Cyber security: Emerging threats and risks with the increased use of virtual platforms to conduct work, and potential vulnerabilities of the entire world

Professor Tshilidzi Marwala - University of Johannesburg

13 August 2021

As Zoom and Microsoft Teams began to trigger a form of online fatigue last year, those of us in senior management at the University of Johannesburg (UJ) witnessed quite a remarkable phenomenon.

Confined to their homes and confronted with social distancing to curb the spread of the coronavirus disease, some of our students and some external elements began gate crashing online lectures to cause disturbances in an unusual form of disruption. Protests have become an increasingly frequent phenomenon in the South African higher education landscape, triggered by the #FeesMustFall movement aimed at stopping annual increases in student fees while increasing government funding of universities. These online protests were characterised by rowdiness and even singing as Zoom crashing and Blackboard bombing became somewhat of a trend. In response, the University had to strengthen online security to ensure that the intruders were kept at bay.

Though it was an intriguing sign of our times, it also served as a stark reminder that as this ‘new normal’ continues to permeate our lives, cyber security has to be of utmost concern. Put simply, cyber security comprises technologies, processes, and practices designed to protect digital platforms from attack, damage, or unauthorized access. The COVID-19 pandemic has been a great definer for digital transformation. As it quickly became apparent that the national lockdowns across the world would not be a reality for just a few weeks, swift shifts to online systems across the board ensued, bringing with it new and exciting ways of learning, working and living.

Yet, as our lives have become infused with technology, we have had to contend with the grim reality of cyber security breaches. Though many institutions have comfortably found ways to operate remotely, there has been a discernible absence of accompanying cyber security measures. The continued increase in remote processes leaves individuals and institutions vulnerable to cyber risk. We are now well into our second year and approaching our third year of remote processes yet little has been done to curb this risk. Though student protests during online lectures are an interesting anecdote, it represents just how easy it is to breach systems in our current times and alludes to far more sinister acts.

Dan Coats, Former Director of National Intelligence of the United States, warned against the danger of cyber security threats. As he put it, “A major attack on our cyber systems could shut down our critical infrastructure - financial systems, communications systems, electric grids, power plants, water treatment centers, transportation systems and refineries - that allows us to run our economy.” This is of particular concern in South Africa as our country’s cybersecurity is poorly ranked.

According to Accenture, South Africa is the third-highest cybercrime-hit country in the world after Russia and China. The Global Cyber Exposure Index ranks SA sixth on the list of most-targeted countries for cyber attacks, with the highest concentration of exposed businesses.

This is perhaps unsurprising when you consider the magnitude of attacks we have seen in recent years. In the first 100 days of the lockdown alone, Mimecast researchers detected huge increases in spam attacks, which were up 46%, impersonation attacks, which were up 75%, and malware, which spiked by 385%. Last year August, South Africa experienced its largest-ever data leak, which exposed the personal information of about 24 million South Africans and nearly 800 000 businesses. According to the South African Banking Risk Information Centre (SABRIC), the country loses over R2.2-billion year-on-year to cybercrime. Given the profound shifts to online modes in the last year, it's safe to assume that this has been compounded.

Just last week, it emerged that a cyberattack on Transnet's IT infrastructure stalled activity at South Africa's ports. As Denys Reva, the Research Officer for the Peace Operations and Peacebuilding Programme at the Institute for Security Studies put it, "Attacks on critical infrastructure, including maritime ports, are likely to increase in severity and quantity. The economic toll for African states will inevitably be high, which means that measures to boost cyber security and protect infrastructure are vital." Globally, we have certainly seen cyber security breaches increase.

Based on data from the World Economic Forum (WEF), CGI, Interpol and Data, there has been 50.1% increase in cyber-attacks and an associated 30,000 cyber-attacks, a 600% increase in phishing attacks, a 300,000% increase in cyber threats and 18 million malware and phishing emails blocked. I would go so far as to argue that these numbers are likely conservative estimates. In April this year, a Norton report found that in the past year, nearly 330 million people across 10 countries were victims of cybercrime and more than 55 million people were victims of identity theft while cybercrime victims collectively spent nearly 2.7 billion hours trying to resolve their issues.

