Whitepaper

PC and Device Encryption for South African Organisations: You have Been Told You Need it, Now Know Why

POPIA legally compels your business to maintain security safeguards, to not be negligent else risk fines & your business. Here are the facts.

May 2021

Introduction

Any company or organisation that holds sensitive data has a critical need to ensure that the information stored is properly protected. Businesses that collect personal, private information – data that is used to deliver superior service and make employees and customers' lives that much easier – nevertheless enter into a trust with employees and consumers. In all-too-common cases already seen overseas, when data breaches occur and make headlines, reputational damage ensues. And, when data breaches occur in industries where governmental regulations are involved, organisations found to be careless in safeguarding data can also face substantial fines. In other cases, the issue is not customer data but sensitive intellectual property belonging to a company, the secrecy of which is essential to that business' competitive advantage.

Proper protection of data can also open the door to new business relationships, especially with institutions that have policies of exclusively selecting vendors and partners that meet certain careful criteria when it comes to data security practices. But in all these cases – whether an organisation is incentivized to invest in data security in order to protect their reputation, to meet regulatory requirements, to safeguard intellectual property, to prepare for new business relationships, or for any other reason – data encryption is one of the first and most critical tools in the data security playbook.

Importantly, implementing encryption does not have to be difficult or cumbersome to an organisation's operations. In fact, encryption functions best when it is unobtrusive and when it is invisible to users.

Data Breaches

With an established Information Regulator in South Africa the commencement of the South African Protection of Personal Information Act – or **POPIA** as it is commonly known – from 1 July 2021, the statute has legal grounds to compel and take punitive actions on any organisation found to be negligent with personal data and those found transgressing the principles of POPIA. This forces South African businesses and organisations of all sizes to review, assess and in most cases, improve their current data security procedures and practices to mitigate risks to become (and remain) compliant.

The news is rife with high-profile examples of data breaches in South Africa and. While the press gives

the most coverage to black hat breaches stemming from hacking and malware intrusion, in truth, data from Privacy Rights Clearinghouse finds that for more than a decade – in fact since 2005, a full two-thirds of breaches have resulted from user/employee oversight or malfeasance including lost and stolen PCs, mobile devices and electronic storage. One example is *Healthcare provider Premier Healthcare which reported the theft of a laptop containing the sensitive personal and clinical information of over 200,000 patients.*

A stolen laptop or a misplaced USB storage device for example could result in exposed records which might consist of identity numbers, usernames, and passwords, financial or medical information, corporate intellectual property, child information, client lists, and other digital information that amounts to a violation of privacy and puts individuals and organisations at risk for identity fraud and losses.

It is important to know that while data breaches of larger magnitudes grab headlines, it is small and medium-sized businesses that can suffer the most harm from them. For SMBs with less capacity to absorb hardships than larger enterprises, the reputational damage, financial pressure of a large regulatory fine, or loss of intellectual property from a data breach can be a devastating – and sometimes fatal – blow.

Keeping Criminals Away from Our Data

SMBs can often have the most to gain from implementing data security measures like encryption and proper device-entry-access (authentication controls). The goal of data security is to keep criminals, corporate spies, disgruntled ex-employees, insider threats, and anyone else with bad intentions from accessing sensitive information. Encryption and Access-Control are highly effective measures because it renders data such that it is unreadable, even if it falls into a criminal's hands.

Other measures working in tandem with encryption are important to robust data security as well. While encryption is a powerful tool, the practices of an organisation's employees and the safety with which they handle data and minimize threats are just as important. Keeping employees well trained and aware of their responsibilities with data – such that they do not put their systems and devices at risk – are key components to achieving effective data security.

For the purposes of this whitepaper, we will focus on data residing on devices – hard drives, smartphones, tablets, external drives – where it ought to be encrypted in case those devices become lost, stolen, or otherwise accessible/compromised.

The "Nuts and Bolts" Of Encryption

Encryption is a powerful defence for data at rest when a device's power is off, and the password to bypass it is secure. The Department of Health and Human Services offers a useful definition of satisfactory encryption with its HIPAA security rule, describing it as "*an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key…and such confidential process or key that might enable decryption has not been breached*."

In short, encryption is essential to data protection and rendering private information unreadable, but it has limits. If a device is stolen or left unattended with the power on and login credentials entered (or if the password is known or can be learned), then encryption is no longer an effective defence.

