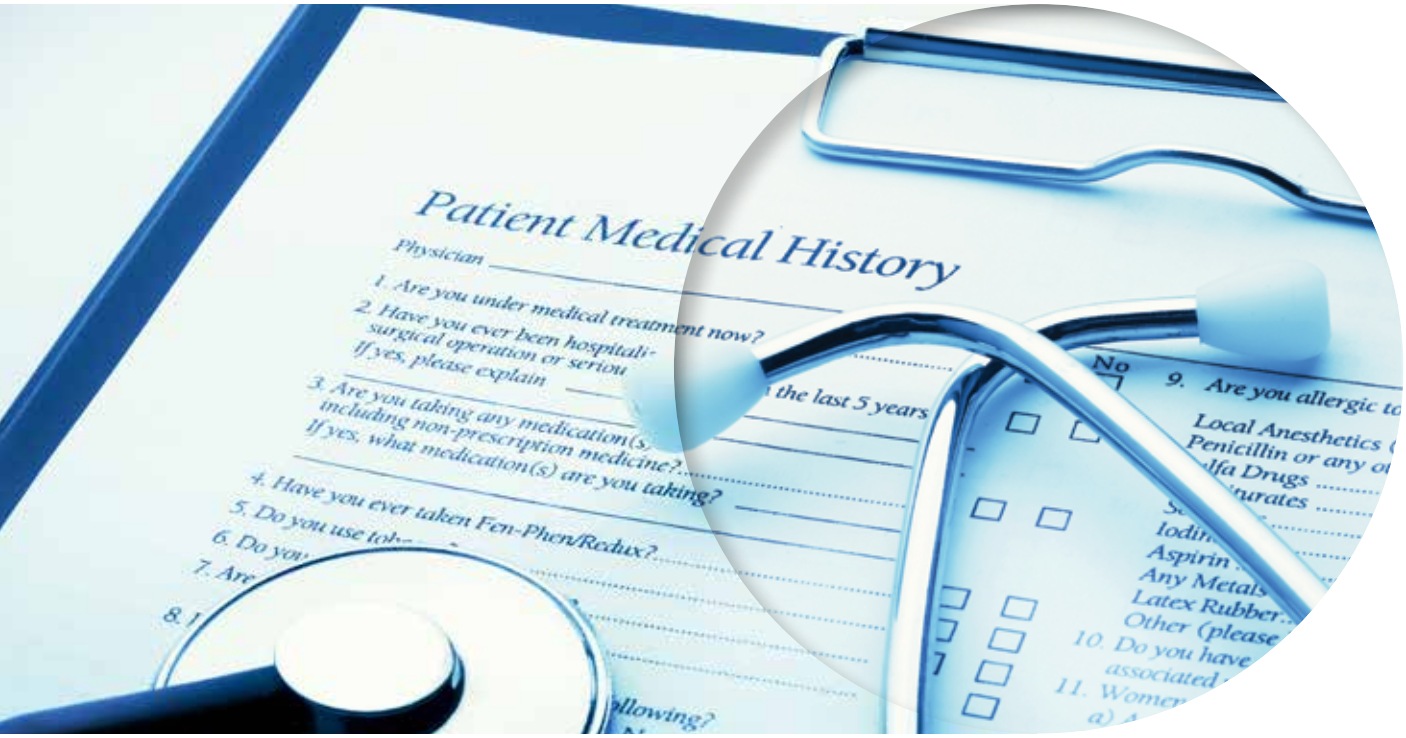
LESSONS LEARNED

Anthem Data Breach



In December of 2014, Anthem, Inc., a major health insurance company, suffered a massive data breach when hackers gained access to a corporate database, reportedly containing personal information from as many as 80 million of the health insurer's current and former U.S. customers and employees.

Initially, it was claimed to be a very sophisticated external cyber-attack. How sophisticated remains to be seen, but now Anthem, Inc. believes the attack began with phishing e-mails sent to a handful of its employees. The e-mails were used to trick the individuals into visiting malicious websites or executing malware.

The company's $100 million dollar cybersecurity insurance policy may be exhausted by the 80 million current and previous customers, staff and investors Anthem is required to notify. (Osborne, 2014) The investigation, potential lawsuits and fines will increase that cost, as will the hit to the company's reputation. In addition, entities and business associates covered by the HIPAA Final Omnibus Rule who are found responsible for violating HIPAA privacy and security rules, and failing to safeguard patient protected health information, could face potential fines up to $1.5 million.

According to an annual survey by the Ponemon Institute, the percentage of healthcare organizations that have reported a criminal cyber-attack has risen to 40 percent in 2013 from 20 percent in 2009. (FINKLE, 2014) This statistic is thought to be a gross underrepresentation as breaches that involve less than 500 people are not required to be reported by law.

