State of the Cyber Insurance Market
Ten Lessons Learned From Major Retailer Breaches

August 2014 • Lockton® Companies

There has been extensive adverse publicity surrounding what has become the largest data breach in the retail industry, affecting Target and two other U.S. retailers. In November–December 2013, cyber thieves executed a well-planned intrusion into Target’s computer network and the point-of-sale terminals at its 1,800 stores around the holiday season and successfully obtained not only 40 million customers’ credit and debit card information, but also noncard customer personal data for as many as 70 million customers. In addition, 1.1 million payment cards from Neiman Marcus and 3 million cards used at Michaels were reportedly exposed.

The respected Ponemon Institute announced this June it believes that hackers have exposed the personal information of 110 million Americans—roughly half of the nation’s adults—in the last 12 months alone, and this number reflects the impact of major retailer breaches and others in different governmental or business sectors, but does not include hacks revealed in July–August 2014.

As this white paper is being finalized, there is news reporting regarding the discovery of large quantities of personal information (including user name/password) mined from many websites by a Russian-based hacker group and new malware threats focused at retailers. According to a report released by the U.S. Department of Homeland Security, technology that is widely used to allow employees to work from home or permit IT and administrative personnel to remotely maintain systems is being exploited by hackers to deploy point-of-sale (PoS) malware that is designed to steal credit card data. This threat is being called “Backoff Malware.” Homeland Security estimates it has been around since October 2013 with a very low antivirus detection rate at the time it was discovered; meaning that even systems with fully updated and patched antivirus software would not be able to identify Backoff as malicious malware.
SNAPSHOT OF TARGET

Target announced at the end of February 2014 that the company’s profit fell by 40 percent in the fourth quarter of 2013. The company reported $61 million pretax expenses related to the breach, but expected $44 million in cyber insurance payments against this figure. These expenses were incurred for legal costs, breach notification, forensics, and PR/crisis management to date. However, the worst financial costs are yet to come. A senior Gartner analyst estimated that the total exposure to Target could be $450–$500M, which considers lawsuits, regulatory investigations, breach response, fines and assessments, loss of revenue, and security upgrades.

- Both the cyber insurance and directors and officers insurance programs at Target are involved, since Target announced significant revenue/profit shortfalls caused by brand damage/customer fallout and costs to improve IT security. At least two derivative shareholder actions have been filed, which have triggered Target’s D&O insurance.
- More than 100 lawsuits are pending against Target at this time, with many consumer class actions and some actions filed by individual financial institutions, claiming for costs of cancelling and reissuing compromised cards, absorbing fraudulent charges made on the cards, and the loss of anticipated fee income from the holiday season. There has been activity to consolidate these lawsuits into three groups of plaintiffs to facilitate the legal process.
- Allegations surround Target giving network access to a third-party vendor, a small HVAC company with weak security, which allowed the attackers to gain a foothold on Target’s network. From that point of entry, the attackers allegedly moved to the most sensitive areas of Target’s network storing customer information. Malware installed at POS terminals utilized so-called “RAM scraping,” and the attack apparently proceeded despite apparent warning signals.

It is not an overstatement to say that there is a “pre-Target and “post-Target” state of the cyber market for major retailers from both the underwriting and the client side.
Target staff had urged the company to review the security of its payment system months prior to the breach, according to American Banker and The Wall Street Journal reports. Some financial institution plaintiffs are alleging that as early as 2007, Target was warned by a data security expert about the possibility of a data breach in its point-of-sale system. Banks claim that a layered security system would have made the hackers’ task more challenging—Brian Krebs, a noted security analyst, describes a “POS kill chain” for more effective layered security posture.

Despite Target having obtained a certification based on the credit card association data security standards (called PCI DSS), the cyber thieves implanted malware on POS terminals and successfully removed massive amounts of sensitive customer information/card information to a server in Eastern Europe. The cyber thieves were able to sell information from these cards via online black-market forums so that later others could use these compromised cards to purchase high-dollar items or extract money from an ATM.

Target executives have appeared at U.S. Congressional hearings and have repeatedly been the subject of adverse media attention, which further compounds financial and brand damage. Target’s chief information officer and chief executive officer have resigned.

Major insurers and Lloyd’s underwriters are involved in the cyber and directors and officers programs of Target and other retailers.
UNDERWRITERS’ VIEW

The lessons learned from these events by underwriters reflect themselves in selection, retention, and limits offered. So what are these lessons?

1. Underwriters understand that there is an underlying security vulnerability of magnetic swipe cards (common in the U.S.) vs. Europe’s adoption of EMV “smart” chip-and-PIN payment cards. Underwriters are responding favorably to a company with major credit card/POS exposure who embarks on tokenization in North America.

2. Hacks are getting more sophisticated, with teams of hackers in multiple countries. Offensive hacking weapons are numerous and cheap, and hackers have learned to quietly roam inside corporate networks for a significant length of time before a pattern of consumer fraud emerges. Underwriters want to understand how the retailer knows its system has not already been compromised.

3. Writing both cyber and directors and officers liability can lead to unacceptable aggregation exposure. Additionally, multiple companies in the U.S., Bermuda, and Europe, of the same insurer, can be writing lines on the same insured. AIG, for example, has a centralized approval for U.S.-domiciled business through its underwriting management team based at its New York headquarters.

4. Insurers wrote layers of major retailers at minimum premiums that now look thin to say the least. Some insurers are no longer writing new major retailers or do not want to be at the thin top of the program. CNA, Axis, and XL are examples of insurers taking such actions.

