Denver Law Review Forum

Volume 93 Article 31

5-9-2016

Cyber Insurance in International Mergers and Acquisitions

Tanya Fuhrman-Wenman

CYBER INSURANCE IN INTERNATIONAL MERGERS AND ACQUISITIONS

I. INTRODUCTION

Does the recent invalidation of the EU-U.S. Safe Harbor Program, regarding the agreed upon data privacy protection standard of EU citizens' data, pose a specific concern for the merger and acquisition (M&A) transaction lifecycle involving data transfers from the European Union (EU)? During the M&A due diligence period, the acquiring company should evaluate the target's compliance with privacy and data protection laws in all of the international jurisdictions the company operates in. Specifically, the EU Member States enforce privacy and data protection laws that are more far-reaching than U.S. laws in restricting cross-border data transfers or exchanges of EU citizens' personal data from coming into countries such as the U.S. This topic is of critical importance in light of the recent October 6, 2015 court opinion by the European Court of Justice (ECJ) invalidating the EU-U.S. Safe Harbor Program,[1] which operated as a company's self-certification to the U.S. Department of Commerce as being in compliance with the European Commission's "adequacy standard for privacy protection,"[2] and upon the proposed adoption of the EU General Data Protection Regulation (GDPR) requiring costly data breach reporting obligations.

As a result, it is no longer adequate that the target company has certified to the EU-U.S. Safe Harbor Program to sufficiently protect the acquirer's interest, causing instead for the buyer to review not only the target's Safe Harbor certification, but to consider further contractual assurances. In addition to the Safe Harbor certification, further assurances may include transfer agreements and other valid supplementary compliance options approved by the EU data protection authorities.[3] However, are these standard contractual assurances alone sufficient protections from liability in the event of an actual data breach? A data privacy secu-

1. Case C-362/14, Shrems v. Data Prot. Comm'r, E.C.R. (2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031.

2. *U.S. – E.U. Safe Harbor List*, SAFEHARBOR.EXPORT.GOV, https://safeharbor.export.gov/list.aspx (last visited Nov. 20, 2015) (The U.S. Department of Commerce administers the EU-U.S. Safe Harbor Program, processing submissions for company self-certification to the Safe Harbor Framework, including certified companies joined and added to the U.S.-EU Safe Harbor List, searchable by organization details for organization and certification status).

3. *See e.g.*, Jana Fuchs, Dancing the Legal Limbo around US/EU Data Transfers, DATA PROTECTION LAW & POLICY (July 2014) (discussing various types of transfer agreements to supplement the EU-U.S. Safe Harbor Program), http://bryancavedatamatters.com/wp-content/uploads/2015/04/Dancing-the-legal-limbo-around-US_EU-data-transfers-1.pdf.

rity (DPS) transactional risk that is due to the inherent uncertainty of a data breach occurring may often require the additional protection of cyber insurance as a necessary solution to DPS liability. Acquiring companies can effectively manage DPS-related transactional risk by ensuring that the purchase agreement contains the relevant insurance provisions that adequately address the target's business and privacy practices, particularly technology companies where EU data transfers may inevitably be involved. This additional cybersecurity due diligence effort for including an increasingly important consideration to cyber insurance should then further enable an acquirer to effectively manage DPS compliance in the post-closing period as well.

Therefore, this article proposes a transactional risk management solution to the following problem: In light of the invalidation of the EU-U.S. Safe Harbor Program, deal parties in international M&A transactions should require cyber insurance representations and warranties to protect against increasing risks of DPS-related liability exposure for failing to comply with more stringent and costly EU data privacy mandates. Part II discusses the status of the EU and U.S. privacy frameworks in the changing regulatory landscape toward data breach accountability and its costly effect on U.S. and European companies. Part III explains the nature of cyber insurance and how it is currently designed to work for companies in managing DPS risks as a risk transfer option, giving special attention to strategically-based insurance options that may prove quite valuable for a buyer after consummation of a deal and during the post-closing period in the context of an international M&A transaction. In the midst of the pending EU regulatory privacy changes, Part IV proposes cyber insurance as a solution in providing further assurances to a buyer within the representations and warranties for DPS in an international M&A transaction, especially where EU data transfers may be involved. Part V addresses the implications that the regulatory changes may have on the cyber insurance market and on obtaining coverage under certain types of cyber insurance policies. The Article concludes by weighing the risks of the target company with the interests of the acquirer, considering the global changes taking place to steadily increase DPS accountability, to determine whether cyber insurance is a solution to DPS-related representations, and warranties in a particular international M&A transaction.

II. CURRENT EU-U.S. PRIVACY FRAMEWORK INADEQUATE: NEW FRAMEWORK BRINGS ACCOUNTABILITY AND COSTS

As the EU adopts more stringent and costly data privacy mandates, U.S. and European companies will need to find a way to pay for increasing risks of DPS-related liability and associated costs to ensure DPS controls are in place. It becomes increasingly more apparent that the EU and U.S. are at the forefront of "co-regulating accountability as a new global

norm."[4] As a result of the recent court opinion by the ECJ finding the EU-U.S. Safe Harbor framework to be inadequate for data privacy protection,[5] the European Union (EU) is drawing nearer to the costly U.S approach in terms of data breach accountability upon the EU's adoption of its proposed General Data Protection Regulation (GDPR). This changing regulatory privacy landscape will have a costly effect on U.S. and European companies by increasing accountability to both EU data protection authorities, as well as to individuals affected by a data breach; thereby, potentially increasing liability costs and risk allocation by M&A deal parties in terms of government fines or lawsuits.

