BCX

CYBERSECURITY IN THE NEW NORMAL

PROTECTING DATA OUTSIDE THE FORTRESS WALLS

TABLE OF CONTENTS

01

THE RISK LANDSCAPE HAS SHIFTED

Chief Information and Security Officers (CISOs) and information security teams at large South African organisations were already grappling with a complex and fast-changing landscape at the outset of 2020 — characterised by more sophisticated cyber-attacks, the advent of new attack vectors stemming from the growth of Internet of Things , artificial intelligence (AI) and cloud, and the dawning of more stringent data privacy and protection regulation.

But if they thought they faced a taxing environment as the year opened, the coronavirus outbreak early in the year compounded every challenge, exposed every shortcoming and amplified the urgency of every imperative in their cybersecurity infrastructures and strategies. The pandemic has pushed security even higher up the agenda.

Most IT departments responded to national lockdown and the social distancing requirements of COVID-19 with laudable speed and agility. In many cases, however, the scramble to enable work from home and digital service channels meant that they needed to take shortcuts to enable business continuity.

With many users working from home on non-trusted fibre networks or mobile broadband connections — often using consumer-grade devices and software — a range of new vulnerabilities have opened up for the average enterprise. All too many companies found themselves ill-prepared for a world where so many users are accessing data and systems outside the campus perimeter.

Now, as they settle into a new normal, enterprise IT departments and risk management teams know that they need to look beyond the makeshift security and patchworked solutions they deployed early in the pandemic. With remote working, digital channel use was expected to form a larger part of the post-COVID-19 world, so most organisations had to retool their security environment accordingly.

This is accelerating them towards a future for which they may have thought they'd had another five years or more to prepare. For forward-thinking CISOs and IT departments, the unwanted challenges of the pandemic provide a catalyst for a transition towards a more flexible yet more resilient cybersecurity posture.

The questions they are asking include: If remote work is the new normal, how do we keep data secure without compromising the end-user experience? Was our information security an enabler or inhibiter for the deployment of new digital solutions under lockdown? Are our security vendors and service providers able to keep pace with our needs during these unprecedented times?

For CISOs that grasp the nettle, the upside of the pandemic could lie in the opportunity to review their current security investments, processes and vulnerabilities — and then reimagine cybersecurity not only as a matter of compliance and business continuity, but also as an enabler for digital transformation and new ways of working.

02

NEW ATTACK VECTORS AND THREATS ON THE RISE

Before we'd even heard of COVID-19, most enterprise IT departments in South Africa were already facing a different sort of pandemic: growing volumes of malware, social engineering scams, attempted network breaches and a range of other cyber-threats growing in number and sophistication.

Indeed, the news headlines over the past two years have included some significant breaches, including a ransomware attack that left prepaid customers in a major city without electricity in 2019[1] , a distributed denial of service attack that left an Internet service provider unable to effectively service customers in 2019[2], and a breach at the credit bureau, that may have exposed the personal information of around 24 million South Africans.[3]

The costs of these large-scale breaches can be high. Research published in 2019 by the Ponemon Institute in the US shows that a single data breach costs South African companies an average R45 million.

These costs include detection and escalation, notification, response to the breach and lost business, but do not factor in the long-term costs to brand and reputation.[4]

Here are a few of the trends adding more complexity to information security for IT departments:

WORK-FROM-HOME

The trend towards remote working was already in motion before the pandemic; and since the onset of COVID-19 and the subsequent national lockdown response, remote working has seen a significant acceleration and/or growth. A GfK study of online South African consumers found that 48% said working from home will continue to be a reality for many companies even after COVID-19.[5]

Despite the potential cost-savings that work from home creates for companies and its lifestyle benefits for employees, work from home raises many information security challenges. IT departments have their work cut out for them not only in terms of rolling out appropriate infrastructure to secure home devices and networks and to manage them remotely – but also in helping employees to understand and avoid the security risks they'll encounter outside the corporate network.

CLOUD MIGRATION

Along with the move towards remote work, organisations have accelerated their move to the cloud. They have less visibility into how their employees are accessing data and what they are doing with it, especially when people are using their own personal devices. Organisations need fit-for-purpose solutions and policies to manage the new threats, particularly multi-factor authentication, complex passwords and mobile device management.

CONNECTED THINGS: A NEW ATTACK SURFACE

The Internet of Things (IoT) market is expected to grow in value to $1.1 trillion by 2026 from $190 billion in 2018.[6] This explosion in connected devices brings with it more complexity for IT departments to manage as cyber-criminals take advantage of a wide, new attack surface — one characterised by rapid change and innovation and one where security practices aren't yet as mature as they are in other segments of the market.

