

The Growing Threat of Cybercrime

Cybercrime has emerged as a significant threat in today's digital age, affecting both individuals and corporations on a global scale. In this article, we will delve into the intricate world of cybercrime, exploring its definition, far-reaching impact, notable incidents, the critical need for robust prevention measures, and the staggering statistics that underscore its magnitude.

At its core cybercrime encompasses a wide range of illicit activities that exploit vulnerabilities in computer networks, software, and online platforms. These activities are not limited to lone hackers but often involve organized groups and even state-sponsored actors, such as reported cases of North Korea's cyber espionage on the US. Cybercriminals target individuals, organizations, or even governments.

The most common forms of cybercrime can be categorized as phishing, ransomware, hacking/identity theft and data breaches. The methods used are constantly adapting and getting more sophisticated over time. Let's take a closer look at some of them:

- **Phishing:** In this scheme, cybercriminals impersonate trusted entities, such as banks or technology companies, sending fraudulent emails, messages, or websites to deceive individuals into divulging sensitive information. Phishing attacks persist because of their relative simplicity and high effectiveness.
- **Ransomware:** Typically, infected emails and attachments are sent to random targets. If an individual then clicks on an infected link or attachment from the email, this malicious software then encrypts a victim's data rendering it inaccessible. The attacker then demands a ransom, typically in cryptocurrency, in exchange for the decryption key. Ransomware attacks have been on the rise due to the potential for significant financial gain.
- **Identity theft:** Cybercriminals steal personal information, such as identity numbers, financial records, or driver's license details, to assume the identity of their victims. This information is often used for fraudulent activities, including opening accounts, making purchases, and committing financial fraud. The consequences can include substantial financial losses and damage to one's reputation.

