KPMG
Private Enterprise

Family Business Cyber:
Cyber-securing your family's legacy

Article 3 of 6

Cybercrime in South Africa is reaching new heights in 2025, with attacks becoming increasingly sophisticated and frequent. According to industry estimates, cybercrime is projected to cost the South African economy over R2.2 billion annually. This surge highlights the urgent need for stronger digital defences across all industry sectors. Traditionally legacy-driven and financially robust, family businesses are no exception. These enterprises often handle sensitive financial, operational, and personal data across a portfolio of investments making them high value targets.

Cyber Risks to the Family Behind the Business

For privately-owned family businesses, the risk considerations are not only for the business, but also for the family members behind the business. Personal information and online behaviour can expose families to physical threats and reputational damage, which in turn can impact the business.

Threats are not contained to the digital space unfortunately. In recent years, South African crime syndicates have adapted their kidnapping and extortion tactics, increasingly using cryptocurrency for ransom demands to minimize the risk of arrest and enhance the anonymity of transactions.

Common Cyber Threats Facing Family Businesses

Ransomware

Ransomware is a type of malicious software designed to restrict access to a victim's system or data until a ransom is paid. These attacks can be devastating, often targeting both business-critical and personal information. Phishing emails or compromised links are common entry points. Once activated, the malware locks users out and demands payment under the threat of data loss or public exposure.

A prominent example occurred in 2019, when Amazon CEO Jeff Bezos was reportedly hacked after receiving a malicious WhatsApp file from an account linked to Saudi Crown Prince Mohammed bin Salman, as reported by CNN Business.

Identity Theft

Identity theft involves the unauthorised acquisition and use of personal or corporate information—such as banking credentials or identification numbers—for financial gain. In family businesses, where personal and professional identities often overlap, such breaches can lead to unauthorised transactions, creation of fraudulent accounts, or resale of information on the dark web.

Deepfakes and AI-Based Impersonation

Thanks to advances in artificial intelligence, attackers can now create deepfake videos, audio messages, or images that convincingly impersonate real individuals. In a business context, this could involve a fake video call appearing to come from a company director, requesting an urgent fund transfer or sensitive data. These high-stakes impersonations are increasingly difficult to detect without advanced verification systems.

Social Engineering and Business Email Compromise (BEC)

Social engineering techniques manipulate individuals into revealing confidential information or authorising fraudulent transactions. Business Email Compromise (BEC) scams are on the rise in South Africa, where attackers gain access to or spoof executive email accounts to issue fake instructions, often targeting finance departments within small firms.

Building Cyber Resilience: Proactive Measures for Family Businesses

To mitigate these risks, family businesses should practice strong cyber hygiene and adopting a robust cybersecurity strategy, including but not limited to:

Strong Password Management: Use unique, complex passwords for all systems and implement a password manager.

Multi-Factor Authentication (MFA): Require additional verification layers beyond passwords for all critical platforms. Avoid SMS based MFA where possible and reply on application-based MFA.

Employee Awareness Training: Educate all team members and stakeholders about cyber risks and safe practices. It is important to reinforce the potential devastating impact that a cyber incident can have on an organisation.

Regular Software Updates: Keep all systems, applications, and antivirus tools up to date – including mobile devices.

Cybersecurity Insurance: Consider policies that cover data breaches, ransomware, and other cyber threats.

Incident Response Plan: Establish and rehearse a step-by-step plan for responding to cyber incidents, including data backups and containment procedures. The true value lies in testing the plan as often as possible and refine according to various scenarios.

Social Media Policy: Protecting Family and Business Reputation

Consider whether your online activity is exposing you, your loved ones and your organisation to risk. Criminals use a combination of open-source intelligence (OSINT) to build a profile of their victims, using publicly available information including social media to plan crafted attacks – both physically and in the digital space. A comprehensive social media policy is essential to safeguard both the family and the business. Such a policy should include:

Privacy Settings: Encourage family members to use strict privacy settings on social media platforms to limit exposure to unwanted attention.

Information Sharing: Advise against sharing sensitive personal information, such as travel plans or financial details, that could be exploited by criminals.

Reputation Management: Highlight the importance of maintaining a positive online presence, as negative publicity can affect both personal and business reputations.

Crisis Communication: Develop a plan for addressing any online incidents that could harm the family's or business's reputation, ensuring swift and effective responses.

Reference

South Africa sees surge in cybercrime: R2.2 billion loss to economy, says Interpol | News24

Cybercrime represents a mounting threat to South Africa's economic backbone—its family-run businesses. As cyber threats evolve in scope and sophistication, these enterprises must recognise the risks and invest in proactive, comprehensive cybersecurity strategies. In doing so, they not only protect their operational continuity but also safeguard the legacy and trust they have spent generations building.

Articles in this Family Business series:

- Article 1: **Governance: Managing Dynamics for Long-Term Success in South Africa**
- Article 2: **Growth: Sustainability**
- Article 3: **Cyber: Securing your family's legacy**
- Article 4: **People: Talent Management**
- Article 5: **Wealth: Legacy Planning – Ensuring Prosperity for Future Generations and Communities**
- Article 6: **Succession Planning: Managing Blind Spots**

Click **here** to read each article.

Authors:

Gustav d'Assonville
Senior Manager, Technology Risk Cyber
M: +27 66 304 2062
gustav.dassonville@kpmg.co.za

Fatih Isik
Senior Analyst, Technology Risk Cyber
M: +27 72 353 5158
Fatih.Isik@kpmg.co.za

kpmg.com/socialmedia