A. Safe Harbor Framework: U.S.-EU Combined Approaches to Data Privacy Protection

In the past, the U.S. and EU have agreed upon a straightforward standard for handling DPS-related transactional risk through the U.S.-EU Safe Harbor Framework. The U.S. approach to data privacy protection promotes industry self-regulation, as encouraged by both the U.S. Federal Trade Commission (FTC) and the U.S. Department of Commerce (DOC), through implementation by U.S. businesses of industry standards in the various sectors for internal data privacy practices and procedures.[6] Unlike the EU government regulatory approach to protecting privacy with its comprehensive national laws, prohibitions against data collection without a consumer's consent, and requiring companies to register any data processing activities with EU government authorities, the U.S. privacy approach is an ad hoc combination of laws and regulations where "free market and freedom-of-speech principles predominate."[7]

Due to the contrasting approaches to data privacy between the U.S. and EU, the U.S. proposed and the EU agreed to a Safe Harbor Program that has permitted U.S. businesses to avoid EU restrictions on data transfers and continue industry self-regulation conditioned on the business's continuous compliance with seven privacy principles: (1) notice; (2)

---

4. Winston J. Maxwell, *Global Privacy Governance: A Comparison of Regulatory Models in the US and Europe, and the Emergence of Accountability as a Global Norm*, EUROPEAN COMMISSION, https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/dae library/global_privacy_governance_a_comparison_of_regulatory_models_in_the_us_and_europe_and_the_emergence_of_accountability_as_a_global_norm.pdf (discussing binding corporate rules (BCRs) and cross border privacy rules (CBPR) under the APEC Privacy Framework principles for becoming an emerging global privacy governance model)

5. Case C-362/14, Shrems v. Data Prot. Comm'r, E.C.R. (2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031.

6. Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Data Privacy Standard*s, 25 YALE J. INT'L L. 1, 70–74, (2000) (discussing the U.S. data privacy approach leading up to the U.S.-EU Safe Harbor Framework).

7. Cynthia J. Larose & Mintz Levin, *Top 5 Commercial Data Security And Privacy Issues In 2012*,
22 No. 7 WESTLAW JOURNAL MERGERS & ACQUISITIONS 12, 3 (2012).

choice; (3) onward transfer; (4) security; (5) data integrity; (6) access; and (7) enforcement.[8] Since the initial agreement between the U.S. and EU authorities, the Safe Harbor Framework has remained in effect as a valid compliance measure to ensure "adequate" data privacy protection against DPS-related transactional risk for the past fifteen years. However, the Safe Harbor Program is no longer a valid option to remain in compliance with the proposed EU data privacy mandates.

B. Recent Court Opinion by the ECJ Invalidating EU-U.S. Safe Harbor Program

The effect of the invalidation of the Safe Harbor Program on M&A transactions will be the increasing need for parties involved in an international transaction to allocate risk of liability for failing to comply with newly adopted adequacy standards for EU data privacy protection. On October 6, 2015, the European Court of Justice (ECJ) invalidated the European Commission's Decision, 2000/520/EC, from July 26, 2000, concerning the adequacy of the EU-U.S. Safe Harbor privacy principles.[9] In *Schrems v. Data Prot. Comm'r*, Mr. Max Schrems had requested that the Irish Data Protection Authority (DPA) prohibit Facebook Ireland from transferring his personal data to be stored on servers in the U.S., but the DPA refused to investigate Mr. Schrems's complaint.[10] The Court held that the U.S.-EU Safe Harbor Program is invalid because there is no guarantee that personal data of EU citizens transferred to the U.S. will receive adequate privacy protection.[11] As a result of the *Schrems's* judgment, U.S. companies that have relied on compliance with the U.S.-EU Safe Harbor Program must immediately find supplementary compliance options to lawfully conduct cross-border data transfers or exchanges of personal data of EU citizens outside of Europe into the U.S.

Although certification and compliance by U.S. companies with the Safe Harbor program was based on voluntary participation, since international data transfers are not restricted under U.S. law, companies affected by the *Schrems's* judgment are mainly those located in the European Economic Area (EEA) doing business and conducting cross-border data transfers or exchanges with U.S. companies under the Safe Harbor Framework.[12] However, even considering only those particular companies meeting the criteria in the EEA for transacting business with U.S.

---

8. Shaffer, *supra* note 7, at 59–61 (listing the seven privacy principles agreed upon by the U.S.-EU in making up the Safe Harbor Framework).

9. Case C-362/14, Shrems v. Data Prot. Comm'r, E.C.R. (2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031.

10. *Id.* at 2.

