accenture

BUILD PERVASIVE CYBER RESILIENCE NOW

Securing South Africa's Future Enterprise Today

COMPANIES ARE RACING INTO THE DIGITAL FUTURE—ADOPTING TECHNOLOGY-ENABLED OPERATING AND BUSINESS MODELS THAT DRIVE GROWTH.

They are not prepared for the new cyber risks that come with the connected, data-driven future enterprise. To be cyber resilient, organisations need to infuse security into everything they do—and every new thing they are preparing to do in the future.

ABOUT THE AUTHORS

Wandile Mcanyana

Security Lead: Accenture Africa

Wandile is a Senior Manager and Lead in Accenture's Security Africa practice with two decades information security experience in the financial services sector as well as with a number professional services firms. Wandile has a proven track record of delivering information security initiatives, programmes and solutions across varied industry verticals.

Clive Brindley

Senior Manager Security: Accenture Africa

Clive Brindley is a technology professional with over 25 years' experience, fusing a background in operational hands-on management with executive leadership. Clive has delivered projects spanning IT transformation and management in various business segments, from Defence to Financial services. Clive holds a Masters in Strategic IT Management and has over the past 5 years worked across Information Risk domains including data security, cyber defence and operations.

Yusof Seedat

Thought Leadership Director of Accenture Research

Yusof leads Accenture's strategic research geography business globally. His core focus is to help and advise Accenture and its clients lead in the NEW by supporting strategic decision making with data and insights, as well as guiding market positioning through thought leadership. He has co-authored several thought leadership papers on business and social related topics which can be accessed on the Africa Observatory.

Madhu Vazirani

Principal Director of Thought Leadership at Accenture Research

She has extensive experience in research and strategy consulting at the intersection of business and development. She is a thought leader focused on ecosystems and technology-led advancements for greater good.

WHEN EVERYTHING IS DIGITAL, EVERYTHING IS AT RISK

74% of South African executives agree that cyber risks will grow substantially in the next few years as a result of business becoming more connected, intelligent, and autonomous.

Around the world, companies are betting on a wholesale shift to tech-enabled business and operating models that promise to deliver bottom-line savings and top-line growth.

The connected, intelligent, and autonomous enterprise also comes with additional cyber risk. All that sensitive data, connectivity, and automation multiply the opportunities for hackers by expanding the "surface area" exposed to cyber attack. And, because digital systems are so embedded in daily operations, the potential damage from even a single security incident is magnified.

The threat is so significant that if cybercrime was a nation, it would be the 27th biggest in terms of GDP, and cost the global economy close to $450 billion a year.[1] In South Africa, the threat of cybercrime is frightening. Consider this:

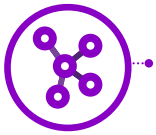
- South Africa reportedly has the third-highest number of cybercrime victims worldwide, losing over R2 billion a year to cyber attacks—the worst in Africa.[2]
- 70 percent of South Africans have fallen victim to cybercrime and other risky behaviour, compared to 50 percent globally.[3]
- 47 percent of South African smartphone users have experienced mobile cybercrime in the past 12 months, compared to 38 percent globally.[4]

We have seen the massive impact that data leaks from unsecure websites can have on major organisations and how easily insurers can fall victim to cybercrime. And let's not forget the infamous WikiLeaks group that hacked into South African banks and released the uncensored Competition Commission report in 2009.

South African businesses today are not only challenged by a fragile socio-political environment, they're also starting to fall prey to sophisticated attacks that can cripple them. Often, the reputational damage alone—including waning customer loyalty—can impose significant indirect costs on the enterprise.

In a recent Accenture survey of over 1,400 C-suite executives from around the world, including more than a hundred from South Africa, respondents agreed that new technologies would raise cyber risk. Nearly 90 percent of executives in South Africa have adopted or plan to adopt technologies such as cloud and the Internet of Things (IoT). Seventy-four percent of executives agreed or strongly agreed that cyber risks will grow substantially in the next few years as a result of business becoming more connected, intelligent and autonomous.

CONNECTED



ALWAYS ON, ALWAYS VULNERABLE

The future business relies on 24/7 connectivity to carry out internal processes, work with partners, and reach customers. Companies are linked electronically across value chains and supply chains with a growing universe of suppliers, partners, distributors, customers, and other external parties—increasingly over wireless networks and over long distances. In addition, with the rise of the Internet of Things, companies are also using digital connections to retrieve data and manage equipment in the physical world.

