FBIC
Fung Business Intelligence Centre
GLOBAL RETAIL RESEARCH & INTELLIGENCE QUICK TAKE
NOVEMBER 20. 2014

RETAILERS NEED TO FOCUS HOLISTICALLY ON CYBERSECURITY

- When it comes to cybersecurity, retailers need to spend smarter, not necessarily more
- Holistic, enterprise-wide cyber-risk detection and prevention are critical first steps
- The role of human error behind the recent cyber-attacks is instructive
- The US shift to chip-and-PIN credit cards will help but only partially

DEBORAH WEINSWIG
EXECUTIVE DIRECTOR-HEAD GLOBAL RETAIL RESEARCH AND INTELLIGENCE
FUNG BUSINESS INTELLIGENCE CENTRE
DEBORAHWEINSWIG@FUNG1937.COM NEW YORK: 646.839.7017

FBIC
Fung Business Intelligence Centre
GLOBAL RETAIL RESEARCH & INTELLIGENCE QUICK TAKE

NOVEMBER 20, 2014

RETAILERS NEED TO FOCUS HOLISTICALLY ON CYBERSECURITY

This Thanksgiving will mark the one-year anniversary of the cyber-attack on US retailer Target, which shook the entire retail industry. Cybersecurity is clearly an urgent challenge and where retailers are increasing their spending.

Since the Target incident, the retail sector has become much more proactive and aggressive in its efforts to prevent future data-breach crises. Cybersecurity risk management is no longer an initiative taken only to protect a company's intellectual property or internal data but, rather, as essential in safeguarding consumer data privacy and corporate reputation. But, despite the industry's heightened investment and vigilance, we have seen a constant stream of data breaches at big-box retailers in 2014.

Selected High Profile Cybersecurity Incidents in the Retail Sector

Date of Discovery	Retailer	Compromised data	Further consequences & notable features
Dec. 2013	**Target**	40 million credit cards 70 million customers' personally identifiable information	Breach lasted 3 weeks. Company now funds sectorwide initiative to share breach information
Jan. 2014	**Neiman Marcus**	Between 350,000 to 1.1 million credit cards	
Jan. 2014	**Michael's**, an arts and crafts retailer	3 million credit cards	Second breach in three years. Previous breach occurred in May 2011
Jul. 2014	**Goodwill Industries**, a network of agencies selling donated clothing and household items	Under investigation	Breach lasted 18 months
Sept. 2014	**Home Depot**	56 million debit and credit card numbers 53 million customers' email addresses	Breach lasted six months between April and September 2014
Oct. 2014	**Staples**, an office supply chain	Under investigation	

As of October 31, 2014
Source: Krebs on Security

Our research found that corporations in the US and abroad have generally sharpened their focus on early detection of external and internal vulnerabilities, and the importance of moving quickly to remedy those vulnerabilities and strengthen defences to prevent future breaches. Entire networks need to be evaluated for security. Companies must ensure that everyone in the organization understands the importance of and is fully engaged in the prevention and the constant monitoring against cybersecurity risks. Here are some additional tips from experts in the field.

Are Retailers Under-Spending on Cybersecurity?

Some may assume that retailers have been underinvesting in cybersecurity risk management. According to a recent Wall Street Journal article, retailers devote far less of their IT budgets on cybersecurity than many other industries. According to Gartner, the IT research company, the retail sector spends 4% of its IT budget on security, versus 5.5% and 5.6% for the banking and healthcare sectors, respectively.

Some of the disparity in cybersecurity budgets can be explained by the differences in regulatory oversight. Retailers aren't as heavily regulated as banks and healthcare firms, which are audited for cybersecurity compliance in the US. In the retail sector, the Payment Card Industry (PCI) standards are not as rigorous and pertain only to the handling of credit cards. If personal information such as social security numbers is leaked, in some jurisdictions there is not even a legal requirement for retailers to announce publicly that a breach has occurred.

Smarter Spending, not More Spending

But more spending is not necessarily the solution. According to cybersecurity consultant Thomas Parenty, the problem facing most companies isn't that they are spending too little but that they are spending unwisely. His advice to companies is to ensure that the security products they buy are linked to a business purpose and are applied across the entire enterprise. Human error can often defeat the best-laid plans. In our interview with him, Parenty cited several examples:

- **Firewalls Installed but Never Tested.** A large global payments brand had a huge budget for cybersecurity and bought security products from every major vendor. However, the company failed to test the whole system. In a risk assessment, it was found that firewalls were installed but never tested. Also, the firewalls were set up to satisfy compliance, but the employees did not recognize the importance of actually using the firewalls.

