RESEARCH ARTICLE OPEN ACCESS

Data Protection in the Era of Digital Innovation

Rakesh .A[1], Prasad C N[2]
1(BCA Department, St. Joseph's Evening College, Bengaluru 560025)

Abstract:

Digital Technology and Digitized Information is recorded in recorded in binary code of combination of the digits 0 and 1, also called bits, which represents words and image. Digital technology includes all types of electronic equipment and applications that use information in the form of numeric codes. The key area on the data management and data protection, which is the process of automating the movement of critical data to online and offline storage, and information lifecycle management, comprehensive strategy for valuing, cataloguing and information assets from application and users errors.

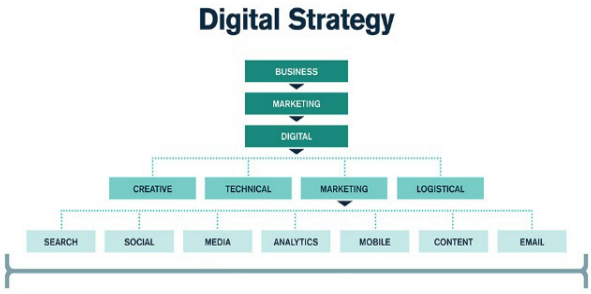
Keywords — **Digitization, Data Security, Cyber Security, Data protection and Cloud Data Security.**

I. INTRODUCTION

Digital technology is a base two process. Digitized [1] information is recorded in binary code of combination of the digits 0 and 1's, also called bits, which represents words and images. Digital technology includes all types of electronic and application that use code that can be represented by stings of only two numeric characters. These characters are usually 0 and 1's. Devices that process and use digital information include personal computers. Calculators, automobiles, satellites and high-definition television sets. A key area on the data management and DATA PROTECTION IN THE ERA INNOVATION [2], which is the process of automating and movement of critical data to online storage, and information life cycle management, a comprehensive strategy for valuing, cataloguing and information assets from applications and users errors.

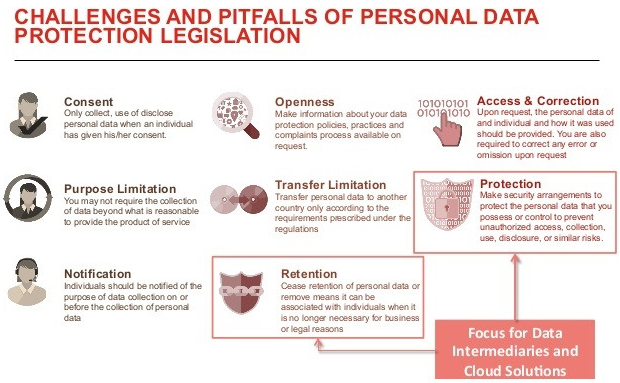
Most of the information people is analogue in nature that is, it varies constantly, and an infinite number of values can be assigned to the information. For example, the brightness of a light bulb dimmed gradually from on the off could be considered analogue information. This infinite number of brightness can divided again and again, until, there are thousands of ranges of values, each of which can be presented by a numerical value.

Once analogue information has been quantized into digital information, it is impossible to perfectly reverse the process and re-create all of the possible analogue signals from the corresponding digital signals. This way most analogy signals are represented by a great number of digital information on analogue information so that a speaker can convert it into sound waves. Some Devices process digital information using a tiny computer called microprocessor. It performs calculations on digital information and then makes decisions based on the results. In Such devices, computer chips called memory chips store digital information, is used to control the sequence of operations in many devices that use digital technology. A sample of strategy is show in with the below sample diagram example:



Data Protection in the Digital Age:

As enterprise network organizations implement new computer hardware services, they are faced with the issue of what to do with issue of what to do with their Older IT assets. Proper disposal and destruction of electronic data storage devices is important compliant to laws and legislations [3] around storing and disposing of personal data and personal identification information. A data breach has many consequences – financial loss, reputational damage and also legal repercussions.



