Are you *prepared?*

Are you prepared to be cyber resilient in the digital age?

syrex
CLIENT INSPIRED SOLUTIONS

Curzon Place, Turnberry Office Park,
48 Grosvenor Road, Bryanston, 2021

T 086 11 syrex (79739) **E** info@syrex.co.za
Suite 176, Private Bag X51, Bryanston, 2021

www.syrex.co.za

contents

Executive summary

Global spending on cybersecurity solutions is expected[1] to surpass the $1 trillion mark cumulatively in the period from 2017 to 2021. Last year alone the worldwide cybersecurity sector was worth more than $120 billion. While this can, in part, reflect a growing awareness of the need for IT security products and services, it also points to the growing number of cybercrime incidents taking place around the world.

Rank		%	2017 rank	Trend
1	Cyber incidents (e.g. cyber crime, IT Failure, data breaches)	38%	1 (30%)	=
2	Business interruption (incl. supply chain disruption)	34%	2 (29%)	=
3	Changes in legislation and regulation (e.g. government change, economic sanctions, protectionism, Brexit, Euro-Zone disintegration)	27%	5 (25%)	^
4	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	23%	3 (28%)	v
5	Natural catastrophes (e.g. storms, floods, earthquakes)	23%	7 (17%)	^
6	Fire, explosion	19%	6 (21%)	=
7	New technologies (e.g. impact of increasing interconnectivity, nanotechnology, artificial intelligence, 3D printing, drones)	19%	10 (14%)	^
8	Climate change/increasing volatility of weather NEW	16%	–	^
9	Loss of reputation or brand value NEW	16%	–	^
10	Macroeconomic developments (e.g. austerity programs, commodity price increase, deflation, inflation)	13%	3 (28%)	v

The Top 10 Business Threats in South Africa[1]

In research published earlier this year covering 2017, 54 percent of organisations admitted to being hit by instances of ransomware. The median financial impact per affected business – a staggering R1.8 million. Even more significantly, an average of two ransomware attacks per organisation were reported.

Even South African companies have not been immune to this. Recent media reports are filled with high-profile incidents of ransomware and other data breaches occurring. While the extent of the local impact is difficult to determine with companies not always disclosing attacks or breaches, expectations are that these are significant.

1. https://cybersecurityventures.com/cybersecurity-market-report/

Executive summary continued...

Given the connectedness of business today and growing consumer expectation for digital solutions, decision-makers need to rethink their approach to cybersecurity. Data has been described as the oil of the digital age. It should therefore stand to reason that protecting it should be an organisational priority. However, this [protection] is not something that happens in isolation of other business processes or is a once-off. Instead, the business should see cybersecurity as an ongoing concern that has to permeate all facets of the enterprise.

In this White Paper, Syrex will examine the steps companies should take to protect themselves (and their data) before, during, and after a data breach takes place. Cyber resilience will be a defining feature of the modern organisation and it must have the solutions in place to ensure its efficacy in dealing with the continually evolving cybercrime environment.

This requires a change in thinking. No longer is it good enough to be aware of cyber security and the associated requirements. Today, it is all about embracing an all-encompassing approach that includes cyber security, disaster recovery, and business continuity management. This is what cyber resilience is all about – it is the ability of a company to continue delivering on its strategic business directives in the face of malicious cyber attacks.

Decision-makers should think of it as a natural evolution from pure cyber security to a cyber resilience approach that is more of a methodology focusing on the measures and policies that need to be put in place to ensure continual business operations

With one in five small to medium enterprises (SMEs) facing closure because of a data breach, prevention should be a top priority. No country can afford to ignore the threat of cybercrime and the impact it can have on its economy and potential for growth.

It is a case of when, rather than if, a data breach will occur. Those organisations who have put in place the correct measures to safeguard their data, and mitigate the risk of an attack, will be the ones best able to adapt to this dangerous new connected world.

