UNIVERSITY OF PUERTO RICO BUSINESS LAW JOURNAL

VOLUME XVII
NUMBER 1
2026

VOLUME XVII **2026** **No.1**

VOLUME XVII **2026** **No.1**

Reshaping Corporate Risk: Liability of Directors and Officers for Cyber Breaches and Its Effect on Insurance

*Linette M. Vega Ortiz**

Table of Contents

I. Introduction

It is easier to see the effects of catastrophes, such as hurricanes, explosions, tornadoes, and earthquakes, because of the imagery they generate at the time. The disaster is evident, and the public can easily see its destruction. However, it is not that easy to see the immediate effects of a cyber incident. This type of incident can cause massive destruction to a business and, depending on the magnitude, a country. If a simple technology glitch can halt operations of an entire state and industry, think about the devastating consequences of a cyber-attack to the most vulnerable data.[1] This destruction can cause damage directly to the target itself, such as an unauthorized release of proprietary information and trade secrets, or indirectly by affecting third parties, such as the release of personal data. "If our security measures are breached, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure."[2] A cyber incident can

* La autora es abogada con más de quince años de experiencia en las áreas de seguros, cumplimiento regulatorio, litigación y asesoría corporativa. Cuenta con una amplia trayectoria en corredores de seguros y aseguradoras multinacionales, liderando iniciativas relacionadas con responsabilidad profesional, litigios, asuntos laborales, cumplimiento normativo y asesoría legal para operaciones de seguros en diversos mercados de Puerto Rico, América Latina y el Caribe. Obtuvo un Bachillerato en Artes de la Universidad de Puerto Rico, Recinto de Río Piedras, graduándose Magna Cum Laude. Posteriormente obtuvo el grado de Juris Doctor de la Escuela de Derecho de la Universidad de Puerto Rico, donde se graduó Magna Cum Laude, y una Maestría en Derecho (LL.M.) con concentración en Derecho de Seguros de la University of Connecticut School of Law. Está admitida al ejercicio de la abogacía y la notaría en Puerto Rico.

[1] Brian Fung, *We Finally Know What Caused the Global Tech Outage - and How Much it Cost*, CNN (July 24, 2024), https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html.

[2] Bressler, Amy & Ross, P.C., *SEC Fines Yahoo! Inc. $35 Million for Failure to Report Cybersecurity Breach,* BRESSLER AMERY & ROSS (May 1, 2018), https://www.bressler.com/sec-fines-yahoo-inc-35-million-for-failure-to-report-cybersecurity-breach.

also cause a business to lose income and incur additional expenses. For instance, during a denial-of-service ransomware attack, a company is pressured to pay to regain access to its own systems. During this interruption, the company is unable to provide services to clients and must incur additional expenses to continue operating. These incidents can be the end of an organization if it lacks adequate cyber risk management tools and protocols.

According to the International Business Machines Corporation's (IBM) Cost of a Data Breach Report of 2024, the global average of a data breach is $4.88 million.[3] The average cost of a data breach jumped to "…a 10% spike and the highest increase since the pandemic."[4] Of these, 46% of breaches involved customer personal data.[5] "Cyber incidents are growing in frequency and severity. Enforcement, too, is ramping up. The D[epartment] o[f] J[ustice], F[ederal] T[rade] C[ommission], and S[ecurity] E[xchange] C[ommission] are all involved in investigating potential violations of law following cyber incidents and prosecuting companies who fail to protect data."[6] Because of the increasing liability that cyber incidents pose to companies, executives are growing more concerned about these risks, particularly given regulatory intervention, shareholder concerns, and plaintiff cases affected by them. The plaintiffs in these cases "…have shown willingness to pursue individual directors following an incident."[7] These types of claims show an evolving trend in corporate liability toward including personal liability.

In the current era of advanced technology and the growing use of artificial intelligence, it is almost impossible to affirm that any company, in any industry, is immune to a cyber threat. There are cyber exposures in the ordinary course of business. Important examples are seen in day-to-day technology, supply chain security, mergers and acquisitions, business transactions, the Internet of Things (hereinafter "IoT"), and, in general, employee access to systems.[8] Whether directly or indirectly, cyber exposure exists for all types of organizations, and their officials must take affirmative actions to manage and control this risk. To "mitigate

---

[3] IBM & Ponemon Institute, *Cost of a Data Breach Report 2024*, (July 2024), https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf.
[4] *Id*.
[5] *Id*. at 6.
[6] Lorelie S. Masters, Esq. *et. al.*, *Cyber and D&O insurance: Maximizing Coverage for Companies and Executives from Cyber Incidents*, 2023 PRINDBRF 0458 (Westlaw).
[7] *Id*.
[8] Aon plc, 2019 *Aon Cyber Security Risk Report*: *What's Now and What's Next* 4-13 (Feb. 2019), https://www.aon.com/getmedia/4c27b255-c1d0-412f-b861-34c5cc14e604/Aon_2019-Cyber-Security-Risk-Report.aspx.

that risk, corporations must exercise constant vigilance over their fast-changing enterprise cyber risk profiles–from the boardroom to the supply chain, and from IT infrastructure to every other facet of business operations."[9] Therefore, adequate cyber risk management controls must be implemented and enforced by a company's directors and officers as part of their primary duties. Otherwise, directors and officers may face additional liability for failure to take appropriate, commensurate actions to mitigate a continuously evolving risk. This is where adequate insurance coverage is crucial as a risk management tool, as liabilities continue to arise. Unlike ordinary course of business insurance, specifically referred to as property and casualty insurance, cyber and D&O insurance are types of professional liability insurance, and their focus is on covering non-tangible losses. This loss does not create visual imagery like a catastrophic hurricane or an explosion, but the consequences are just as fatal if not managed adequately.

The following analysis examines the current shift in corporate risk, emphasizing evolving trends in cyber risk and the measures that corporations and their executives must take to minimize or prevent this exposure. It will introduce the background of directors' and officers' management liability, the foundations underlying the ever-changing cyber risks, and the current insurance policies available to cover these risks. It will then emphasize the evolution of cyber liability by discussing the most significant cyber breaches and the types of claims that emerged from them. A comparison of the types of insurance policies available, the role each policy could play in cyber incidents, and the gaps that are still open in insurance will follow. Finally, it will identify alternatives in cyber risk management that different types of corporations can take to control these cyber risks.

a. Background on Directors and Officers Liability and its Insurance

Directors and officers ("D&Os") liability has significantly evolved and will continue to develop. "For most of the twentieth century, no one worried very much about the possibility that corporate directors and officers might incur personal liability to the corporation or its shareholders…"[10] However, things changed when the public began to experience the effects of the D&Os' actions on the economy. History still remembers the

[9] *Id*. at 21.
[10] Mark A. Sargent & Dennis R. Honabach, *The World of D&O Liability Law,* DIRECTORS AND OFFICERS LIABILITY HANDBOOK §1:1 (Oct. 2016).

collapses of Enron Corporation, WorldCom, and Tyco, and, consequently, the 2001 Wall Street bubble burst. These events led to numerous lawsuits, particularly against the D&Os of these corporations, alleging breach of duty that, shareholders claimed, caused the downfall of these companies. Because of these lawsuits and the public awareness they generated, the liability of the D&Os has come under scrutiny.