According to a report from F-Secure, the number of attack events measured from January through to June was 12 times higher when compared to the same period in 2018, with the increase largely driven by IoT-related traffic.

The biggest share of attack traffic (760 million events) was measured on the Telnet protocol, which is used by IoT devices.[7]

INSIDER RISKS

Insider threats remain one of the single biggest sources of security breaches for most organisations. In some cases, disgruntled employees may seek to damage systems or steal data out of malice; in other instances, the motivation might be greed.

However, accidental leakage of sensitive corporate information is as often a result of negligence or carelessness as it is as of criminal intent. According to one global study, the number of insider-related breaches increased by 47% in 2020, and 60% of organisations suffered over 30 incidents a year.[8]

As with many other security threats, insider risk has grown as a result of more people working from home, out of the watchful eye of the IT department.

SOCIAL ENGINEERING AND PHISHING

Whether they take the form of mass phishing emails that are cheap and easy to launch or more elaborate and personalised voice calls or text messages, social engineering scams continue to proliferate. They target a desire to please, a fear of authority or financial loss, and other human emotions to persuade end-users to give a criminal their access credentials.

Such scams are low risk, yet highly effective, allowing cybercriminals to breeze past security using legitimate logins and passwords that a user has surrendered to them.

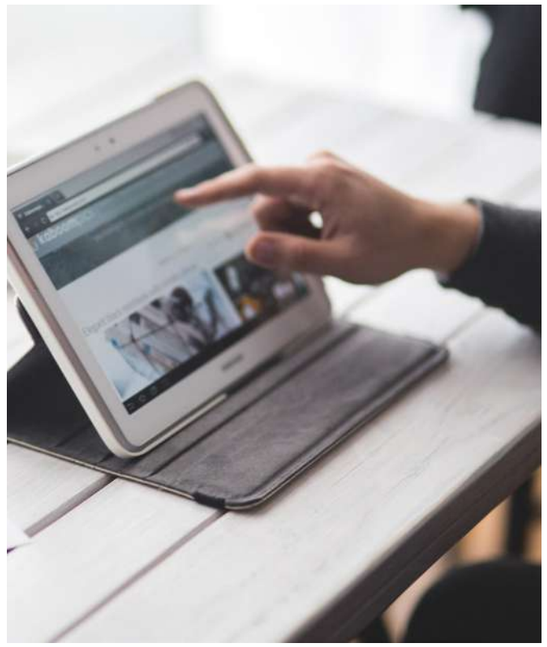
According to Kaspersky, there were nearly 617,000 phishing attacks in South Africa in the second quarter of 2020 alone. Phishing attacks have become increasingly elaborate and individually targeted, according to the security vendor.[9]

SOPHISTICATED RANSOMWARE

Massive outbreaks like NotPetya — which crippled more than 30,000 laptop and desktop computers as well as 7,500 servers at Merck alone[10] — and WannaCry — estimated to have hit more than 200,000 computers worldwide[11] — have put ransomware near the head of the threat list for most enterprises. Ransomware has proliferated because of the availability of cheap, easy-to-use ransomware kits on the dark web, allowing criminals with limited technical skills to launch low-risk, high-reward attacks. Businesses, rather than individuals, are increasingly the targets because they often prove more willing to pay the ransom.

DIGITAL ECOSYSTEM PARTNERSHIPS

Whether it is by giving users outside the enterprise — business partners, customers, suppliers and so forth — credentials to access selected systems and data or by using application programming interfaces (APIs) to interconnect with external organisations' systems, companies are opening internal systems to the outside world. While this enables new business models or closer relationships with their stakeholders, it also creates new vulnerabilities. Allowing external developers and partners to tap into app ecosystems and software platforms via APIs, for example, creates new gaps for bad actors to exploit.



03

BEST PRACTICES FOR THE NEW NORMAL

In the wake of the COVID-19 pandemic and with the pace of digital change accelerating, it's clear that the cybersecurity models of the past are no longer adequate. Today's enterprises need to put in place seamless, integrated and flexible security solutions that enable them to stay ahead of emerging threats without constraining agility or hampering end-user productivity.

AUDIT YOUR ENVIRONMENT

Organisations should conduct regular audits of their IT security risks, practices and infrastructure to ensure that they are well prepared for emerging threats and dangers in a fast-changing regulatory and security risk landscape. This process will help pinpoint potential vulnerabilities or gaps in compliance with standards (ISO/IEC 27001) and regulations (like PCI-DSS); highlight opportunities to improve operational efficiencies; support the formulation of appropriate security policies; ensure the organisation is updated with the latest security best practices; and create incident response and continuity plans in case of a breach.