South African market assessment

Irrespective of company size, all businesses should be aware of the risks associated to storing, managing, and analysing data in a connected environment. While there is not a culture of data management in South Africa yet, regulation like the Protection of Personal Information Act (POPIA) and the European General Data Protection Regulation (GDPR) are contributing to increased awareness.

Sadly, many organisations are not taking compliancy seriously despite the significant fines and reputational damage they could face if found in breach. However, while regulatory compliance is important, Syrex has found that the focus should be on the impact that a data breach could have on the organisation. This forms part of an integrated approach that will see alignment to compliance requirements as well.

Several breaches have been happening in South Africa, with the focus more recently being on that of ransomware. Companies are not able to effectively deal with it. So, even though they have backup solutions and security policies in place, these do not cover all the touch points. Thanks to social media, connected devices (through the Internet of Things), and people's growing reliance on mobile, companies are faced with multiple channels of attack into their organisational systems.

This is where the difference between cyber security and cyber resilience becomes evident. By focusing too much on the nuts and bolts of security solutions, decision-makers risk losing sight of the bigger organisational impact of attacks. It is not a case of installing software and thinking that is enough to stay secure. It is about a systemic approach to all facets of cybersecurity, business continuity, and organisational resilience to keep operating in the wake of these threats and attacks.

South African market assessment continued...

When it comes to small businesses, much focus is placed on maintaining their core activities and daily operations without much attention being placed on IT security and data protection. There is also a view that they are not appealing targets to hackers or other malicious users.

This could not be further from the truth. Even though large multinational organisations present lucrative targets, the fact that security is minimal (generally speaking) in small businesses, mean they are easy pickings for quick attacks.

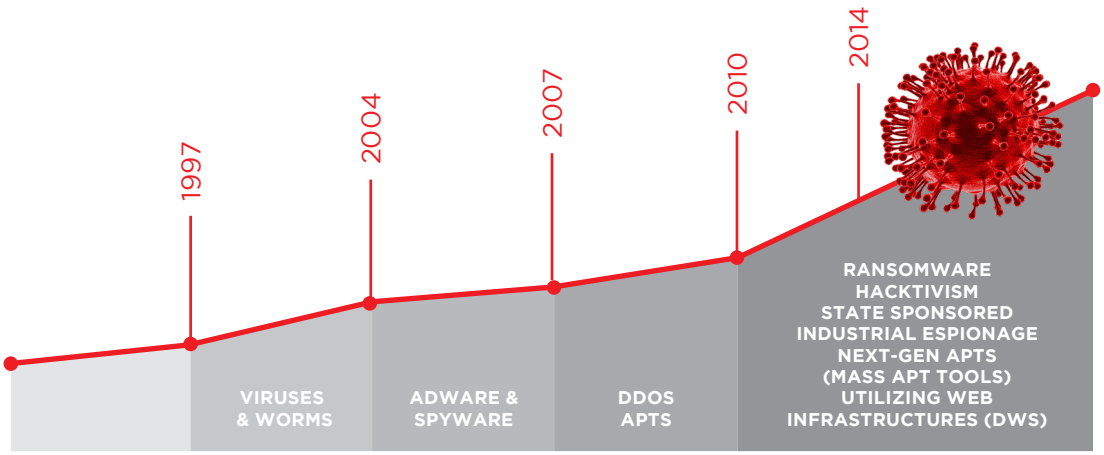
Cybersecurity is not a one-size-fits-all approach or simply a matter of installing a piece of software for protection. It entails a layered approach that incorporates the technology, the systems and processes, as well as the human resources within an organisation. In this way, security covers all the potential entry points into the organisation. This layered way of combating cybercrime is something that is integral to how Syrex approaches security and talks to all the various solutions and processes it has in place and offers its customers.

EVOLVING THREAT LANDSCAPE

Cyber risks are as old as technology itself. Even before the first connected computer, we had such delightful viruses as the Bouncing Ball and Stoned. While certainly annoying and degrading the performance of (what would by today's standards be considered too slow to use) computers of the time, there was no significant financial risk to yourself or your company.

