INSIDE THIS EDITION.....

CYBER CLAIMS LANDSCAPE
A SAMPLING OF LARGE CYBER SETTLEMENTS
LEGAL SPOTLIGHT, PRIVILEGE & EXPERTISE
CLAIMS REPORTING BEST PRACTICES
A VIEW INTO CYBER CLAIMS

As Director of the Willis Claim & Legal Group (CLG), I am excited to welcome you to the inaugural edition of The Willis Cyber Brief. This semi-annual publication comes to you from the CLG team, a group of dedicated and knowledgeable claim professionals. The team, all attorneys, will draw from their extensive experience to provide valuable insights to help clients navigate the rapidly changing world of cyber claims. While most cyber coverage disputes have centered on availability of coverage under commercial general liability policies, we expect to see an increase in the number of claims brought under cyber insurance policies. Therefore, as we have done in this edition with John Mullen of Lewis Brisbois, an attorney and leading expert on cyber matters, we will partner with leading experts in the cyber field, including legal, regulatory, and insurance to bring you the latest cyber liability developments, as well as cutting edge views on claim issues that matter most to you... our clients.

Enjoy the first of many publications!

Ken Ross
Director
Finex North America, Claims & Legal Group
+1 212 915 8083
ken.ross@willis.com

For additional information, please contact your Willis Client Advocate® or FINEX_NA@WILLIS.COM.
The cyber risk landscape is rapidly evolving. Governments are facing an unprecedented level of cyber attacks and threats with the potential to undermine national security and critical infrastructure. Similarly, businesses across a wide range of industry sectors are exposed to potentially enormous physical losses as well as liabilities and costs as a result of cyber attacks and data breaches.

Given the risk landscape, it is no wonder companies of all sizes continue to be subject to increasing data breach liability, both in the form of single plaintiff or class action lawsuits and regulatory investigations and proceedings. Negligence, breach of fiduciary duty and breach of contract are just some of the allegations that a company may face as a result of a systems failure or lax security that compromises the security of customers’ personal information or data.

Plaintiffs in data breach class actions typically allege that businesses failed to adequately safeguard consumer information and gave insufficient and untimely notice of the breach. Companies may also face class actions from banks and credit unions seeking damages for administrative expenses, lost interest, transaction fees and lost customers. Settlements of data breach class actions can be exorbitant. For example, 25 class action lawsuits were settled in the wake of the 2007 data breach of retailer involving the theft of data related to over 45 million credit and debit cards. The settlement included: up to $1 million to customers without receipts; up to $10 million to customers with receipts ($30 per claimant); $6.5 million in plaintiffs’ attorneys fees; and three free years of credit monitoring, with total costs reportedly up to $256 million. More recently, in 2014, two major retailers reported that the total costs of data breach and related class action lawsuits (less expected insurance recovery) was estimated at $63 million and $191 million, respectively. And, this year, two major healthcare companies are separately facing several lawsuits as a result of data breaches that reportedly exposed the personal records of 80 million and 11 million people, respectively. While these matters have yet to be resolved, the anticipated costs of litigation and settlement may set records.

**REMEDIES SOUGHT**

Most data breaches result in first-party loss to the victim of the cyber breach. For example, a business sustaining a cyber breach or failure to protect confidential consumer information may incur the following expenses to remedy the issue (i.e. first-party costs):

- Costs to restore its computer system, remove viruses, malicious code, Trojan horses

*continued on page 3*
- Costs related to loss of business (such as a denial-of-service computer attack on a company’s network that limits the ability to conduct business)
- Costs to conduct a forensic investigation as to the cause of the unauthorized access
- Legal consultation costs or “breach counsel” to consult the business regarding all statutory requirements
- Costs to notify affected consumers, and costs to offer credit monitoring services to customers
- Costs to retain public relations assistance or advertising to rebuild a company’s reputation after an incident
- To the extent that there was a cyber-attack on the business’ network in an attempt to extort money (“cyber extortion”), costs to settle such extortion demands, as well as costs of hiring a security firm to negotiate with blackmailers may also be at issue

Companies affected by a cyber breach may also face liability to third parties, which may result in defense costs, settlements, judgments and, sometimes punitive damages. Third parties bringing lawsuits against businesses for damages are increasingly seeking to expand the nature of injuries and remedies sought in light of early case law which determined that there was no injury in fact sustained by the cyber breach and thus no standing to sue. The Federal Trade Commission (FTC)’s Bureau of Consumer Protection has increased its investigations of data breaches on behalf of consumers given the rise in the number of organizations that rely on “Big Data” in their advertising and marketing campaigns. In 2014, the agency issued a press release announcing its 50th Data Security Settlement on behalf of consumers. One of those settlements involved the much publicized 2006 settlement with a data aggregation company wherein the company agreed to pay $10 million in civil penalties and $5 million in consumer redress for time customers may have spent to monitor and repair their credit following a breach that exposed their personal information.

