Data Security and Policy Assurance

James Grey

**Data Security and Policy Assurance**

The electronic computers that progressed from small experimental initiatives in 1940s, became real-world data processors in the 1980s. They have become an integral part to store and process data in our everyday life but the concern about security and protection of valuable data has risen (Robling Denning, 1982). When computers became accessible to everyone and malwares started to effect computers. After viruses were discovered, programmers often generated to send a joke or to check programming capabilities. But soon it became a real concern when government operated computer systems were hacked, and confidential information started to leak.

Data security is the study of approaches to protect data stored in computer and communication systems from unauthorized disclosure and modification. Since 1975, data security has advanced rapidly. Data security provides a predefined set of technologies and standards which tend to shield data from accidental or intended damage, exposure, or modification. Data security can be applied in numerous ways to protect the data. They include a variety of methods and techniques like physical security, logical and administrative controls, structural standards, and more practices that stop unknown and unauthorized individual or processes to access the sensitive information.

Cryptography is used as a method for data security which involves the algorithm derived from mathematical concepts to convert the sensitive data to a code. In this way instead of raw data, the coded information is transmitted, and the chances of data theft are reduced significantly.

There has been considerable advancement in methods of cryptography which includes key safeguarding schemes, Data Encryption Standard (DES), digital signature, key distribution protocols, and public-key encryption. There are also algorithms developed to validate the programs to ensure that no confidential information is leaked, and level of security clearance is suitable. New and advanced controls are established to keep data in statistical databases safe, as recently several methods to attack and damage this data have appeared. A better understanding of hypothetical and practical drawbacks of current security is developed (Robling Denning, 1982).

The information technology departments of many great mainframe computing companies of 1960s and 1970s created security approached which were applicable and effective in their era nut now they now gone outdated for two major reasons. One of the reasons, is that the number of dedicated users has increased significantly. The applications developed are user friendly so that everyone can use them conveniently. Among large number of users, many are not aware of the potential threats to their systems. Even those who know about these threats, are not capable to deal with them. The other factor, that has made the initial efforts to protect data ineffective, is development of Networked remote-access system. the devices are being interconnected for various communication purposes. Also, the number of people using the internet has increased significantly. Due to which the person operating a mainframe may not know one device is accessible to a huge number of users throughout the world. It has become important to comprehend risks and actions required (Pfleeger & Pfleeger, 2002).

Another method of data security is to implement steganography. In steganography, the important data is hidden with other data in such a way that unimportant bits in a computer file are replaced with invisible data. In this way, the hacker will not be able to extract the valuable data. It is a simple process however, it has some downsides regrading maintenance of security, extraction, strength, and capacity to embed data. Moon & Raut proposed technique where the image and audio are embedded as confidential data into the arbitrarily selected frames of video through multi frame using the modification direction (MFEMD) algorithm. This makes it hard to interpret which video part hides the data. A forensic tool for verification is implemented at the receiving end which enhances the data security. To improve the extraction and efficiency of the method, multiple attacks were applied during the transmission of video, including histogram, visual, chi-square etc. (Moon & Raut, 2018).

Big data is a recent technology which deals with large structured or unstructured data and methods to process and analyze the data sets which cannot be processed with traditional computer systems. The importance of big data is now appreciated by tech companies, industries and government. The effective mining of Big Data provides viable benefits in various sectors like medical, social, economic and research etc. Usually it is observed that the aim of Big Data Security is to monitor data in real-time so that it can perceive liabilities, risks, and anomalous actions, casual access based on role, and showing indicators based on security level (Fatima-Zahra Benjelloun & Ayoub Ait Lahcen, n.d.).