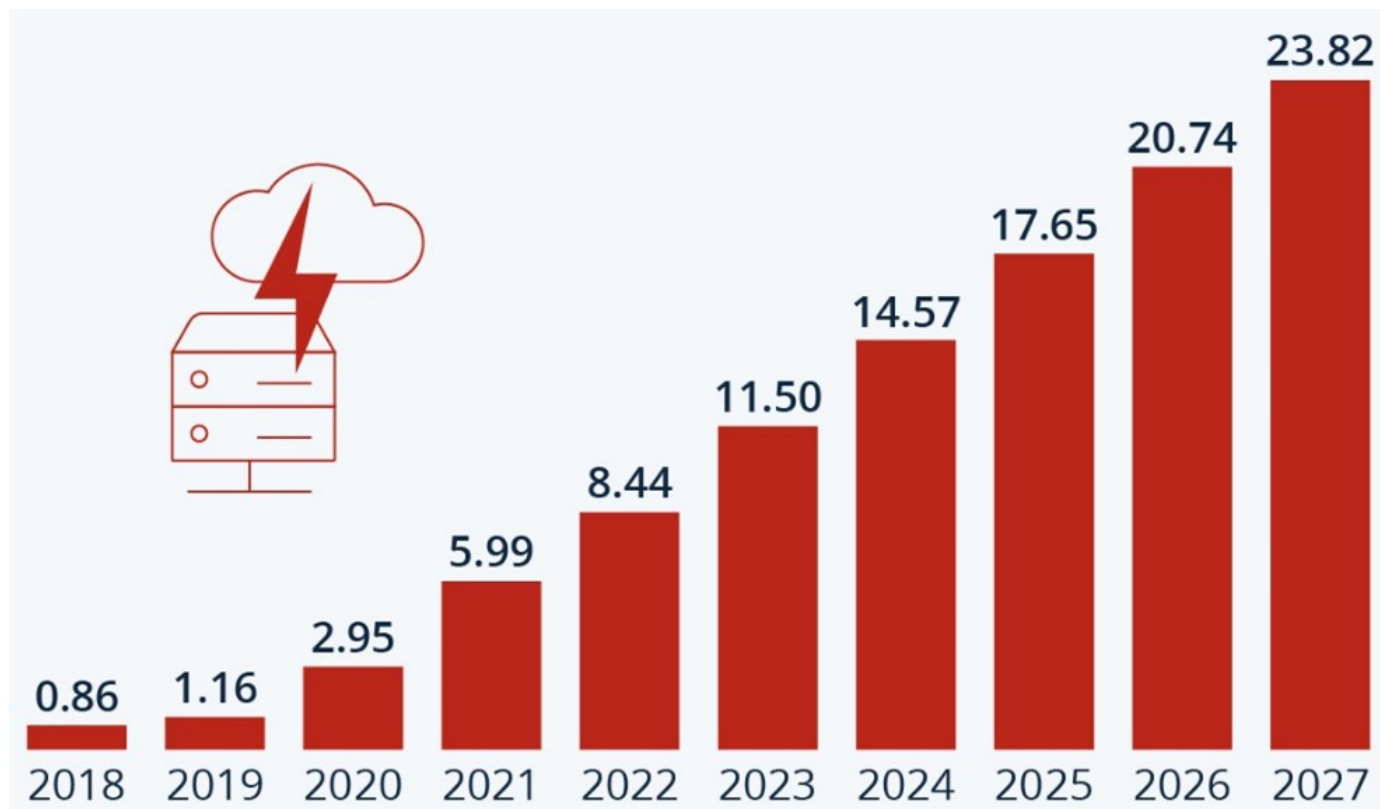
The Impact of Cybercrime

The repercussions of cybercrime are far-reaching. Individuals can suffer financial losses, exposure of personal information, and emotional distress. In contrast, corporations face significant financial setbacks, reputational damage, loss of intellectual property, and potential legal issues. The 2021 Cybersecurity Risk Survey by Deloitte revealed that 40% of respondents experienced at least one cybersecurity incident in the past year, highlighting the pervasive nature of this ominous menace.

The Scale of the Issue

A study that was commissioned by the cybersecurity company Surfshark, identified South Africa as the fifth-most affected country in the world in terms of cybercrime. While the widely quoted figure of R2.2 billion lost annually to cybercrime in South Africa comes from a 2013 report by the South African Banking Risk Information Centre (Sabric). Reports from BusinessTech indicate a very concerning 356% increase in impersonation fraud between April 2022 and April 2023. In addition, a cybercrime report by Interpol discovered that more than 230 million cyber threats were detected in South Africa in 2021, the highest number on the continent. Some more startling statistics are that cybercrime is more profitable than the global drug trade, as well as costing more per year than all natural disasters combined! If it were a global economy (measured in GDP), it would rank as the third largest after the USA and China! Chart 1 below illustrates how massive the scale of the problem is and just how costly cybercrime will be in the coming years:

Chart 1: Estimated cost of cybercrime worldwide (in trillion U.S. dollars) as of November 2022



Source: Statista Technology Outlook, National Cyber Security Organizations, FBI, IMF

Targeting Critical Infrastructure

It is essential to acknowledge that cyber threats transcend national borders. Cybercriminals operate on a global scale, and trends in attack techniques and targets often cross geographical boundaries. Understanding these global dynamics is crucial for individuals and organizations seeking to elevate their cybersecurity defences. Cybersecurity has become paramount in safeguarding critical infrastructure, including pipelines, energy grids, water distribution, and food-processing plants.

Notable Global Cybercrime Incidents

- **SolarWinds Hack (2020):** A highly sophisticated supply chain attack compromised numerous U.S. government agencies and private companies, with cybercriminals inserting malicious code into software updates for prolonged access to sensitive data.
- **Colonial Pipeline Ransomware Attack (2021):** This major fuel supplier in the U.S. fell victim to a ransomware attack that demanded \$4.4 million in cryptocurrency, leading to fuel shortages and economic disruption.

One of the most targeted sectors within South Africa is the financial services industry. This makes intuitive sense as companies working in this industry have access to confidential information and documents related to client information such as ID numbers, bank account details etc. All of which are valuable details to be used by cybercriminals to perform their nefarious activities such as fraud, setting up false bank accounts and the list goes on. Think of all the emails and text messages you receive on a regular basis from your 'colleagues' or 'clients'. These relentless attempts by cybercriminals aim to gain access to information from unsuspecting victims. Individuals can't afford to let their guard down, as the consequences for a single lapse in concentration can be dire.

Here are some local examples of just how serious the consequences can be.

Notable South African Cybercrime Incidents

- *Ransomware attack took down R2 trillion investment administration company for five days:* Even though the money was not at risk, the outage prevented the financial service provider's clients from processing investment-related instructions or offering other services. Its asset management clients include Old Mutual, Sanlam Investments, and Futuregrowth.
- *Department of Justice hit with ransomware attack:* The department said the attack led to all its information systems being encrypted and unavailable to both internal employees as well as members of the public. All electronic services provided by the Department including issuing of letters of authority, bail services, email, and the departmental website were affected.

