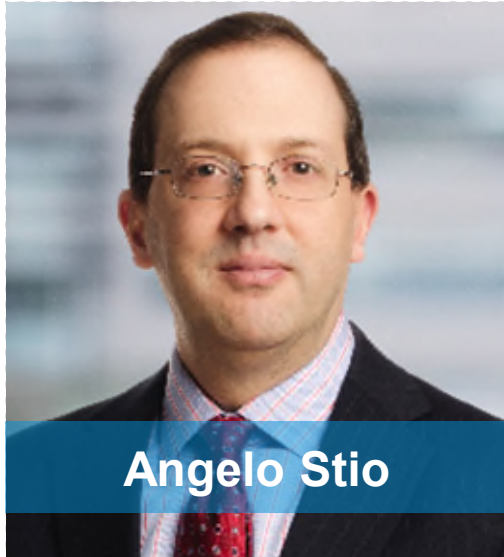


From Chaos to Control

Navigating Third-Party Breaches
and Data Ownership

KROLL

troutman
pepper



Angelo Stio

Partner, Privacy + Cyber

Troutman Pepper

angelo.stio@troutman.com

Clients in financial services and higher education rely on Angelo to handle their toughest complex commercial, privacy, and security disputes. He helps clients achieve their objectives by building a meticulous factual record and offering effective arguments throughout all phases of litigation.

Angelo has a long track record of defending clients in class actions, litigating complex business to business disputes, and handling corporate governance disputes. He is recognized as a “Local Litigation Star” by Benchmark Litigation (2019-2023); by New Jersey Super Lawyers (2011-2017) for business litigation; and in Best Lawyers in America®: Commercial Litigation (2023).

In the data privacy and security space, Angelo has defended clients in class actions and assisted business in disputes with other businesses and individuals involving privacy and technology issues.



**Global Head of Threat
Intelligence**

Kroll

keith.wojcieszek@kroll.com

Keith Wojcieszek is the global head of threat intelligence in Kroll's Cyber Risk practice, based in Washington, D.C. office. Keith joined Kroll from the U.S. Secret Service, where he served with distinction for 15 years. Keith founded and leads Kroll's Cyber Threat Intelligence program, manages a wide range of cybercrime, data loss and incident response investigations and is a trusted advisor to clients involved in compliance-related or sensitive local and global cyber security matters. He also has extensive experience working with international stakeholders on complex transnational investigations and initiatives.

In addition, Keith supervises multidisciplinary teams investigating cybercrime and data loss investigations, including but not limited to ransomware and malware, business email compromise, unauthorized access to cloud-based environments (e.g., Office 365), and vulnerabilities originating in third-party software and services. He has additionally provided consulting support on hundreds of engagements involving diverse business and legal issues, including intellectual property theft, defensible PII-PHI deletion, accounting fraud, money laundering, employee misconduct and forensic application development.



Partner, Privacy + Cyber
Troutman Pepper
sadia.mirza@troutman.com

Sadia leads Troutman Pepper’s Incidents + Investigations team, advising clients on all aspects of data security and privacy issues. She is the first point of contact when a security incident or data breach is suspected, and plays a central role in her clients’ cybersecurity strategies.

Sadia’s practice is dedicated to counseling clients on complex data security and privacy issues. Capitalizing on her extensive experience guiding clients through security incidents, she handles pre-incident planning and readiness, breach investigations, and litigation matters. Sadia leverages her 360-degree knowledge of the incident response lifecycle to ensure clients can present a positive and defensible narrative to plaintiffs or regulators.

Clients also turn to Sadia for best practices related to privacy compliance and novel data-use questions and concerns. An active and respected voice in the privacy and data security bar, she writes and speaks frequently on trends and developments affecting clients and consumers. Sadia has been a panelist on numerous privacy and cybersecurity panels across the U.S. and is a member of the Program Committee for the Law Track for the RSA Conference.

Third-Party Breaches



Third Parties: a vendor/partner or subcontractor that provides products and services to other organizations.



A Third Party's data security incident creates additional considerations for counsel and carriers.



These additional considerations are not limited to the incident response process; they extend to breach litigation and regulatory investigations.



We will discuss these additional considerations and practical ways to address them, including through the use of new technologies.