The D&Os have several duties that the corporation expects and that the law requires due to the positions they hold. Their duties arise from common law and are based on a fiduciary duty to the corporation. This fiduciary duty enforces the D&Os to act in the best interest of the corporation. This duty also requires them to have loyalty, obedience, due care, and good faith to the corporation that they serve. Among these duties, a crucial one is due care. The duty of due care "imposes an affirmative duty on D&Os to act with diligence and care in carrying out their respective roles."[11] It also requires the D&Os to use "the care an ordinarily prudent person in a like position would exercise under similar circumstances."[12]

In contrast, the duty of good faith is the most generalized duty that D&Os have.[13] The duty of good faith requires the D&Os to act with a conscious regard for their responsibilities as fiduciaries.[14] This duty appears to encompass several other duties necessary for day-to-day official activities. Thus, this demonstrates the uncertainty and ambiguity still surrounding the proper application of the rule.[15]

As with all duties, there come increasing liabilities due to the potential breach of those responsibilities. Thus, adequate management of this liability is a top priority for D&Os seeking to manage and transfer this risk. Particularly, under these duties, D&Os are being held liable for a company's actions even when there is no evidence the official knew about the wrongdoing because "[c]ongress has not required 'awareness of some wrongdoing' in order to hold responsible corporate agents accountable for violating the statute."[16] Initially, the liability of the D&Os for the duties owed to the corporation they serve was very straightforward. They invoked the business judgment rule as a defense against any wrongdoing attributable to their decision-

---

[11] Cory A. McKenna, *FDIC v. Rippy: Due Care and the Business Judgment Rule in the Fourth Circuit and the Potential Implications for the Banking Industry*, 20 N.C. BANKING INST. 189, 193 (2016).
[12] *Id.* at 192.
[13] McKenna, *supra* note 11, at 192.
[14] *Id.*
[15] *Id.* at 190.
[16] United States v. DeCoster, 828 F.3d 626, 634 (8th Cir. 2016) (citing *United States v. Park*, 421 U.S. 658, 672–73 (1975)); Britt Eilhardt & Beata Aldridge, The Yates Memo's Impact On D&O Liability, 20160511 A N.Y.C. BAR 16 (2016).

making. The standard to impose liability on D&Os in potential claims was gross negligence. Gross negligence has been established as a decision "…so one-sided that no businessperson of ordinary, sound judgment could conclude that the corporation has received adequate consideration."[17]

As a result of the emerging trends and evolution of claims against D&Os, the demand for insurance has increased over the years because, "[a]s the bases for liability of officers and directors have broadened, the number of claims against D&O policies has increased."[18] Luckily, insurance has adapted to these types of claims against the D&Os. D&O management liability policies cover third-party claims[19] that arise from their conduct and decision-making as follows:

> "The purpose of D&O policies is to shift to the insurance carrier the risk of third-party liabilities arising from actions taken by corporate directors and officers in their official capacity. D&O policies provide protection to a company's directors and officers and serve as a tool for a company's risk management." [20]

Traditional D&O policies include coverage for "(1) directors and officers for liabilities that their company does not reimburse, (2) the company for director and officer liabilities that the company legally may reimburse, or (3) the company for liabilities caused by actions taken by officers and directors but attributed to the company itself."[21] Coverage for the D&O liability that the company does not reimburse is also known as Side A coverage. The Side A insurance provides coverage for the direct and nonindemnifiable liability of the D&Os within the scope of their duties to a company. The language varies between policies, but it usually goes as follows:

> "The Company shall pay, on behalf of each of the Insured Persons, Loss for which the Insured Person is not indemnified by the Organization and which the Insured Person becomes legally obligated to pay on account of any Claim first made against the Insured Person, during the Policy Period or, if exercised, during the Extended Reporting Period, for a Wrongful Act by such Insured Person before or during the Policy Period."[22]

---

[17] *In re* Walt Disney Co. Derivative Litig., 906 A.2d 27, 52 (Del. 2006).
[18] James W. Hubbell, *Emerging Issues in Directors' and Officers' Liability Insurance Coverage*, 17 COLO. LAW. 1031 (1988).
[19] Third party claims differ from first party claims: "A first-party insurance claim involves filing a claim directly with your own insurance company for damages or losses. This type of claim typically covers incidents affecting you or your property. On the other hand, a third-party insurance claim refers to the process of filing a claim with someone else's insurance provider, usually after an incident where you are not at fault. This claim is filed against the insurance of the party responsible for the damages or injuries suffered." Scott Armstrong, *First-Party Vs. Third-Party Personal Insurance Claims*, ARMSTRONG LEE & BAKER LLP (2024), https://albtriallawyers.com/what-is-the-difference-between-a-third-party-and-first-party-insurance-claim.
[20] Leo M. Pruett, A. Thomas Morris & Sheldon B. Sommer, *After Enron: Maximizing Coverage in D&O Policy, 2002 ACCADKT 44 (*Westlaw).
[21] *Id.*
[22] Marissa Jeffrey, *Nuts & Bolts: Directors & Officers Liability Policies*, 15 J. TEX. INS. L. 13, at 14 (2017) (citing Chubb Group of Ins. Cos., Asset Management Protector SM By Chubb, *Private Company Directors and Officers Liability Coverage Part* (Form No. 14-02-13781, Feb. 2008)).

This coverage is usually activated when the corporation has a legal requirement to indemnify the D&Os or in cases of a company's insolvency.[23] Furthermore, coverage for the company's D&O liabilities that the company may legally reimburse is known as Side B coverage. The language goes as follows:

> "Insuring Clause (B): Insured Person Indemnification Coverage
> (B) The Company shall pay, on behalf of an Organization, Loss for which such Organization grants indemnification to an Insured Person, and which the Insured Person becomes legally obligated to pay on account of any Claim first made against the Insured Person, during the Policy Period or, if exercised, during the Extended Reporting Period, for a Wrongful Act by such Insured Person before or during the Policy Period."[24]

Presumably, this portion of the policy should apply to intentional and negligent acts, with the appropriate exclusions.[25] Finally, Side C coverage, also known as *entity coverage, applies when the* company faces liability for wrongful acts committed by its directors or officers in their official capacity.[26]

All coverage sections have one thing in common: they will provide insurance coverage for a "Wrongful Act". Even though this definition will vary depending on the policy, it is usually referred to as an "actual or alleged error, a misstatement, a misleading statement, act, omission, neglect, or a breach of duty by the insured while acting in his corporate capacity."[27] This definition is broad enough to cover emerging trends in claims and potential risks that continue to evolve in this economy. Failure to maintain adequate cyber insurance or cyber risk protocols appears to fall within the policy's scope.

b. Foundations of Cyber Risks

The concept of cyber risk began in the early 1990s. At the time, the perception was that only entities directly involved in technology development were vulnerable to cyber incidents. Alongside this surge, initial policies addressing cyber risks began to emerge, marking cyber risk as an emerging professional risk for software and technology companies. "The initial policies were a product of the times, offering limited coverage--none for first-party losses--with reverse-engineered language from existing forms of insurance."[28]

---

[23] Pruett, Morris & Sommer, *supra* note 25, at 46.
[24] Jeffrey, *supra* note 23, at 14.
[25] Pruett, Morris & Sommer, *supra* note 25, at 51.
[26] Pruett, Morris & Sommer, *supra* note 25, at 46.
[27] Jeffrey, *supra* note 23, at 13.
[28] Margaret A. Reetz *et. al.*, *Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law*, 122 PENN ST. L. REV. 727, 730-31 (2018).