Countering Cybercrime

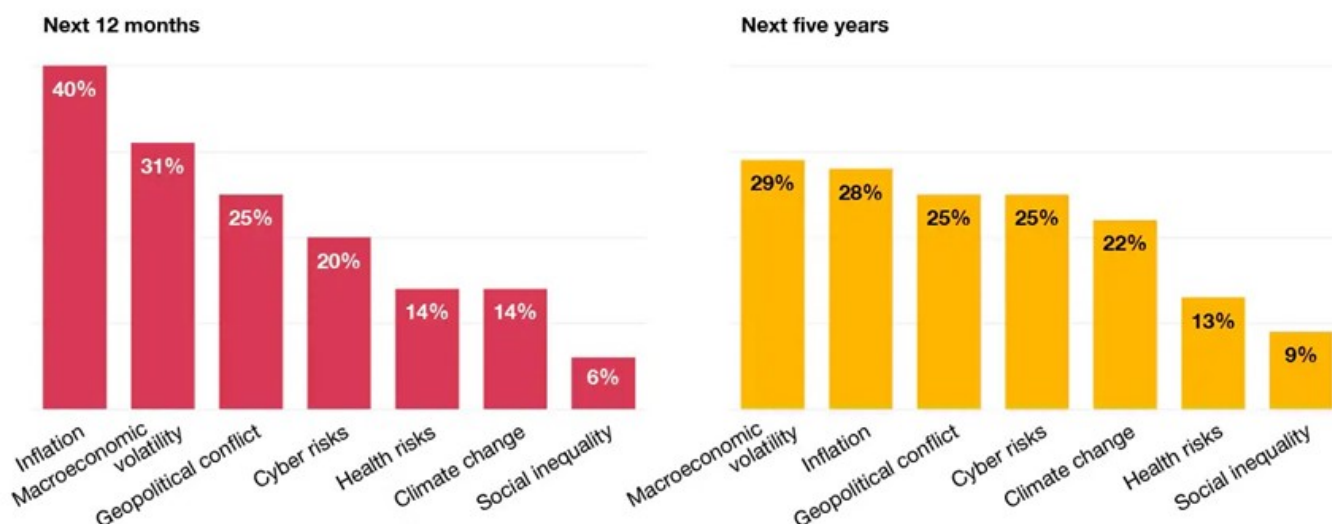
Effectively countering cybercrime necessitates proactive measures, including:

- Maintaining strong cyber hygiene, such as regular software updates, strong passwords, and two-factor authentication.
- Investing in cybersecurity software, encompassing firewalls, intrusion detection systems, and antivirus solutions.
- Continuous education and training to empower employees and users with cybersecurity best practices.
- Implementing advanced threat detection systems and active network monitoring for swift threat identification.

Investing in the latest and most advanced cybersecurity programs in the market is of the utmost importance. It is one of the best ways in which to combat any potential risks. This is a high priority for global business leaders.

According to PWC's 26th Annual Global CEO survey in 2023 which spanned 4,410 chief executives, Cybercrime was highlighted as a greater potential risk than climate change and an equal risk to Geopolitical conflicts over the next 5 years. It underscores how seriously top business leaders globally are taking this endemic problem.

Chart 2: PwC Survey Question - How exposed do you believe your company will be to the following threats in the next 12 months and next 5 years?



