Case Study: Low-Cost IT Infrastructure Decisions Cost Minimum of MYR18,700.00 Losses Due to Insider Threat in Malaysia

Chew, Kean Ho[1]

[1]ZORALab Enterprise
kean.ho.chew@zoralab.com

March, 2022; 1st Issue

1 Abstract

Saving on IT infrastructure expenses is an usual business practice that usually yields a costly consequences if the strategy is not upgraded through the mid development. There are other considerable aspects aside financing when it comes to technological selection. Otherwise, deciding based on finance alone will create problem with snowball effect causing damages far greater than the initial thinking of saving. This paper presents a real case amounting MYR18,200.00 losses as of November 15, 2021 after 2 years of utilization.

This case study paper explores a medium-sized enterprise customer salvaging a sinking circumstances where its own vendor had caused numerous trust and data loss damages. It studies the details of the work scope, the problem, how ZORALab approaches it, and the total cost of mitigating the circumstances back to stability.

For the sake of protecting privacy for all parties, all personal and enterprise identifiable information were replaced with anonymous aliases and any sensitive evidences were redacted.

2 Introduction

Selecting an enterprise technology requires a proper technological oriented and related talent and the right financing budget to get it right from the start. Otherwise, any decision made will eventually cause a snowball effect problem that can be costly if not mitigated. For this case, it caused a significant loss amounting MYR18200.00 in total as of November 15, 2021 only after 2 years of utilization.

This case study paper explores a medium-sized enterprise customer salvaging a sinking circumstances where its own vendor had caused numerous trust and data loss damages. It studies the details of the work scope, the problem, how ZORALab approaches it, and the total cost of mitigating the circumstances back to stability.

For the sake of protecting privacy for all parties, all personal and enterprise identifiable information were replaced with anonymous aliases and any sensitive evidences were redacted.

3 The Aliases

To protect the privacy of the every parties involved, personal and enterprises, this paper

shall fully utilize aliases to replace the actual identity, concealing every information. Therefore, any resemblance with any of aliases is purely coincidence and unrelated to the actual entity.

The aliases are detailed in the following sub-sections.

3.1 Victim

In this paper, we shall address the victim enterprise as **Atlas Firm or Atlas**, which is a ZORALab client.

3.2 Supporting Parties

In this paper, a number of supporting parties were involved to assist ZORALab and Atlas for recovering the losses. Among them were:

1. **Zenus Apollo** – a consulting attorney.
2. **Yarin Bryan** – a Malaysian Royal Police officer who is ZORALab's regular consultant for this case.

3.3 Antagonist

In this paper, we shall address the antagonist IT service provider as **Misstro Company or Misstro**, which was an Atlas's IT vendor. There was only 1 antagonist as the IT services are "All-in-One" package.

4 The Problem

In this section, the paper looked into the immediate problems that caused Atlas to hire ZORALab for resolution and mitigation solution. Then, the paper analyzed the situation and study the root cause.

The immediate complication was that Atlas had grown itself for 2 years with Misstro services, generating a large amount of enterprise-grade data from emails to localized data files. Somehow in year 2021, Misstro caused data loss to Atlas.

4.1.1 Extremely Misconfigured

After remotely surveying all Atlas computing endpoints, it was found that every endpoints and the cloud services were severely misconfigured. Among the known misconfigurations were:

1. **Email client software was using POP3 instead of using IMAP protocol. It was originated by advice from Misstro that** caused a lot of home-brew localized email data fragmentation across every computing end-points.
2. **A consistent TWO (2) of the email account suffered data losses (by 2 week policies) not due to email client software configurations** (e.g. Microsoft Outlook email retention policy).
3. **DATA were localized and only accessible within the premise** local network, at one particular computing endpoint.
4. The cloud service from Misstro only offers **file synchronization across Internet was using FTP protocol**.
5. **DMARC policy was set before DKIM and SPF were properly configured** that caused frequent bounced sent emails.

4.1.2 Unexpected Complications from Nature

The incident happened during Malaysia's worst Covid19 Pandemic lockdown in June 2021 as shown in Figure 4.1.3.1[1][2] where ZORALab can only fix the issue by remote access.

