PECB

When Recognition Matters

WHITEPAPER

NO **ISO 27001 CERTIFIED** COMPANIES AMONG LARGEST DATA BREACHES 2014-2015

ISO 27001 CERTIFICATION PROVIDES CONCRETE BENEFITS

www.pecb.com

CONTENT

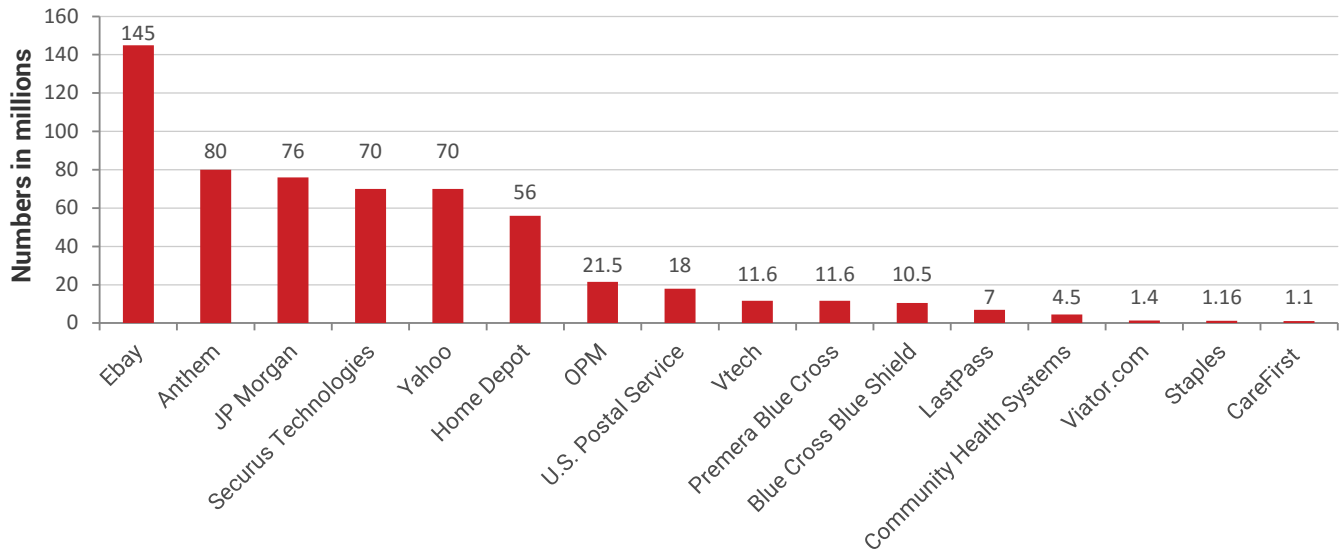
INTRODUCTION

Corporate data breaches reports constantly hit new headlines, which serve to remind us that nowadays our information is unsecured more than it's ever been before. In 2015, data breaches, cybercrimes, and hacking were top business issues that garnered much media attention and compromised the integrity of many companies.

PECB has conducted a research on the biggest data breaches done in 2014 and 2015. According to this research, no industry – online dating, health insurers, toy manufactures, service providers, federal governments, and other sectors of industry – was immune to cyber–attacks. From the 20 biggest breaches, on average, each one affected about 35 million people. The company that was affected the most was eBay, followed by Anthem and JP Morgan.

None of the hacked companies were certified against **ISO/IEC 27001** at the time of the data breach.

NUMBER OF PEOPLE AFFECTED BY DATA BREACHES PER COMPANY



As cyber-security incidents increase and breaches become more significant, they cause a high financial impact. Approximately $191 million have been spent by companies in 2014 to overcome the losses caused by data breaches. A data breach costs large organizations on average $93 million of losses. Hence, the need for secure information is becoming not only a desire, but also a necessity.

