LESSONS LEARNED

Home Depot Security Breach

Home Depot is an American retailer of home improvement and construction products and services. It operates many big-box format stores across the United States, all ten provinces of Canada, as well as Mexico.

In September 2014, Home Depot, the US home improvement retailer, confirmed it experienced a breach in security that affected as many as 56 million credit and debit cards in Canada and the US. Criminals used unique, custom-built malware to steal account numbers from Home Depot's point-of-sale systems. The do-it-yourself retailer has 180 stores in Canada and more than 2,200 in the US.

Despite ongoing efforts to improve internet security systems, hackers continue to find holes in various industries, causing mayhem to both corporations and consumers that trust their information will be protected. Inadequate company safeguards and the mishandling of consumer data can come at a high price, not only in the form of lawsuits but also consumer mistrust, resulting in devalued company stocks. The security breach could cost Home Depot $3 Billion[i].

bsi.

...making excellence a habit.™

Breach

According to Home Depot's Press Release dated September 18, 2014, the investigation revealed:

- **"Criminals used unique, custom-built malware to evade detection. The malware had not been seen previously in other attacks, according to Home Depot's security partners.**
- **The cyber-attack is estimated to have put payment card information at risk for approximately 56 million unique payment cards.**
- **The malware is believed to have been present between April and September 2014. [ii]"**

Home Depot's statement also indicated it had completed a security upgrade that should prevent any further breach of its systems in US stores and will roll out enhanced encryption to its Canadian stores by early 2015.

According to Home Depot, terminals identified with the malware were taken out of service and the malware has been eliminated from company's systems.

Canadian credit and debit cards have chip technology that should protect customers, it said. Home Depot said it has rolled out enhanced encryption of payment data to all its U.S. stores and plans to have the same safeguards in place in Canada by next year.

Home Depot repeated its assurance that there is no evidence the cybercriminals gained access to customers' PINs.

Related Incidents – Celebrity Hacking & Target

Home Depot's story is not an isolated incident. Recently, Jennifer Lawrence and other celebrities, whose private pictures were leaked online, may have had their Apple's iCloud passwords stolen by hacking software.[iii] Inappropriate pictures of Jennifer Lawrence and many other celebrities were posted on anonymous message board 4Chan and other internet sites, infuriating the stars and their management.

US discount retailer Target suffered stagnant sales and its profits were hard-hit by its security breach during the holiday season of 2013.

Industry Impact

Data theft has become a disturbing trend, expanding worldwide at an alarming rate. Unlike traditional theft crimes, data information theft is difficult to detect and even more difficult for companies to overcome. On top of the financial losses of lawsuits, payouts, and litigation costs, individuals within the company could also face jail time if their actions are deemed fraudulent, negligent or wholly indifferent to the potential harm of the consumer.

Many of these types of losses could possibly be avoided if a verifiable management system standard such as ISO/IEC 27001, for Information Security, is in place. Such a management system would have helped prevent violations involving electronic commerce, online transactions, and publicly available information.

bsi.

ISO/IEC 27001 takes a risk-based, holistic approach to security and has an overarching top-down governance process supported by 114 built-in controls that address people, processes, and technology to ensure that information security is an integral part of information systems through the entire lifecycle of a transaction and across the enterprise. This also includes the requirements for information systems, which provide services over public networks. Certain controls in ISO/IEC 27001 address public networks and transactions, specifically A.14.1.2 *Securing application services on public networks*, to protect information "from fraudulent activity, contract dispute and unauthorized disclosure and modification" and A.14.1.3 Protecting application services transactions to "prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay."

Home Depot Responds

The size of the hack makes it more likely Home Depot will face steep costs. Bill Guard, a personal finance security service, estimated the potential fraud to cost as high as $3 billion for the company.[iv]

Already, it faces a class-action suit on behalf of Canadian customers, launched by Saskatchewan lawyer Tony Merchant. He estimates up to four million Canadians may be affected by the breach.[v]

Home Depot hastened to assure investors that it is on track to meet its target sales in the third quarter. In its September 18, 2014 news release, Home Depot estimated its sales will grow by 4.8 percent and raised its estimate of third quarter profit per share to $4.54, from $4.52.

Home Depot's profit estimates take into account the costs of investigating the data breach, providing credit monitoring services to its customers as well as legal and professional services. It has pledged that no customer will be on the hook for any fraudulent charges.

But it has not factored in any losses related to the breach, including liabilities on consumer credit and debit cards and from any civil litigation.

"Those costs may have a material adverse effect on the Home Depot's financial results in the fourth quarter or future periods," according to its news release.

BSI Solutions

BSI provides certification to standards, developed to protect your organization. As an Information Security Management System, ISO/IEC 27001 is designed to help you select adequate and well-balanced security controls which will protect information assets and give confidence to interested parties, including your customers. Certification to ISO/IEC 27001 is an essential safeguard for any organization. In addition to certification services, BSI offers a range of training courses that are designed to provide the tools you and your staff need to learn and understand ISO/IEC 27001, as well as oversee audit programs for your management system. BSI works with this standard, and many more, to protect your organization and its most valued assets, including the relationship between you and your customers, from potential threats.

About BSI

One Company, One Solution. By packaging assessment, training, and a management system toolset, BSI delivers a business improvement solution that combines it all in a comprehensive service offering and allows us to provide an integrated approach to meet the needs of an organization and embed excellence across the business. BSI presents a one-stop value proposition from the decision to improve systems through to registration and continual improvement. From start to finish, BSI helps turn complexity into simplicity.

Cloud Security

For Cloud Security, BSI and CSA Star Certification provide a comprehensive set of offerings for cloud provider trust and assurance. The CSA STAR Program is a publicly accessible registry designed to recognize the varying assurance requirements and maturity levels of providers and consumers, and is used by customers, providers, industries, and governments around the world. The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Control Matrix, a specified set of criteria that measures the capability levels of the cloud service.

i http://www.cbc.ca/news/business/home-depot-credit-card-security-breach-could-cost-3b-1.2768043

ii https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf

iii http://www.people.com/article/jennifer-lawrence-FBI-investigating-phone-hack

iv http://blog.billguard.com/2014/09/home-depot-data-breach-estimated-impact/

v https://www.merchantlaw.com/classactions/homedepot.php

bsi.

To find out more, visit www.bsigroup.ca

BSI Group Canada Inc.
6205B Airport Road, Suite 414
Mississauga, Ontario
L4V 1E3
Canada

Tel: 1 800 862 6752
Fax: 1 416 620 9911
Email: Inquiry.canada@bsigroup.com
Web: www.bsigroup.ca
www.bsigroup.ca/fr

BSI Group America Inc.
12950 Worldgate Drive, Suite 800
Herndon, VA 20170
USA

Tel: 1 800 862 4977
Fax: 1 703 437 9001
Email: inquiry.msamericas@bsigroup.com
Web: www.bsiamerica.com

BSI/CA/142/MS/1014/E