

A Review of Some Negative Effect of Information Systems and Their Proposed Solutions

Fredrick Boafo^{1*}

¹ Computer Science, Lancaster University Ghana, Accra, Ghana

Email Address

f.boafo@lancaster.edu.gh (Fredrick Boafo)

*Correspondence: f.boafo@lancaster.edu.gh

Received: 22 July 2023; **Accepted:** 15 August 2023; **Published:** 31 August 2023

Abstract:

Information technologies have clearly revolutionized the way we work and communicate and have become a crucial part of our daily life. Numerous advantages are provided by them, such as increased operational effectiveness, cost savings, better decision-making, and greater customer service. However, it is crucial to understand that frequent use of information systems, such as computers and mobile phones, can result in a few health problems, ethical issues, job loss, cost, addiction to IS usage amongst others. These issues are frequently the result of bad ergonomics, spending too much time in front of the screen, and not taking breaks. This paper therefore examines and review some few negative repercussions of IS and even how we can eradicate them based on literature.

Keywords:

Information Systems, Artificial Intelligence, Automation, Ergonomics, Computerized Systems, Operational Effectiveness, Ethics

1. Introduction

Information systems have become inseparable from our day-to-day life. Most workplaces use information systems to work. Information systems is the interrelationship between components to help in business and activities in terms of hardware components and software component, database, procedure people and telecommunications [1]. Sociotechnical views are also expressed as the use of social and technological systems to create, maintain services and produce goods [2]. Information systems have transformed how organizations run and how people use technology. These systems' introduction has expedited procedures, boosted productivity, and created several advantages. The growing use of information systems has brought about numerous advantages, but it has also resulted in job displacement, when individuals are at risk of losing their jobs as a result of automation and other technical improvements. We can all agree that the development of information systems has fundamentally changed how we work, live, and engage with the world. Our reliance on information systems has grown significantly, from the ease of online

shopping to the seamless sharing of information across great distances. To be sure, there are advantages and disadvantages to any technological advancement.

Numerous facets of our lives have changed due to technology. We now access information, communicate with others, and carry out tasks that were once difficult and time-consuming thanks to smartphones, laptops, and other devices. With chatbots, virtual assistants, and sophisticated algorithms that guide our decisions on everything from what products to buy to what jobs to apply for, AI is also becoming more and more pervasive in our daily lives. There is no doubt that technology and AI have many benefits. They can help us save time, increase productivity, and make more informed decisions. For example, in healthcare, IS is being used to help diagnose diseases and develop new treatments. In finance, IS is being used to analyze market data and make investment decisions. In transportation, IS is being used to improve safety and efficiency on our roads and in the skies. However, there are also risks associated with over-reliance on technology and AI.

The paper therefore seek to review few critical effects of IS and educate us on how we can remedy, mitigate or curtail them.

2. Results and Discussion

2.1. Some Negative Effects of IS and their Solution

2.1.1. Over reliance on IS Issues

One of the most significant risks of IS is that it can make us lazy and complacent, leading to a decline in cognitive abilities [3]. According to Perez B. P. [3], our need to think critically and creatively can be diminished by an overreliance on technology and AI, which is one of the main ways in which this can make us lazy. We are less likely to actively think through issues and solve problems when we rely on technology to do so. Instead, we learn to receive information passively and rely on technology to give us the solutions we require. Weakening our capacity for memory and information retention is another way that an overreliance on technology and AI can make us lazy. Information is less likely to be committed to memory when it is stored and retrieved using technology.

Simms A. S. [4], states that to prevent people from becoming overly dependent on artificial intelligence (AI) and to maintain a healthy balance between human input and AI-driven decision-making, managers and leaders can take several measures. They can establish clear parameters and expectations. They must specify the duties that humans, IS and AI systems have within the organization. They must establish precise guidelines for when and how they should be used, and effectively convey these expectations. Managers must give people the freedom to balance IS and AI recommendations with their own insights while encouraging them to take responsibility for their work and decisions.

Moreso, they should encourage human-AI cooperation; stress the value of collaborating with computerized IS rather than relying solely on it or on human intelligence. Supervisors must encourage the notion that emerging technologies are tools to supplement rather than take the place of human capabilities. Hence, they must encourage people to collaborate with IS systems, combining their data processing prowess with human intuition as a strength. More thorough and reliable decision-making processes may result from this collaboration.

