Incident Response as a Lawyers' Service

Incident Response as a Lawyers' Service

Daniel W. Woods and Rainer Böhme

Department of Computer Science
University of Innsbruck, Austria
daniel.woods@uibk.ac.at *rainer.boehme@uibk.ac.at*

***Abstract*—Thousands of incidents each year are now managed by external law firms. Victim firms call a hotline and delegate incident response to external counsel without a pre-existing relationship. We assemble preliminary evidence on how this model breaks from conventional incident response and outline questions for future research.**

I. Introduction

Incident response (IR) is increasingly managed by external law firms specialising in security and privacy incidents. Such firms (called *external counsel* throughout) collectively managed over 4 000 incidents in 2018 [1] and a leading IR firm report that half of their investigations take place under the direction of external counsel [2]. Many of these firms operate under the *breach coach* trademark, the trademark holder's blog explains that:

> Breach coaches are attorneys ... [whose] first role is to protect the response process under privilege. We will obtain forensics providers as necessary to uncover the cause and scope of the breach. We analyze those facts to identify what legal duties are triggered and then work with the client to satisfy those duties, which can include providing notice of the breach to affected individuals, regulators and the media. We will retain related service providers on behalf of the client, including printing, mailing, call center and credit monitoring.

External counsel go beyond merely providing legal advice, as shown in Figure 1. They control the IR value chain by subcontracting multiple service providers including forensics firms, and prioritise protecting client–attorney privilege above other concerns. In the US legal system, privilege is a legal defense that prevents documents and communications being used by litigants. For example, privilege might be invoked to prevent a forensics report being used as technical evidence that the victim firm breached their duty of care to customers or shareholders.

These concerns around litigation risk are a continuation of the trend identified by Bruce Schneier [3]. He claims that the 1990s were the decade of prevention, the 2000s the decade of detection, and the 2010s the decade of response. In each stage, the timing of the associated security tasks is shifted forward relative to the incident—prevention is pre-incident, detection is ideally immediately after, response covers clean-up and recovery that should be completed within weeks, and external counsel are concerned by litigation months or even years after the incident.

In another sense, this new *hotline model* of breach response represents a significant break from conventional incident response. Victim firms' response can be as simple as noticing an incident, calling a hotline and following the operator's guidance. Operators—often but not always a law firm—must then understand the incident based on the call and hire the most suitable post-breach service provider. Philosophically, this represents a collapse in the problem space. Conventional incident response planning had to cover the universe of possible vulnerabilities and threat actors, much like prevention or detection. In contrast, *hotline IR* must only respond to a particular threat actor who has used a particular exploit.

This paper explores how this development changes incident response. We characterise how the new model of IR breaks from what came before in Section II. We collect together industry reports to describe what is known about external counsel in Section III. We describe open and pressing questions in Section IV, and then conclude in Section V.

II. Conventional Incident Response

To characterise what came before incident response as a lawyers' service, we turn to a US standard to understand "what incident responders actually do" [4, p. 33]. Indeed, a systematic review of academic and practitioner reports found that "current practice and experience seem to be in line" [5] with industry standards. NIST-800-61 describes incident response best practice in terms of organizational structure and processes rather than the specifics of data collection. Figure 2 highlights how *hotline IR* differs from conventional IR as embodied in NIST-800-61. The new model is not incompatible conventional IR, but it does go against a number of recommendations.

The conventional model recommends extensive forward planning in which IR responsibilities and processes are established and rehearsed on an ongoing basis. NIST 800-61 describes the need for a "formal, focused, and coordinated approach" tailored to the firm's unique requirements [6, S. 2.3.2]. Less planning is required to engage external counsel, which can be as simple as calling the dedicated hotline with no pre-existing contact. Although this suggests unpreparedness, one could argue external counsel continually rehearse the plan when working for other clients.

