

# Collaborative Discussion Initial Post – IS Failure

OOIS\_ x

Object\_ x

File Fi\_ x

ER Dis\_ x

using\_ x

Norm\_ x

Third\_ x

Kids V\_ x

(13) V\_ x

Wome\_ x

some\_ x

Docu\_ x

ERD: l\_ x

+

my-course.co.uk/mod/hsuforum/discuss.php?id=255257

Apps Properties Mamz... UnionBank Login New Tab

Reading List

University of Essex

Online

My Modules

Kikelomo Obayemi

OOIS\_PCOM7E May 2021

Participants

Grades

Module Home

Tutor Office

Deadline Details

Seminars

Module Resources

e-Portfolio

Codio

eBook


Unit 1

Unit 2

Unit 3

Unit 4

## « Collaborative Discussion 1: Information System Failure



Kikelomo Obayemi

Initial Post

71 days ago

8 replies

Last 45 days ago

### Case Study: The Irish Elections, June 2004

The Irish government, in 2004, launched an electronic voting system which was envisaged to make voting results easier to compute and eliminate the traditional paper and pencil approach. The e-voting system was planned for use in local and European elections and was believed at the time that it will improve the overall voting experience of European citizens (Melia & Byrne, 2012). A pilot test of the e-voting system was conducted in three constituencies during the 2002 elections and the Irish government seemed pleased with the outcome despite public opposition and a few problems (Collins, 2009).

However, an Independent Electoral commission advised against the use of this system for the 2004 elections as its accuracy and security could not be verified (Zelic & Stahl, N.D). It turned out that the expensive voting machines were flawed in the sense that they could not produce printouts for vote results to be double-checked (Melia & Byrne, 2012). Hackers also demonstrated how easy it was to re-program the machine to enable stealing of votes (Smyth, 2006). This debacle led to the Irish government abandoning its e-voting agenda and reverting to the old manual paper system just 5 days to the June 2004 elections (Zelic & Stahl, N.D).

OOIS\_ x

Object\_ x

File Fi\_ x

ER Dis\_ x

using\_ x

Norm\_ x

Third\_ x

Kids V\_ x

(13) V\_ x

Wome\_ x

some\_ x

Docu\_ x

ERD: l\_ x

+

my-course.co.uk/mod/hsuforum/discuss.php?id=255257

Apps Properties Mamz... UnionBank Login New Tab

Reading List

University of Essex

Online

My Modules

Kikelomo Obayemi

OOIS\_PCOM7E May 2021

Participants

Grades

Module Home

Tutor Office

Deadline Details

Seminars

Module Resources

e-Portfolio

Codio

eBook

Unit 1

Unit 2

Unit 3

Unit 4

2009). This debacle led to the Irish government abandoning its e-voting agenda and reverting to the old manual paper system just 5 days to the June 2004 elections (Zelic & Stahl, N.D).

Melia & Byrne (2012) reported that the failure of the e-voting system resulted in a loss of €55m of tax-payers' money. €51m of that was spent on acquiring 7500 voting machines and another €4m spent on storage costs. According to Zelic & Stahl (N.D), the outcome of the 2004 elections were massively swayed as the ruling party experienced the worst election results since 1920s. Nedap, the Dutch Firm that manufactured the voting machines was also criticized for producing faulty equipment (Smyth, 2006).

### References

Collins S. (2009) Rise and fall of Irish e-voting: a brief but expensive history, *The Irish Times* Available from: <https://www.irishtimes.com/news/rise-and-fall-of-irish-e-voting-a-brief-but-expensive-history-1.751993> [Accessed 09 May 2021]

Melia P. & Byrne (2012) €54m machines scrapped for €9 each. *Independent.ie*. Available from: <https://www.independent.ie/irish-news/54m-voting-machines-scrapped-for-9-each-26870212.html> [Accessed 09 May 2021]

Smyth J. (2006) Hackers warn of flawed e-voting machines, *The Irish Times*. Available from: <https://www.irish-times.com/news/hackers-warn-of-flawed-e-voting-machines-1.1011847> [Accessed 09 May 2021]

Zelic B. & Stahl B. (N.D), *The Influence of Realist Ontology on Technological Projects: The Case of Irish Electronic Voting*, Available from: <http://ceur-ws.org/Vol-130/Zelic.pdf> [Accessed 09 May 2021]

Reply

Maximum rating: -

8 replies

1

Post by [Michael Justus](#)

Peer Response

[23 days ago](#)

Hi Kikelomo,

You raise an interesting example of software failure. You raised the point that hackers could demonstrate the ability to hack into the machines and steal votes. In this example, what are your thoughts on how the Dutch company could have prevented their software from being easily hackable?

Following on from the hacking question, are cloud computing solutions more reliable and resilient for use in e-voting? I'm thinking in respect to the Software as a Service paradigm and whether, as professionals, we can leverage this in a lot more scenarios due to the reliability and scale of the vendors providing the service. If their service experiences faults, perhaps they are able to resolve the issues far quicker than, say, the Dutch supplier of the Irish voting machines?