Managers must also educate and train employees on AI and IS, provide training courses and other materials to help them better understand technologies and their drawbacks. So that they can more accurately interpret and assess the outputs, teach them about the underlying concepts and algorithms used in AI systems. People can effectively contribute their own thoughts and insights to the decision-making process by understanding how AI functions. It is the responsibility of managers to create a culture of critical thinking by encouraging people to do so and highlighting the value of independent thought and analysis. This entails encouraging a culture where contesting and challenging AI-generated suggestions or judgments is welcomed. They must encourage workers to actively interact with IS, be aware of its limitations, and form well-informed opinions based on their own experience and knowledge.

2.1.2. Cost Issues

The high cost of information systems can be a disadvantage because it may limit access to the technology for individuals or organizations with limited financial resources. According to Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R., Krishnamurthy, B. [5], implementing new solutions costs time and money. Business services frequently experience interruptions as new operational stages are introduced. Additional personnel training is required, and customers can see a drop in service quality while the deployment is taking place [5]. Although the cost of information technology solutions has decreased as a result of technological advancements, businesses with stringent compliance requirements must still take care to follow all laws and regulations to avoid facing legal trouble and fines. Another instance where high cost is a disadvantage in information systems is that it can limit the ability of the organization to invest in other important ideas. If an organization invests heavily in expensive information systems, it may not have the resources to invest in other areas such as marketing, research and development, or employee training. This can result in a competitive disadvantage for the organization.

A remedy to the high cost of information systems is to explore open-source software or cloud-based solutions which can be more affordable options additionally carefully evaluating the specific needs and requirement of an organization can help ensure that the technology investment is targeted and cost effective [5]. Open-source software is typically free and can provide similar functionality to proprietary software. Open-source software is software whose source code is available to the public, allowing anyone to view, modify, and distribute it. This contrasts with proprietary software, which is owned by a specific company and does not allow for the same level of access to modification. Open-source software is often free to use and can be a cost effective alternative to proprietary software for organizations. An example is the WordPress content management system, used to create and manage websites and blogs. Cloud-based solutions can offer a more cost-effective option than traditional on-premises solutions because they require less hardware and infrastructure investment. Carefully evaluating an organizations needs can help ensure that technology investments are targeted and effective, which can help maximize the value of the investment and reduce costs.

2.1.3. Health Issues

In a review by Norman, V. T. [6], he talks on a book by Larry D. Rosen called 'iDisorder'. In the review, he points out a chapter called "Obsessively Checking in with Your Technology ... 24/7" in which the author discusses how technology,

particularly mobile devices, frequently causes compulsive behavior. He talks about how people have become attached to their devices and the issues its causes, especially psychologically, but most people do not have a choice when using technology especially when it's for their jobs.

One of the disadvantages is the health issues they bring about. Prolonged use of Information systems such as computers and phones lead to health complications with some leading to other serious problems if not treated properly. Some health issues caused by prolonged use of devices for extended periods of time according to Tucker, F. [7]. These issues include;

a. Musculoskeletal Problems: this is the feeling of numbness in ones arms, hands or back. These issues could arise as a result of your presumably inappropriate computer-using posture. You might discover that your workplace is not ergonomically designed for your body, or that your chair is uncomfortable. However, you can fix this by determining the ideal desk and chair heights so that your computer screen is at eye level or a little lower.

b. Vision problems: Devices such as computers are known for their bright lights, glare and flickering images that can cause strain on the eyes. When one spends extended time Infront of the screen without necessary breaks it can lead to issues with one's vision and can become permanent if not managed properly. But there is a way to prevent this and that is by avoiding straining your eyes, making sure to adjust the brightness on your computer screen. You should lower the brightness of your computer screen, for instance, if you are sitting in a dark environment because it will likely be too bright and strain your eyes. Your screen can be tilted to lessen glare. Keep your eyes at a comfortable distance from the screen, and do not forget to blink.

c. Headaches: Common headaches might result from either heightened muscle tension or neck pain. Headaches can also be brought on by any eye strain or vision issues. To remedy this one should attend routine eye checkups to focus on addressing any visual issues. When using a computer, try your best to keep a straight neck and take rests.

Individuals who work in front of devices for extended periods of time are at an increased risk of these health issues.

2.1.4. Security Issues

Security in relation to the topic is the safeguarding of information or data by an entity to prevent data breach or privacy breach. In today' s day that data is fed into complex systems by customers and services, it has become a priority to secure data and information. Security is an important feature of information systems, yet it may also be harmful.