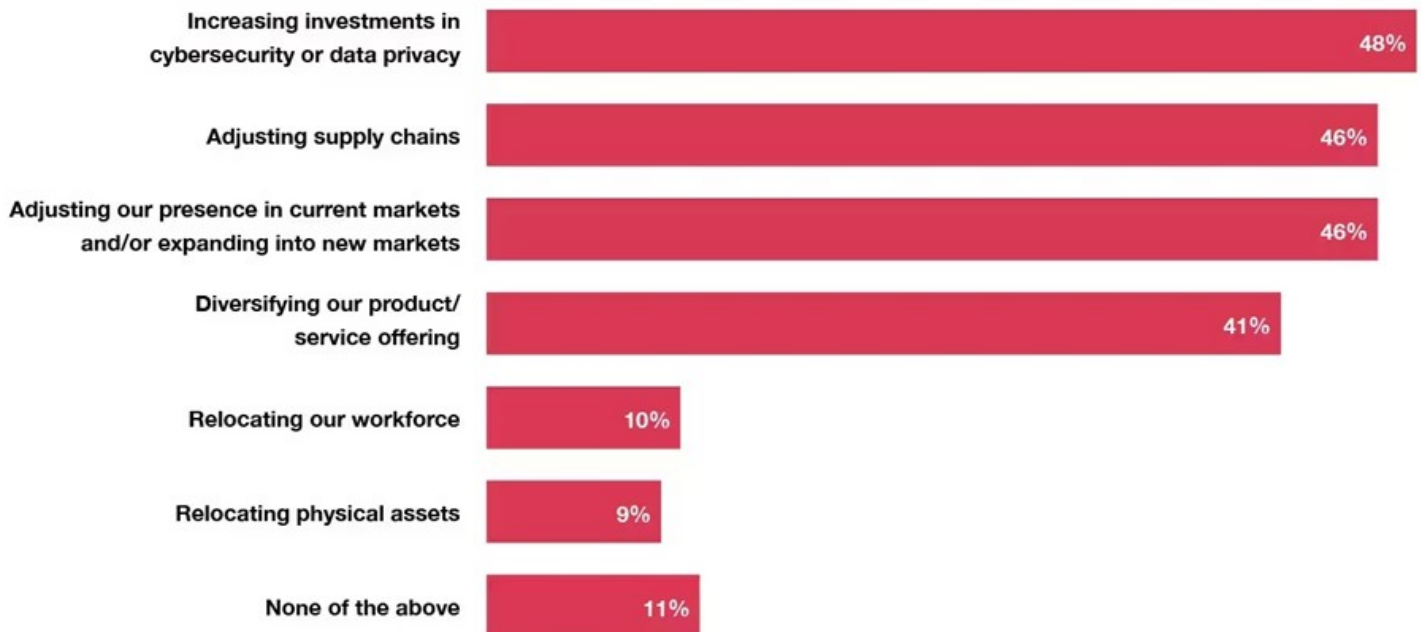
Source: PwC's 26th Annual Global CEO Survey

Investment Opportunities in Cybersecurity

Some individuals have taken advantage of the investment case for cybersecurity and explored opportunities among the top companies within this sector, including Palo Alto Networks Inc, Fortinet Inc, and Zscaler Inc amongst others. The need for and importance of these types of companies will only be increasing in years to come.

Chart 3 below, also from the recent PwC Global CEO survey underpins what can be considered as an investment case for cybersecurity companies. Almost half of CEO's surveyed said that they would be increasing their spending on cybersecurity and data privacy in the upcoming year.

Chart 3: PwC Survey Question - Which of the following actions, if any, is your company considering to mitigate against exposure to geopolitical conflict in next 12 months?



Source: PwC's 26th Annual Global CEO Survey

Why Cybersecurity's Multifaceted Significance is Important

From a personal perspective, being aware of cybersecurity is crucial as our digital lives are increasingly intertwined with personal information and assets. Cyberattacks can lead to identity theft, financial loss, or invasion of privacy. As technology and AI continue to advance, cybercriminals become more sophisticated, making personal vigilance essential.

Understanding and analysing the potentially far-reaching impact on the investment landscape is also becoming more and more prevalent. Whilst there can be significant growth opportunities within cybersecurity linked sectors, analysing the impact of data breaches on all businesses and how they can result in significant financial losses, reputation damage, and legal liabilities is also key. The resilience of a company's cybersecurity measures is fast becoming a pivotal factor in investment decisions, determining who is better positioned to mitigate risks and safeguard their financial performance. As technology evolves, so will the sophistication of cybercrime, intensifying the importance of these considerations.

