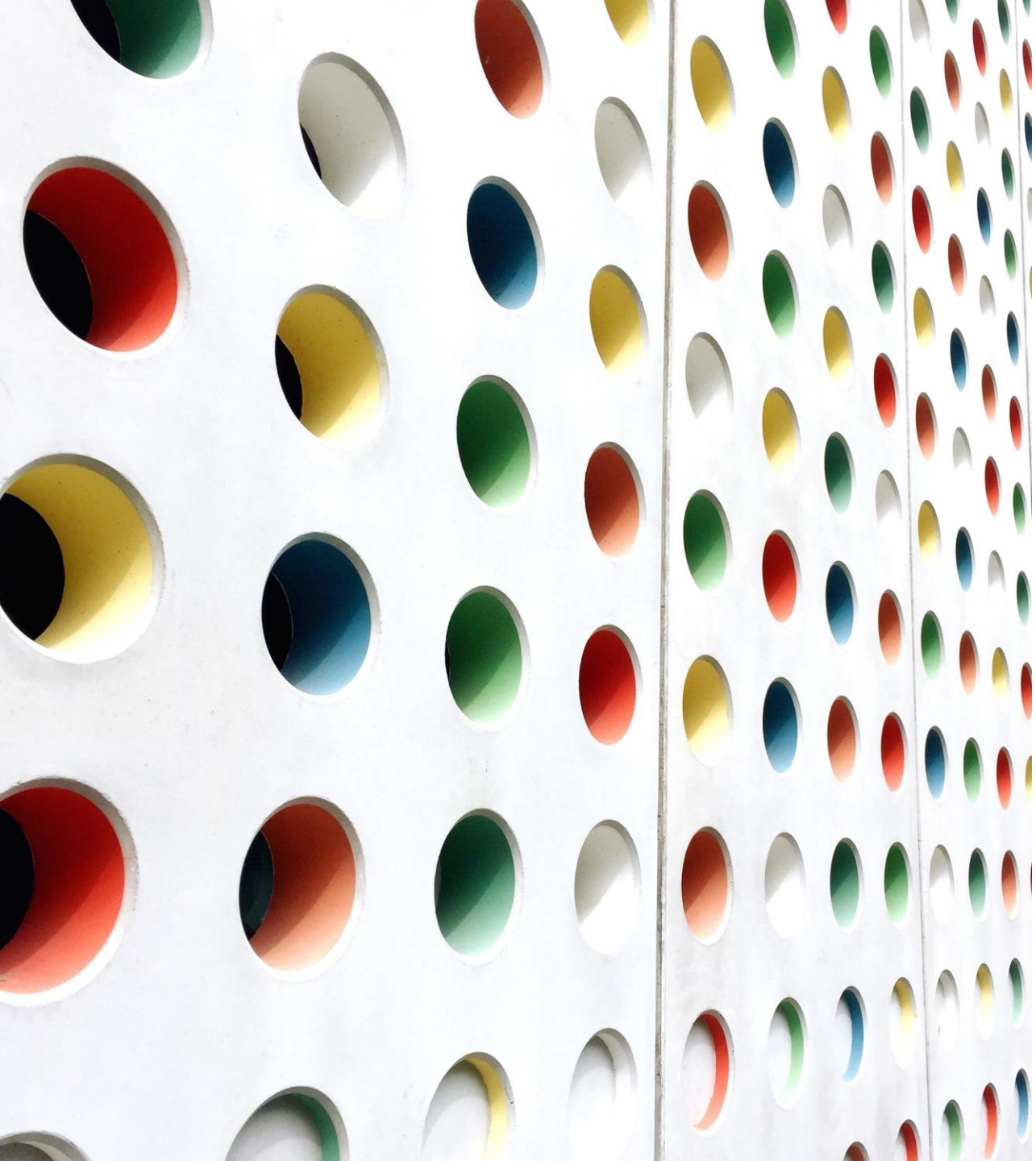

Peer Discussion & Reflections:

NEELAM PIRBHAI-JETHA

Unit 1: Introduction to Information System
&
Unit 2: Information Systems and their importance

Initial Post:

Failures of information systems are quite “unavoidable” (Goldfinch, 2008: 918). During my readings, two incidents retained my attention. The first one was from the sports retailer Reebok, which found itself offering free pairs of trainers worth £100. Customers were charged only delivery fees. Reebok apologised to its clients, cancelled the orders, refunded the postage and gave them a 20% discount (Smithers, 27 November 2013). While this incident annoyed the customers, caused a few forgettable criticisms towards Reebok, and could have caused a loss of profits and other internal crises, other IT errors can be more life-threatening.

In 2015, for instance, about 50 million customers could not reach the emergency line ‘911’ for some hours (Knutson, 17 July 2015). The same incident was recorded over the years and even in 2020, the line was not reachable for a few hours (Hollister, 29 September 2020). We can imagine the fatal impacts of such a failure, and the number of lives that could not be saved.

