Cyber Liability: Data Breach in Europe[1]

By: Elena Jelmini Cellerini and Christian Lang

Elena Jelmini Cellerini is a senior claims expert for EMA where she deals with complex and multijurisdictional matters. She's also Swiss Re Corporate Solutions Global Practice Leader for Cyber Claims.

Christian Lang is Swiss Re Claims Key Case Advisor for EMEA and Asia/Pacific. In this capacity, he deals at group level with the largest exposures of Swiss Re's Property & Casualty business and supports the regional claims teams in legal matters.

How often has your data been hacked? Have you received a notice from your bank recently about suspicious transactions? Have you already adapted to the "new reality" of data (in)security?

Although the topic of cyber security is much broader than the data breach example, the media focus is usually on data breaches, which occur at a higher frequency than other cyber events. Ransomware attacks, where hackers encrypt data on the targets' computers and only release it in return for the payment of a ransom, have increased substantially in the

[1] Repurposed for the membership of the International Association of Defense Counsel and the *Defense Counsel Journal* in collaboration with Swiss Re Ltd. Although all the information discussed herein was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the information given or forward-looking statements made. The information provided and forward-looking statements made are for informational purposes only and in no way constitute or should be taken to reflect Swiss Re's position, in particular in relation to any ongoing or future dispute or be construed to be legal advice. In no event shall Swiss Re be liable for any loss or damage arising in connection with the use of this information and readers are cautioned not to place undue reliance on forward-looking statements. Swiss Re undertakes no obligation to publicly revise or update any forward-looking statements, whether as a result of new information, future events or otherwise.

last couple of years. However, data breaches have so far generated the majority of the cyber-related insurance claims, which is why we limit the scope of this article to those types of events.

While data breaches might have become commonplace, their effect on the breached entity (and the affected individuals) are often far-reaching. The majority of headline-making data breaches have occurred in the United States, but cyber-attacks are a global issue, affecting the economy worldwide. The recently implemented new European General Data Protection Regulation (GDPR)[2] is expected to lead to more reported cyber events in the European Union.

This article looks at the consequences of a data breach in Europe and compares the situations in Europe and the U.S. with regard to the major features of such an event. Watching the case law developing, in particular in the UK which has taken some landmark decisions in this area, is also an indicator for where Europe seems to be heading. The UK intends to fully implement the GDPR in spite of Brexit.[3]

The cyber insurance market is growing constantly, but the penetration of cyber coverage is still small relative to the value of the tangible and intangible assets that could be impaired by a cyber security breach.[4] According to an AON/Ponemon study, in 2015 only around 12% of information assets were covered by insurance.[5] Since then, the market has grown, but a huge protection gap still remains.

I. Background

A. What is a data breach and why is coverage so critical?

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), available at http://ec.europa.eu/justice/data-protection/reform/files/ regulation_oj_en.pdf.

[3] *See* Transcript from UK Parliament, Testimony of Secretary of State for Culture, Media and Sport, November 7, 2016, available at https://hansard.parliament.uk/commons/2016-11-07/debates/1611071000004/InformationCommissioner%E2%80%99SOfficeTriennialReview#36WS. While the UK will implement the GDPR as planned, changes are possible after the country leaves the EU.

[4] *See generally* SwissRe, *Cyber risk: getting to grips with a complex risk*, *Sigma,* No. 1, January 20, 2017, available at http://www.swissre.com/library/sigma_01_2017_en.html (last visited June 6, 2018).

[5] Aon/Ponemon Institute, *2015 Global Cyber Impact Report*, April 2015, at 6. Available at http://www.aon.com/risk-services/thought-leadership/2015-global-cyber-impact-report.jsp?utm_source=aon.com&utm_medium=banner&utm_campaign=ponemon (last visited June 6, 2018).

One of the current problems for data owners is that they often have no control over where their data actually goes. Service providers manage the data, and many of these providers use sub-contractors for certain tasks. This is the reality of the connected world in which we live; data is stored in different places way beyond the control and the reach of the data owner's judiciary.[6] The perpetrators' methods are similar, irrespective of where the data breaches occur. The targets of cyber-attacks are often companies that store large volumes of data for themselves, or for third parties.