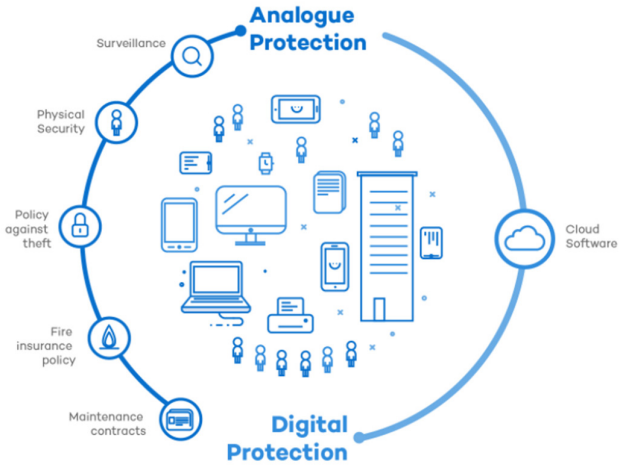
Online Predators and Digital Security

In a report on the cost of Cyber Crime, the Ponemon [4] institute also says that as more sensitive and confidential information and transactions move onto the cloud, the number of online attacks continue to increase. In the same report it is shown that currently there are average of 138 successful cyber-attacks per week in the USA [5], a number that has risen significantly over the past five years. That large companies with massive IT security infrastructures are becoming victims highlights the sophistication of the attacks as well as the danger for business of all types.

There are however some steps that small business can take that won't require a huge capital investment.

- Encrypt employee smart phones so that data is secure if phones are lost or stolen.
- Regularly update software to ensure security holes are patched.
- Limit access to the network resources and network services with sensitive information.
- Deploy, install and configure Anti-Malware software agents on all computers and block access to risky sites network firewall level.

Cyber-Security:



Policies to protect both digital and paper documents.

Paper remains a core component of office life, and as such, there are still plenty of printers, photocopies, servers, external hard drives and similar devices in every office. What people of often fail to realize is that the devices used to copy, scan and store documents contain hard drivers that store the confidential information passing through. Nearly every digital copier built since 2002 contains hard drive – just like the one on your personal computer – That stores an image of every document. Additionally, according to IT consultants, 80 percent of the corporate laptops and desktops contains sensitive information on their hard drive. Despite, this little is paid to what happens to these devices, an in turn the confidential information stored on them, is rarely taken devices are often stockpiled instead of being destroyed.

There are three simple workplace guidelines need to remember designed to safeguard hard drives:

- Perform a regular cleaning of storage facilities and avoid stockpiling unused hard drives.
- Destroy all unused hard drives using a third party provider who has a secure chain of custody and confirms destructions, to help give you peace of mind and ensure your data is being out of hands of fraudsters.
- Regularly review your organizations information security policy to incorporate new emerging form of electronic media.

More than ever, business need to consider their data security as a whole and have a plan in place that will ensure their client's data is safe. Neglecting to take the proper precautions today sets up business to be tomorrow's victims.

Legal than ever, business need to consider to consider their data Security as a whole and have a plan in place that will ensure their and their client's data is safe. Neglecting to take the proper precautions today sets up business to be tomorrow's victims.

II. Legal Impact of Data Protection and Management in the Digital Age

Organizations should be aware of the prevailing legal regulations that govern ever growing popular technology solutions such as cloud storage, collection, analysis, and offshore storage of customer data.

Below are few tips for organizations to ensure that they comply with legal regulations where they operate in.

- **Have a clear understanding of how personal data is used and managed in your organization:** In some instances, data storage and protection is managed on behalf of an organization by an outsourced service provider. Organization need to understand the level of data protection provided by the outsourced service provider and ascertain whether regulations, including, sector specific ones, permit offshoring or cross-border data sharing. There appears to be growing trend of data localization which means organizations are not permitted to transfer any such of data overseas.

- Conduct regular audits and penetration testing – The authorities do recognize the fact that cyber criminals often use sophisticated measures in their attacks. However, as seen with many data breaches around the world, it is most often the case that the organization itself has failed to have sufficient security measures in place. It is also known fact that many organizations need to meet the regulatory standards for data protection and compliance.