2



Reply to

[Michael Justus](#) from [Kikelomo Obayemi](#)[18 days ago](#)

Re: Peer Response

Hello Michael

Thanks for weighing in and apologies for late response.

"What are your thoughts on how the Dutch company could have prevented their software from being easily hackable?"

The Irish elections of 2004 raised so many questions about the Nedap machines for use in the Netherlands. According to Jacobs & Pieters (2009), a pressure group outlined the two main issues with these machines:

- 1) The programmable EPROM chips were easy to replace such that an attacker will be able to have the machine count incorrectly, without being detected.
- 2) It was possible to eavesdrop on the voting machine via a tempest5 attack. This involves listening to radio emissions from the device.

To solve these problems, the chips were replaced with non-programmable ones, the voting machines were sealed, and an intelligence agency was able to limit the signals emitted by the Nedap machines but not totally eliminate (Jacobs & Pieters, 2009),.

It is evident that security was not a topic of discussion the Irish Government and Nedap. Otherwise, these problems could have been forestalled.

On the topic of cloud computing, I would say yes. Benefits of using cloud computing technology in e-voting include cost efficiency, ease, reliability amongst others but as you are aware, it also comes with its own security concerns. You might already be familiar with this, but I just came across an implementation methodology called “Desktop as a Service” that can be used in e-voting.

Zissis & Lekkas (2011) explains that:

“Desktop as a Service is a container of a collection of virtual objects, software, hardware, configurations etc., residing on the cloud, used by a client to interact with remote services. “

The objective here is to centralize security because a voter’s personal computer is the weakest link in an e-voting environment (Zissis & Lekkas, 2011). The reference journal below explains more about it.

### References

Jacobs, B. and Pieters, W. (2009). Electronic Voting in the Netherlands: from early Adoption to early Abolishment. In *Foundations of security analysis and design V* .121-144. Springer, Berlin, Heidelberg.

Zissis, D. and Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly*, 28(2), 239-251. Available from:<https://doi.org/10.1016/j.giq.2010.05.010> [Accessed May 16, 2021]

3

Reply to  **Kikelomo Obayemi** from **Michael Justus**

Re: Peer Response

[16 days ago](#)

Thank you Kikelomo,

Your statement is true gold: "It is evident that security was not a topic of discussion...Otherwise, these problems could have been forestalled"

Security should never be considered a second-class system of any information system, but as Steward et al (2012) point out, security only comes to mind when something happens to the system or its data--confirmed by the statement.

The Desktop as a Service sounds very interesting, thank you for the link to the article. The e-Citizen cloud system proposed by Zissis et al (2011) makes for an interesting consideration especially in light of the failures experienced by the Irish government and their hackable Nedcap machines.

#### References

<https://neurac.org/security-should-never-be-an-afterthought-while-implementing-devops/>

Steward Jr., C, Wahsheh, L.A, Ahmad, A., Graham, J.M., Hinds, C.V., Williams, A.T. & DeLoatch, S.J. (2012). "Software Security: The Dangerous Afterthought": *2012 Ninth International Conference on Information Technology - New Generations. Las Vegas, NV, USA, 16-18 April 2012*. DOI: 10.1109/ITNG.2012.60.

4

Post by **Suresh Sigera**

Peer Response

[18 days ago](#)

Hi Kikelomo,

First, thank you very much for the wonderful case study. It seems the engineering team has failed to write secure code and test it as they should. Also, instead of having on-premises storage units, it would better to have cloud storage; so the demand system can expand the storage services. What're your thoughts on that?

[Reply](#)



Reply to



**Suresh Sigera** from **Kikelomo Obayemi**

17 days ago

Re: Peer Response

Hi Suresh

Thanks for your comment.

Just as I said to Michael, I doubt that there was a robust discussion on the issue of security when it comes to those machines, how much more conducting tests.

The storage units in this case were used for keeping the voting machines. I do not think we can eliminate physical machines as they will be needed at polling stations. However, be it polling station voting or remote voting, cloud computing solution offers great benefits in the areas of cost reduction, privacy, providing user friendly environment to the voter amongst others (Jadav et al., 2015).

#### Reference

Jadav et al., (2015). Cloud Computing E-Voting: A Technical Review. *International Journal for research in emerging science and technology*. 2(11).

Available from: <https://ijrest.net/downloads/volume-2/issue-11/pid-ijrest-211201502.pdf> [Accessed 16 May 2021]

6

Post by [Sergio Rafael Zavarce Caldera](#)[17 days ago](#)

Peer response

Hi Kikelomo,

It seems that this example showcases a complete failure of several components of an information system. The hardware component along with network and communications components were not planned accordingly to such an important task. The software component also failed, making it impossible to print out vote results.

It could be argued that the other components of the information system also failed. For example, the people component comprises all those involved in the process, from the testers to the officers who validated the system despite criticism and problems. The data and process components did not deliver the required results for the information system. All the components work together, and it might be considered that only the software failed, but in the end, it is a whole system where every component plays its part to make it work successfully.

7

Reply to  [Sergio Rafael Zavarce Caldera](#) from [Kikelomo Obayemi](#)

Re: Peer response

[17 days ago](#)

Thanks Sergio. Good points.