Employees will always seek out ways to be their most productive, and this means that thoughtful training in best practices and the importance of data security is needed for most encryption regimens to be truly effective. Bad passwords effectively negate encryption; too often employees will write down their passwords near the device they need to authenticate, or passwords written on the surface of the USB devices they need to read or have used common passwords which can be easily guessed by a savvy attacker. Devices left unattended during open sessions leave data fully exposed. In some scenarios, formerly authorised users become unauthorised (ex-employees, for example), but their access is not revoked as it ought to be.

There are also cases like the one in 2018 at Coca-Cola, which suffered a data breach when an employee took home 55 work laptops – likely with intentions beyond just getting some work done over the weekend. Employees should be trained in proper password security and vigilance over their credentialed sessions, and organisations should demonstrate proper diligence in managing access controls, as well as keeping track of all the company or employee devices with access to sensitive information.

However, in the end it is most effective for organisations to support workers by taking the responsibility for data security out of their hands as much as possible. Data controls than can be implemented remotely are able to provide organisations with the capabilities they need to delete sensitive data from compromised devices and to revoke access to users in the case that credentials are compromised (either because login information has been stolen or because an employee has gone rogue.) It's a best practice to remove access for employees and contractors when they leave the company for whatever reason - companies need the tools to cut off access and remove company data from ex-employees' own personal devices as well.

The right way to reconcile the need for data security with the needs of employees is to implement security that steps so lightly that workers forget it is there while ensuring it is powerful enough to be effective – and training employees to understand why data security is so critically important.

Who Is Buying Encryption?

Which organisations are investing in encryption? Let us look at some of the primary motivations:

When encryption is necessary (or all but necessary) to meet compliance regulations

Organisations subject to regulation – such as those in South Africa covered by POPIA, the EU covered by GDPR, or those that apply to US industries like HIPAA which oversees the medical industry or FINRA which watches the financial industry – most often MUST implement data encryption to be in good standing. Regulators and agencies in certain industries that deal with private information have recognised that data breaches continue to occur and to carry the risk of devastating harm to customers, and as a result have adjusted required practices and regulatory audits to specify encryption as a solution.

Again, the fact that some organisations are compelled to invest in data security solutions (or safeguards) due to a begrudged necessity to follow legal compliance requirements is unfortunate, because a mindset that does not also encourage employee training and a valuing of data safety can certainly reduce the effectiveness of any measures put in place.

POPIA

Privacy is a fundamental human right enshrined in the South African Constitution. Someone once said, "you can have security without privacy, but you cannot have privacy without security", so the security safeguards you implement form a vital foundation from which to build upon to improve your overall data security posture to avoid being in violation of the Constitution and the Protection of Personal Information Act (POPIA).

POPIA requires adequate safeguards for all personal data collected, processed, or retained by an organisation. The act also mandates that the data subject (the person whose information it is) must be informed in the event of a data breach.

The effect of POPIA is that organisations in all industries must adapt their practices and improve their security measures to comply. Organisations and businesses should become familiar with several terms and definitions used with POPIA.

Common POPIA Terms and Definitions

"POPIA" means South Africa's Protection of Personal Information Act.

"Responsible party" means any person or organisation that, alone or jointly with others, determines the purposes and means of the Protected Personal Information.

"Data Subject(s)" means any natural or juristic persons whose data is being processed such as suppliers, supplier employees, customers, including customers' employees.

"Protected Personal Information" means **personally identifiable information (PII)** about data subjects located in the South Africa and may include, but is not limited to, the following:

(i) categories of data subjects: prospective customers, customers, business partners, and vendors; and

(ii) types of personal data: name, title, position, email address, phone number/s, location, IP address, device name, computer username, device/computer mac address, encryption certificates/keys.

"Process(es)" or **"Processing"** of South African Protected Personal Information means any operation or set of operation that is performed on Protected Personal Information whether by automated means, such as collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure, or dissemination, and erasure or destruction.

"Operator" means any natural or legal person, public authority, agency, or other body that processes Protected Personal Information of Data Subjects on behalf of Responsible Party.

In the case of managed IT services, you are the Responsible Party, and we (the MSP) are the Operator under POPIA.

What about BYOD?

The use of personal devices, especially in small and mid-sized businesses and organisations and contingent workers are very common. Furthermore, it is found that smartphones and tablets as well as USB storage devices like external hard drives and memory sticks make up the bulk of personal devices also used for work purposes.