However, with technology permeating every facet of our lives in the digital world, cyber risk has evolved to become a systemic threat to businesses the world over. Perhaps more concerning for every decision-maker, is how threats are becoming increasingly sophisticated on a regular basis. For example, in 1997 there were 1 300 known computer viruses. By 2014, more than 100 000 new malware variants were identified daily.

South African market assessment continued...



An ever-changing threat landscape. Every year THREATS are becoming more sophisticated and more frequent. (Source: Check Point)

We must keep in mind that as our technology becomes more advanced, so too does the threat landscape. So, even though security software is updated on a continual basis, it is a never-ending battle against malicious software that is even faster to evolve. What is more, incidents of successful attacks are more frequently reported in the media.

Considering how the threat landscape encompasses things like hacktivism, ransomware, state-sponsored industrial espionage, next-generation advanced package tools, compromised Web sites, and many more, a constant state of vigilance is required.

INCIDENT RESPONSE EXAMPLE

South African market assessment continued...

By way of example, managing an incident of ransomware encompasses four key steps – preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity:

Preparation

This entails preparing a business for the types of malicious events and incidents likely to occur. In cybersecurity, once an incident has been detected it is already too late. A business therefore needs to do a detailed security assessment of its existing processes and solutions. This should include a candid view of how effective it is in dealing with various kinds of attacks, including ransomware.

End-user education is a vital part of this. After all, it is likely that an employee will be the first point of contact between ransomware and the organisation. The classic example of leaving a USB drive containing one file (Salaries.xls) that is infected with malicious software still holds true. The best policies and procedures in the world mean very little if someone opens a compromised email or document or visits a spoofed Web page.

Phishing attacks take on many different forms in the connected business. They are also getting increasingly sophisticated. Users need to be continually educated on how to identify attacks or scams.

Beyond the social aspect of cybersecurity, companies must ensure that their anti-virus and endpoint security solutions remain updated and maintained. Installing a solution is not enough. It must be managed all the time along with the cybersecurity policy to reflect changing attack styles, types, and trends.

For preparation to be effective, the business must have a plan in place on how to respond to malicious software. A clearly defined, up-to-date incident response plan with pre-defined roles and responsibilities is imperative in the preparation phase.

Detection

If an organisation detects its data has been compromised, it becomes mission-critical to identify the systems that have been infected as quickly as possible. The company needs to minimise the risk to mission-critical files and, in the case of ransomware, limit the extent at which data gets encrypted and be held for ransom.

South African market assessment continued...

Even though each variant of ransomware and other malicious attacks are unique, companies must make sure that their cybersecurity systems are able to effectively identify when instances of attacks occur.

Analysis

Analysis consists of two elements – malware identification and root cause analysis.

It is important to identify the variant of ransomware or other malicious software within the network. Each variant has unique capabilities that require different approaches to combat. This is potentially one of the more difficult stages of combating attacks as few companies have the internal resources on hand to identify the variant and deal with it effectively.

A root cause analysis should be done to help the business understand how the malicious software was introduced into the organisation. A more formal analysis can be done during the post-incident phase, but it is important to get an indication as quickly as possible to avoid a repeat of the infection cycle while still combating it.

Containment

Once a system has been identified as infected with malicious software, it should be removed from the network. This means not only 'unplugging' it but disabling its wireless connectivity (in the case of mobile devices). While the temptation exists to immediately shut it down, the security team should put the system in a state of hibernation to more effectively analyse what caused the infection in the first place.

Furthermore, mobile devices should be isolated on their own virtual network. Tools can then be used to manage these devices for remote blocking and wiping of data.

If a system cannot be identified quickly enough to counter the rate of infection, the company should consider taking critical files off-line to minimise the potential damage. All access to file servers (whether on the cloud or locally hosted) should be terminated with immediate effect.

Eradication and recovery

This phase deals with removing the malicious software from infected systems. Once done, that system should be rebuilt from a trusted source with testing being conducted to ensure the effectiveness of its security.

South African market assessment continued...