In an academic paper last year on cyber security in the age of COVID-19, Singh Lallie et al found, "The COVID-19 pandemic, and the increased rate of cyber-attacks it has invoked have wider implications, which stretch beyond the targets of such attacks. Changes to working practises and socialization, mean people are now spending increased periods of time online. In addition to this, rates of unemployment have also increased, meaning more people are sitting at home online- it is likely that some of these people will turn to cyber-crime to support themselves." Given this context and the likelihood of remote working and living being a reality for us for quite some time, what is to be done?

Already, South Africa has established a Cybercrimes Act to mitigate digital attacks and intrusions. While the Act identifies the South African Police Service (SAPS) as the leading agency to coordinate investigations, there is currently little capacity to carry this out. The Act defines cybercrime as including, but not limited to, acts such as: the unlawful access to a computer or device such as a USB drive or an external hard drive; the illegal interception of data; the unlawful acquisition, possession, receipt or use of a password; and forgery, fraud and extortion online. The Cybercrimes Act and the recently implemented Protection of Personal Information (POPI) Act are closely connected, with the latter underscoring data privacy.

The next year will be crucial to determine just how effective these acts and what kind of support we may need from external stakeholders. Last year, the Presidential Commission on the Fourth Industrial Revolution (PC4IR), of which I am deputy chairman, presented a set of recommendations to parliament. The recommendations we have made include investing in human capital, establishing an AI institute, creating a platform for advanced manufacturing, securing and availing data to enable innovation, as well as incentivising 4IR industries and platforms. The other recommendations are building 4IR infrastructure, reviewing and amending legislation, and, finally, establishing a 4IR strategy implementation coordination council.

Of critical importance to our discussion today is the recommendation to secure and avail data to enable innovation. As we outlined in our report, the principal opportunity in the 4IR is the storage of large sums of data, which will be critical for building e-government services across sectors such as health, transport and justice. This could be achieved through the creation of the National Data Centre, which will consolidate the available computational power and create a national data repository for all of our data. However, our cybersecurity systems needs to be bolstered in order to safeguard the public. The pandemic has certainly demonstrated how crucial this is. The report calls for the establishment of a National Cybersecurity Institute.

Without this, South Africa could face a number of digitization risks. To quote the PC4IR report, “The security or trust dimension is an important element required to build citizen confidence when using digital technologies.” This is crucial to implement and understand from a legislative perspective as well as from a consumer perspective, which may require enhanced artificial intelligence capabilities. The government has a cybersecurity company called Comsec, linked to the National Intelligence Agency, which was established in 2003 and secures government’s communications against any unauthorised access and from technical, electronic or any other related threats.

To be competitive in the 4IR, the government would need to strengthen Comsec’s mandate to include cybersecurity. Already, the Department of Public Service and Administration has established a Standing Committee on Information Systems Security (SCISS), which is where all government departments are represented to discuss matters related to information security and cyber-security. This, however, should be seen as just an initial step in a much larger strategy. Of course, cybersecurity is not a concern confined to government, its affiliated agencies or public institutions, it is a serious consideration all companies and individuals have to take into account.

Accenture found that South African were generally less aware of cyber threats compared to people from other countries. Around 50% of South African respondents were not aware of multi-factor authentication or its benefits, for instance. Addressing public knowledge around cyber threats and cybersecurity is an important initial step. This, however, must be accompanied by active and deliberate investment. This is imperative to ensure that organisations have the processes in place to respond to threats immediately and effectively.

According to McKinsey, two of the greatest challenges brought about by the pandemic is how to increase the security of working at-home tools and processes and how to secure confidentiality, integrity and availability of consumer-facing network traffic. Just

as we have physical security on our premises, we have to see this as simply an extension of this. The last year has certainly demonstrated how precarious and fragile our systems are without it. Not only are we as institutions and individuals vulnerable to attack but by proxy, so are our networks.

As Bruce Schneier appropriately wrote in a 1997 essay, “History has taught us: never underestimate the amount of money, time, and effort someone will expend to thwart a security system. It's always better to assume the worst. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens, you'll be glad you did.”