Deloitte.

IT services in uncertain times – COVID 19 cyber security update

2020

Introduction

With the COVID-19 lockdown, most Namibian businesses had to find creative ways to continue operations while keeping their employees, customers and suppliers safe. More often than not, this took the form of remote working arrangements. The increased use of IT in combination with the distance between users and the IT function resulted in an uptick of cyber-attacks[1]. None-the-less, the lockdown period also taught us valuable lessons about what is actually possible to achieve if the need for rapid change arises. This article explores the implications of remote working arrangements on IT service provision and highlights key findings from our survey.

Survey results

Deloitte conducted a Cyber Security Update: COVID 19 survey in April 2020 and May 2020 which investigated both the prevalence of cyber-attacks in the Namibian market and respondents' preparedness in terms of COVID-19 lockdown measures.

Only 20% of respondents indicated that they had been the target of a cyber-attack and that the impact of those attacks was moderate to minor, whereas global statistics indicate an uptick in cyber attacks of up to 30%. This may indicate that either Namibian entities are not yet aware of the breach having occurred (the mean time for users to identify a data breach in 2019 was 206 days[2]) or that, mercifully, cyber criminals found bigger targets elsewhere to focus on. Whatever the reasons may be, given the general lack of sophistication of Namibian IT users in terms of internet security remarked upon in previous Deloitte Namibia Cyber Surveys[3], we predict that Namibian entities may yet find themselves the target of cybercrimes related to COVID 19.

80% of our respondents assessed the digital maturity of their organisation as "partial", with limited paper trails and most critical functions being able to operate remotely, while the remainder (20%) indicated limited digital maturity whereby only administrative functions are able to operate remotely. This presents an opportunity for further investigation and development of remote working capabilities even post-COVID 19 lockdown, as fixed costs such as office rental and parking space could be reduced while also affording staff the opportunity to arrange their working day more flexibly[4].

This transition to a remote workforce would need to be carefully managed in the light of some critical risks – see graphic on next page. The risk that respondents identified as having the highest chance of disruption was that existing processes are inadequately automated, resulting in labour intensive activities that do not lend themselves to remote working.

---

[1] See https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/ and https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/

[2] As per the Ponemon Institute's "Cost of a Data Breach report 2019"