As an additional precautionary measure, all passwords inside the organisation should also be changed. Web sites and email systems need to be continuously reviewed and monitored for potential entry points as well. It is also important to consider something like multi-factor authentication to curb the practice of employees simply writing down their passwords (especially if they are changed often).

When the malicious software has been contained and the root cause identified, only then can the road to recovery commence. Depending on how the attack started, companies can perform a restore process from their local backups or the hosted environment.

In an ideal world, ransomware can be overcome by having the systems and processes in place to ensure business continuity. However, some companies might feel they have no choice but to pay the ransomware demands. This could either be due to not having adequate backups in place or exhausting all possible options. The risk this poses is that it gives credibility to the attackers and could result in future attacks being perpetrated.

Post-incident activity

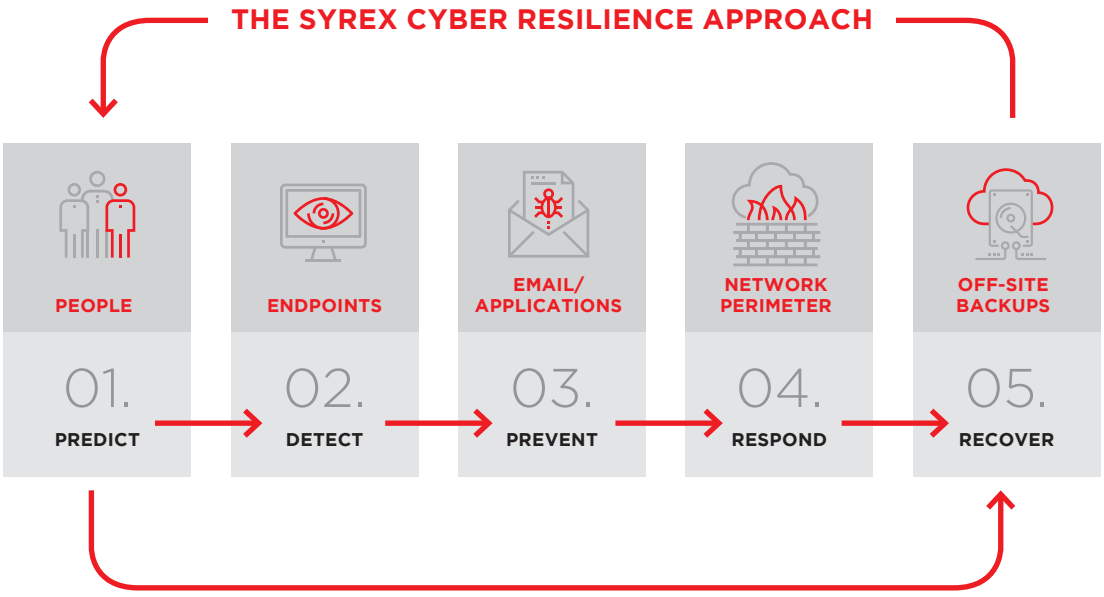
The final stage sees detailed post-incident activity taking place. This includes reviewing the lessons learnt during the incident response, what detection and security controls may or may not have been effective, and what could be done to avoid a future occurrence from happening.

Each organisation will be unique in its approach. The key is to honestly assess and discuss the incident findings with all relevant stakeholders and adapt the specific systems of the business accordingly.

The Syrex approach

The core principle behind the Syrex approach is that of adopting a layered way of managing cybersecurity. As an organisation, we are driving cyber resiliency as the cornerstone of how we manage data protection in its entirety. From protection to recovery and business continuity, Syrex believes that this is fundamental to ensure that each of the various entry points into an organisation is safeguarded.

Realistically, paying a ransom is not a solution. Nor is losing data and not being able to get the business up and running as quickly as possible. Preventative maintenance is vital with businesses requiring an all-encompassing cyber resilient approach.