There are several models and a total acronym soup for approaches to the IT strategy for the use of personal device such as **BYOD** (Bring Your Own Device), **CYOD** (Choose Your Own Device), **COPE** (Company Owned / Personally Enabled), **COBO** (Company Owned / Business Only), plus a few more. All these however, largely relate to enterprise mobility.

This has always been a grey area, and no one wants to carry two phones, nor do smaller businesses want the costs of owning this asset, and at the same time employees resist employers controlling their device with fears of snooping and personal communication access. One security framework has taken strides to provide clarity and so the Cyber Essentials certification, which are simplified controls for UK SMEs, provides good definitions and guidance for BYOD. Cyber Essentials places any user-owned device which access organisational data or service as "in-scope".

- **Organisational data** includes any electronic data belonging to the organisation. For example, emails, office documents, database data, financial data.
- **Organisational services** include any software applications, Cloud applications, Cloud services, User Interactive desktops and Mobile Device management solutions owned or subscribed to by the organisation. For example, Web applications, Microsoft 365, Cloud-CRM, Virtual Conferencing applications, MDM, etc.

This means that if a mobile phone is used solely for phone calls and text messages as well as receiving 2-factor authentication (2FA) codes, it is not in scope, however, as soon as that device is used for accessing organisational email or any other organisational data, it would come into scope.

This is a useful reference as POPIA does not define nor care where the device is or in whose ownership it is, but as the "responsible party" the organisation is responsible for the safeguards of personal data under custody, even if that data is stored on is being accessed from a user-owned device i.e., BYOD.

The good news is that SMBs need not burden themselves with the complexity nor sophistication of enterprise mobility, containerisation, and the likes, but instead implement a strategy that works for them. This gives rise to a model we call **POBS** (Personally Owned / Business Secured) where the balance is weighted towards whole device security, rather than device control, segmented data access & control, and user tracking. This provides for reasonable measures to protect the data on the device.

Implementing a security app which is non-invasive, unobtrusive, and non-controlling of the user-device will lend itself better to getting users to embrace and allow the organisation to secure the user-owned device for the overall security of the organisation (as well for the benefit of the user) and can aid with POPIA compliance.

What about Work-From-Home?

In today's work-from-anywhere (**#WFA**), work-from-home (**#WFH**) and bring-your-own-device (**BYOD**) work environment's, employees may be working with sensitive customer data on their own laptops, phones, or tablets, and it is critical that they know how to handle that access responsibly. Training and education about this responsibility and the compliance requirements of every employee and/or contingent worker must form a vital component of your overall security programme.

Just as importantly, the organisation must also have security controls with the ability to revoke access and protect that data remotely if the potential for a data breach arises. Avoiding enforcement actions and securing data subject personal data must now be a top priority for any business, not only to avoid steep fines but also to avoid the reputational damage that comes with a public declaration that a business or organisation cannot protect their customers' private/persona data, and the social media virality of your organisation's negligence or mishandling of customers personal data!

Learning lessons from overseas examples

GDPR

Like POPIA, the EU's General Data Protection Regulation (GDPR) places the responsibility on the controller (Responsible Party under POPIA) and the processor (Operator under POPIA) to implement appropriate technical and organisational measures to secure personal data, however GDPR deliberately does not define which specific technical and organisational measures are considered suitable and effective in each case, to accommodate individual factors and technological advances.

Encryption of personal data has additional benefits for controllers and/or order processors. For example, the loss of an encrypted mobile laptop or USB storage device which holds personal data is not necessarily considered a data breach, which must be reported to the data protection authorities. In addition, if there is a data breach, the authorities must positively consider the use of encryption (and any other risk mitigating measures and protections) in their decision on whether a breach notice is required and what amount a fine is imposed as per Article 83(2)(c) of the GDPR, suffice to say that data/device encryption has a vital role to play in relation to breach notification duty and obligations – especially if originations (data controllers) are to do so within 72 hours of uncovering a breach.

In the case of a theft of a laptop belonging to an employee from Eir – a provider of fixed-line and mobile telecommunications in Ireland - the data protection commissioner there found that it was necessary for Eir to provide a public data breach notification under GDPR as the stolen laptop was NOT encrypted (although password protected) and therefore could result is the possible exposure of personal data of an estimated 37,000 Eir customers.

This is a good example where the local data protection authority considered the levels of protection/security implemented on the laptop, and the use of encryption as being a key technical protection measure.

Other industry codes and compliance regulations

Many industries and localities have specific requirements around data security that are enforced by various industry associations, bodies, or governmental agencies, so organisations must maintain an awareness of the industry specific codes and compliance regulations which apply to their sector.