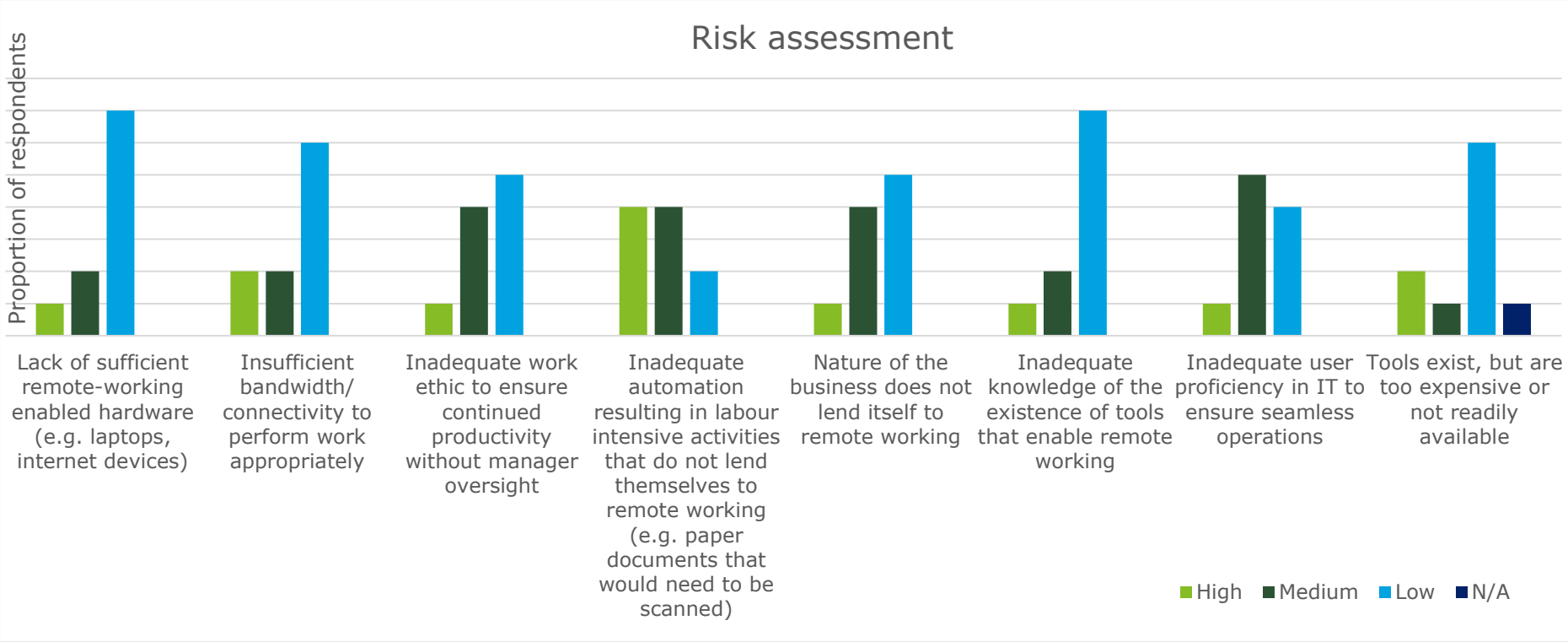
[3] https://www2.deloitte.com/na/en/pages/risk/articles/namibian-perspective-on-cyber-security-2020.html and https://www2.deloitte.com/na/en/pages/risk/articles/namibia-cybersecurity-survey.html

[4] See also our thought leaderships on the Future of Work available at https://www2.deloitte.com/global/en/pages/about-deloitte/topics/combating-covid-19-with-resilience.html?icid=covid-19_dcom_home-page_desktop

Other key risks noted to be of moderate impact in addressing the COVID 19 lockdown requirements (and that may become exacerbated in the longer term) were:

- inadequate work ethic to ensure continued productivity without manager oversight,
- the nature of the business not lending itself to remote working, and
- inadequate user proficiency in IT to ensure seamless operations.

The good news is that these risks can be addressed and managed with targeted process re-engineering and user training and the lockdown has resulted in the rapid deployment of tools that enable remote working.



Of the 80% of respondents that indicated they had a business plan, 37% indicated that their business plan did not contain sufficient actions to enable them to react appropriately to the lockdown. Despite this, 90% of respondents were able to react to the lockdown within a week or were only resolving minor issues, with 40% having put all critical measures in place within 24 hours. This indicates significant effort on the part of key decision makers and undoubtedly placed great pressure on key resources to manage the crisis.

Qualitative comments to our survey indicated some satisfaction that measures implemented enabled the business to keep critical services operational throughout the crisis, while 30% of commenters acknowledged the importance of continued cyber awareness and thoroughly tested business continuity plans that also involve simulated emergency exercises to be performed by all staff to ensure that emergencies do not catch enterprises off guard.

Conclusion

It is self-evident that not all operations will be able to be fully digitised or operate without significant human interaction, foremost amongst these being tourism and hospitality operations as well as retailers. However, COVID 19 has illustrated a remarkable resilience in Namibian enterprises that can be leveraged for the future in new ways of doing business. Even where our respondents have indicated that full digitisation is unlikely to be a reality in the long term, COVID 19 highlighted some weaknesses that can and should be remediated and has possibly sparked innovation and the adoption of currently available technologies that could result in more efficient processes.

Contacts

Melanie Harrison

Director

Risk Advisory

Tel: 061 285 5003

Email: melharrison@deloitte.co.za

Nicoline Badenhorst

Senior Manager

Risk Advisory

Tel: 061 285 5056

Email: nbadenhorst@deloitte.co.za