Cyber Liability Risk on the Rise Due to Court Decisions

Implications for Companies in Structuring an Insurance Program

▶ By Steven H. Anderson, Daniel Simnowitz and Ariel Fliman

When evaluating cyber risk and the potential impact of a data breach, companies consider reputational damage, lost business, and the cost of post-incident mitigation and recovery efforts. Class action lawsuits filed by plaintiffs whose data has been stolen or otherwise comprised have also presented a potential exposure for these organizations.

Historically, plaintiffs have experienced only mixed success in class action lawsuits filed in the wake of a data breach because they were unable to consistently demonstrate an injury-in-fact, which is necessary to establish standing under Article III of the US Constitution. However, decisions in 2016 and 2015 by the Sixth Circuit and Seventh Circuit Courts of Appeals may be a harbinger of change, finding that the imminent risk of harm presented by a data breach is sufficient to establish an injury-in-fact. In the most recent of these cases, the Sixth Circuit Court of Appeals concluded that the plaintiffs suffered an injury even though they could not demonstrate that their stolen data had actually been used. The Sixth Circuit even pointed to the defendant's efforts to prevent the actual misuse of the data stolen by hackers as part of the rationale for its conclusion that the plaintiffs had demonstrated an injury-in-fact.

These decisions may provide a roadmap for data breach class action complainants to satisfy the standing requirement, raising the prospect of future success and potentially increasing the frequency of such class actions. Risk managers may also need to consider whether and how post-breach mitigation efforts, in some cases required by state law, may impact class action exposure. This expanding threat underscores the importance of insurance to protect against the risk. To better understand and address the threat of data breach litigation, a more detailed examination of the court decisions and insurance options is warranted.

The Lawsuits

Insurance Company Data Breach[1] (2016)

The situation: Hackers stole the personal information of 1.1 million customers of an insurance company, including names, dates of birth, marital status, employment status, Social Security numbers, and driver's license numbers. The company advised its affected customers to take steps to mitigate or to prevent misuse of their stolen data, such as monitoring bank statements and credit reports for unusual activity. The company also offered to engage a third-party vendor for up to one year for credit monitoring and fraud protection (up to $1 million in services).

The lawsuit: Plaintiffs alleged violations of the Fair Credit Reporting Act for failure to adopt required procedures to protect the sensitive data, negligence, and invasion of privacy by public disclosure of private facts based on the insurance company's failure to secure the data. Plaintiffs argued that they had incurred "financial and temporal" costs in connection with hiring credit monitoring and reporting services, ordering financial information from banks, and placing/removing credit freezes, among other categories of mitigation efforts. Significantly, the plaintiffs had not alleged that their stolen personal information had been misused.

The decision: The district court granted the insurance company's motion to dismiss on several grounds, including lack of Article III standing. The Sixth Circuit, however, overturned the district court's decision because the plaintiffs' "allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage." In reaching this conclusion, the Sixth Circuit determined that the plaintiffs' standing to sue the insurance company could be based solely on imminent future harms, which is significant given that the plaintiffs had not actually alleged that their data had been misused.

The court deemed sufficient the plaintiffs' allegation that "the theft of their personal data places them at a continuing, increased risk of fraud and identity theft beyond the speculative allegations of 'possible future injury' or 'objectively reasonably likelihood' of injury that the Supreme Court has explained are insufficient."

Significantly, the court cited to the insurance company's post-breach mitigation efforts, including its offer to provide credit monitoring and identity theft protection – the cost of which may be reimbursed as a first party expense under cyber insurance programs – to support its conclusion that the plaintiffs' injuries were imminent.

The Sixth Circuit's decision in this case also discussed earlier data breach-related precedents that analyzed whether plaintiffs had sustained an injury-in-fact sufficient to trigger Article III standing.

Retailer Chain Data Breach[2] (2016)

The situation: Hackers stole the credit card information of approximately 350,000 of the retailer's customers, and 9,200 of those customers found fraudulent charges on their cards. The retailer offered credit monitoring and identity theft protection to all customers who shopped at its stores for the one-year period leading up to the discovery of the breach.

The lawsuit: A group of customers whose information was stolen filed a putative class action on behalf of all 350,000 consumers. To establish standing, the plaintiffs claimed several types of injury: an increased risk of fraudulent charges and identity theft in the future; money and time spent to guard against that risk; overpayment for defective cybersecurity; and loss of control over personal information. The retailer moved to dismiss the lawsuit on standing grounds.