Cyber Resilience *– No longer is it good enough to be aware of cyber security. Today, it is all about embracing an all-encompassing approach that includes cyber security, disaster recovery, and business continuity management. This is what cyber resilience is all about – it is the ability of a company to continue delivering on its strategic business directives in the face of malicious cyber attacks.*

The Syrex approach continued...

LAYER 1 – E-MAIL

A large amount of ransomware and other malicious content is distributed via e-mail. It is imperative that a business blocks this by implementing a comprehensive e-mail security solution. While there are many products available, the world leader is Mimecast.

The company specialises in cloud-based email management and is at the forefront of research, development, and continuous innovation in terms of dealing with cybercrime in this environment

When it comes to security, Mimecast delivers a cloud-based service that delivers threat protection, is adaptable to stay ahead of the latest attacks, email protection, is available to prevent any communication outages, and recovers the data that matters most. Like us, it understands the continually evolving threat landscape. The Mimecast solution is designed to keep email flowing in the event of an attack and recover lost data quickly, so business operations can continue as normal.

LAYER 2 – INFRASTRUCTURE

Your infrastructure and network should be protected by a next-generation firewall. Historically, this type of solution would have been out of reach for a small business from a cost perspective. However, with advances in this segment and a growing small business market, there are quality firewalls available to the SME. These companies now have access to enterprise-level protection without the complexity, cost, and expertise previously required.

Check Point, for example, has great small business devices that are affordable but still offer the same protection and security that are provided to large enterprises.

Additionally, strong encryption on a wireless network should be used (for example, consider WPA2 with AES encryption). Further protection can be provided by encrypting wireless communication using a virtual private network (VPN).

The Syrex approach continued...

Cloud storage and applications are great for small businesses. However, they should be treated with caution. Any content migrated to the cloud can, at times, be out of the control of the organisation. Cyber criminals are taking advantage of weaker security by some cloud providers. Decision-makers should also be weary of how those cloud services are accessed. Many companies use open remote desktop connections that are not secured behind a VPN connection. This leaves their cloud servers exposed if malware is present on the internal network.

LAYER 3 – ENDPOINTS

Companies must protect devices on the network from running unauthorised programs that could compromise the network. The endpoint layer should run in conjunction with a next-generation firewall to ensure best practice around content, application, and network protection.

These next-generation firewalls combine the traditional solution with other network device filtering functionalities. It can include an application firewall using in-line deep packet inspection and intrusion prevention systems. Syrex partners Check Point provide a fully managed service for enterprise firewalls encompassing these next-generation components. Using a single, consolidated view of the security infrastructure, security professionals can do more work with less stress and redundancy, reducing operational expenses and providing peace of mind.

PREVENT ZERO-DAY ATTACKS

Threat Extraction & Emulation for Endpoints

Deliver sanitised content

Emulation of original files

Protects web downloads and file copy

IDENTIFY & CONTAIN INFECTIONS

Anti-Bot for Endpoints & Endpoint Quarantine

Detect & Block C & C

Pinpoint infections

Quarantine infected host

EFFECTIVE RESPONSE & REMEDIATION

Automatic Forensic Analysis & Attack Remediation

Incident analysis – saves time & cost

Make network detection actionable

Understand Endpoint AV detections

Clean & remediate the full attack

Sandblast Agent *– Zero-day Protection for Endpoints. (Source: Check Point)*

The Syrex approach continued...

LAYER 4 – HUMANS

Humans remain the biggest risks in a business. It is also the most difficult aspect to manage as people think differently and security is seldom top of mind. Businesses need to look at enforcing policy and educating staff regularly about security.

A business must define and enforce policy around access and usage. Risky applications such as Bit Torrent and other peer-to-peer file-sharing services should be blocked. Users should be educated about how cyber criminals build profiles of company employees to ensure that phishing and social engineering attacks are more successful.

Companies must also enforce a strong password policy. In many cases, this is the first line of defense and quite often overlooked.

Ultimately, people are going to make mistakes when it comes to security. Often, they might not even be aware of their indiscretions. It is therefore important for the business to implement cyber security solutions that balance the need for protection without being too restrictive and negatively impacting employee productivity.

