



Information Systems Failure: Peer Responses

Course: MSc Computer Science

Module: Object-Oriented Information Systems

Assignment: ePortfolio

Date: Monday 20th July 2021

Student ID: 126853

Peer Response 1:

In response to:



Post by [Hendrik Van Rooyen](#)

Peer Response

69 days ago

Hi Kieron,

Its fascinating that such a seemingly small change would lead to such a snowball effect. I would like to know why they went ahead and add capacity if they were already running close to a thread count limit as configured in the OS? Furthermore, its also very interesting that they have so many services dependent on each other, which in this scenario definitely made a bigger issue from what could have been a smaller one. Better of course if avoided!

To me, it seems like a lack of information that was available to whomever that had the unfortunate responsibility of performing this task and from my experience it could be various things like failure to mention it during a technical discussion from the peers, lack of documentation, lack of analytics, etc.

I really do like the "Don't put all of your eggs in one basket" idiom and luckily today we do have many alternative cloud providers, but this idiom holds more true when we are not very sure about things. If you look at the service level agreement(SLA) from Amazon Web Services(2020), it states a commitment of at least 99.99% uptime. You could argue that the .01% can lead to a noticable economic loss for rather large organisations, especially ones that have data as their primary product like Facebook, Youtube etc. So, I would say here its about the analysis each company has to do and determine which cloud provider best suit their needs, or to at all go to the cloud. An example would be how organisations in the biopharma industry had requirements like compliance, reliability and security before deciding to go to the cloud(Amazon Web Services, 2017).

References

Amazon Web Services. (2020) Amazon Compute Service Level Agreement. Available from:

<https://aws.amazon.com/compute/sla/> [Accessed 12 May 2021].

Amazon Web Services. (2017) AWS and SAP: How and Why Companies Run Regulated Workloads in the Cloud. Available from: https://d1.awsstatic.com/Industries/HCLS/Resources/AWSandSAP_Dec2017_Final.pdf [Accessed 12 May 2021].



Reply to [Hendrik Van Rooyen](#) from [Andrey Smirnov](#)

66 days ago

Peer Response

Hi Hendrik,

Just wanted to say that I completely agree with your remark that the committed uptime of the main compute and capacity services offered by the major public cloud providers such as AWS and Azure would most likely satisfy the operational needs of many small to mid-sized companies. The are of course multiple reasons why companies might want to adopt the multi-cloud approach, however avoiding the so-called "vendor lock-in" does not seem to be one of the primary decision-making factors (Petcu, 2013). There are also both technical and administrative considerations that might disincline some companies from going multi-cloud, so it is indeed a choice that requires careful deliberation.

Another interesting approach towards managing performance demands is the so-called "cloud bursting", which is a hybrid cloud architecture that enables handling peak times by utilizing public cloud resources on an as-needed basis. This configuration, supported by a connection between the company's private cloud or data center and one of the public clouds, has proven to be an especially effective choice for managing peaks in IT demand (Mattess et al., 2012). There are also models that can be used to calculate the optimal private cloud capacity and the expected cost savings that the cloud bursting architecture could bring in particular circumstances, which can ultimately help the business representatives to make an informed decision (Lilienthal, 2013).

References

Lilienthal, M. (2013) A Decision Support Model for Cloud Bursting. *Business & Information Systems Engineering* 5: 71-81. <https://doi.org/10.1007/s12599-013-0257-5>

Mattess, M., Vecchiola, C., Garg, S. & Buyya, R. (2017) Cloud Bursting: Managing Peak Loads by Leasing Public Cloud Services. *Cloud Computing: Methodology, Systems, and Applications*. Available from: https://www.researchgate.net/publication/267962397_Cloud_Bursting_Managing_Peak_Loads_by_Leasing_Public_Cloud_Services [Accessed 14 May 2021].

Petcu, D. (2013) Multi-Cloud: expectations and current approaches. *Proceedings of the 2013 international workshop on Multi-cloud applications and federated clouds (MultiCloud '13)*: 1-6. DOI: <https://doi.org/10.1145/2462326.2462328>

Post:

Hi Hendrik/Andrey,

Thank you both for your detailed responses and discussions.

