Object-oriented Information Systems August 2021

Home / / My courses/ / OOIS_PCOM7E August 2021 / / Unit 1 /

/ Collaborative Discussion 1: Information System Failure / / Initial Post /

« Collaborative Discussion 1: Information System Failure

Michael Botha

Initial Post

64 days ago

9 replies

Last 55 days ago

Recently, the failure of an important information system within my work environment severely impacted daily operations (University of Essex Online, 2021). The system primarily facilitates resource management for the Telecommunications division by providing a multitude of functions and valuable information such as: site asset records, open fault tasks, billing records, and more (Bird, 2018). Records are accessed, altered, and deleted through a front-end application called WorkPlace, which many personnel in the organisation use in their daily activities (Codecademy, 2021). The WorkPlace software interacts with the relevant database which physically resides remotely, via the Structured Query Language (SQL), using the company's intranet as a connection medium (Kalman, 2003). Failure of the system inhibited the access of important information, halted the updating of records, and prevented the usual business workflows enabled by the information system (University of Essex Online, 2021).

According to reports received from key individuals, the mass storage pertaining to the Virtual Machine (VM) hosting the database failed (VMware, 2011). This raised questions regarding redundancy and failover (Swanson et el., 2010). Especially, since critical databases should contain a Redundant Array of Independent Disks (RAID) configuration (Swanson et el., 2010). Additionally, the system was originally setup with a primary and secondary server configuration, which facilitated constant updates between relevant mass storage. Performing a basic a root cause analysis (Peune College, 2020) would yield the following:

1. Direct cause (Peune College, 2020): failure of Hard Disk Drive.
2. Indirect cause (Peune College, 2020): no failover to redundant drives in RAID; no failover to redundant server system.
3. Root cause (Peune College, 2020): lack of information system security policies and procedures relating to the system; no maintenance schedule; lack of specialised training or relevant service contract.

In the interim between failure and full system restoration, various manual workflow techniques had to be reverted to. If the services lost related to a company selling their services as opposed to a division servicing an Organisation, the consequences could have been dire (University of Essex Online, 2021).

References:

Bird, K. (2018) What is Resource Management. Available from: **https://www.apm.org.uk/blog/what-is-resource-management/** [Accessed 13 August 2021].

Codecademy. (2021) Front end vs. back end: Where should you start?. Available from: **https://www.codecademy.com/resources/blog/front-end-vs-back-end/** [Accessed 13 August 2021]

Kalman, Deborah. (2003) *Encyclopedia of Information Systems*. Netherlands: Elsevier.

Peune College. (2020) *Incident Management and Root Cause Analysis: Learner Guide* [PDF Notes]. Incident Management and Root Cause Analysis One-week Course. Peune College.

Swanson, P., Bowen, P., Philips, A., Gallup, D., Lynes, D. (2010) *NIST Special Publication 800-34 rev.1: Contingency Planning for Federal Information Systems*. United States of America: National Institute of Standards and Technology. Available from: **https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf** [Accessed 14 August 2021]

University of Essex Online. (2021) *Introduction to Information Systems* [Lecturecast]. OOIS_PCOM7E AUGUST 2021 Object-oriented Information Systems. University of Essex Online

VMware. (2011) *DBA guide to Database on VMware*. Available from: **https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/solutions/dba-guide-to-databases-on-vmware-white-paper.pdf** [Accessed 14 August 2021].

Reply

Maximum rating: -

9 replies

1 Post by **Oliver Buckley**

62 days ago

Good post

Thanks for posting this Michael, there's some interesting bits in there - what do you think that most pressing issue was to cause this?

Reply

2 Reply to **Oliver Buckley** from **Michael Botha** ↑

60 days ago

Re: Good post

Hi Oli,

I believe that due to the complexity of modern Information Systems, and their various interrelated as well as interconnected parts, it would generally be hard to come by one specific cause. Additionally, most failures are the culmination of multiple smaller ones along the way. But if I was forced to select one, in this circumstance it would have to be a lack of IT governance. If the correct governance was in place one of the smaller failures along the way could have been flagged and the slow snowballing-effect prevented.

