WHEN THE TROJAN HORSE STRIKES: CYBERSECURITY MEASURES FOR YOUR BUSINESS

Category: IT Law,Technology Law
written by Tshegofatso Phahlamohlaka | November 10, 2025

The legend of the Trojan Horse tells how Greek soldiers, unable to breach the fortified city of Troy, turned to deception. They built a massive wooden horse, hollow inside, and presented it to the Trojans as a peace offering. Believing the war had ended, the Trojans pulled the horse into their city walls, unaware that it concealed their enemies. This ancient tale serves as a timeless reminder that threats often can disguise themselves as gifts. Modern “Trojan” malware operates on the same principle, appearing harmless or even beneficial while concealing malicious code designed to infiltrate and compromise systems from within. In the same way that the Trojans welcomed the wooden horse into their city, organisations today may unknowingly invite cybercriminals into their systems through deceptive emails, infected attachments, fraudulent websites, or compromised software updates, leading to data theft, financial loss, operational disruption, and reputational harm.

For this reason, understanding and defending against such hidden threats is not merely a matter of caution, however, it is a critical obligation to mitigate and prevent cybercrimes that could impact your business or organisation. The *Cybercrimes Act,* 19 of 2020 (the "**Cybercrimes Act**") imposes certain obligations to some institutions, including financial institutions, to implement measures that prevent and investigate cybercrimes and to report such incidents to the South African Police Service[1]. The Act further criminalises a broad range of cyber offences, including unlawful access to computer systems or data, unlawful interception of data, use of malicious software tools, and cyber fraud, forgery and extortion[2], all of which are modern manifestations of the Trojan Horse principle.

Businesses and organisations face a range of cybersecurity threats, many of which are specifically criminalised under Act. Understanding these threats from both an operational and legal perspective is important for compliance and risk mitigation. The following are a few common cybersecurity threats that businesses and organisations face and need to be aware of:

Social engineering threats

Social engineering attacks manipulate human behaviour to gain access to sensitive information.[3] In these types of threats, the attacker would usually pose as a wealthy individual such as a "Nigerian Prince" promising a reward for assistance. Individuals are often tempted to share specific information or perform a specific task as they are promised a reward for their assistance. Under the Act, such attacks constitute cyber fraud and are effective as they rely on the exploitation of human error or behaviour to extract certain information.

Ransomware

Individuals and businesses can fall victim of a ransomware through infected websites, attachments, emails, and links in messages.[4] Once the ransomware is downloaded on a device, it can quickly spread and corrupt the device or data or clock the user's access to the device. The attacker behind the ransomware will usually demand a ransom to be paid for the victim to regain access to the files or data.

Malware

Another example of a cybersecurity threat is malware which can take various forms, including viruses, Trojan horses, spyware, and worms.[5] It allows attackers to steal data, corrupt systems, or conduct unauthorised actions on devices belonging to individuals, businesses, or organisations. The creation, distribution, or use of malware is criminalised under unlawful acts in respect of software or hardware tools and can also involve unlawful interference with computer data storage or systems in terms of the Act.

Man-in-the-Middle (MITM) Attacks

Man-in-the-Middle attacks occur when an attacker intercepts communication between two parties without their knowledge, potentially monitoring, altering, or stealing data.[6] Usually, attackers target public Wi-Fi hotspots users by setting up fake Wi-Fi hotspots.

Insider Threats

Insider threats occur when an employee or contractor abuses their authorised access to sensitive information, either to commit fraud, steal data for personal gain, or otherwise cause harm to the organisation.[7]

Measures that Businesses and Organisations can Implement to Address Cybersecurity Threats

In order to mitigate or prevent cybersecurity threats, it is important for businesses and organisations to design and implement robust policies and practical measures. These measures not only protect systems and data but also ensure compliance with legal frameworks, such as the *Cybercrimes Act*, 19 of 2020 and the *Protection of Personal Information Act*, 4 of 2013. Some of the mitigation strategies include:

1. Regulation and Adoption of Policies

Depending on the size, industry and operation of the organisation, an organisation or business must consider implementing a compliance framework, which identifies industry-specific laws, maps the organisation operations against these laws and adopts policies to ensure compliance with such laws. Organisations must consider implementing clear cybersecurity policies that define how technology, data, and systems are used, accessed, and protected. Examples of such policies include Incident Response Policy and Data Protection and Privacy Policy.

2. Education and Training

Organisations must ensure that its employees are trained to identify potential threats, such as phishing, malware and ransomware. A common entry point for cybercriminals generally is through human error. Focusing on cybersecurity awareness and ongoing education are critical in reducing the risk posed by human error.

3. Access control

Businesses and organisations should restrict access to sensitive and confidential information to authorised persons only.

4. Investing in Cybersecurity

Organisations should maintain up-to-date systems and software, implement encryption on devices, and enforce strong password policies. Ensuring regular system updates, patching vulnerabilities, and investing in cybersecurity infrastructure are crucial to preventing security compromises.

5. Vigilance and Preparedness

It is not a matter of ***if*** a cyber incident will occur, but ***when***. As technology evolves, organisations must remain vigilant, continuously monitor for potential risks and maintain proactive cybersecurity measures to safeguard their systems and data.

The tale of the Trojan Horse reminds us that cybersecurity begins with vigilance and preparedness. The fall of Troy was not due to a lack of strength, but a failure to question what appeared harmless. Similarly, in the digital age, resilience lies in learning from the past and ensuring that no “Trojan Horse”, be it malware or a phishing attack find its way through your organisation’s gates.

---

[1] Section 54 of the *Cybercrimes Act*, 19 of 2020. This section has not yet come into effect.

[2] *Cybercrimes Act*, 19 of 2020.

[3] “What is Social Engineering” available at https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html.

[4] “Types of cyberthreats” available at https://www.ibm.com/think/topics/cyberthreats-types.

[5] “Types of cyberthreats” available at https://www.ibm.com/think/topics/cyberthreats-types.

[6] “Types of cyberthreats” available at https://www.ibm.com/think/topics/cyberthreats-types.

[7] “Types of cyberthreats” available at https://www.ibm.com/think/topics/cyberthreats-types.