The most frequent data breaches involve personal information like names, addresses, credit card and account numbers, health insurance numbers, PIN-codes, Social Security numbers and other financial information of a large number of individuals. It is important to note that although laws give a definition of what personal data is (usually any information allowing to identify the person directly or by combining data elements), these laws keep changing. Courts around the world continue to broaden those definitions. For example, a zip code has been considered personal data, and so has a person's browsing history on Google.[7] Furthermore, the European Court of Justice decided on October 19, 2016 that IP addresses may now also be considered "personal data".[8]

A "breach" of such data takes place when unauthorized individuals view, copy, steal or use such information in any other way.

B. Who are the (h)actors and what are they after?

Hackers' motives can be several, such as fun, political, religious, or – presumably most often – financial gain. Behind most of the publicly disclosed cases (e.g. Target, Ashley Madison, Equifax, Uber), these unauthorized individuals were supposedly professional hackers.[9]

---

[6] Microsoft successfully challenged a U.S. warrant seeking e-mails stored on a server in Dublin, Ireland. The case defined for the first time the limited reach of U.S. warrants when it comes to data stored outside of the United States. However, the decision does not limit the government from seeking assistance from the country where the information is hosted by way of judicial assistance.

[7] https://www.judiciary.gov.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf.

[8] Case C-582/14 *Breyer v Republik Deutschland* [2016] ECLI :EU :2016 :779, Available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1034974.

[9] But this is not always true. One of the most publicized European data breaches, the hack of the broadband firm Talk Talk, was committed by a 16-year-old teenager who wanted to impress his friends. *See Boy, 17, admits hacking offences linked to TalkTalk attack*, SKYNEWS, Nov. 15, 2016, available at

The so-called "dark net"[10] has become a lively market place for stolen data that can be used for identity theft, credit card fraud, and other criminal activity.

Identity theft is when criminals use someone's name, credit rating, health insurance number, or any other stolen data to gain a financial advantage in that person's name, including obtaining goods, services, credit or other benefits.

Credit card fraud is a particular form of identity theft, involving a payment card as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.[11]

Extortion cases are not limited to so-called distributed denial of service attacks (DDoS) or ransomware attacks, but also take place in connection with data breaches. In such cases, the hackers steal data and threaten to disclose it publicly unless a certain sum of money is paid,[12] often in bitcoins. This is often easy and quick money for the hackers because they don't need any infrastructure to "monetize" the stolen data.

Cases of cyber espionage, including IP theft, whether against private companies, states or governmental institutions, take place, too, but rarely become public. Usually, these situations do not give rise to large insurance claims. This article, therefore, does not look at such events.

---

http://news.sky. com/story/boy-17-admitsadmits -hacking-offences-linked-to-talktalk-attack-10658405.

[10] The "dark net" mainly consists of webpages which are both provided and can be accessed anonymously. They are not indexed and hence, cannot be found via Google or other search engines. Access is only possible via browsers that support special anonymization technologies. Furthermore, for illicit activity, actors often use web-forums within the dark net, and access to those forums is often restricted to admitted users/conspirators. While there is also a lot of legitimate activity such as information sharing platforms for journalists, whistleblowers, political chat rooms, instant messaging services, artist platforms, the dark net has become infamous mainly for the illegal activity which takes place there. The currency used is normally bitcoins. *See* Steven Viney, *What is the dark net, and how will it shape the future of the digital age?*, ABCNEWS, July 20, 2017, available at http://www.abc.net.au/news/2016-01-27/explainer-what-is-the-dark-net/7038878.

[11] In the case of credit card fraud, the person whose data has been stolen usually does not suffer a loss because the fraudulent transactions will not be charged to him/her but rather picked up by the banks and credit card companies participating in the transaction.

[12] Amounts are usually relatively low (USD $20,000 to $30,000). The total amount paid in ransom globally was estimated at more than USD $1 bn per year by former FBI Agent James Trainor; *see* Handelsblatt, Düsseldorf, January 13, 2017.