Even so, these initial cyber policies only covered liability when third-party information was compromised and exposed. However, later in the late 2000s, the notion of only third-party victims began to cease to include first-party victims as well. "The mid-2000s ushered in the next wave of growth following the tremendous upswing in malicious activity typified by identity theft and data breaches."[29] As a result, insurance companies began offering policies covering both first-party losses and third-party liability.

The various types of cyber breaches that have occurred over the past few years have given rise to claims in many well-known industries worldwide. In its early stages, the claims were brought by consumers whose personal information was compromised, directly affecting them. As technology became more sophisticated, so did the cyber-attacks. These cyber-attacks resulted in significant financial losses, increasing the number of stakeholders at risk. Claims began to include shareholder suits against D&Os for failing to take adequate measures to prevent the breaches that caused the losses. Allegations against the D&Os for breach of duties of loyalty, care, and good faith by "failing to implement and enforce a system of effective internal controls and procedures with respect to data security" and failure to exercise oversight duties by not monitoring the company and failure to comply with federal and state laws and regulations were prominent in these claims.[30]

The year 2022 was a tipping point due to highly publicized ransomware surges.[31] As a result of evolving cyber risk trends, cyber and privacy insurance now covers both property (first-party) and liability (third-party) cyber risks.[32] "There is no standard policy form, which means that the coverage offered by one insurer can (and often does) differ dramatically from that offered by another insurer."[33] The first-party coverages usually include: Privacy Notification and Crisis Management Expense; Business Interruption; Extra Expense; Data Assets; Cyber-Extortion; Computer Fraud; Funds Transfer Fraud; and Social Engineering/Fraudulent Instruction Coverage.[34] The third-party coverages usually include: Information Security and Privacy Liability;

---

[29] *Id.* at 731.
[30] Kevin M. LaCroix, *Wendy's Settles Data Breach-Related Derivative Lawsuit*, THE D&O DIARY (May 9, 2018), https://www.dandodiary.com/2018/05/articles/director-and-officer-liability/wendys-settles-data-breach-related-derivative-lawsuit/.
[31] R&I Editorial Team, *Cyber Insurance Growth Slows But Opportunities Remain: Swiss Re*, RISK & INSURANCE (Dec. 2, 2024), https://riskandinsurance.com/cyber-insurance-growth-slows-but-opportunities-remain-swiss-re/.
[32] Peter A. Halprin & Nicholas A. Pappas, *Ransomware, Cybersecurity, and Insurance*, 2021 WL 1878496, at *2 (May 11, 2021).
[33] Thomas H. Bentz, Jr., *Is Your Cyber Liability Insurance Any Good? A Guide for Banks to Evaluate Their Cyber Liability Insurance Coverage*, 21 N.C. BANKING INST. 39, 40 (2017).
[34] Steven M. Hickey, Waleed Haddad & James Parry Jr., *Advising Clients on Cyber Liability Insurance and Cybersecurity Practices*, 98-MAR MICH. B.J. 22, 23 (2019).

Regulatory Defense and Penalties; Payment Card Industry Fines and Assessments; Website Media; Bodily Injury and Property Damage Liability.[35]

The first-party coverages of Privacy Notification and Crisis Management Expense, Business Interruption and Extra Expense are known as post-breach response coverages. These policy parts "…provide extensive coverage for the cost of replacing data, as well as many other consequential losses that flow from cybercrime"[36] and are classified as theft of property coverage. These types of coverage pay insured claims arising from a cyber incident in which the ultimate victim is the insured itself. Losses from these crimes may include the cost of replacing data that has been corrupted (sometimes referred to as "restoration expenses"), the loss of the property that has been stolen, the cost of giving notices required by statutes or regulations, lost income on account of the inability of the business to function (business interruption), and crisis management costs for public relations efforts to mitigate the reputational damages associated with a cyber-crisis event.[37] In response to these losses, many insurance companies offer coverages that include "First-and Third-party protection in a comprehensive coverage form; First-party coverage includes Loss of Digital Assets, Non-Physical Business Interruption and Extra Expense, Cyber-Extortion, Cyberterrorism, and Security Event Costs."[38] The language of the policy varies, and it is usually negotiated, but it usually goes as follows:

> "Breach Response Insuring Agreements--The insurer will reimburse or pay … notification costs resulting from an actual or suspected privacy breach; … computer and legal expert costs resulting from an actual or suspected 1) privacy breach, 2) security breach, or 3) cyber extortion threat …; restoration costs, directly caused by a security breach; …. [and] public relations costs, resulting from an actual or suspected: 1) privacy breach, 2) security breach, or 3) media act ….
>
> Cyber Crime Insuring Agreements--The insurer will pay the insured entity for its direct loss of money, securities, or other property, directly caused by computer fraud that is discovered during the policy period …. [And] the Insurer will pay the insured entity for its direct loss of money or securities, directly caused by social engineering fraud [or] by telecom fraud that is discovered during the policy period.
>
> Business Loss Insuring Agreements--The insurer will pay the insured for its business interruption loss that is directly caused by any of the following: … 1) A security breach that results in a total or partial interruption of a computer system, 2) a system failure … [and]

---

[35] *Id*.
[36] Jack Montgomery, *Cybercrime Losses and Insurance for Property Damage and Third-Party Claims*, 27 ME. B.J. 158, 162 (2012).
[37] *Id.* at 159.
[38] Montgomery, *supra* note 36, at 162.

> 3) The voluntary shutdown of a computer system by the Insured, …. to minimize the loss caused by a security breach or privacy breach."[39]

The third-party liability portion of the cyber policy provides coverage for breaches to the insured that result in direct damages to third parties. This is perhaps the most well-known coverage in cyber insurance. The losses associated include:

> "Indemnification paid to the information owner based upon (i) the cybercriminal's use of the information to steal money or purchase goods using the information stolen; (ii) losses to the third party for damage caused by the transmitted virus or malware; or (iii) losses caused by a third party's lack of access to the victim's network for purposes of transacting business.
>
> Exposure of businesses that hold data owned by others to various claims arising out of their failure to protect that data (possibly subject to significant limitations).
>
> Losses arising out of the insured's unauthorized use or infringement of the copyright, trademark, or other intellectual property of the third party, by cyber transmission, or defamation."[40]

The insuring coverages usually include "Network Security and Privacy Liability, Employee Privacy Liability, and Electronic Media Liability; Covered Cause of Loss includes administrative or operational mistakes; Breach of Privacy coverage – which includes damages resulting from alleged violations of HIPAA, state, federal, and foreign privacy protection rules; Customer Breach Notice Expense and coverage; Public Relations Expense coverage;".[41] The language varies between policies, but it usually reads as follows:

> "Network Security Wrongful Act--[This phrase means] an actual or alleged act, error or omission by or on behalf of the insured in the performance of the Company's business that causes or fails to prevent: 1) unauthorized access to or unauthorized use of the covered network, 2) the transmission of any malicious code from the covered network to a third party's computer systems, 3) business interruption, and/or 4) a network disruption …
>
> Privacy Wrongful Act--[This term means] any actual or alleged: 1) negligent act, error or omission by or on behalf of the insured in the performance of the Company's business that actually or allegedly causes or fails to prevent unauthorized access to, unauthorized use of … [or] the loss of any laptop, smartphone or other portable device that contains protected information … [or], 2) violation of any federal, state, local or foreign law or regulation regarding the maintenance, protection, use or disclosure of protected information…."[42]

---

[39] Willy E. Rice, *Cyber-Technology Torts and Insurers' Ambiguous Obligations to Defend Professionals and Business Entities Under Evolving Cyber-Insurance Contracts: Statistical and Legal Inferences from Traditional Insurers' Declaratory Judgments, 1940-2019* (2019) (citing The Travelers Indemnity Co., Form CYB-16001 Ed. 01-19-CyberRisk Insurance Policy 1-2 (2019), https://www.travelers.com/iw-documents/apps-forms/cyberrisk/cyb-16001.pdf (https://perma.cc/43J5-LS8J)).