A second difference relates to who holds responsibility for IR. NIST 800-61 recommends internal stakeholders hold

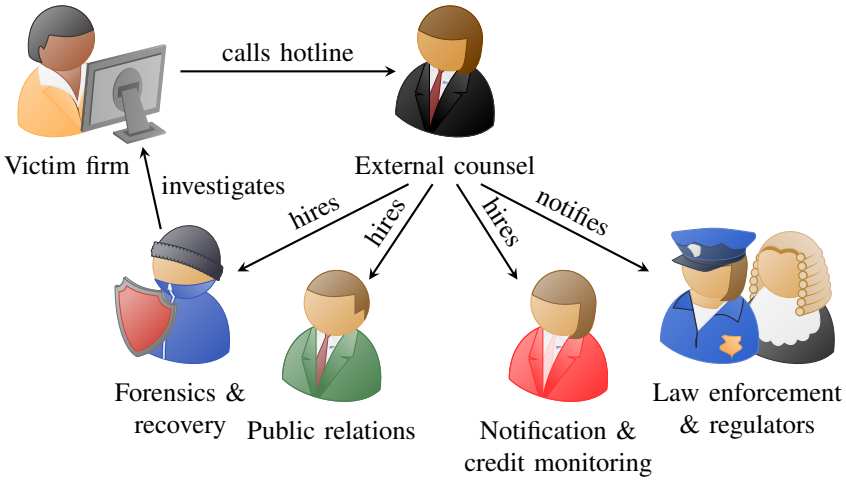

Fig. 1. External counsel control the incident response value chain and interactions with authorities.

responsibility as evidenced by the internal incident response team operating as the central coordinator [6, Fig. 2]. Even when IR is fully out-sourced, the standard suggests internal employees should be "supervising and overseeing the out-sourcer's work" [6]. Along this spectrum of internal–external responsibility, external counsel operating as breach coaches are given significant responsibility in issuing legal advice and also in subcontracting all other service providers.

There is further difference in terms of which tasks are out-sourced. NIST 800-61 [6, p. 14] states that the most common arrangement out-sources detection in the form of "24-hours-a-day, 7-days-a-week (24/7) monitoring". One firm offering such a monitoring solution, Verizon, provide an insight into who adopts conventional incident response. Their main customers, classified by industry, were "Finance and Insurance (33%), Retail Trade (17%), and Manufacturing (15%)" [7].

In spite of this, detection is far from a solved problem and many firms rely on external notifications [5]. CrowdStrike report that only 16% of compromises are detected within 24 hours [2]. Delayed detection and firms relying on external notifications is likely because pro-active detection is expensive and requires high security maturity. As a result, detection lies entirely outside the hotline model of incident response (see Figure 2) as firms simply call the hotline when someone notices the attack.

This has implications in terms of the information available for forensics investigations. Conventional IR plans integrate detection and response so that investigations can draw on information collected during pre-incident monitoring. This also means systems can be designed and configured to preserve evidence, such as keeping extensive log records for longer periods. In contrast, the *hotline model* is engaged once an incident has been detected and the forensics firm likely has no pre-existing access to the victim's IT environment [8].

Although not strictly defined in the standards, relationships with firms offering detection are generally contracted via *retainer agreements*. In such an agreement, the client contracts and pays for IR services before the incident has occurred. This allows an IR plan to integrate detection and response. It also means victims need not negotiate under the pressure of an ongoing incident. In contrast, contracts with external counsel and their subcontractors are generally signed under time pressure after an incident has been detected. The benefit of negotiating post-incident is making a more plausible claim that the services were contracted in anticipation of litigation and hence the report is protected by privilege [9].

This ties into the skill set guiding IR. In the hotline model, a lawyer guides response decisions and in many cases oversees the forensic provider's work [8]. In contrast, NIST-800-61 recommends that the "appropriate skills" [6, p. 19] consists of technical expertise and merely states that legal and public relations "may need to participate". Further, a technical lead should hold "responsibility for the quality of the team's technical work". Indeed, the systematic review finds that "response and learning activities mainly include technical staff" [p. 55][5].

Finally, conventional incident response also covers a reflective exercise to distill *lessons learnt* [4]. Tøndel et al. [5] report that although this varies across organisations, it skews towards collecting "technical information" and insights tend not to be shared externally. In one case, the resulting insights led to a 92% reduction in monthly incidents. In contrast, external counsel are less likely to feed insights back into mitigation measures because they often have no pre-incident relationship (although many offer risk consulting). However, external counsel can apply insights and experience accrued working for other clients.