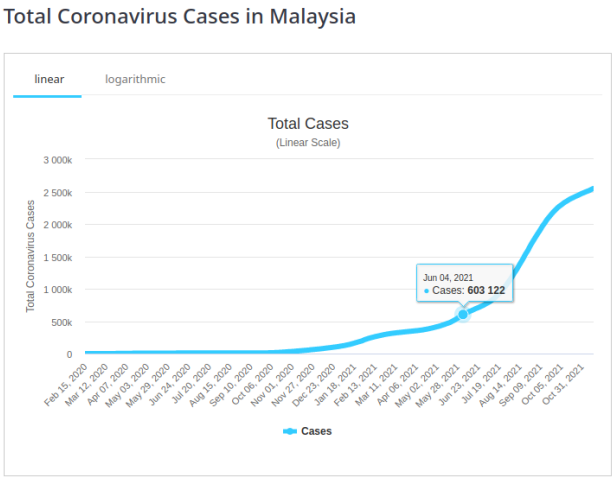

Figure 4.1.2.1: Total Coronavirus Cases in Malaysia for June 2021 (Rising cases)[2]

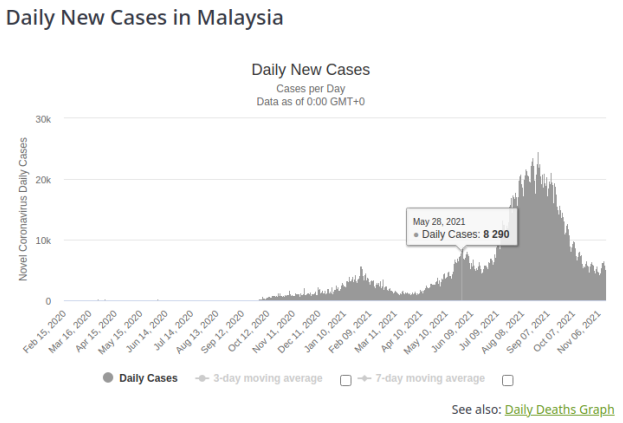

Figure 4.1.2.2: Daily New Cases in Malaysia for June 2021 (Beginning of the Largest Hike)[2]

Moreover, the CEO of Atlas was admitted into hospital during the same time, leaving ZORALab with limited communications and access to solve the issue.

4.1.3 Unexpected Heavy Resistances from Misstro

As ZORALab always track progress using data-driven manner, there was an unexpected threat where many data pointed to Misstro's internals themselves were intentionally obstructing the data recovery and migrations efforts. Their consistent messages were forcing Atlas to upgrade its subscription.

5 Solving The Problem

In this section, the paper explores how ZORALab solved the technical problems and took the approaches dealing with Misstro that arrived to an undesired conclusion.

5.1 Keeping Business Running

Without much options, ZORALab had to assemble our own computing assets to extract existing fragmented email data via cloud connection by bulks across each computing endpoint. These consolidated data and re-synced to the server which later being deposited into our assets for transitions.

All these were done over the Malaysian 1 weekend timeline in order for Atlas to work remotely on Monday without any business downtime.

5.2 Misstro Negligence

Throughout the resolution, it was detected that Misstro's negligence multiple times. Some unforgivable negligence were:

1. **Setting enterprise-wide bandwidth capacity limitation where it shouldn't**. This caused multiple suspension to Atlas IT system including domain name suspension.
2. **Unreasonably suspend a paid domain** due to previous negligence, where Atlas uses other 3rd-party services where Misstro has zero (0) access to. In other

words, Misstro has ZERO (0) rights to threaten Atlas entire business domain over its own server related service disputes.

3. **Lies and falsely made up multiple reasoning to the suspension** and repeatedly requesting Atlas to either upgrade the infrastructure or have its business completely shut down despite Atlas was a paid and zero overdue customer.

Those data above, for a paid and has zero (0) records of underpay customer, all the data seemly suggest that Misstro was trying to sabotage its proper client in order to have them upgraded to a higher pay packages during the Covid19 lockdown pandemic. As per ZORALab understanding, that's a business breach of trust and they can no longer be trusted with housing and protecting any sensitive data: an insider threat.

5.3 Confronting Misstro

With the captured data, unreasonable business suspension, and forceful upgrade request, ZORALab confronted Misstro multiple times to restore all the accesses and business continuity. The journey was not delighting; unsecured; distrustful; and frequent stands-off and threat exchanges.

5.3.1 Originated from CTO

In some interactions between ZORALab and Misstro's CTO, it turns out that the CTO was the one that specify POP3 is the right protocol for email client software instead of the correct IMAP version.

6 Atlas Ultimatum

After reverting to Atlas with the findings, ZORALab was finally given instruction to migrate all data, business and personal, from email to localized data files, into ZORALab's vendors for securing Atlas operations. The objective is simple: to secure Atlas business continuity and blacklist Misstro from doing any businesses in the future. Again, all operations where done in another 2-days weekend to ensure everyone can operate properly while working in office and working from home.

