Disruptions to critical services highlight urgent need to dig deep into digital vulnerabilities

Digital transformation needs to be better managed with a greater focus on building a resilient system across the board.

Vivek Choudhary and Michael Tan

One doesn’t need to imagine how far-reaching the consequences of these disruptions can potentially be. ST PHOTO: LIM YAOHUI

The recent disruptions to some online services in Singapore’s banking and healthcare sectors serve as a cautionary tale, underlining the importance of strengthening our digital infrastructure.

On Oct 14, DBS Bank faced a significant service disruption, with its digital banking services and automated teller machines (ATMs) unavailable for more than 12 hours. Citibank experienced disruptions to its digital banking services that evening.
Over 800,000 attempts to access the digital banking platforms of both banks failed in that time, leading to thousands of customer complaints.

Another incident on Nov 1 affected the healthcare sector, where the websites of several hospitals became inaccessible. And more recently, OCBC Bank’s digital banking app and Internet banking and Nets-related services faced disruptions.

It’s not just an issue of inconvenience, as such disruptions affect people in significant ways when it comes to livelihoods and emergencies. One doesn’t have to imagine how far-reaching the consequences of these disruptions can potentially be.

Just days ago, a nationwide outage experienced by Australia’s second-largest telecommunications provider Optus left millions in the country without communication and crippled transport networks. The company has struggled to explain the issue but ruled out a cyber attack. The impact of the massive disruption was felt across sectors, including healthcare, transport and banking.

These recent events, at home and abroad, underscore the vulnerability of digital systems despite all the benefits they have brought and will continue to bring.

Call for backup

Singapore has made substantial investments in the digitalisation of pivotal sectors such as banking and healthcare.

The focus on cashless payments, digital healthcare records and online services not only promises increased productivity and efficiency, but also reduces the demands on manpower by streamlining processes, from financial transactions to the retrieval of patient records.

This approach paves the way for harnessing the power of cutting-edge technologies, such as artificial intelligence, to elevate the overall customer service experience.

But with digitalising services comes a great level of dependence on technical infrastructure for service delivery. Key components, including data centres responsible for data retrieval and storage and service websites facilitating tasks like appointment booking and transactions, play a crucial role.

To keep operations running while protecting data and sensitive information, resilience is key. Backup systems and other security strategies are essential to guarding against equipment failure or cyber attacks targeting these infrastructures.

In the case of the DBS and Citibank disruptions, preliminary and subsequent investigations revealed that the issue with their online banking services and ATMs was linked to their data centres, which digital infrastructure company Equinix manages.

According to Equinix, the problem stemmed from an error made by a contractor, resulting in an incorrect signal that led to the closure of valves controlling the chilled water buffer tanks. This, in turn, affected the chilled water flow to the cooling system. Equinix has stated that it is examining its processes and undertaking additional audits to avoid a similar problem during future upgrades.
Data centres can encounter various potential failure points, including in cooling systems, power sources, network connectivity, storage systems, uninterrupted power supplies (backup power sources), and fire suppression systems.

**MORE ON THIS TOPIC**

**Australia to investigate massive Optus Internet and phone outage**

2.5 million transactions affected by recent DBS, Citibank outages: 810,000 login attempts failed

Thus, mitigating single-point-of-failure situations – where any failure can lead to a complete disruption of service operations – becomes key.

One such mitigation strategy is redundancy. A common method that is employed involves activating a backup server when one fails.

Equinix lacks a robust contingency plan for swiftly activating backup servers during downtime. The Monetary Authority of Singapore (MAS) has instructed both banks to conduct a comprehensive inquiry into the reasons behind the delay in their backup data centres’ ability to restore systems within a short timeframe.

Given that the issue was traced back to a third party sending an incorrect signal, it is imperative to establish a stringent process control mechanism to prevent such errors in the future.

There have been calls for banks to establish backup data centres, which are crucial for real-time operations. Even with such a fail-safe measure, it must be noted that modern data centres cannot ensure 100 per cent uptime. MAS’ standard allows for no more than four hours of unscheduled downtime per year, equivalent to slightly over 99.95 per cent uptime.

While backup data centres may increase costs significantly, it could be a worthwhile investment to avoid regulatory penalties and to enhance consumer trust. One would think that the banks can afford this. But there’s a reason why it may not be a preferred choice.

A backup data centre with real-time data replication may introduce transaction latency. Essentially, this gives rise to longer waiting time for consumers and the question of whether we are willing to accept it. This is because data is initially added in the primary centre and then replicated in the backup, a process similar to data synchronisation found in tools like OneDrive or Dropbox.

Another apparent solution is to minimise recovery time with the understanding that downtime will happen. Efforts should then focus on its reduction.

**MORE ON THIS TOPIC**

4 of the 5 major DBS disruptions in 2023 were bug- or software-related: CEO Piyush Gupta

MAS suspends DBS from new business ventures, reducing branch and ATM networks over disruptions

Safer with segregation

While the online banking issues were caused by internal malfunctions and the companies had full control over the situation, the healthcare websites’ failure was attributed to an external cyber attack known as distributed denial of service (DDoS).

In DDoS attacks, cyber criminals deploy multiple bots to inundate the website with queries and requests, overwhelming the server and disrupting normal access for users.

Fortunately, there was no data theft or unauthorised patient data access. Internet services were also partitioned – computer systems and networks were separated from the public Internet and services that are accessible via the Web – to contain the impact. This helped to isolate DDoS attacks and facilitate team communication.

However, a cause for concern is that these bots were triggered from compromised computers belonging to the general population. The distributed nature of the attack made it challenging to trace the source back to the original attackers. Such DDoS attacks can be scaled easily to generate massive traffic volumes, making them highly effective in overwhelming target systems and causing service disruptions.

When a DDoS attack occurs, it indicates that numerous computers, which could belong to anyone, inside or outside of Singapore, have been taken over by hackers without the owners’ knowledge or consent. These compromised devices are often part of a larger network, and they’re used to flood a target website or online service with an overwhelming amount of Internet traffic.

If patients’ computers are taken over by hackers and the Internet traffic sent to flood the hospital websites is of legitimate activities such as arranging appointments or requesting drug refills, the hospital websites will not be able to block them.

Preventing DDoS attacks remains a challenge, but there are strategies to improve defences.

MORE ON THIS TOPIC

‘I carried around my piggy bank’ Amid DBS, Citibank service outage; cash is king

Some users still left with pending transactions one day after DBS’ PayNow hit by service delays

Increasing the network load capacity can buy time for technical teams to address issues during an attack. Firms in Singapore could also collaborate with Internet service providers to detect unusual traffic targeting specific websites.

Additionally, creating an internal operating system solely on backed-up server data can ensure business continuity during a cyber attack, with data replication to the main server once the issue is resolved.

These significant incidents serve as opportunities to enhance the resilience and security of Singapore’s digital systems. The digital banking disruptions and the DDoS attack might have been temporary, but they must prompt a permanent and renewed focus on strengthening our digital infrastructure.