11. *Id.* at 107.

12. Lothar Determann, *Data Transfers: U.S. Privacy Safe Harbor—More Myths and Facts*, BNA PRIVACY LAW WATCH: NEWS ARCHIVE (Nov. 9, 2015) (discussing some inaccuracies of analyzing the *Schrems's* judgment).

companies, the companies affected by the recent *Schrems's* judgment are numerous where compliance under the Safe Harbor Program's self-certification has been relied upon for almost two decades. Therefore, allocation of DPS-related transactional risk could be a potential deal breaker in certain international M&A transactions where cross-border data transfers might occur under the EU's proposed General Data Protection Regulation (GDPR).

C. The EU and Colorado: Data Breach Notification, Accountability and Costs

The possibility of a data breach by the target company arising during an M&A transaction can be a potential deal breaker where accountability and costs under newly enacted data breach notification laws and regulations continue to increase on a global scale. To complicate matters even more for a U.S. company that is part of an international M&A deal are the data protection obligations it may be required to comply with in a diverse and complex range of jurisdictions. In particular, the EU's proposed General Data Protection Regulation (GDPR) includes a mandatory data breach notification scheme with an obligation to report a data breach to the relevant data protection authority (DPA), giving DPAs' enforcement responsibility to impose penalties and fines of up to "five percent" of a company's annual global revenue in the case of negligence or a data breach.[13] On November 19, 2015, the EU Data Protection Supervisor (EDPS) issued an opinion defining "accountability" as responsible business practices in performing data protection impact assessments and audits, as well as designating a data protection officer or related expert on staff to ensure the effective functioning of an "accountable internal control system."[14]

Under Colorado's mandatory data breach notification law, the attorney general treat data breach or non-compliance violations , in relevant part, by bringing "an action in law or equity to address violations . . . and for other relief that may be appropriate to ensure compliance . . . or to recover direct economic damages resulting from a violation, or both."[15] Additionally, Colorado permits an individual or commercial entity to use its own "information security policy" and procedures that are "consistent with the timing requirements" stated in the statute, as well as permitting the use of the procedures established by another state or federal law which regulates that particular individual or commercial entity, in order

---

13. William Long, *EU General Data Protection Regulation Comes into Sharper Focus*, COMPUTER WEEKLY, (July 21, 2015).

14. Giovanni Buttarelli, *Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design And Accountability*, EUROPEAN DATA PROTECTION SUPERVISOR, (Nov. 19, 2015), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf.

15. COLO. REV. STAT. § 6-1-716(4) (2010).

to be in compliance with Colorado's procedure for notice requirements.[16] In sum, Colorado does not impose any set penalty or fine for a violation of non-compliance in the event of a data breach, operating more on a case-by-case basis, and maintains flexibility in its required notification procedures that require only "the most expedient time possible and without unreasonable delay."[17] Therefore, a company may risk subjecting itself to multiple and uncertain financial penalties and regulatory fines for any non-compliance under a wide range of data breach notification laws and regulations, with varying notice requirements, for all the various locations in which it does business. As a result, an acquiring company in an international M&A transaction will want additional assurances by the seller to further support its DPS-related representations and warranties, such as global cyber insurance coverage, during the pre and post-closing periods in the M&A transaction lifecycle.

III. WHAT IS CYBER INSURANCE AND HOW DOES IT WORK?

In light of the changes and additions being made globally in data breach notification laws increasing accountability and costs, and in order for the acquiring company to protect the value of its investment in the target company, the buyer and seller should negotiate cyber insurance into a coordinated insurance program to provide added protection in the event of a data breach incurring unexpected losses or liabilities, including insurance protection into the post-closing period of an international M&A transaction. The definition of "cyber liability insurance cover" is defined, generally, through identifying the elements and typical span of cyber policy coverage by insurers, including four main areas of cover: (1) data breach/privacy crisis management cover; (2) multimedia/media liability cover (e.g., intellectual property infringement, defamation, etc.); (3) extortion liability cover (e.g., confidential information, securities, etc.); and (4) network security liability cover.[18] The first area of cover noted above, involving "data breach/privacy crisis management," is often the primary reason for seeking cyber insurance in order to protect against costly expenses attributed to an actual data breach incident, including regulatory fines arising from data breach notification laws as well as the associated notification and credit monitoring costs to each victim affected by the breach, along with litigation costs and investigations. In terms of global importance, any U.S. business that has a virtual presence, such as an online website, that serves, or has a potential to serve, customers from the EU is essentially at risk of violating the EU's stringent privacy laws restricting data transfers by the mere act of receiving and processing

16. COLO. REV. STAT. § 6-1-716 (3)(a)–(b) (2010).
17. COLO. REV. STAT. § 6-1-716 (2)(a) (2010).
18. Sarb Sembhi, *An Introduction to Cyber Liability Insurance Cover*, COMPUTER WEEKLY, (July 2013), *available at* http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover.

the EU customer data.[19] For example, the EU's proposed GDPR would attach to a U.S. business that is involved in the collection and processing of EU citizens' data for marketing purposes of selling goods or services, and in the behavioral monitoring aspect to understand individual preferences or habits.[20] Therefore, a seller of the target company should consider its global cyber risk transfer options, as well as post-closing insurance options, in order to provide support for its DPS-related representations and warranties given for the buyer's acceptance.