5. PCI DSS standards (required by credit card associations) do not guarantee immunity from the ever-evolving tactics used by the global criminal community to exploit data and systems. The complexity of questions being asked about credit card security and POS is at much greater depth, and PCI DSS compliance is viewed as a minimum—underwriters want to know what areas of security are even better than the PCI DSS standards.

6. The retail industry lacks threat intelligence, unlike the major financial institutions that have had a long-established ISAC and interactions with senior law enforcement agencies. Recently, an ISAC was formed for the retail industry. Underwriters want to know the extent of threat intelligence available to a retailer to build on its internal IS knowledge.

7. Static defense models (e.g., antivirus and intrusion detection) upon which many companies rely, are not sufficient to prevent a systemic data breach or “advanced persistent threats.” The “kill chain” concept is part of the more knowledgeable underwriter’s vocabulary.

8. Outsourcing provides process efficiencies and expense reduction, but it does not reduce security risk, particularly in the age of ever-evolving technology, the shift to IT/software/communications as a service (including cloud), and multiplicity of access points to vendors (such as Target’s HVAC contractor). For example, vendors may store multiple clients’ sensitive data in a single database—that has happened in a breach involving a major e-mail marketing/customer loyalty program vendor. Underwriters want to understand vendor risk management, which is comprised of due diligence, contractual provisions including a strong indemnity, and cyber insurance requirements. Is such sensitive customer data encrypted and held in separated databases when
stored by vendors? With regard to credit cards and third party providers, merchants need to implement policies and procedures in line with PCI DSS Requirement 12.8, which is part of the updated PCI DSS 3.0 security standards issued late last year. Recently the PCI governing body issued new guidance to merchants to help them fulfil this requirement, focusing on due diligence, risk assessment, contractual requirements, and monitoring PCI compliance. Demonstration of compliance in this area is a significant concern in the underwriting process.

9. Better underwriters want to be aggressive on quality risks but are becoming more selective and considering the use of increased retentions, limits containment, and, in some cases, pricing changes. We have successfully navigated these waters with our major retailers through a much more thorough underwriting briefing presentation, in which we assist and rehearse with our client’s presenters.

10. A note on privacy is needed here—some major markets have cut back on privacy coverage, particularly on criminal eavesdropping (critical for a call center exposure), violation of TCPA and other consumer protection laws, wrongful collection, and aggressive marketing practices. Law and regulation is constantly evolving with new and greater exposure. The E.U. is talking about the “right to be forgotten.” We have focused on this area and have been alerting our clients to privacy risk vs. privacy coverage and negotiating much better terms than basic forms allow.
PEER GROUP VIEW

Our major clients are asking this essential question post-Target at their shop: “How bad can a bad day be?” Since the Target breach, major retailers generally want higher towers if they purchased less than $50M. The average limit is $50M now, but there are retailers at $100–$125M. Prior to the Target breach, the average limit was $25M.

- **Post-Target, we have seen some retailers ask underwriters for a higher retention quote in order to shift funding to severity (i.e., higher tower), but there is no equal swap for retention to fully fund another $10M on the tower.** For $1B plus revenue retailers, retentions start at $1M and typically range to $2.5M—certainly $5M would be on the top end. It is critical from our broker perspective to find the right balance between premium and risk.

- **Our clients are asking to have best market wordings for their security and privacy exposures, and we are constantly evolving our coverage requests with insurers.** We deliver underwriting specifications as part of the submission, rather than just forwarding underwriting data. An example of an innovation from Lockton is including nonreimbursable defense coverage for TCPA to at least $1M. We are able to achieve better results because we recognize the underwriters’ concern for better information, and we are known for providing a strong underwriting briefing for all underwriters to listen to and ask questions.

- **Our clients are concerned about the whole data breach response and coordination with underwriters.** A breach can cause not only major financial loss, but also significant damage to brand and reputation if handled badly. We have developed a coordinated approach with clients so that all major aspects of breach response are built into the program they purchase, including preapproved forensics and external legal counsel. The response must consider possible jurisdictions and venues of the affected individuals who could be in multiple states, provinces, and countries.

More than 5,300 professionals at Lockton provide 41,000 clients around the world with risk management, insurance, and employee benefits consulting services that improve their businesses. From its founding in 1966 in Kansas City, Missouri, Lockton has attracted entrepreneurial professionals who have driven its growth to become the largest privately held, independent insurance broker in the world and 10th largest overall. Independent researcher Greenwich Associates has awarded Lockton its Service Excellence Award for risk management for large companies. For five consecutive years, Business Insurance magazine has recognized Lockton as a “Best Place to Work in Insurance.” To see the latest insights from Lockton’s experts, check Lockton Market Update.

We attract and retain the best talent to ensure that our clients have access to a team with an enviable spectrum of skills. This is particularly evident within our Global Technology and Privacy Practice (“GTPP”), where we have drawn together experienced individuals from legal, broking, and underwriting backgrounds in the U.S. and in London. Clients across the globe count on us for risk management and specialist insurance solutions.

GTPP is recognized as an innovator in the industry. We design cyber insurance programs for first and third party exposures and the client’s desired approach for data breach contingency response. We have unique facilities, as well as proprietary wordings with leading underwriters, including intangible risk and reputation harm. We also provide consultation services and benchmarking information on privacy and security risks for our clients.

For more information on security and cyber risk, contact your Lockton account team.
Our Mission

To be the worldwide value and service leader in insurance brokerage, employee benefits, and risk management

Our Goal

To be the best place to do business and to work