C. Reaction to a data breach

When an entity is faced with a breach, it is dealing with an immediate crisis. The consequences of losing someone else's data can be harsh – both for the person to whom the data relates and to the entity which has caused or suffered the breach.[13] The major elements of a breach response include the following:

Forensic investigation: the breached company requires IT specialists to perform a forensic investigation to assess what happened. This investigation will deter-mine what data was accessed and/or stolen, start date of the intrusion, whether the hackers are still within the system, and how to restore lost or corrupted data. This part of the breach response is similar around the world.

Public relations: it is vital for a breached entity to carefully manage communication to mitigate reputational damage to the company and potential corresponding loss of business. The economic damage caused by loss of business after a breach has often been far larger than the costs actually spent on the breach response.[14] Poor communication can have a major impact on the company's reputation and, therefore, the overall loss. This part of the action plan is mainly influenced by the relevant market and less so by the jurisdiction in which the breached entity operates.

Notification: depending on the relevant jurisdiction(s), the breached entity may need to inform the individuals whose data was accessed or stolen. In the United States, there are 50 different state notification laws which govern timing, content and form of required notifications to the competent authorities and to the individuals affected by the breach. In Europe,

---

[13] For the costs of a data breach in the U.S., *see* SwissRe, *Cyber Liability. Features of a data breach*, March 22, 2016, at 2 *et seq*. Available at http://www.swissre.com/library/Cyber_liability_Features_of_a_data_breach.html (last visited June 6, 2018). In Europe, the experience with breach response cost is not yet as broad while at the same time the law and the vendors' market is still developing.

[14] *See* for smaller breaches, Ponemon Institute/IBM, *2016 Cost of Data Breach Study*, at 19, available at https://securityintelligence.com/media/2016-cost-data-breach-study/ (last visited June 8, 2018). For large scale breaches *see* Deloitte, *Beneath the surface of a cyberattack*, p. 8 *et seq*. (2016), available at https://www.2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf (last visited June 8, 2018).

notification to authorities and to the data subjects only became mandatory in May 2018 when the new GDPR came in force.

Credit monitoring: the offering of free credit monitoring for at least one year has become standard when sensitive data of U.S. residents has been breached. To ensure no illicit activity using the sensitive data is taking place, the chosen credit monitoring agency will inform the individual if suspicious activity is detected or, generally, when new credit card or bank accounts are opened in her or his name. Credit monitoring is an important safeguard in the U.S. Credit reporting agencies track a person's credit history and are normally involved in any new credit application. Accordingly, they are ideally placed to detect suspicious activities in connection with an individual's credit card or bank account (given the wealth of sensitive data these agencies collect and process, it was no surprise that one of them, Equifax, became the victim of a data breach itself in September 2017).[15]

In Europe, credit monitoring activities are restricted by law in most jurisdictions,[16] and therefore, a person's "credit history" cannot be tracked and used in connection with other commercial transactions. As a result, there are no institutions comparable to the U.S. credit reporting agencies where different transactions in a person's name can be systematically scrutinized for suspicious activities. Therefore, U.S.-style credit monitoring cannot be offered in Continental Europe and, as a result, does not create such breach response costs. Some vendors in Europe, however, have started to offer so-called "web monitoring," which includes scanning the Internet and the dark net for sensitive personal data of affected individuals. If such data is found, the individual receives an alert that will allow him or her to take action such as informing his or her bank, or other companies, to prevent fraud. The UK is the European exception; credit monitoring is common and

[15] *Equifax finds more victims of 2017 breach*, BBC NEWS, March 1, 2018, available at http://www.bbc.com/news/ technology-43241939 (last visited June 8, 2018).

[16] In France, for example, creating black lists is forbidden by law. Only the Banque de France is allowed to get information about people's *incidents de paiement* (debts). The Banque de France is then allowed to share this information with credit companies /banks (*arrêté du 26 oct. 2010 relatif au fichier national des incidents de remboursement des crédits aux particuliers*).

routinely offered in connection with data breaches in the UK.