A. Cyber Risk Transfer Option: Cost to Coverage Level; Types; Exclusions; Claims Process

The appropriate type and coverage level of insurance needs to be determined to adequately protect the acquiring company's interest in the target company. The reported average cost for $1 million of coverage ranges from $12,500 to $15,000 depending on the type of data held by a company, such as sensitive consumer information, and the specific type of industry being covered, noting that retailers, healthcare firms and financial services companies are considered high-risk sectors to insure at a higher premium.[21] Example coverage levels of retailers, recently targeted by data breaches, and their policies include: Target's $100 million cyber insurance policy; Home Depot's $105 million policy; and Sony's $60 million policy.[22] At present time, American International Group, Inc. (AIG) is a major carrier of cyber insurance, in its product called "CyberEdge," that covers both third-party claims arising from a data breach along with the corresponding direct first-party costs associated with the data breach incident.[23] Depending on the specific type of cyber policy, exclusions and limitations may involve excluding coverage for the defense, loss, injury, damage, costs or expenses arising out of acts of war, false or misleading advertising, government action, intellectual property, prior notice of a reported security failure that was known to the insured prior to the establishment of its policy, or a failure to protect or comply, in the absence of exercising any duty of care, with any law concerning personal and confidential information.[24]

---

19. Dan Jerker B. Svantesson, *The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses*, 50 STAN. J. INT'L L. 53, 74 (2014) (analyzing extrajurisdictional claims directly impacting U.S. business activities overseas).

20. Long, *supra* note 13.

21. Keith Kirkpatrick, *Cyber Policies on the Rise*, COMMUNICATIONS OF THE ACM VOL. 58 NO. 10 (2015), http://cacm.acm.org/magazines/2015/10/192376-cyber-policies-on-the-rise/fulltext (discussing also the inadequacy of the policy coverage levels in light of the retailers' data breaches).

22. *Id.*

23. *CyberEdge: End-to-End Cyber Risk Management Solutions*, AIG.COM, http://www.aig.com/chartisint/internet/US/en/files/AIG_CyberEdge0418finalsingle_tcm1247-575268.pdf (last visited December 8, 2015).

24. *CyberEdge PC*, AIG.COM, http://www.aig.com/chartisint/internet/US/en/files/CyberEdge%20PC%20Policy%20Final%202014_tcm1247-595896.pdf (last visited December 8, 2015).

Therefore, it is important to select the appropriate types of coverage to fit a company's cyber risks, including any international cyber exposure and regulatory compliance issues. In particular, "first-party" insurance typically covers damage to digital assets, business/service interruptions and reputational harm as contrasted to "third-party" insurance that covers liability concerning data breach notification and related litigation costs as well as regulatory fines; however, a cyber policy still needs to be worded specifically to effectively include "multifaceted" risk response coverage to match an insured's "actual" cyber exposure.[25] AIG also has a global cyber program, in its service platform called "Passport," that is aimed to address global cyber exposure by establishing a "worldwide policy" along with any "requested locally-admitted policies" issued from AIG's local offices located in various countries to ensure compliance and adaption with any local regulations, industry practices, or certain types of cyber exposure unique to a particular country.[26]

A major obligation of an insured covered under an AIG CyberEdge Policy is to report, without delay, a triggering event that is then handled by its breach resolution team devoted to handle cyber-specific, first-party and third-party claims for any suspected, potential, or actual data breach.[27] Cyber event response coverage attaches and payment of a claim is made for "event response costs" only after the insured provides AIG, in writing, with a detailed proof of loss as a result of the triggering event.[28] A 2012 study of actual claims payouts for covered data breaches, conducted by NetDiligence, found that, of the submitted claims payout information provided by major cyber liability underwriters from fifty-eight events, payouts associated with the events included legal damages and crisis services as the two largest components of costs paid on the claim.[29] It should also be noted that three main issues in recent cyber insurance litigation have included disputes concerning the scope of policy coverage in determining fraudulent or unauthorized system access, intentional or negligent acts, and the extent of considering a policyholder's internal cybersecurity measures, risk-management techniques and mitigation practices.[30] Deal parties need to cautiously consider these liti-

---

25. Lucian Constantin, *5 Things You Need to Know: Cybersecurity Insurance*, CIO MAGAZINE (Apr. 25, 2014), http://www.cxo.com.

26. *Supra* note 23.

27. *Supra* note 24.

28. *Id.*

29. Mark Greisiger, *Cyber Liability & Data Breach Insurance Claims: A Study of Actual Payouts for Covered Data Breaches*, NETDILIGENCE, (Oct. 2012), http://www.netdiligence.com/files/CyberClaimsStudy-2012sh.pdf.

