Collaborative Discussion 1: The 4th Industrial Revolution

Discussion Topic

- Read the Schwab (2016) article from the World Economic Forum and discuss the impact of industry 4.0 on the sector in which you are involved or interested.

Instructions

- Identify a specific incident (not covered in your reading list) where the failure of an information system has had a significant impact.
- Your post could consider a range of impacts of the failure, including: the implications to customers, the economic cost, the reputational cost, or any other relevant impacts.
- Review lecturecast 1 and read papers provided in the references list.
- Go to the discussion forum and create an initial post of your contribution to the discussion.
- You should demonstrate that you understand the topic covered and ensure you use references to academic literature (journals, books, reports, etc.).

Learning Outcomes

- Understand the applicability and challenges associated with different datasets for the use of machine learning algorithms.
- Systematically develop and implement the skills required to be an effective member of a development team in a virtual professional environment, adopting real-life perspectives on team roles and organisation.

Initial Post

by Anastasia Rizzo - Tuesday, 9 May 2023, 6:22 PM

Number of replies: 3

The ongoing digitalization of numerous industries, as highlighted in the World Economic Forum's Future of Jobs report, represents a significant advancement. However, this paradigm shift requires employees to acquire new competencies, adopt a new work ethic, and conscientiously study data security on a daily basis (Schwab, 2017).

If these processes are not handled with the utmost care and precision, the resulting failure of an information system can have disastrous consequences for both its users and the organisation that depends on it. Such failures can be triggered by a range of factors, including hardware or software malfunctions, human errors, cyber attacks, or even natural disasters.

The medical industry has seen instances of information system failures with significant impact. One example is the data breach of Anthem Inc., a major health insurance company in the United States. In 2015, the company disclosed that cyber attackers had gained access to the personal information of approximately 80 million customers, including sensitive data such as names, birthdates, social security numbers, and medical identification numbers (Pierson, 2017).

This breach had severe implications for customers, leaving their personal information vulnerable to identity theft and other malicious activities. Anthem incurred significant economic costs, spending millions of dollars on investigation, remediation, and legal fees. Additionally, the company's reputation suffered as customers and the general public lost confidence in its ability to protect their data (Pierson, 2017).

The breach also had broader ramifications for the healthcare industry. It exposed the vulnerability of healthcare organisations to cyber attacks and emphasised the need for robust cybersecurity measures to safeguard patient information. The breach prompted regulatory authorities to issue new guidelines for protecting patient data and increased scrutiny of security practices across the industry (Pierson, 2017).

Another example of an information system failure in the medical industry resulting from natural disaster is Hurricane Katrina in 2005. The storm caused extensive destruction to healthcare facilities, including hospitals and clinics, in the affected regions. Most of these facilities relied on electronic health record systems to manage patient data. However, the storm caused power outages and flooding, which destroyed or damaged the equipment necessary to access and utilise these systems (Rodríguez & Aguirre, 2006).

This led to healthcare providers being unable to access crucial patient information, resulting in delays and disruptions in care delivery. Patients had to be transferred to other facilities outside of the affected areas, putting additional strain on the healthcare system. The economic cost of the destruction was assessed to be in the billions of dollars, and the reputational cost to the healthcare providers unable to provide timely and effective care was substantial (Cerise, 2010).

This case highlights the importance of disaster preparation and backup systems for critical healthcare infrastructure, including information systems (Cerise, 2010).

As demonstrated by these examples, information system failures can have significant consequences, including financial costs, reputational damage, and legal repercussions. It is therefore essential for organisations to prioritise the establishment of robust cybersecurity strategies and backup systems to prevent or mitigate the impact of such incidents. By investing in these measures, organisations can ensure the integrity and security of their systems and data while safeguarding the trust and confidence of their stakeholders.

References:

Cerise, F. (2010) Hurricane Katrina and the Health System: Lessons Learned. Disaster Medicine and Public Health Preparedness, 4(S1), S12-S14.

Pierson, B., (2017) Anthem to pay record $115 million to settle U.S. lawsuits over data breach. Available from: https://www.reuters.com/article/us-anthem-cyber-settlement-idUSKBN19E2ML [Accessed 8 May 2023].

