

POPIA Webinar Series – Nr 9

Presenter:

Lettie Janse van Vuuren CA(SA)



14 APRIL 2021

The Protection of Personal Information Act (POPIA)
Security Safeguards

Presenter

Lettie Janse van Vuuren CA(SA), RA, CBA(SA)

- Lettie joined SA Accounting Academy in November 2017 as Head of Technical. She is a Chartered Accountant, Registered Auditor and Certified Business Accountant.
- She is a **professional trainer and webinar host**, and with her relaxed and humorous presentation style, she is able to hold the attention of an audience. She has a unique ability to communicate with delegates at their respective levels of knowledge and experience. Over the last 20 years, she has trained thousands of partners, managers, trainee accountants and other professionals.
- She is responsible for our MCLU (Monthly Compliance and Legislation Updates).
- She was the Professional Development Manager at SAICA for 4 years and in charge of accrediting new training offices and monitoring existing ones (including the moderation of training offices and trainee assessments).
- Lettie is passionate about improving the efficiency and standardisation at practices. She has extensive experience on a variety of technical and practical topics which she consults on, including: SAICA re-accreditation assistance and preparation, IRBA inspection assistance and preparation, audit file reviews (post-issuance monitoring and EQCR), Quality control implementation, other office-specific manuals, and FASSET skills development facilitation.



About SAAA

Creating opportunities to connect our partners to succeed

SAAA offers CPD training for accountants, auditors, bookkeepers and tax practitioners. We give you access to professional and technical content that ensures both your knowledge and skills are maintained so you remain professionally competent.

The CPD policy is compliant with IFAC IES7

All training offered by SAAA is recognised for CPD hours by the relevant professional bodies.

SAAA Rewards

CPD Subscribers gain access to various rewards

These can be accessed from your profile by logging in and navigating to your [“My Rewards”](#) > [“Find out more”](#) to see the reward partner benefits and claim it.

These rewards include discounts, reduced premiums and free stuff.

Reward Partners



Acts Online provides legislation, including amendments and regulations, in an intuitive, online format.



Draftworx provides automated drafting and working paper financial software.



EdNVest offers an exciting and unique product that leverages Section 10(1)(q) of the Income Tax Act



InfoDocs Company Secretarial Software.

Reward Partners *(continued)*



Practice Ignition simplifies onboarding - from engagement letter creation to securing client signatures.



QuickBooks Cloud Accounting Platform: The one place to grow and manage your entire practice.



Join the largest accounting and tax franchise in Southern Africa.

Webinar Housekeeping

The **Source & Bonus Documents** will be uploaded to your SAAA profile after the webinar – it's usually a good idea to check the next day.

The **webinar recording** and **presentation** will also be available at the end of the webinar within your SAAA profile.

These can be accessed from your profile by logging in and navigating to your [“My Dashboard”](#) > [“View Events”](#) and then clicking on [“Links & Resources”](#) next to the webinar title.

The webinar is available under the [“Recording\(s\)”](#) tab and the **Source & Bonus Documents and Presentation** under the [“Files”](#) tab.

Claiming CPD Hours

You can claim your CPD hours for this webinar at the end of the webinar within your SAAA profile.

This can be accessed from your profile by logging in and navigating to your [“My Dashboard”](#) > [“View Events”](#) and then clicking on [“Links & Resources”](#) next to the webinar title.

The [“Claim My CPD”](#) option is available under the [“CPD”](#) tab.

Once claimed you will be able to view and download your certificate.

Complete the [Self-Assessment Questions](#) to qualify for an additional **1 bonus hour of CPD**

Disclaimer

Disclaimer

Whilst every effort has been made to ensure the accuracy of this presentation and handouts, the presenters / authors, the organisers do not accept any responsibility for any opinions expressed by the presenters / author, contributors or correspondents, nor for the accuracy of any information contained in the handouts.

Copyright

Copyright of this material rests with SA Accounting Academy (SAAA) and the documentation or any part thereof, may not be reproduced either electronically or in any other means whatsoever without the prior written permission of SAAA.

Ask Questions

To ask questions and interact during the webinar please use the chat sidebar to the right of the video / presentation on the screen.

→ ***NB = Please include the topic that your question is about for easy identification purposes***

Feel free to ask your questions during the webinar in the chat, these will be addressed live in the formal Q & A at the end of the presentation.

Where appropriate, a **Q & A Summary will be uploaded to your profile as soon as all answers have been documented.**

WHAT'S ON THE AGENDA?





Contents

- Recap:** Where did we end with the previous webinar?
- Module 1:** Common security risks
- Module 2:** Case Studies
- Module 3:** Best Practice recommendations
- Module 4:** Compliance Safeguards



"Every time you indulge into any sort of online activity, your data can be easily monitored and checked."