In the global survey, 77 percent of respondents cited the IoT as the technology that will increase cyber risk moderately or significantly. In South Africa, even more respondents—85 percent—cited the IoT as a potential source of cyber risk. Companies are installing IoT technology to control factory machines and manage physical environments—for example, turning off the lights and heat in a meeting room when sensors detect that it is unoccupied. The IoT is also being used extensively in supply chains to increase operational efficiencies, manage and track assets and monitor vital processes.

Cloud computing—using remote computing and storage facilities and services—was cited by 70 percent of respondents as posing a growing risk. Increasingly, companies rely on cloud setups to gain greater flexibility in IT operations and to access specialised services, such as AI analysis. Cloud computing is also used behind the scenes in many smartphone apps to do the data crunching that a phone can't do, creating another potential vulnerability in the Bring Your Own Device (BYOD) or virtual work environment, which was cited by 67 percent of companies in South Africa as another potential cyber risk.

Top executives in South Africa are also highly concerned about the potential dangers of sharing data with third parties. In our survey, nearly 60 percent of respondents said they expect data exchanges with strategic partners and other third parties to raise cyber risk, and 90 percent of C-suite leaders anticipate that the number of third parties and strategic partners in their ecosystems will increase in the next three years.

Companies also expect to make and sell many more connected consumer devices—everything from connected cars and "smart" appliances to wearable health monitors and even Internet-enabled pacemakers. These products introduce potentially catastrophic cyber risks—expanding the risk from monetary and reputational loss to possible loss of life and physical disruptions. Nearly 90 percent of South African executives recognise that smart products and connected devices would raise cyber risks for their companies.

INTELLIGENT

MORE DATA BRINGS MORE RISK TO PRIVACY AND IP

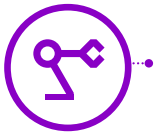
Intelligent systems use a combination of advanced technologies, such as artificial intelligence (AI), and large data sets to take on tasks once performed by humans, and to do things that humans cannot easily do—like finding hidden patterns in massive files of social media data that point to changes in consumer preferences.

Using AI and machine learning, companies can extract ideas for new ways to boost sales—a tweak in pricing, a design refresh, or a custom offer for specific shoppers. Behind the scenes, intelligent systems enable continuous improvement in operations—for example, optimising how production machinery is used or raising customer satisfaction in the call centre by analysing performance data.

Executives from companies represented in our survey are well aware of the risks that they are assuming with the wider use of intelligent technologies. More than 85 percent of South African executives cited cybersecurity concerns regarding AI, making it the riskiest new technology in their view. The same AI technology that enables banks to create sophisticated profiles of individual consumers to customise loan offers can also be used by hackers to track consumers' online activity to steal account passwords.

Given the intersection of AI, machine learning and big data within businesses, companies will need to address both security and privacy risks. Protecting larger amounts and new kinds of sensitive data is a major concern for executives. Three-quarters of respondents in South Africa, the same number as global respondents, said they believe that storing business-critical information, such as corporate strategy, trade secrets, and intellectual property (IP) on their systems will increase cyber risk; 65 percent have similar concerns about the risks they face in trying to protect sensitive customer data.

AUTONOMOUS



SELF-DIRECTING SYSTEMS ALWAYS NEED PROTECTION

In the future business, a good deal of work is done autonomously. The most obvious form of autonomy is robotics—the cognitive systems used to perform difficult, repetitive, or dangerous tasks in production processes. Nearly 60 percent of respondents in South Africa say that robotics will be a growing source of cyber risk. As was the case with IT systems, security was an afterthought in the creation of robots. But unlike a computer system, a powerful self-directed robot that is hacked could put employees in grave danger.

Autonomous machines are spreading rapidly beyond the factory. Flying drones are being dispatched to inspect power lines and refinery pipes. In the back office, robotic process automation (RPA) is being introduced to standardise and streamline a wide range of business processes. Often, this involves autonomous machine-to-machine communication, such as automatically generating an order in a supplier's computer when the procurement system signals that inventory is running low.

Businesses also rely on application programming interfaces (APIs), which two-thirds of South African respondents say will increase cyber risk. Open APIs used in platform-based business models, such as the Apple app store or the Alibaba eCommerce platform, enable third-party developers to interact with the company's systems and data to design their own applications—such as iPhone games or AliExpress shopping apps.

