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

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

32nd USENIX Security Symposium · Anaheim, CA · 9 August 2023
“One of the most important parts of incident response [...] : learning and improving.”

NIST 800-61, p. 38

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

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

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

Knake, Shostack & Wheeler 2021 (Harvard Belfer Center)
Market Failure?

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

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

Victim firm

BP

Victim firm’s breach attorney

Privilege

DFIR provider

Work product immunity

From: Daniel Woods <daniel.w...@ed.ac.uk>
To: rainer.boehme...@uibk.ac.at
Subject: =?utf-8?B?UmU6IFVTRU5JWCBMZXNzIExvc3Qg4oCTIFRhbGsgcHJlcA==?= 
Thread-Topic: =?utf-8?B?VVNFTklYIExlc3NvbnMgTG9zdCDigJMgVGFsayBwcmVw?=
Thread-Index: AQHZxVZd51TKSxnbxUeW7uloXUL9C6/YISwR
Date: Thu, 3 Aug 2023 07:31:47 +0000
Message-ID: <PR1PR05MB559398DB2710605C3D3@uibk.ac.at>
References: <F46DC31C-AF0D-42A0-85AD-C7B7C63DBF84@uibk.ac.at>

Relevant US: “reasonably calculated to lead to the discovery of admissible evidence”

Rainer Böhme: Lessons Lost · Incident Response in the Age of Cyber Insurance and Breach Attorneys
Consequences

Reasons to keep cybersecurity efforts confidential

- Limit litigation risk
- Negative publicity
- Regulatory actions

Measures taken

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

Challenges for DFIR

- Onboard new provider during a crisis
- Mix of legal and non-legal goals
- Written reports: contents and distribution
Conventional incident response (e.g. NIST-800-61)

Hotline incident response

Role of Insurers

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

Number of DFIR and legal providers on insurers’ panels

<table>
<thead>
<tr>
<th>Company</th>
<th>DFIR</th>
<th>Legal</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIG</td>
<td>15</td>
<td>25</td>
</tr>
<tr>
<td>Chubb</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Beazley</td>
<td>17</td>
<td>13</td>
</tr>
<tr>
<td>Ascot</td>
<td>12</td>
<td>28</td>
</tr>
<tr>
<td>Axa XL</td>
<td>18</td>
<td>22</td>
</tr>
<tr>
<td>CFC</td>
<td>16</td>
<td>24</td>
</tr>
<tr>
<td>Corvus</td>
<td>14</td>
<td>26</td>
</tr>
<tr>
<td>Allianz</td>
<td>12</td>
<td>28</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Breach attorney</th>
<th>A17+18</th>
<th>A21</th>
<th>A7</th>
<th>A8</th>
<th>A9+10</th>
<th>A22</th>
<th>A23</th>
<th>A16</th>
<th>A13</th>
<th>A14</th>
<th>A12</th>
<th>A11</th>
<th>A19</th>
<th>A1</th>
<th>A4</th>
</tr>
</thead>
</table>

#### 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

---

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

---

Rainer Böhme: Lessons Lost - Incident Response in the Age of Cyber Insurance and Breach Attorneys
• Early-adopter of public cloud strategy in the highly regulated financial industry
• Major breach in 2019, exposes 30 GB of credit application data
• Technical: SSRF + AWS EC2 weakness + ability to decrypt encrypted data
• Legal: court ruled that incident report is discoverable because it was driven by business rather than legal considerations.
### Qualitative Data (cont’d)

<table>
<thead>
<tr>
<th>Breach attorney</th>
<th>A17+18</th>
<th>A21</th>
<th>A7</th>
<th>A8</th>
<th>A9+10</th>
<th>A22</th>
<th>A23</th>
<th>A2</th>
<th>A16</th>
<th>A3</th>
<th>A13</th>
<th>A14</th>
<th>A6</th>
<th>A20</th>
<th>A12</th>
<th>A5</th>
<th>A11</th>
<th>A19</th>
<th>A1</th>
<th>A4</th>
</tr>
</thead>
</table>

#### Pre-breach activities
- takes steps to establish confidentiality
- discourages activities due to confidentiality
- confidentiality protected

#### Post-breach response
- confidentiality protected
- contract forensics firm
- prefers hiring new firm
- attends 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

---

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

*There’s just less reports written than there used to be. Only the most sophisticated clients are asking for reports these days and only for the most complicated incidents.*
• Insurance improved IR planning, especially for SMEs.
• Technical best practices collide with the litigation system.
• Attorneys are not adversaries:
  the net impact of lawyer-led IR is hard to evaluate.
• However, lawyer-led IR introduces barriers to how firms (and
  the wider community) learn from security failures.
• Potential solutions are future work — see paper for avenues.
Notes on Methodology

- Multi-stage, multi-method inspired by **grounded theory** (“everything is data”)
- **~ 70 expert interviews** covering the DFIR and breach attorney markets
- Twitch validation session with Chatham House rules during the pandemic
Thank You
Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys

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

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

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

<table>
<thead>
<tr>
<th>Major driver of cyber claims</th>
<th>Personal data breach</th>
<th>Ransomware</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>early 2000s–2017</td>
<td>since 2018</td>
</tr>
<tr>
<td>Litigation risk</td>
<td>high</td>
<td>low</td>
</tr>
<tr>
<td>Legal costs</td>
<td>high</td>
<td>low</td>
</tr>
</tbody>
</table>