Fraud risk, specifically cybercrime, and the subsequent threat to business sustainability

Charles Francois Weber

The World Economic Forum ‘Global Risks Report 2017’ indicated an increase in cyberattacks and ranked massive incident of data fraud or theft as their fifth highest risk on their top five global risks in terms of likelihood.

Prof. Mervyn King (SC) was asked at the Association of Certified Fraud Examiners South Africa (ACFE SA) Gauteng 2016 Year End function whether he viewed fraud risk as an increased threat to businesses’ sustainability. He replied that he did and specifically emphasised the significant increase in cybercrime.

The World Economic Forum *Global Risks Report 2017* indicated an increase in cyberattacks and ranked massive incident of data fraud or theft as their fifth highest risk on their top five global risks in terms of likelihood. The report concluded that:

> *… by assessing the risks associated with how technology is reshaping physical infrastructure: greater interdependence among different infrastructure networks is increasing the scope for systemic failures – whether from cyberattacks, software glitches, natural disasters or other causes – to cascade across networks and affect society in unanticipated ways.*

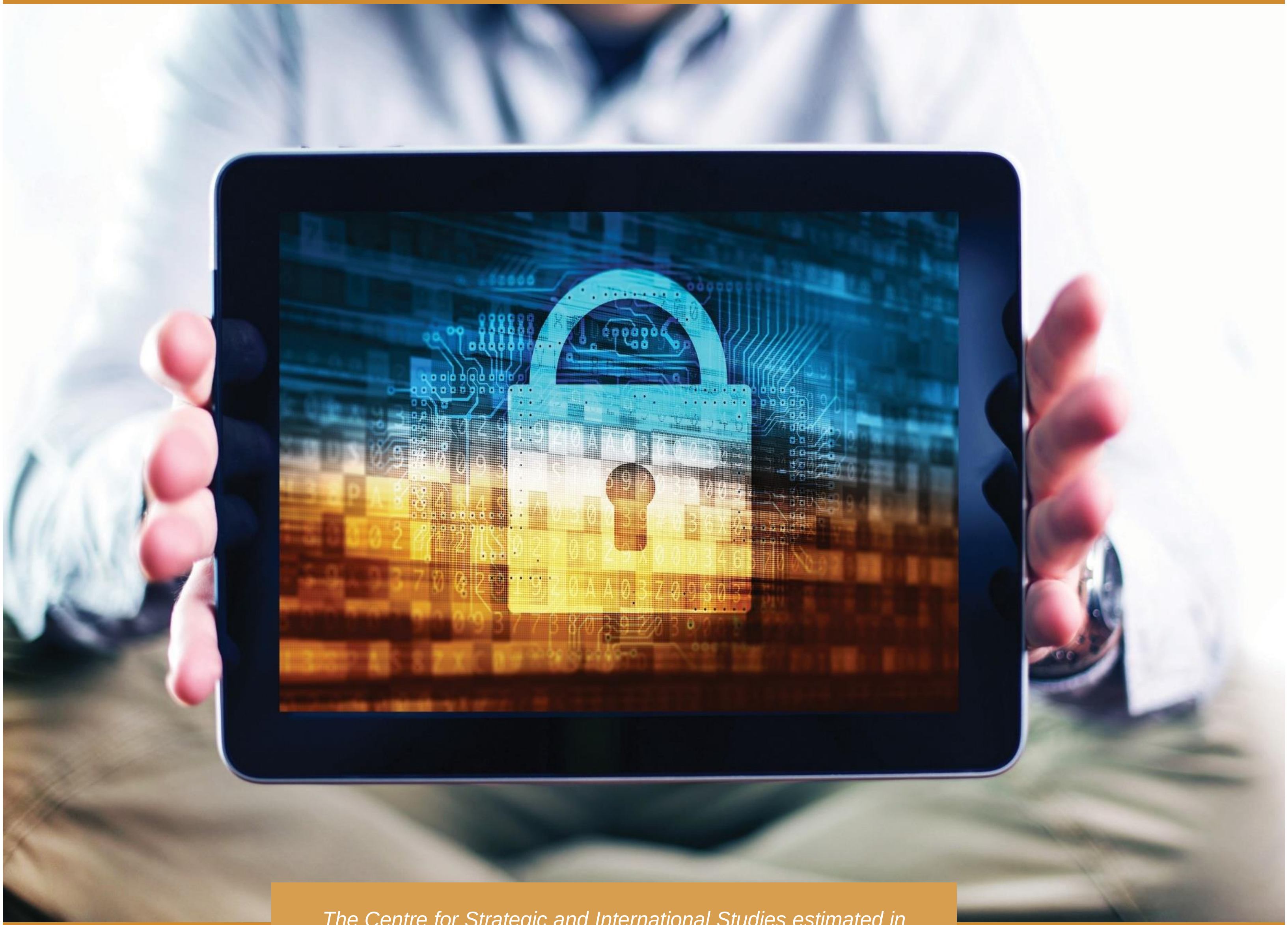
The report identified the top five trends that determine global developments and rising cyber dependency was ranked fourth. This increase was cited ‘due to increasing digital interconnection of people, things and organisations’.[1, 2]

The report identified the top five trends that determine global developments and rising cyber dependency was ranked fourth.