The decision: The district court granted the defendant's motion to dismiss, but the Court of Appeals for the Seventh Circuit found that the increased risk of fraudulent charges and identity theft were sufficiently "imminent" to establish standing. The Seventh Circuit reasoned:

- The personal data of the 350,000 customers had already been stolen, and the presumed purpose of a hack is "sooner or later, to make fraudulent charges or assume those consumers' identities." The plaintiffs "should not have to wait until hackers commit identity theft or credit card fraud" before spending time and money to protect themselves.
- Unlike the insurance company case, 9,200 customers had already experienced harm due to fraudulent charges. The Seventh Circuit noted that "[t]hose victims have suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized charges."
- Similar to the Sixth Circuit, the Seventh Circuit cited the significance of offering credit monitoring and identity theft protection to the defendant's customers, noting that the defendant would not have "offered one year of credit monitoring and identity theft protection" to potentially compromised customers if the risk was "so ephemeral that it can be safely disregarded."

Restaurant Chain Data Breach[3] (2015)

The situation: In response to a data breach affecting an unknown number of its locations, a restaurant chain responded with letters to its customers advising them of the breach and encouraging them to watch for fraudulent charges and to monitor their credit reports. Some customers found fraudulent charges on their credit cards and others, after hearing of the breach, spent time monitoring credit card statements and credit reports.

The lawsuit: The plaintiffs alleged a number of injuries, including ones similar to the injuries alleged in the aforementioned retailer case – namely, an increased risk of future fraudulent charges and identity theft and money and time spent to guard against that risk.

The decision: After the district court dismissed the action for lack of standing, the Seventh Circuit reversed, holding that the plaintiffs described many of the same injuries as the retailer case plaintiffs did due to stolen data, and such injuries "are concrete enough to support a lawsuit." Other key aspects of the court's decision included:

- It is "plausible to infer a substantial risk of harm from the data breach" because "a primary incentive for hackers is sooner or later to make fraudulent charges or assume … consumers' identities."
- With respect to plaintiffs who had already incurred fraudulent charges – even if such charges were stopped before the plaintiffs made any payments on them – they have spent sufficient time and effort to resolve the effects of the data breaches. This includes time and effort to monitor credit card statements and financial information as a guard against fraudulent charges and identity theft.

Implications for Risk Managers

The implications of the recent rulings are two-fold for risk managers.

First, the frequency of data breach litigation and the severity of the litigation exposure may rise because the courts have provided some guidance to plaintiffs' counsel to establish standing in data breach litigation. With added confidence that their actions can survive a motion to dismiss for lack of standing, plaintiffs' counsel may have an increased incentive to bring data breach class actions.

Second, risk managers now face the reality that routine – and in some cases state-mandated – mitigation efforts, such as notice to all affected customers, may adversely impact the defense of subsequent data breach class actions.

These developments render the need for risk managers to have a comprehensive cyber risk management plan even more urgent. The question is whether they will spur companies to action. In PwC's 2016 Global Economic Crime Survey, only about one in three organizations had a fully operational response plan for cyber incidents, and a similar proportion had no plan at all.[4]

Structuring an Insurance Program to Address the Increased Risk

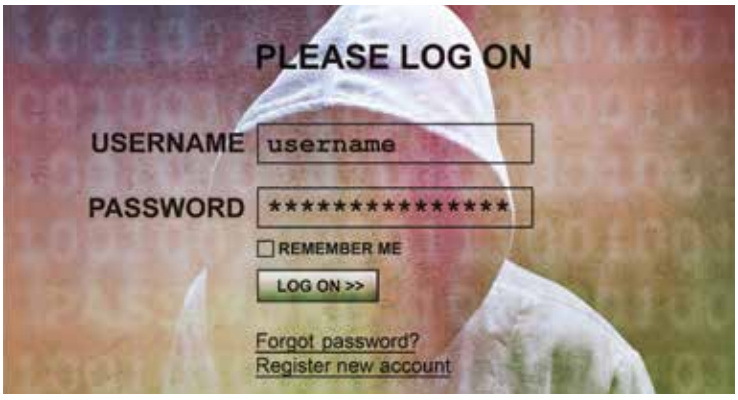
A robust plan for guarding against and mitigating cyber incidents requires a coordinated effort across many areas of a company, such as IT, employee training, legal, communications, and vendor management. Given the ever-changing and increasingly complex nature of cyber threats, however, one constant holds – no plan will be perfect.

For this reason, cyber insurance serves as a critical component of any cyber risk management plan. Risk managers must closely monitor the range of programs available because, just as the cyber threat is rapidly evolving, so too are the products and services in the insurance plans. The quality of the available policies and the experience and capability of the carriers involved vary widely.