- **Incomplete Installations.** After the Home Depot breach, it was revealed that encryption software that could have reduced the scale of the breach had been purchased for the POS terminals. But, according to a BusinessWeek report, employees admitted that the software had not been completely installed.

- **A Lack of Internal Controls.** An employee at an Asian auto manufacturer managed to obtain and leak blueprints of a car design because the company's information-sharing system was categorized by department. Regardless of rank or job function, everyone in the same department could access all the data. When the IT systems architect was asked why he did not modify the information-sharing platform to provide security for the stealth-mode project, he replied, "No one ever asked me to."

Early Risk Detection and Prevention Are Key

Part of the cybersecurity challenge is well understood, but the retail industry and the related banking and payments sectors had simply not acted quickly enough to implement solutions. If retailers had known about the vulnerabilities in their IT networks before disaster struck, they would have taken action to mitigate the risks. After all, recovering from a breach is about five times as expensive as preventing one, according to Garnet research. For every $5 spent recovering from a breach, companies could have spent $1 on encryption technologies that could have diminished the impact.

Death of the Magstripe Will Help but Only to a Point

The security risk of credit cards with magnetic stripes—the mainstay of the US-issued credit card system—has been known for years: They contain all of the customer information needed to produce flawless counterfeit cards: account number, expiration date and a secret code call the CVV.

After years of resistance because of the considerable transition costs, the US is finally embracing the more secure chip-based authentication systems called EMV (the standard pioneered by Europay, Mastercard and Visa) that most of the rest of the world has already adopted. The first milestone for US retailers is the October 2015 deadline, when the industry will be required to switch to the sophisticated point-of-sale readers needed to accept chip-and-PIN cards or face having to eat more of the costs of fraud and data breaches. The late adoption of more secure credit card technology makes the US an easier target in data theft—half of the world's credit-card fraud happens in the US.

But the move toward chip-and-PIN is only a partial solution. Having a chip in your card doesn't make online transactions safer. The retirement of the magstripe and the ongoing development of tokenization technologies—which replace the static credit-card number with a temporary token that changes for each transaction (used by Apple Pay and Visa's newly announced Visa Token service)—should go a long way in curbing the spread of cyber fraud and identify theft, for both in-store and online transactions. Target's case is instructive. Chip-and-PIN credit card technology would not have prevented the data breach, according to Krebs on Security. This is because data transmission between Target's POS terminals and the card-issuing banks was not encrypted and, therefore, still exposed to hacking. End-to-end encryption would be required to fully protect consumer data.

Elevate Cybersecurity on IT Priority List

IT department goals are often at odds with those of cybersecurity risk management, and may not always provide the right incentives to avert risks. IT departments are typically rewarded when technology systems operate smoothly, but are not rewarded for managing risks or averting a future problem. Cybersecurity consultant Parenty likened this mindset to what can pervades some parts of the construction industry. "Construction companies get paid to put up buildings," he said. "They don't get paid to make sure the building is still standing 20 years from now."

To elevate the incentives for long-term cybercrime prevention, cybersecurity experts advise that the CISO (chief information security officer) report directly to the CEO or to the board of directors, instead of reporting to the CIO.

Conclusion: A Holistic Approach Is Imperative

The mistakes made by companies in some cybersecurity incidents may seem obvious in hindsight. But the vulnerabilities were undetected at the time. Many of the data breaches of 2013-14 had been in place for several months before they were detected (perpetrators have sometimes chosen the Thanksgiving and Christmas shopping season in order to wield maximum damage).

For retailers looking to strengthen their cybersecurity protocols and procedures and resolve any problems before it's too late, the imperative starting point would be an overall risk assessment, interdepartmental coordination and continued monitoring—and to make cybercrime prevention a top priority within the IT department. Retailers, banks and payment solution providers need to evaluate risk in their systems and networks as a whole.

Deborah Weinswig, CPA
Executive Director – Head Global Retail Research and Intelligence
Fung Business Intelligence Centre
New York: + 646.839.7017
Hong Kong: +1.852 6119 1779
deborahweinswig@fung1937.com

Marie Driscoll, CFA
mariedriscoll@fung1937.com

Christine Haggerty
christinehaggerty@fung1937.com

John Harmon
johnharmon@fung1937.com

Amy Hedrick
amyhedrick@fung1937.com

Fong Lau
fonglau@fung1937.com

Lan Rosengard
lanrosengard@fung1937.com

Freda Wan
fredawan@gmail.com

Jing Wang
jingwang@fung1937.com