In addition, the Federal Identity Theft Enforcement and Restitution Act provides that perpetrators of identity theft must reimburse their victims for the value of the time the victims spent repairing their credit records. The enactment of ITERA and the growing recognition in the business community that time spent repairing credit may constitute an injury in fact, may create an increased willingness of courts to find consumer standing to bring such actions and thus an increased liability risk to businesses. Increased regulation at federal and state levels related to information security and breach notification is expanding the legal avenues that may be pursued. Forty-seven states plus Puerto Rico, Washington D.C., and the Virgin Islands, have enacted laws requiring companies to notify consumers of breaches of personal data. Federal laws, such as the Health Insurance Portability and Accountability Act, the Gramm Leach Bliley Act and the Fair Credit Reporting Act, have requirements to safeguard the privacy of personal information, and some states require notification to the state attorney general. Given this ever-evolving and regulatory landscape, companies should expect an increase in third party liability claims led by federal regulatory agencies as evidenced by a March 2015 federal court decision involving a large hotel chain wherein the court held that the FTC has regulatory authority to enforce data security practices.
A SAMPLING OF LARGE CYBER SETTLEMENTS*

There have been hundreds of cyber-related claim settlements in the last few years. Many of these claims have been resolved confidentially, while others have managed to make the headlines. To assist clients in evaluating the potential exposures associated with cyber claims, Willis has been amassing a database of cyber-related losses. In this section, we provide you a sampling of some of this loss data. For additional information about the referenced claims or additional claim examples, please contact your Willis Client or Claim Advocate.

<table>
<thead>
<tr>
<th>SETTLEMENT AMOUNT</th>
<th>INDUSTRY</th>
<th>DATE</th>
<th>TYPE OF CLAIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>$60 Million</td>
<td>Financial Services</td>
<td>2008</td>
<td>Data breach, resulting in reissuance of cards to consumers</td>
</tr>
<tr>
<td>$40 Million</td>
<td>Retail</td>
<td>2007</td>
<td>Unauthorized intrusion into computer systems, exposing approximately 45 million customers’ credit and debit card numbers</td>
</tr>
<tr>
<td>$25 Million</td>
<td>Telecommunications</td>
<td>2015</td>
<td>Alleged failure to protect approximately 280,000 customers’ personal information at call centers</td>
</tr>
<tr>
<td>$20 Million</td>
<td>Government</td>
<td>2009</td>
<td>Theft of laptop at the home of VA analyst resulting in data breach of approximately 26.5 million veterans</td>
</tr>
<tr>
<td>$19 Million</td>
<td>Retail</td>
<td>2015</td>
<td>Settlement with financial institutions that issued Master-card-branded credit and debit cards affected by data breach of retailer’s customers’ personal information</td>
</tr>
<tr>
<td>$15 Million</td>
<td>Financial Services</td>
<td>2006</td>
<td>Compromise of personal financial records of more than 163,000 consumers following a data breach</td>
</tr>
<tr>
<td>$15 Million</td>
<td>Consumer Electronics</td>
<td>2011</td>
<td>Hackers breached company’s network and obtained data of approximately 31 million online game users</td>
</tr>
<tr>
<td>$10 Million</td>
<td>Retail</td>
<td>2015</td>
<td>Settlement of multi-district litigation involving 2013 data breach that resulted in compromise of approximately 110 million customers’ personal information</td>
</tr>
<tr>
<td>$10 Million</td>
<td>Telecommunications</td>
<td>2014</td>
<td>FCC fined company for failure to protect consumers’ proprietary information and alleged deficient data security practices</td>
</tr>
<tr>
<td>$6.5 Million</td>
<td>Financial Services</td>
<td>2008</td>
<td>Former financial analyst allegedly sold customers’ personal records to other lenders in the mortgage industry as leads for new loan pitches</td>
</tr>
</tbody>
</table>

*Some of these losses may have been insured.*
When – not if – an organization suffers a data security event, its gut reaction may be to rely on its general services outside counsel to handle investigating and responding to the event. However, just as a general medical doctor lacks skills and experience in knee replacement surgery, these (otherwise very talented) professionals likely have little or no experience in investigating and managing data privacy events, identifying and complying with applicable state and federal data privacy laws, and executing an efficient multi-pronged response. If done properly, the appropriate approach will mitigate brand and reputational damage and limit third-party or regulator claims that may result from an event.