- Victoria Ivey,
Beta News



**THEY WANT
WHAT YOU'VE
GOT.
DON'T GIVE
IT TO THEM.**



Where did we end last time?

Focus was on the last 4 conditions of POPIA:

- Quick recap – the role of the Information Officer
- Last 4 conditions of POPIA
 5. Information quality
 6. Openness
 7. Security safeguards
 8. Data subject participation
- Common challenges
- Compliance solutions



Today we deal with Data Security Risks & Safeguards for compliance

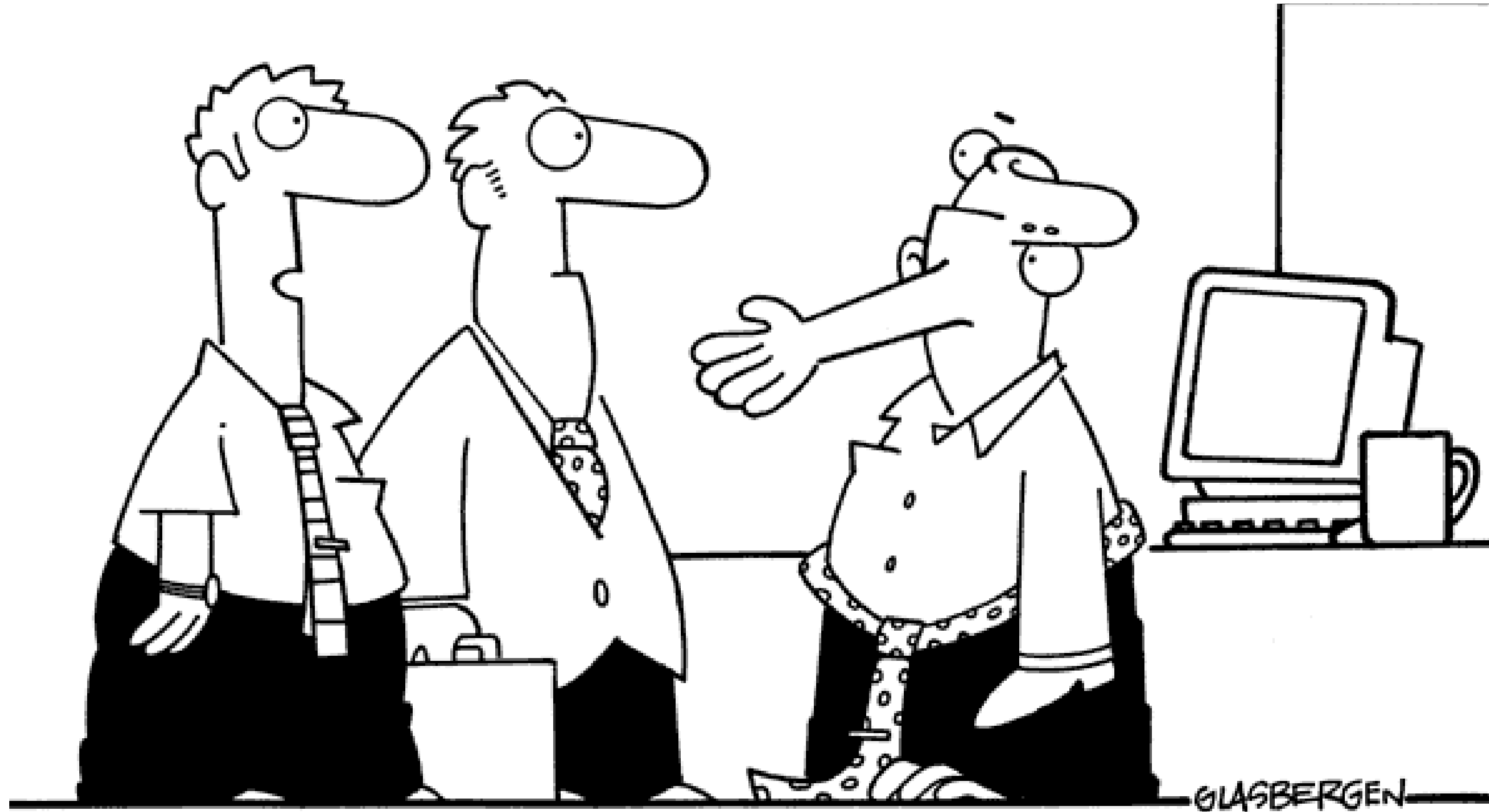


GUEST PRESENTATION

Enjoy today's detailed presentation by



Karabo Letlaku
&
Stephane Geldenhuys



“That’s our CIO. He’s encrypted for security purposes.”

Guest Presenter

Karabo Letlhaku

Karabo's interest in data protection was ignited in 2013 when the POPI Act was first introduced.

