BIZCOMMUNITY

The major cybersecurity trends of 2023

By Gerhard Swart

9 Jan 2023

Cybersecurity has become crucial as digital technologies change our world-whether for online banking, e-commerce, chatting on WhatsApp or working from home, we need online protection. Just as we lock our homes and safeguard our valuables, we must take measures that stop online criminals from taking what is not theirs.

Gerhard Swart, CTO of Performanta | image supplied

The battle against cybercrime is not new. But the world and South Africa have experienced a significant escalation in the past several years, leading to rapid evolutions in the security industry and a growing understanding among business leaders that they need to step up their engagement. Meanwhile, tried-and-tested attack methods are growing bolder.

These factors predict that 2023 could be a defining year for cybersecurity trends.

Phishing escalates and expands

Phishing is a method where criminals create fake correspondence to dupe victims into giving up account details or access to their systems. It remains the primary way for criminals to target us—according to Mimecast, phishing attacks targeted an astounding 94% of SA companies between mid-2021 and 2022.

The criminals are increasing their focus on financial targets, including banks and other areas such as e-commerce transactions, creating a 65% jump between Q1 and Q2 of 2022 (Kaspersky). Moreover, phishing activities have expanded beyond email to include SMS, phone calls, social media and WhatsApp messages.

Criminals are starting to offer 'Phishing-as-a-Service' products that anyone can use to launch such attacks. Phishing will continue to grow more widespread and dangerous during 2023.

Ransomware voids cyber insurance

Criminals use ransomware to encrypt company data and force businesses to pay a ransom in return for access to their files. Ransomware attacks have targeted major South African organisations, such as Transnet and the Justice Department, not to mention countless SMEs. Many companies pay the ransom, ultimately fuelling this practice. It is so endemic that Australia is considering making ransomware payments illegal.

Major organisations try to mitigate the ransomware risk by taking on cyber insurance, but this is a race to the bottom. In Q1 of 2022, cyber insurance premiums rose at an average of 37% and by a staggering 83% for some companies, according to Gallagher Consultants. The requirements for such insurance are already very stringent, and it's likely that in 2023 we'll see cyber insurance becoming untenable for most organisations, primarily because of ransomware.

Cloud architecture security gains prominence

Though not causation, there is a correlation between rising cybercrime activity and our adoption of connectivity and cloud services. Check Point's 2022 Cloud Security Report claims that 27% of polled organisations had experienced a public cloud security breach during the year. This result is likely conservative due to under-reporting and does not cover other areas such as hybrid and public cloud.

Most such attacks are avoidable, but organisations often make fundamental mistakes. Many still assume the cloud is naturally more secure, which is only partially true. Cloud systems often have more rigorous security, but these systems cannot cover all possibilities—especially regarding their clients' practices and internal systems.

Organisations must still rise to the challenge, ensuring they have proper security practices in place. We're seeing more of this attitude take root, and it will be a primary consideration for cloud users in 2023.

Security knowledge for business leaders

Cybersecurity is gaining a more prominent space in the minds of business leaders, who recognise the immense threat it poses to their operations and solvency. Part of this change is due to legislation such as the Protection of Personal Information Act, which places more punitive responsibilities on organisational leaders.

But recognition differs from the knowledge that helps embed cybersecurity as part of business thinking and strategy.

2023 is unlikely to be the year when we see senior business courses vividly incorporate cybersecurity as part of their education. Yet expect this conversation and requirement to expand. Such education is different from cyber hygiene and safety courses. We need more education that contextualises cybersecurity to specific roles. What should a CFO or COO understand? What must boards ask and know?

The scope is broad: CMOs should see cybercrime in the context of communications and social media. CXOs need to grasp how cybercrime manipulates experiences. This level of education should extend from executives' formal learning channels. Perhaps we'll one day see MBAs and business degrees with thorough cyber resilience modules—that would be a step in the right direction.

ABOUT GERHARD SWART

Gerhard Swart is the Chief Technology Officer of Performanta, a cybersecurity provider based in South Africa, Israel and the United Kingdom. Previously Performanta's Head of Sales Engineering and Senior Security Engineer at Dimension Data, Swart is highly qualified across numerous cybersecurity areas and business credentials, and is a Manchester Business School alumni.
- #BizTrends2023: The major cybersecurity trends of 2023 - 9 Jan 2023

View my profile and articles...