LESSONS LEARNED

11 Arrested in Blue Cross Blue Shield of Michigan Insider ID Theft Scheme

In a story published by Health Information Security, a former customer service representative at Blue Cross Blue Shield of Michigan (BCBSM) and ten other individuals were recently arrested in connection with an alleged identity theft scheme. More than 5,500 health plan members were affected, resulting in hundreds of thousands of dollars in credit fraud. (McGee, 2015)

According to the indictment, the BCBSM employee had an agreement with outside sources to receive payments in exchange for providing personal identifying information (PII) of patients covered by health plans administered by BCBSM. The employee would obtain screenshots of the PII and would print them out to be sold for use in identity theft and credit fraud. The indictment notes that the theft activities went on for about two years from around January 2012 until December 2014. (Local 4 - ClickOnDetroit news staff, 2015)

The information stolen included names, addresses and Social Security numbers and was used to create counterfeit credit cards and open fraudulent lines of credit in the victims' names. (McGee, 2015) Several fraudulent accounts were opened with major department stores across the country.

bsi.

...making excellence a habit.™

Let's look at the facts of the case and see how this incident may have been avoided or its impact minimized if a verifiable management system standard, such as ISO/IEC 27001 for an Information Security Management System (ISMS), was in place using exact quotes from the story/ indictment.

The indictment noted that Patton was authorized by BCBSM "to access individually identifiable health information of patients who received health coverage from health plans administered by BCBSM, for only such purposes as permitted by the HIPAA regulations." (McGee, 2015)

ISO/IEC 27001:2013:

A.9.2 User access management

A.9.2.1 User registration and de-registration

Control – A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

A.9.2.5 Review of user access rights

Control – Asset owners shall review users' access rights at regular intervals.

A. 9.2.6 Removal or adjustment of access rights

Control – The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

The employee allegedly had an agreement with accomplices "whereby she received payments in exchange for obtaining and disclosing individually identifiable health information of patients covered by health plans administered by BCBSM for purposes not authorized by HIPAA." Screenshots of the fraudulently obtained PII were printed out by the employee to be sold to the co-conspirators for use in identity theft and credit fraud, prosecutors say. (McGee, 2015) While the employee needed to be given access to information in order to perform her job, the full range of the information accessible may have been more than the job required. (See below.)

A.9.4 System and application access control

A.9.4.1 Information access restriction

Control – Access to information and application system functions shall be restricted in accordance with the access control policy.

Information could have been limited to what was required for the purpose of the job role.

A.9.4.4 Use of privileged utility programs

Control – The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

A.12.4 Logging and monitoring

A.12.4.1 Event logging

Control - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

A.16 Information security incident management

A.16.1.1 Responsibilities and procedures

Control - Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

A.16.1.2 Reporting information security events

Control - Information security events shall be reported through appropriate management channels as quickly as possible.

A.16.1.6 Learning from information security incidents

Control - Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

The indictment states the employee "had access to the [company's] computer system and databases and had received training in and became familiar with her obligations of confidentiality under the HIPAA regulations."

A.7 Human resource security

bsi.

A.7.2 During employment

A.7.2.2 Information security awareness, education and training

Control - All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

A.8.2 Information classification

A.8.2.1 Classification of information

Control - Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

A.8.2.3 Handling of assets

Control - Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

A.9.4 System and application access control

A.9.2.3 Management of privileged access rights

Control - The allocation and use of privileged access rights shall be restricted and controlled.

A.9.2.4 Management of secret authentication information of users

Control - The allocation of secret authentication information shall be controlled through a formal management process.

National Accounts Service Company (NASCO) based in Georgia is the company that provides IT Solutions to Blue Cross Blue Shield plans across the nation. (Local 4 - ClickOnDetroit news staff, 2015)

NASCO Customer Service Workstation (NCSW) is a computer application which enables users to research and document eligibility, benefits, claims, payment information, maximums, coordination of benefits and provider data in response to inquiries from subscribers and providers. NCSW pulls eligibility, claims and provider information from NASCO Mainframe (NPS). NASCO's mainframe NPS is located in Lexington, Kentucky.

A.15 Supplier relationships

A.15.2 Supplier service delivery management

A.15.2.1 Monitoring and review of supplier services

Control - Organizations shall regularly monitor, review and audit supplier service delivery.

A.9.4 System and application access control

A.9.4.1 Information access restriction

Control - Access to information and application system functions shall be restricted in accordance with the access control policy.

A.9.4.4 Use of privileged utility programs

Control - The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

About BSI

BSI provides training, assessment and certification, and software solutions 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.

BSI's range of training courses are designed to provide the tools you and your staff need to 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 its most valued assets, including the relationship between you and your customers, from potential threats.

Bibliography

Local 4 - ClickOnDetroit news staff. (2015, March 10). ClickOnDetroit. Retrieved from http://www.clickondetroit.com/news/11-charged-with-stealing-fraudulently-using-blue-cross-blue-shield-of-subscriber-information/31716154

McGee, M. K. (2015, March 15). Healthcare Information Security. Retrieved from http://www.healthcareinfosecurity.com/11-arrested-in-insider-id-theft-scheme-a-8000?rf=2015-03-12-eh&mkt_tok=3RkMMJWWfF9wsRonu6%2FIZKXonjHpfsX57ewtWqSg38431UFwdcjKPmjr1YIAWp8na%2BqWCgseOrQ8kFkJV9qtVc0Sqal%3D

bsi.

To find out more, visit www.bsiamerica.com

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 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/USA/440/MS/415/E