A less obvious form of autonomy involves employee activity. Increasingly, companies are using virtual work arrangements for contractors or employees who work remotely, often using their own devices. These "mobile workers" interact with company systems and data over public networks, raising cyber risk. In South Africa, 62 percent of respondents said that remote work arrangements would create additional cyber risk, only slightly less than the two-thirds of respondents in the global sample.

TODAY'S SECURITY STRATEGIES ARE NOT WINNING—THE LAST WAR

The future is arriving before companies have developed a broad perspective on the cyber risks, responses, and remediation plans that are required in the new business environment. Today's security approach will not be enough to win tomorrow's battles. The connected, intelligent, autonomous business needs pervasive cyber resilience—with proven methods for keeping cyber attacks from crippling the business and security baked into everything the organisation does. Security expertise must be dispatched to the front lines and security must be embedded not only in IT, but in product design, business processes, and the daily work of employees as well.

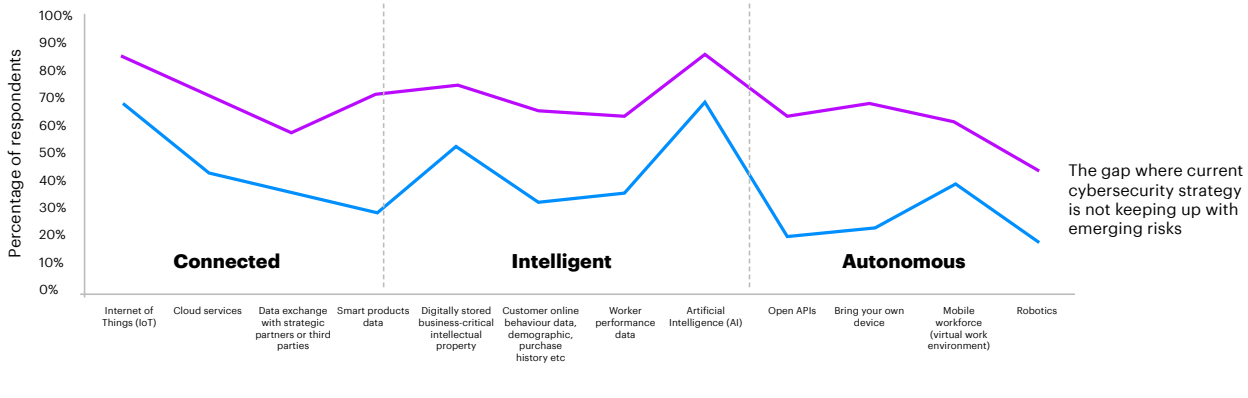
Closing the gap between risk and protection

There is a growing gap between the risks that companies are assuming and their cybersecurity posture or strength. Companies are not hesitating to race ahead with investments in new tech-enabled ways of doing business, often in response to competitors and "disruptors" in their markets. But there is a disparity between what C-suite executives say are the emerging areas of concern and the cybersecurity strategies employed. For example, while companies say that the growing volume of data exchanged with third parties is a risk, few companies attempt to ensure data integrity beyond their own operations. Forty-one percent of companies in South Africa rely on the protocols of the third parties or simply trust third parties to protect information that they share.

Figure 1

THERE'S A WIDE GAP BETWEEN RISK AND PROTECTION

There is a consistent pattern of gaps between awareness of growing risks and the protection afforded by current cybersecurity strategies



Source: Accenture Survey 2018, see "About the research"

As Figure 1 illustrates, our survey data exposes a consistent pattern of gaps between awareness of growing risks and the protection afforded by current cybersecurity strategies. For example, 64 percent of respondents in South Africa say that open APIs will raise cyber risk, but only 20 percent said that open API technology is protected by their cybersecurity strategy—indicating a wide gap of 44 percent between awareness of risks and their protection. In South Africa, wide gaps are also found in smart products and customer data, and the BYOD/virtual work environment.

To close the gap between current capabilities and future cyber resilience needs, companies must update the way they plan and execute cybersecurity. Companies today are waging war with outdated, backward-looking battle plans. For example, 92 percent of companies in South Africa base their cybersecurity investments solely on today's known risks and cybersecurity needs, and do not consider future business needs in the investment plan.

8%

of companies draw up security budgets based on past, present, and future risks

In general, companies are not governed, organised, and managed to deal with the pervasive risks of the future business. Responsibility for security is left largely to the chief information security officer (CISO) and the cybersecurity team, and it's not surprising to learn that half of CISOs feel their responsibilities for securing the organisation are growing faster than their ability to address them. Business-unit leaders are rarely asked to build security into product designs or other offerings—or held accountable for cybersecurity.