30. Molly McGinnis Stine & John F. Kloecker, *Everything Old is New Again: Issues in Recent Cyber Insurance Litigation*, LOCKE LORD LLP (July 28, 2015), http://www.lockelord.com/newsandevents/publications/2015/07/everything-old-is-new-again (discussing three cases: *Universal Am. Corp. v. Nat'l Union Fire Ins. Co.*, 25 N.Y. 3d 675 (2015); *Travelers Prop. Cas. Co. v. Federal Recovery Servs., Inc*., 103 F.Supp.3d 1297 (2015); *Columbia Cas. Co. v. Cottage Health Sys*., No. 2:15-cv-03432 (C.D. Cal., May 7, 2015).

gated issues since legal damages may create the largest financial losses and costs to an acquiring company after the closing of an M&A deal.

B. M&A Post-Closing Insurance Considerations

Cyber insurance can be used as additional protection for specific DPS transactional risk in an M&A deal where other types of insurance coverage prove inadequate. The National Association of Insurance Commissioners (NAIC) has stressed the need for an additional cyber-specific liability insurance policy to adequately cover cyber-related risks.[31] The NAIC cautions against a company's overreliance on its standard commercial insurance policy for covering increasing risks of cyber-related liability because such a standard policy is limited in providing protection for only general liability coverage, such as injury to the business or property damage, not for covering the unique and complicated risks of cyber liability exposure.[32] As a result, a buyer in an M&A transaction should negotiate one or more additional layers of insurance protection against the target company's risks of cyber-related liability exposure in the event that any unexpected losses or liabilities arise, such as a data breach, after the closing of the transaction. Importantly, the target company's insurance policies will likely cancel coverage upon the consummation of the deal, leaving the acquiring company with any financial losses, unless certain insurance options are coordinated together to adequately protect the buyer into the post-closing period as well.

Because most insurance options can be in the form of primary or excess insurance,[33] parties in an international M&A transaction can seek a coordinated insurance program that includes an additional layer of cyber-specific liability insurance protection along with other post-closing insurance options. For example, Seth Gillston at ACE USA points out a number of M&A insurance options aimed to prevent the acquiring company from inheriting a target company's liabilities that may arise after the transaction closes.[34] Specifically, a Loss Portfolio Transfer (LPT) is a "retroactive insurance program" for previously-incurred liabilities, as well as legacy liability insurance that "absorbs successor liabilities for both retrospective and prospective claims" arising from prior acts by the target company.[35] For an international M&A transaction, a controlled

---

31. *Cyber Liability Policies*, NATIONAL ASSOC. OF INS. COMMISSIONERS, http://www.naic.org/cipr_topics/topic_cyber_risk.htm (last visited Dec. 9, 2015).

32. *Id.*

33. *See e.g.*, *CyberEdge PC*, AIG.COM, http://www.aig.com/chartisint/internet/US/en/files/CyberEdge%20PC%20Policy%20Final%202014_tcm1247-595896.pdf (last visited Dec. 8, 2015); *see also HCC Products*, HCC.COM, http://www.hcc.com/DivisionsProducts/HCCGlobalFinancialProductsHCCGlobal/English/Products/tabid/685/Default.aspx (last visited Dec. 9, 2015).

34. Seth Gillston, *Risk Management Pitfalls in Mergers and Acquisitions*, TREASURY & RISK (Feb. 19, 2014), http://www.treasuryandrisk.com/2014/02/19/risk-management-pitfalls-in-mergers-and-acquisitio?t=risk-management&page=4.

35. *Id.*

master program (CMP) is a type of insurance that identifies the "potential inadequacies of the target company's local or admitted insurance policies," including international exclusions, by coordinating foreign insurance policies.[36] Similarly, AIG's "Passport" global cyber program, mentioned above, operates as a CMP in coordinating its policyholder's worldwide policy with locally-admitted policies.

Another post-closing insurance option that may adequately protect an acquiring company's interest when coordinated with an additional cyber insurance policy is representations and warranties insurance in an M&A context, such as a seller's representations and warranties concerning a target's compliance with local DPS-related regulations and contractual assurances with EU data protection authorities for cross-border data transfers that are later proved to be inaccurate, that indemnifies the buyer for the discovered inaccuracy.[37] HCC Global provides such international transaction risk insurance (TRI), also known as warranty and indemnity (W&I) insurance, that is available for corporate-level business transactions that include mergers and acquisitions.[38] Further, a target company's directors' and officers' (D&O) liabilities can be covered under a non-cancellable, pre-paid policy that a target company purchases for up to a six-year period, known also as a run-off or tail coverage.[39] Additionally, HCC Insurance Holdings, Inc. provides professional cyber liability insurance in the U.S. for corporate leaders, covering D&Os' first-party risks of cyber liability exposures as well as third-party liability protection.[40] Both HCC insurance options, mentioned above, are flexible in the form of either primary or excess insurance coverage based on an acquiring company's needs. These additional insurance options to transfer cyber risks, including international cyber insurance coverage, may help to supplement standard contractual assurances for EU data transfers where such assurances fall short of a complete solution in adequately covering DPS liability for an acquirer's interest in the event of an actual data breach of the target company.