In the first place, the most significant impact on individual users in terms of security comes from individual users themselves. Individual users are people who interact with and use information systems within the context of information security. Individual users are also known as end users. They are essential to the achievement of success or failure in the deployment of information security inside an organization [8]. The person who owns the data in a firm is the one who chooses which workers inside that company are permitted access to the company's data. They are generally responsible for protecting the confidentiality, integrity, and availability of information assets in accordance with established rules, standards, and procedures. Additionally, they need

to be aware of potential dangers, well-versed in appropriate protocol, and cognizant of their own tendencies in areas such as procrastination, impulsivity, and intelligence [9]. A minor misspelling or misunderstanding on the part of an employee is often the starting point for an attack on a computer system or network. Compliance with policies and procedures is very necessary if one wishes for information security measures to be effective and for the security of the whole system to be preserved. On the other hand, the results of this include data loss and leaks, both of which may result in a variety of security risks.

On the other hand, some possible solutions to the problem include performing routine maintenance and applying frequent updates to patches. Information systems can only remain secure if they are regularly maintained and updated with new patches. By some teachings of Patch Management: Definition & Best Practices [10], First, a software developer will typically push out a security patch update to all affected devices. The lack of knowledge of a vulnerability or flaw in the system before to the software's original release or a major update's rollout is a common reason of patch update delays after, a security patch is applied, it closes any vulnerabilities that were there before whiles, errors and hacker-exploitable security flaws are common; hence patches are often required [10]. Fixes and updates may shield firms from these assaults. It is possible to repair software with a patch if vulnerabilities are discovered after it has been released [11]. Doing so makes it less likely that the resources in your immediate vicinity will be exploited. Using patch management is crucial for several reasons, including preventing exploitation of your environment's assets and safeguarding your business from cybercrime [12]. Proactively updating software on a regular basis protects against the threat and impact of data loss - in terms of severity, risk, and cost. This is achieved by fixing security vulnerabilities present in the software, which can be accomplished through regular software updates and patches. While security patches are an important part of every update, the addition of new features and enhancements is another way in which updates may fortify your system's defenses [12].

Furthermore, training individual users in information systems would remedy the negative effect while creating the awareness of data and information security breach. Personnel training is an excellent way to avoid data breaches and data mismanagement in information systems. Regular and mandated data protection training may help staff remain up to speed on the newest knowledge for both digital and physical hazards, as well as how to protect themselves and the organization from data breaches [13]. Data security training should include a broad range of topics, such as data breach detection and management, record retention, bring-your-own-device regulations, email and internet usage restrictions, workstation safety, and more [13]. Training could also be adjusted based on an employee's career stage, organizational level, and the type of environment in which they work [14]. Properly trained staff are more efficient and less prone to make errors, saving money, improving safety, and increasing production. Incorporating data security training into an organization's overall employee education program ensures that courses are periodically evaluated and refreshed, and that program effectiveness is regularly monitored [14]. Regular training and professional development opportunities can also help increase employee engagement, motivation, and retention to improve the security systems by human-handled errors whiles reducing the risk at which the security of information and data is breached or stolen.

However, as well as educating users about the dangers of data leaking and training efficient working employees. Businesses and enterprises should make it their responsibility to ensure that customers understand user terms agreement and are aware of maliciousness that may cause data breach. Raising awareness is an effective method of preventing data breaches and loss. Developers must have security knowledge and experience to proactively avoid and identify access control vulnerabilities in online applications, which are a key cause of many data breach instances [15]. Security awareness education is critical in modern culture in order to handle the difficult challenges that arise in computer security and computer ethics [16]. Information security events are important challenges to contemporary enterprises, and companies think that investing in information security helps them prevent security mishaps. However, little study has been conducted on the economic effects of information security investment. According to empirical research, information security-related expenditure may minimize the likelihood of information security incidents. Top management support and workers' information security knowledge are elements that lead to information security breaches in businesses [17]. Awareness training programs are effective in boosting people's awareness of cyber hazards. Organizations are adopting and improving security awareness and training programs to guarantee that the largest risks are reduced by human aspects. A survey of the literature on security awareness and training includes a categorization system as well as a conceptual research model to give insights into the current body of knowledge in the field. Trends and analysis from the examined articles are also offered, which may help organizations improve their security awareness programs [18]. This is because data loss and security breaches can have a negative impact on a company's reputation and bottom line. They should also provide their staff with training services and conduct employee surveys to assist in the process of improving the systems that they utilize.