Threat Intel Briefing

troutman
pepper

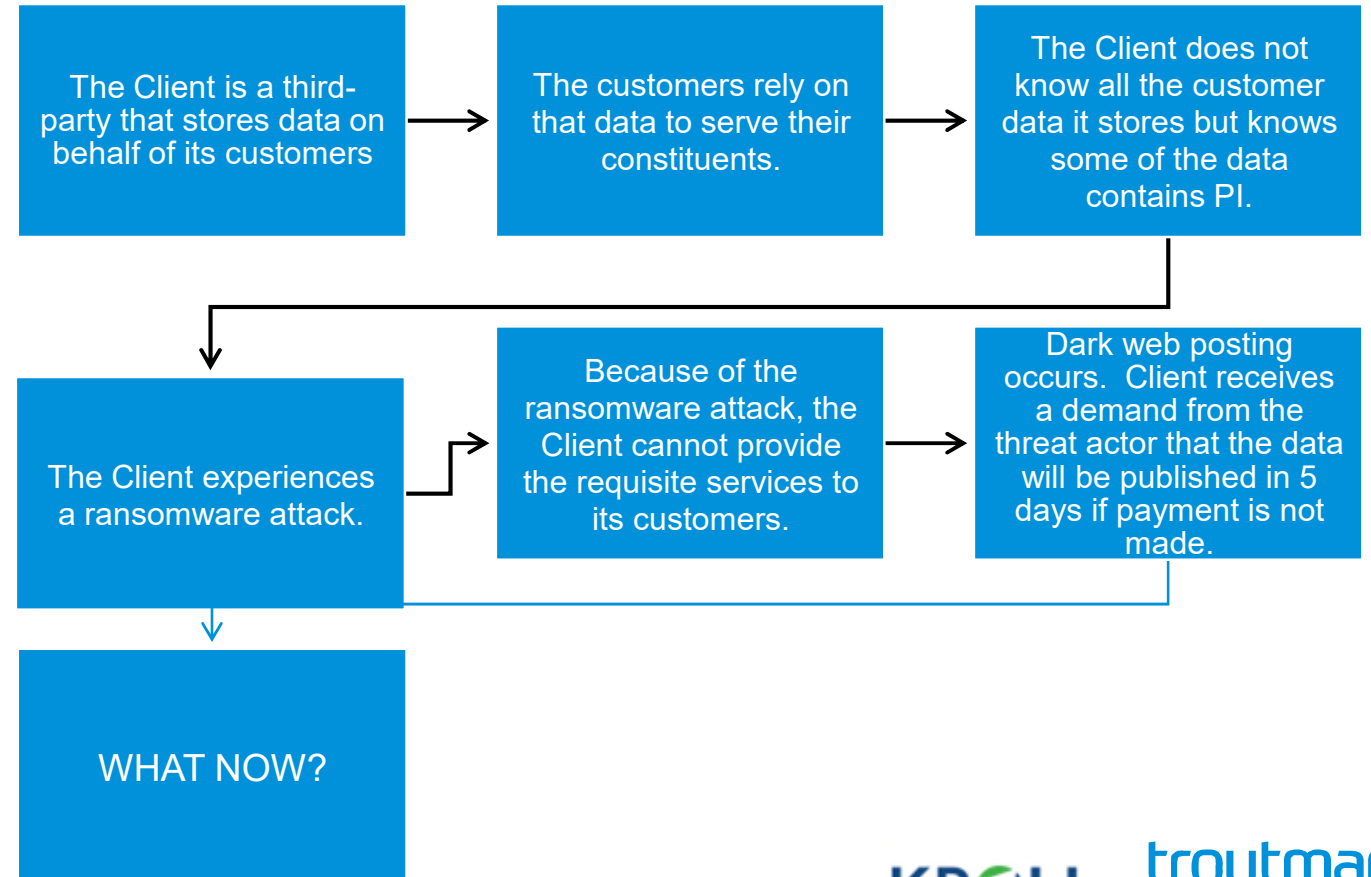
KROLL

Mock Third-Party Incident


troutman
pepper

KROLL


The Incident




Third-Party Breaches: Special Considerations




Messaging




Contract Management



Forensics and Data Mapping



Containment Decisions



Consumer and Regulatory Notifications

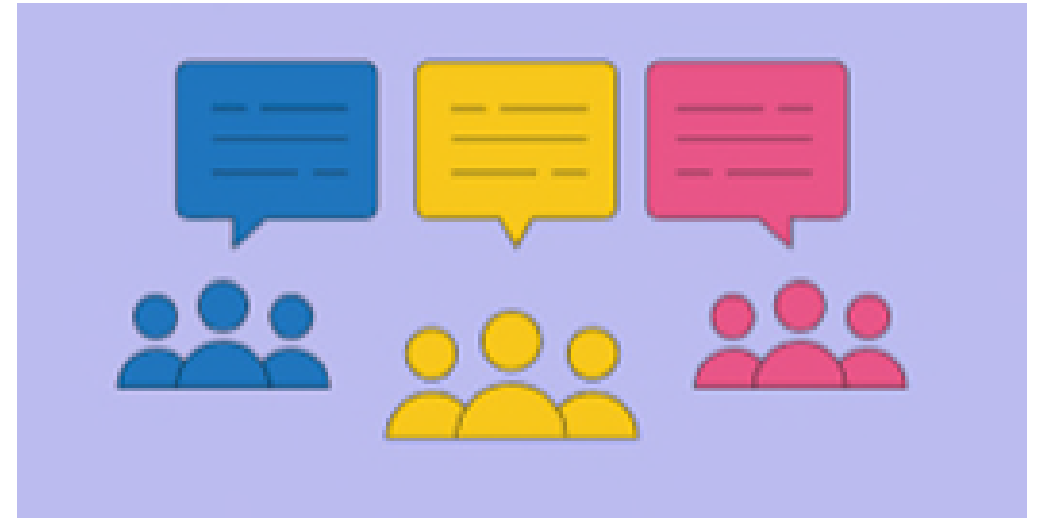


Forgotten Communication – Litigation Potholes

Third-Party Breaches – Special Considerations

