Cybersecurity Concerns for E Services in the Digital Information Age

– **Subodh Kesharwani**
Associate Professor, SOMS, IGNOU, New Delhi
https://orcid.org/0000-0001-8565-1571 skesharwani@ignou.ac.in

– **Jyoti**
Research Scholar, SOMS, IGNOU, New Delhi
https://orcid.org/0000-0002-1945-3005 jyotiningania@gmail.com

– **Shailza**
Research Scholar, SOMS, IGNOU, New Delhi
https://orcid.org/0000-0001-5414-2467 shailza509@gmail.com

Article History
Paper Nomenclature:
Argument Based Credential (ABC)
Paper Code: CYBNMV1N5OCT2019ABC2
Submission Online: 03-Oct-2019
Manuscript Acknowledged: 05-Oct-2019
Originality Check: 11-Oct-2019
Originality Test Ratio: 0%
Peer Reviewers Comment: 11-Oct-2019
Blind Reviewers Remarks: 15-Oct-2019
Author Revert: 20-Oct-2019
Camera-Ready-Copy: 25-Oct-2019
Editorial Board Citation: 28-Oct-2019
Published Online First: 31-Dec-2019

With the emergence of technological era security risks has become the one of the most problematic elements of cybersecurity when it comes to the services being delivered online. As the new technologies emerge and existing technology is used in new or different ways, new avenues of attack are developed. Without proper security measures in place, organisations are at risk of losing their customers' data and revenue. Cybersecurity is continually being by hackers which leads to the distortion of sensitive information which surely calls for organisations for risk management and changing cybersecurity.

Keywords : Cybersecurity | AI | IoT

Introduction:

E services refers to the services which are delivered through the use of information and communication technologies (ICTs). The main components of E services are considered as service provider, service receiver and the service delivery channel. For example, in case of public E services, public agencies and corporations providing services becomes the service provider, citizens utilizing and availing the services becomes the service receiver and the medium through which services are delivered from the service providers to the service receiver is the technology. As a famous phrase says every coin has two sides, same is applicable for the technology. With its huge advantages such as delivering of services online medium technology has got disadvantages as well, due to which privacy which is considered to be a major concern to the users of any industry and is being compromised continuously with the prompt rise in cyberattacks, which are usually aimed at assessing, changing, misusing and distorting sensitive information of users, extorting their money and thus interrupting the functioning of a normal business process. The consequences of cyberattacks are huge, these are continually growing in sophistication with attackers using an ever-expanding variety of tactics, which negatively results in distorting organisations reputation and image, loss of sensitive information and data , identity theft and extortion attempts. Cybercrime has become a big business and increasing at rapid speed. According to a study conducted by Brominum, in 2018, the cybercrime economy was estimated to be worth $1.5 trillion. To protect the sensitive information of users, organisations, systems, programs and networks from these digitals attacks demands the cybersecurity. Cybersecurity helps in preventing the breach of data and sensitive information, identity theft, ransomware helps in aiding risk management. It protects the internet-connected system including software, hardware, and data and integrity of the assets connected belonging to an organisation's network. It protects the computer

systems from any unauthorised access or being otherwise damaged that can result in huge damage or loss to the system being compromised. Implementing proper cybersecurity measures can help organisations to protect data assets from attacks that if placed in wrong hands can cause serious damage to the organizations or individuals and lead to losses in terms of reputation, money, theft of data, deletion of data and fraud. The costs of cyber security breaches are rising it can cost organizations billions of pounds. Impacted organisations stand to lose sensitive data, and face fines and reputational damage. Cybersecurity has never been an easy task as with the technological disruptions, as there are more devices than people attackers are being innovative. In recent years, due to the rapid increase of attacks and its substantial impact to the organisation cyber security has fallen under media scrutiny. Every organisation must implement appropriate security measures to protect Cyber security is a critical business issue for every organisation and to implement cyber security measures demands more focus and dedication.

Why is cyber security important For E services?

To ensure the smooth flow of e services it is very much required by the organisations to take preventive measures against the prospect cyberthreats due to the following reasons:

- Cybersecurity will prevent any unauthorized access to the digital assets of the organisations
- It will protect the sensitive information, data and networks
- It will protect organisations against the major cyber threats such as malware, ransomware, phishing and social engineering
- It will ensure the protection of the end users and their personally identifiable information (PII)
- If implemented well it will boost the confidence of the organization and build image in the eyes of customers.

Pillars of cybersecurity:

Robust cybersecurity addresses people, processes and technology. Aligning these three pillars will provide businesses with a more secure defence as discussed below:

Three pillars of cybersecurity

1. People: Human errors can be devastating for organisations, human errors itself provides for more than 90% of cyberattacks. Therefore, to safeguards the organizations form cyberattacks the first and foremost requirement is to educate its people or employees about cybersecurity. For this they should be provided with proper trainings and guidance to enhance their understanding of how to keep themselves and the data and system they have access to protected from the cyberattacks. Every employee needs to be aware of their role in preventing cyber threats and must comply with the basics of data security by choosing strong passwords, being cautious of data backup or any attachment in email etc.

2. Process: Cyber threats are constantly evolving, so the processes need to be regularly reviewed. Organisations must have a static framework to deal with the prospect cyber threats and a stringent process clearly defining organisation's activities, roles and documentation must be followed to mitigate them. Associated risks and threats of organisations can be identified by using proper methods and must be updated with the pace of changes in the cyber threats.