Retail merchants touch upon a high volume of sensitive data as customers make payment transactions and must follow strict rules to keep this customer information safe. To govern the practices of merchants and any processors of payment card data, the payment card industry's Security Standards Council, founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., has implemented the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS delineates requirements by which cardholder data must be stored, processed, and

transmitted, specifying strong access control measures, password safety practices, and an emphasis on robust encryption.

Similarly, the Law Society of South Africa (LSSA) and the Health Professions Council of South Africa (HPCSA) are examples of industry bodies which has recognised the need for precise data security standards governing practices where member organisations should adhere to more specified guidelines, and it has recommended standards and operating practices requiring that businesses have enforceable, auditable, and persistent plans for making sure that sensitive data is safeguarded – all but requiring that encryption be in place.

When encryption is good for business

One segment of the organisations investing in encryption includes those motivated by the importance of protecting data as a positive business practice. Data security is in fact a valuable and cost-effective business asset.

Here is a good example of this: a business in the chemical industry, was concerned with protecting its intellectual property (which employees would carry on portable devices). These included laptops and smartphones used by traveling salespeople and workers in the field, devices holding proprietary chemical formulas, client lists, and other sensitive data. With BeachheadSecure™, the company is now protected by cloud-based mobile device security management, which includes data encryption. Beyond that, the company can now make a call to their MSP (e.g., Itblue Solutions) for even greater protection, including the ability to remotely (and instantly) lock (quarantine) or wipe data from compromised devices. In this case, implementing data security has provided more than just peace of mind – it has saved the company from major breaches a few times. Devices containing sensitive data have been left behind in taxis and airplanes, and, in every instance, the data encryption and data quarantining or wiping capabilities in place have prevented leaks that could have done untold damage to their business. The company's data security strategy helps shield it from insider threats as well, protecting each PC with encryption at the user level. This means that an employee (e.g., domain administrator) with credentials and bad intentions could enter the CFO's office, and then authenticate (or get access to) their laptop but not have access to the sensitive data. (If they could see that protected financial information, they might discover how the company's investment in data security has paid for itself by keeping company secrets secure.)

Beyond protecting intellectual property, many businesses find that implementing encryption opens the doors to new business partnerships and opportunities. For example, a business with clients in the financial field found that, in the aftermath of the JPMorgan Chase hack and other similar incidents last year, many large financial institutions adopted a policy of strict data security guidelines – not only for themselves but for any vendors they do business with. In this case, the company in question leveraged the BeachheadSecure™ service offered by their MSP to fulfil this business development requirement, and in turn was able to secure valuable relationships because they could secure valuable data.

Organisations with the wisdom to recognise the positive reputational advantages of encryption and

data security – and avoiding data breach incidents that can devastate reputations and customer trust – will count these solutions as important business investments. Unfortunately, the reality is that the segment of customers with this mindset is only starting to grow, and the syndrome of believing "it's never going to happen to me" about data security issues has ruled the day. Customers must realise the importance of meeting applicable compliance mandates but should also recognise the opportunities that may become available when implementing data security practices that achieve a level of competitive differentiation.

The challenges of supporting or offering managed encryption (until now)

So why is encryption not enforced on every PC, Mac, iPhone and iPad, Android, and USB storage device? Unfortunately, in going about the task of crafting data security strategies to fit our brave new device world, companies often gravitate toward one of two extremes. Many companies tend to overlook or ignore the need to comply with regulations, overwhelmed at what seems like a monumental chore. This approach seems perfectly reasonable, of course – until a data breach occurs.

Others, meanwhile, overestimate the complexity of the issue. They impose a tangled mesh of measures that prove costly and difficult to implement – developing a separate security program for each platform or operating system in use, for instance. These security provisions can hinder the increased employee productivity afforded by the new generation of mobile devices and can in the end undercut many of the advantages that led the company to adopt a more flexible, device-diverse work environment in the first place.

Poorly implemented and cumbersome solutions that make data security and encryption difficult for users certainly do not help matters. Some solutions require that users remember and follow certain procedures, such as remembering to put sensitive data in particular file locations or using secondary authentication methods. With some less user-friendly solutions and interoperability challenges, implementing encryption can take many hours. Some solutions may require internet connectivity to work properly and deny users important access when not online. Some may increase system latency to a frustrating degree. Unfortunately, these difficult solutions have earned encryption a bad reputation for generally hindering usability and user productivity – and being a pain to manage on the IT side as well. But the truth is this does not have to be the case!

