Cyber security – what the board of trustees needs to know

Ndabezinhle Manzini,
Executive Head: Risk & Internal Audit,
NBC Holdings

The vast majority of business transactions and the storage of data are done on digital platforms.

In respect of retirement funds, key functions such as the maintenance of a members' individual records, monthly updates of contributions, investments/disinvestments and the payment of claims are all done on digital platforms.

The Global Initiative Against Transnational Organized Crime (GI-TOC) conducted a risk assessment of organised crime in South Africa. In their report of findings issued in September 2022, they state that according to Interpol during the period January 2020 to February 2021 South Africa experienced the highest number of cyber threat detections in Africa and the number of detections amounted to 230 million for that period alone.

It is therefore imperative that any entity that utilises digital platforms has cybersecurity mechanisms/systems in place to ward off cyber risks.

What is cybersecurity

Cybersecurity is the protection of computer systems and networks from attack by malicious actions that may result in the following:

- Unauthorised information disclosure.
- Theft or damage to hardware, software, or data.
- Disruption or misdirection of services conducted on computer networks or systems.
- Commission of cybercrimes that lead to financial losses.

Cybersecurity is attained using three processes

Threat prevention, detection and response.

These processes are based on various policies and system components which include the following:

- User account access controls and cryptography are put in place to protect system files and data. End-user training is key in ensuring that these processes work effectively.
- Firewalls are by far the most common prevention systems because they shield access to the internal networks of entities and block cyber-attacks. Firewalls are both hardware and software-based.
- Intrusion Detection Systems (IDS) are software-based products that are designed to identify network attacks and also assist in post attack investigations.
- Response refers to the actions that an entity takes to respond to cyber threats.

Retirement funds may be exposed to the following cybercrimes/vulnerabilities

- **Phishing** - This is a form of cyber-attack in which communication from a seemingly reputable source is sent to a target to "trick" them into disclosing sensitive information such as banking details or performing an action that could compromise their system. Phishing is mainly through SMS's, websites and emails.
- **Business Email Compromise (BEC)** - This occurs when attackers impersonate a senior person in the governance structures of an entity and send emails instructing junior staff to make payments into fraudulent accounts. BEC also entails the actual infiltration of business email accounts and thereafter the cyber criminals gather the information that can be used to commit cybercrimes.

- **Data breaches and leaks** - These occur when there is unauthorised access or disclosure of confidential data through the manipulation of individuals or the exploitation of vulnerable systems. The perpetrators may be individuals within the organisation.
- **Ransomware** - This involves the use of malicious software (malware) to encrypt an entity's data or lock the entity's system in order to disrupt its normal operations. A ransom payment is demanded by the attackers for them to decrypt the entity's data and allow the entity to regain access to its system. According to Interpol, South Africa was the most targeted country in Africa in terms of ransomware attacks in the first quarter of 2021.

The Board's responsibility

Section 7D(b) of the Pension Funds Act states that one of the duties of the Board is to ensure that proper controls are employed by or on behalf of the Board. Cybersecurity forms part of the controls that funds need to have in place and the ultimate responsibility resides with the Board. The Board may perform the following actions to ensure that cybersecurity measures are in place and are adequate to ward off cyber risks:

01 Conduct annual due diligence of current service providers. This can be done by way of a questionnaire in which the Board can ask the service provider to confirm that they still have cybersecurity measures in place as well as provide details of any enhancements done to those measures. The service providers should also be requested to provide details of any cyber-attacks that may have occurred.

02 For potential service providers, the Board should request details of their cybersecurity measures in place as part of the due diligence processes.

03 Cyber risks should be included in a fund's risk register and the Board should monitor that the cybersecurity measures in place remain effective in warding off cyber risks.

04 Cybersecurity measures include training end-users and the Board should include cybersecurity training in its training calendar.

Draft Joint Standard - Cybersecurity and cyber resilience requirements

The Financial Sector Conduct Authority (FSCA) issued a draft joint standard that seeks to set out minimum requirements for sound practices and processes of cybersecurity and cyber resilience within financial institutions. Key highlights in the draft joint standard include:

- Financial institutions will be required to have a cybersecurity strategy and framework.
- Guidance to financial institutions on the required regulatory reporting - as far as any cyber incidents that they may experience.
- Financial institutions will be required to have a governance strategy in place for cybersecurity and cyber resilience.
- Financial institutions will be required to carry out penetration testing at least annually to obtain an in-depth evaluation of their cybersecurity protection.