3. Technology: Majority of the devices that we use these days are found to be Internet of Thing (IOT) & Artificial intelligence (AI) enabled. This in a way allows our personal data and habits to be passed back and forth on the servers on the internet. This calls for the strong preventive actions from the organisations. Three main entities including endpoint devices, cloud & networks and routers must be protected by installing technology driven essential security tools such as anti-virus software, firewalls, DNS Filtering, malware protection, email security solutions etc.

Conclusion

Among the various kind of e services the issues of security have raised the much attention as any breach of it leads distortion to the company's reputation, confidence and general confidentiality among its customers. Protecting the privacy of confidential information is quickly becoming a measure of success in the business world. Therefore, to increase the trust of the customers and users with the working of the organisations requires the proper implementation of cybersecurity frameworks.

References:

- Dubey, P. G. (2016). E-Commerce-Study of Privacy, Trust and Security from Consumer's Perspective. *International Journal of Computer Science and Mobile Computing , 5* (6), 224-232.
- Kazeem, K. D. (2015). E-Service Security: Taking Proactive Measures to Guide against Theft, Case Study of Developing Countries. *International Journal for e-Learning Security , 5* (2), 454-461.
- https://economictimes.indiatimes.com/definition/cyber-security
- https://www.happiestminds.com/services/cyber-security/
- https://www.mmrit.com/news/security/three-pillars-of-cyber-attack-and-defence/
- https://www.dnvgl.com/article/the-three-pillar-approach-to-cyber-security-starts-with-people-134252
- https://digitalstrategy.ie/security-issues-in-e-commerce/

Dr. Subodh Kesharwani is an academician with a bronze medal in his post graduate and Doctorate in ERP System in 2002 from Allahabad University. He is one of the researchers who had concentrated his research on Total Cost of Ownership [TCO] & Critically evaluate ERP vendors including SAP. Dr.Kesharwani is presently an Associate Professor, School of Management Studies with a total 20 years of hardcore teaching and research in Information System and its linkages with various domains of management at Indira Gandhi National Open University, New Delhi

skesharwani@ignou.ac.in

Miss Jyoti is currently pursuing her Doctoral Research study from SOMS (IGNOU), New Delhi. She has done her B.Com (H) and M.com from University of Delhi and qualified UGC- NET JRF. She has been a part of various Seminars, Paper Presentations, Faculty Development Programme and National and International Conferences. She is an enthusiastic learner who believes in maintaining and maximizing the quality of life by implementing her skills, and experience gained through education, hard work and dedication

jyotiningania@gmail.com

Miss Shailza is a Research Scholar at SOMS (IGNOU), New Delhi. She has done her B.Com (H) from Vivekananda College and M.Com from Delhi School of Economics, University of Delhi and qualified UGC- NET JRF. She has been a part of various Seminars, Paper Presentations, Faculty Development Programme and National and International Conferences. She is a hardcore believer to work on her own initiative and also as a part of team. She excels in her analytical skills with a global outlook and foresightedness which is the need of hour.

shailza509@gmail.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
11-Oct-2019	D61548454 (urkund)	1819	10723

Urkund Analysis Result

Analysed Document: Modified CYBERSECURITY CONCERNS FOR E SERVICES IN THE DIGITAL INFORMATION AGE.docx (D61548454)
Submitted: 10-10-2019 4:37:00 PM
Submitted By: skesharwani@ignou.ac.in
Significance: 0 %

Sources included in the report:

Instances where selected sources appear: 0

Note: Cybernomics runs an Urkund plagiarism tool for the originality check of an article before publication. Urkund is developed by Prio Infocenter AB based in Stockholm, Sweden.

Reviewers Comment

Reviewer Comment 1: The article is well structured and it has well aligned the E services provisions to the cyber threats.

Reviewer Comment 2: The article focuses on the needs to take precautionary measures again the cyber-attacks that can lead to the huge financial as well as non -financial damage to the organisations and its related people.

Reviewer Comment 3: With the digital transformation everyone seems to be fascinated by and engaged in using services online that were traditionally being done manually, in this context , it becomes very important to educate the users about the prospect threats and consequences of cybersecurity and its threats.

Editorial Excerpt

At the initial time of submission (TOS) the paper had 20% plagiarism, which on the later stages had been reduced to the 0%, which is an acceptable percentage for the publication. The article has been modified by the authors (Subodh, Jyoti & Shailza) with the preliminary stage remarks and minor revision as suggested by the editorial board and blind reviewers at the successive stages as and when required to do so. The comments related to this manuscript are noteworthy and related to the "**Concerns of Cybersecurity and E services in Digital Information Age**" both subject-wise and research wise. The authors have crafted the paper in a well-structured manner. Due to the digital transformation there has been huge change in the medium of services being delivered this has also given rise to the prospects of cyber threats that necessitates the implementation of proper cybersecurity measures by various organisations. The article provides an overview of threats and security issues in delivering of services over internet. All the comments had been shared at variety of dates by the authors in calculation. By and large all the editorial board and reviewers' suggestions had been incorporated in the article and the manuscript had been earmarked and finalised to be published under "**Argument Based Credentials**" Category.

Scholastic Seed Inc.
www.scholasticseed.in

Citation
Subodh Kesharwani, Jyoti and Shailza
"Cybersecurity Concerns for
E Services in the Digital Information Age"
Volume-1, Issue-5, Oct 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had
no conflict neither financially nor academically.