1. Revamping regulations in Europe

The consequences of a data breach are materially influenced by the legal landscape in which the breached entity operates.

While there are several federal data security and breach notification bills pending in the U.S. Congress,[17] at the time of writing, a variety of federal and state laws still regulate the topic in the U.S.[18]

Europe, on the other hand, is going through major changes in data privacy law with the GDPR,[19] which came into force on May 25, 2018. The GDPR applies directly and replaces all existing national data protection laws in the EU Member States.[20] Another piece of relevant recent EU legislation is the Network and Information Security Directive (NISD) adopted on July 6, 2016. The NISD is a "Directive" and, therefore, required implementation by the EU Member States into their national laws by May 2018.

These two laws are complementary initiatives with the common goal to modernize and harmonize the data protection and network security frameworks across the EU. The purpose of the NISD is to enhance online security in the EU and goes beyond mere data protection. It applies to operators of essential services [21] and digital service providers.[22] The GDPR focuses on protecting personal data wherever and however it is stored. It applies to anybody who is storing or processing data of European data subjects, including data processors located outside of the EU. The GDPR is expected to have the most direct impact on future data breaches. In

---

[17] *See* Alissa M. Dolan, *Data Security and Breach Notification Legislation: Selected Legal Issues,* Congressional Research Service (December 28, 2015), available at https://fas.org/sgp/crs/ misc/R44326.pdf (last visited June 8, 2018).

[18] For the different state laws that apply to notification, *see* National Conference of State Legislatures, "Telecommunications and Information Technology," available at http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx (last visited June 8, 2018).

[19] *See supra* note 2.

[20] For a list of the current EU Member States, *see* http://en.strasbourg-europe.eu/member-states,3322,en.html (last visited June 8, 2018).

[21] The NISD defines the operators of essential services as the entities which provide a service which is essential for the maintenance of critical societal and/or economic activities. EU Member States are required to identify operators of essential services; these will include the energy, transport, financial services, health, and digital infrastructure related industries.

[22] Digital Service Providers are providers of online marketplaces, online search engines or cloud computing services.

this article, we focus on the impact of this new legislation, which is primarily expected in the fields of notification requirements, regulatory fines and compensation for damages.

2. Notification

In Europe, except for certain industries (for example, telecom), prior to GDPR there was no mandatory obligation to notify a data breach. This could explain why there were many fewer reported data breach cases in Europe compared with the United States. But fewer reported cases does not necessarily mean that data breaches do not regularly occur in Europe as well. Some have made the headlines and have increased awareness of this topic in Europe.[23]

Under the GDPR, notification of a breach to the supervisory authority became mandatory in all cases where the breach poses a risk to the rights and freedoms of natural persons. [24] Notification to the affected data subjects, however, is only mandatory where there is a *high* risk to the rights and freedoms of natural persons.[25] Unfortunately, the GDPR does not contain a definition of "risk" and "high risk". Time will tell what direction the European regulators and ultimately courts will take with regard to this distinction.

Please see the table below for a summary of the requirements of a notification under the GDPR:

[23] For examples of EU data breaches, *see* Presentation of Elena Jelmini Cellerini and Catherine Lyle, *Cyber Claims: Expert forum on Cyber Risks*, January 29, 2016, available at http://media.swissre.com/documents/Presentation_Catherine_Lyle+and_Elena_Jelmini_Cellerini1.pdf (last visited June 8, 2018).

[24] GDPR, Art. 33.

[25] *Id.* at Art. 34.

	Notice to Supervisory Authority	Notice to Data Subject
Risk to the rights and freedoms of natural persons	mandatory	not mandatory
High Risk to the rights and freedoms of natural persons	mandatory	mandatory
Timing	no later than 72 hours	without undue delay
Content	nature of personal data breach; categories and number of affected subjects and records contact details of data protection officer likely consequence of the breach a) measures taken or proposed	a) nature of personal data breach b) contact details of data protection officer c) likely consequence of the breach d) measures taken or proposed
Form	not defined	not defined
Exceptions from notice requirement	breach is unlikely to result in a risk to the rights and freedoms of natural persons	i. the personal data is unintelligible, such as encrypted, or ii. if the entity has taken action subsequent to the breach to ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialize, or iii. when the notification to each data subject would "involve disproportionate effort", in which case alternative communication measures may be used