[40] Montgomery, *supra* at 159.

[41] Montgomery, *supra* at 163.

[42] Willy E. Rice, *Cyber-Technology Torts and Insurers' Ambiguous Obligations to Defend Professionals and Business Entities Under Evolving Cyber-Insurance Contracts: Statistical and Legal Inferences from Traditional Insurers' Declaratory Judgments, 1940-2019* (2019), 19 (2019)

As mentioned, the current cyber insurance market offers a variety of coverages that protect the insured in the event of a cyber incident. As cyber threats continue to rise and other insurance policies exclude related incidents, demand has increased for policies specifically designed to address cyber risks.[43] However, the circumstances under which this policy is triggered are very limited compared with other types of insurance. There is no one way to define a cyber incident.

Therefore, when new cyber risks emerge, or new types of claims arise, insurance companies would have to decide whether to insure them by adding more coverage to their policies. If there is one thing the insurance industry has learned from the foundations of cyber risks, it is that claimants will get creative and cyber losses will become more crucial in the corporate world than other types of losses.

II. Analysis of the Main Issues in Cyber and D&O Insurance

As demand for these types of insurance grows with the evolution of technology and claims, it is important to ensure that the entities that purchase insurance are adequately covered not only for current risks and liabilities but also for evolving future risks and claims. New laws are being enacted every day, and companies are now paying more attention to their cyber risks because of the financial impact they have shown. As management liability claims continue to unfold in the era of data breaches, the courts are also becoming more punitive towards decision-makers who fail in their duties and harm the public. Therefore, D&OS must take appropriate measures to address cybersecurity issues.

In this section, the basic but crucial tools in the D&O handbook of cyber risk management will be discussed. It will outline the evolution of the most highly publicized breaches that have resulted in million-dollar claims, the available insurance coverages for claims arising from a cyber incident, and other risk management techniques that D&Os may consider covering insurance gaps and comply with their fiduciary duties.

(citing Great Am. E & S Ins. Co., Great American Ins. Group, Cyber Risk Insurance Policy - Form D62100 2 (2017), http://www.abais.com/Data/Sites/1/media/specimen/sbg/gaiccy-berpolicy.pdf [https://perma.cc/PG4U-FFBQ]).

[43] David J. Baldwin, Jennifer Penberthy Buckley & D. Ryan Slaug, *Insuring Against Privacy Claims Following A Data Breach*, 122 PENN ST. L. REV. 683, 718 (2018).

a. How Cyber Claims Evolved from Sony to Marriott to Uber

One of the initial events that raised public awareness of cyber risks was Sony's PlayStation Network data breach. In 2011, 77 million PlayStation accounts were breached. The affected accounts contained users' personal information, including addresses, credit card numbers, and bank account details. A consumer class action was filed alleging that Sony "failed to provide reasonable network security, including utilizing industry-standard encryption, to safeguard Plaintiffs' personal and financial information stored on Sony's network."[44] The consumer class action was settled in 2014 for around $15 million. No additional claims were filed in this matter. It is important to note that at that time cyber risks were believed to be mostly directed at technology companies such as Sony. This company's purpose was highly vulnerable to a cyber breach. However, as technology continues to be a central tool in day-to-day business, this vulnerability will persist not only in technology companies, but in all types of businesses.

A distinguishable cyber breach case that set an important regulatory precedent is the Wyndham Worldwide Corporation LLC ("Wyndham") case. Between 2008 and 2010, a cyber breach occurred in which hackers gained access to Wyndham's main network and stole credit card information for over 619,000 customers.[45] Unlike in the Sony case, the first to file a complaint against Wyndham for this breach was the Federal Trade Commission ("FTC"). Under the regulatory powers conferred to them by federal statute, "[t]he FTC filed suit in federal District Court, alleging that Wyndham's conduct was an unfair practice and that its privacy policy was deceptive."[46] Particularly, the FTC alleged that Wyndham's unfair cybersecurity practices "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[47] Wyndham filed a motion to dismiss challenging whether the FTC has authority to regulate cybersecurity and, if so, whether Wyndham had fair notice that its specific cybersecurity practices could fall short, which the District Court denied, and the Third Circuit Court of Appeals confirmed.[48] In light of this decision, Wyndham reached a settlement agreement with the FTC under which it will adopt a comprehensive

---

[44] *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 953 (S.D. Cal. 2014).
[45] Timothy Cornell & Clifford Chance, *Wyndham – A Case Study in Cybersecurity: How the cost of a relatively small breach can rival that of a major hack attack*, CCBJ (Mar. 19, 2015), https://ccbjournal.com/articles/wyndham---case-study-cybersecurity-how-cost-relatively-small-breach-can-rival-major-h#_ftn1.
[46] F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).
[47] *Id*.
[48] *Id*. at 242.

information security program to protect consumer data and submit to annual audits to ensure compliance with this agreement. The most significant aspect of this case was that the Third Circuit recognized the FTC's authority to regulate cybersecurity under the unfair practices statute. No monetary settlement was reached, but the Third Circuit opinion put businesses at risk of regulatory infringement by the FTC and other regulatory agencies that may find that a cybersecurity breach violates their statutes. To this point, the regulatory agency capable of bringing an action against a corporation for this type of issue was the Securities and Exchange Commission ("SEC"). Because cyber risk encompasses a wide range of issues that affect different populations, more agencies can assert jurisdiction and file enforcement actions against these companies for failing to take adequate action.

Regulatory infringement was not the only consequence that Wyndham faced after the cyber breach. In February 2014, a shareholder derivative suit was filed against Wyndham for breach of fiduciary duty arising from its failure to take reasonable steps to maintain the security of its customers' personal and financial information.[49] However, this case reflected a failed attempt to establish liability to D&O for breach of fiduciary duties in failing to attain adequate cybersecurity for the corporation. The case was dismissed in 2014, with no further discussion of D&O liability for cyber breaches. Nonetheless, because of the precedent exposure Wyndham faced for unfair practices violations, this regulatory exposure opened the door to litigation on D&O liability for breach of fiduciary duties, with an emphasis on breach of the duty of care and due diligence.

