Cybersecurity
Introduction

insights

Fast facts of cybersecurity

Cyber attacks cost businesses in excess of $400bn every year.

There are more than 1 Million unfilled information security jobs globally.

The WEF global risks 2017 views Data Fraud / Theft and Cyberattacks as 2 of the top 10 Global risks in terms of likelihood.

From 2016 to 2019 global cyber crime costs are expected to greatly increase, reaching US $ 2.1 Trillion.

US government spent US $ 14 billion on cyber security in 2016 with plans to spend US $ 19 billion in 2017.

South Africa is reported to have 3rd highest rate of phishing attacks in the world.

In 2016, 7% of South African organisations experienced targeted attacks.

There has been a 67% increase in the number of ransomware, and an increase of 15% in the number of cyber-related incidents in South Africa.

Among all insider breaches, 55% are caused by misuse of privileged accounts.

In this world of hyper connectivity, the traditional way of connecting with people , doing business and managing stakeholders has long moved from face to face engagement to engagement via one communication platform or the other. Every 60 seconds, there are approximately 422 340 tweets, 3.3 million facebook engagements, 205,6 million emails sent and 3.1million google searches!

Globally, technology is transforming industries and with technological advancements comes risk.

Cybersecurity has become a business continuity necessity that needs to be woven into the fabric of every company and integrated into every business process and every employee action. Our reliance on digital systems makes everyone a potential victim.

Cyber-crime is costing the global economy an estimated US$400 billion.

- In 2014, it was estimated that cyber-crime has an economic impact equal to about 0.14% of the country's total GDP. With a GDP contribution of close to R4.1 trillion, cyber-crime is costing the economy R5.8 billion a year. An estimated increase of R2.38 billion a year ago.
- A worldwide leader in security solutions revealed that five African nations were among the top 10 most-attacked countries. Botswana was the most-attacked country, followed by Malawi in second place, Namibia in fourth, Uganda in ninth and the Democratic Republic of Congo in tenth place. South Africa moved up to 31 on the list from 58th position in October, while Kenya dropped to 24th (from 22nd in October) and Nigeria climbed slightly to 108th position, from 116th the previous month.

Type of cybersecurity threats

1. Ransomware

Hackers take control and withhold data/ information. Computers and mobile devices are prime targets for this type of extortion.

2. Blastware

Hackers infiltrate systems, gather data and then wipe out the information on systems and hard drives to cover tracks and thwart forensics.

3. Hacktivism

Hackers use of computer networks to promote political agenda. Often related to free speech, human rights and freedom of information. Affect companies reputation.

4. Industrial state / Espionage

Industrial espionage targets enterprises with highly lucrative tenders / procurement / patents, etc offerings. State sponsored espionage seek to improve the strategic capabilities of their host nation to protect and serve national agendas

5. Cybercriminals

Hackers seek to gain profit and often run their operations similarly to a legitimate business, albeit with much less ethical considerations. Nowadays – cybercrimials infiltrate environments and stay on undetected for long periods of time.

nkonki

Registered Auditors | Accountants | Advisors

Impact of cybersercurity crimes:

1. Loss of personal information

2. Reputational impact

3. Loss of revenue

4. Litigations costs

5. Short term business interruption

Top Four cybersecurity trends

Cybersecurity Trends #1 – Government Intervention

CYBERCRIMES AND CYBERSECURITY BILL, 2017

The Cybercrimes Bill was first published on 28 August 2015. An updated version was released on 19 January 2017 and will likely be introduced in Parliament in late January 2017.
The primary aim of the Bill is to deal with cybercrimes and cybersecurity. The current position in South Africa is that cybercrimes are investigated in terms of the Criminal Procedure Act, 1977.

The Bill aims to rationalise the SA laws of which deals with cyber-crime and cybersecurity into a single Bill and to that extent the Bill:

- Creates offences and imposes penalties which have a bearing on cybercrime;
- Criminalises the distribution of malicious communications and provides for interim protection measures;
- Regulates jurisdiction to provide for the transnational dimension of cybercrimes;
- Regulates the powers to investigate cybercrimes;
- Regulates mutual assistance to deal with cross-border investigation of cybercrimes;
- Provides for the establishment of a 24/7 Point of Contact to facilitate mutual assistance in the investigation of cybercrime;
- Regulates the proof of certain facts by affidavit;
- Imposes obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes;
- Provides for the establishment structures to promote cybersecurity and capacity building;
- Provides for the identification and declaration of critical information infrastructures and implementation of measures to protect critical information infrastructures;
- Provides that the Executive may enter into agreements with foreign States to promote cybersecurity; and
- Provides for the repeal and amendments of certain laws.