3. Regulatory fines

The GDPR authorizes regulators to levy hefty fines in amounts as high as four percent of the breached entity's annual turnover, or EUR 20m, whichever is greater. However, only a few articles of the GDPR deal with data security and breach notification, and only these provisions of the law are relevant in connection with a data breach.[26] There is ambiguity in the GDPR as to whether a data breach could attract the full 4%/EUR 20m fines or only the lower 2%/EUR 10m fines pursuant to article 83 paragraph 4 of the GDPR.[27] It appears that fines for an inadequate reaction to a data breach are limited to 2% of the annual turnover or EUR 10m (whichever is greater), while the fine for systematic inadequacies in data security could go as high as 4%/EUR 20m. It remains to be seen how the competent authorities and courts will interpret the GDPR in this regard. One way or another, fines of this magnitude must put data security issues on the agenda of every diligent management and board of directors.

Factors taken into account for the assessment of the fines include the following:[28]

- the nature, gravity and duration of the infringement, the number of data subjects affected and the level of damage suffered by them;
- the categories of personal data affected by the infringement;
- mitigation measures taken by the breached entity;
- previous infringements by the breached entity; and
- adherence to approved codes of conduct or certification mechanisms by the breached entity.

Already under the current law, regulators are looking at aggravating or alleviating factors in a similar way.[29]

---

[26] *Id.* at Articles 5, 24, 25, 28 and 32–34, which address data security and breach notification.

[27] Infringement of the provisions specifically dealing with risk assessment, data security and notification (GDPR, Articles 25 to 39) attract a fine of up to 2% of the annual turnover of the non-compliant company or EUR 10m, whichever is greater. Infringement of GDPR Article 5, which is dealing with "the principles relating to processing of personal data", including ensuring "integrity and confidentiality" of such data, can be fined up to 4% / EUR 20m.

[28] For the full catalogue of criteria and factors, *see* GDPR Art. 83.

[29] The UK regulator fined the telecom company Talk Talk, with a GBP 400 000 fine (the maximum being GBP 500 000) for a data breach. The regulator in this case considered the following aggravating factors: the number of individuals affected;

4. Contractual fines and penalties

Where credit card information is stolen in a data breach, affected credit card companies can impose substantial fines. Merchants or service providers who accept credit cards, and from whom such data may be stolen, have contractually agreed to pay fines and penalties for the loss of credit card information which they hold. The standard contracts between credit card companies, banks and merchants define a complex mechanism for the calculation of such contractual fines and penalties. Penalties are issued for the violation of the applicable PCI standards.[30] The basis for the fines, the so-called assessments, include the operational expenses incurred by the issuing banks for the replacement of the affected credit cards and the amount of fraudulent transactions that can be traced back to the data breach. The individual customer is usually not charged for fraudulent transactions or the replacement of the credit card.[31] Basically, the credit card companies operate by a similar set of rules in Europe and the United States.[32]

5. Developing case law

In 2016, the UK landmark decision of *Vidal-Hall v. Google* became final and binding when Google withdrew its appeal against it.

The case was about Google's unlawful practice of storing and analyzing individuals' internet surfing history. The decision was particularly important for its finding that (i) a claim involving personal data can be brought without having suffered economic damages; and that (ii) emotional distress alone is sufficient to give plaintiffs the right to make a claim in a court of law. This decision is in line with Article 82 of the GDPR which explicitly states that "any person who has suffered material or non-material damage … shall have the right to receive

---

the sensitive nature of data (incl. bank account numbers and sort codes); previous attacks; that Talk Talk could reasonably have anticipated such an attack. Experts reported that under the GDPR, Talk Talk could have incurred fines of up to GBP 73m.

[30] The Payment Card Industry Data Security Standards (PCI) contain a list of twelve information security requirements promulgated by the Payment Card Industry Security Standards Council, a self-regulating body founded by the five global payment brands – American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. The PCI are the benchmark for all organizations and environments where cardholder data is stored, processed, or transmitted and require merchants to implement a number of measures to protect cardholder data.