These differences should not be taken as absolute. Despite the value placed on technical expertise, NIST 800-61 states that the overall lead (e.g. an attorney in the new model) need only be "technically adept" [6, p. 16]. Similarly, Figure 2 depicts the idealised version of each approach. Plans may blend the approaches in actuality, such as by developing an IR plan that integrates information collected by active monitoring

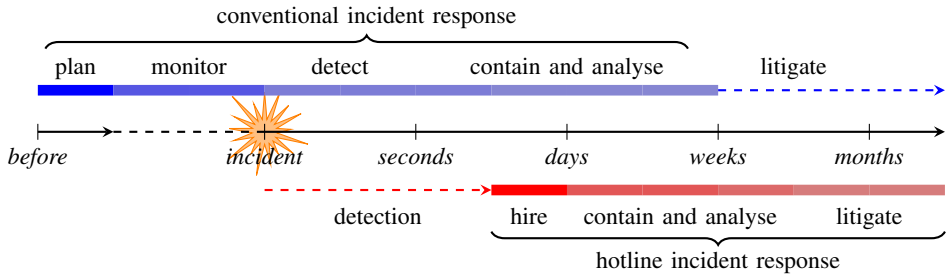

Fig. 2. A stylised comparison of conventional and hotline incident response. Dashed lines are outside the plan.

while also engaging external counsel. The extent to which external counsel led IR differs is an empirical question, to which we now turn.

III. What is Known about External Counsel

A short answer to this section would be *not much*. We rely on industry reports in the knowledge that the rich internal data of market participants is often distorted by commercial interest.

a) Cyber Insurance: Research into cyber insurance often touches on the role of external counsel because cyber insurance indemnifies post-breach services including external counsel [10]. One large US insurer attributes the lower litigation rate among his policyholders (18% vs 42% industry average) to the insurer's choice of post-breach services [11]. Insurers control which service providers get work by building lists of approved service providers [11], could these lists explain the rise of external counsel managing incident response?

A survey [1] of firms in the cyber insurance post-breach ecosystem provides the opportunity for an ad hoc statistical test. The survey asks 23 law firms for the number of data breaches they managed in the past year and the number of insurers who list them as a preferred provider. To translate responses to real values, we replace any interval with its midpoint and "x plus" with x. The Spearman's rank correlation coefficient between responses to these two questions is 0.79, which is statistically significant at the $p = 0.001$ level. This suggests insurers have significant control over which law firms receive incidents.

While scepticism should be maintained given the data is self-reported and from an unknown sampling methodology, the surveyed law firms collectively dealt with over $4\,000$ incidents in a single year. For reference, the most extensive data breach study covers $6\,000$ breaches occurring across over fifteen years in the US [12]. Given the survey [1] is also US focused, this suggests lawyers are responding to a significant fraction of cyber incidents in the US. The prevalence of incident response as a lawyers' service outside the US is an open question, which we address in the next section.

While the surveyed law firms seem to rely on cyber insurers to get work, the forensic firms in the survey [1] vary more in their dependence on cyber insurance. Two examples of IR firms relying on insurers are Ankura (founded in 2014) and Arete (2015) who both report working on $3\,500+$ network security cases. Ankura also report working $3\,500+$ insurance claims and Arete say 80% of their cases come from insurance [1]. Firms who existed before the first cyber insurance firm are less dependent, such as Ernst Young (1989) and Envista (1984) with 3% and 13% of their network security cases coming from insurance respectively [1]. More generally, a study of how cyber insurance shapes incident response [10, p. 14] found that insurers favoured service-based forensics firms over firms who sell products, the former require no pre-existing access to networks and so suit hotline IR.