2.1.5. Job Issues

The introduction of automation and artificial intelligence (AI) capabilities through the use of information systems, which have replaced job activities done by human labor, has transformed numerous sectors. Increased precision and efficiency in different operations are the results of this technical progress. Traditional work positions are, however, also faced with a major threat.

Furthermore, skills mismatches are another problem. Technology is advancing quickly, and as a result, so are the abilities necessary for many employment responsibilities. Workers who lack the necessary skills to use information systems effectively run the danger of being replaced and may find it difficult to remain competitive in the employment market. Various businesses are increasingly relying on information technology, automation, and AI, which calls for expertise in digital literacy, data analysis, programming, and problem-solving. Those who lack these abilities can have trouble finding work or run the risk of going out of style. Individuals need to invest in ongoing education and skill development to keep up with the demands of the modern workforce and secure job stability and career advancement.

Businesses can provide internships and on-the-job training while educational institutions can create pertinent courses and training modules customized to the demands of the labor market. This will help close the skills gap. Together, these

parties can create possibilities for individuals, encourage a diverse and adaptable workforce, and ensure that technical breakthroughs benefit society.

Support for entrepreneurship is a remedy for automation and AI. Promoting entrepreneurship is a potent countermeasure to job displacement brought on by technical improvements. There are many ways to assist displaced workers, including providing them with funding, mentorship opportunities, and business development training. These people can use their knowledge and experience to launch their own businesses by supporting an entrepreneurial environment, which can result in innovation and new job possibilities. Through entrepreneurship, displaced workers can use their skills and knowledge to fill market gaps and meet new demands.

3. Recommendations and Conclusions

In conclusion, information systems have undoubtedly become an integral part of our daily lives, revolutionizing the way we work and communicate. They offer many benefits, including enhanced operational efficiency, cost reduction, improved decision-making, and better customer service. However, it is essential to recognize that the prolonged use of information systems, such as computers and mobile phones, can lead to various health issues. The most common health problems associated with extended device usage are musculoskeletal problems, vision issues, and headaches. These complications often result from improper ergonomics, excessive screen time, and lack of breaks. To mitigate these risks, individuals should prioritize their well-being by ensuring proper ergonomic setups, taking regular breaks, adjusting screen brightness, and maintaining a comfortable distance from the screen. Even though information systems have undeniable uses, when used unmonitored can cause more harm to the individual than good. It is therefore important to have proper work ethics when in use to maintain healthy use and reduce health issues that may arise. Hardware, software, databases, processes, and telecommunications are all interconnected in information systems. They are necessary for business and operations, with complementary assets being extra resources contributed to boost sales or competitiveness. Security, on the other hand, may have a negative impact on individual users, cost, complexity, behavioral consequences, and limits. End users are responsible for ensuring the confidentiality, integrity, and availability of information assets while interacting with and using information systems. Policy and procedural compliance are critical for successful information security measures. Data loss and leaks may occur as a consequence of security vulnerabilities. Routine maintenance and patch updates are recommended to ensure security. Patch management protects businesses against threats and ensures that resources are not misused. Patch management is critical for avoiding data loss and protecting organizations from cybercrime. Regular software upgrades and patches address security flaws, while information system training raises awareness and lowers the chance of data breaches. Employee education includes issues including data breach detection, record retention, and internet use limitations. To reduce instances, businesses could also educate consumers about user terms and maliciousness, create awareness, and engage in security awareness programs. Organizations may strengthen their security systems and decrease risks by providing training services and conducting staff surveys.

Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this article.

Acknowledgments

The author would like to acknowledge Elton. Canny, Chukwunonso, Amanda, Christine, Wright and all the FDN Cohort 2 group.