Reply

Maximum rating: -

3 Post by Neelam Pirbhai-Jetha

61 days ago

Peer Response

Hi Michael,

Thank you for sharing your personal experience. After having read your post, I wanted to learn more about the factors and implications of information systems failures, which do not occur from hacking. I googled and came across the paper of Gunawardhana & Perera (2015) (https://www.researchgate.net/publication/309902379_Classification_of_Failure_Factors_in_Information_Systems), where the author talked about hard and soft factors of these failures.

The question of 'human error' was raised, and many systems fail due to the fact that things are not done properly. And if I've read your post accurately (well it's 10.30 pm zzzzz), I think most of them could have been avoided.

Reply

4 Reply to Neelam Pirbhai-Jetha from Michael Botha ↑

60 days ago

Re: Peer Response

Hi Neelam,

ha ha 22:00 is way too late to be working for me, especially since my bedtime is somewhere around 21:00... Thank you for your comment. I agree - there is a lot of hype around hacking, which is essentially legitimate considering some of the attack statistics published by various firms (NIST, 2020). However, as you point out hacking is just one risk to consider. There are many ways that a system may fail, and organisations must not lose focus on the fundamentals of Information System security encompassed by the well-known security triad (Bourgeois, 2014). For instance, secure DevOps, redundancy, backups, policies, preventative maintenance and so on.

Yes, human error was at the core of this failure, but I read a LinkedIn article sometime back where a gentleman was debating that the blame of IT system failures should not be placed on employees. He stated that ultimately IT governance should be blamed (ISACA, 2020). Human error will exist in governance policies and procedures too, but at least with an agreed "policing-structure" systems can be protected and used to attain maximum business value (Bourgeois, 2014).

References:

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

NIST. (2020) 20 Cybersecurity Statistics Manufacturers Can't Ignore. Available from: **https://www.nist.gov/blogs/manufacturing-innovation-blog/20-cybersecurity-statistics-manufacturers-cant-ignore** [Accessed 18 August 2021].

ISACA. (2020) The Value of It Governance. Available from: **https://www.isaca.org/resources/news-and-trends/industry-news/2020/the-value-of-it-governance** [Accessed 18 August 2021].

Reply

Maximum rating: -

5 Reply to **Michael Botha** from **Neelam Pirbhai-Jetha** ↑

60 days ago

Peer Response

Hi Michael,

Thanks for your comments and for sharing the links. I'll definitely read the articles.

Best wishes,

Neelam

Reply

6 Post by **Ian Wolloff**

61 days ago

Re: Initial Post

Hi Michael an interesting read especially the bit about the root cause of the outage being down to a storage failure. While we know any device with physical components such as Hard Drives will fail. BlackBlaze one of the cloud storage providers even does an annual report on failure Rates (**https://www.backblaze.com/blog/backblaze-hard-drive-stats-q2-2020/**) between drives. This can and should and should be accounted for in an organisations Disaster Recovery (DR) and Business Continuity Planning (BCP) Plan.

Also being how the solution was based on a VMware technology stack meant that VMware technology such as VMware High Availability (HA) and VMware Vmotion that enable migration of a live VM to a new host could also have been used to mitigate some of the risk of a failure causing an outage. The Human factor also appears to be at play here with the design setup and configuration of the system not matching the actual business requirements for High availability 24/7 operation.

these technical white papers from VMware explain how the technology that would have been available in this case could have mitigated some of the impact but technology is no replacement for having effective system monitoring and maintenance procedures and a plan that has been tested that can be put into action in the event of a problem.

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmw-server-wp-bestpractices-white-paper.pdf (Anon)

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-vmotion-performance-vsphere5.pdf (Anon)

VMware ® High Availability (VMware HA): Deployment Best Practices VMware ® vSphere ^{TM} 4.1. [Accessed 17 August 2021a].

VMware vSphere ® vMotion ® Architecture, Performance and Best Practices in VMware vSphere ® 5. [Accessed 17 August 2021b].

Reply

7

Post by **Michael Botha**

60 days ago

Re: Initial Post

Hi Ian,

Thanks for the holistic response. Successful Risk Management indeed requires the use of various mitigation strategies such as technical, administrative, and physical controls (Nieles, 2017). It is wise to have a risk framework and risk assessment performed on organisational information systems to ensure the Disaster Recovery and Business Continuity Plan are effective (Nieles, 2017).

