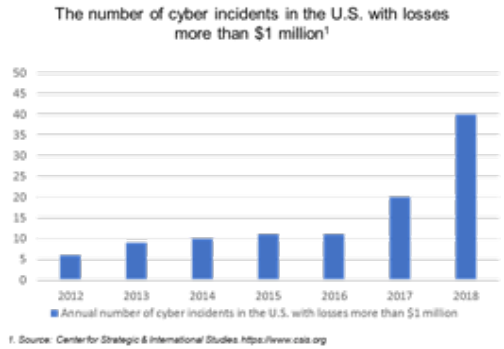
Client Alert – Cyber Risk is D&O Risk

Much has been written about cyber risk's impact on Directors' & Officers' ("D&O") risk, and evidence suggests it is evolving. While a historical perspective may suggest that cyber risk was predominately a personally-identifiable information ("PII") risk, more recent developments provide examples of business interruption losses stemming from cyber risk, which additionally manifests in claims relating to regulatory responses and shareholder litigation. The combination of these emerging developments is increasingly relevant to corporate boards and leaders, as the nature of cyber risk grows and evolves.

Fundamentally, the escalating nature of cyber risk can be segmented into two trends. First, the number of cyber incidents is increasing according to the Center for Strategic & International Studies[1]. The frequency of significant incidents has grown nearly eight-fold since 2012. Second, the reliance of business upon technology and the Internet of Things is growing. The amalgamation of these two trends can be significant, and can include reputational harm, financial loss, and legal costs. Given the growing frequency and potential harm to both consumers and the organization, it is no surprise that both regulators and investors have reacted to this exposure, as exemplified in the following summaries.



Looking Back – Regulatory Responses (GDPR)

On May 25, 2018, the European Union General Data Protection Regulation ("GDPR") took effect in European Union ("EU") member states. The GDPR already has had significant impact on companies that serve EU residents, and the regulation is expected to significantly increase exposure to directors and officers of those companies operating in the EU, as well as those companies that have compliance obligations as a result of processing or controlling covered data.

What is the GDPR?

The GDPR impacts organizations around the world that handle the personal information of individuals residing in the European Union, regardless of where the organization is physically located or domiciled. As the regulation imposes significant obligations and possible fines for non-compliance, it creates new challenges for global organizations.

The GDPR applies globally to organizations that process the personal data of individuals in the EU in the context of offering goods or services or monitoring behavior, regardless of where the actual processing takes place. It applies to information which directly or indirectly identifies an individual, including but not limited to customer lists, contact details, genetic/biometric data, and online identifiers like internet protocol addresses.

What are some of the requirements of the GDPR?

The GDPR contains several requirements for businesses, including:

- Only collect personal data needed to fulfill specific, documented purposes, and where there is a permitted basis under the GDPR for the collection.

We're here to empower results

If you have any questions about your specific coverage or are interested in obtaining coverage, please contact your Aon broker.

www.aon.com

[1] *https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity*

Empower Results®

- Embed privacy controls into operations and implement mandatory privacy-risk impact assessments for any new project likely to result in a high risk to individuals' privacy.
- Appointment of a Data Protection Officer with expert knowledge for public authorities, organizations processing large amounts of special categories of data, or whose core activities involve the regular and systematic monitoring of individuals.
- 72-hour notification requirement for all personal data breaches to the relevant supervisory authority, except those which are unlikely to pose a risk to individuals. In the case of serious incidents, there will also be a duty to notify the affected individuals of the breach.

What are the enforcement measures? Are there associated fines?

In case of non-compliance with the GDPR, the regulator may impose fines up to € 20 million or 4% of an organization's annual global turnover, whichever is higher. The GDPR also allows the regulator to enforce compliance regardless of whether a breach of network security or privacy occurred and EU citizens have a private right of action under the regulation.

GDPR Conclusion

The GDPR was intended to safeguard private information, and it was anticipated that it could lead to an uptick in regulatory actions related to the failure to comply with GDPR and more complaints resulting from breaches of privacy. It is certainly possible, even likely, that these types of claims may arise. The GDPR is just one signal of regulators' intense focus on cybersecurity and privacy compliance initiatives; other examples include the U.S. Securities & Exchange Commission's Cybersecurity Disclosure Guidance, as well as the California Consumer Privacy Act, which will be effective in January 2020.

Looking Back – Regulatory Responses (U.S. Securities & Exchange Commission)

On February 21, 2018, the U.S. Securities & Exchange Commission ("SEC") released its Cybersecurity Disclosure Guidance ("Guidance"). The Guidance is intended to provide suggestions for public companies when preparing disclosures about cybersecurity risks and incidents and communicates the SEC's views on the importance of maintaining comprehensive policies related to cybersecurity. We believe the Guidance aligns an SEC focus area with the emerging trend that "Cyber Risk is D&O Risk."