MARKET REPORT

30 September 2023

		3m	YTD	1yr	3yr pa	5yr pa	10yr pa	5yr Vol1	10yr Vol1
LOCAL MARKET INDICES									
FTSE/JSE All Share Index (ALSI)	ZAR	-3.5%	2.2%	17.7%	14.5%	9.3%	8.6%	17.0%	14.1%
FTSE/JSE SA Listed Property	ZAR	-1.0%	-5.4%	12.9%	16.8%	-3.5%	1.5%	26.9%	21.3%
SA All Bond Index (ALBI)	ZAR	-0.4%	1.5%	7.2%	7.0%	7.2%	7.2%	8.4%	8.0%
SA Cash Index (SteFI)	ZAR	2.0%	5.8%	7.5%	5.3%	5.9%	6.3%	0.5%	0.4%
Balanced Benchmark	ZAR	-2.4%	5.1%	16.1%	11.6%	8.8%	9.0%	11.6%	9.5%
SA Inflation (1 month lag)	ZAR	1.4%	4.1%	4.8%	5.8%	4.9%	5.1%	1.4%	1.4%
GLOBAL MARKET INDICES BASED TO USD									
Global Equity (Datastream World)	USD	-3.4%	11.6%	22.6%	8.6%	7.8%	8.8%	18.5%	14.7%
Emerging Markets Equity (Datastream EM)	USD	-2.8%	2.2%	12.2%	-1.3%	0.9%	2.5%	19.3%	17.0%
Global Property	USD	-6.9%	-5.5%	0.0%	0.2%	1.0%	3.7%	18.9%	15.3%
Global Bonds (Barclays Global Bond Index)	USD	-3.6%	-2.2%	2.2%	-6.9%	-1.6%	-0.4%	6.9%	5.8%
Global Cash	USD	1.3%	3.7%	4.7%	1.8%	1.8%	1.3%	0.5%	0.4%
MAJOR INDICES BASED TO RANDS									
FTSE/JSE All Share Index (ALSI)	ZAR	-3.5%	2.2%	17.7%	14.5%	9.3%	8.6%	17.0%	14.1%
Global Equity (Datastream World)	ZAR	-3.6%	23.5%	28.5%	13.1%	14.2%	15.9%	16.1%	15.3%
Emerging Markets Equity (Datastream EM)	ZAR	-3.1%	13.1%	17.6%	2.7%	6.9%	9.1%	13.6%	13.2%
Global Property	ZAR	-7.2%	4.6%	4.8%	4.4%	6.9%	10.4%	17.1%	16.0%
SA All Bond Index (ALBI)	ZAR	-0.4%	1.5%	7.2%	7.0%	7.2%	7.2%	8.4%	8.0%
Global Bonds (Barclays Global Bond Index)	ZAR	-3.9%	8.3%	7.2%	-3.1%	4.2%	6.0%	14.2%	13.8%
COMMODITIES									
Gold (US Dollars)	USD	-2.2%	3.1%	11.9%	-0.3%	9.5%	3.5%	14.2%	13.7%
Gold (Rands)	ZAR	-2.5%	15.1%	17.3%	3.8%	16.0%	10.2%	18.7%	17.2%
CURRENCIES									
Rand / Dollar	ZAR	-0.7%	-11.2%	-4.7%	-4.3%	-6.0%	-6.6%	15.1%	14.9%
Rand / GBP Pound	ZAR	3.4%	-12.1%	-14.7%	-2.3%	-4.5%	-3.6%	12.9%	14.3%
Rand / Euro	ZAR	2.4%	-9.6%	-13.2%	-0.8%	-4.0%	-4.0%	12.5%	13.0%
Spot Rates									
		29-Sep-23	Latest Quarter	1 Year Ago	5 Years Ago	10 Years Ago	20 Years Ago		
CURRENCIES									
Rand/US\$	Rand	18.8	18.8	18.0	14.2	10.1	7.0		
Rand/GBP	Rand	23.0	23.0	20.1	18.4	16.3	11.6		
Rand/EUR	Rand	19.9	19.9	17.6	16.4	13.6	8.1		
RATES									
Libor 6m \$	US\$	5.9	5.9	4.2	2.6	0.4	1.2		
Repo Rate	Rand	8.25	8.25	6.25	6.50	5.00	10.00		
Prime	Rand	11.75	11.75	9.75	10.00	8.50	14.50		
All Bond Index Yield	Rand	10.8	10.8	11.6	9.7	8.0	9.7		
COMMODITIES									
Gold (\$/oz)	US\$	1,856.8	1,856.8	1,674.1	1,191.5	1,330.8	385.3		
Platinum	US\$	923.0	923.0	864.0	815.0	1,411.0	710.0		
Oil (Brent Crude) \$	US\$	95.4	95.4	88.2	82.8	108.9	28.2		
INFLATION									
SA Inflation	%	4.8	4.8	7.5	4.9	6.0	9.4		

data provided by FE Analytics

Fundhouse is a leading investment adviser specialising in fund research, ratings and portfolio construction services. We help clients manage investments on behalf of the end investor. Our experienced team understands the complexities of the fund management world. We apply this knowledge alongside a client first mindset to improve the outcome for the end investor.

Fundhouse was founded in 2007 by professionals from the investment management industry. We currently operate from offices in the United Kingdom and South Africa, where we cover the local and global fund industry first hand. Our business is 100% independent and owner managed which means we can offer objective advice and services in the best interests of our clients.

Email: adviser@fundhouse.co.za | Web: www.fundhouse.co.za

FUNDHOUSE
investment clarity