Reuters reported last year that personal health information is worth 10 times more than credit card numbers on the black market. According to experts who have investigated cyber-attacks on healthcare organizations, this data is used to create fake IDs, buy medical equipment or drugs for resale, or to file false claims with insurers. Hackers have found that hospitals typically have poor information security safeguards and it is relatively easy to harvest large amounts of personal information. (FINKLE, 2014)

Industry Impact

These breaches are bleeding into other critical areas, including risks to medical devices, threatening not just privacy but human lives. The reality is that hackers are exploiting basic flaws in security systems. Many of the cracks in the security walls are caused by human error; however, others are due to organizations settling for basic "compliance" rather than continual improvement through a formal information security management system. For instance, as noted by security experts, HIPAA doesn't expressly require encryption if an organization documents that it has used another "reasonable and appropriate" safeguard to protect data. (McGee, 2015)

In an interview with Healthcare IT News on the new HIPAA rules, the Department of Health and Human Services' Office for Civil Rights Director, Leon Rodriguez, was asked where HIPAA-covered entities most often make their biggest misstep. Rodriguez pointed to risk analysis inadequacies. It's the "failure to perform a comprehensive, thorough risk analysis and then to apply the results of that analysis," he said.

Many of these types of losses may be avoided if a verifiable management system standard, such as ISO/IEC 27001 for Information Security Management System (ISMS), is in place. This type of ISMS helps prevent violations caused from an inadequate risk management program, lack of encryption and inadequate employee training. An effective ISMS can fill the gaps in the HIPAA security rules by instilling a process of continual improvement and greater accountability through proactive, rigorous third-party audits that spur root cause analysis and corrective action.

In a recent article published by HeathInfo Security, a number of privacy and security experts offered tips outlining actions that healthcare organizations can take to avoid becoming the next hacking victim, all of which can be implemented through the specifications outlined in ISO/IEC 27001 and ISO/IEC 27002 guidance. (McGee, 2015)

Experts recommend a multi-layered approach to information security, suggesting the following steps, which can be pegged to the associated ISO/IEC 27001 controls.

Re-evaluate workforce training to help prevent employees from falling victim to social engineering hoaxes, such as phishing.

- ISO/IEC 27001:2013 – 7.2 Competence; determine the necessary competence of person(s) doing work under its control that affects its information security performance; ensure that these persons are competent on the basis of appropriate education, training, or experience; evaluate the effectiveness and retain appropriate records as evidence.
- 7.3 Awareness; Persons doing work under the organization's control shall be aware of: Security policy, their contribution to the effectiveness of the information security management system and the implications of not conforming with the information security management system requirements.
- A.7.2.2 Ensuring Information security awareness, education and training for all employees including contractors as appropriate.

bsi.

Scrutinize Data Storage Practices

- ISO/IEC 27001:2013 - A.9 Access control (Policy, User Access Management, User Responsibilities, System and Application Access Control)
- 7.5.3 Control of documented information – (Protection, Distribution, Storage and protection and Retention and Disposal)

Carefully Assess Encryption

- A.10 Cryptography - Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

Implement and Test Detection Tools

- A.13.1 Network security management - Objective: To ensure the protection of information in networks and its supporting information processing facilities.
- A.14 System acquisition, development and maintenance (Security requirements of information systems , Security in development and support processes, Test data.

Go Beyond a Focus on Compliance

- All of ISO/IEC27001. It has been prepared to provide requirements for establishing, implementing, measuring, maintaining and continually improving an information security management system.

Limit Social Security Number Use

- ISO/IEC 27001:2013 - A.9 Access control (Policy, User Access Management, User Responsibilities, System and Application Access Control)

Keep an Eye on Vendors

- ISO/IEC 27001:2013 - A.15 Supplier relationships (Information security in supplier relationships, Supplier service delivery management)

Share Cyber-Intelligence with Peers

- ISO/IEC 27001:2013 - 7.4 Communication - The organization shall determine the need for internal and external communications relevant to the information security management system.
- A.6.1.4 Contact with special interest groups - Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
- A.16.1 Management of information security incidents and improvements Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

About BSI

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 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.

Bibliography

http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

McGee, M. K. (2015). Protecting Against Anthem-Like Attacks. HealthInfo Security.
http://www.healthcareinfosecurity.com/protecting-against-anthem-like-attacks-a-7896

Osborne, C. (2014). Anthem data breach cost likely to smash $100 million barrier. ZDNet.
http://www.zdnet.com/article/anthem-data-breach-cost-likely-to-smash-100-million-barrier/

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/422/MS/215/E