I agree that this issue was likely caused by a lack of information and analytics available to the data centre engineer(s) responsible for the upgrade. With AWS being a front-runner in technological advancements, an outsider would have expected their data-centre management/inventory system to provide lists of crucial systems/values to check before upgrades in a checklist-type fashion. However, it could quite well have been the case that the engineer(s) responsible for this upgrade had performed this exact task successfully (in the same way) many times before, causing them to potentially overlook the other checks. The snowball effect certainly shows you the hierarchy of underlying technology within the AWS ecosystem!

When looking at historic cloud outages, Joey D'Antoni (2020) states that "each outage has been limited to a single region within a single provider -- or, in a few rare cases, a single service across the provider". One recent example of this was the fire experienced at the SBG datacenters hosted by OVHCloud (Rosemain & Satter, 2021), which had affected no additional regions. This suggests that a multi-region configuration would likely ensure high availability of a product/service whilst maintaining an element of resilience in disaster recovery. Although, as you have both alluded to, the costs/skills required to maintain this would need to be assessed on a case-by-case basis, which may be more suitable for large companies as opposed to SME's.

However, I believe that the increased service offerings by cloud providers are making cloud interoperability much more challenging to achieve in a working environment, especially when trying to achieve a like-for-like setup in case of a single provider failure. Many organisations are trying to work towards a set of open standards for the cloud computing sector to avoid vendor barriers and incompatible services (Sheppard, 2017).

My workplace, a small local authority, utilise this hybrid-style approach Hendrik refers to in the above responses. We are using cloud-based infrastructure to handle and mitigate potential attacks (Using the Azure WAF offerings) and serving our public products (Websites, webforms, etc.). Although these front-ends are cloud-based, the vast majority of the data served/interacted with is hosted on proprietary software packages, which are on-premise (and linked over a VPN tunnel). Which was a decision we had come to following much deliberation and cost-analysis.

References:

Rosemain, M & Satter, R. (2021) Millions of websites offline after fire at French cloud services firm. Available From: <https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU> [Accessed 16th May 2021].

Sheppard, D. (2017) Cloud interoperability and portability – necessary or nice to have?. Available From: <https://insightaas.com/cloud-interoperability-and-portability-necessary-or-nice-to-have/> [Accessed 17th May 2021].

D'Antonio, J. (2020) The Night the Lights Went Out in the Cloud: Lessons from the AWS Outage. Available From: <https://redmondmag.com/articles/2020/12/02/lessons-from-aws-outage.aspx> [Accessed 17th May 2021].

Screenshot:



 Reply to  **Hendrik Van Rooyen** from **Kieron Holmes**
Re: Peer Response

63 days ago

Hi Hendrik/Andrey,

Thank you both for your detailed responses and discussions.

I agree that this issue was likely caused by a lack of information and analytics available to the data centre engineer(s) responsible for the upgrade. With AWS being a front-runner in technological advancements, an outsider would have expected their data-centre management/inventory system to provide lists of crucial systems/values to check before upgrades in a checklist-type fashion. However, it could quite well have been the case that the engineer(s) responsible for this upgrade had performed this exact task successfully (in the same way) many times before, causing them to potentially overlook the other checks. The snowball effect certainly shows you the hierarchy of underlying technology within the AWS ecosystem!

When looking at historic cloud outages, Joey D'Antoni (2020) states that "each outage has been limited to a single region within a single provider -- or, in a few rare cases, a single service across the provider". One recent example of this was the fire experienced at the SBG datacenters hosted by OVHCloud (Rosemain & Satter, 2021), which had affected no additional regions. This suggests that a multi-region configuration would likely ensure high availability of a product/service whilst maintaining an element of resilience in disaster recovery. Although, as you have both alluded to, the costs/skills required to maintain this would need to be assessed on a case-by-case basis, which may be more suitable for large companies as opposed to SME's.

