IMAGE: Envato Elements

BY EUGENE YIGA

Global Threats, Local Challenges

The increasingly complex problems in cybersecurity require a new mindset to solve them.

As chief information security officer of the MTN Group, Justin Williams has led this function for over eight years. But even though he's transformed security across the telecommunications organisation, much like he did as executive director responsible for cybersecurity at EY, it can be hard to keep up.

"There's so much happening in the world around us, with numerous pressures that translate into activities impacting us directly," he says. "We're constantly alert, monitoring everything closely and reacting to every little thing before it potentially escalates. There are teams on standby and on call 24/7, monitoring all that's going on. This creates a low-grade stress, constantly present, with the concern that something could happen at any point in time, or something happening could be bigger than it seems."

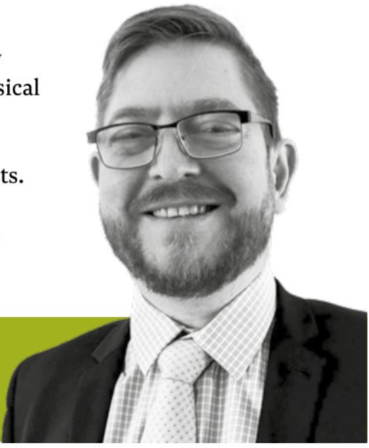
For Williams, one growing concern is the rise of generative AI and large language models (LLMs). He describes the rate of progress as absolutely phenomenal, highlighting both the advancements and potential risks.

"An alarming aspect emerges when looking at hacker channels where malicious users manipulate these models," he says. "By removing the ethical guardrails, they enable the AI to respond to queries it would typically refuse due to potential harm. This creates a significant disadvantage for defenders, who are fighting with one hand tied behind their back, while attackers exploit the model capabilities without restraint."

Telecommunications companies are evolving

Another challenge is the fact that security elements can't be separated from the physical world in which we operate. Over the last few years, many global hotspots have emerged, each hosting a variety of conflicts. Each incident impacts the perceptions of organisations and countries, which alters the nature and identity of threat actors.

'Something could happen at any point in time.'



Justin Williams

One growing concern is the rise of generative AI.

"Whether it's global conflicts or localised regional conflicts, someone somewhere is using what's happening," Williams says. "As telecommunications providers, being critical national infrastructure, someone with a point to prove will target us to convey their political message. We've certainly seen heightened activity as a result of that."

Williams has also seen a shift as telecommunications companies evolve into tech and platform entities. This requires him to confront both traditional telco threats and new challenges emerging from adjacent sectors. Indeed, the transition into cloud computing, virtualisation, and the incorporation of AI and LLMs into customer service chatbots introduces a whole new spectrum of security threats.

"These are not challenges that can be tackled in isolation," he says. "So there's a heavy reliance on third parties in the supply chain. All of these elements come together, and it's clear that one can't even think of handling it alone. If you try to do so, you're going to fail, and fail quickly. However, collaboration can become problematic when entities refuse to share information due to geopolitical issues. We'll have to see how that all plays out."

Finding talent isn't easy

What makes all this harder is the fact that there's a major talent shortage, a reality that is particularly striking across all markets in Africa. Despite occasionally finding brilliant individuals, Williams has

CYBERSECURITY TIPS

As the former executive assistant director for the FBI Information and Technology Branch, James Turgal has more than two decades of experience in investigating and solving cybercrimes. He now serves as Optiv Security's vice-president for cyber risk, strategy, and board relations. He has also personally helped many companies respond to and recover from ransomware attacks. Here are his top cybersecurity tips.

Shift your mindset.
For too long, companies have dismissed cybersecurity because they viewed it as a cost centre and business inhibitor. Companies adopting this mindset typically do what's required to check the box on the compliance front but fail to put security and resilience strategies in place until they are forced into action by a cyber incident. By then, it's too late. That's why companies need to shift their mindset to view cybersecurity and cyber resilience as powerful ways to maintain business continuity in the face of any type of data loss event.

Identify the crown jewels.
With this new mindset, companies can start getting proactive about cybersecurity and resilience. The attack surface of a company has grown considerably with the cloud, the "bring your own device" trend, the work-from-home movement, and other digital transformation initiatives. That means it's now impossible to protect everything within an organisation. To make things more manageable, companies must identify the assets that are most likely to be targeted by cybercriminals and protect those first.