Another significant claim was the Target Corporation ("Target") cyber breach. In December 2013, around 110 million credit card records were stolen in a breach of the company's POS Systems.[50] Initially, the claim filed against Target was a consumer protection class action, just like the Sony case. However, due to the loss to the corporation itself, the focus shifted to the D&Os' handling of the cybersecurity issues. In 2014, the shareholders filed a derivative suit for breach of D&Os' fiduciary duties. The plaintiffs allege, "[t]hat the company "failed to take reasonable steps to maintain its customers' personal and financial information," and

[49]Palkon v. Holmes, No. 14-CV-01234, 2014 WL 5341880, at *5 (D.N.J. Oct. 20, 2014).
[50] Ben Popken, *Target estimates breach affected up to 110 million*, NBC NEWS (Jan. 10, 2014), https://www.nbcnews.com/business/business-news/target-says-stolen-info-data-breach-hit-70-million-people-flna2d11894083.

failed to give customers prompt notice of the breach.[51] Specifically, with respect to the possibility of a data breach, the plaintiffs alleged that the defendants failed "to implement any internal controls at Target designed to detect and prevent such a data breach."[52] The D&O derivative suit was dismissed because a special litigation committee established that it would not be in Target's best interest to pursue the claim. However, this was one of the first cases to consider a violation of fiduciary duties by D&Os arising from the cyber breach. It unequivocally had a significant impact on the company and how cyber liability interrelates with D&O management liability.

Presumably one of the most notable shareholder claims arising from a cyber breach was the Yahoo! class action lawsuit. This case arose from three breaches that occurred between 2013 and 2016. In these breaches, hackers gained access to over 1 billion accounts. The information stolen included personal information of users such as dates of birth, addresses, emails, passwords, financial information, and contents of users' emails.[53] The consumers filed a class action suit alleging that Yahoo knew about the breaches and the cyber risk it faced but failed to promptly report them to its users. Later in January 2017, the shareholders filed a class action lawsuit against certain D&Os due to the breach and alleged that:

> "…the defendants made false or misleading statements or failed to disclose that: (i) Yahoo failed to encrypt its users' personal information and/or failed to encrypt its users' personal data with an up-to-date and secure encryption scheme; (ii) consequently, sensitive personal account information from more than 1 billion users was vulnerable to theft; (iii) a data breach resulting in the theft of personal user data would foreseeably cause a significant drop in user engagement with Yahoo's websites and services; and (iv) as a result, Yahoo's public statements were materially false and misleading at all relevant times."[54]

In sum, the allegations against the D&Os revolved around their alleged breach of fiduciary duty for failing to adequately oversee the company's data security practices, just like the Target derivative suit. Unlike Target's dismissal, this claim was settled for $29 million in January 2019. It confirmed the Wyndham and Target hypothesis that shareholders' derivative suits would continue to arise. Therefore, not only is a cyber

---

[51] Kevin LaCroix, *Target Corporation Cybersecurity-Related Derivative Litigation Dismissed*, THE D&O DIARY (July 9, 2016), https://www.dandodiary.com/2016/07/articles/cyber-liability/target-corporation-cybersecurity-related-derivative-litigation-dismissed/.

[52] *Id.*

[53] *In re Yahoo! Inc. Customer Data Security Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *2 (N.D. Cal. Aug. 30, 2017).

[54] Fernando M. Pinguelo, Angelo A. Stio III & Hasan Ibrahim, *Even As Data Breaches Continue to Increase, Obstacles Remain for Litigants Seeking to Pursue Securities Fraud and Derivative Suits*, SCARINCI HOLLENBECK LLC ATTORNEYS AT LAW (Apr. 11, 2018), https://scarincihollenbeck.com/law-firm-insights/shareholder-securities-fraud#title-1.

risk a matter for a cyber liability policy to respond to the breach of privacy of third-party consumers, but it is also a matter of breach of fiduciary duties that the D&O policy will have to respond to due to the shareholder's derivative suit.

The Home Depot breach is another significant incident that occurred in 2014 and is often compared to the Target breach. In this case, the breach occurred when hackers gained access to the company's POS network and stole information from 56 million credit cards.[55] Home Depot's consumers filed several suits against the company for its failure to "implement reasonable measures to prevent or to mitigate the effects of the data breach".[56] These claims were settled in 2016 for $19.5 million.[57] Moreover, in August 2015, shareholders filed multiple derivative complaints against Home Depot's D&Os alleging:

> "...that the defendants breached their duty of loyalty because the defendants failed to institute internal controls sufficient to oversee the risks that Home Depot faced in the event of a breach and because they disbanded the Board of Directors committee that was supposed to have oversight of those risks. The plaintiffs also alleged that the defendants wasted corporate assets and that the defendants violated Section 14(a) of the Securities Exchange Act in their 2014 and 2015 proxy filings."[58]

The shareholder's derivative suit was dismissed, and the parties settled while the appeal was pending. As part of the settlement agreement, Home Depot agreed to reform its corporate governance and maintain adequate cybersecurity measures to prevent future attacks. The agreements in this settlement also raise an interesting dilemma about which policy will apply in this case. Since part of the settlement required taking action to manage cyber risks, the D&O policy will not cover it, as it only covers monetary loss. The cyber policy will not cover it either, as the actions required under the settlement are preventive in nature.

Another important cyber breach was reported by Wendy's in February 2016, after an internal investigation revealed malware in its POS systems. As a result of this breach, Wendy's faced a consumer class action suit, a financial institution suit, and a shareholder derivative suit. Wendy's settled with the financial institutions for $50 million. Moreover, in May 2018, Wendy's shareholder derivative suit for breach of

---

[55] Kevin M. LaCroix, *Data Breach-Related Derivative Lawsuit Filed against Home Depot Directors and Officers*, THE D&O DIARY (Sept. 9, 2015), https://www.dandodiary.com/2015/09/articles/cyber-liability/data-breach-related-derivative-lawsuit-filed-against-home-depot-directors-and-officers/.
[56] *Id.*
[57] Tom Spring, *Home Depot Agrees To $19.5 Million Settlement To End 2014 Breach Nightmare*, THREATPOST (Mar. 18, 2016), https://threatpost.com/home-depot-agrees-to-19-5-million-settlement-to-end-2014-breach-nightmare/116884/.
[58] *In re The Home Depot, Inc. Shareholder Derivative Litigation,* 223 F. Supp. 3d 1317, 1321 (N.D. Ga. 2016).

fiduciary duties "was settled for cybersecurity changes, corporate governance therapeutics, and $950,000 in plaintiffs' attorneys' fees"[59]. Even though Wendy's breach occurred after the Yahoo breach, their officials quickly moved to settle the claims. The Wendy's case reflects accurate risk management techniques in identifying the breach, informing the public, and settling the claims. This case is a great example of the D&Os' duties to the company and their responsibilities of protecting it and its brand at all costs.

Another leading case in cyberlaw is the Equifax cyber breach. Since this breach occurred after several significant breaches, consumers and the government were better prepared to deal with Equifax's liability. In September 2017, Equifax announced a cyber breach in which hackers had gained access to their customers' personal information, including Social Security numbers, addresses, and dates of birth. The breach occurred when the hackers exploited a vulnerability in the company's website. The impact was estimated to reach around 143 million customers. Subsequently, consumer claims were filed against Equifax for negligence in cybersecurity and for delaying disclosure of the breach to the public.

In addition to the consumer lawsuits, a securities suit against the company's D&Os was filed. The lawsuit alleged that "(1) the Company failed to maintain adequate measures to protect its data system; (2) the Company failed to maintain adequate monitoring systems to detect security breaches; (3) the Company failed to maintain proper security systems, controls and monitoring systems in place; and (4) as a result of the foregoing the Company's financial statements were materially false and misleading at all relevant times"[60]. Unlike the previously mentioned D&O class actions, this securities lawsuit was under intense scrutiny because, just days before the breach was announced, Jun Ying, Chief Information Officer of Equifax U.S.

