Nexia SAB&T
accountants | auditors | consultants

CYBERCRIME IS A REALITY

IS YOUR BUSINESS CYBER RESILIENT?

May 2017

The digitised world is growing at a phenomenal pace. Businesses are embracing the digital era in order to realise technological advantages as much as out of necessity to keep up with competitors, as the Internet of Things drives entrepreneurship.

The falling costs of information and communications technologies is helping Africa realise a fundamental transformation in the continent's economic, political and social environment. Especially impressive has been digitisation's benefits to disadvantaged consumers, such as those without bank accounts or electricity. Major drivers of the continent's digitisation include for example the various cable systems connecting the African continent to the rest of the world such as SEACOM, East African Submarine Marine Systems (EASSy), West African Cable System (WACS), and the rapid diffusion of mobile phones and smart devices.

Companies around the world, but particularly in Africa where defences are inadequate, are highly vulnerable to cyber-attacks. Africa's businesses and governments are several steps behind the smart operators quietly entering networks to access valuable data, disrupt activities and blackmail companies.

According to the United Nations, cybercrime covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them.

Malware and Ransomware are now concepts that businesses need to understand as cybercriminals use these to attack their digital infrastructure, which cost business and their clients millions of Rands every year. The rise of cybercrime has been astonishing and totally under estimated.

Potential impact of a ransomware attack on your organisation:

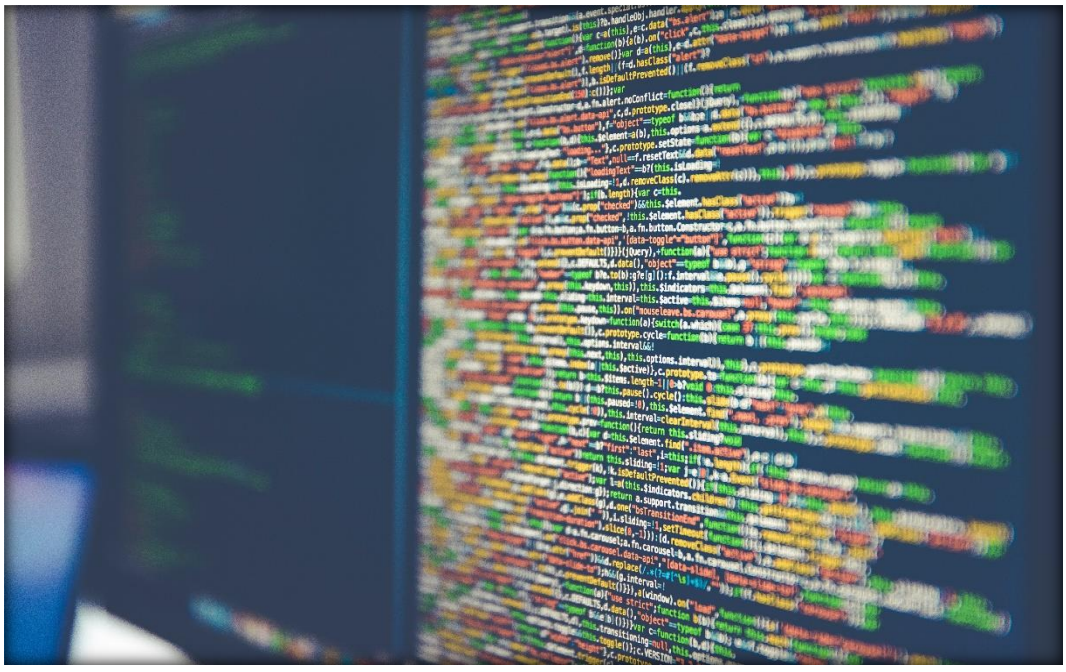
- Inability to trade
- Loss of revenue
- Loss of intellectual property
- Loss of confidential client information
- Loss of confidential employee information
- Loss of reputation
- Identity theft
- Potential liability for damages resulting from lost data

Ransomware attacks go hand-in-hand with cyber extortion. The ransomware encrypts all your documents and denies you access to your systems or data, thereby potentially disabling your ability to trade. After the ransomware has successfully encrypted your data it will present you with a message letting you know that the key to decrypt your data will be provided to you, provided you transfer a specific amount in Bitcoin (which is an untraceable currency).

When your systems are down following a ransomware attack, you may be unable to access your information, making normal trading almost impossible due to the vast reliance on data and information organisations have.

