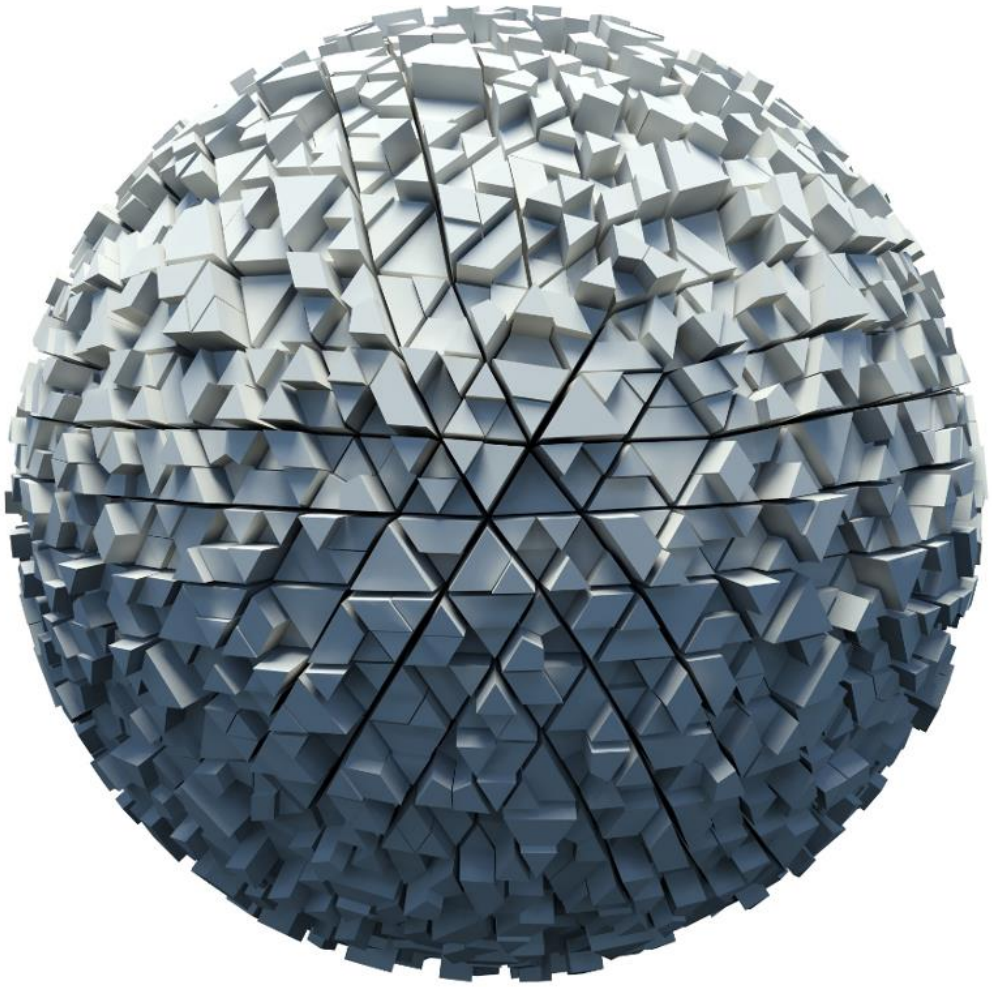
Deloitte.

JSE



Thought Leadership Series:

The impact of cyber on critical infrastructure in the next normal

Executive summary | July 2020

MAKING AN IMPACT THAT MATTERS since 1845

As COVID-19's ramifications ripple through the global economy and other sectors, one thing is certain: technology will be among the most powerful weapons in every organisation's arsenal for responding effectively and decisively to this challenge.

Introduction

The outbreak of the COVID-19 pandemic has bought numerous challenges and opportunities for market participants and stakeholders within the Capital Markets eco-system with the severity of the financial impact varying by sector. Whilst the disruption created is severe, many organisations are using this moment to challenge traditional thinking and business models to be fit for the future.