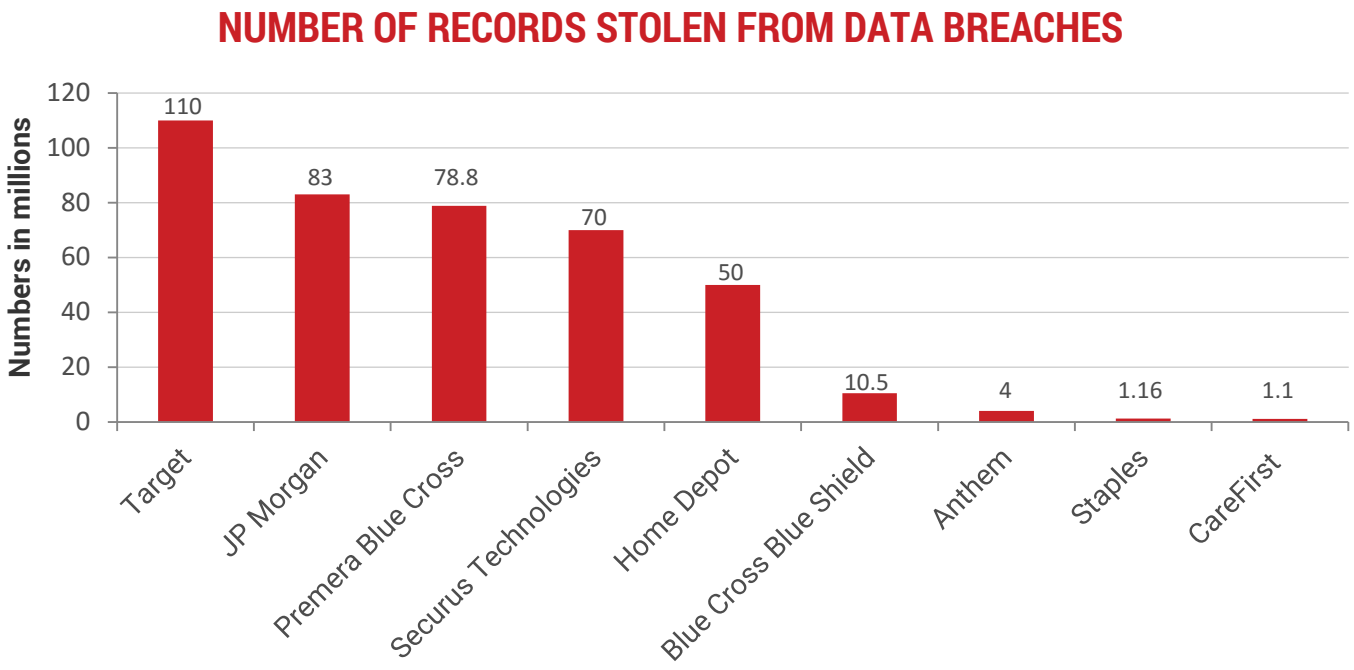
The Global State of Information Security Survey 2015 conducted by PricewaterhouseCoopers (PwC) indicates that the number of detected information security incidents rose 66% per year since 2009. The survey of 2014 reported that the total number of security incidents has increased to 42.8 million around the world, which is 48% higher compared to incidents in 2013.

From the **20 biggest breaches**, on average, each one affected about **35 million people**.

What should be learned from companies that have been hacked?

The research analyzed 20 biggest data breaches during 2014-2015 with the aim of detecting what companies are doing wrong and what needs to be done to deal with these issues. Among the hacked companies were companies that offer information security services as well. These companies certainly had powerful technical controls over the information such as firewalls, antivirus and similar safeguards, which apparently were not enough.

However, technology alone will not safeguard your data. Companies have to look every aspect of the operation including all controls in order to establish a proper information security. Within the ISO/IEC 27001 framework, training and technical practices are among the suggested activities to look at closely (check the "selected list of controls" in Annex A). From these data breaches, millions of people were affected by losing personal information such as names, addresses, dates of birth, phone numbers, social security numbers, payment card numbers, internal emails, and other personal information. The chart below shows which companies have had the highest number of data loss.



Something very valuable revealed from this survey is the fact that none of these companies were certified against ISO/IEC 27001 at the time of the data breaches. They either were not implementing the ISO/IEC 27001 Information Security Management System, or were not implementing it properly.

Thus, the question of how these breaches can be avoided or at least reduced if Information Security Management System (ISO/IEC 27001) was implemented within organizations arises. The answer is that it can improve information security systems, quality assurance, increase security awareness among employees, customers, vendors, prevent violations caused, etc. It provides a framework for IT security implementation and can also assist in determining the status of information security and the degree of compliance with security policies, directives and standards.

In addition to this, ISO/IEC 27001 Annex A has 114 controls that help organizations to keep information assets secure, even though not all of them are related to technology, but indirectly, all of them are related to information security. Experts recommend a multi-layered approach to information security, suggesting the following steps, which can be pegged to the associated ISO/IEC 27001 controls.

Taking into consideration that some attacks have begun with phishing e-mails sent to employees, an organization wishing to comply with ISO/IEC 27001 shall at least:

1. Identify the skills required to ensure the proper functioning of the ISMS.
2. Implement a training program for personnel performing work affecting the ISMS.
3. Implement an awareness program on information security appropriate to different stakeholders.
4. Implement a communication program to inform stakeholders of the ISMS about changes that may affect them.
5. Evaluate the effectiveness of actions taken and keep records.

