

Yahoo’s 10K: Lessons on What Not to Do in a Breach

Technology, Privacy, and eCommerce



In the wake of the Equifax security breach, it's hard to find any in-house counsel who isn't reviewing their respective company's data security breach management response plan. As more information has come out about the Equifax breach, to a large extent, the response among both the legal and corporate communities has been a collective wonder as to how the company could have taken so many bad turns. Yet, Equifax is far from the only company that didn't act in line with what most of us would consider best practices. If you haven't read Yahoo's 2016 10K yet, you should (especially pages 46 and 47). The 10K is full of numerous excellent lessons and, in many ways, speaks for itself.

To set the stage, Yahoo had three large-scale security incidents. The "2013 Security Incident" involved an unauthorized third party stealing one billion user accounts. Yahoo didn't disclose this until December 2016. The "2014 Security Incident" involved the theft of 500 million user accounts, possibly by a state-sponsored actor. Yahoo didn't disclose this until September 2016. Then the "Cookie Forging Activity," an unauthorized third party, accessed Yahoo's proprietary code to learn how to forge certain cookies resulting in approximately 32 million user accounts for which forged cookies were used or taken in 2015 and 2016. Again, Yahoo didn't disclose this until December 2016.

As a result, Yahoo recorded expenses of US$16 million related to the security incidents in 2016, of which US$5 million was associated with the ongoing forensic investigation and remediation activities and US$11 million was associated with nonrecurring legal costs. The damage didn't end there: 43 consumer federal and state class actions were filed against the company; a stockholder class action was filed with 10(b) and 20(a) claims against the company and some of its officers; four stockholder derivative actions brought against current and former directors and officers; and federal, state, and foreign investigations were conducted by the SEC, FTC, the US Attorney's and Attorney General's office, among others. Simply put: a complete, total, expensive, and very public mess.

The Independent Committee of the Board of Directors provided some key lessons from Yahoo's experience in the 10K.

Lesson 1: The board of directors must treat cybersecurity as an enterprise-wide risk management issue.

> "…the Company's information security team had contemporaneous knowledge of the 2014 compromise of user accounts, as well as incidents by the same attacker involving cookie forging in 2015 and 2016."

The IT department isn't the best option to manage information security, because it can disconnect the company from taking responsibility for its data and is often stretched thin from a resource perspective. By making cybersecurity an enterprise-wide risk management issue, the board can ensure that the company is protecting data in a strategic, cross-departmental, and cost-effective manner.

> "In late 2014, senior executives and relevant legal staff were aware that a state-sponsored actor had accessed certain user accounts by exploiting the Company's account management tool…. [I]t appears certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known internally by the Company's information security team."

If the board creates a system where they receive, at a minimum, quarterly updates on the status of the company's cybersecurity management programs, it can account for the company's larger ecosystem (e.g., vendors), and can encourage each department to participate in identifying high-probably and high-impact security breaches.

> "Specifically, as of December 2014, the information security team understood that the attacker had exfiltrated copies of user database backup files containing the personal data of Yahoo users but it is unclear whether and to what extent such evidence of exfiltration was effectively communicated and understood outside the information security team. However, the Independent Committee did not conclude that there was an intentional suppression of relevant information."

> "The Independent Committee found that failures in communication, management, inquiry and internal reporting contributed to the lack of proper comprehension and handling of the 2014 Security Incident."

To remedy these problems, the board will also need to seek assurances that management is taking an enterprise-wide approach to cybersecurity by creating a board-appointed cross-organization management team consisting of stakeholders from all key departments. Once the board establishes ownership of the problem, a CLO/GC (with enough resources and support), CFO, or COO can be the right senior leader to lead the cross-departmental charge. This team needs to meet regularly and develop reports to the board, conduct audits, keep updated matrices, and develop and adopt an organization-wide cyber-risk management plan and internal communication strategy. The benefit of this approach is that the team can work together to develop and adopt a cybersecurity-sufficient budget that is not tied to any one department.

Lesson 2: Legal is responsible for ensuring the board understands the legal implications of cyber risks in a context of their specific company.

“Understanding cybersecurity regulations is a simple feat,” said nobody ever.

On the federal level there is a complex mix of regulations from the SEC, FTC, FCC, Dodd-Frank, HAS, OCR, FDA, and others. Most states also have their notice of disclosure of personal information requirement with state Attorney Generals’ Offices pursuing enforcement along with state financial regulators. To make matters even more problematic, the imposing GDPR cloud is nearly upon us, and will impact on how companies collect, store, transfer, and use data of EU citizens.