However, I believe that the increased service offerings by cloud providers are making cloud interoperability much more challenging to achieve in a working environment, especially when trying to achieve a like-for-like setup in case of a single provider failure. Many organisations are trying to work towards a set of open standards for the cloud computing sector to avoid vendor barriers and incompatible services (Sheppard, 2017).

My workplace, a small local authority, utilise this hybrid-style approach Hendrik refers to in the above responses. We are using cloud-based infrastructure to handle and mitigate potential attacks (Using the Azure WAF offerings) and serving our public products (Websites, webforms, etc.). Although these front-ends are cloud-based, the vast majority of the data served/interacted with is hosted on proprietary software packages, which are on-premise (and linked over a VPN tunnel). Which was a decision we had come to following much deliberation and cost-analysis.

References:


Rosemain, M & Satter, R. (2021) Millions of websites offline after fire at French cloud services firm. Available From: <https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU> [Accessed 16th May 2021].

Sheppard, D. (2017) Cloud interoperability and portability – necessary or nice to have?. Available From: <https://insightsaas.com/cloud-interoperability-and-portability-necessary-or-nice-to-have/> [Accessed 17th May 2021].

D'Antonio, J. (2020) The Night the Lights Went Out in the Cloud: Lessons from the AWS Outage. Available From: <https://redmondmag.com/articles/2020/12/02/lessons-from-aws-outage.aspx> [Accessed 17th May 2021].

Peer Response 2:

In response to:



Hendrik Van Rooyen

Initial Post

71 days ago

5 replies

Last 64 days ago

TechCrunch and Reuters(2018) reported that In 2018, an attack on Facebook led to the exposure of over 50 million user accounts. The attackers managed to exploit vulnerabilities in a video uploader feature that would generate an access token, if you viewed the profile using the "View As" feature. This essentially meant that the attackers could use this access token and get information of the user through the facebook apis.

Facebook countered the attack by logging out about 90 million people, thus invalidating the access tokens. However, the damage was done and the shares of Facebook fell by 2.6% shortly after the announcement, not to mention the damage to the consumers' trust. The attack could have been prevented by proper reviewing and penetration testing before going live with the feature.

References

TechCrunch. (2018) Everything you need to know about Facebook's data breach affecting 50M users. Available from: <https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/> [Accessed 10 May 2021].

Reuters. (2018) Facebook says big breach exposed 50 million accounts to full takeover. Available from: <https://www.reuters.com/article/us-facebook-cyber-idUSKCN1M82BK> [Accessed 10 May 2021].

Auth0. (n.d) Access Tokens. Available from: <https://auth0.com/docs/tokens/access-tokens> [Accessed 10 May 2021].

Post:

Hi Hendrik,

I find this to be quite an interesting issue, especially compared to the various breaches and data privacy concerns surrounding Facebook over recent years. In this instance, TechCrunch (2018) report that information accessed includes Names, Genders and Hometowns, all of which is data that Facebook considers to form part of your 'public profile' (And is therefore accessible through Graph API's) (Facebook, n.d.) which suggests that no private information was revealed.

DevBridge (2019) states that a common risk when using access tokens is that developers often forget to adequately manage token expiration, a practice that can reduce the time in which a malicious user has access to the system. Two approaches that could be used for this task are using Refresh Tokens (to renew

short-lived access tokens) or regularly requiring users to confirm their password to continue using the platform (A relatively non user-friendly approach).

Do you believe that Facebook has an overall preference to focus on user convenience and service accessibility over security/privacy improvements?

What is your opinion surrounding the quantity/severity of the breaches Facebook are experiencing? (Would you consider the working culture and inadequate practices/testing to be a contributory factor?)

References:

TechCrunch. (2018) Everything you need to know about Facebook's data breach affecting 50M users. Available From: <https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/> [Accessed 12th May 2021].

Facebook. (n.d.) What is public information on Facebook?. Available From: <https://www.facebook.com/help/www/203805466323736> [Accessed 12th May 2021].

Aleksandrovas, Artūras & DevBridge. (2019) Five risks and tips when securing user authentication tokens. Available From: <https://www.devbridge.com/articles/five-risks-and-tips-when-securing-user-authentication-tokens/> [Accessed 12th May 2021].