 Information technology has greatly influenced the public sectors including finance and business. And hence the significance of data security is inevitable too. This becomes more significant when a disaster hits an area. The damage caused to assess also include loss of data at computing systems. It can be physical loss of data or at such vulnerable times, the hackers attack to steal data. It greatly effects the data security and business of numerous. For such incidents business continuity plans are prepared and implemented. These also includes plan to avoid security breaches during a catastrophe as there is huge need to address the issues of integrity and confidentiality of data. It is often noted that the major threat to business continuity is unavailability of services like bank’s payment gateway goes out of order. This disrupts the transaction process. In some situations, after the damages from disaster effect the banking system. Therefore, bank is not able to proceed with transactions due to data unavailability or administrative issues. This results in financial loss to the bank and dissatisfaction of clients. Apart from mismanagement, in certain cases the personal and confidential data is exposed. For this reason, there are cautionary measures to avoid the loss of data. The data can be transferred to a secure location and be recovered in better conditions. It is arguable that Data security is a significant part of Business Continuity Plans for any organization. It sets parameters of authorized access to systems and information during disaster and recovery period. It also defines the measures which are essential to stop intrusions. There are many cases where a company gets access to data center of its competitor and uses its information to drive it out of business. It is also very crucial for a company to implement BCP to protect the data of its customers. For a bank which does not protect data of its customer efficiently can face loss of millions through identity theft and hacking. Moreover, if bank does not have enough means to secure integrity of data and utilizes services of a third party for this purpose, the government can take strict action against it.

It is well-known fact that baking sector is perfect and easiest target for data theft and hacking. According to a survey conducted in 2016, it is stated that every year there is an average of 85 serious breach attempts on banks and 36% of them were successful in their aim. In response to this, the companies and industries are developing methods to have more control over cyberspace. One of the data threats is attack of malware. One of the malware types is Ransomware which operates in two ways. It either encodes data or it steals it. In order to release the data, the cybercriminal asks for money. It all happens in cyberspace hence it is more difficult to catch the criminal. This problems not only involves security of a single company but also has consequences on national and international levels (Wilner et al., 2019).

One of the highlighted examples of such attack was ransomware attack on the City of Atlanta in March 2018. Due to this attack, the computer systems operated by government, city services, courts, parking services and other utilities were greatly affected. Many offices were compelled to complete the essential tasks manually as computer were out of services for 5 consecutive days. The attackers asked for $52,000 as ransom amount. After paying ransom and gaining control, the total cost spent to recover fully was $17 million. Out of which $3 million were paid to crisis management forms and emergency IT Consultants. After the regain of control, the complete recovery took several months. This incident revealed that the city of Atlanta was not prepared for this. An audit two month before this attack had revealed cyber-vulnerabilities ranging from 1,500 to 2,000. The reason was use of outdated softwares and IT applications through undocumented processes. This example became a significant lesson and reason to include Cybersecurity in BCPs of any organization (Blinder & Perlroth, 2018)

 A rapid increase in cybercrimes in the past few years have enhanced the need to integrate data security measures in risk management systems and plans. Also, many companies have made teams of business continuity and disaster management as integral part of their companies. Backup solution might not be able to stop the loss of data but will provide means to recover the data quickly.

**References**

Blinder, A., & Perlroth, N. (2018, March 27). A Cyberattack Hobbles Atlanta, and Security Experts Shudder. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

Fatima-Zahra Benjelloun, & Ayoub Ait Lahcen. (n.d.). Big Data Security: Challenges, Recommendations and Solutions. *IGI Global*. Retrieved from https://www.researchgate.net/profile/Ayoub\_Ait\_Lahcen/publication/278962714\_Big\_Data\_Security\_Challenges\_Recommendations\_and\_Solutions/links/577bfc8808ae213761cab725.pdf

Moon, S. K., & Raut, R. D. (2018). Information security model using data embedding technique for enhancing perceptibility and robustness. *International Journal of Electronic Security and Digital Forensics*, *11*(1), 70–95. https://doi.org/10.1504/IJESDF.2019.096528

Pfleeger, C. P., & Pfleeger, S. L. (2002). *Security in Computing* (3rd ed.). Prentice Hall Professional Technical Reference.

Robling Denning, D. E. (1982). *Cryptography and Data Security*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

Wilner, A., Jeffery, A., Lalor, J., Matthews, K., Robinson, K., Rosolska, A., & Yorgoro, C. (2019). On the social science of ransomware: Technology, security, and society. *Comparative Strategy*, *38*(4), 347–370. https://doi.org/10.1080/01495933.2019.1633187