References:

Nieles, M., Dempsey, Kelly., Pillitteri, V. (2017) *An Introduction to Information Security*. Revision 1. United States of America: National Institute of Standards and Technology. Available from:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf [Accessed 21 July 2021]

Reply

Maximum rating: -

8 Post by Ian Wolloff

59 days ago

Peer Response

Good Discussion While sat here ironically dealing with my own post upgrade IT systems failure from the examples we have all provided there does not appear to be one absolute cause of system failures they mostly seem to stem from a cascade of failures both technological factors and human factors but I think from the example we have we can split the failures into a couple of categories.

Hardware Failure Simplest of the reasons of a system failure the underlying hardware that supports the Information system either is not up to the tasks being demanded of it (Capacity Planning) good paper on that subject [https://www.oocities.org/mtarrani/PredictingComputingCapacity.pdf] (Shallahamer) or planning for hardware component failure has not taken place during the development and implementation phase of the life cycle. Also, this one that the easiest to plan for during a system implementation.

Software Error Bugs or Issues that were not picked up during the development of the system that leads to the failure of the system while no software is perfect having unit testing & stress testing as a core part of the development process can overcome a lot of these issues or at least that is the conventional wisdom until I started reading around the subject in the paper On the Relation Between Unit Testing and Code Quality (Gren and Antinyan, 2017) They Find **“if files have 100% or 0% unit test coverage, the differences in defects between these two groups only showed a small effect. The effect size was as low as 2.9%, therefore, the assumed causal relationship between unit tests and code quality is dubious”**

And Finally End user error or what used to be described in less enlighten times as a PEBKAC (Problem Exists Between Keyboard and Chair) error which can be unfair as a lot of times these errors are a result of users of the system having inadequate training and guidance on how to use the system which could have been overcome with a proper induction and user training plan.

Ian

References

Gren, L. and Antinyan, V. (2017). *On the Relation Between Unit Testing and Code Quality*. In: August 2017. [Online]. Available at: doi:10.1109/SEAA.2017.36.

Shallahamer, C. A. *PREDICTING COMPUTING SYSTEM CAPACITY AND THROUGHPUT*.

Reply

9

Post by Michael Botha

55 days ago

Summary Post

Thank you all for the interesting discussion. In summary, one can state that the reason for an information system ultimately failing is due to any of the core facets of such experiencing issues, namely: hardware, software, data, processes, and people (Bourgeois, 2014). Additionally, smaller isolated failures in any one of these components may not cause the whole system to fail, but typically multiple issues across the various components culminate in a holistic failure, and the inability for the system to be used as required (Bourgeois, 2014). Furthermore, the source of a failure may occur in any one or multiple of the phases within the life cycle of an information system (Bourgeois, 2014). For instance: a bad design may not account for certain extreme conditions; during implementation the system installation may not have been performed correctly; or when the system was in use various elements were not maintained as they should have been (Bourgeois, 2014).

In order to prevent a failure, a pre-emptive risk assessment must be done on the system to locate potential threats and hazards, thereafter relevant mitigating controls put in place (Nieles et al., 2017). Furthermore, security techniques and best practices must be applied within all aspects of the information system's life cycle (Brookshear & Brylow, 2018). Consequently, information system governance is a key factor, as it will specify the overarching rules pertaining to the various elements within the system (ISACA, 2020).

Incident management is of critical importance in the event of a failure arising (Nieles et al., 2017). To limit the impact of a systemic failure a Business Continuity Plan (BCP) must be in place, which will 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). Furthermore, a disaster recovery plan is required to facilitate the restoration of a system which is vastly damaged within the shortest amount of time (Nieles et al., 2017).

References:

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

Brookshear, J., Brylow, D (2018) *Computer Science: An Overview*. 13th ed. London: Pearson.

ISACA. (2020) The Value of It Governance. Available from: **https://www.isaca.org/resources/news-and-trends/industry-news/2020/the-value-of-it-governance** [Accessed 18 August 2021].

Nieles, M., Dempsey, Kelly., Pillitteri, V. (2017) *An Introduction to Information Security*. Revision 1. United States of America: National Institute of Standards and Technology. Available from: **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf** [Accessed 21 July 2021]

Reply

Maximum rating: -

Add your reply

Your subject

Type your post

Choose Files No file chosen

Submit

Use advanced editor and additional options

Older discussion

Initial Post

Newer discussion

Summary Post