When a company is hacked information may be stolen and that information, which could contain sensitive trade, client or employee information, is then sold on what is referred to as 'the dark web', which is the part of the internet the normal internet user does not have access to, and from where cybercriminals operate. Cybercriminals then use that information either to scam their targets, or to commit identity theft, using all the personal information obtained to pose as a different person to buy houses or run up massive amounts of expenses in that individual's name. You as the company have the responsibility to look after your customers and your employee's information, and if you don't and that information is leaked, the company could then potentially be held liable for those damages suffered by the affected third parties.

WannaCry Global Cyber-Attack



A global cyber-attack was launched on Friday, May 12, 2017, and continued through the weekend. The attack was executed as a form of ransomware called WannaCry that encrypted the data on vulnerable computers on the networks it managed to penetrate and demanded payment to restore access to the data.

The ransomware targets a specific vulnerability on computers running the Microsoft Windows operating system, exploiting the vulnerability and then encrypting data and demanding ransom payments in the Bitcoin crypto-currency. It is one of the worst ransomware attacks to date. The attack leveraged hacking tools believed to be developed by the U.S. National Security Agency that was leaked online last month by a nefarious group known as "The Shadow Brokers."

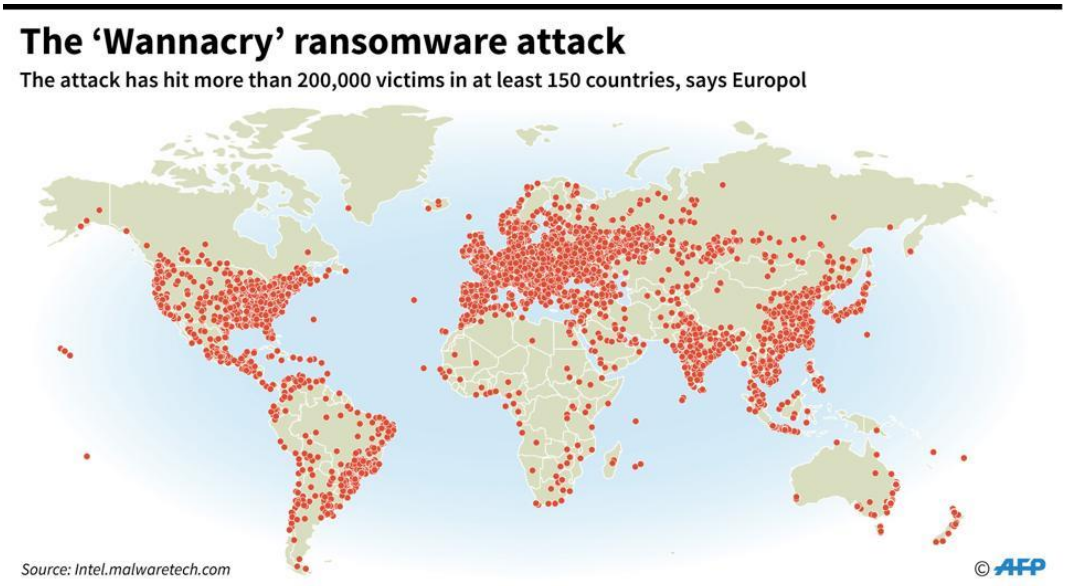
The attack infected more than 230,000 computers in nearly 150 countries, by spreading across local networks and the Internet to systems that have not been updated with the most recent security updates, to directly infect any exposed systems.

It even disrupted Britain's health system and global shipper FedEx. At least 16 hospitals in the United Kingdom were forced to divert emergency patients as their systems were rendered useless and physicians unable to access electronic medical records. Perhaps this could be the beginning of a new trend for international organised crime, experts have told the BBC. http://www.bbc.com/news/av/uk-39905839/the-next-step-for-organisedcrime

Europol, the pan-EU crime-fighting agency, said the threat was escalating and predicted the number of ransomware victims was likely to grow across the private and public sectors. Cyber security experts said the malware could spread through computers with unpatched versions of Microsoft Windows.
https://www.theguardian.com/technology/2017/may/14/cyber-attack-escalate-working-week-begins-experts-nhs-europol-warn

Image of the message users received on systems that were successfully attacked by the ransomware WannaCry.

South African companies and individuals have also been the victim of the WannaCry ramsonware although not to the same degree as some of the other countries as seen in the picture below.



It goes without saying that the phenomenon goes far beyond the common scams perpetrated through emails - the famous Nigerian "419" scam. https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerianscams

Recently, a number of South African companies' and government institutions systems were infiltrated by cyber attackers and data was stolen or held for ransom. These incidents illustrate the risks that the use of cyberspace poses to the African continent in the 21st Century.