LAYER 5 – DISASTER RECOVERY AND BUSINESS CONTINUITY

This layer should be paramount in any business. Having secure, encrypted backups will ensure that a business can survive even if compromised. Most small businesses find it adequate to copy data onto an external hard drive and believe this is an effective solution. Sadly, it I not. If the source data is infected, then so is the backup.

Small businesses also seldom test their backups. They quickly discover that it might be useless when disaster strikes.

An effective disaster recovery and business continuity approach minimise human intervention. People make mistakes, they get sick, and have accidents. Backups should be automated with transparent granular reporting and control.

The Syrex approach continued...

Data backups should be held off-site in a secure location. Companies must choose a partner that has access to a data centre that they control. Furthermore, data should be encrypted at source using 256-bit AES (GCM) encryption. It must also be protected using TLS ciphers during cloud and off-site backup communication.

Backups should also provide the business with several retention options as well as an archiving option for legacy data. A solution should be selected that can scale as the business grows. Companies should avoid those solutions that charge license fees per device that is backed up.

Of course, the single most important aspect of any disaster recovery and business continuity solution is how easy it is to recover. What recovery options does the backup provide? How long will the business take to become operational once an infection has been removed or a compromise fixed?

For example, Redstor offers businesses the ability to access critical data immediately whilst performing a full or partial system restore. This provides the option of ensuring a company can restore operational critical data, whilst other files restore in the background.

Conclusion

Decision-makers in South Africa (and the rest of the world) need to be educated about the importance of effective cybersecurity policies and solutions. In the digital business environment, ignorance can no longer be used as an excuse. Similarly, no company (irrespective industry or size) can afford not to have cybersecurity integrated into all facets of the organisation.

Even though there are numerous freely available cyber security solutions available, the reality is that they do not offer the same degree of robustness as premium versions. And ultimately, do you really want to leave the protection of your organisation up to a piece of software anybody can download and is ostensibly designed for consumer application?

The biggest concern around cybersecurity in recent months is that of ransomware. According to Check Point research[2], these attacks have escalated 300 percent since January 2016 with an incident occurring every 40 seconds. With companies of all sizes across industry sectors all vulnerable to these and other attacks, decision-makers need to revisit their cybersecurity approaches.

IT is no longer just an enabler for business but has a direct impact on its operational structure. However, the Internet, broadband, high availability of data, and open access have created the potential for many different waves of attack. This means that there is not a single piece of technology capable of addressing all facets of cybersecurity.

Cybersecurity in the digital business environment is not about enforcing draconian policies that act as a hindrance for productivity. Instead, it is something that must be monitored effectively and continuously as organisations seek to protect themselves from malicious attackers. It is imperative to embrace cyber resiliency as a way of doing business if companies are to mitigate the risks that operating in a digital environment can bring.

Organisations need to think of risk as total approach that incorporates prevention, security, and recovery if they are to remain effective and safeguard their data. More importantly, security is not purely about technology any longer but also about the people and processes. Cyber resiliency helps with this and prepares businesses for those times they are not only under attack but need to recover from it as well.

2 https://www.checkpoint.com/downloads/product-related/whitepapers/wp-ransomware-identify-block-and-remedy.pdf

Glossary

Advanced package tools: Free software user interface that works with core libraries to handle the installation and removal of software on Debian, Ubuntu, and other Linux distributions.

AES encryption: The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the US government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

Cyber resilience: Refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events. Cyber resilience is an evolving perspective that is rapidly gaining recognition.

Hacktivism: The practice of gaining unauthorized access to a computer system and carrying out various disruptive actions as a means of achieving political or social goals.

Internet of Things: The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Phishing: The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Ransomware: A type of malicious software designed to block access to a computer system until a sum of money is paid.

TLS ciphers: A cipher suite is a set of algorithms that help secure a network connection that uses Transport Layer Security (TLS) or Secure Socket Layer (SSL). The structure and use of the cipher suite concept is defined in the TLS standard document.