For small and many medium sized businesses with no IT staff, or with a small and overburdened one, implementing encryption internally is almost impossibile. Deploying an encryption solution, managing that solution, and using it to remediate issues when they arise – these tasks all but require a dedicated service provider with the expertise to make the most of the data security tools at hand. Therefore MSPs most often play such a key role in the execution of data security solutions for SMBs.

BitLocker alone on Windows PC leaves gaps

BitLocker is a good starting point for encryption in your business. However, it should not be viewed as a complete solution to the challenges that organisations face in terms of compliance, cost, complexity, and user adoption. By adopting the recommended Microsoft® approach for PC data encryption of using Encrypting File System (EFS) encryption and BitLocker encryption, in tandem, gives organisations more complete protection and distinct advantages for protecting the data in-use and at-rest on any employee-used PC - desktops or laptops. The implementation of two separated "layers" of encryption enhances the overall security effectiveness; one where the files and data-blocks are protected by two different cryptographic technologies, and the other where the file encryption keys for EFS on the OS-drive are further secured by BitLocker (block-level) drive encryption. BitLocker keys are typically safeguarded external to the drive itself by key protectors located on the Trusted Platform Module (TPM) chip.

Do not fear though, these can all be overcome by using the right platform agnostic management tool to get the best from the technology. The important thing is to know where BitLocker and EFS fits in the bigger picture, its benefits, and pitfalls, and acquiring the additional supporting technology and layers of safeguards to ensure your business PCs and the data stored on it is secure, compliant, and getting the most from BitLocker and EFS.

Alone, the individual methods of encryption are reasonable, but combined, it will provide any auditor – or POPIA regulator – a high level of confidence that your organisation is above the "reasonable" measure for encrypting the personal, sensitive and consumer data on PCs.

Several tools may offer the ability to turn-on native encryption from a central console but most offer rudimentary functionality, lack full automation and innate sophistication to ensure a compliant solution; and notably most cannot easily and effectively manage both BitLocker & EFS using a single agent the way BeachheadSecure™ does!

Benefits of our managed service for your Windows PC include but are not limited to persistent enforcement of native encryption methods, separated data access and profile shielding, mitigating a network-borne attack risk, effective on and off network defensive actions, safe key store (key escrow) external to the domain in case your network is breached, auditing and incident reporting for POPIA compliance and audit.

The Solution:

The BeachheadSecure™ Managed Service by ITBLUE Solutions

There is a better solution for organisations seeking data security and encryption: cloud based BeachheadSecure™, as offered and managed by ITBLUE in South Africa. Using the remotely managed BeachheadSecure™ platform, our trained security administrators or your own IT staff enforce unobtrusive

encryption and data security for all company and employee-owned devices in use within your organisation, including PCs, laptops, phones, tablets, and USB storage devices. Our partnership enables us as an Authorised Beachhead MSP partner to provide BeachheadSecure™ as a monthly-managed or annual subscription service, with no hardware or software purchases or long-term commitment required. Fitting within our monthly or annual pay-as-you-go programme, we can completely handle every aspect of the solution on your behalf, from deployment to management.

Subscribing to the BeachheadSecure™ managed service, you can achieve protection for all PCs and laptops used within your organisation, as well as phones, tablets, and USB storage as needed, all under the same managed service and with the same inherent security benefits including for a distributed work computing environment such as remote-worker and work-from-home. The worry and hassle-free BeachheadSecure™ service is the only monthly pay-as-you-go service that not only encrypts data, but with just a call to us as your MSP we or your internal service administrator can lock out access (quarantine) or kill a device completely, in the event that this becomes necessary.

For those unfortunate scenarios where encryption is not enough – when a password is compromised, when devices have open sessions with credentials entered and fall into the wrong hands, when malicious former employees have access via their devices – BeachheadSecure™ can be thought of as encryption-*Plus.* It delivers the means to cut off these avenues that would otherwise result in data breaches. The closed-loop communication of BeachheadSecure™ maintains a line of sight to your managed devices and with its integrated reporting it makes it very simple to not only monitor and audit, but effectively prove your controls and security measures on devices for your POPIA compliance efforts.

The ITBLUE BeachheadSecure™ managed service offers superior data protection, and helps you sleep better at night, and enables you to build and maintain trust, compliance, and competitive advantage!

itblue
https://www.itblue.co.za

Any questions or comments write to us
info@itblue.co.za