Financial Lines | Claims trends series

Rise in cyberattacks pose increased risk for directors and officers

By:

Nima Rafiee
Senior Underwriter for
Nordics, Financial Lines
AIG

Rise in cyberattacks pose increased risk for directors and officers

Cyber is, and has been, a hot topic during the last couple of years. We have seen an increase in targeted attacks against certain individuals and organizations, but also more widespread attacks such as WannaCry and NotPetya.

We have also seen some high profile data breaches in the US. Some of these data breaches have led to shareholder claims against the company and its directors and officers, triggering the D&O policy.

With the GDPR implemented in 2018, there is a risk that boards in European companies face the same experience as their counterparts in the US, now that the data regulation in Europe is stricter than ever.

Developments in the US

In recent years, following the increase in cyber incidents and awareness from shareholders, we have started to see data breaches develop into shareholder lawsuits against listed companies and its directors and officers. **When a cyber security breach does take place, the actions of the board and senior management may be under scrutiny.** Board members may have breached their fiduciary duties to the company and its shareholders if they have failed to implement appropriate security systems and controls, or if having implemented such systems and controls, they have failed to monitor or oversee these.

It is almost inevitable, when companies experience significant losses due to cyberattacks, that criticism will be directed at the board and senior management, particularly given that cyber security is now widely recognized as a boardroom issue.

Before presenting some examples of data breaches that have led to claims against directors and officers, the background to these claims should be touched upon. **A necessary element for a successful lawsuit is a drop in stock price.** If a data breach has had no effect on stock price, then it is difficult for shareholders to claim they have suffered a loss and the claim usually gets dismissed.

This was the case in e.g. “Target, Home Depot, Wyndham Worldwide and Wendys”, cases tried by the shareholders in District Courts, where there was no dip in stock price. In these cases, the plaintiffs chose to direct shareholder derivative lawsuits. All these cases were dismissed except the Wendys case which settled before a dismissal was reached. The settlement did not involve any payment of funds to the company itself but rather involved an agreement that the company adopt certain remedial cyber security measures.

The Home Depot case was dismissed but, just like the Wendys case, ultimately settled for an agreement to adopt certain remedial measures and not to involve payment of any funds to Home Depot itself. The bar for derivative lawsuits alleging that the board has failed in its fiduciary duties is high since it is protected by the business judgement rule and shareholders must show that the board completely or consciously failed to exercise its responsibilities.

Thus, it does not come as a surprise that the plaintiffs' lawyers are now focusing on bringing securities class action lawsuits instead of derivative lawsuits and make sure that there was a stock price drop following the news of the data breach, as was the case in e.g. the Yahoo, Equifax and PayPal cases. The main issue in securities fraud litigations usually is whether the company has made a material misrepresentation or omission that deceived the market.

What companies say about data security in their financial reports, press releases and other communications is critical. Furthermore, shareholders need to show:

1) That the information provided in public disclosures before the breach was in some way misleading or erroneous.

2) That the company either withheld or was too slow disclosing the data breach after it was detected

In the US, there have been a number of shareholder derivative actions and securities-related class action lawsuits against companies and their directors and officers for alleged failure to take adequate steps to prevent a breach of the company's cyber security defenses, but also for alleged inadequate post-breach disclosures.

For example last year, shareholders filed a securities class action lawsuit against Equifax following the credit monitoring and reporting company's disclosure that it had sustained a data breach involving more than 140 million US customers. The stock price dropped almost 17 % following the announcement. Shareholders pointed to information provided by the company in the financial reports for 2015 and 2016 where Equifax disclosed that it developed new technology to enhance the security of the services it provides. The class action complaint alleged that the company failed to monitor its systems to detect breaches, failed to maintain proper security systems and controls and failed to protect its data. Equifax has filed a motion to dismiss to the federal judge and is waiting for a decision.

In 2018, Yahoo settled a data breach-related securities class action lawsuit for $80 million. Yahoo's proposed settlement came soon after the SEC provided new guidance that requires public companies to be more forthcoming when informing the market about cyber risks and incidents. Following the series of breach related disclosures by Yahoo, the stock price dropped by more than 30%.

Intel Corp. stock price fell over 3 % following news about a security flaw in its computer processor chips and Intel Corp. admitting that the chips are susceptible to hacking. In a securities class action lawsuit, the plaintiffs allege that they bought shares during the class period based on artificially inflated prices relying on previous statements from Intel Corp. which failed to mention the security flaw.

PayPal also faced a securities class action lawsuit following information from the company in 2017 about potential compromise of 1.6 million customers' personal identifiable information. The plaintiffs alleged, among other things, that PayPal provided misleading information and failed to disclose that the data security program was inadequate to safeguard sensible information and that these vulnerabilities threatened the continuing operation of the specific platform, thus potentially having a negative effect on revenue. The defendant's motion to dismiss was granted by the court as the judge ruled that the plaintiffs' allegations, among other things, failed to satisfy the scienter of the falsity upon which their alleged loss was predicated.

Finally, on November 30th, 2018, Marriott disclosed that a huge breach in its acquisition Starwood's guest reservation system had occurred and that hackers had stolen information about 500 million guests. One day later, on December 1st, 2018, plaintiffs filed a securities class action lawsuit against Marriott, the CEO, the CFO and the Chief Accounting Officer. The class alleges false and misleading statements in SEC filings with regard to cyber security. The stock price dropped 5.5 % following the news of the breach.