III. Cloud Security Enabling Innovation in the Digital Age

Cloud Computing has been one of the key innovations that is changing the landscape of technology and driving digital transformation across all industries. Lower costs of ownership, improved business agility, innovation and enhanced customer experience are some of the main reasons why cloud, whether private, public or hybrid, has attracted such a crowd.

Digital transformation is about changing the business models and about business taking advantage of huge opportunities created by the technologies that are disrupting society. Increasingly more business are developing or moving their workloads to the cloud and this transition has enabled them to deliver competitive advantage to their end user.

IV. Security at the Outset

Security is the critical design component at the starting point of a project, so that when you spin up new systems, security controls, are already in place. With the Speed of the cloud and the amount of automation used, business can't rely on manual intervention. Before, security used to sit in a dark

corner of IT Department and only called upon when there was a breach or an audit to respond to it. Digital Transformation provided an opportunity for security systems to collaborate across different functions – these must be fully exposed to the requirements of the business process owners.

Changing threat landscape – attackers targeting the application layer

Understanding your security responsibilities in the cloud based environment and employing security tools that allow you to continuously monitor and maintain secure configurations and patching are critical to protecting your company's assets from application – layer attacks.

With the application workloads in the cloud, business need to be mindful of the risks and have visibility in their cloud stack for all systems, especially those that are exposed or hold sensitive data.

The Impact of a breach data

A breach is a much a security issues, a business one. When a web application is compromised, several different scenarios cloud play out. Customers data could be stolen, confidential information regarding the company or employees cloud be leaked, the availability of web application could be impacted, and with any of these scenarios a business is likely to have a deal with the post-breach activities and bear costs in investigate, remediation, legal, publicity and regulatory actions to name a few.

This, however requires the company's leaders to take ownership of understanding the risk and attack surface of their workloads and business-critical web applications, and ensure that they identify high- risk areas to address before the attackers get there first.

V. CONCLUSIONS

Data Protection involves the toughest challenges in today's era of today's IT world. With a lot of technological advancements involved and implemented, data protection still involves a lot of mechanisms that which should be expanded and various level in the cloud technology platform.

The maintenance of an individual or organization's data from abuse are under close scrutiny and in order to avoid breaches of the Act it is suggested that every organization take the following action:

- Establish whether you should 'notify' [6] the commissioner of your data processing.
- Audit all manual filing systems and automated records, including personnel files, to check compliance with the principles.
- Audit the activities involving personal data; is it being processed and for what purposes?
- Audit the occasions on which personal data is collected and from whom.

Effects of data security breach on various levels with different corporations face a common entity of breach levels which is majorly causing a threat to the enterprise networks.

ACKNOWLEDGMENT

This research was supported by Technology Manager **Syeda Nasheerunia**, ANZ Technology services, Bengaluru, India and **Mamtha Basvaraju**, SAP Technical Architect. I also thank my technology associates who provided insight and expertise that greatly assisted the research.

Thank you very much, everyone.

References

[1] *SAP News, "news.sap.com," SAP, May 2017. [Online]. Available: https://news.sap.com/digitization-vs-digitalization-wordplay-or-world-view/.*

[2] *i-Scoop Corporation, "i-scoope.eu," i-SCOOP, 2016-2020. [Online]. Available: https://www.i-scoop.eu/digitization-digitalization-digital-transformation-disruption/.*

[3] *crown, "legislation.uk," crown, [Online]. Available: https://www.legislation.gov.uk/ukpga/1998/29/contents.*

[4] *Ponemon Institute, "ponemon org," Ponemon Institute , [Online]. Available: https://www.ponemon.org/library.*

[5] *"securityweek," Wired Business Media, 2017. [Online]. Available: http://www.securityweek.com/cost-cyber-attacks-jumps-us-firms-study.*

[6] *BCS, "BCS.ORG," The Charted Institute of IT, 2017. [Online]. Available: http://www.bcs.org/content/ConWebDoc/2751.*