Similarly, the Institute of Risk Management South Africa *Risk Report: South Africa Risks 2017*, launched on 21 February 2017, ranked escalation in large-scale cyberattacks as their eighth risk of their top ten South Africa industry level risks and the third ranked risk of the financial services of the top three industry risks. The report engaged with various subject matter specialists to further explore this specific risk and enquired their view on an effective risk response(s) on

[1] Schalk Burger ‘Detecting advanced cyberattacks to be key security focus in 2017’, *Creamer Media’s Engineering News* (3 February 2017), available at <http://www.engineeringnews.co.za/article/detecting-advanced-cyberattacks-to-be-key-security-focus-in-2017-2017-02-03> (accessed 6 March 2017).

[2] WEF *Global Risks Report 2017*.



The Centre for Strategic and International Studies estimated in 2014 that 'South Africa loses 0.14% of its GDP to cybercrime activities, amounting to around R5.7 billion annually'.

an industry and national level. Herewith, one subject matter specialist's views:

On an industry level, consideration could be given to:

> *Identify the nature and type of the risk. [W]ill it come from an internal or external source?*
> *Secure digital platform[s] that are fundamental to the success of the business.*
> *Invest in new solutions.*
> *Realistic policy and procedures, for example BYOD [Bring your own device].*

The PWC Global Economic Crime Survey 2016 indicated that 'cybercrime continues to escalate – ranking as the second-most reported crime' globally and the fourth ranked risk for South Africa.

On a national level, consideration could be given to:

> *Government taking the lead and setting up a cyber-security hub and setting the tone of good preventative measures.*
> *Investment in digital security.*
> *Ensure that this is seen as everyone's risk, part of their 'DNA'.*
> *Education.*
> *Continuous awareness campaign.*[3]

The PWC *Global Economic Crime Survey 2016* indicated that 'cybercrime continues to escalate – ranking as the second-most reported crime' globally and the fourth ranked risk for South Africa.

The PWC *Global Economic Crime Survey 2016* further concluded that 32% of all organisations surveyed 'experienced cybercrime, and this figure is growing rapidly'. The three leading observations from the report included cybercrime as a 'threat to all aspects of business'. Two key concerns highlighted were that 'most organisations are still not adequately prepared' and that leadership engagement was also insufficient, as the survey showed that only '48% of board members request information about their organisation's state of cyber-readiness'.[4]

A key recommendation from the report was 'a proactive stance when it comes to cybersecurity and privacy', which requires 'that everyone in the organisation – from the board and C-suite to middle management and hourly workers – see it as their responsibility'. Some basic elements in terms of readiness include 'sufficient board involvement, correct system configurations and adequate controls over third party business partners that have access to the corporate network'. Given board members' risk management responsibility, the report recommends the following: 'boards incorporate cybercrime into their routine risk assessment; communicate the plan up, down and across organisational lines, and discuss specifically with the IT department at what point they want to be alerted of a breach'.[5]

In the KPMG *Global Profiles of the Fraudster Report May 2016*, a similar view is substantiated to the above from PWC, as the report cited cyber fraud to be 'the most frequently cited emerging threat by KPMG offices around the world'. The key aims of cyber fraud from the report/survey indicates 'theft of personal data and intellectual property, senior executive's e-mails, strategic access to company data and denial of services'. The report recommended strong internal controls and data analytics' as well as 'to share insights with other companies to stay on top of a fast-changing threat landscape' as some risk responses.[6]

[3] Institute of Risk Management *Risk Report: South Africa Risks 2017*, 3rd edition.

[4] PWC *Global Economic Crime Survey 2016*, 5th South African Edition (March 2016).

[5] Ibid.

[6] KPMG *Global Profiles of the Fraudster* (May 2016).

The Centre for Strategic and International Studies estimated in 2014 that 'South Africa loses 0.14% of its GDP to cybercrime activities, amounting to around R5.7 billion annually'.[7]

AON South Africa, an insurer, identified the following anticipated challenges that could prevent successful recovery of the above risk or losses via standard insurance policies:

- 'General liability and property policies cover risks that damage physical assets. Since cybercrime is a relatively new risk, the loss covered under conventional property policies *do not extend to incorporeal assets nor losses* caused by non-physical perils such as viruses or hackers.
- Professional indemnity policies cover damage resulting from a failure of the defined professional services and *may not extend* to losses resulting from data and privacy breaches.
- Crime policies generally cover money, securities and tangible property with *no coverage* for third party property such as customer data.'[8]