I guess that most services must be using an ERP system, “which is an application with a centralized database that can be used to run a company’s entire business” (Bourgeois, 2014: 11). But very little information is given on the sources of the failures mentioned above. According to me, there must have been issues in the maintenance phase of the system development lifecycle (Buckley, 2021), or a bug that was not taken care of. It must, however, be mentioned that “IT investments are expensive and of high risk” (Bartis & Mitev, 2008), and even with maximum effort or security systems, there are many unidentified factors that can lead to bugs and system failures. The question we ask ourselves is who should shoulder the responsibilities of any system failures?

References:

Bartis, E. & Mitev, N. (2008) “A multiple narrative approach to information systems failure: a successful system that failed”. *Eur J Inf Syst* **17:**112–124. Available from: https://doi.org/10.1057/ejis.2008.3 [Accessed 14 August 2021]

Bourgeois, D. (2014) *Information Systems for Business and Beyond.* Saylor Academy.

Buckley, O. (2021) Unit 1: Introduction to Information Systems, Lecture Notes, Object-oriented Information Systems OOIS_PCOM7E, University of Essex Online, delivered August 2021.

Goldfinch, S. (2007) Pessimism, Computer Failure, and Information Systems Development in the Public Sector. *Public Administration Review*. Available from: https://www.researchgate.net/profile/Shaun-Goldfinch/publication/286533228_Dangerous_enthusiasms_and_information_systems_development_in_the_public_sector/links/5b4934a4aca272c6093f71a7/Dangerous-enthusiasms-and-information-systems-development-in-the-public-sector.pdf [Accessed 14 August 2021]

Hollister S. (September 29, 2020) 911 outages have become a fact of life — are we even fixing this? *The Verge*. Available from: https://www.theverge.com/2020/9/29/21494652/911-outage-centurylink-lumen-intrado [Accessed 14 August 2021]

Knutson, R. (July 17, 2015) FCC Cracking Down on 911 Service Failures. *The Wall Street Journal*. Available from: https://www.wsj.com/articles/fcc-cracking-down-on-911-service-failures-1437173901 [Accessed 14 August 2021]

Smithers, R. (November 27, 2013) “Reebok runs into trouble over mistaken free trainers offer”**.** *The Guardian*. Available from: https://www.theguardian.com/money/2013/nov/27/reebok-free-trainers-offer [Accessed 14 August 2021]

Classmates mentioned=Michael Botha, Aidan Curley, Ian Wolloff, Grace Clarke, Thien Liu

Summary Post

In this post, I will try to sum up the *Initial Posts* and *Peer Responses* of my classmates on the class forum. During the first three weeks, the causes and consequences of information systems' failures were discussed. Some potential solutions were also put forward.

Causes of IS failures:

Even if they are sometimes "unavoidable" (Goldfinch, 2008: 918), failures of information systems (IS) can be caused by technical issues, human errors and by hacking or malevolent people especially if there are security flaws in the systems. As Michael Botha puts it in one of the class's posts, "most failures are the culmination of multiple smaller ones" and from "a lack of IT governance". Aidan Curley mentions that errors in the software and the lack of quality control by the testing procedures implemented by the software development team can cause IS failures. For Ian Wolloff, the Human factor can bring failures, especially if the IS system is poorly designed, set up, implemented and managed.

Consequences of failures:

IT failures are not without consequences and can even be life-threatening such as unavailability of emergency lines (Neelam Pirbhai-Jetha) and death of patients when healthcare systems fail (Ian Wolloff). Grace Clarke explained the financial costs of system breakdown. Most classmates mentioned the economic/financial loss and the reputational loss for the company in case of IS failures. Questions of security and safety of data were also raised.

Solutions:

According to Ian Wolloff, companies must have effective system monitoring, maintenance procedures and action plans in case of IS failures. Michael Botha suggested the setting up of:

i) an Information System Governance which will oversee all the rules and elements of an IS system

ii) an Incident Management System to take care of any issues immediately after the failure.

iii) a Business Continuity Plan (BCP) to "ensure that operations can be maintained even with the loss of the system, thereby preventing a huge loss in revenue or clientele" (Nieles et al., 2017; Bourgeois, 2014).

iv) a disaster Recovery Plan to quickly restore the damaged IS system (Nieles et al., 2017).

Thien Liu also suggested having a "back-up system". Deep learning and machine learning applications can also become the solution to predict and protect against failures such as deletion of data.

For Aidan Curley, one solution to reduce hacking, "phishing, tailgating, spear-phishing, etc" is by offering regular employee training and education.

On a final note, according to Michael Botha, in order to have a proper IS system, "security techniques and best practices must be applied within all aspects of the information system's life cycle" (Brookshear & Brylow, 2018). He adds that the IT governance should shoulder the responsibilities of any system failures.