The JSE together with Deloitte, have created a virtual event series for business leaders and the investor community to share and learn as they navigate their business through these uncertain times. The first in the series, held on 15th July 2020, focused on the shifts in cyber threats through and beyond COVID-19. Zanele Morrison, JSE Director, led the discussion with guest speakers: Eric McGee, Deloitte Cyber Risk expert and Brian Pinnock, Director of Sales Engineering at Mimecast.

Eric Mc Gee, Deloitte Africa - Cyber Risk, Associate Director

Brian Pinnock, Mimecast - Director, Sales Engineering

Zanele Morrison, JSE – Director of Marketing & Corporate Affairs

Executive Summary

How cyber will impact critical Infrastructure in the 'next normal'

As Covid-19 dramatically reshapes global society into the 'next normal', many organisations that never considered themselves part of the cyber critical infrastructure discussions are now classified as such. This fact is not lost to cyber threat actors. While most organisations impacted by cyber-attacks may risk losing data or financial information, a successful attack on critical infrastructure could potentially impact health, safety or the environment.

In addition, the transition of countless employees, contractors, and third parties to remote work has left many organisations unprepared to monitor or detect insider threats that may arise. Just as critically, however, the turbulence created by Covid-19 is proving fertile ground for malicious insiders. Many users are new to the remote working experience and will quickly have to rise to the cybersecurity challenges and regulator's compliance mandates.

The rising risk of cyber attacks

Whilst some industries may be more prepared that others to empower employees to work from home and to continue with business operations in the "new normal," none of the industries have been prepared for the current scale of employees working at home and pressures on business infrastructure that we currently face. This has brought about a fresh set of cyber risks and the Mimecast 2020 state of email security report shows the increase in threats and attacks over the past 12 months including:

- 45% impacted by ransomware
- 46% increase in impersonation fraud
- 35% say they experienced data loss
- 76% have experienced downtime from an attack

Technology will be among the most powerful weapons in every organisation's arsenal for responding effectively and decisively to this challenge.

Recommendations for Technology and Risk Management Leaders in their short-term cyber response

Globally, Deloitte have adopted a three-phased framework of Respond, Recover and Thrive as a method for organisations to lead their business through the crisis. In the Response phase of reacting to cyber threats, the key consideration relates to the susceptibility of the workforce to social engineering methods cyber criminals who exploit the fear and uncertainty that the current situation brings.

These methods focus on tricking employees to disclose their login credentials or other sensitive information that can assist the criminals. These are delivered through targeted phishing emails that delivers malware that can infiltrate information or trigger ransomware attacks inflicting severe damage to organisations. It was recommended that the following measures be adopted to immediately respond and protect organisations:

- Ensure remote working is done through VPN to ensure corporate security controls remain in place;
- Consider endpoint detection and response (EDR) technology, multifactor authentication to better protect against remote working cyber threat;
- Run awareness campaigns to ensure employees are vigilant not to fall for social engineering and phishing tricks;
- Ensure offline backups are done and tested to ensure recoverability;
- Use threat intelligence to block command and control traffic on your network;
- Extend your monitoring and detection measures to ensure malicious activity is detected; and
- Prioritise IT helpdesk functionality for your employees.

Recommendations for Technology and Risk Management leaders in the Recovery phase

As businesses move into the Recover phase, Technology and Risk Management leaders will be considering protecting the brand and future proofing the organisation against potential risks and threats. With remote working stretching into the medium term, business leaders will consider the infrastructure

challenges arising, including the impact which load shedding in South Africa and the impact of employee connectivity and productivity.
Key considerations are:

- Preparing for life without the data centres;
- Rationalise technology projects and portfolios;
- Equip your connectivity, security and infrastructure for new traffic and use patterns;
- Determine critical business services and adjust service level agreements (SLAs);
- Be prepared for cash flow constraints, but also be ready to fight for additional investments; and
- As employee home networks become part of the critical infrastructure, consider how employees can be assisted and supported.