Considering the above sources cited, it thus seems that cybercrime is more prevalent whether businesses and/or individuals are aware (directly affected) of this trend or not (indirectly affected). No industry or profession is necessarily less vulnerable to be targeted, as even law practitioners have experienced an increase in cyberattacks. In a recent *Risk Alert Bulletin* for law practitioners, recommendations were provided on insurance policies to cover cybercrime and 'top-up cover' was recommended. It was advised that practitioners 'who have top-up insurance must study the wording of their top-up policies carefully to ensure that they are covered for cyber related claims'.[9]

The national response to the above was the drafting of the Cybercrimes and Cybersecurity Bill (first published 28 August 2015), which is currently in progress to be enacted by parliament. The aim will be 'to stop cybercrime and improve the security of the country'. The scope of this bill could impact all of the following parties (not an exhaustive list necessarily):

- 'People involved with IT (or POPI) regulatory compliance.
- All [e]lectronic [c]ommunications [s]ervice [p]roviders (ECSPs).
- Financial institutions.
- Representatives from various government [d]epartments.
- Cyber criminals and terrorists.
- Providers of software or hardware tools that could be used to commit offences.
- Information [s]ecurity experts.
- Anyone who owns an [i]nformation [i]nfrastructure that [g]overnment could declare as critical.
- Everyone who uses a computer or the Internet.
- The [p]olice [s]ervice.'[10]

To better understand the offences to be governed by the above bill, the concept of cybercrime is further broken down into the following parts 'related to data, messages, computers and networks. For example – hacking, unlawful interception of data, distributed-denial-of-service attack (DDoS attack), ransomware, cyber forgery and uttering, or cyber extortion'.[11]

[7] Bryon O'Connor and Verusha Moodley 'The growing need for cybercrime insurance in South Africa', Cliffe Dekker Hofmeyr (10 August 2016), available at <https://www.cliffedekkerhofmeyr.com/en/news/publications/2016/dispute/dispute-resolution-alert-10-august-the-growing-need-for-cybercrime-insurance-in-south-africa.html> (accessed 6 March 2017).

[8] Ibid.

[9] Cyber scam matters – practitioners continue falling victim to scams', *Risk Alert Bulletin* (February 2017), available at <http://www.derebus.org.za/wp-content/uploads/2017/02/DR_JanFeb2017b.pdf> (accessed 6 March 2017).

[10] 'South Africa's new Cybersecurity Bill will affect everyone who uses the Internet', *MyBroadband* (22 January 2017), available at <https://mybroadband.co.za/news/government/195276-south-africas-new-cybersecurity-bill-will-affect-everyone-who-uses-the-internet.html> (accessed 6 March 2017); 'Cybercrimes and Cybersecurity Bill – Overview of the Cyber Bill', Michaelsons (28 February 2017), available at <https://www.michalsons.com/blog/cybercrimes-and-cybersecurity-bill-the-cac-bill/16344> (accessed 6 March 2017).

[11] Ibid.

Considering the above sources cited, the increase in cyber threats and the subsequent Cybercrimes and Cybersecurity Bill discussed above, the following is recommended:

- A cyber-specific **risk assessment** should be undertaken and consideration should be given on whether internal and/or external resources (subject matter experts) would aid in an appropriate risk response to such risk(s) identified.
- Increase/improve cyber **risk awareness** efforts to ensure a holistic view and a holistic approach to assist individuals, businesses, industries and the country to improve cyber safety and cybersecurity.
- Review standard **insurance policies** against the identified cyber risk(s) to ensure adequate insurance cover is aligned with the board approved risk tolerance.
- The **board members** should review their 'cyber security risks and the legal implications' for their organisation as it relates to the 2017 version of the Cybercrimes and Cybersecurity Bill.[12]

Charles Francois Weber is a professional with an excess of 11 years' full-time combined experience in the fields of corporate governance, enterprise-wide risk management, internal audit and fraud investigation in both privately owned and publically listed companies, including experience across various industry sectors.

Charles has worked for more than five national organisations and is currently the Africa-based Business Risk Manager at Lonrho.

His qualifications include a BCom Accounting Sciences degree and a BCom Honours degree in Internal Auditing, both from the University of Pretoria, and a Master of Business Management and Administration degree (MBA) from the University of Stellenbosch Business School.

His MBA research report covered the field of corporate governance under the supervision of Dr Daniel Malan, with his research report titled: *KING III Report on Governance: Practical Obstacles to the effective application with specific focus on the principles of Director Independence*.

He is also a certified internal auditor and has certifications in control self-assessment and risk management assurance from the Institute of Internal Auditors South Africa. In addition, he is a certified fraud examiner (CFE), a certified risk and compliance management professional and a certified enterprise risk manager.

Charles acted as the chairman of the Johannesburg regional committee of the Association of Certified Fraud Examiners South Africa (ACFE SA) in 2015 and 2016. He was also awarded the 2016 CFE of the Year Award by the ACFE SA.

Charles is an advocate of sound corporate governance as a strategic necessity for all organisations' sustainabillity and supports all institutions with a similar goal.

Author

[12] Ibid.