BUILD CROSS-FUNCTIONAL PARTNERSHIPS

Since information security affects every function, process and system in the enterprise, it cannot be the sole responsibility of the CIO and the IT department. IT leaders should build close relationships with risk & compliance, finance, legal, HR and other competencies to shape policies and processes that align with regulatory mandates and data protection requirements. This can help to ensure buy-in from security and to tighten protections without unduly impeding end-user experiences and productivity.

FOCUS ON END-USER EMPOWERMENT AND EDUCATION

An enterprise's investments in the latest and best information security solutions will be for naught if an end-user accidentally gives his or her credentials to a phisher or uses a password that an attacker can easily guess. Robust information security is not just built on processes, systems and policies — it is also based on end-user awareness and a culture that embeds secure behaviour into the business.

IT departments can work with business unit heads and HR to drive security education programmes that help end-users to not only understand the rules and processes, but also why they are important.

Against the backdrop of the new work-from-home normal, it becomes even more important to ensure employees are empowered with information that helps them make good judgment calls around information security.

SHARPEN ENDPOINT PROTECTION

Most enterprises traditionally focused on perimeter-based security as the established model for keeping data and systems safe.

However, as they shift towards more remote working, they need to focus on creating secure and sustainable ways of managing devices used outside the premises.

This includes putting in place a solid mobile device management platform to ensure the IT team can monitor devices remotely, enforce compliance with corporate security standards, and make sure the devices are equipped with the right security software (including antimalware) and the latest patches.

EMBRACE AUTOMATION

The high cost and scarcity of information security professionals mean it can be attractive to automate security operations using today's tools, especially with AI and machine learning offering increasingly powerful ways to detect and respond to professional threats.

Automated tools can save a wealth of time for the security team while helping to improve outcomes — from basic patch and vulnerability management to sophisticated security information and event management (SIEM) platforms that identify, categorise and analyse incidents and events based on vast quantities of data from multiple security systems.

LEVERAGE SPECIALIST SKILLS

Few companies can keep up with the rapid pace of change in the security and privacy landscape, including new regulatory and legal requirements and the emergence of complex new security threats. It is also expensive for them to build up their own in-house capabilities to manage an area as complicated and specialised as security.

For most, the optimal route is to partner with best-of-breed vendors and service providers who have the focus and resources to stay ahead of the latest trends in the security sector.

BUILD A MORE RESILIENT ORGANISATION

CIOs and CISOs will partner with risk & compliance, HR and other functions to monitor threats to business information, systems and continuity. The goal will be to create an organisation with the resilience to rapidly recover from any breaches or outages, while mitigating the impact that such incidents have on customers, business continuance and reputation.

04

PARTNERING WITH BCX TO SAFEGUARD YOUR ENTERPRISE

BCX has the experience and expertise to secure even the largest and most complicated enterprise network. We can audit the current state of your infrastructure and applications, identify your readiness for the transition to a secure digital business model, set your objectives for the future, and plot a course from your as-is-state to your 'cyber-secure' environment of tomorrow.

