The Yahoo! debacle: Should the lawyers lead on cybersecurity protection and data breach remedial action?

December 2017

Key Takeaways

- The company's lawyers should either lead the cybersecurity effort or be closely involved, both for defences and for remedial action following breach.
- Cybersecurity is a team effort and the lawyers need to be across what others in the team are doing.
- Checklists are not enough.
- Lawyers don't need to be computer specialists to do this well.
- It's a bet the bank issue.

Speed Read


Lawyers And Data Breaches -- Why Your General Counsel Should Sit At The Crisis Management Table

Christopher P. Skroupa, CONTRIBUTOR

I focus on the intersection of government, Wall Street & main street. FULL BIO

Opinions expressed by Forbes Contributors are their own.

The General Counsel of Yahoo! lost his job this year because his legal team knew enough in 2014 to take stronger action to deal with cybersecurity breaches, including to notify the board and audit committee, but didn't act.

The Yahoo! breach affected more than a billion customers, with quantified losses of at least US$340M. While at the big end of town, this scenario raises issues just as relevant for smaller NZ companies and their lawyers.

At least one cybersecurity expert reckons the Yahoo! debacle shows that the lawyers must lead dealing with cybersecurity instead of, say, the CIO or the Chief Information Security Officer (CISO). Reasons include:

- The central role of legal issues in every facet of cybersecurity. As one expert correctly says:

> *Virtually every aspect of a data security incident response is rife with delicate and complex legal issues. The Yahoo experience and related investigative findings serve only to highlight and reinforce the critical and indispensable role of counsel. Indeed, one could argue that the Yahoo disclosures have actually set a new standard, increasing the governance and fiduciary expectations relating to the role of legal counsel when such events are encountered.... Above all else, the legal ramifications of any cybersecurity incident or failure can be calamitous or even fatal for any public or private company.*

The Yahoo! debacle: Should the lawyers lead on cybersecurity protection and data breach remedial action?

- The risk advisory role of the lawyers overlapping with close reporting lines to senior management and the boards.
- The multi-faceted nature of cybersecurity, both setting up defences and dealing with the fallout from data breaches (e.g. there's the roles of IT, Legal, HR, Finance, Board, CEO, Communications, Risk, Audit, and so on).
- The legal privilege potentially available in the lawyer-client relationship, which, as in all crisis management scenarios, may be appropriately leveraged (for example, by having remedial cybersecurity experts such as penetration testers reporting to the lawyers instead of the CIO or CISO, so that there can be confidentiality).

Other experts also see the role of the lawyers as critical and to the forefront of any response as part of the core team led by another such as the CISO.

Most experts agree that the lawyers need to be fully across cybersecurity, and that compliance checklists alone are not enough.

The Detail

Yahoo! – also a supplier dumped by Spark in May 2017 after major security problems – had two large cybersecurity breaches, one in 2013 (with 500 million customers' data records stolen) and then another in 2014 (this time over one billion customers were affected). At least in 2014, Yahoo! managers knew about the hack but took only limited steps to fix the issue and did not report this publicly until 2016.

In addition to spending US$16M to fix the problem and suffering major reputational damage, the purchase price for the Yahoo! business, then under offer from telco Verizon, dropped US$330M as a consequence.

The Yahoo! board appointed an independent committee with independent forensic and legal advice to provide a report. There was a big focus in their report on the lapses by the lawyers and also that the issues had not been escalated to the board and the audit committee. As Yahoo! reported to the market this year:

> *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.*
>
> *The Company took [limited] remedial actions. …*
>
> *[The Independent] 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… 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…*

John Reed Stark, that expert who reckons the lawyers should lead the cybersecurity effort, lists many aspects where the legal role is key to cybersecurity. Notably, even deeply tech areas buried within IT departments are in focus:[1]

> *Even the most traditional realms of IT dominion such as exfiltration analysis, malware reverse engineering, digital forensics, logging review and most technological remediation measures are rife with legal and compliance issues and a myriad of potential conflicts.*

As he says, this doesn't mean that the lawyers must have computer degrees and get into the tech detail. Like other areas of the business, they need to have or outsource some understanding of the area, with *"vigorous, sceptical, intelligent..."* review.

John Reed Stark also, correctly, sees as particularly important the role of the lawyers due to the protection of legal privilege, particularly in addressing the fallout from data breaches. As he says, there is nothing unusual or wrong about that:

> *This is standard practice in the context of any other type of investigation – a cyber incident is no different. There is nothing nefarious or extraordinary about this approach, it is a time-honored and tested standard operating procedure. The involvement of counsel establishes a single point of coordination and a designated information collection point. This model enhances visibility into the facts, improves the ability to pursue appropriate leads and, most importantly, ensures the accuracy and completeness of information before it is communicated to external audiences. Otherwise, incomplete and/or inaccurate information could be released, only to have to later be corrected or even retracted.*

Insightful also is an interview of Michael Dolan, who is both a CISO and a seasoned lawyer, in a Forbes article, *Lawyers and Data Breaches – why your General Counsel Should Sit At The Crisis Management Table*. He sees that 'quarterback' role as staying with the CISO but the lawyers having a key role in the team. He adds:

> *A long-standing challenge in this area is translating cyber-security defenses into language that demonstrates meeting regulatory expectations and legal requirements. The industry response to this challenge has traditionally been checklists—a way for legal/compliance personnel to translate requirements into "layman" terms and for IT professionals to translate technology into something others can understand upon review—but checklists alone likely aren't sufficient any more.*
>
> *One reason for this is increasing demands from securities regulators. In an increasing number of jurisdictions, boards are either expressly told that cyber security must be an issue within their oversight or it's overtly implied.*

Typically, cybersecurity is near the top of company's risk registers, or should be. So this needs close focus.

---

1. John Reed Stark, "Yahoo's Warning to GCs: Your Job Description Just Expanded (Big-Time)" (29 March 2017) (https://www.linkedin.com/pulse/yahoos-warning-gcs-your-job-description-just-expanded-john-reed-stark/)

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com