The Way Forward

Businesses need to embrace new technologies and understand they're exposing themselves to new risks. The questions are how to guard against data breaches, how to mitigate damages, and how to manage cyber risk. The world is changing at a bewildering pace due to rapid digitisation and urgent solutions are needed to ensure that businesses are cyber resilient.

Security has to be on management's and the board's agenda. They need to be constantly thinking about the worst-case scenario: what would happen if your information were stolen? How badly would your business be damaged if one individual were bribed or blackmailed? What are all the possible ways someone could attack?

There are two key areas to consider: the regulatory environment and organisational culture.

Regulatory Environment	Organisational Culture
A crucial aspect is the impact of different regulatory environments. Today's globalised and digitally integrated world means that most organisations are to some extent international. Whether it's a business, which serves a global market or a manufacturer hooked into global supply chains, awareness and adherence to local rules and regulations in all areas of operation are crucial. The EU General Data Protection Regulation (GDPR), due to come into effect in 2018, which requires every organisation operating in Europe to abide by several regulatory provisions – and this doesn't just mean companies based in Europe, but also those offering goods or services to EU markets in a way that involves processing any European-owned data. Cyber challenges are global, and regions everywhere will need to come up with appropriate regulatory responses.	Management or the board members can't do everything themselves. You need to build security awareness into your organisation's culture by making it part of every employee's roles and responsibilities. Give the employee responsibility, and encourage them to speak up. If everyone thinks about security, they'll ask the right questions. For example, a recruiter can consider how much a planted employee could steal. They might then be proactive and help ensure you have the right vetting processes in place. Other security issues can result from scammers working on the inside or employees not being educated about the risks of accepting for example free USB drives or bringing their own devices to work. Business owners should consult with security professionals.

If businesses do nothing, assuming a "nothing can happen to us" mentality, then it's only a matter of time before a security hack occurs.

Companies, multinationals, government and individuals can't avoid an attack. It's going to happen eventually. You can do everything possible to recover what's been stolen and catch the criminal, but eventually they'll find that tiny hole and squeeze through.

The trick is to make sure you have layers between your systems. If your customer data is behind another wall, it's safer. You want to make sure your most valuable information is hidden – even from your own employees. You don't see bank vaults out on the street. They're behind checkpoints, cameras and closed doors. Do the same with your data.

Nexia SAB&T

So, what can you or your organisation do? How can you protect yourself?
These are complex questions that you need to address, but for now, consider the following:

- **Get educated about cybersecurity.** You can't defend from what you don't understand. Cybercrime is real. It's a threat to all organisations. It's no longer a matter of "if" but "when".
- **Implement a cybersecurity strategy.** Are you taking the proper measures to adequately protect your organisation? How will you know if a hacker is on your network?
- **Have an incident response plan.** How will you bounce back after an attack? Have a plan in place to respond and bounce back after an attack.

Nexia SAB&T's Cyber Security Offering

Nexia SAB&T offers various ICT security assessments or Security Audits, including vulnerability assessments and penetration testing covering your ICT environment and systems such as servers including mail servers, network authentication servers, file servers, network devices, database review, security awareness training, etc.

We also offer a Unified Security Management Platform. This platform will monitor network traffic for any vulnerabilities including the existence of any ransomware ,malware and other known viruses within you organisation as well as identifying the source within your ICT systems to identify the origin of the particular attack.

This article was adapted from an article published by Sujata Jaffer, CPA (T) PP; CISA of Nexia SJ, Tanzania.

Contact Us

Herman Van Der Merwe
herman@nexia-sabt.co.za
www.nexia-sabt.co.za
Contact: +27 12 682 8800

Disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in future, and, to the extent permitted by law. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Nexia SAB&T does not accept liability for any loss arising from any action taken, or omission, on the basis of the content in this article or any documentation and external links provided.

Nexia SAB&T is a member firm of the "Nexia International" network. Nexia International Limited does not deliver services in its own name or otherwise. Nexia International Limited and the member firms of the Nexia International network (including those members which trade under a name which includes the word NEXIA) are not part of a worldwide partnership. Member firms of the Nexia International network are independently owned and operated.

Nexia International Limited does not accept liability for any loss arising from any action taken, or omission, on the basis of the content in this publication or article or any documentation and external links provided.

References to Nexia or Nexia International are to Nexia International Limited or to the "Nexia International" network of firms, as the context may dictate.

For more information, visit www.nexia.com.