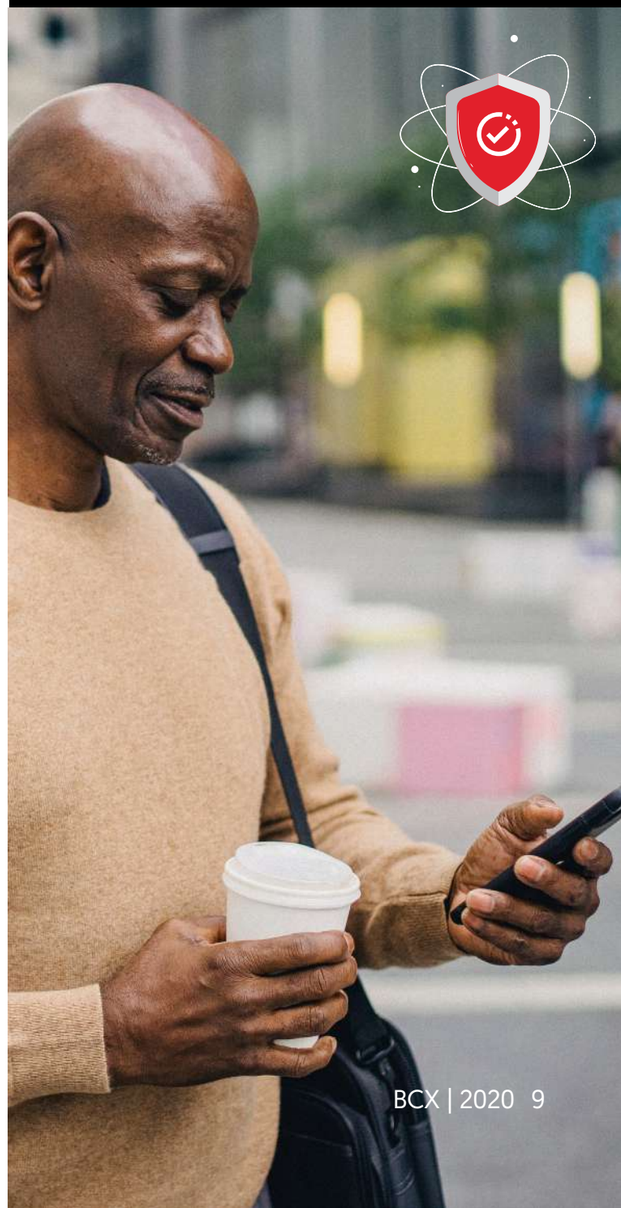
We have helped many clients on this journey – and during the pandemic, we transitioned our own staff complement of 4,500 people to secure remote working. From auditing and assessing your security environment to managing day-to-day security operations to strategic consulting, we offer a comprehensive portfolio of security solutions:

- BCX's **Security Advisory and Governance** services can evaluate your infrastructure and security policies, making appropriate recommendations and providing detailed reports for your peace of mind.
- Our **Managed Security Services** department will provide the tools needed to detect suspicious activity across your network, defend your computers from viruses and intercept malicious attacks on your endpoints.
- BCX's **Security Monitoring and Detection** team can help ensure that your IT infrastructure is properly secured.
- You can work with BCX **Risk, Audit, Assurance & Compliance Services** for expert advice around legal and regulatory mandates, contractual obligations, internal policies and best practices.

As Africa's premier end-to-end digital solutions partner, BCX has the skills and solutions required to help organisations – no matter how large or complex – to securely transition to digital modes of working.

Our experts in your vertical market can work alongside your business, HR and technology teams to review your current infrastructure and your goals for the future.

Contact BCX on [email] to arrange a meeting with one of our account executives to learn more.



REFERENCES

1. "Ransomware hits Johannesburg electricity supply", BBC, July 26, 2019. https://www.bbc.com/news/technology-49125853

2. "Carpet-bombing' DDoS attack takes down South African ISP for an entire day", ZDNet, September 24, 2019. https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/#:~:text=All%20the%20attacks%20that%20have,the%20DDoS%20amplification%20attack%20term.

3. "Experian says it may have found hacked data online after breach", Business Day, September 3, 2020. https://www.businesslive.co.za/bd/companies/financial-services/2020-09-03-experian-says-it-may-have-found-hacked-data-online-after-breach/

4. "The average cost of a data breach in South Africa", BusinessTech, September 10, 2019. https://businesstech.co.za/news/enterprise/339763/the-average-cost-of-a-data-breach-in-south-africa/

5. "Research shows how SA turned to e-commerce during lockdown", TechCentral, July 27, 2020. https://techcentral.co.za/research-shows-how-sa-turned-to-e-commerce-during-lockdown/99964/

6. "The 4 best Internet of Things stocks to buy", InvestorPlace, July 17,2020. https://investorplace.com/2020/07/the-4-best-internet-of-things-stocks-to-buy-now/#:~:text=A%20May%20report%20from%20Fortune,[CAGR]%20of%2024.7%25.

7. "Attack Landscape H1 2019: IoT, SMB traffic abound", F-Secure, 9 December,,2019. https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/

8. "Insider threats have increased 47%", Panda, February 6, 2020. https://www.pandasecurity.com/mediacenter/security/cost-insider-threat-report/

9. "The year of social distancing or social engineering?", Kaspersky, August 18, 2020. https://kaspersky.africa-newsroom.com/press/the-year-of-social-distancing-or-social-engineering-phishing-goes-targeted-and-diversifies-during-covid19-outbreak-with-2-million-attacks-in-q2-in-africa?lang=en

10. "Merck cyberattack's $1.3 billion question: Was It an act of war?", Bloomberg, December 3, 2019. https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war

11. "WannaCry ransomware attack", Wikipedia, retrieved September 20,2020. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Find us:
BCX/@BCXworld

www.bcx.co.za

Tel: +27 0861 520 521 | Web: www.bcx.co.za