[59]Jonathan Maze, *Wendy's Agrees to Pay $50M to Settle Data Breach Claims*, RESTAURANT BUS. ONLINE (Feb. 13, 2019), https://www.restaurantbusinessonline.com/financing/wendys-agrees-pay-50-million-settle-data-breach-claims; Kevin M. LaCroix, *Wendy's Settles Data Breach-Related Derivative Lawsuit,* THE D&O DIARY (May 9, 2018), https://www.dandodiary.com/2018/05/articles/director-and-officer-liability/wendys-settles-data-breach-related-derivative-lawsuit/.

[60] Kevin M. LaCroix, *Equifax Data Breach Litigation Now Includes Securities Suit*, THE D&O DIARY (Sept. 13, 2017), https://www.dandodiary.com/2017/09/articles/cyber-liability/equifax-data-breach-litigation-now-includes-securities-suit/.

Information Solutions, sold a personal stake in the company.[61] On March 7, 2019, he pled guilty to the respective insider trading charges.[62]

Furthermore, Equifax's stock dropped after the company suffered a breach, despite its business model being centered on protecting private information.[63] Given the significance of the company's losses, the D&O litigation drew more shareholder interest than the other D&O cases that were ultimately dismissed. On February 13, 2020, the shareholder derivative suit was settled for $149 million.[64] Apart from the hefty settlement paid in this case, the D&Os would have to implement adequate risk management strategies to reestablish the public's faith in the brand.

The Facebook and Marriott data breaches highlight particular aspects absent from other cyber breaches: the exposure arising from noncompliance with the General Data Protection Regulation ("GDPR"), Europe's privacy regulation.[65] This law was enacted in May 2018 and established rigorous privacy requirements for companies operating in Europe. This particularly affected multinational companies that had adopted certain cyber measures but were now being held to higher standards to avoid penalties from Europe. Both Facebook and Marriott faced securities lawsuits over the cyber breaches and their failure to adequately implement measures and comply with GDPR, which could have been avoided to minimize the breaches.

Finally, one of the most recent decisions on D&O liability for cyber breach was confirmed by the Ninth Circuit Court of Appeals on March 13, 2025. This was the case of Joseph Sullivan, former Chief Security Officer and Deputy General Counsel for Uber Technologies. He was convicted of obstruction of justice and felony misprision by covering up a 2016 cyber breach that exposed the personal data of 57 million Uber users and of 600,000 Uber drivers.[66] The cover-up occurred while the Federal Trade Commission ("FTC") was already investigating Uber for a 2014 cyber breach. This Court of Appeals judgement is "[t]he first instance of a

---

[61] Anders Merlin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*, BLOOMBERG (Sept. 7, 2017), https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack.
[62] Press Release, U.S. Att'y's Off. N. Dist. of Ga., *Former Equifax Employee Sentenced for Insider Trading* (June 27, 2019), https://www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading.
[63] Kevin LaCroix, *Equifax Data Breach-Related Securities Suit Settled for $149 Million*, THE D&O DIARY (Feb. 17, 2020), https://www.dandodiary.com/2020/02/articles/securities-litigation/equifax-data-breach-related-securities-suit-settled-for-149-million/.
[64] *Id.*
[65] *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 543 F. Supp. 3d 96, 149-50 (D. Md. 2021).
[66] United States v. Sullivan, 131 F.4th 776, 780-81 (9th Cir. 2025).

corporate executive being held criminally liable for mishandling a data breach, and Sullivan's conviction—given the novel extension of personal liability for strategic decisions in the management of a cyber incident…"[67] confirms the tendency that has been occurring since the Sony case, cyber liability for D&O action will continue to rise and enforced by the regulators.

The cases summarized and discussed are just a sample of the most highly publicized cases for cyber breaches and the liability they generate. There are currently numerous claims filed against many important companies due to cyber breaches in their systems. The common denominator is the type of claims that arise from these breaches. The claims are not limited to consumer claims; they also include securities class actions and regulatory enforcement. For example, in October 2021, the Civil Cyber-Fraud Initiative was created to apply the False Claims Act ("FCA") against cybersecurity-related fraud by government contractors and grant recipients.[68]

Furthermore, the FTC has been an important element in protecting data privacy standards under Section 5 of the FTC Act, which enforces civil penalties for failing to safeguard data.[69] Therefore, implementing adequate risk management tools is essential for responding effectively in the event of a breach. Ultimately, however, insurance will bear most of the financial burden when claims inevitably arise.

b. Which Coverage Applies? Comparison of Insurance Policies

Initially, when cyber incidents began, companies turned to their existing insurance policies to cover the resulting losses. However, as cyber insurance emerged, these traditional coverages incorporated market exclusions to limit recovery for cyber-related claims. Therefore, the market has actively sought to ensure that cyber incidents are covered only by cyber insurance. As cyber incidents have given rise to other types of claims, such as securities and derivative suits, D&O insurance has also had to step in. The particularity of cyber risks is that it is not one size fits all, and traditional insurance seems to be insufficient because "cyber-attacks can come from anywhere in the world, at any time, and can impact thousands of businesses at

---

[67] Matthew Baker, *Ninth Circuit Upholds Conviction of Former Uber Security Chief Joseph Sullivan in Connection with 2016 Uber Data Security Breach*, JD SUPRA (Mar. 20, 2025), https://www.jdsupra.com/legalnews/ninth-circuit-upholds-conviction-of-6160333.
[68] *Cyber and D&O Insurance: Maximizing Coverage for Companies and Executives from Cyber Incidents*, HUNTON ANDREWS KURTH LLP (July 25, 2023), https://www.hunton.com/insights/legal/cyber-and-d-and-o-insurance-maximizing-coverage-for-companies-and-execs-from-cyberincidents.
[69] *Id*.

approximately the same time, making cyber losses correlated risks."[70] Therefore, a diligent company and its D&Os need appropriate coverages that evolve with trends while remaining flexible enough to accommodate emerging cybersecurity risks.

Initially, as third-party claims began, the Commercial General Liability ("CGL") policy was the first policy considered to provide coverage, such as payment of the sums the insured is legally obligated to pay as damages in such suits. This coverage was very broad and could potentially cover emerging third-party liability arising from cyber breaches and hacks. However, in 2004, the Insurance Services Office, Inc. ("ISO") restricted the CGL policy language in connection with loss of electronic data, which reads as follows: "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[71] It is well known that CGL does not cover data breaches. However, Insuring Agreement A states:

> "We will pay those sums that the insured becomes legally obligated to pay as damages because of "bodily injury" or "property damage" to which this insurance applies.
>
> "Bodily injury" means bodily injury, sickness or disease sustained by a person, including death resulting from any of these at any time.
>
> "Property damage" means: a. Physical injury to tangible property, including all resulting loss of use of that property. All such loss of use shall be deemed to occur at the time of the physical injury that caused it; or b. Loss of use of tangible property that is not physically injured. All such loss of use shall be deemed to occur at the time of the "occurrence" that caused it. For the purposes of this insurance, electronic data is not tangible property."[72]

Its coverage usually stems from bodily injury or property damage. This last part is very significant because, as cyber incidents affect infrastructure that cause bodily injury and property damage, then the breach between these two policies is complementary. As a result, cyber insurance necessarily complements this coverage.

