www.liquid.tech

The critical components of a successful cyber security programme

Cyber Security White Paper
August 2021

BUSINESS | CLOUD | CYBER SECURITY
HOME | LABS | NETWORKS | SATELLITE | SEA

AFRICA'S DIGITAL FUTURE

LIQUID
CYBER SECURITY

An **in-depth examination** of evolving cyber security threats, the structural components necessary to protect systems and networks, and the management of internal risks.

Cyber Security White Paper
August 2021

Contents

Introduction: Data is the new oil

Data is widely considered to be the new oil; **a valuable asset that is essential to the success of every business.** The process of collecting, managing, storing, and sharing data therefore represents a high level of risk for any company or organisation, and it is a top priority to protect it from threats from both within and outside the entity.

"Rapid digitalisation poses an entirely new level of threat – and it comes at a time when cybercriminals are becoming more sophisticated and as new threats to data security emerge every day."

In recent years, **the rapid pace of digitisation has significantly heightened the risk of bad actors breaching data security.** Since 2020, this risk has increased exponentially as businesses across all sectors have had to adapt to new ways of working in the wake of the Covid-19 pandemic.

When the hard lockdown was introduced in South Africa in March of that year, changes to systems and procedures had to be instituted virtually overnight, vastly expanding the sphere of risk to include multiple off-site workers. This has been complicated by the fact that hacking, spamming and phishing techniques are becoming more sophisticated and continue to evolve all the time. The risk to confidential business information, personal information, and financial transactions has never been greater.

Now, more than ever, it is critical for every business to identify the nature and extent of the risks to its data security **and to ensure that its cyber security programme has all of the essential components in place to protect operations against attack.**

The value of data

The value of data lies in the fact that it is **essential to the enablement of every business.** It is each business's single most important asset and is critical to decision-making. The data needs of businesses nevertheless differ by company as well as by sector. This is why it is so important that the vulnerabilities of each system or service be identified and analysed individually and that the critical components necessary to protect that business be developed specifically to meet its requirements.

"Data means different things to different organisations and is used in many different ways. The common denominator is that it is almost certainly the organisation's single most important and valuable asset – and therefore one of its most vulnerable."

In the **medical field,** for instance, the accuracy of patient records is essential to ensure that each patient is diagnosed, treated, and monitored correctly. These records are, of course, highly sensitive and therefore have to be stringently protected against breaches. Increasing digitisation and the sharing of information between practitioners, providers, and institutions only makes this data more vulnerable. This is largely because it is no longer simply a case of protecting personal information on individual systems, but a matter of **protecting information as it moves between various environments.**

In the **agricultural sector,** data is used in a different way and therefore the nature of the risk is different. Detailed data is collected and analysed in order to make operations more effective and productive. Records of planting times, rainfall, fertiliser usage, and yield are essential in order to maximise output. So, while agricultural operators do not have the same level of risk when it comes to personal records, **their operations would be crippled if their data were to be corrupted or lost.**

In **manufacturing and retailing**, the quality of data and the way in which it is managed is the very foundation of a company's competitive advantage. Data enables companies to keep track of metrics such as inventory, sales, payments and, in particular, customer engagements. Rich and well-managed data sets give them the capacity to respond quickly to challenges as diverse as stock shortages, product defects, changes in demand, and customer dissatisfaction. **This flexibility is nothing short of gold** and could, in times of stress and crisis, even mean the difference between survival and failure.

In **ICT,** the value of data differs yet again. Companies operating in this sector need to be agile and need to respond quickly to market developments. The data they accumulate enables them to identify the responses and solutions that have been successful and to analyse those that haven't worked. In this environment, data again gives companies a **competitive advantage,** especially by enabling them to respond quickly to client needs and to diagnose and address problems timeously and effectively.

The quality of customer service management is another key differentiator and the business's systems need to be robust and secure enough to support efficiency in that area. Like manufacturers and retailers, ICT companies benefit from well-managed and efficient customer engagement, all of which is data driven. In this environment, users also have to have the ability to **collect and analyse behavioural data** in order to maximise their selling potential.

In the case of **banks and financial institutions,** cyber security takes on an entirely different meaning because these institutions have the responsibility to protect not only the personal identities and information of their clients, but their **financial transactions and records** too. In a related way, online retailers have to guarantee the security of transactions on their sites and the integrity of the information they hold on their clients.