1/2

of CISOs admit that their responsibilities are growing faster than their ability to address them

While most companies have hired a CISO or assigned cybersecurity to a C-suite executive, such as a CIO, these leaders often have limited impact beyond the security organisation. Nearly half of respondents in South Africa say the CISO is brought into discussions only after a new business opportunity has been agreed by top management, for example.

Companies are doing little to spread security knowledge among employees and to create a "security-first" culture that will support pervasive cyber resilience. Only 29 percent of CISOs in South Africa—fewer than the low 40 percent at global level—said establishing or expanding an insider threat programme is a high priority.

HOW TO PROTECT THE FUTURE

To make the future business cyber resilient, companies must prepare for the risks that come with new business models and technologies, such as artificial intelligence and machine learning. Many C-suite respondents in our survey expect cybersecurity risks to diminish substantially in the next few years, thanks to new cybersecurity technologies.

But new technologies alone will not do the job. To build the pervasive cyber resilience needed for the intelligent enterprise to grow safely, companies need to embed security into everything that they do. Companies must instill a "security-first" mindset—connecting security to the business, making security everybody's job, and extending protection beyond the boundaries of the enterprise.

Companies can start by developing a coherent cyber strategy and investment plan that focuses on the key issues of data governance and protection. They will need to disperse security expertise and accountability across the organisation, educate the workforce and customers, and work with strategic partners, third parties, and industry alliances.

We identify five ways to start building pervasive cyber resilience:

1 Make the business leader a trusted security partner.

Today, cybersecurity tends to be highly centralised. Just 19 percent of companies in South Africa make business-unit leaders accountable for cybersecurity, even though business units are developing their own data-driven processes and conducting business online without involving the CISO at times. Business leaders should be held accountable for the security of their products, services, and operations—and be given incentives to embrace cybersecurity.

To disperse expertise, companies can create new security roles within business units to help with product design or protections for consumer data, for example. General Electric is one company that has created CISOs for region and business units. A primary goal for these frontline CISOs is to weave security into the product life cycle, ensuring that GE's products are secure and the people and organisations using them are protected.

2 Make the security leader a trusted business enabler.

Many companies have hired CISOs or other C-level executives to take charge of cybersecurity. But few security chiefs exert influence across the organisation. This is owing to many factors, including a lack of understanding of cyber risks among business executives, and sometimes, a failure by CISOs to take the initiative to collaborate. Only 34 percent of South African companies surveyed said that their CISO and business leaders collaborate on a cybersecurity plan and budget.

Security must be in the room when strategy is being decided and options are being weighed. Over 80 percent of executives in South Africa agree that the CISO will need a seat at the table when discussions about strategy, new businesses, and new technology adoption are taking place among business leaders. AT&T's Security Advisory Council, for example, is a forum that brings security and business leaders together to address strategy and security priorities.

While CISOs and other security professionals are doing a good job defending companies against well-established threats, new roles and skills are needed to implement pervasive cyber resilience. One approach that reflects the wide-ranging needs of the future business is the creation of a "Chief Digital Trust, Security, and Resilience Officer" who can oversee security in the broadest possible context and serve as a bridge between security and business units, as well as with the CEO and board.

3 Make employees part of the solution.

Cybersecurity experts polled by Accenture say that, after outside attacks, they are most worried about accidental or intentional acts by employees that compromise security, such as publishing confidential data or sharing a password with a hacker. Few companies, however, have placed a high priority on engaging employees in the cybersecurity effort. Despite their concerns about employees' role in breaches, only 52 percent of companies in South Africa said all employees receive cybersecurity training upon joining the organisation and then receive regular updates throughout their employment.

Companies should make sure all employees are trained in the basics and given the tools to identify possible threats and assist in fashioning protections. For example, all Cisco employees go through the "Security Ninja" training programme, in which employees who master the basics earn a white belt certification. Software developers, engineers, and managers at Cisco can earn more rigorous green, brown, or black belt certification with modules customised to their roles, which focus on building products and services in a secure way.

1/2 of companies provide cybersecurity training to all employees

Training and reinforcement can reduce the risk of employees accidentally helping cyber criminals. To catch employees who are actively pursuing or abetting cybercrime, companies can monitor employees, in addition to using standard data protection techniques. User and entity behaviour analytics (UEBA) systems, for example, can flag suspicious employee activity, such as unusual file transfers that could indicate criminal intent.

To enact an effective insider threat programme, the CEO must rally human resources, learning and development, legal and IT teams to work closely with the security office and business units.