Screenshot:



Post by **Kieron Holmes**
Peer Response

68 days ago

Hi Hendrik,

I find this to be quite an interesting issue, especially compared to the various breaches and data privacy concerns surrounding Facebook over recent years. In this instance, TechCrunch (2018) report that information accessed includes Names, Genders and Hometowns, all of which is data that Facebook considers to form part of your 'public profile' (And is therefore accessible through Graph API's) (Facebook, n.d.) which suggests that no private information was revealed.

DevBridge (2019) states that a common risk when using access tokens is that developers often forget to adequately manage token expiration, a practice that can reduce the time in which a malicious user has access to the system. Two approaches that could be used for this task are using Refresh Tokens (to renew short-lived access tokens) or regularly requiring users to confirm their password to continue using the platform (A relatively non user-friendly approach).

Do you believe that Facebook has an overall preference to focus on user convenience and service accessibility over security/privacy improvements?

What is your opinion surrounding the quantity/severity of the breaches Facebook are experiencing? (Would you consider the working culture and inadequate practices/testing to be a contributory factor?)

References:

TechCrunch. (2018) Everything you need to know about Facebook's data breach affecting 50M users. Available From: <https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/> [Accessed 12th May 2021].

Facebook. (n.d.) What is public information on Facebook?. Available From: <https://www.facebook.com/help/www/203805466323736> [Accessed 12th May 2021].

Aleksandrovas, Artūras & DevBridge. (2019) Five risks and tips when securing user authentication tokens. Available From: <https://www.devbridge.com/articles/five-risks-and-tips-when-securing-user-authentication-tokens/> [Accessed 12th May 2021].

Bibliography:

Auth0. (n.d.) Understanding Refresh Tokens. Available From: <https://auth0.com/learn/refresh-tokens/> [Accessed 12th May 2021].

Peer Response 3:

In response to:



Post by [Hendrik Van Rooyen](#)
Peer Response

66 days ago

Hi Kieron,

While it may be true that no private information was revealed, it did generate enough panic for facebook to log out 90 million people and generate negative media coverage that had an impact on their shares and their reputation.

Yes, it should be extremely important to have expiration on those tokens. I generally like to stick with a 2 hour expiration and then just fetch a new token if the user is still online, but the old one expired. Way more user friendly than redirecting to a log in page again :-)

Your first question is very hard to answer. You could argue and say privacy and security forms part of user convenience as it will be very inconvenient for me to get my account hacked. So I would say that they are all very high on the priority list, or so I would hope!

Facebook is a big company and it will continue to attract the interest of people that want to exploit the platform. Having said that, Facebook also has access to some of the most talented people that are working hard at preventing disasters and producing good software.

To answer your question. In my original post I mentioned reviewing and penetration testing as you usually would pick up on those errors. Having said that, features get deployed all the time and what may have passed the pentest before, doesn't now anymore. This is where a good audit can reveal those flaws too. However, because I don't work there, I cannot say for sure how they will go about.

Post:

Hi Hendrik,

Thank you for the comprehensive response; despite my very broad/vague questions! I've just touched briefly upon the media coverage surrounding this breach, as I forgot to include this in my previous response.

I think most of the news articles covering this breach actually downplay the potential severity of the issue, only touching upon the fact that the "public profile" information was accessed. In fact, the level of access associated with access tokens would have given malicious actors the ability to access/modify many details on their profile (View Private Messages, Ad Preferences/Interests, and information that could be considered protected characteristics under the Equalities Act), with potentially severe ramifications for the individual if these attacks were in fact targeted.

With regards to User Convenience and Security, you raise a very good point - that account hacking/misuse would be highly inconvenient for the end-user. I had intended to refer to the fact that Facebook may be rushing through new features and services at the cost of not performing internal code reviews or penetration testing before the public release (Perhaps running them on a monthly schedule, for example). Although, without knowing the inner working practices of the company, it would be impossible to tell!