IV. PROPOSED SOLUTION: CYBER INSURANCE IN REPS & WARRANTIES

Cyber-specific insurance may prove to be an effective solution for enhancing the value of the buyer's investment in the target company's digital assets in an M&A deal and in preventing DPS transactional risk

---

36. *Id.*
37. *Id.*
38. Product Sheet, Transaction Risk Insurance, HCC.COM (Nov. 2015), http://www.hcc.com/Portals/0/Subsites/HCCGlobal/downloads/HCC%20Global%20TRI%20-%20English.pdf.
39. Gillston, *supra* note 34.
40. Product Sheet, Professional Cyber Liability, HCC.COM http://www.hcc.com/DivisionsProducts/HCCGlobalFinancialProductsHCCGlobal/English/Products/ProfessionalCyberLiabilityUS/tabid/1083/Default.aspx (last visited Dec. 9, 2015).

from being a potential deal breaker when conducting cybersecurity due diligence on a target's high-risk profile. Cyber insurance can be particularly effective when a cyber insurance provider is also the target company's auditor who will assist in the cybersecurity due diligence process and ongoing cyber risk management consultations. The inclusion of cyber insurance in the purchase agreement involving an international M&A deal may be an especially important measure to manage DPS-related transactional risk where the target company is involved in transferring personal information from Europe, is a multinational corporation operating internationally and within Europe, or when a European company is involved in the transaction and requests further contractual assurances for data privacy protection by a U.S. company. For these reasons and from those set out above in Part III of this article, during the M&A due diligence period, the acquiring company's review of a target company's compliance with relevant international DPS laws, including any EU transfer arrangements and regulatory approvals from the necessary EU data protection authorities, should also include considerations to negotiating the inclusion of cyber insurance provisions into DPS-related representations and warranties. Additionally, the specific details for the precise wording in cyber insurance provisions should strategically reflect the target's risk profile, its digital assets, and insurer/auditor risk management program controls.

A. Assess Cross-Border DPS-Related Risks of Target

Understanding and carefully assessing the target company's risk profile under the EU's proposed GDPR is essential to DPS transactional risk management in the international M&A due diligence process since this will inform negotiations for the buyer in order to pinpoint the most effective type of cyber insurance coverage as well as coverage level needed to adequately protect its interest. In being mindful of assessing appropriate cybersecurity measures to determine whether or not an "accountable" internal control system is in place, as discussed above in Part II of this article, a major focus should be on asking the right questions concerning cross-border data transfers and exchanges. Specifically, the acquiring company should determine the global reach of the target's business practices in the handling of personal information concerning EU citizen data and various compliance measures, as follows:

i. Global Reach and Foreign Accessibility to Personal Information

Does the company maintain any global or regional databases or applications that store personal data? If so, have the company identify each and describe the functions (e.g., enterprise resource planning systems, software-as-a-service or other cloud solutions, e-mail, collaboration tools, customer relationship management databases, etc.).

ii. Transfer Arrangements: 'In Addition to' Safe Harbor Certification

Does the company have an established approach to address cross-border data transfer restrictions under non-U.S. data protection laws (e.g., individual consent, standard contractual clauses, binding corporate rules)? Ask the company to explain in detail.

iii. EU Regulatory Approvals

Ascertain whether the company has completed registrations with any non-U.S. data protection authorities or taken steps to comply with non-US data protection laws.[41]

Once there is a complete understanding of the target company's data flows and the relevant technologies have been tracked from the acquirer's due diligence efforts, more effective negotiations may be conducted for "insuring" the target's transactional risks in DPS representations and warranties with regard to cross-border data transfer and exchanges. This will also help in the next stage, discussed below, when determining specific insurance coverage of the target's digital assets and in gaining the cooperation from the insurance provider with insurer-based cybersecurity due diligence audits.

B. Negotiate and Tailor Cyber Insurance to Digital Assets and Insurer Audits

As discussed in Part III of this article, a buyer may want a coordinated insurance program that will protect its long-term, post-closing, interest for investment in the target company. To negotiate the most cost-effective options for a cyber insurance policy with cooperation from the actual cyber insurer, negotiating the inclusion of cyber insurance provisions into DPS-related representations and warranties is a strategic process that also includes prioritizing insurance coverage of the target company's "digital crown jewels," the crafting of clear and "unambiguous" wording, and in tying cyber insurance to "audits." As Daljitt Barn, director of cybersecurity at PricewaterhouseCoopers, advises, "the best approach is to identify and secure the company's digital crown jewels, then quantify and insure the remaining risk"[42] because it is too cost prohibitive to broadly protect against all cyber threats.[43] Therefore, efficient cyber insurance protection is all determined in the details of coverage type(s) and levels to compensate adequately any of the buyer's future financial losses or liabilities after acquiring the target company. Being of

41. *See* Brian Hengesbaugh & Harry A. Valetk, *Buyer Beware: Merger-and-Acquisition Diligence Tips to Reduce Data Privacy & Security Risks*, BLOOMBERG BNA PRIVACY & SECURITY LAW REPORT, 13 PVLR 39 (Oct. 6, 2014).

