

Information Security: about Its Mechanism and Significance

Alan Xu

Oct. 20, 2024

When the information was written on paper, people started to have the need to keep the information secure. With civilization improving, information security is a more and more important subject. The main theories on this subject have been applied in the army, government, and manufacturing industry not only in a subclass of computer science.

So now, a question arises, why the information security so significant for us? How does information security protection works and why should people protect their information safety?

Before we talk about the topic, let's see some main ideas on information security. The core theory of information security consists of three parts of information system: Communication, Software and Hardware, and three main portions: Confidentiality, Integrity and Availability. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." [1][2]. By ensuring these three levels' security and three portions, your computer can make sure that your data is correct and never been changed by any destroyers.

After understanding its main theories, another question comes: How these things react with each other to prevent our data from attacking? Let's see some threats the information security faces first. Information security threats come in many different forms.[3] Here are many common threats: software attacks, theft of intellectual property, theft of identity, theft of equipment or information and information extortions.[4] These attack methods can influence the confidentiality, integrity or availability. For example, Trojan horse is a normal attack of software attacks. "Trojan horse is any malware that misleads users of this true intent by disguising itself as a standard program." [5] It can destroy any system or network resources and make some service can not being accessed. This situation can affect the availability. To Trojan horse, an effective cybersecurity software is front line of protection. It should run fast,

frequent scans and tell the user that Trojan virus is detected. This approach is by protect software safety to defend availability. Just like this instance show, only ensure that any part of information system, the information security can be guaranteed.

Now, we have known how information security protection mechanism, let's discuss the significance and some cases. With the development of information tech, the way information is delivered becomes more complex so that it is more and more hard to ensure the information safety. The necessity on information protection service increases rapidly. This is because it can protect all categories of data or information from theft and damage.[6] Also, if a person or an organization is lack of information security. It may lead to losing or stealing key information, creating a poor customer experience and reputational harm. Here are some cases where lack of attention to information security led to serious consequences: Between 2013 and 2014, Yahoo experienced several significant data breaches, this results in the theft of information from over 3 billion user accounts. This event affects that the sale of the company to Verizon and the decrease in investor confidence.[7] Also in 2011, Sony's PlayStation Network was subjected to a massive attack. The hackers gained access to person information of 77 million users, including the credit card details. This attack led to outage of the service in several weeks and forced Sony to bear substantial compensation costs and a decline in consumer trust.[8] Last but not least, in 2013, the well-known design and creative software company experienced a massive cyberattack, the hackers breached Adobe's servers, stealing approximately 153 million user accounts' information. This event led to that Adobe faced significant legal liabilities and expenses and the users; trust diminished.

In conclude, a strong and effective information security mechanisms are essential for a safeguarding system and ensuring data confidentiality, integrity and availability. The necessity for robust information protection services has grown fast with the advancements in

technology, as the complexity of data delivery increase. If lack of pro information security, it can lead to serious consequences.

Reference:

1. Cherdantseva Y. and Hilton J.: "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals". In: *Organizational, Legal, and Technological Dimensions of Information System Administrator*. Almeida F., Portela, I. (eds.). IGI Global Publishing. (2013)
2. [Committee on National Security Systems](#): National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.
3. Rahim, Noor H. (March 2006). *Human Rights and Internal Security in Malaysia: Rhetoric and Reality*. Defense Technical Information Center.
4. Kramer, David (September 14, 2018). ["Nuclear theft and sabotage threats remain high, report warns"](#). *Physics Today* (9): 30951.
5. Wikimedia Foudation(2024, October 4). *Trojan horse(computing)*. Wikipedia
[http://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](http://en.wikipedia.org/wiki/Trojan_horse_(computing))
6. Tunggal, A. T.(n.d.) *Why is cybersecurity important? Upguard*. RSS.
<http://www.upguard.com/blog/cybersecurity-important>
7. Periroth, N. (2017, October 3). *All 3 billion Yahoo accounts were affected by 2013 attack*. The New York Times. <https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3->

[billion-users .html](#)

8. Team, S. (2024, September 26). Sony Data Breach: What happened and how to prevent it.

<https://www.strongdm.com/what-is/sony-data-breach>