Although, in this case, the issue seemed to have been picked up by regular systems monitoring. I agree that future penetration testing/audits, combined with the public reporting mechanisms (Such as HackerOne) would have highlighted this issue.

Screenshot:



Reply to



[Hendrik Van Rooyen](#) from [Kieron Holmes](#)

64 days ago

Re: Peer Response

Hi Hendrik,

Thank you for the comprehensive response; despite my very broad/vague questions! I've just touched briefly upon the media coverage surrounding this breach, as I forgot to include this in my previous response.

I think most of the news articles covering this breach actually downplay the potential severity of the issue, only touching upon the fact that the "public profile" information was accessed. In fact, the level of access associated with access tokens would have given malicious actors the ability to access/modify many details on their profile (View Private Messages, Ad Preferences/Interests, and information that could be considered protected characteristics under the Equalities Act), with potentially severe ramifications for the individual if these attacks were in fact targeted.

With regards to User Convenience and Security, you raise a very good point - that account hacking/misuse would be highly inconvenient for the end-user. I had intended to refer to the fact that Facebook may be rushing through new features and services at the cost of not performing internal code reviews or penetration testing before the public release (Perhaps running them on a monthly schedule, for example). Although, without knowing the inner working practices of the company, it would be impossible to tell!

Although, in this case, the issue seemed to have been picked up by regular systems monitoring. I agree that future penetration testing/audits, combined with the public reporting mechanisms (Such as HackerOne) would have highlighted this issue.

Peer Response 4:

In response to:



Taylor Edgell

Initial Post
75 days ago

6 replies
Last 63 days ago

One prominent example of a system failure, that has been in the news recently, is that of the Horizon IT system used by the Post Office.

The horizon system, created by Fujitsu and introduced fully in 1999, was the United Kingdom Postal Services bespoke system to process a variety of transactions and automate services within its network. The system was estimated to have been used by at least 11,500 Post Office branches, in addition to the Post Office stating that it has process over 6 million transactions a day (Prodger, 2013). Reliance on the Horizon system can be seen to have been fundamental to the daily operation of the postal service.

It has been found that there were many faults and bugs within the system, with the consequences of these negatively affecting many of the Post Office employees greatly. The greatest issue with the system was based around the potential for "any data or data packet error having the potential to produce apparent shortfalls" (Bates V. Post Office, 2019). The led to the appearance of various accounting errors during the bookkeeping process which the individual Postmasters were expected to cover.

The fallout of this error led to a variety of consequences including Postmaster's and Sub-postmaster losing their jobs and businesses, receiving fines, and in some instances jail time. All these negative instances were generated by data and evidence generated and provided by the Horizon system. The implications of this error have seen a variety of cases being taken to court to rectify the injustices created by this error. One of the most famous cases was that of Bates V Post Offices, with the judgment setting the precedent for the system error being the fault of the Post Office. This was the first judgement for which the Post Office were ordered to pay significant damages and costs. Since then, the CCRC (Criminal cases review commission) has brought more than 51 cases, based on evidence generated by the Horizon system, to be brought to appeal (CCRC, 2021).

The root cause of these failure seems to be based around both Fujitsu and the Post Office failing to audit their system correctly. Although there is some evidence of their awareness of these issues, neither company made any significant and apparent preventative action. "These should include system checks to detect an either prevent or report on suspicious behaviour or mistakes" (Christie, 2020). It has also been seen that Fujitsu did have its own error reporting system, but this was not employed and actively used by the Post Office. Further issues were created as the Post Office had the legal right to act as its own prosecutors and investigation service. This led to them using primarily erroneous data generated by the Horizon system.

This example emphasises the ethical implications of relying on evidence generated by an IT system alone to deem fault. The detriment produced to many employees was due to the reliance on the flawed system and the belief that it was infallible. It can be seen as unfair and unjust that in some cases people were convicted on the singular evidence generated by an IT system that they had no direct control over. It can be understood that no matter how "robust" a system appears to be it should not be relied upon alone, particularly in relation to legal issues.