In all instances, the precipitous move to cloud utilisation in recent years has only heightened the risk of data being compromised and has brought with it the need for **an entirely new level of security.**

Defining the risk

Unsurprisingly, the 2021 Cloud Security Report shows that organisations continue to adopt cloud technology rapidly in order to deliver on key business objectives. The report indicates that **33% of the 500 organisations surveyed are running more than half of their workloads in the cloud today,** and that this percentage is set to rise by 56% by the end of 2022. More significantly, **71% of the organisations surveyed indicate that they are pursuing a multi-cloud strategy** to facilitate the integration of services, improve scalability, secure business continuity, or take advantage of solutions that make use of the Internet of Things (IoT).

In 76% of cases, on-premise systems are augmented by at least two cloud providers, meaning that businesses are now operating in an expanded and diversified digital landscape.

In August 2020, Liquid Intelligent Technologies commissioned a survey to gain greater understanding of these developments with specific reference to the African environment. A notable 57% of respondents stated that their **threat levels had risen significantly since the advent of Covid-19,** especially as 71% were making use of cloud-based services.

A follow-up survey conducted in July 2021 examined a number of evolving issues, including **concerns about security breaches related to cloud-based solutions and the increasing number of employees working from home.**

In South Africa, 79% of respondents indicated that they had experienced cyber security threats in the preceding twelve months, while 78% of respondents in Kenya and 82% in Zimbabwe indicated the same. Significantly, an average of 91% of respondents across all three countries stated that they are making use of cloud-based services in their businesses.

As importantly, 69% of respondents in South Africa indicated that the majority of their staff are working from home, with Kenyan respondents tracking closely at 66%. In Zimbabwe, the figure is much lower, partly due to lack of infrastructure, with only 32% of respondents indicating that the majority of their staff are working from home.

The increasingly common **hybrid model of working,** which encompasses both on-site and off-site working arrangements and makes extensive use of cloud-based applications, is raising concerns about the security of data, the ubiquity of shadow IT, and the many implications of serious security breaches.

Cloud utilisation dramatically increases the risk of breaches and of data being compromised, especially if the appropriate safeguards are not put in place. This is because **threats can no longer be contained or managed within the private network perimeter.** Each off-site device connected to the organisation's network increases the threat level, as does exposure to unsanctioned cloud-based applications and the sometimes-porous borders between these applications and the internet in general.

"With remote working now fully entrenched within most organisations, it is no longer feasible – or safe – to allow multiple devices just to follow users and data throughout the working day. A new level of security is needed to ensure that a single policy and procedural framework can follow users – and the data they have access to – wherever they go."

Globally, 64% of workers are now working remotely, an increase of 148% since the start of the pandemic. This has driven a 97% increase in the use of managed personal devices which, in turn, has nearly doubled exposure to risky apps and external web sites from within corporate systems.

A further threat in most organisations – and one that is less well-known – is that of **shadow IT.** Also known as embedded, fake, stealth, rogue, feral, or client IT, this term refers to IT systems, applications and processes that are deployed in a decentralised way by individual departments or staff without the knowledge, input or control of the centralised IT function. This is usually done to work around shortcomings within the centralised system but can create vulnerable back doors that provide easy access.

Securing networks at key touchpoints

When addressing information security threats, both for our own company and for our clients, we draw on the well-known **CIA Triad.** This identifies the three critical areas of information security, namely **confidentiality, integrity, and availability.** Each has to be considered when developing IT policy and strategy; identifying and mitigating information security risk; and implementing both technical and non-technical security controls.

At Liquid Intelligent Technologies, we now have a **dedicated cyber security unit,** supported by strategic vendor and service providers as required, which considers the CIA Triad requirements to give context to all of our work and to provide **end-to-end digital security solutions for our clients.**

While we have been operating in this space for some time and have fifteen years of knowledge in the field, we recently took the decision to **streamline our cyber security offerings into one unit** in order to be able to offer a single point of contact and control for IT and cyber security decision-makers and to help them secure their businesses effectively.

"The entire environment needs to be protected, from the periphery right through to the core. Valuable data – whether in use, in motion, or at rest – has to be reliably secure."

A comprehensive framework and in-depth defence approach that is appropriate to an organisation's landscape is needed to secure data, individual and organisational devices, systems, networks, and organisational exposure in the cloud, as well as to safeguard decentralised services.