[31] For a more detailed explanation of this mechanism, *see* SwissRe, *Cyber Liability, supra* note 13, at 4 *et seq*.

[32] For the fines after large data breaches in the U.S. *see id.*

compensation ... for the damage suffered."

The next important case was the June 2016 UK decision *TLT et al. v. Secretary of State for the Home Department*, [33] which, for the first time, put a price tag on such claims for non-economic damages. The case involved the accidental disclosure of 1,600 asylum seekers' personal information. The judge applied *Vidal-Hall v. Google*, finding that compensation for distress arising from the breach was available. The claimants were awarded between GBP 2,500 - GBP 12,500 in compensation per person.

These two decisions show that the UK is following the path taken by the U.S. courts in broadening access to the courts for individuals who have been the victim of a data breach. With Article 82 of the GDPR not yet in force at the time of the decision, the *Vidal-Hall* case applied the overarching EU Charter of Fundamental Rights [34] to come to the same result.

6. Scope of class actions generally broadened in Europe

While U.S.-style class actions are not known in Europe, different forms of collective redress are on the rise.[35]

The Commission of the European Union issued a Recommendation in 2013, [36] suggesting that the Member States should introduce forms of collective redress for consumers. But when doing so, the Member States should avoid the introduction of U.S.-style class actions by, among other things, permitting only qualifying not-for-profit consumer associations to represent a class. [37] The GDPR follows this same approach and suggests that such forms of collective redress should be

[33] [2016] EWHC 2217 (QB), available at https://inforrm.files.wordpress.com/2016/10/tlt-v-sshd.pdf.

[34] The Court considered the EU Charter of Fundamental Rights (the "Charter"), in particular Article 7 (the right to respect of one's private and family life) and Article 8 (the right to protection of one's personal data) and decided that section 13(2) of the UK Data Protection Act should be disapplied on the grounds that it conflicts with the rights guaranteed by Articles 7 and 8 of the Charter. The consequence of this is that compensation is available for any damage, including anxiety and distress suffered by an individual whose data has been breached. Whether Brexit might have an impact on this UK case law remains unclear to date.

[35] In 2016, France and Germany both introduced laws recognizing the right of consumer associations to bring actions in case of violation of data protection laws. *See* the German *Unterlassungsklagengesetz* (UKlaG). In France, the draft of the "*loi de Justice du XXIème siècle*" was adopted on October 12, 2016 but was constitutionally challenged a few days later and thus is not (yet) in force.

[36] Commission Recommendation 2013/396/EU, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013H0396&from=EN (last visited June 8, 2018).

[37] *See id.* at Para. III.4 (a).

available for data subjects under the GDPR.[38] The Member States, however, are free to decide whether collective redress procedures shall be available for claims for damages, or only in connection with non-monetary judicial remedies.[39]

Because a data breach usually affects many individuals in a similar way, they will regularly look towards such collective redress procedures to seek remedy for their injury. If combinable with non-economic damages like emotional distress, such collective redress actions could change the legal landscape in the respective jurisdiction and materially increase the exposure of breached companies. However, not all EU Member States allow for damages to be claimed in collective redress actions. The respective national introductory laws to the GDPR are expected to deal with this question.

7. First collective redress action filed in the UK

The first European collective redress action following a data breach has been filed in the UK. The action, however, is based on the UK Group Litigation Orders procedure, which was introduced in 1999. This procedure allows the grouping of cases which give rise to common or related issues of fact or law. The first such action in connection with a data breach in the UK launched in 2015 with the *Morrisons Supermarket* case.[40] Some 6,000 employees opted in and all claimed damages for emotional distress based on the *Vidal-Hall* decision.

On December 1, 2017, the Court rendered a long decision where Morrisons Supermarket lost, not on the grounds that they had found to have primary liability for breach of the UK Data Protection Act because they didn't take reasonable steps to keep the data safe, but because they were vicariously liable as employer for a leak by their employee. Though the Court didn't say anything in terms of quantum, this decision constitutes a landmark decision pre-GDPR.