42. Constantin *supra* note 25.

43. *Id.*

critical importance, companies should carefully craft clear and unambiguous wording in a policy and related insurance provisions to match the exact pre and post-closing needs of the one it is intended to insure,[44] namely the acquiring company's interest, with the target's most valuable digital assets.

A target company should also provide a self-assessment questionnaire that reviews any existing cross-border data transfer agreements, including outsourcing of its technology for data security issues, as well as provisions related to insurance and indemnification that a data breach could trigger.[45] Additionally, cyber insurance should tie to cybersecurity audits conducted by the actual cyber insurer to enable reduced premiums in negotiating risk management controls and for showing that a cybersecurity program is in place.[46] For example, the AIG cyber insurance provider, analyzed above in Part III of this article, has partnered with K2 Intelligence in order to use K2 Intelligence's experts for assisting AIG's policyholders in their "cybersecurity due diligence" efforts related to an M&A transaction.[47] Furthermore, the combination of the target company's internal controls, its cybersecurity measures and cyber insurance will be consistent with the changing regulatory compliance standards of the EU's proposed GDPR requirement for maintaining an "accountable internal control system" where the target's handling, transfer or exchange of personal information from the EU may exist.

V.IMPLICATIONS OF REGULATORY CHANGES ON CYBER INSURANCE

When standard representations and warranties for DPS are not enough, the inclusion of cyber insurance may help to supplement against the inherent uncertainties in DPS-related transactional business risks; however, insurers and various regulatory authorities may exclude, condition, or adjust insurance policy coverage and premiums in response to newly enacted DPS laws and regulations accordingly. As a result, cyber insurance is continuously evolving along with regulatory changes in data protection being implemented, impacting the cyber insurance market, and increasing the need for third-party cyber insurance.

---

44. Richard Levick, *Cyber Crisis Insurance: GCs and their Companies Face Major Decisions*, INSIDECOUNSEL, (Apr. 29, 2015) http://www.insidecounsel.com/2015/04/29/cyber-crisis-insurance-gcs-and-their-companies-fa.

45. Richard Levick, *Cyber Crisis Insurance: GCs and their Companies Face Major Decisions*, INSIDECOUNSEL, (Apr. 29, 2015) http://www.insidecounsel.com/2015/04/29/cyber-crisis-insurance-gcs-and-their-companies-fa (discussing steps general counsel should take in its company's self-assessment for a cyber insurance application).

46. Noah G. Susskind, Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know, 11 N.Y.U. J. L. & BUS. 573, 613 (2015) (discussing also strategies for international companies in managing cyber risk).

47. *Supra* note 23.

A. State of the Cyber Insurance Market: U.S. and Abroad

U.S. companies have already been taking advantage of cyber-specific insurance coverage at a national level; however, expect an increase to a "global" policy at an international level upon the adoption of the EU's proposed GDPR as well. According to broker Marsh & McLennan, the U.S. accounts for the majority share of the cyber insurance market at approximately $1 billion in premiums involving roughly thirty-five carriers, with Europe accounting for a small fraction of that amount with only approximately $150 million in premiums, with the remaining balance of the policy value shared throughout all other countries.[48] The U.S. being the leading market for cyber insurance policies has been attributed to the "[forty-seven] state privacy laws that require companies to disclose data breach incidents," based on the analysis of Christine Marciano, president of Cyber Data-Risk Managers LLC, a Princeton, NJ-based cyber-insurance broker.[49] Neil Gurnhill, head of digital risk at brokerage Safeonline L.L.P. in London, has agreed with Marciano's analysis in similarly stating, "[O]ne of the drivers of cyber insurance buying in the United States has been the steps that need to be taken to notify most state legislatures of breaches."[50] A Fortune 500 company study revealed also that loss of confidential data, loss of reputation, malicious acts, and liability are the top concerns of companies for obtaining cyber insurance policies.[51] It is further predicted that the trend toward cyber insurance will continue to increase since public companies covered under cyber policies are permitted to have reduced disclosure obligations concerning cybersecurity risk with the U.S. Securities and Exchange Commission (SEC).[52] Additionally, as new competitors are expected to enter the market in the near future, insurance capacity will only increase to keep premiums lower.[53]

In the U.S., the Federal Insurance Office (FIO) and the National Association of Insurance Commissioners (NAIC) have given some regulatory recognition to the positive relationship between "expanding the cyber risk marketplace" by increasing access to cyber insurance and significant "risk mitigation" in cybercrimes by requiring that companies implement more effective risk management systems before being ap-

48. Kirkpatrick, *supra* note 21

49. *Id.*

50. Sarah Veysey, *European Union Gets Serious about Data Protection: Upcoming Law Tightens Cyber Breach Enforcement*, BUSINESS INSURANCE, http://www.businessinsurance.com/article/20150802/NEWS06/308029995/european-union-gets-serious-about-data-protection?tags=%7C75%7C83%7C302 (Aug. 3, 2015).

51. Christian Biener, Martin Eling & Jan Hendrik Wirfs, *Insurability of Cyber Risk: An Empirical Analysis*, PALGRAVE-JOURNALS (June11, 2014), http://www.palgrave-journals.com/gpp/journal/v40/n1/pdf/gpp201419a.pdf.