Put a plan in place.
With a newfound understanding of the most critical assets, companies can determine their appetite for risk and then implement security and resilience strategies accordingly. Plans should be based on the company's current IT and business landscape and include basic technologies such as identity controls, multifactor authentication, vulnerability management, anti-malware, patching, encryption, application whitelisting, monitoring, network segmentation and data loss prevention.

Enforce governance.
Companies should ensure security teams implement monitoring and benchmarks so that they and leadership can keep tabs on how cybersecurity and resilience plans are performing. This way, they'll know what may need to be adjusted to align with changing business demands and security threats as well as how they are enabling the business with secure operations.

Learn from every incident.
Even with strong cybersecurity and resilience plans in place, no company is immune from cyber risk. If a cyber incident happens, instead of playing the blame game, take it as an opportunity to improve the business. Gather all stakeholders involved, assess what went wrong, and determine strategies to prevent it from happening again.

Learn more: https://www.optiv.com/

seen how the scarcity of such talent leads to shortages that persist for extended periods.

"We are hopeful that by using technologies like [Microsoft] Copilot and similar tools, we can supplement the skills of individuals, making them more effective in their roles," he says. "These technologies provide access to vast knowledge bases without requiring individuals to spend an exorbitant amount of time sifting through information. This represents the positive side of leveraging technology. However, the ongoing challenge lies in continually developing people for various programs to ensure we can find even a glimpse of the needed talent."

Looking ahead, given the difficulty of navigating the overwhelming amount of information, Williams believes that staying on top of cybersecurity concerns requires breaking through all the noise to find what matters most. Often, a cybersecurity incident becomes sensationalised once a journalist reports on it, which leads to a flurry of headlines. But upon closer examination, what seems like a new problem may actually be an old or misrepresented issue that's been seen before.

"The rapid spread of such articles, when people want immediate responses and assessments of implications, can be distracting and overwhelming," he says. "So to build trust within the organisation, we have to reassure everyone that we're monitoring everything in real time and will keep them informed about what's happening and its implications for us. This effort helps protect the technical teams focused on their day-to-day tasks from unnecessary diversions. It's unhelpful for them to be reactively addressing every piece of news, rather than proactively maintaining the control environment essential for the organisation's security."

Justin Williams is a CA (SA), MBA, CISSP (certified information systems security professional), CRISC (certified in risk and information systems control) and CGEIT (certified in the governance of enterprise IT). He is a previous audit committee and board member for ISACA South Africa and was awarded the Thomas H Fitzgerald Award for achieving the highest score for the CISA (certified information systems auditor) exam in December 2014.

RANSOMWARE CASE STUDIES

In early 2023, the notorious LockBit ransomware group struck financial services company ION. LockBit claimed that ION paid the ransom to restore its operations but there was no formal confirmation of this claim.

"ION didn't share a lot of details about the incident except the initial acknowledgement," says Ilia Sotnikov, a security strategist at Netwrix. "However, we can assess the consequences of this attack and qualify them as severe."

The attack specifically impacted the derivative clearance division and lasted for about a week until the company fully restored all service operations. This disruption impacted dozens, if not hundreds, of ION customers worldwide. Unable to use the software, some investment banks and brokers were forced to fall back on manual processes, extending the time required for trade transactions and compliance reporting.

"There are other notable security incidents in the financial sector worth mentioning," Sotnikov says. "The foreign currency exchange operator Travelex was hit by REvil ransomware on New Year's Eve in 2020. The attack caused a disruption for over a month (!) and impacted both Travelex exchange offices as well as several global banks that relied on Travelex for currency exchange operations. The firm reportedly also paid the ransom but was still unable to restore operations for weeks after that."

Another notable case was when the insurance company CNA Financial was attacked by Phoenix Locker ransomware group in March 2021. They also paid the ransom and needed weeks to fully restore operations. "All these stories are further evidence that paying ransoms doesn't guarantee fast recovery from the attack and will not return the business back on track swiftly," Sotnikov says.

Learn more: https://www.netwrix.com/

KEY TAKEAWAYS

Ransomware recovery

Jason Garbis, founder and principal of Numberline Security, shares these key takeaways:

1. Ensure you're ready to respond to a ransomware attack with regular, reliable, and tested system backup and recovery that's stored in a way that it's inaccessible to ransomware.
2. Enforce the principle of 'least privilege' on your network via Zero Trust based segmentation. A flat, open network allows ransomware to spread broadly and have a major impact, versus being contained within just a handful of machines.
3. Analyse third-party dependencies around critical business processes and make an informed decision about the risk and impact of their unavailability. GIBS

Learn more: https://numberlinesecurity.com/