Threat hunting becomes a critical component to cyber defense

Threat hunting services increase the visibility of the different phases of an attack whilst it is being produced, thus reducing the number of successful attacks. The investigation can shed light on seemingly isolated events that may not represent a threat by themselves but can be part of more sophisticated attacks.

In the Recover and Thrive phases it is imperative to increase the ability to detect threat actors and the ideal opportunity to enhance current cyber controls. Advanced threat hunting enables visibility of attackers where traditional cyber detection methods fail.

Advanced threat hunting requires a solution tailored to each environment and should consider the following:

- Complementary approach in order to detect behaviours that are undetectable using a classic monitoring approach;
- Proactive searching methods to identify threats that are traditionally undetectable using reactive monitoring methods;
- Specialised industry threat intelligence that provides in depth insight into an attack and the weaknesses that were compromised for the attack to take place; and
- Highly specialised capabilities to perform deep analysis of such undetectable behaviours.

Threat Hunting services offer an extension to the traditional IT security monitoring approach by increasing the detection scope and finding threats that are typically overlooked to traditional detection based on rules and enable preventing breaching as early as possible in the kill chain.

Empowering the workforce – cyber training is critical

"We have found that cyber awareness and training is very effective in combating threats and risks. Educating users on the best use of cyber practices has proven effective."

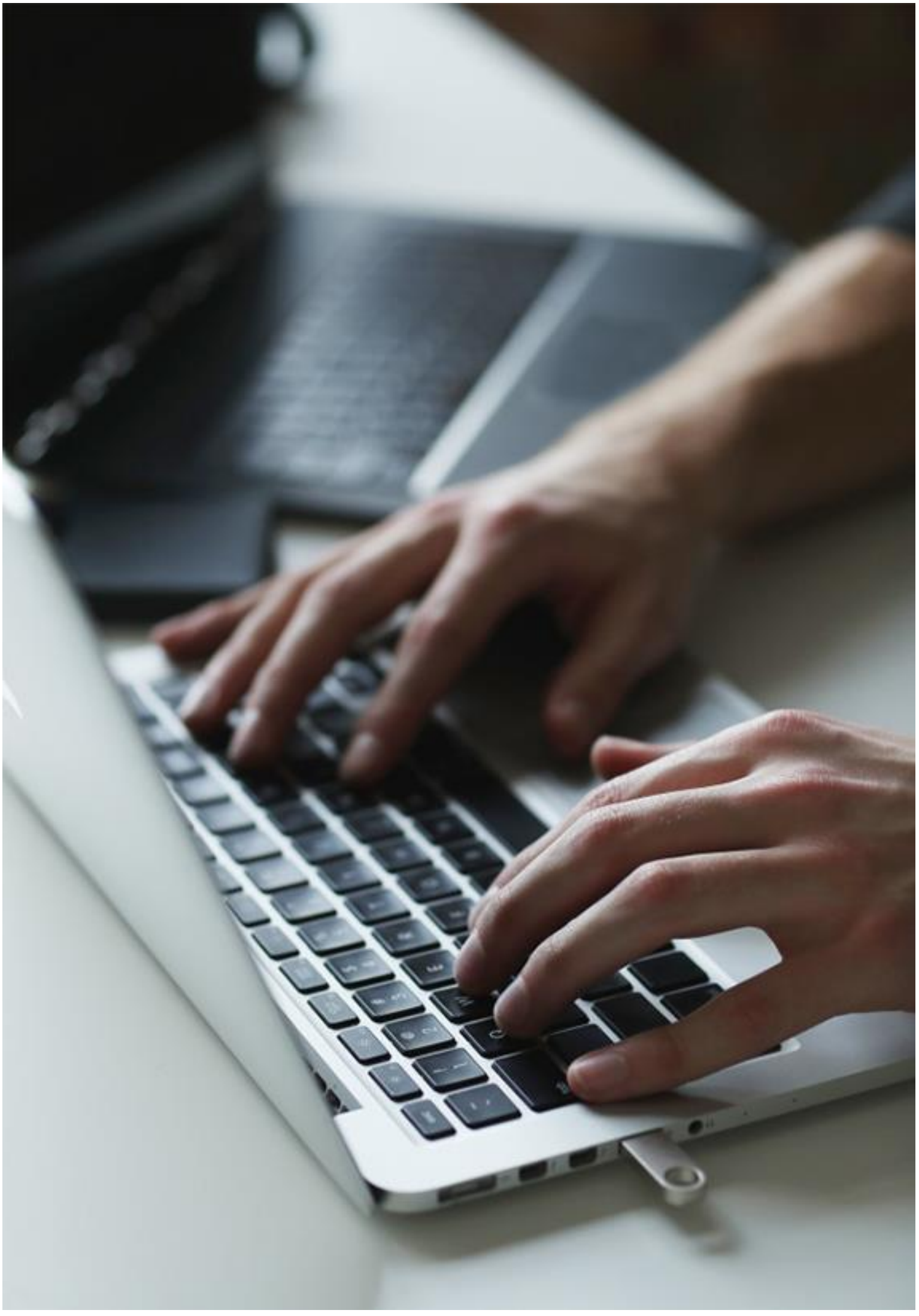
- *Brian Pinnock, Mimecast, Director: Sales Engineering*