From the Guidance, several recommendations and observations relevant to D&O Liability Insurance emerge:

Carefully Determine Materiality Specific to Your Organization - The SEC disclosure requirements cite "materiality" as the threshold for determining whether any matter, including a cyber incident, must be disclosed to an investor. The SEC reminds companies that it must tailor its disclosures to that company's particular cybersecurity risks and incidents, further mentioning that companies should avoid generic cybersecurity disclosures. The SEC also identifies several accommodative considerations with regard to materiality determination, including the recognition that companies are not expected to disclose information that could compromise its cybersecurity defenses, that it may take time for a company to evaluate an incident and determine materiality, and that required cooperation with law enforcement may affect the scope of disclosure.

Timely and Comprehensive Disclosure is Critical - The Chairman of the SEC, Walter Joseph Clayton III, noted in the Guidance that timely reporting is expected. "Where a company has become aware of a cybersecurity incident or risk that would be material to its investors, we would expect it to make appropriate disclosure timely and sufficiently prior to the offer and sale of securities..." The SEC further affirmatively states that ongoing investigations – both internal and external – do not, on their own, provide a reason for companies to avoid timely disclosure of a cybersecurity incident.

Ensure Board Oversight of Cybersecurity - The Guidance reminds companies that, "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company." The Guidance further advises that, particularly at those companies where cybersecurity risks are material to a company's business, companies should disclose the nature of the

board's involvement with oversight of cybersecurity. These specific comments by the SEC, along with prior litigation targeting the directors and officers of companies with cybersecurity breaches, highlight the importance of board engagement with cybersecurity.

Insider Trading and Cybersecurity Intersect - The Guidance reminds companies that issuers, their directors and officers, and other insiders must comply with trading rules regarding material non-public information, which can include information related to cybersecurity incidents as well as vulnerabilities. The Guidance reminds issuers that it is illegal to trade securities, "on the basis of material nonpublic information about that security or issuer, in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively, to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information." The Guidance cautions companies to avoid even the appearance of insider trading by implementing stricter disclosure and insider trading protocols.

SEC Guidance Conclusion

Public company directors and officers have a duty to understand the ramifications of cybersecurity on their business, and to proactively design risk mitigation procedures and internal disclosure guidelines specific to their company's unique cybersecurity needs. Further, it is believed that the potential for insider trading based upon knowledge of cybersecurity incidents is firmly within the SEC's crosshairs, and possible cause for further corporate governance focus. The SEC's recent Guidance on the cybersecurity topic is believed to signal a growing and continued focus on this matter and serves as notice that all companies must be prepared.

Looking Back – Investor Scrutiny

Event-Driven Litigation ("EDL") is a significant exposure for corporate leadership. Several types of EDL have emerged as common sources of litigation, including:

- Product failure / bodily injury arising from products
- Harassment / #MeToo movement
- Cybersecurity and cyber incidents

Cyber incidents are particularly fertile ground for the new wave of class action securities claims arising from claims of corporate mismanagement, some of which are in response to breaches and privacy violations under the GDPR. In one example of litigation arising from a cyber breach, the securities class action seeks to recover damages for alleged violations of the federal securities laws claiming that throughout the class period the company made materially false and/or misleading statements and/or failed to disclose that its end users had their personal information exposed. Further allegations include that the company actively concealed this data breach for several months, violating the company's purported data privacy and security policies. The complaint goes on to allege that the discovery of the wrongdoing could foreseeably subject the company to heightened regulatory scrutiny and that prior public statements were materially false and misleading. Following a major media outlet's article exposing the private data of hundreds of thousands of users, the company's stock price fell.

Following is a high level summary of other litigation examples:

Filing Year	Industry	Overview	Status
2018	Hospitality	• Hackers breached company's guest reservation system and stole the personal data of millions of guests. They had multiple years of unauthorized access. • Securities Class Action lawsuit filed shortly after breach was announced.	*Pending*
2018	Technology	• Unauthorized party gained access to a company database that hosts user data, resulting in a drop of company shares and a Securities Class Action filing	Voluntarily dismissed *2019*
2018	Technology	• Data breach was discovered that exposed the personal data of over half a million users • Two Securities Class Action lawsuits filed in Fall of 2018	*Pending*
2018	Technology	• GDPR-related changes affected the company's growth rate, resulting in material stock price drop • Securities Class Action filed Summer of 2018	*Pending*
2018	Technology	• Allegations include failure to disclose impact of GDPR • Announcement led to notable decline in market capitalization • Securities Class Action filed Spring of 2018	*Pending*
2017	Financial Institutions	• Hackers breached company's database and accessed millions of records containing personally identifiable information • Securities Class Action filed in Fall 2017	*Pending* In 2019 a dismissal motion was denied and granted in part
2017	Technology	• Data breach resulting in the theft of personal user data due to failure to encrypt users' personal account information • Nine figure purchase price reduction following two breaches • Securities Class Action filed Winter 2017	*2019* Eight figure securities claim settlement *2018* Eight figure derivative settlement
2016	Food/ Agriculture/ Beverage	• Malware, which had been installed through the use of compromised third-party credentials, affected sales systems. Later, another data breach was detected, and company concluded that more than 1,000 locations were affected. • Derivative suit arising from a data security breach filed in Winter 2016	Settlement includes cybersecurity changes, corporate governance therapeutics, and six figure plaintiffs' attorneys' fees *2018*
2014	Retail	• 56 million customer credit cards breached • Breach-related derivative lawsuit filed the following year	Settlement includes corporate governance reforms and up to seven figures in $1.125 million of plaintiffs' attorney's fees *2017*
2008	Hospitality	• Three data breaches over multiple years which resulted in the compromise of more than 619,000 consumer payment card account numbers and eight figure fraud losses • Derivative suit filed • Largely viewed as a "road map" to successful defense	*Dismissed* *2014*