6.1 Damage Calculations

The total cost and man-hours charging at an already discounted of ~MYR120.00 per hour for the initial case resolution and infrastructure migration tasks yielded at MYR10060.00 in total. This fee includes the vendors' subscription fees upto 1 year.

However, due to Misstro's misconducts and negligence, they caused an additional amount of MYR8640.00 extra man-hours just to deal with them. This part of the cost is unexpected for both Atlas and ZORALab.

7 Authorities Support

After Atlas business operations are secured, both Atlas and ZORALab seek assistance from relevant Malaysian authorities. This section explores all available options from authorities both considered and taken by Atlas.

7.1 Royal Police Malaysia

ZORALab did approached Royal Police Malaysia and filed 2 reports for Misstro case on behalf of Atlas. However, the Royal Police Malaysia closed both cases immediately stating that there were no criminal aspects from it and recommended Atlas to pursue civil filing.

7.2 Civil Filing

Upon consulting Zenus Apollo, the lawyer; and Yarin Bryan, the police consultant; their insights were exactly the same as Royal Police Malaysia's conclusion: civil filing. However, Zenus Apollo, as per his experience, stated that there is a complication.

The amount was too small and is very likely only for covering legal and court expenses even-though Atlas has a strong win. Hence, this direction was considered but not pursued.

7.3 Malaysia Communications and Multimedia Commission

Ultimately, ZORALab suggested to Atlas to file a case against Misstro to Malaysia Communications and Multimedia Commission.

After consulting with Zenus Apollo, he mentioned that the monetary damage is most likely unrecoverable if this direction is pursued. This direction only gain would be revenge satisfactions since the commission will definitely give Misstro some enjoyable moments and it is not the commission's jurisdictions and power to help victims for seeking back the monetary damages.

8 Lessons and Recommendations

This section covered the learning and recommendations from the case. The goal is to ensure no further victims in the future both in Malaysia and global business owners.

8.1 The Malaysian Tech Ecosystem

It was a deeply sadden lesson to learn that both authorities and legal directions were unhelpful against a malicious tech service provider in Malaysia tech ecosystem, even at the monetary damage of MYR18700.00. Filing a complaint to Malaysian Communications Multimedia Commission and Malaysia's National Cyber Security Agency will definitely punish Misstro but will not recover the monetary damages which is vital to Atlas.

Hence, these were the recommendations and lessons from the case:

1. **As long as the total damages were under MYR18700.00, Malaysia's IT service providers can perform any malicious at their will without getting any consequences from the relevant authorities or civil court proceeding**. They can confidently betting on this circumstances based on this case study alone.
2. **Hence, it's best to spend a little bit more upfront for hiring a proper consultant like ZORALab from the start** to make the right, secured, and cost effective decision.
3. **Although senseless and not advisable, the total monetary damages shall go beyond 6 digits** in order to enable the victim to proceed with civil filing legal process.
4. **Be very vigilant when selecting Malaysia's tech service provider** as their knowledge may be ill-equipped like the CTO of Misstro did.

5. **Do not focus solely on low price when dealing with technological selection** as that will cost you more in the near future, especially dealing with enterprise-level business needs.

9 Conclusion

Assembling and selecting enterprise business technologies based on low-cost is an intuitive decision. However, overdoing it without considering other technological aspects with a technological-oriented talent like reliability, trust, privacy protection requirements, support quality, interactions, and backup can cause a whooping monetary damages amounting a minimum of MYR18200.00 in near future.

In Malaysia, tech service provider can suffer no consequences should they, intentionally or unintentionally causing malicious damages to their own customer. The amount of MYR18200.00 is too small for legal civil filing while the authorities only can punish them but unable to reimburse or to recover the monetary damages back to victim.

To avoid this from happening again, it is best to spend a bit more for hiring a proper tech consultant like ZORALab upfront during technological selection stage to make the right, secured, and cost effective decision as on overall.

10 License

11 Reference

[1] RAM ANAND; 2021; “Malaysia’s Covid-19 lockdown to be extended beyond June 28: PM Muhyddin”; *Asia* > *SE Asia*; SPH Media Limited Co. (Reg. No: 202120748H); accessed on November 15, 2021; available at: https://www.straitstimes.com/asia/se-asia/malaysias-covid-19-lockdown-to-be-extended-pm-muhyiddin

[2] WORLDMETER; 2021; “Coronavirus in Malaysia”; *Coronavirus* > *Country*; WorldMeter via Worldmeter.info, accessed on November 15, 2021; available at: https://www.worldometers.info/coronavirus/country/malaysia/