COVID-19 burdens technology risk: What we must think of as we deploy technology in the fight against the virus

Humanity's instinct to survive can be surprising. What is not surprising is how the COVID-19 pandemic has accelerated the digital journey for many organisations. According to forbes.com, organisations that will weather the storm will need to intensify use of technology if they are to continue serving customers and remain competitive. However, as we deploy these solutions, we must do so cautiously. Below are some measures that organisations should consider having in place in this era of disruption.

Speed to deploy

With organisations eager to deploy new solutions that facilitate business continuity in this era of social distancing, they should ensure that customers have unfettered   access to services even during restricted movement. Unfortunately,the pressure to quickly deploy such solutions may lead to releases whose functionality and security have not been adequately tested and thus are susceptible to data breaches; lead to errors , reputation damage and ultimately financial loss.

Technology risk needs to be considered from the onset in determining just how 'raw' the minimum viable product can be, before being introduced in the market. Organisations that have embraced agile ways of working will have already embedded risk management practises and risk practitioners into their project teams to perform these checks and instill confidence on these products. Having your vulnerability assessment team on speed dial at such a critical time as this, is no longer a nice to have but a must to have.

Therefore, even as we look to quickly deploy new solutions to the market, we must ensure that key functionalities are adequately tested and security reviews have been performed. The technology risk team must be the 'front and centre' in determining the extent to which testing must be done before go-live. The key is to move quickly, but carefully.

Remote access

A critical success factor in this war against COVID-19 is social distancing through working from home which organisations must facilitate their staff in order to remain operational. This may require providing remote access to critical applications. Indeed, it has been a treacherous mine field for organisations that have never deployed these methods before; especially when the policy on secure remote access was written to 'pass an audit' and now has to be dusted, enriched and implemented.

Stringent user access policies will have to be adhered to. The level of approval to obtain remote access to critical systems should be escalated to the highest levels in the organisation. This will limit the number of individuals that are granted access to critical systems. Furthermore, it will also be important to vet individuals before granting them access to these systems. This will involve conducting background checks to determine whether they have a history of integrity issues or are susceptible to commit fraud either on their own or with the help of a third party. Once this is done, remote access should be granted only when it is absolutely necessary.

The assumption here is that this access will be granted via secure links or over a virtual private network. Stakeholders must understand the level of security of connectivity and encryption of data being transmitted. The main advantage for organisations that have been performing frequent security testing is that vulnerabilities are identified early and resolved. All technology intensive enterprises should make security testing a regular exercise.

The capacity for infrastructure to transmit more data and handle numerous connections (load and stress) should also be considered. Previously, fewer staff may have been granted remote access. The 'work from home' arrangement will undoubtedly necessitate increased remote connections. Technical teams should test supporting infrastructure and adjust to accommodate demand.

The mode of approvals will also need to be adjusted. Remote working means that some approvals will have to be done via email. The nature and impact of the approval could necessitate secondary confirmation methods such as a video or phone call. It is also prudent for the system actions to enforce 'maker-checker' controls, multi-factor authentication, etc.

It is important to note that remote access is a no-go zone, if there are no measures to log and monitor user activities. Stakeholders must ensure that stringent monitoring controls are implemented to facilitate near immediate detection of anomalous activity and subsequent resolution. This requires continuous monitoring capabilities. Where this is not possible, the frequency of review of activity logs must be increased. Technical support during this time is critical and should be available to solve any access or processing issues.

Remote technology project management

Presently, remote working and access challenges have exacerbated for institutions that were in the middle of large-scale technology implementations before the pandemic. It is now inevitable that platforms that facilitate remote working and conferencing be deployed. Facilities that enable large file sharing and collaboration are also critical at this time and hence project teams need to embrace them and accept that this is the new normal. Project managers can re-engineer project activities and deliverables around this eco-system. All security considerations relating to remote access, such as remote system testing and access to data for migration also apply in this case.

It is critical that project quality and risk management controls be maintained. They should not be discarded just because the mode of project delivery has changed. These controls should be adapted and effectively enforced even when teams are in different locations.

In summary, proactive and intentional application of technology risk management and assurance is a mandatory requirement.

That is why the workload for technology risk teams has doubled since the first day the COVID-19 was captured in organisational risk logs. If we rely on technology to beat COVID-19, then technology risk management and assurance is without doubt an essential service.

Management by wandering around

On a light note, the directive to work from home must have sent a cold chill down the spines of managers who prefer 'management by wandering around'. Initiatives exist that can assist with 'remote management by wandering around'. However,depending on the nature of the business, it may be necessary to adapt to other methods of supervision.COVID-19 made one thing clear, the choice to change is no longer in your hands – something else is!

> **If we rely on technology to beat COVID-19, then technology risk management and assurance is without doubt an essential service."**

Raymond Mugo
Senior Manager
IT Advisory
KPMG Advisory Services Limited
E: rmugo@kpmg.co.ke

The views expressed herein are personal and do not necessarily represent the views of KPMG.

kpmg.com/socialmedia

kpmg.com/app