> Independent third-party certification enables companies to validate that all **ISO/IEC 27001** requirements are being implemented.

Some clauses of ISO/IEC 27001 are presented below that can help towards the above mentioned issues:

ISO/IEC 27001, clause 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 to the information security management system requirements.

An organization should consider awareness of stakeholders as main objective to reinforce or modify their behavior and attitudes, and encourage them to adhere to the values of the organization. The awareness messages must be focused on the use and user behavior.

ISO/IEC 27001, clause 7.2 Competence – Determine the necessary competence of person(s) doing work under their control that affects their information security performance; ensure that these persons are competent on the basis of appropriate education, training, or experience.

ISO/IEC 27001, clause 7.4 Communication – The organization shall determine the need for internal and external communications relevant to the information security management system including on what to communicate, when to communicate, etc.

In this matter, an organization should ensure appropriate involvement of personnel whose competence is being developed, as part of the training process, and may result in personnel feeling a greater sense of ownership of the process, resulting in their assuming more responsibility for ensuring their success.

Data Storage Management

ISO/IEC 27001, clause 7.5.3 Control of documented information – (Protection, Distribution, Storage, Retention and Disposal)

Documented Information is the information required to be controlled and maintained by an organization and the medium on which it is contained. It can be in any format and media and from any source such as paper, magnetic, electronic or optical computer disc, photograph, master sample, etc.

ISO/IEC 27001, control A.11.1.2 Physical entry controls – Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Secure areas provide controls that protect against unauthorized physical access, damage and interference to the premises, equipment and information, e.g. dedicated computer rooms and data centers. There are a number of considerations in implementing adequate security over nominated areas.

Network security management

ISO/IEC 27001, control A.13.1.1 Network controls – Networks shall be managed and controlled to protect information in systems and applications.

Controls should be implemented to ensure the security of information on networks and the protection of connected services from unauthorized access. In particular, the following items should be considered:

- Responsibilities and procedures for the management of networking equipment should be established;
- Appropriate logging and monitoring should be applied to enable recording and detecting actions that may affect, or are relevant to information technology;
- Systems on the network should be authenticated;
- Systems connection to the network should be restricted.

For more information, check ISO/IEC 27002 and ISO/IEC 27033.

Information transfer

ISO/IEC 27001, control A.13.2.2 Agreements on information transfer – Agreements shall address the secure transfer of business information between the organization and external parties.

To maintain the security of information transferred within an organization and with any external entity, formal transfer policies, procedures, and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

Some of the analyzed companies have implemented the requirements of ISO 27001, but without an independent third-party certification. This fact makes it impossible to determine how well they comply to the ISO/IEC 27001 requirements. Obtaining a certification by an independent third-party registrar like PECB, serves as a proof for stakeholders and clients that all the requirements and controls are being implemented correctly.

ISO/IEC 27001 Certification

The ISO 2014 Survey of Management System Standard Certifications specifies that the information security standard experienced a 7 % growth of companies being certified against ISO/IEC 27001 in 2014. In 2013, 22,349 companies were certified against ISO/IEC 27001, and this number increased for 1,623 additional companies in 2014. However, it is important to point out that UK has the most important growth, reducing the cyber-security incidents.

This implies that companies should pay more attention and get certified with ISO/IEC 27001 in order for them to reduce and/or eliminate data breaches resulting in millions of lost records and affected stakeholders.

The information security standard experienced a **7 %** growth of companies being certified against **ISO/IEC 27001** in **2014**.

About PECB

As a global provider of training, examination, audit, and certification services, PECB offers a wide range of services which inspire best practices for implementing, managing and auditing information security management system and supportive controls and practices. Among others, PECB offers certification services for various standards including but not limited to ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27032, ISO/IEC 27034, ISO/IEC 27035, ISO/IEC 20000, etc.

PECB is highly committed to provide its clients comprehensive evaluation and certification services that inspire trust and benefit society as a whole. We develop training based on best practices to provide protection for your organization. Until now, there are more than **5,000** individuals worldwide certified by PECB against ISO/IEC 27001 schemes alone. Our aim to help society embrace best industry standards that improves performance and reduces damages is gradually being accomplished.

For more information, visit PECB's ISO/IEC 27001 Certification of Individuals, and ISO/IEC 27001 Audit and Certification for Organizations.

Join the family of more than **5,000** professionals certified with PECB's **ISO/IEC 27001** schemes, and don't be part of the list.

+1-844-426-7322

customer@pecb.com

Help Center

www.pecb.com