Cybersecurity Trends #2 – Increase in Risk Oversight

Oversight includes:

- Boards view on Cybersecurity;
- Risk appetite and tolerance limits;
- Investments in more GRC solutions;
- Appointment/ Sourcing of a Chief Information Security Officers; and
- Compliance to the King code, ECT Act, and preparation for POPI.

Cybersecurity Trends #3 – Security Professionals

- Greater need for cybersecurity professionals;
- Higher salaries are being demanded;
- Cybersecurity qualifications are being offered; and
- Global career opportunities for skilled resources.

Cybersecurity Trends #4 – Who will be spared?

Attackers will look to most valuable and easy targets. In addition, mobile platform attacks are on the increase as security is an afterthought.

- The attackers are getting better - The perpetrators are more sophisticated, better funded and have more resources than ever before;
- The possibility of an attack by a malicious employee is a key threat that organisation should be aware of; and
- The economics of cybersecurity favours the attacker as tools and techniques are readily available and cheap.

The Solution

"We must know ourselves and our enemies and select a strategy to positively influence the outcome of battle. There is no reason to fear the attack but there is reason to be concerned about our readiness to defend ourselves from the attack and respond appropriately." Sun Tzu

Combating Cyber attacks goes beyond technical solutions. It is job number one……a job that begins at the top and ends at the top.

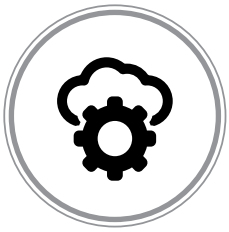
A Call To Board Action

Leadership and understanding is critical – Boards must appreciate the context and utilise the governance tools at their disposal to evaluate, direct and monitor this critical risk.

The growing number of security related incidents needs preventative mitigation. Board direction goes beyond technical to include education, awareness and training programs for employees.

Cyber-crime is a business issue and cannot be remediated by IT alone as it affects every facet of the organisations sustainability and prosperity.

Seek the optimal balance of security i.e risk vs return. A culture of cybersecurity risk is entrenched into business considerations.



Establish a cybersecurity capability process and prepare a roadmap to your desired target maturity level.

Our Contact Details

Johannesburg - Head Office

Physical Address:
Nkonki House
1 Simba Road
Sunninghill

Tel: +27 11 517 3000

Postal Address:
P.O. Box 1503
Saxonwold
2132

Durban Office

Physical Address:
131 Jan Hofmeyr Road
Westville
Durban

Tel: +27 31 2747 400

Postal Address:
P.O. Box 1427
Wandsbeck
3631

Stanger Office

Physical Address:
84 Balcomb Street
Stanger

Tel: +27 32 551 1111

Postal Address:
P.O. Box 501
Stanger
4450

Pretoria Office

Physical Address:
Crestway Office Park, Block E
20 Hotel Street
Persequor Park

Tel: +27 12 993 9500

Postal Address:
P.O. Box 1569, Garsfontein East
Pretoria, Gauteng
0060

Bloemfontein Office

Physical Address:
95B Kellner Street
Westdene
Bloemfontein

Tel : 051 430 9290

Postal Address:
P.O. Box 11977
Universitas
Bloemfontein
9321

Cape Town Office

Physical Address:
1st floor, Block A, Regent Square
Kenilworth

Tel: +27 21 797 4594

Postal Address:
P.O. Box 2926
Cape Town
8000

Alberton Office

Physical Address:
DVM Office Park, 1st Floor
16 Kingfisher Crescent
Meyersdal

Tel: +27 11 867 1400

Postal Address:
P.O. Box 1363
Alberton
1450

Northwest Office

Physical Address:
48 Proctor Avenue
Golf View
Mafikeng

Tel: +27 18 381 1660

Port Elizabeth Office

Physical Address:
3 Redheart Crescent
WaveCrest
Jeffreys Bay

Tel: +27 82 788 3344

Postal Address:
P.O. Box 11977
Universitas
Bloemfontein
9321