Yahoo incident reinforces vital role of counsel in cybersecurity

8 March 2017
Cybersecurity Alert

Because cybersecurity is now a board-level issue across a range of industries, Hogan Lovells wants to alert you to a recent development involving the resignation of the general counsel of Yahoo! Inc that our cybersecurity team is tracking.

It has widely been reported that Yahoo has experienced significant legal and business impacts as a result of several cybersecurity breaches. On 1 March, Yahoo disclosed the findings of an independent board committee and subsequent actions taken by the board with respect to how Yahoo responded to the cybersecurity breaches experienced by this company.

Notably, as you can read in the highlighted text from Yahoo's Form 10-K filing, the board found that, among other things, the in-house legal team at Yahoo did not sufficiently pursue the investigation of a security incident in 2014. In connection with that lack of action Yahoo has accepted the resignation of its general counsel. The CEO will forfeit her 2016 cash payout as well as her 2017 equity award and Yahoo will undertake corrective actions in how the company investigates such incidents going forward—the very last paragraph under "Excerpt from Yahoo! Inc Form 10-K Report Filed March 1, 2017:" is very useful to read in that respect.

What happened at Yahoo reinforces the vital role played by a company's lawyers to understand the organisation's cybersecurity posture and to seek the technical and other facts needed to appropriately advise and guide the company.

Hogan Lovells' top-ranked cybersecurity team is deeply experienced in helping clients structure and implement incident response plans, and offers an online resource for incident response planning at www.hoganlovells.com/readysetrespond. We would be pleased to arrange a discussion with them.

Excerpt from Yahoo! Inc Form 10-K Report Filed March 1, 2017:

Security Incidents

Description of Events

On September 22, 2016, we disclosed that a copy of certain user account information for approximately 500 million user accounts was stolen from Yahoo's network in late 2014 (the "2014 Security Incident"). The Company believes the user account information was stolen by a state-sponsored actor. The user account information taken included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with the "bcrypt" hashing algorithm) and, in some cases, encrypted or unencrypted security questions and answers. Our forensic investigation indicates that the stolen information did not include unprotected passwords, payment card data, or bank account information. Payment card data and bank account information are not stored in the system that the investigation found to be affected. We have no evidence that the state-sponsored actor is currently in or accessing the Company's network.

On December 14, 2016, we disclosed that, based on our outside forensic expert's analysis of data files provided to the Company in November 2016 by law enforcement, we believe an unauthorized third party stole data associated with more than one billion user accounts in August 2013 (the "2013 Security Incident"). We have not been able to identify the intrusion associated with this theft, and we believe this incident is likely distinct from the 2014 Security Incident. For potentially affected accounts, the user account information stolen included names, email addresses, telephone numbers, dates of birth, hashed passwords (using the MD5 algorithm) and, in some cases, encrypted or unencrypted security questions and answers. The stolen information did not include passwords in clear text, payment card data, or bank account information.

In November and December 2016, we disclosed that our outside forensic experts were investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the investigation, we believe an unauthorized third party accessed the Company's proprietary code to learn how to forge certain cookies. The outside forensic experts have identified approximately 32 million user accounts for which they believe forged cookies were used or taken in 2015 and 2016 (the "Cookie Forging Activity"). We believe that some of this activity is connected to the same state-sponsored actor believed to be responsible for the 2014 Security Incident. The forged cookies have been invalidated by the Company so they cannot be used to access user accounts.

The 2013 Security Incident, the 2014 Security Incident, and the Cookie Forging Activity are collectively referred to herein as the "Security Incidents." With respect to each of the Security Incidents, the impacted users and appropriate regulatory and law enforcement agencies have been notified.

The Company, with the assistance of outside forensic experts, has concluded its investigation of

the Security Incidents. The Company continues to work with U.S. law enforcement authorities on these matters.

Current and Future Expenses and Losses

We recorded expenses of $16 million related to the Security Incidents in the year ended December 31, 2016, of which $5 million was associated with the ongoing forensic investigation and remediation activities and $11 million was associated with nonrecurring legal costs. The Security Incidents did not have a material adverse impact on our business, cash flows, financial condition, or results of operations for the year ended December 31, 2016. However, we have subsequently incurred additional expenses related to the Security Incidents to investigate and take remedial actions to notify and protect our users and systems, and expect to continue to incur investigation, remediation, legal, and other expenses associated with the Security Incidents in the foreseeable future. We will recognize and include these expenses as part of our operating expenses as they are incurred. The Company does not have cybersecurity liability insurance.

Litigation, Claims, and Governmental Investigations

To date, approximately 43 putative consumer class action lawsuits have been filed against the Company in U.S. federal and state courts, and in foreign courts, relating to the Security Incidents. The plaintiffs, who purport to represent various classes of users, generally claim to have been harmed by the Company's alleged actions and/or omissions in connection with the Security Incidents and assert a variety of common law and statutory claims seeking monetary damages or other related relief. In addition, a putative stockholder class action has been filed against the Company, and certain current officers of the Company, asserting claims under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 and seeking class certification, unspecified damages, interest, and an award of attorney's fees and costs. Four stockholder derivative actions have also been filed purportedly on behalf of the Company against current and former directors and officers. See Note 12—"Commitments and Contingencies" in the Notes to our consolidated financial statements for additional information. Additional lawsuits and claims related to the Security Incidents may be asserted by or on behalf of users, partners, shareholders, or others seeking damages or other related relief.

In addition, the Company is cooperating with federal, state, and foreign governmental officials and agencies seeking information and/or documents about the Security Incidents and related matters, including the U.S. Securities and Exchange Commission ("SEC"), the U.S. Federal Trade Commission, the U.S. Attorney's Office for the Southern District of New York, and two State Attorneys General.

Independent Committee Investigation

As previously disclosed, an independent committee (the "Independent Committee") of the Board of Directors (the "Board") has investigated the Security Incidents and related matters,

including the scope of knowledge within the Company in 2014 of access to Yahoo's network by the state-sponsored actor responsible for the theft and related incidents, the Company's internal and external reporting processes and remediation efforts related to the 2014 Security Incident and related incidents. The Independent Committee has concluded its investigation, although it will continue to review developments regarding the Security Incidents and report to the Board on these issues, and cooperate with various government entities. The Independent Committee was assisted by independent counsel, Sidley Austin LLP, and a forensic expert. The Board has separately been advised by other outside counsel regarding the Security Incidents and recommendations regarding remedial actions.

Based on its investigation, the Independent Committee concluded that 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. 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 certain remedial actions, notifying 26 specifically targeted users and consulting with law enforcement. While significant additional security measures were implemented in response to those incidents, it 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. 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.

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. 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. 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.

Actions the Company is Taking in Response to the Independent Committee's Findings

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.

Management Changes

In response to the Independent Committee's findings related to the 2014 Security Incident, the Board determined not to award to the Chief Executive Officer a cash bonus for 2016 that was otherwise expected to be paid to her. In addition, in discussions with the Board, the Chief Executive Officer offered to forgo any 2017 annual equity award given that the 2014 Security Incident occurred during her tenure and the Board accepted her offer.

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.

Other Remedial Actions

Additionally, in response to the Independent Committee's findings and recommendations, 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.

> Read the full article online