The UK group action scheme does not require that collective actions be brought by not-for-profit consumer associations only. The advent of claims by other collectives will likely create different dynamics in connection with such claims.

---

[38] *See* Hogan Lovells, *The Era of Mass Data Litigation*, May 2018, https://www.hoganlovells.com/en/publications/data-class-actions-the-era-of-mass-data-litigation (last visited June 8, 2018).

[39] *See* Art. 80 and Whereas-clause 142 of the GDPR.

[40] The matter involved an internal auditor who intentionally leaked personal records of 100,000 employees including salaries, bank account details, etc. and posted the information online.

8. Comparison: Europe vs United States

While some aspects of a data breach will be materially different in Europe compared to the U.S., the table below clearly indicates that the two major legal systems, U.S. common law and the civil law (which dominates the European Union) are moving closer to each other with the implementation of the GDPR.

Data Breach response – Cross border differences

	USA	EU pre GDPR	EU with GDPR (as of 25 May 2018)
Notification	50 State breach notifications laws + proposal for a federal law in Congress	Only limited obligations based on national laws	Notification mandatory, with important exceptions
Forensics	No legal obligation, but expected loss mitigation measure of a prudent management	No legal obligation, but expected loss mitigation measure of a prudent management	No legal obligation, but expected loss mitigation measure of a prudent management
Public Relations	No legal obligation, but expected loss mitigation measure of a prudent management	No legal obligation, but expected loss mitigation measure of a prudent management	No legal obligation, but expected loss mitigation measure of a prudent management
Credit Monitoring	Required by some State laws – Common practice:1 or 2 year of free credit monitoring	US style credit monitoring prohibited in Continental Europe, but allowed in UK	US style credit monitoring prohibited in Continental Europe, but allowed in UK
Regulatory Fines	50 State breach notifications laws + several federal laws	Only based on national laws	Up to 2% of annual turn over *OR* 10M €, whichever is greater (possibly up to 4%/20M € if breach of general principle of GDPR)
Contractual Penalties and Fines	Assessed by credit card companies and ultimately imposed on breached entity	Assessed by credit card companies and ultimately imposed on breached entity	Assessed by credit card companies and ultimately imposed on breached entity
Third party liability: Civil Actions, incl. Class Actions	Individual and class actions. Standing granted to affected individual without proof of material damage. Also, standing granted for *future* risk of identity theft or fraud (Zappos decision, March 2018)	Individual actions, but no US style class actions in EU. Restricted consumer class actions in some states. UK: Vidal-Hall decision finds standing to sue for emotional distress. TIt (2016) decision put price tags to emotional distress. Morrissons decision is the first data breach related class action.	Individual actions, but no US style class actions in EU. Claims for material and non-material damages admissible. Restricted consumer class actions in some states.

Swiss Re

Grey: similar
Pink: some similarities, but different

II. Coverage under a cyber stand-alone policy?

Awareness of cyber risks in Europe remains much lower than in the United States. According to a survey conducted by Swiss Re in cooperation with IBM in 2016, 39% of corporations surveyed in North America plan to buy (more) cyber insurance, while only 27% of European corporations have such plans.[41] With only 12% of information assets globally being protected by insurance in 2015,[42] there still remains much to do to make our "information society" more resilient. A survey of security professionals in 2016 indicated that only around a quarter of firms use detailed quantitative cyber risk models back then,[43] while apparently 60% of companies in Continental Europe have never estimated the financial impact of a cyber loss scenario.[44]

Risk transfer should be one element in a comprehensive cyber strategy. Cyber policies cover both first-party losses and third-party liability. The covered first party losses encompass crisis management costs (forensic investigation, public relations, notification, credit monitoring) and regulatory fines, to the extent they are insurable under applicable local laws.

Covered under the third-party liability section are claims which a breached entity will face, including respective defense costs. Depending on the jurisdiction, the element of defense costs should not be underestimated.

Indemnification for contractual penalties and fines is not necessarily part of the standard coverage. However, coverage for these so-called credit card company assessments can be purchased by endorsement but is often subject to a sub-limit.