At Liquid Intelligent Technologies, our approach – and our recommendation to customers – is to establish **a cyber security framework** that is enabled using best practice guidelines.

This should comprise of the following two key pillars:

1. An **Information Security Management System** (ISMS) that aligns to best practice standards such as the ISO 27001 Standard. It is critical that the ISMS addresses the governance, risk, compliance, people, process, and technology concerns needed to meet all CIA Triad requirements.

2. A **Cyber Resilience Security Control Framework** that supports the ISMS, using a best practice standard or framework that is most appropriate to cover the organisation's business and information landscape. Examples of such standards and frameworks are ISO 27001 Annex A, the NIST Cyber Security Framework (CSF), and the CIS Top 20 Security Controls. Specific industries should also consider industry standards such as PCI DSS, SWIFT CSP, etc.

The Cyber Resilience Security Control Framework should consist of technical and non-technical security controls that support the ISMS and have the following key cyber security resilience abilities: identification, protection, detection, response and recovery, testing, situational awareness, as well as the ability to learn and evolve.

Our cyber security offering delivers all of the key competencies necessary to achieve the above-mentioned pillars and outcomes:

1. **Security Consulting Services,** which consist of both technical and non-technical advisory and assessment services.

2. **Security Product Solutions and Security Professional Services,** which are enabled by embracing the latest vendor offerings and evolving trends.

3. **Security Management Services,** which provide threat defence by assisting those organisations that are not able to effectively manage their own cyber security posture.

4. **Security Operation Centre Services,** which provide threat detection, actionable threat intelligence, and threat response for organisations that don't have the ability to do so or are unable to establish situational awareness and provide assurance to their stakeholders.

Dealing with the threat within

Cyber criminals understand where the vulnerabilities lie within a business. They know that employees have many entry points and, using a variety of methods – including phishing, vishing, links to malicious web sites, and malware – they can use them to penetrate any network.

As the remote workforce grows, **opportunities to penetrate networks are proliferating.** This is especially true if off-site workers access networks through unprotected personal devices. A Kaspersky report published in May 2020 indicated that up to 75% of employees working from home at the time had not received security awareness training and that the security on their devices had not been upgraded to protect against network intrusions.

We recognise that cyber security is about more than just technology; it is about helping and securing the people within a business as well as the devices they use. Correctly trained and well-supported employees are a company's greatest security asset and its first line of defence; a human firewall.

"Managing the threat to data security from within the organisation has to be multi-faceted in order to be effective. It also has to be an iterative process. Employees need continuous training and support in order to be able to identify and deal with new threats as they arise. They also need devices that are secured against the most sophisticated forms of invasion."

The value of empowering employees to be a human firewall cannot be underestimated. A report entitled *The state of cyber security in Kenya and South Africa in 2020,* which was the output of the survey we commissioned at the height of the pandemic, revealed that **compromised passwords** (72%) and **phishing attacks** (67%) pose the greatest threats to company networks. The report resulting from the follow-up survey conducted in 2021, entitled *IT Decisionmakers' views on Cyber security in South Africa, Kenya and Zimbabwe,* shows that this is a consistent trend.

In all three countries, the top cyber security threats are **e-mail attacks, malicious applications, web- and cloud-based attacks, and data breaches.** In Zimbabwe and Kenya, this is compounded by a high risk of malware and ransomware being introduced onto corporate networks via the cloud. All of these threats have a common denominator: **human error.** A single, absent-minded click on a phishing e-mail or a careless visit to an insecure web site can expose a whole corporate network, often with costly or devastating consequences.

This is one of the many reasons we have **a dedicated unit** that is exclusively focused on developing cyber security solutions and services **in partnership with some of the world's leading vendors and providers.** Through this, we can ensure that there is internal protection in place at multiple levels, including awareness training.

"At Liquid Intelligent Technologies, we believe that the first step to ensuring a secure digital environment is training employees so that they can safely navigate and grow in a digital-first world. This enables us to deliver the 'secure people' aspect of cyber security as confidently as we deliver every other component of our cyber security solutions."

To find out more about what Liquid Intelligent Technologies can do for your business, visit us at

www.liquid.tech

or contact us on the following

LinkedIn 

Facebook 

Twitter 

Email