While the track record of successful litigation arising out of cyber incidents (as far as surviving the motion to dismiss) is mixed, it is expected that the plaintiffs' bar and aggrieved investors will continue to pursue companies that experience cyber incidents. Those cases are likely to include allegations of wrongdoing against the leadership of those companies and damages may include remediation costs, business interruption loss, and reputational harm.

Looking Forward – 2019 and Beyond

Companies continue to face ever-increasing regulation around privacy and cyber security. Most notable are California's new laws around privacy and connected devices. As we saw with California's 2002 data breach law, other states tend to follow California's lead around regulation. The potential for corporate liability around these regulations remains yet unseen, however it is an area that we believe to be ripe for potential litigation from a D&O perspective.

Privacy Rights: The California Consumer Protection Act

In 2018, California passed the California Consumer Privacy Act ("CCPA"), AB 375, effective January 1, 2020. Like the GDPR, the CCPA provides Californian consumers expanded privacy rights and greater control over their own data, while imposing potential civil penalties and statutory damages for noncompliance. However, as of May 2019, many aspects of the law are still subject to change via several proposed bills. Some of these bills seek to strengthen the rights of California consumers, while other seek to revise the language of the regulation to be more commercial for California businesses.

What is applicable under the CCPA?

The CCPA applies to any company doing business in California, or that collect information on California residents, who meets one or more of the following:

1. More than $25,000,000 USD in annual gross revenue
2. Buy, receive, sell or share the personal information of 50,000 or more consumers or devices
3. Derive 50% or more of their annual revenue from selling consumers' personal information

The CCPA also redefines and expands "personal information" to include biometric data, browsing history, and commercial information such as purchasing histories, geolocation data, IP address information, etc.

What are some of the rights under the CCPA?

- Right to deletion – California consumers may request of businesses to delete their data, or "opt -out" of the sale of their data.
- Access and required response – businesses will have to disclose what personal information is being collected and how it's used within 45 days of a verifiable request from a consumer. This includes providing the categories of third parties with whom the data has been shared.
- Notice and consent – the law requires company websites to add a clear link titled "Do Not Sell My Personal Information" to further assist consumers who want to exercise their "opt-out" rights
- Mandated "opt-in" before sale of children's information (under the age of 16).
- Private right of action for data breaches.

What are the enforcement measures and possible penalties?

The law includes both civil and statutory penalties. Any person, business or service provider that intentionally violates the bill may be liable for up to $7,500 per violation enforced by the Attorney General, though the law does not describe what constitutes a "violation". Consumers now are also allowed to bring a private action, but only related to security breaches that meet specific criteria. Recoverable damages amount to not less than $100 and not greater than $750 per consumer per incident.

Cybersecurity Law and the Internet of Things

California has also introduced an Internet of Things (IoT) law, SB 327, which is also effective on January 1, 2020. This law applies to manufacturers and component part suppliers of connected devices sold in California and requires that they have "reasonable" security features. These features are intended to prevent unauthorized access of the device by setting a unique password or changing the default password. However, guidance suggests that the law is intended to be intentionally vague, as the "reasonableness" of security features may vary be device. This law is intended to be enforced by the California Attorney General, and there is no private right of action. While we have not seen other states pass laws similar IoT laws, there have been several IoT-related bills that have been introduced on a federal level, however none have made it to a vote.

The Regulation Will Not Stop

Given that California is the largest state economy in the U.S. and leverages great influence, companies need to prepare themselves over the next year to address the CCPA. Since California passed the CCPA in 2018, 15 other states have introduced similar privacy legislation. We believe that additional regulation – both as respects privacy and cyber security – is on the horizon, with additional regulators soon to join the mix, perhaps even on a federal level.

Conclusion

Cyber risk is, indeed, D&O risk, as companies becoming increasingly reliant upon technology and cyber incidents continue to grow in frequency. Both regulators and investors have responded to cyber incidents that result in reputational, business, and financial harm. The examples of these responses are already plentiful and expected to grow over time.

About Aon's Financial Services Group

Aon's Financial Services Group is the premier team of executive liability brokerage professionals, with extensive experience in representing buyers of complex insurance products including directors' and officers' liability, employment practices liability, fiduciary liability, fidelity, and professional liability insurance. FSG's global platform assists clients in addressing their executive liability exposures across their worldwide operations. Aon's Financial Services Group manages more than $2.4 billion in annual premiums, assists with annual claim settlements in excess of $800 million, and uses its unmatched data to support the diverse business goals of its clients.

AON
Empower Results®