Yet, the legal team will need to be at the forefront of managing any type of breach.

> “Nonetheless, the Committee found that the relevant legal team had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it. As a result, the 2014 Security Incident was not properly investigated and analyzed at the time, and the Company was not adequately advised with respect to the legal and business risks associated with the 2014 Security Incident.”

And the fallout of failing to adequately inform the board are unpleasant:

> “The Independent Committee also found that the Audit and Finance Committee and the full Board were not adequately informed of the full severity, risks, and potential impacts of the 2014 Security Incident and related matters.”
>
> “Based on the Independent Committee’s findings, the Board has taken the management related actions described below, adopted certain process and structure changes to address the Company’s issues with respect to the Security Incidents, and taken certain other disciplinary actions.”
>
> “On March 1, 2017, Ronald S. Bell resigned as the Company’s General Counsel and Secretary and from all other positions with the Company. No payments are being made to Mr. Bell in connection with his resignation.”

As part of its guidance to the board, the legal department should also consider existing insurance coverage and the company’s plans to avoid, accept, mitigate, or transfer cyber risks. A company’s cyber-risk tolerance must be consistent with its strategy and resource allocation, and it’s a good idea to address the following questions:

- What data and how much of it is the company willing to lose or have compromised?
- How does the company assess the impact if cyber events?
- How can certain cyber risks be transferred?
- How should risks be mitigated?

Lesson 3: The board must have adequate and regular access to cybersecurity expertise.

If your company's board isn't already considering doing so, adding a board member with cyber and/or IT expertise may be worthwhile. At a minimum, legal can play a key role in advising the board to schedule deep dive briefings with third-party experts, leverage independent advisors, and encourage board members to participate in education programs. The board will also need to make sure that management isn't downplaying the true state of the company's exposure and preparedness in the event of a security incident.

> "…the Board has directed the Company to implement or enhance a number of corrective actions, including revision of its technical and legal information security incident response protocols to help ensure: escalation of cybersecurity incidents to senior executives and the Board of Directors; rigorous investigation of cybersecurity incidents and engagement of forensic experts as appropriate; rigorous assessment of and documenting any legal reporting obligations and engagement of outside counsel as appropriate; comprehensive risk assessments with respect to cybersecurity events; effective cross-functional communication regarding cybersecurity events; appropriate and timely disclosure of material cybersecurity incidents; and enhanced training and oversight to help ensure processes are followed."

While there is no one-size-fits-all solution to adequately assess, prevent, and respond to a breach, the Yahoo 10K illustrates the aforementioned lessons because "hindsight is 20/20." In addition to some of the tactical considerations, Yahoo's actions demonstrate the importance of regularly reviewing your company's approach to cybersecurity to ensure it can appropriately respond to the latest threats. The key takeaway is that, across the company, communication on this topic must take place early and often to avoid the pitfalls highlighted in the Yahoo 10K.

Olga V. Mack



Fellow

CodeX

Olga V. Mack is a fellow at CodeX, The Stanford Center for Legal Informatics, and a Generative AI Editor at law.MIT. Mack shares her views in her columns on ACC Docket, Newsweek, Bloomberg, VentureBeat, Above the Law, and many other publications.

Mack is also an award-winning (such as the prestigious ACC 2018 Top 10 30-Somethings and ABA 2022 Women of Legal Tech) general counsel, operations professional, startup advisor, public speaker, adjunct professor, and entrepreneur. She co-founded SunLaw, an organization dedicated to preparing women in-house attorneys to become general counsels and legal leaders, and WISE to help female law firm partners become rainmakers.

She has authored numerous books, including Get on Board: Earning Your Ticket to a Corporate Board Seat, Fundamentals of Smart Contract Security and Blockchain Value: Transforming Business Models, Society, and Communities. She is working on her next books: Visual IQ for Lawyers (ABA 2024), The Rise of Product Lawyers: An Analytical Framework to Systematically Advise Your Clients Throughout the Product Lifecycle (Globe Law and Business 2024), and Legal Operations in the Age of AI and Data (Globe Law and Business 2024).

Katia Bloom



Commercial Lawyer and Associate General Counsel

ForgeRock

Katia Bloom is a fast-paced and strategic commercial lawyer. Currently, she is the associate general counsel at ForgeRock. Previously, she headed up legal for Avira, Inc., was a founding partner at E Squared Law Group, advising many start-up clients and was in-house counsel at Anesiva. She is actively involved in the Association of Corporate Counsel and a number of organizations promoting

women in the legal profession.