Messaging

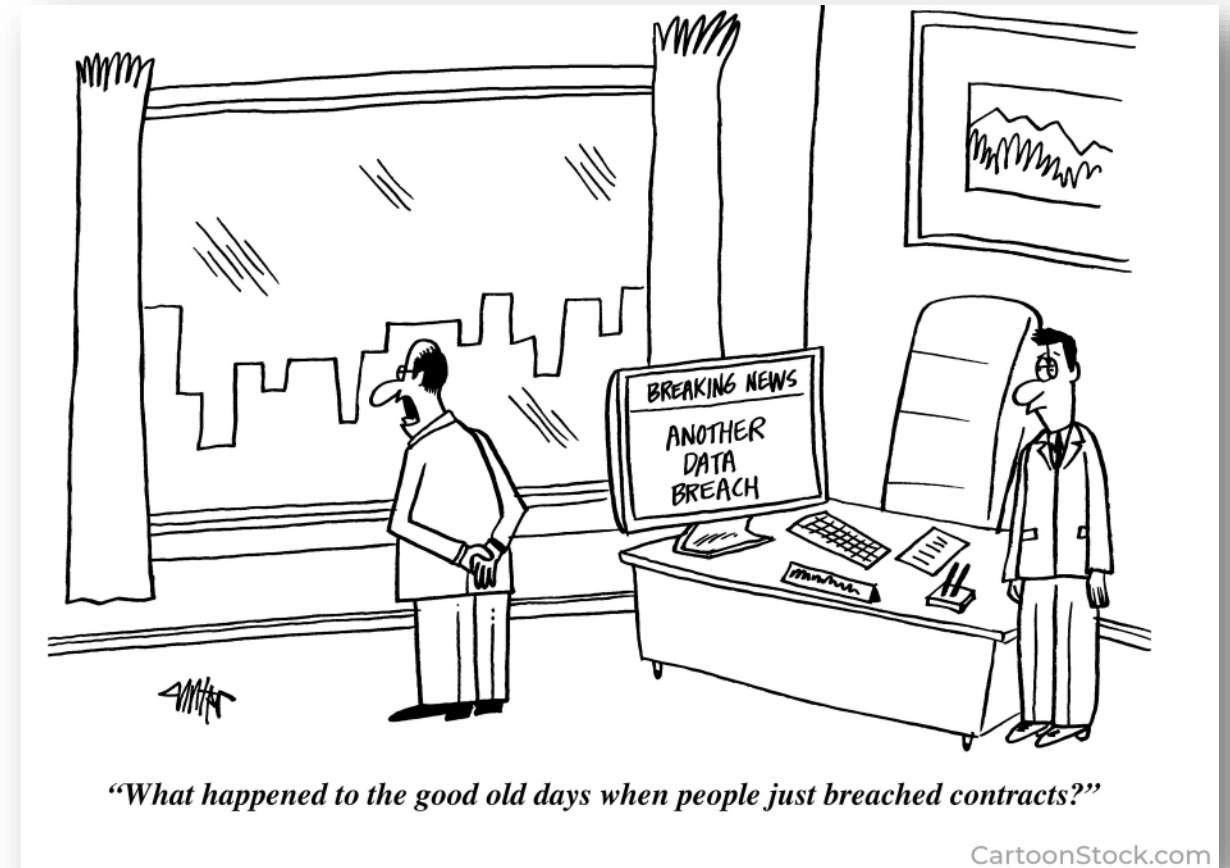
- Are you required to notify the Client’s customers directly? What about the customers’ constituents (i.e., consumers/individuals)?
- If there is no requirement, should you let customers know?
 - “Proactive” vs. “Reactive” approach
 - Pros and Cons with each approach
- How much should you tell customers about the incident?
- Litigation concerns at this stage.
- What about the dark web posting? What happens in 5 days?