Moving beyond the insurance ecosystem is necessary to fully understand how external counsel shapes IR. For example, the Advisen survey [1] over samples firms who rely on insurers. We know that some law firms win work independently of insurance given that CrowdStrike report that 50% of their engagements come from external counsel while just 10% of their network security investigations come from cyber insurance [1]. Law firms not reliant on cyber insurance includes external counsel who respond to all legal issues for a client regardless of whether the case concerns security and privacy.

b) External Counsel: Insights into what external counsel does can be gleaned from annual reports [9, 8] published by Baker Hostetler, who were not part of the Advisen survey [1]. Illustrating the growth in external counsel, the reports were based on 200 cyber incidents in 2014 rising to $1\,000$ in 2019 [8]. Such reports rival many quantitative cyber risk studies in terms of data size [12] and excel in capturing emerging trends, such as the so-called ransomware epidemic. In incidents managed by Baker Hostetler, the average ransom payment went from \$29k in 2018 to \$303k in 2019, even though the majority of firms (73%) restored from back-up without paying a ransom in 2019 [8].

Despite acting primarily to defend privilege, external counsel are involved in very little litigation. Baker Hostetler dealt with just 18 lawsuits from 2018–2019 across over $1\,800$ incidents [8]. Nevertheless, privilege is important when lawsuits occur, such as the one brought by CapitalOne's customers following the firm's 2019 breach [13]. The judge ruled that the post-incident forensics report can be used by litigants. The pre-existing contract, which is common in conventional IR, with the IR firm (Mandiant) was considered to be evidence against privilege applying [13].

External counsel's legal advice primarily relates to the breached firm's duties to notify regulators and customers. The scope of these obligations can be seen in business email compromise (BEC) incidents. Adversaries compromise email inboxes primarily to launch social engineering attacks rather than to exfiltrate data. Nevertheless, an investigation to establish what personal data may have been leaked leads to notifying individuals and regulators in 90% of BEC incidents [8]. The cost of investigation and notification partly explains why the mean cost of incidents in which records were lost is over triple those in which records were not leaked across 785 cyber insurance claims in 2019 [14].

Litigation and notification services do not replace technical response—total forensic fees are more than double total external counsel fees in the average cyber insurance claim [14]. External counsel also monitor and evaluate the quality of subcontracted forensics work. Speaking to the quality of IR, network intrusion investigation costs fell by 45% year-on-year as firms shifted towards cheaper solutions like "automated triage scripts" and away from more sophisticated "imaging, log, and malware analyses" [8, p. 8].

Acknowledging that the sample of incidents are different, we can use industry reports to quantitatively compare the two models of incident response. Precise comparisons are misguided but it is telling that Baker Hostetler measure detection time in days (mean and median of around 10 and 60 days respectively [8]) while CrowdStrike estimates the industry's average detection time in hours (120 [2]). Another estimate of the industry average can be seen in Kroll, a conventional IR firm, reporting that 87% of surveyed firms contain incidents within 12 hours [15].

Although such figures are undoubtedly distorted by commercial incentives, one would expect CrowdStrike to overestimate the industry average given it provides a baseline comparison for their own detection services (which are reported in minutes [2]). Despite the incentives to inflate this figure, the average detection time is an order of magnitude lower than average time reported by the law firm [8], which suggests that hotline incident response is less responsive than the conventional model that establishes continuous monitoring that feeds into an IR plan.

The same comparison for time to investigate and time to re-mediate reveals similar results (e.g. measuring in days vs hours) [8, 2], which suggests the forensics providers hired by law firms are slower. Echoing the logic behind NIST-800-61, Baker Hostetler [8] argue that a lack of IR planning leads to inefficient investigations, with further recommendations including: longer log retention, more backup and restoration testing, and contracting providers before an incident occurs. This suggests even hotline IR firms believe in aspects of conventional incident response, such as adequate forward planning.

In summary, our survey of industry reports suggests three main findings: (1) insurers have significant influence over which law firms win work, which echoes a separate study [10]; (2) the hotline model of IR is less responsive; and (3) investigations hired by law firms are less efficient and rely on automated tools. All of these findings should be treated with scepticism as commercial surveys and reports unreliable data sources. Nevertheless, they point to interesting directions for future work to understand how external counsel influences incident response.

