On July 4, 2018, social media aggregator Timehop lost a database containing about 21 million customer records. With nearly four million European customers, Timehop became one of the first to breach personal data under the new GDPR regime. The Timehop breach was stunning in its openness and detail. Nick Selby was Timehop’s incident response lead, called in just two hours after the company realized it had been breached. This talk will describe what was being discussed in the War Room: the formation of the strategy, the argument over details, the decisions about what to disclose, which all took place as the company was locking down its cloud computing environment and creating an immediate security response, and a recovery architecture; speaking with the press from the US and Europe; coordinating with local and federal law enforcement; and handling the fallout from customers while monitoring for new attacks. There were five people in the room. The breach itself was ho-hum: The cause was bad security and a 2FA mishap - Nick will discuss it. But this presentation is the exciting story of how events played out, from initial disclosure and customer reaction, to the horrifying realization that the first disclosure left out some rather key facts - kicking off another set of discussions about how to make the second disclosure. After all: if you say, “Oh, and we also lost 20.4 million dates-of-birth,” how do you answer the question that even the world’s dumbest reporters will be rightly demanding be answered: “Why didn’t you tell us this the first time, and how can we believe you’re telling us everything now?” What the company did is a model of transparency and will serve as a template of how to do it. From inviting reporters in to watch the deliberations, to the gutsy choices to release specific timelines, table schemas, IP addresses and timestamps, and continuous updates, the company won over its user base and the security company by owning it. As Timehop’s COO told NBC News, “If everybody in the world always disclosed in 72 hours, and it was routine for people to update later, it wouldn’t be so bad. But because it is so abysmal from a PR perspective to keep reporting, no one wants to be quick.” “It’s a chicken-and-egg problem,” he continued. “So we were like, ‘Screw it, I guess we’ll be the egg.’”