References:

Prodger, M. (2013). 'Bug found in Post Office row computer system, *BBC*, 13 July. Available at: <https://www.bbc.co.uk/news/uk-23233573> (Accessed: 05 May 2021).

Christie, J., 2020. The Post Office Horizon IT Scandal and the Presumption of the Dependability of Computer Evidence. *Digital Evidence & Elec. Signature L. Rev.*, 17, p.49.

'Bates V. Post Office (2019) High court of Justice, Queen's bench division, Case EWHC 3408 (QB). Available at: <https://www.judiciary.uk/wp-content/uploads/2019/12/bates-v-post-office-judgment.pdf> (Accessed: 5 May 2021).

CCRC. (2021). 'CCRC refers four more Post Office Horizon cases, [Press release]. 20 January. Available at: <https://ccrc.gov.uk/ccrc-refers-four-more-post-office-horizon-cases/> (Accessed: 5 May 2021).

Post:

Hi Taylor,

You raise some excellent points regarding both the lack of regular/comprehensive audits and the inability of the Post Office/Fujitsu to verify the claims caused by erroneous data independently.

Mason (1986) states that "Misinformation has a way of fouling up peoples lives, especially when the party with inaccurate information has an advantage in power and authority". I believe this quote links well with your statement that the Post Office was in a position of authority, whereby they could bring private investigations and

prosecutions against individuals without any form of independent verification (Such as an independent legal provider or the Crown Prosecution Service).

Information provided to ComputerWeekly (2021) states that within Fujitsu's working environment, the issues with the Horizon system were abundant during development, with the system being labelled as "not fit for purpose" by senior development staff. It is also believed that there weren't regular code reviews, developer documentation, peer reviews or coding standards.

Setting audits aside, do you believe this issue could have been prevented by introducing comprehensive test suites and developer documentation? Or do you think it is a broader issue with the working culture within Fujitsu, and the inability to formulate adequate system planning at the earlier stages of the development lifecycle?

References:

Mason, R. (1986) MIS Quarterly. Four ethical issues of the information age. 10(1): 5-12. Available From: https://www.jstor.org/stable/248873?seq=4#metadata_info_tab_contents [Accessed 14th May 2021].

Wallis, N. (2021) Fujitsu bosses knew about Post Office Horizon IT flaws, says inside. Available From: <https://www.computerweekly.com/news/252496560/Fujitsu->

[bosses-knew-about-Post-Office-Horizon-IT-flaws-says-insider](#) [Accessed 14th July 2021].

Screenshot:



Post by [Kieron Holmes](#)
Peer Response

66 days ago

Hi Taylor,

You raise some excellent points regarding both the lack of regular/comprehensive audits and the inability of the Post Office/Fujitsu to verify the claims caused by erroneous data independently.

Mason (1986) states that "Misinformation has a way of fouling up peoples lives, especially when the party with inaccurate information has an advantage in power and authority". I believe this quote links well with your statement that the Post Office was in a position of authority, whereby they could bring private investigations and prosecutions against individuals without any form of independent verification (Such as an independent legal provider or the Crown Prosecution Service).

Information provided to ComputerWeekly (2021) states that within Fujitsu's working environment, the issues with the Horizon system were abundant during development, with the system being labelled as "not fit for purpose" by senior development staff. It is also believed that there weren't regular code reviews, developer documentation, peer reviews or coding standards.

Setting audits aside, do you believe this issue could have been prevented by introducing comprehensive test suites and developer documentation? Or do you think it is a broader issue with the working culture within Fujitsu, and the inability to formulate adequate system planning at the earlier stages of the development lifecycle?

References:

Mason, R. (1986) MIS Quarterly. *Four ethical issues of the information age*. 10(1): 5-12. Available From: https://www.jstor.org/stable/248873?seq=4#metadata_info_tab_contents [Accessed 14th May 2021].

Wallis, N. (2021) Fujitsu bosses knew about Post Office Horizon IT flaws, says inside. Available From: <https://www.computerweekly.com/news/252496560/Fujitsu-bosses-knew-about-Post-Office-Horizon-IT-flaws-says-Insider> [Accessed 14th July 2021].