Regulatory fines under GDPR are considered not insurable in most EU jurisdictions.[45]

Cyber stand-alone policies often also cover business

---

41 SwissRe/IBM, *Cyber: in search of resilience in an interconnected world,* at 12, available at http://www.swissre.com/library/archive/Demand_for_cyber_insurance_on_the_rise_joint_Swiss_Re_IBM_study_shows.html (last visited June 6, 2018).

42 AON/Ponemon, *supra* note 5, at 6.

43 SANS Institute, *Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey*, June 2016. Available at http://www.advisenltd.com/wp-content/uploads/2016/06/bridging-insurance-infosec-gap-2016-cyber-insurance-survey-2016-06-21.pdf (last visited June 8, 2018).

44 Marsh, *UK Cyber Risk Survey Report: 2016*, September 2016, available at https://www.marsh.com/uk/insights/research/uk-cyber-risk-survey-report-2016.html, and Marsh, *Continental European Cyber Risk Survey: 2016 Report*, October 2016, available at http://www.hkbb.ch/uploads/6869 (last visited June 8, 2018).

45 https://www.dlapiper.com/en/us/insights/publications/2018/05/the-price-of-data-security/ (last visited June 8, 2018).

interruption that is directly linked to the data breach. However, loss of revenues after a breach (churning, reputational damage) mostly remains uncovered. Shareholders' derivative actions against directors and officers (D&O) for negligence and breach of fiduciary duties can result. Even when dismissed, [46] covered defense costs alone can be substantial and, accordingly, D&O policies have regularly come into focus.

Knowing that IT security is the Achilles heel of companies that process and store personal data, boards are well advised to make cyber security a priority topic on their agenda and review their cyber and D&O coverage on a regular basis.

III. Summary

The web is worldwide. Therefore, data breaches are a global threat. The response by various jurisdictions, however, has been quite different up until now. With the regulatory changes in the European Union, Europe's and the United States' way of dealing with data breaches is becoming more aligned. After implementation of the GDPR, the major differences that remain predominantly arise out of the inherent differences between the civil law and the common law systems.

The possibility to bring class actions creates a dynamic risk landscape in the U.S. In Europe, we see a cautious opening towards such forms of collective redress, combined with a clear goal to avoid the implementation of a U.S.-style class action system. [47] Moreover, the GDPR grants an unequivocal right for victims to be compensated for material and non-material damages arising out of a violation of the GDPR. Obviously, in those jurisdictions where the combination of claims for non-material damages with forms of collective redress are or will be possible, the risk for breached entities to be held liable for substantial amounts in damages increases significantly.

Another key difference that will remain is that a person's credit history is still an important feature of the U.S. economy. The use of

---

[46] *See* dismissal of the D&O claim in the Home Depot matter in the U.S., *in re* Home Depot Shareholder Litigation, No:15-CV-2999 (M.D. Ga. Nov. 30, 2016), available at http://www.dandodiary.com/wp-content/uploads/sites/265/2016/12/home-depot-decision.pdf (last visited June 8, 2018).

[47] European Commission, Memo 08/741, *Green Paper on Consumer Collective Redress – Q&A*, Question 9, available at http://europa.eu/rapid/press-release_MEMO-08-741_en.htm (last visited June 6, 2018). SwissRe, *Making Collective Redress Work Across Europe*, May 21, 2015, available at http://www.swissre.com/library/expertise-publication/Making collective_redress_work_across_Europe.html (last visited June 8, 2018).

credit history data is not common or even prohibited by law in most of Continental Europe. The cost factor created by credit monitoring in the U.S. is substantial, while such losses are very limited in the European context. Only the UK allows credit monitoring activities similar to the U.S.

The fines under the European GDPR are expected to be much more aggressive than those currently imposed in U.S. The U.S. legal system traditionally places more importance on the preventive and deterrent effect of private law suits, including class actions. Time will tell whether European regulators will become major players/controllers in the cyber arena, or whether civil actions brought by affected consumers will have the greater impact.