Third-Party Breaches – Special Considerations

Contract Management

- Do we know all customers for whom the Client possess data potentially impacted by the incident?
- Are there contracts in place governing the data at issue?
 - Do those contracts have notification provisions?
 - Are the notification provisions the same?
 - Do those contracts have indemnity provisions?
 - Do those contracts limit the Client's downtime?
- Do we know the correct points of contact for the Client's customers.
- What are the litigation concerns from breach of contract perspective re: timing of notifications?



Third-Party Breaches – Special Considerations

Containment Decisions

- Suspending/terminating customers' access to the Client's network
 - Who decides?
 - Who bears the cost?
- Re-connecting customer's access to the Client's network
 - Who decides?
 - Who bears the cost?
 - What do customers usually ask for before reconnection occurs?



Third-Party Breaches – Special Considerations

Forensics and Data Mapping

- What happens during forensics? How do we determine what data was accessed or exfiltrated? What documentation is provided?
- Data mapping issues to consider:
 - Identify where Client stores data for each customer
 - Identify the intended fields for storing data impacted by the security incident
 - Identify how such data is stored (e.g., encrypted)
 - Identify if special software/applications are needed to access the data
 - Can the customer access that data even when the Client's network is down?



Third-Party Breaches – Special Considerations

Consumer and Regulatory Notifications

- Is there an expectation for the client to notify consumers and regulators?
- What is the process and how can third parties help facilitate that process?
- How has technology developed on this front to assist with this process?



Third-Party Breaches – Special Considerations

Forgotten Communications – the Litigation Potholes

- Internal communications (e.g., Teams, Slack, etc.)
- Communications with customers and law enforcement
- Communications with customers' constituents (i.e., individuals/consumers)
- Other discoverable communications?



What Happened to the Dark Web Post?

Our client did not pay the ransom and customer data was ultimately leaked.

- Where does it get posted?
- What do these posts typically look like?
- How is it accessed?
- How long does it stay there?
- What's the concern? How does this type of post impact us from a litigation perspective?



Summary of Special Considerations

Educate Clients about the importance of:

1. Understanding contractual obligations and how they may vary across the board from an IR perspective (notification, indemnification, liability, etc.)
2. Communications can make or break your client's incident response efforts. There is an increased expectation of transparency these days, but that must be balanced against potential litigation risk and compromising ongoing investigations.
3. Data mapping – even though Clients may not have rights to view their customers' data, they should understand how their products and services function, and what data they expect to be stored
4. Being aware of potential notification obligations early on the incident response process. Who you need to notify and how may help you determine what vendors to engage and when.
5. Developing a positive story and making decisions that are viewed as being consumer and customer friendly.



QUESTIONS?

troutman
pepper

KROLL