IV. What is Unknown About External Counsel

Throughout we have argued that external counsel provides more than just legal advice. Rather law firms are fundamentally changing how incident response is conducted. This motivates a broad research agenda to understand the following high-level topics.

a) The Demographics of Incident Response: External counsel are now managing thousands of incidents per year [1] but what fraction of total incidents does this represent? Let us call the total number of yearly incident N. We know that $N > 4\,000$ as at least this many are managed by law firms [1]. Before understanding the demographics of IR, we need a better picture of the size and composition of these N incidents. For example, search light effects lead academics to focus on the < 600 publicly reported data breaches per year [12].

One problem is that the definition of an incident is unclear. The conventional model of incident response is likely to identify comparatively more incidents because active network monitoring introduces incentives to detect as many *incidents* as possible. In contrast, the hotline model may only be engaged when firms cannot otherwise ignore the incident, such as during a ransomware infection. These distortions mean hotlines likely receive on average more harmful incidents as the benign ones would not even be detected.

A common definition would allow us to meaningfully ask what the N responses to the N incidents look like. For a sufficiently low threshold in the definition of an incident, the response will commonly be doing nothing. Active responses include: external counsel led, detection provider led, internally led or even alternative models of IR. For example, this paper has entirely overlooked public institutions like law enforcement and Computer Emergency Response Teams (CERTs) who also respond to incidents.

Mapping out the N incidents and corresponding N responses would represent a demographic survey of incident response, which seems particularly relevant as the decade of response has now passed [3]. Importantly, the demographic survey must explore regions beyond the US, which the previous section failed to do due to data availability.

We anticipate that IR as a lawyers' service will be less prevalent elsewhere because of the cyber insurance market and jurisdictional differences. First, we showed the number of relationships with cyber insurers explains the number of cases each law firm works. There is less cyber insurance outside the US [16], which is the most developed market, and so there are less insurers pushing clients towards lawyer-led IR. Second, the US may be exceptional in terms of the litigious business culture and the risk being correspondingly lower elsewhere would suggest less demand for lawyer-led IR.

This is especially true in jurisdictions where client-attorney privilege is less established (e.g. most of mainland Europe).

b) The Economics of Incident Response: The model of IR described by NIST-800-61 requires significant ex-ante investment in security, whereas calling a breach hotline and following external counsel's instructions requires no investment until an incident has been detected. Assembling IR providers post-incident would normally incur transaction costs as the victim firm searches and negotiates under the time pressure of the incident. External counsel and insurers function to reduce such costs by finding firms ahead of time and advising on quality.

So what is the result? Given the falling cost of forensics [8], the hotline model seems to be increasing access to professional IR services, which is crucial given 36% of firms have no structured incident response process in place [15]. This figure is striking given Kroll only surveyed firms with 700+ employees and "revenue of more than $500 million" [15]. Smaller firms are likely even less well prepared to respond internally.

External counsel being engaged by firms with relatively low IT maturity may explain why detection times are so high [8]. The preliminary evidence suggests that the quality of IR may be falling as providers switch to automated solutions [8, p. 8]. While automated investigations may be justified for commoditised attacks, applying such techniques to sophisticated adversaries will likely lead to botched incident response and costly re-infection.

A narrow view of incident response would blame the response firm, but a broader view sees this as a failure of the operator's ability to triage. Solving the meta-problem of matching incidents with the right service-providers will determine the success of hotline incident response. Service providers have the relatively simple task of specialising in certain incidents. The hotline operator has the devilish task of assigning providers based on oral reports about an incident and evaluating the quality of these decisions over time.

c) Legal vs Technical Risk: The proverb "to a man with a hammer, every problem looks like a nail" undoubtedly applies to incident response. Law firms extol the importance of protecting privilege, even though litigation rates are around 1% while ransomware payments grew 1000% year-on-year [8]. Perhaps re-orienting attention towards addressing technical risk is necessary during the current ransomware epidemic. This ties into the NIST-800-61 standard's recommendation to appoint a technical lead to incident response.