A security policy manual alone will not prepare people to take the right actions. For this purpose, cybersecurity training is an essential component. By reinforcing the right behaviour, organisations will become more secure, vigilant, and resilient against cyber threats. Delivering online and on-site technical and awareness programmes and sessions is the best and only way to face digital transformation.

Opportunities to knowledge share

Our guest speakers recognised that there have been many examples where organisations receive a wave of negative response post a cyber-attack. Whilst organisations need to commit to protecting their customers and workforce from cyber-crime, it is important to note that organisations which experience cyber breaches are indeed the victim of a criminal act. In response, there is an opportunity to engage more widely within vertical industries amongst business leaders that fell victim to attacks and are responsible for protecting their organisation, as these forums can play an important part in the global ecosystem to share intelligence and technology controls in the global fight against cyber-crime.

Click here for supporting information, tools and resources



Key Contacts

Eric Mc Gee, Deloitte Africa: Cyber Risk, Associate Director

Email: erimcgee@deloite.co.za

Telephone: +27 (0)11 517 4715

Eric Mc Gee is an Associate Director within the cyber practice at Deloitte. He entered the cyber security space when he joined the BCX Group in 1998 at Nanoteq where he managed the security product development. In 2004 he moved from Nanoteq to BCX Networks, where he assisted in starting the Information Security Competency. Since 2008 he managed the Security Line of Business for BCX and became the Managing Executive for the Communications and Security Business Unit in 2014 where he looked after cybersecurity and network managed services.

Brian Pinnock, Director: Sales Engineering

Email: pinnock@mimecast.com

Telephone: +27 (0)11 722 3726

Brian joined Mimecast in October 2016 as Director of Sales Engineering, overseeing the sales engineering function in Middle East and Africa. Brian has over 20 years' experience in pre-sales, sales, R&D and product development in network communications, messaging and information security. His current focus is driving the expansion of Mimecast cloud-based email and web security as well as threat intelligence by helping organisations leverage their existing security investments.

Zanele Morrison, JSE – Director of Marketing & Corporate Affairs

Email: zanelemo@jse.co.za

Telephone:+27 (0) 11 520 7777

Zanele Morrison is the Director of Marketing and Corporate Affairs for the Johannesburg Stock Exchange (JSE). Her core areas of expertise include change and journey management, communications, stakeholder engagement, leadership and change management delivery within financial services, public sector, telecommunications, mining and manufacturing environments. In her role, she oversees the JSE's group marketing and branding, communications, events, policy as well as regulation. She also manages the retail strategy and the JSE's Broad Based Black Economic Empowerment agenda.

.

Deloitte.