Moreover, under Insuring Agreement B, there is coverage for Personal and Advertising Liability. This agreement states the following in the relevant parts:

---

[70] Christopher C. French, *Five Approaches to Insuring Cyber Risks*, 81 MD. L. REV. 103, 107 (2021).
[71] COMMERCIAL GENERAL LIABILITY COVERAGE FORM § 2(p) (Ins. Servs. Off., Inc. 2012).
[72] Ins. Servs. Off., Inc., COMMERCIAL GENERAL LIABILITY COVERAGE FORM, CG 00 01 04 13, at 13, 15 (2012).

> "We will pay those sums that the insured becomes legally obligated to pay as damages because of "personal and advertising injury" to which this insurance applies. We will have the right and duty to defend the insured against any "suit" seeking those damages".[73]
>
> "Personal and advertising injury" means injury, including consequential "bodily injury", arising out of one or more of the following offenses:
>
> a. ...
> b. ...
> c. ...
> d. Oral or written publication, in any manner, of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services;
> e. Oral or written publication, in any manner, of material that violates a person's right of privacy;
> f. The use of another's advertising idea in your "advertisement"; or
> g. Infringing upon another's copyright, trade dress or slogan in your "advertisement"."[74]

This coverage is significant because it contains language that could potentially provide coverage for a third-party privacy breach or cyber incident related to a Personal or Advertising injury. The Fourth Circuit Court of Appeals thought so as well in *Travelers Indemnity vs. Portal Healthcare Solutions*. This case was a class action in which the plaintiffs alleged that Portal Healthcare Solutions engaged in conduct that resulted in medical records being published on the internet for 4 months.[75] The court ordered Travelers to provide defense and indemnity coverage for the insured, Portal Healthcare, arising from the electronic publication of content that resulted in the disclosure of personal information.[76] Even though experts say this case is an exception rather than the norm, depending on the policy language and endorsements, this type of event would be covered unless explicitly excluded. However, under this agreement, there is coverage only for intentional publication, not for negligent disclosure of information. Thus, the language restricts recovery and generates a gap in this area. Furthermore, there is only coverage for actual damages. There is no coverage for compliance with privacy laws or investigations resulting from this intentional act.

Another policy that could be interpreted as responding to a cyber incident is the property policy under the Electronic Data Protection ("EDP") coverage. This EDP coverage provides recovery for a first-party loss.

---

[73] *Id*. at 6.
[74] Id. at 15.
[75] Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C., 644 F. App'x 245, 246 (4th Cir. 2016).
[76] Andrew G. Simpson, *What to Know About Travelers' CGL Cyber Ruling*, INSURANCE JOURNAL (May 23, 2016), https://www.insurancejournal.com/magazines/mag-features/2016/05/23/408580.html.

EDP coverage is found under Inland Marine policies and refers to the direct damage to hardware, media, software, and data. The language found in EDP coverage is similar to the following:

> "We will pay for accidental direct loss to:
> (1) The following types of "computer programs" and "electronic data" that you own, license from others, lease from others, or rent from others:
> (a) "Computer programs" used in your business operations;
> (b) The "electronic data" that exists in "computer" memory or on "computer" storage media, used in your business operations;
> (2) That portion of your customers' "electronic data" that is supplied to you for processing or other use in your business operations. Coverage for customers' "electronic data" is limited to the specific data file(s) containing the information you are processing or using in your business operations.
> We do not cover any property you lease to others, rent to others or license to others. We do not cover "computer equipment" or removable data storage media under this Extension Of Coverage. This coverage extension is included in the Limit Of Insurance shown on the Schedule Page.
> Loss does not include any consequential loss except as may be provided in the optional Loss Of Income And Extra Expense coverage."[77]

The first-party recovery is limited to direct physical loss of hardware, data, or media. The cause of loss which activates it is a mechanical, electrical, or magnetic breakdown. It also provides coverage for business interruption due to these covered causes of loss. However, EDP does not extend coverage for damage to the covered equipment caused by a hack, virus, or dishonesty by the insured or their D&Os. Therefore, recovery for a loss arising from a cyberattack, rather than from a mechanical, electrical, or magnetic breakdown, is available only under cyber insurance.

Another important policy under which a claim could be reported for a cyber breach is the Crime policy. The Crime policy is a type of first-party property policy that provides coverage for loss of money or other property resulting from dishonest or fraudulent acts. Specifically, this Crime policy includes coverage for: "(a) employee dishonesty, (b) forgery or alteration, (c) money and securities, (d) money orders and counterfeit, (e) computer fraud and funds transfer fraud, and (f) kidnap, ransom and extortion."[78] The language of the Computer Fraud coverage in the Crime policy is the following:

> "We will pay for:
> (1) Loss resulting directly from a fraudulent:
> a. Entry of "electronic data" or "computer program" into; or

[77] Camp's Grocery, Inc. v. State Farm Fire & Cas. Co., No. 4:16-CV-0204-JEO, 2016 WL 6217161, at *3 (N.D. Ala. Oct. 25, 2016).
[78] William Austin, *Crime Insurance – The Other Property Policy*, INMI (Mar. 1, 2009), https://www.irmi.com/articles/expert-commentary/crime-insurance-the-other-property-policy.

b. Change of "electronic data" or "computer program" within; any "computer system" owned, leased or operated by you, provided the fraudulent entry or fraudulent change causes, with regard to Paragraphs 6.a.(1)(a) and 6.a.(1)(b):
    i. "Money", "securities" or "other property" to be transferred, paid or delivered; or
    ii. Your account at a "financial institution" to be debited or deleted.

(2) Loss resulting directly from a "fraudulent instruction" directing a "financial institution" to debit your "transfer account" and to transfer, pay or deliver "money" or "securities" from that account."[79]

To determine which policy is triggered in certain cyber events, it is important to identify the cause of the breach and the type of loss incurred. For example, in *Medidata Solutions, Inc. v. Federal Insurance Co.*[80], the insured filed a claim under its Crime policy for a spoofing incident involving the company's email, which resulted in an employee transferring funds to an outside bank account.[81] The insurer denied coverage for this claim arguing "that there was no coverage under the Computer Fraud coverage because the emails did not require access to Medidata's computer system, a manipulation of those computers, or input of fraudulent information."[82] The court established coverage for the loss under the Computer Fraud and Funds Transfer Fraud coverages of the Crime policy.[83] One takeaway from this recent decision is that "the deceptive process, as well as the exact acts undertaken in response to that process, appears to be the key focus of the courts."[84] Another particular factor that is addressed in this case is the human resource factor. The human resource factor can create a cybersecurity risk due to employee negligence or intentional acts to steal information from the company. That is why either crime insurance or cyber insurance may respond, depending on the source of the cyber breach.

Insurance experts have tried to differentiate these coverages: Crime covers tangible property and tangible loss, while cyber first-party insurance covers intangible property and intangible loss.[85] However, with recent developments and technological evolution, these definitions are beginning to blur.

---

[79] State of Ohio, Department of Administrative Services, *Crime Insurance Policy* (based on ISO Commercial Crime Coverage Form CR 00 26 11 15), OHIO.GOV (Nov. 2025), https://dam.assets.ohio.gov/image/upload/das.ohio.gov/property-services/risk%20management/Crime%20Insurance%20Policy.pdf.
[80] Medidata Sols., Inc. v. Fed. Ins. Co., 268 F.2d 471 (2nd Cir. 2018).
[81] *Id.*
[82] Margaret A. Reetz *et al.*, *Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law*, 122 PENN ST. L. REV. 727, 747 (2018).
[83] *Id.*
[84] *Id.* at 750.
[85] Founder Shield, *What's the Difference Between Crime and Cyber Insurance?,* FOUNDER SHIELD (last visited Mar. 14, 2026), https://foundershield.com/blog/crime-and-cyber-insurance/.