Developments outside the US

In 2018, we started to see cyber related securities class action lawsuits outside the US. Shareholders of Chinese hotel group Huazhu recently filed a securities class action in connection with a stock drop following a cyber breach. When the news of the breach of 500 million records of personally identifiable information reached the media, the company's share price immediately dropped over 4 % and continued to drop in subsequent days, according to the lawsuit. The lawsuit, which is filed on behalf of those who acquired the company's stock between May and August 2018, alleges that the company "failed to disclose material adverse facts about the company's business," including that it "lacked adequate security measures to protect customer information". These are similar arguments to those brought by the shareholders of Equifax.

British Airways is threatened with a class action lawsuit by a UK law firm, under the GDPR, following news that payment card data connected to 380,000 transactions had been stolen. British Airways have offered to reimburse those customers that suffer a direct financial loss. However, under the GDPR, the customers have a right to compensation for non-material damage such as inconvenience, distress and annoyance linked with the data breach. The fact that companies subject to the GDPR have to compensate for non-material damages increases the risk of a stock price dip following news about a data breach since it means that a data breach will probably cost a company a substantial amount of money in defense, rectification and/or settlement. British Airway's owners, International Airlines Group, stock price dropped 4 % following the news of the breach.

In the Nordics, we should not be surprised if we within soon start seeing cyber related securities class action lawsuits. They might be smaller in size than in the US, but that is more related to the fact that **in the Nordics you have to "opt in" in order to be part of a class action while in the US you usually have to "opt out" of a class action.**

We know that data protection authorities in the Nordics have staffed up during 2018 and are focusing on taking corrective actions against companies. The GDPR is already beginning to show its strength with fines imposed by data protection authorities in Austria, Portugal, Germany and Norway. Although these fines have been quite small in size, there is nothing to rule out the introduction of more sizeable fines within soon.

It remains to be seen if a major data breach in the Nordics will affect the stock price of the affected company and if shareholders will try to hold the company and its directors and officers accountable for potential losses incurred.

The recent developments in Level I ADR exposures which we presented in an article last year (read here), coupled with the data breach related exposure presented in this article, most certainly present a new headache for directors and officers in Nordic public companies.

What do these developments potentially mean for D&O underwriting?

Recent years have seen an increase in event-driven lawsuits filed by a handful of "emerging" law firms who are responsible for the significant part of the increased volume of securities class action lawsuits in the US. A quick lawsuit following news of a cybersecurity incident is regarded as an event- are not always particularly well formulated, so the success rate of these might be lower than more traditional lawsuits. However, these event-driven lawsuits trigger defense costs which a standard D&O policy would pick up - leading to increased costs both for insureds and insurers which has been evident in recent years.

For D&O underwriters, it would be prudent to pay specific attention to the cyber exposures of the client, especially those that are publicly traded and have a wide geographical footprint. It could be wise to touch upon cyber specific questions during the underwriting process to understand how clients work with cyber security, what their main concerns are, how and what they disclose about cyber security and how often cyber topics are included in the board agenda.

Risk and insurance managers may want to highlight to their boards the recent cyber related D&O claims. If the board can show that it takes cyber security seriously and that there are robust defenses and strong disclosure procedures in place, then the board has come a long way limiting its members' personal liability.

It is important to work on disclosure procedures both pre and post breach. Pre breach concerns information provided in financial reports, on webpages and in press releases while post breach touches upon how and when a company informs the market about a suspected or actual breach. The post breach disclosure process is delicate. Informing the market about a breach as early as

possible is vital. If the company takes too long to disclose information to the market about a data breach, the class period is extended which could lead to more plaintiffs in a potential securities class action lawsuit.

Some clients have purchased cyber insurance to demonstrate their commitment to cyber security, but that alone is not enough to support an argument that you have adequately handled your cyber exposures.

AIG, as a market leader on D&O insurance, often sees the overall trends developing and has the ability to act accordingly. With our leading position and long history, we have great experience in defending directors and officers against claims, regardless of the complexity and size.

With the GDPR implemented in 2018, and the increase in cyber related securities class action lawsuits, both in the US and outside of the US, the need for experienced D&O claims handling is more important than ever.

Whereas in recent years D&O insurance occasionally has been seen as a commodity product, the risk of large and complex lawsuits against individuals, connected to the increasing number of cyber-attacks and data breaches, is expected to change the view on D&O insurance.

Going forward, we expect to see much more emphasis being laid on the actual experience of the D&O insurer to defend the insureds in these types of claims compared to recent years' focus on coverage and premium, taking D&O insurance back to the core of its purpose.

For more information about increased exposure for directors and officers, please read our article about ADR's released in November last year.

AIG Europe

AIG Europe S.A. is an insurance undertaking with R.C.S Luxembourg number B 218806.

AIG Europe S.A. has its head office at 35 D Avenue J.F. Kennedy L-1855, Luxembourg.

Denmark

AIG Europe S.A., Danish branch office of AIG Europe S.A. Luxembourg, has its registered branch office at Osvald Helmuths Vej 4, 2000 Frederiksberg.

Branch registration number CVR nr. 39475723 | Telephone: (+45) 91375300 | Fax (+45) 33732400

Finland

AIG Europe S.A., Finland branch office has its registered branch office at Kasarmikatu 44, 00130 Helsinki, and branch registration number CVR-NR 2922692-7. Tel: + 358 20 7010100.

Norway

AIG Europe S.A., Norway branch office of AIG Europe S.A. Luxembourg | Rosenkrantz' Gate 22 | P.O. BOX 1588 Vika | NO-0118 Oslo | Telephone + 47 22 00 20 20 | Telefax: + 47 22 00 20 21 | www.aig.no

Sweden

AIG Europe S.A. Filial i Sverige är en svensk filial av AIG Europe S.A. i Luxembourg.

Adress: Västra Järnvägsgatan 7, 8 tr.| Box 3506 | 103 69 Stockholm | Org. nr. 516411-4117 | Tel. (+46) 8 506 920 00 | Fax (+46) 8 506 920 90