52. *See* Noah G. Susskind, Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know, 11 N.Y.U. J. L. & BUS. 573, 613 (2015) (discussing the rationale for the SEC allowing reduced disclosure for cyber insured public companies).

53. *Id.* at 600.

proved for coverage.[54] However, aside from receiving some economic incentives from cyber insurers for having an adequate cybersecurity program in place, calculating cyber insurance premiums along with the necessary coverage level is still often challenging. Therefore, an international M&A deal involving a target company's sensitive consumer information within a high-risk industry sector should be calculated cautiously for a cyber policy coverage level that adequately protects any potential losses to an acquirer's interest. However, since calculating the precise coverage level necessary in advance of a potential data breach is not often feasible, using cyber-specific insurance as an "additional" layer of protection in a coordinated insurance program with other post-closing insurance options may provide, together, the best protection for an acquiring company.

B. EU's Increased Need for Third-Party Cyber Insurance

When economically feasible, and depending on a target company's risk profile, combining cyber insurance coverage types together may provide the most diverse coverage for safeguarding against any inherent uncertainty for the manner in which a possible data breach and corresponding regulation(s) may end up affecting a company. As shown above, the U.S. and EU insurance markets differ in maturity where third-party insurance is most common in the U.S., due to its established data breach notification laws, and first-party insurance is presently more common in Europe; however, that scope is expected to change to a rapidly growing need for third-party insurance upon the proposed adoption of the EU GDPR requiring strict data breach notification obligations and costly fines.[55] In addition, although the EU's proposed GDPR may cause an increased demand for third-party cyber insurance, generally, legal restrictions are also expected to prevent specific types of cyber insurance coverage to be available since the ability to insure against regulatory fines is prohibited within many countries.[56] Further, the GDPR would significantly impact insurers for making adjustments to many present policy conditions when the new regulation is adopted.[57] The uncertainties involved in regulatory changes that are making insurers react are due to "data scarcity."[58] However, as data becomes available, cyber policy conditions should adjust to the new data and will likely generate fairly-priced premiums over time as a result of the increased market development.[59] In sum, some insurers are already providing flexibility in certain

54. Peter H. Bickford, *Cyber Insecurity*, INSURANCE ADVOCATE, (Apr. 27, 2015), http://www.insurance-advocate.com/magazine/ (discussing New York State's inconsistent views on the cyber insurance market).

55. *Supra* note 25.

56. Biener, Eling & Wirfs, *supra* note 51.

57. BIENER, ELING & WIRFS, *supra* note 56.

58. *Id.*

59. *Id.*

established global cyber policies, such as AIG's "Passport" service platform, discussed above in Part III of this article, which adapts and conforms to local DPS regulations, and this will likely become the norm as insurers attempt to meet the increasingly complex cyber risk transfer needs of companies operating globally.

VI. CONCLUSION

In conclusion, changes in international data breach notification requirements for increasing accountability and costs are necessitating a growing need for a buyer to negotiate DPS representations and warranties that include cyber insurance provisions within the purchase agreement for an international M&A deal, particularly when involving the probability of EU data transfers occurring in a target company's business practices, in order to more sufficiently protect the acquirer's interest. Specifically, reliance on a cyber-specific insurance policy as a cyber risk transfer option may be best utilized as an "additional" layer of insurance protection within a coordinated insurance program that also includes consideration to post-closing insurance options for protecting the value of an acquiring company's long-term interest with its investment in a target company. The determination for cyber insurance provisions should be weighed only after fully understanding a target's risk profile, in terms of cross-border DPS transactional risk, and in prioritizing digital asset protection with insurer audits during the cybersecurity due diligence period of the M&A transaction lifecycle. However, as the state of the cyber insurance market is still evolving and reacting to new regulatory changes in data protection, especially in the EU, there will likely be adjustments by insurers in policy conditions and premiums. Most importantly, an acquiring company needs to carefully craft insurance provisions to fit the exact needs of the acquirer's interest as the "intended" insured, considering both pre and post-closing periods of the M&A transaction lifecycle, and calculate the cyber policy coverage level to accurately reflect any sensitive consumer information in a high-risk industry of the target company for adequately protecting against unexpected financial losses or liabilities. In sum, these "direct bottom-line consequences"[60] should naturally drive the solution for inclusion of cyber insurance provisions in international M&A transactions.

Tanya C. Fuhrman-Wenman[†]

60. Richard Levick, *Cyber Crisis Insurance: GCs and their Companies Face Major Decisions*, INSIDECOUNSEL, (Apr. 29, 2015) http://www.insidecounsel.com/2015/04/29/cyber-crisis-insurance-gcs-and-their-companies-fa (discussing the emerging role of general and outside counsel for having responsibility in data breach response plans).

† LL.M Candidate, International Business Transactions, May 2017; J.D., 2007, University of Denver Sturm College of Law; M.S. Information Management & Library Information Science, 2013, Syracuse University School of Information Studies, Syracuse, New York.