The best programs offer a combination of comprehensive coverage and prevention and response services that can be tailored to a company's unique needs.

The best programs offer a combination of comprehensive coverage and prevention and response services that can be tailored to a company's unique needs. From a coverage standpoint, risk managers and their brokers should consider looking for policies that include some or all of the following coverages:

- **Privacy and network security liability** that covers third-party claims arising from a failure of the company's network security or a failure to protect data. This is the critical component of coverage that guards against the increased risk of litigation, including class action litigation. The coverage typically also responds to regulatory actions in connection with a security failure, privacy breach, or failure to disclose.
- **Event management coverage** that responds to a security failure or privacy breach by paying costs of consumer notifications, public relations and other services to assist in mitigating a cyber incident. Coverage for costs incurred by the company in connection with forensic investigations, legal consultations and identity monitoring costs for victims of a breach may also be included.



- **Business interruption coverage** that addresses a material disruption of the company's business operations caused by a network security failure by reimbursing for operating expenses and lost income. In some cases, contingent business interruption coverage should also be available in case a key supplier suffers a cyber incident that impairs the company's ability to deliver its product or service.
- **Cyber extortion coverage** that applies to the threat of calculated security attacks against an organization by an intruder attempting to coerce money, securities, or other valuables. This coverage should also address monies paid to end the security threat and the cost of investigations to determine the cause.
- **Cyber media coverage** for the liability faced by companies that distribute media content via their website. The coverage should provide protection against numerous perils including copyright infringement, trademark infringement, defamation and invasion of privacy.

Equally important to the quality of the coverage is the underwriting expertise of the insurance company providing it, because the underwriting process itself may help the risk manager identify and address weak spots in the insured company's cyber defense and response plan. The more experienced insurance companies will be better able to evaluate the security of a company's information network, the training of employees, governance procedures, vendor access, and incident response plans.

In some cases, the companies will also offer services as part of the cyber insurance program to help the company further improve its risk profile. Frequently, the services are offered through third party vendors that are best equipped to keep abreast of the latest practices and offer specialized platforms to help risk managers strengthen their cyber defenses and respond effectively to data breaches, network attacks and other security issues.

Tools and services may include the following:

- Cyber-risk assessment surveys
- What-if modeling to estimate the cost of a breach
- Breach notification guides and suggested steps to take following a network or data breach incident
- Research tools to monitor the type, frequency and severity of incidents occurring in the insured company's business sector
- Access to a library of best-practices articles, white papers and webinars from leading technical and legal practitioners

Conclusion

The increased threat of class action litigation due to a data breach heightens the importance of having a fully developed preparedness and response plan and a strong cyber insurance program. Risk managers must consider that the nature of their response to an incident can be used by plaintiffs to establish standing. They must also be aware of the variations in the insurance products and services available due to the rapidly evolving nature of cyber risk, as well as the underwriting and claims experience of the companies offering them.

Authors

Steven H. Anderson, RPLU+
VP, Product Executive – Privacy & Network Security
QBE North America
972.398.8477
steven.anderson@us.qbe.com

Daniel Simnowitz
VP, Product Development
QBE North America
646.341.8049
daniel.simnowitz@us.qbe.com

Ariel Fliman
AVP, Product Development
QBE North America
212.497.9632
ariel.fliman@us.qbe.com

Media Contact

Carla Ferrara
VP, Corporate Communications & Branding
QBE North America
212.497.9604
carla.ferrara@us.qbe.com

Business Contact

Steven H. Anderson, RPLU+
VP, Product Executive – Privacy & Network Security
QBE North America
972.398.8477
steven.anderson@us.qbe.com

About QBE

QBE North America is part of QBE Insurance Group Limited, one of the largest insurers and reinsurers worldwide. QBE NA reported Gross Written Premiums in 2016 of $4.6 billion. QBE Insurance Group's 2016 results can be found at www.qbena.com. Headquartered in Sydney, Australia, QBE operates out of 37 countries around the globe, with a presence in every key insurance market. The North America division, headquartered in New York, conducts business through its property and casualty insurance subsidiaries. QBE insurance companies are rated "A" (Excellent) by A.M. Best and "A+" by Standard & Poor's.* Additional information can be found at www.qbena.com, or follow QBE North America on Twitter.

[1] *Galaria v. Nationwide Mutual Insurance Co., 2016 WL 4728027 (6th Cir. Sep. 12, 2016)*
[2] *Remijas v. Neiman Marcus Group LLC, 794 F.3d 688 (7th Cir. 2015)*
[3] *Lewert v. PF Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016)*
[4] *PwC, Global Economic Crime Survey 2016. Retrieved from https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf*