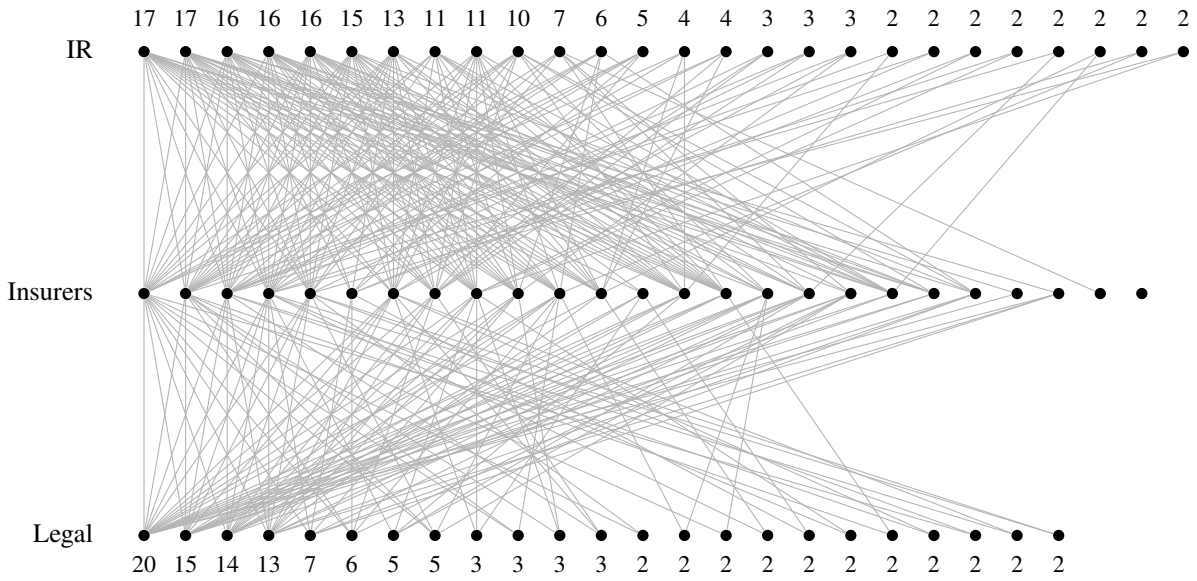

Figure 4: Mapping the post-breach market: technical services (top, 193 listings in total) are less concentrated than legal services (bottom, 119 listings in total). Figures indicate the number of listings per provider. Providers which appear on less than two panels are omitted. Data from 2022.

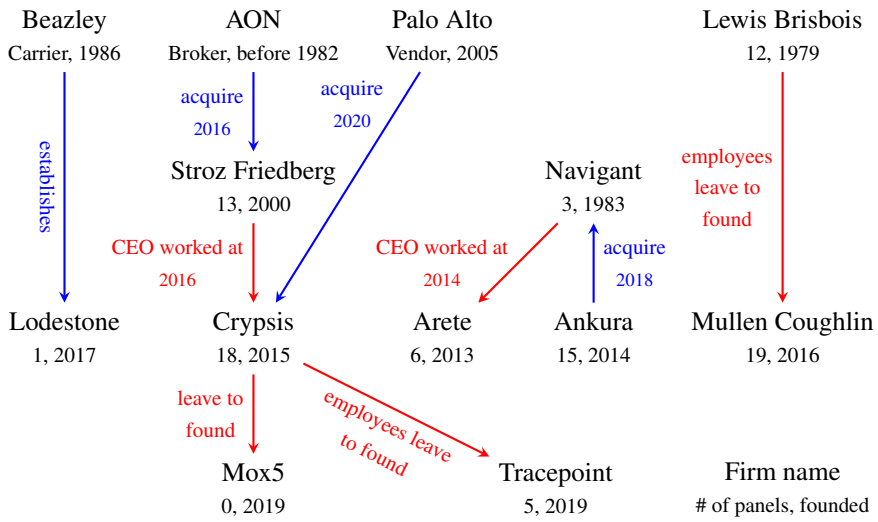

Figure 5: A non-exhaustive description of company relationships (blue) and senior leadership moves (red).