Meanwhile, the Beazley cyber policy coverage for fraudulent transfers is defined as follows:

> "Fraudulent Instruction means the transfer, payment or delivery of Money or Securities by an Insured as a result of fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions provided by a third party, that is intended to mislead an Insured through the misrepresentation of a material fact which is relied upon in good faith by such Insured.
>
> Funds Transfer Fraud means the loss of Money or Securities contained in a Transfer Account at a Financial Institution resulting from fraudulent written, electronic, telegraphic, cable, teletype or telephone instructions by a third party issued to a Financial Institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by the Insured Organization at such institution, without the Insured Organization's knowledge or consent."[86]

Even though the Crime policy provides coverage for computer and fraudulent transactions, the cyber policy is much broader and includes many aspects which are not necessarily covered by the Crime policy. Nonetheless, not all cyber policies include this language, and an adequate analysis of the current insurance is necessary to ensure this risk is adequately covered. If there is an uncovered gap in this risk, it could lead to a significant uncovered loss to the company.

An emerging cyber risk that could be covered under both Crime and Cyber insurance is a cyber incident involving IoT. "IoT devices are everywhere in the workplace, though many businesses may not realize it, and each device is a potential security risk. Network-connected IoT devices, such as conferencing systems, security cameras, printers, and building-automation sensors and controls, can easily outnumber the organization's managed IT assets.[87] A breach in an IoT device could result in ransom and kidnapping using surveillance and restricting liberty until money is paid. It could result in computer fraud by hacking a laptop's webcam. It could also result in a privacy breach by illegally monitoring employees or customers or even accessing private information. Therefore, if an insurer wants to limit the type of recovery, it must explicitly exclude that type of recovery.

---

[86] Beazley, *Media Tech Insurance Policy* 8 (Feb. 2019), https://www.beazley.com/globalassets/product-documents/policy-form/beazley-media-tech-policy-us.pdf.
[87] Aon plc, *Aon Cyber Security Risk Report*: *What's Now and What's Next* 4, 8 (Feb. 2019), https://www.aon.com/getmedia/4c27b255-c1d0-412f-b861-34c5cc14e604/Aon_2019-Cyber-Security-Risk-Report.aspx.

A type of claim that has been discussed previously is the D&O management liability claim for breach of the fiduciary duty of care and due diligence, arising from failure to take adequate measures to implement a cybersecurity program. Part of an adequate cybersecurity program includes appropriate coverage for a type of loss in the event of a cyber incident. As previously stated, the D&O coverage is very broad, and this type of claim could be covered unless a specific exclusion is applied. "So far, neither the courts nor commentators have reached a consensus on how D&O policies should be interpreted. This is because such agreements, on which so much is at stake, are ambiguously written."[88] However, language limiting coverage, such as an exclusion for invasion of privacy or breach of contract, could serve as a legitimate basis for D&O insurers to avoid paying claims arising from cyber incidents. As cyber claims continue to rise, insurance companies are looking for ways to limit coverage while not affecting the current book of business.

An interesting issue that could shape how insurers respond to D&O insurance for cyber claims is the timing of the claim notification. D&O policies have the particularity of having a retroactive date.[89] A retroactive date bars coverage for wrongful acts, as defined in the policy, that occur before a specific date. This policy condition is particularly significant in cyber incidents because breaches often go undetected for extended periods, and companies may take years to discover and report them.

Another basis for excluding cyber incidents from D&O liability is the "failure to maintain insurance" exclusion. The exclusion language is similar to the following:

> "The Insurer shall not be liable to make any payment for Loss in connection with any Claim made against an Insured … alleging, arising out of, based upon or attributable to any failure or omission on the part of any Insured to effect or maintain adequate insurance."[90]

This exclusion outlines the need for adequate cyber insurance in the event of a cyber breach. If there is a cyber breach and the insured has a D&O policy but not a cyber policy, the D&O policy would not cover D&O management liability arising from the failure to have cyber insurance and the resulting financial loss.

---

[88] James W. Hubbell, *Emerging Issues In Directors' And Officers' Liability Insurance Coverage*, 17 COLO. LAW. 1031 (1988); *see generally* Oettle & Howard, D*&O Insurance: Judicially Transforming a 'Duty to Pay' Policy into a 'Duty to Defend' Policy*, 22 TORT & INS. L.J. 337 (1987); Johnston, *Corporate Indemnification and Liability Insurance for Directors and Officers*, 33 BUS. LAWYER 1993 (1978).
[89] Robert D. Chesler & Lisa M. Campisi, *The ABCs of D&O Coverage*, 211 N.J. LAW. 23, 24 (Oct. 2001).
[90] Kevin M. LaCroix, *Executive Protection: D&O Insurance Policy Exclusions*, THE D&O DIARY (Oct. 19, 2010), https://www.dandodiary.com/2010/10/articles/d-o-insurance/executive-protection-do-insurance-policy-exclusions/.

This exclusion could also serve as a loss-control alternative; to activate the D&O insurance, the cyber insurance must be activated as well. Therefore, there is a gap in insurance if a company has D&O but not cyber liability.

Finally, one of the most protected assets of a corporation is the proprietary information and trade secrets. If a cyber breach compromises information, a company can lose its most important assets. Unfortunately, insurance cannot give back the loss of proprietary information. Alternative risk management is necessary to avoid this loss. Finally, the damage to the brand from a cyber breach cannot be undone either. The loss of public faith and brand damage may sometimes mean the end of the business, no matter how much insurance is acquired.

III. Conclusion

There is not one single form of protection against cyber risks. When it comes to adequately implementing a cybersecurity program, companies must be just as meticulous as they are in protecting their tangible assets from risk. Ultimately, failure to act can result in serious financial loss. Corporate risk is not what it was 20 years ago. Corporations were worried about planes flying so low that they could see how they were manufacturing products and steal their business plans. Corporate espionage meant having an infiltrated competitor on the payroll. The distribution of private information meant publishing information in the media. Nowadays, social media runs the everyday life of the public and businesses. An employee can work from home on their cellphone without touching the computer. Admittedly, conducting business is easier but riskier. Information from customers or vendors is uploaded to an internal system for easier access. However, greater accessibility also increases risk.

Initially, corporate officials and D&Os were worried about complying with their fiduciary duties and protecting the company. As new risks evolved, those duties grew as well. Now, as cyber breaches continue to occur, D&Os have the responsibility to protect their companies from them while advancing their technology and expanding public access. It is not a simple task, but it must be carefully addressed. As claims continue to be filed for cyber breaches, regulatory agencies will want to penalize the companies that fail to protect the public.

In response to these emerging risks, the insurance industry has offered various options to help companies protect their assets. However, there are many risks and equally as many insurance policies, and whether a policy responds depends on the specific risk involved. Nonetheless, not every risk is insurable, and insurance only covers financial loss up to the policy's limit.

Finally, as cyber risks continue to evolve and new types of breaches emerge, companies must be prepared to address them effectively. Time is key to keeping the brand intact and maintaining business operations. While corporate officials may not always have the answer, their risk management programs will determine whether they recover from a cyber incident or close their doors forever.