It behooves an organization to engage an experienced breach coach immediately after discovering there may have been a data security incident. One of the benefits of having data privacy insurance in place is having access to these experts. The leading insurers know who to call.

A breach coach knows what needs to happen, and when, to appropriately respond to a data security incident. What law enforcement agencies should be notified of an event, and when? Should third-party forensic investigators be brought in, and if so, when and who? Should the media be informed and, if so, when and who? What other messaging, and to what constituents, may be needed? Are vendors needed to provide print notification, call center and credit/identity monitoring to affected individuals? Are there any business partners or other third parties that must be informed even as an investigation into the nature and scope is ongoing? Missing or mishandling these issues can result in lost or unavailable evidence, incorrect or inconsistent messaging, incomplete investigations, and defensive communications which may result in public scrutiny, lost business, regulator inquiry, litigation, assessments or fines, as well as brand and reputational harm.

A breach coach is a lawyer who directs a response effort to best ensure safety to the organization, position communications and prepare for regulatory and or litigation inquiries...protected by attorney-client and attorney work-product privileges. Yes, an organization can keep the effort with counsel they know from other engagements. Or it may directly engage a vendor to study its systems and staff and identify vulnerabilities. However, rarely is a sufficiently experienced and skilled forensic vendor engaged or the investigation appropriately directed to ensure that the event is terminated and that the information needed to sufficiently communicate regarding the incident is secured. Moreover, the vendor’s oral and written material and communications with the organization may not be privileged and may be discoverable.

A breach coach will identify issues, select appropriate and experienced vendors to provide necessary services, retain those vendors in the appropriate fashion and at the necessary speed, direct the investigation to ensure it is sharply focused and thorough, and determine what communications and material should and should not be prepared.

A breach coach has subject matter expertise in this constantly developing and evolving area of law. The value of using the proper counsel cannot be overstated. A good breach coach will not replace or cut out your general or local counsel’s involvement in the process. When choosing counsel to manage such an event, ask these easy questions: how many data privacy breaches did you handle in the last year; how many attorneys at your firm are solely dedicated to data privacy crisis management response work.....then compare their answers to their web site bios.

After being a victim itself, the last thing an organization needs is “help” from counsel who are learning on the job. The first and best step an organization can take when it believes it has suffered a data security incident is to call its broker and/or its carrier. They will identify a breach coach, to whom the organization has 24/7 access under the cyber insurance policies currently in the marketplace. The carriers did their homework. Take advantage of it.
Advise the insurer and your insurance broker as soon as a breach is detected or suspected because most policies require the insurer’s consent prior to incurring any costs for the retention of vendors and outside counsel.

After notifying the insurer, you should engage your breach response team in addressing obligations under your cyber insurance policy, including vendor selections. In some cases, an insurer will immediately assign “first responder” counsel to provide legal advice as to next steps.

- One of the first vendors to retain is a forensic investigator to conduct an investigation as to the nature of the breach. You may also want to simultaneously retain a breach coach to preserve privilege with respect to information discovered and reported by the forensic investigator.
- Once the breach has been confirmed, you should engage your breach coach. Counsel should have knowledge of the different notification laws and the insured’s obligations in the event of a breach.
- You may wish to also retain a consumer notification service vendor who will assist with the notification process and set up a call center for the individuals affected by the breach.
  - Part of the notification process is to advise the affected individuals that the insured will provide free credit monitoring for a set period of time through a credit monitoring or identity theft protection service.
  - Finally, you may want to consider retaining a PR firm to assist with the crisis management aspect of the breach.

Consider reporting the matter to other lines of coverage, if applicable, and tailor the notice accordingly.

- Cyber claims include not just the above noted first-party losses, but possibly also associated third-party lawsuits. These third-party lawsuits can be from individuals affected by the breach, shareholders of a company if the company experienced a stock drop as a result of the breach or government entities bringing regulatory actions.

The key to maximizing insurance recovery under your cyber liability insurance policy is early notification and keeping the lines of communication with the insurer open. In addition, keep the insurers advised of the developments of the forensic investigation and notification process. It is also crucial to review your insurance policy and consult closely with your insurance broker to ensure your understanding of the claim reporting process, the applicable retentions and/or sub-limits of coverage, and any vendor preferences of the insurer to maximize coverage.

Note that most insurers typically have a panel list of outside counsel and vendors they have worked with in the past and with whom they have preferred rates; the insured should consult this list and the insurer as soon as possible to get the right team in place.