While legal risk can be measured via litigation rates and regulatory fines, evaluating the quality of technical incident response has been a long standing research problem [5]. Basic metrics like time to detect, investigate and remediate incidents are a starting point, with preliminary evidence suggesting external counsel led IR is lagging behind industry standards [2, 8]. Key metrics in the ransomware epidemic are recovery rate (currently 73%) and average ransom paid—both would be more favourable to victims and insurers if the quality of technical recovery services improved.

d) Local vs Global Knowledge: In shifting responsibility from an internal team to a service-provider, the response loses understanding of the victim's IT environment (local knowledge) and gains experience dealing with threat actors (global knowledge). Investigators contracted post-breach must rely on existing technology, which is often badly configured or unfamiliar [8, p. 8]. This may explain the preliminary evidence that investigations contracted by external counsel are slower than industry standards [2, 8].

External forensics firms can, however, take advantage of global knowledge related to common technology products and concentration in cybercrime operations [17]. The latter means investigators may face the same actor repeatedly, which makes automated triage scripts possible [8, p. 8]. It can also turn interactions with ransomware gangs into repeated games, which tend to have better outcomes [18]. It is an empirical question as to whether the relative increase in global knowledge compensates for the loss of local knowledge, with a well-formulated IR plan likely to optimise both.

e) The Insurance Ecosystem: Our ad-hoc statistical test shows relationships with insurers are associated with the volume of incidents a law firm has produced. Investigating how this control changes the incentives for providers is a next step for researchers given technical IR firms in this ecosystem have to satisfy two parties—the law firm who selected them and the insurer who pay their fees [10].

In terms of the ransomware epidemic, insurers may be fuelling ransom inflation by funding ransom payments [16] or they may be improving the situation by ensuring firms use professional negotiators, much like how post-breach services improved one insurer's litigation rate [11]. Further open questions include how insurers generate knowledge from incidents suffered by policyholders, and whether they provide incentives for victims to improve their security posture post-incident.

f) Mandatory Breach Notification as Policy: Policymakers pass mandatory breach notification laws and consumers receive notification, but external counsel are the sausage factories through which notifications are managed. Lawyers coordinate investigations into what data was breached, such as trawling through email inboxes following a BEC incident, and then advise on which notification laws apply. This process may explain delays in notifying individuals (approaching 3 months since compromise on average [8]) that may fall short of notification windows defined in law.

Many of these processes will be automated given the costs and time pressures of notification, but this raises two questions for policymakers: what is a tolerable level of false negatives when notifying individuals?; and, are the resources invested in notification the best way to remedy the violation of data subjects' privacy rights?

V. Conclusion

Increasingly firms, commonly cyber insurance policyholders, respond to cyber incidents by calling a hotline and delegating responsibility to external counsel. This breaks from

conventional IR's forward planning and integration with monitoring solutions. External counsel functions primarily to mitigate litigation risk by shrouding the response in client-attorney privilege, which involves sub-contracting tasks to other firms. Thus legal professionals triage thousands of cyber incidents per year [1] and match them with forensics providers. Such providers must work in unfamiliar and often badly configured IT environments due to the lack of forward planning—it is instructive that both forensics [19, p. 43] and law firms [8] operating under the hotline model recommend firms establish ex-ante plans.

This raises a set of questions about how this trend shapes incident response. Hotline IR requires less IT maturity than the ISO-800-61 standard [6], this seems to increase access but does quality suffer? Does the lack of planning lead to more costly investigations due to insufficient logs? Is this offset by specialisation gains as IR firms work similar tasks repeatedly? What would the optimal hybrid model look like? What data should firms collect to support investigations under the hotline model? Researchers should not shy away from such questions given corporate cybersecurity breaches drive financial and privacy harms to individuals at scale.

Looking forward, the centrality of external counsel to incident response could be a sign of the next decade of computer security (after prevention, detection, and response [3]). Over 40% of breaches managed by one law firm result in notification [8], which will be intensified by privacy laws like GDPR and any laws yet to be passed. Ransomware incidents require legal advice more frequently now the US treasury has issued guidance on paying sanctioned groups and ransomware gangs shift to threatening to leak stolen data [2]. The surrounding problems, such as how classification errors in algorithmic approaches to identifying leaked personal data weigh on individuals' rights to privacy, will animate research in both law and computer science.

