Employees working from home? The crippling effects of cyberattacks you may not be prepared for

As the Coronavirus (COVID-19) forces more people globally to work from home, we are becoming increasingly reliant on technology to live, work and play. However, many organisations are ill-equipped to deal with employees working remotely and the cybersecurity risks that come with it. However, with the commencement of South Africa's Protection of Personal Information Act, 2013 ("**POPIA**") on **1 July 2020**, it has never been more important to ensure the security of organisational data. How can companies protect themselves from this scourge? One way is by implementing the global standards set out in ISO Standards 27001, 27005 and 27032.

Unintentional and intentional human actions

In response to the ever-changing and complex nature of work and systems, organisations have a wide array of systems, controls, processes and procedures to safeguard client data and company intellectual property, such as firewalls, regular password changes and multi-factor authentication. However, these safeguards can be rendered ineffective if employees compromise them by, for example, accessing websites that are infected with viruses. Occasionally, and perhaps due to economic pressures experienced by staff (especially during the pandemic), employees may also find themselves on the other side of the law by intentionally colluding with cyber criminals to manipulate company systems and client data with the promise of financial reward.

Outdated legal frameworks

Companies like Life Healthcare, Honda, the World Health Organization, Nedbank, Amazon and Microsoft have all experienced incidents of cyberattacks this year. However, the law is not necessarily well-equipped to deal with this problem. For example, South Africa's current legislation dealing with cybercrime, primarily the Electronic Communications and Transactions Act, 2002, has not kept up with the dynamic and constantly evolving nature of technology and associated cybercrime. In addition, the new Cybercrimes Bill, which will codify numerous existing offences related to cybercrime and will create a variety of new offences, has still not been passed by parliament. Further complicating matters is that the effective investigation and prosecution of these types of crimes is complex, requiring specialist skills, and raises challenging issues of cross-jurisdictional cooperation between law enforcement agencies. As such, implementing measures to prevent a cyberattack from

happening in the first place should be a top priority for companies.

ISO guidelines

The International Organization for Standardization ("**ISO**") has issued a number of standards that provide information security risk management and cybersecurity guidelines for organisations. The focus of these standards is to address internet security issues and to provide technical guidance in addressing common internet security risks.

Risk assessment

ISO 27032 recommends that an organisation conducts a risk assessment to identify relevant risks. In conducting this risk assessment, some of the issues that should be considered are:

- Identifying critical assets: it is not cost-effective to protect all assets equally. It is therefore essential that critical assets are identified so that particular care may be taken to protect them. The designation should be made from a business context by considering what the impact on the business would be if the asset was lost or degraded.
- Identifying relevant risks: current risks faced in a business context, as well as additional and evolving risks, threats and attacks that may become relevant when participating in cyberspace, should be considered.
- System or service retirement: systems or services that are no longer required should be retired and all security-related information should be invalidated to ensure that interfacing or related systems are not compromised.
- Consistency: the approach to risk management should apply across the entire cyberspace.

Cybersecurity controls

A few of the cybersecurity controls recommended by ISO 27032 include:

- Server protection controls are used to protect servers against unauthorised access and the hosting of malicious content. These controls include server configuration to ensure appropriate access controls on programs and system directories, enabling audit trails on systems and regularly conducting audit trails. Implementing and running appropriate anti-virus and anti-spyware software on servers is also recommended.
- End-user controls include using the latest supported software applications with the most updated security patches to ensure that programs are secure and any known vulnerabilities have been addressed. Anti-virus and anti-spyware tools should be installed and appropriate safeguards implemented. Further controls include using phishing filters and enabling personal firewalls and host-based intrusion detection systems.
- Introduce policies that govern information security risk management, basic policies governing the creation, collection, storage and transmission of data, as well as corporate policy statements and penalties relating to the misuse of cyberspace applications.
- Organisations should include awareness and training as part of their cybersecurity so that they regularly and continually raise their employees' awareness to cybersecurity threats and how to identify and deal with these threats.

POPIA

Having a robust and organisation-specific cybersecurity plan is vital considering that South Africa has enacted POPIA, which will commence on 1 July 2020. POPIA obliges organisations to report data breaches and it is therefore essential that an organisation takes steps to manage the risk of a cyberattack materialising and to mitigate against any consequent harm.

Cyberattacks can have a crippling effect on organisations. Not only can they cause significant damage to reputation, impact on business continuity and result in the loss of sensitive and confidential information, but damages may also have to be paid to individuals whose data has been breached.

In part two of this article, we will discuss the most common types of cyberattacks and how to protect your organisation from them.

Suad Jacobs
Forensics | Executive
sjacobs@ENSafrica.com