4 Be an advocate for customer protection.

Digital trust and privacy are becoming major factors for consumers in their purchase decisions. Consumers are now alert to the privacy cost of using social media, consuming free content, and shopping online. Companies in our survey say that managing customer requirements for data protection is the second most urgent priority for their cybersecurity investments, just after their top priority of preventing high-profile incidents.

Companies must make security a top priority in the design and development of connected products and services. Companies must also assure their customers that their data is not going to be abused and educate customers about data protection, going beyond regulatory compliance to build trust. Consider Danske Bank's "Keep It Safe" programme, which helps customers learn how to protect their data. The programme provides advice on simple everyday routines and procedures that can protect consumer data and gives customers a way to test their computer security. The bank uses humour and a friendly communication style to make the material more accessible to consumers.

Companies that make the effort to educate customers about how to protect themselves and are transparent about what they do with customer data will be rewarded. Turning this into companywide practice will take a clear mandate from the top.

5 Think beyond your enterprise to ecosystem.

The future enterprise might conduct business electronically with hundreds or even thousands of suppliers and partners around the world, each of which can expose the company to a cyber attack. Companies need to work with these ecosystem partners to jointly protect their organisations.

Companies should work with partners to establish mutually-accepted rules (which can be backed up in contracts) for protecting the data they share. Companies should also participate in the standards efforts that are underway in most industries and work across industries to share cybersecurity knowledge and services.

BT, for example, shares threat information with other large telecommunications companies such as Orange and Verizon, as well as with national security agencies. The progress on information sharing is also an opportunity to shape participation in standards organizations. In our survey, 51 percent of CISOs in South Africa said they are contributing to creating a cybersecurity standard for their industry. Over 80 percent of respondents said that they expect to collaborate with companies in different industries in the next three years to improve cyber resilience.

80% of executives expect to work with companies in different industries to share knowledge of cyber threats and security solutions

GROW THE FUTURE BUSINESS WITH CONFIDENCE

Companies are finding exciting new ways to run their businesses and drive growth with tech-enabled processes and business models. Top leaders can ensure the success of the connected, intelligent, autonomous business by making security a core competency across the organisation. If they do this, companies will not only keep the enemy at bay, they will also build trust with customers and partners and develop the bulletproof business processes that will make them stronger competitors. With pervasive cyber resilience, the future business can grow with confidence.

ABOUT THE RESEARCH

WHAT IS A CYBER RESILIENT ENTERPRISE?

In this study, we define the cyber resilient enterprise as: an organisation that brings together the capabilities of cybersecurity and business continuity, and has strategies to quickly respond to threats, minimise damage, and continue to operate in the face of attack. As a result, the cyber resilient enterprise can proceed with innovation in digital business models, strengthen customer trust, and grow with confidence.

ABOUT THE SURVEY

In early 2018, Accenture Security surveyed 1,460 executives to understand the extent to which organisations prioritise security in new business initiatives, whether their security plans address future business needs, what security capabilities they have, and their level of internal and external collaboration on security. These executives represent companies with annual revenues of US$1 billion or more from 14 industries and 16 countries across the world—including 107 executives from South Africa. Half of the respondents were Chief Information Security Officers or equivalent roles, while the remaining 50 percent were CEOs and other C-suite executives.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 459,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.
Visit us at www.accenture.com.

ABOUT ACCENTURE RESEARCH

Accenture Research shapes trends and creates data driven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients' industries, our team of 300 researchers and analysts spans 20 countries and publishes hundreds of reports, articles and points of view every year. Our thought-provoking research — supported by proprietary data and partnerships with leading organizations, such as MIT and Harvard — guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients. For more information, visit www.accenture.com/research

REFERENCES:

[1] http://rickcrouch.co.za/wp/cyber-crime-and-south-africa/

[2] SABRIC: https://www.iol.co.za/mercury/sa-has-the-third-highest-number-of-cyber-crime-victims-worldwide-15608267

[3] Norton: https://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html

[4] http://rickcrouch.co.za/wp/cyber-crime-and-south-africa/

Copyright © 2019
Accenture All rights reserved.

Accenture, its logo, and High Performance Delivered are trademarks of Accenture.

Accenture, its logo, and High Performance Delivered are trademarks of Accenture.

The views and opinions expressed in this document are meant to stimulate thought and discussion. As each business has unique requirements and objectives, the ideas should not be viewed as professional advice with respect to your business.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.