Acknowledgments

We also thank the reviewers and Jono Spring for detailed and insightful comments. We also received useful feedback from the Cyber Insurance Special Interest Group at FIRST. 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.

Biographies

Daniel Woods (daniel.woods@uibk.ac.at) is a Postdoctoral Fellow at the University of Innsbruck in Austria. His research interests cyber insurance, risk quantification, and online privacy, all studied through the lens of security economics. He received his PhD from the Department of Computer Science at the University of Oxford.

Rainer Böhme (rainer.boehme@uibk.ac.at) is professor of Computer Science at the University of Innsbruck, Austria. His research focuses on interdisciplinary approaches to study cyber risk, cyber insurance, digital forensics, and behavioral aspects of information security and privacy. He holds an M.A. degree in communication science, economics and computer science (2003) and a Ph.D. in computer science (2008), both from Technische Universität Dresden, Germany.

References

[1] Advisen Ltd. Adivsen's Cyber Guide Available: https://www.advisenltd.com/2019-Cyber-Guide-Survey, 2019. [Online; accessed 4-Jan-2021].

[2] CrowdStrike. CrowdStrike Services Cyber Front Lines Report!: Available: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeServicesCyberFrontLines.pdf, 2020. [Online; accessed 4-Jan-2021].

[3] Bruce Schneier. The future of incident response. *IEEE Security & Privacy*, 12(5):96–96, 2014.

[4] Jonathan Michael Spring. *Human decision-making in computer security incident response*. PhD thesis, University College London, 2019.

[5] 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.

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

[7] Verizon. Incident Preparedness and Response Report: Available: https://enterprise.verizon.com/resources/reports/vipr/, 2019. [Online; accessed 1-Jul-2021].

[8] BakerHostetler. Data Security Report Incident Response Report: Available: https://e.bakerlaw.com/cv/6f9612451000150b6112e70ff680002d07ec7bae/p=8213342, 2020. [Online; accessed 4-Jan-2021].

[9] BakerHostetler. Data Security Report Incident Response Report: Available: https://e.bakerlaw.com/rv/ff00498db267a11ce4182d53934889997a36f6d4/p=8213342, 2019. [Online; accessed 4-Jan-2021].

[10] 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.

[11] Josephine Wolff and William Lehr. Roles for policymakers in emerging cyber insurance industry partnerships. 46th Research Conference on Communication, Information and Internet Policy (TPRC 46), 2018.

[12] Daniel W. Woods and Rainer Böhme. SoK: Quantifying cyber risk. In *IEEE Symposium on Security and Privacy*, pages 909–926, Oakland, CA, May 2021.

[13] Sullivan and Cromwell LLP. Federal court compels the production of cybersecurity firm's incident response report in capital one customer data security breach litigation, 2020. [Online; accessed 4-Jan-2021].

[14] NetDiligence. Cyber Claims Study: Available: https://netdiligence.com/cyber-claims-study-2020-report/, 2020. [Online; accessed 4-Jan-2021].

[15] Kroll, Red Canary, and VMware. The state of incident response 2021: It's time for a confidence

boost: Available: https://www.kroll.com/en/insights/publications/cyber/state-of-incident-response, 2021. [Online; accessed 30-Jun-2021].

[16] Jamie MacColl, Jason RC Nurse, and James Sullivan. Cyber insurance and the cyber security challenge. *Royal United Services Institute Occasional Paper Series*, 2021. Accessed: 2022-03-11.

[17] Tyler Moore, Richard Clayton, and Ross Anderson. The economics of online crime. *Journal of Economic Perspectives*, 23(3):3–20, 2009.

[18] James Carse. *Finite and infinite games*. Simon and Schuster, 2011.

[19] Crypsis. Incident Response & Data Breach Report: Available: https://start.paloaltonetworks.com/cybersecurity-threat-report.html, 2020. [Online; accessed 1-Jul-2021].