References

- [1] Zinszer, D. (2020, June 17). What Are Information Systems? — Defined and explained in 2023 - PlexTrac. PlexTrac. Available online: <https://plextrac.com/what-is-an-information-system-defined-andoutlined/> (accessed on 15 August 2023).
- [2] B. J. (n.d.). Socio-technical systems theory. Socio-technical Systems Theory | Centres and Institutes | University of Leeds. Available online: <https://business.leeds.ac.uk/research-stc/doc/sociotechnical-systems-theory>.
- [3] Perez, B.P. (2023). The Lazy Mind: The Effects of Over-reliance on Technology and AI on Creativity, Critical Thinking, and Problem-solving. Available online: <https://www.linkedin.com/pulse/020-lazy-mind-effects-over-reliance-technology-ai-creativitybala#:~:text=One%20of%20the%20main%20ways,active%20thinking%20and%20problem%2Dsolving> (accessed on 15 August 2023).
- [4] Simms, A.S. (2023). Methods for Preventing Over-Reliance on Artificial Intelligence. Available online: <https://www.linkedin.com/pulse/methods-preventing-over-reliance-artificial-alexandria> (accessed on 15 August 2023).
- [5] Malandrino, D.; Petta, A.; Scarano, V.; Serra, L.; Spinelli, R.; Krishnamurthy, B. (2013, November 4). Privacy awareness about information leakage. Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society. DOI: <https://doi.org/10.1145/2517840.2517868> (accessed on 15 August 2023).
- [6] Norman, V.T. (2015). iDisorder: Understanding Our Obsession with Technology and Overcoming Its Hold on Us. Perspectives on Science and Chrtian Faith, 67(2), 146+. Available online: <https://link.gale.com/apps/doc/A461945248/AONE?u=unilanc&sid=bookmark-AONE&xid=94cca512> (accessed on 15 August 2023).
- [7] Tucker, F. (2016, June 15). Top 10 Computer Related Health Problems - MicroHealth. MicroHealth. Available online: <https://www.facebook.com/microhealthllc>. <https://www.microhealthllc.com/top-ten-computer-related-healthprolems/> (accessed on 15 August 2023).
- [8] Huah , K. (n.d.). What factors can positively and negatively impact the implementation and use of information security? What Factors Can Positively and Negatively Impact the Implementation and Use of Information Security? | LIGS University. Available online: <https://ligsuniversity.com/blog/what-factors-can-positively-andnegatively-impact-the-implementation-and-use-of-information-security> (accessed on 20 July 2023).

- [9] The Collage of New Jersey. (n.d.). Available online: <https://security.tcnj.edu/program/security-responsibilities/third-party-systemadministrator-guidelines/> (accessed on 20 July 2023).
- [10] Patch Management Definition & Best Practices - Rapid7. (n.d.). Rapid7. Available online: <https://www.rapid7.com/fundamentals/patch-management/>
- [11] The need for regular software updates and patch management to prevent vulnerabilities - Cyber Unit. (2022, December 20). The Need for Regular Software Updates and Patch Management to Prevent Vulnerabilities - Cyber Unit. Available online: <https://www.cyberunit.com/blog/the-need-for-regular-software-updates-and-patchmanagement-to-prevent-vulnerabilities> (accessed on 20 July 2023).
- [12] How to Prevent Data Loss: 13 Simple Ways. (n.d.). How to Prevent Data Loss: 13 Simple Ways | Cypress Data Defense.
- [13] Borromeo. (2022, September 20). Training to Combat Data Breaches. Training to Combat Data Breaches. Available online: <https://trainingindustry.com/articles/it-andtechnical-training/training-to-combat-data-breaches/> (accessed on 20 July 2023).
- [14] Privacy Technical Assistance Center. (2011). Data Security and Management Training: Best Practice Considerations. Data Security and Management Training: Best Practices, 249–3072(855). Available online: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Data%20Security%20and%20Management%20Training_1.pdf (accessed on 20 July 2023).
- [15] Zhong, L. (2023, April 20). A Survey of Prevent and Detect Access Control Vulnerabilities. arXiv.org. <https://arxiv.org/abs/2304.10600v1>.
- [16] AlShormrani, & Mehdim. (2012). The importance and Dilemmas of Security in Information System.
- [17] Lee, H.; Kwon, E.; Yoo, K.; Chai, S. (2016). An impact of information security investment on information security incidents. Proceedings of the 18th Annual International Conference on Electronic Commerce E-Commerce in Smart Connected World - ICEC '16. DOI: <https://doi.org/10.1145/2971603.2971644>.
- [18] Pattabiraman, A.; Srinivasan, S.; Swaminathan, K.; Gupta, M. (n.d.). Fortifying Corporate Human Wall. Advances in Information Security, Privacy, and Ethics, 142–175. DOI: <https://doi.org/10.4018/978-1-5225-2604-9.ch006>.



© 2023 by the author(s); licensee International Technology and Science Publications (ITS), this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (<http://creativecommons.org/licenses/by/4.0/>)