Rodríguez, H. & Aguirre, B.E. (2006) Hurricane Katrina and the healthcare infrastructure: A focus on disaster preparedness, response, and resiliency. Front Health Serv Manage, 23(1):13-23, discussion 25-30.

Schwab, K. (2017) The Fourth Industrial Revolution. New York: Crown Business.

The European Space Agency, (2023) Swarn. ESA's magnetic field mission. Available from: https://www.esa.int/Applications/Observing_the_Earth/FutureEO/Swarm [Accessed 8 May 2023].

Peer Response:

by Piotr Sieminski - Thursday, 11 May 2023, 6:49 PM

Hi Anastasia,

I am curious about the Hurricane Katrina. It seems that the hurricane destroyed the hardware necessary to access the data, was not there any other possibility, like even using a laptop? Nowadays most of the data sits on the cloud so usually it is a matter of having VPN access rights and the data can be accessed from any device. Was that not the case for them?

Peer Response:

by Dominic Lambert - Thursday, 11 May 2023, 8:07 PM

Anastasia,

I'm with Piotr on this - I suspect you may have misread the article that you cited from Rodrigez et al. (2006). It say "The aftermath of Hurricane Katrina provides a window of opportunity to address a frail and failing healthcare system." this would indicate that the system was failing prior to the hurricane not because of it.

In fact the article goes on to say, that it allowed for better planning for the hospitals. Furthermore, it makes no reference to IT systems, and the likelihood is that the term infrastructure is more applicable to public services, highways and what would be termed as national infrastructure.

Whilst I agree with your statements regarding the importance of disaster recovery planning and your quote from Cerise. F (2010) I would consider that the substantive cost was not wholly in relation to IT costs but more likely to be that of the actual facilities. See also BBC-Bitesize website for the list of significant costs (IT isn't on it) - at Case study: Hurricane Katrina, 2005 - Extreme weather - CCEA - GCSE Geography Revision - CCEA - BBC Bitesize.

It is noted by Voice Of America (VOA) in October 30, 2009 that one of the biggest issues was the not just the loss of buildings and facilities but also the inability to communicate that caused some of the biggest challenges.

In truth though, Hurricane Katrina and later Irma (2017) were both probable improbabilities.... in that it is known that a catastrophic even will eventually occur but the size and scale was not fully anticipated and therefore insufficient preparations were made to cope with it. It is widely acknowledged that there isn't a single answer to ensure that people, property and services are in a state of preparedness though, Zolnikov (2018).

Lastly - to disagree with Piotr, most patient data is not hosted on cloud platforms... and certainly wasn't in 2005 when hurricane Katrina hit. Devadass et al in 2017 indicated that cloud computing has gained attention gradually... and this was twelve years after Katrina. In addition, VPN's need the base communications network to utilise... With the phone lines, mobile towers and other infrastructure components destroyed having data in cloud wouldn't have helped immediate care - but it would have helped when links were restored.

References

Cerise, F. (2010) Hurricane Katrina and the Health System: Lessons Learned. Disaster Medicine and Public Health Preparedness, 4(S1), S12-S14.

Devadass, L., Sekaran, S.S. and Thinakaran, R., 2017. Cloud computing in healthcare. International Journal of Students' Research in Technology & Management, 5(1), pp.25-31. [online] Available at: ijsrtm.2017.516-pg-25-3120191229-95916-1xgoyey-libre.pdf (d1wqtxts1xzle7.cloudfront.net) Accessed: May 11, 2023

VOA. (2009, October 30). Hurricane Katrina: Plans, decisions and lessons learned. Voice of America (VOA News). https://www.voanews.com/a/a-13-2005-09-16-voa63-67541507/285971.html Accessed May 11, 2023.

Zolnikov, T. R. (2018). A humanitarian crisis: Lessons learned from hurricane Irma. American Journal of Public Health, 108(1), 27–28. [online] Available at: https://ajph.aphapublications.org/doi/full/10.2105/AJPH.2017.304192 Accessed May 11, 2023.