

# Cybersecurity

Issued by [Regent Business School](#)

18 Apr 2023

Recent studies<sup>1</sup> have shown that South Africa is experiencing a skills gap in the field of cybersecurity. As a forward-thinking higher education entity, [Regent Business School](#) (RBS) recently presented a webinar designed to help business leaders, from small business owners to corporate executives, understand the current cybersecurity landscape and learn the steps necessary to protect their organisations from potential cyberattacks. With the help of experts in the field, the webinar not only provided an overview of the cyberthreats businesses face, but also provided actionable strategies to mitigate cyber-risks. Attendees were empowered with a better understanding of the importance of cybersecurity and the steps necessary to ensure their organisations are as secure as possible.



“In the current digital world, security threats have become a major concern for businesses and individuals alike. Valuable insights into the latest cybersecurity trends and best practices, as well as the resources available to protect data and systems from malicious attacks were explored during this webinar which was by invitation to our alumni. A discussion around the potential risks and vulnerabilities associated with cybersecurity, and the steps you can take to stay safe and secure in the digital age,” commented Professor Osman Seedat, deputy dean at Regent Business School and moderator of the webinar.

New cybersecurity technologies are emerging to combat the increasing threat of cyberattacks on organisations, as they face the challenge of keeping their environments protected in the age of cloud computing and IoT (internet of things) devices. According to recent statistics, small and medium-sized enterprises (SMMs) are particularly vulnerable, with many lacking basic or any security measures to protect their systems.

One of the major challenges faced by organisations is the issue of cloud vulnerabilities, as more companies adopt the latest technologies hosted or managed in the cloud. However, not all organisations are prepared for the cloud adoption framework, leading to complexities and increased expenditure. Remote work has further complicated cybersecurity, with many employees connecting on networks outside of the organisation’s firewall, exposing sensitive data. Companies need to ensure that employees follow best practices, such as using a virtual private network (VPN), enforcing password policies, using multi-factor authentication and providing cybersecurity training.

“As individuals, we must take responsibility for our own online safety by setting goals and following best practices to protect our sensitive data. This includes identifying all connected devices, limiting unnecessary applications, using password

managers, and using public Wi-Fi with caution. However, small to medium enterprises must also prioritise cybersecurity by implementing policies and following frameworks like NIST Cybersecurity Framework. In the event of a breach, it's important to respond quickly and efficiently, while keeping clients and employees informed. Ultimately, cybersecurity is a team effort, and everyone must play their part," says Liaqat Wahid Hassan, managing director of Cyberedge Security, who was on the panel of experts.

Organisations must measure their cybersecurity effectiveness, list their current capabilities, identify vulnerable assets, and practice regular patching and updates. In the event of an attack, organisations should be able to know their response time and the time it will take to remediate the issue.

According to another panel expert, Craig Law, chief information security officer of corporate and investment banking at Standard Bank, the onus is on you to protect yourself from cybercriminals. He stressed the importance of recognising phishing emails and social engineering through social media: "As technology continues to evolve, cybercriminals have found new ways to steal personal information and commit fraud. Phishing emails and social engineering through social media are two common tactics that these criminals use to deceive people. Phishing emails are fraudulent emails that appear to be from legitimate sources, but in reality, they are sent by cybercriminals to steal personal information. Social engineering through social media involves creating fake profiles or posing as legitimate individuals or organisations to gain the trust of targets. Once trust is established, attackers may request personal information or convince victims to click on malicious links.

"It is crucial for people to be aware of these tactics to prevent the devastating consequences of falling victim to them. By staying vigilant and learning to recognise these tactics, individuals can better protect their personal information and avoid falling victim to fraudulent schemes. Don't become a victim of cybercrime. Stay informed, stay vigilant, and protect yourself from phishing emails and social engineering through social media," Law warned.

Emerging technologies such as artificial intelligence and machine learning are set to revolutionise cybersecurity by offering advanced predictive abilities that monitor user behaviour without human intervention. These technologies will be widely used in the coming years to make cybersecurity stronger and more powerful.

With the adoption of these emerging technologies, organisations will have the tools they need to stay protected from cyberattacks and ensure their cybersecurity best practices. As technology continues to evolve, it is imperative that organisations remain vigilant and proactive in implementing the latest cybersecurity solutions to stay ahead of potential threats.

*Reference 1: Fortinet's 2023 Cybersecurity Skills Gap report based on a survey of over 1,800 IT and cybersecurity decision-makers from 29 countries, including South Africa.*

**Become future-ready by joining one of accredited MBAs, postgraduate qualifications, degrees, diplomas, or higher certificates! All 2023 students will receive a free Management Development Programme valued at R7,000. T's and C's apply.**

**Regent Business School celebrates the exceptional achievements of its first cohort of DBA graduates** 9 May 2024

**Regent Business School's webinar: Thought-provoking National Budget 2024 analysis** 5 Mar 2024

**Building a strong personal brand in the digital age: Insights and strategies** 18 Dec 2023

**Celebrating 25 years of RBS - A legacy of excellence in higher education** 2 Nov 2023

**Empowering tomorrow's workforce: Thriving in the talent battleground** 10 Oct 2023

## Regent Business School



Regent Business School was established to satisfy the demand for management education in southern Africa.

[Profile](#) | [News](#) | [Contact](#) | [Twitter](#) | [Facebook](#) | [RSS Feed](#)

For more, visit: <https://www.bizcommunity.com>