PECB

When Recognition Matters

EQUIFAX HACKING

POSSIBLY ONE OF THE WORST CYBERATTACKS IN HISTORY

UP TO 143 MILLION PERSONAL DATA HACKED

On Thursday, September 7, Equifax, one of the three major credit reporting agencies stated that hackers had breached and gained access to the company's data, and more precisely, have potentially hacked personal information of up to 143 million American customers. According to Equifax, the probably largest data breach in the United States took place between mid-May and July. Specifically, hackers gained access to names, addresses, birth dates, social security numbers, or even driver license numbers. Equifax emphasized that not only American customers' data have been subject to the cyberattack; this attack affected the UK and Canadian residents' personal information as well.

Such cyberattack represents one of the largest breaches of personal information in the recent years, and it is also the third attack reported by Equifax since 2005. Pamela Dixon, the executive director of the World Privacy Forum said that "This is about as bad as it gets. If you have a credit report, chances are you may be in this breach. Chances are much better than 50 %," she added.

Referring to Equifax's investigation and security specialists, cyber criminals accessed certain documents in the organization's system from mid-May to July by exploiting a feeble point in site programming. The agency said that it identified the intrusion on July 29, and since then, it has not detected proofs of unauthorized access on their customers' data or business credit reporting databases. The CEO of Equifax, Richard Smith, said that "This is clearly a disappointing event for our company and one that strikes at the heart of who we are and what we do." One of the first shattering consequences of this attack was that the Equifax's shares fell 19 percent in the market trading, after the immediate reaction of the investors on the possible data exposure of almost half of the United States population.

A major response to this attack came also from the US Senator Mark Warner, who is also the Vice chairman of the Senate Select Committee on Intelligence, who stated that "exaggeration to suggest that a breach such as this represents a real threat to the economic security of Americans."

If we look at another major cyberattack, such as the one that Yahoo encountered in 2016, in which occasion they confirmed that more than one billion (yes, billion), accounts were compromised, it eclipses the Equifax in numbers and size; however, the Equifax breach is worse in terms of severity and disastrous impact that it can cause. What makes this attack particularly concerning, is the type of personal data that were accessed without authorization, such as consumer's medical histories, employee accounts, bank accounts and much more.

This is why organizations ought to consider the implementation of ISO/IEC 27001 security controls and follow the standard's framework to ensure the protection of their organizations from attacks such as the one that took place in a large company, such as Equifax. The proper security awareness programs for employees, including training and education of the personnel, patch management, and regular backup system are the instruments that improve the organization's response to potential cyber-threats.. Controls incorporated in ISO/IEC 27001 standard, equip us with the most recent and most advanced anti-malware protection strategies which ensure that we have a legitimate and working security structure in our organizations.

PECB provides training and certification services for ISO/IEC 27032 Lead Manager. For more information, please visit: https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27032

Author: Ardian Berisha