As the lead in the Policies and Procedures management project at Eskom Pension and Provident Fund at the time, Karabo was in charge of ensuring that all policies and procedures of the Fund were updated and compliant with the various regulatory requirements affecting financial services and Pension funds.

She joins Montana Data Company as an Account Executive specialising in assisting clients to find simplified yet effective ways of managing data and complying with data related regulation.

She is currently a candidate in the Masters in ICT Policy & Regulation programme with Wits and holds a Communication Science and a Media Ethics degree from UNISA.



Guest Presenter

Stephane Geldenhuys

Stephane' motto in life is simple, "BE the CHANGE you want to see in the world - it starts with YOU as the individual."

She is a highly accomplished and committed Management Professional that has a vast knowledge in designing and deploying sales and marketing strategies and programmes. She has a passion for customer centricity and believes that at the heart of any successful business is a satisfied customer.

Steph has 21+ years ICT and Telecommunications experience with a strong technical and solution selling understanding from Network/ Last Mile Connectivity, Voice, Mobile, Data Centre Solutions, Call Recording and Data Management. She joined the Montana Data Centre team as Sales Executive and with her knowledge and experience from the ICT environment has the main responsibility of customer engagement in the Data Management side of business.



1



Accountability

Responsible parties must comply with these eight conditions & ensure they can prove it – evidence-based accountability.

2



Processing Limitation

Personal information should only be obtained by limited and lawful processing that does not unnecessarily infringe privacy

3



Purpose Specification

The purpose for which personal information is collected must be specific, explicitly defined and lawful

4



Further Processing Limitation

Further processing must be compatible with the purpose for which personal information is collected

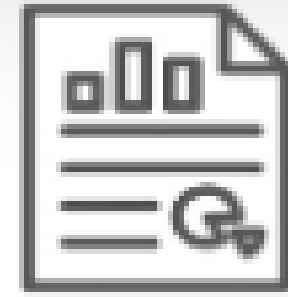
5



Information Quality

Reasonably practicable steps to ensure personal information is complete, accurate, not misleading and updated

6



Openness

Advise the data subject of certain mandatory information in respect of collection

7



Security Safeguards

The integrity and confidentiality of the personal information must be secured

8



Data Subject Participation

The data subject has certain access rights, including a right to request its deletion

Condition 7: Security safeguards

1. Security measures to be put in place to ensure integrity & confidentiality of information
 - Put in place both technical & organisational safeguards and processes to prevent loss / damage / unlawful access and processing
 - Identify and mitigate foreseeable internal & external security risks
2. Security measures for information processed by “Operators” / 3rd parties
 - All information processed MUST only be done with knowledge and approval from responsible party.
 - A contract MUST be in place that attends to data security measures and consequences of breach
3. Notification of any security compromises

See further reading attached as Section 19 & 22

MODULE 1

COMMON SECURITY RISKS



© 2007 by Randy Glasbergen. www.glasbergen.com



“You caught a virus from your computer and we had to erase your brain. I hope you’ve got a back-up copy!”

Copyright 2002 by Randy Glasbergen. www.glasbergen.com



“I know a lot of highly-confidential company secrets, so my boss made me get a firewall installed.”

10 RISKIEST EMPLOYEE PRACTICES

1



Accessing the Internet via unsecured wireless networks

2



Failing to delete unnecessary but confidential information from computers

3



Sharing passwords with others

4



Using the same user name and password for different websites and/or online accounts

5



Using generic USB drives that have not been properly encrypted to store confidential information

6



Leaving computers unattended when outside the workplace

7



Failing to notify organizations after losing USB drives that contain confidential data

8



Failing to use privacy screens when remotely working on confidential company documents

9








Carrying unnecessary sensitive information on laptops when traveling

10



Using personally owned mobile devices to access the organizational network

To manage the human error effect:

-  • Introduce **regular** training & awareness about the risks
-  • Introduce policy & **easy to follow** procedure
-  • Introduce random “privacy health checks”
-  • Create a **culture** of privacy – “Privacy by design”
-  • Get Insurance cover

NB: Secure both digital **AND** physical information

MODULE 2

SOME CASE STUDIES





The phone numbers and email addresses of 533 million Facebook users have been exposed in a data breach

The phone numbers and email addresses of 533 million Facebook users have been exposed in a data breach

Warning—Apple Suddenly Catches TikTok Secretly Spying On Millions Of iPhone Users



Zak Doffman Contributor ⓘ ⊕

Cybersecurity

I write about security and surveillance.



The World Health Organization – 2020

The World Health Organization was recently the victim of a cybersecurity attack. Various groups working on the coronavirus pandemic saw staff emails and passwords dumped online, including the National Institutes of Health, the World Health Organization and the Gates Foundation. How did it happen? There's not a clear answer as no one knows where or when the data breach came from or if the passwords and email addresses gave hackers an entry point. It is thought that the 'Elite Hackers' might be behind this cyberattack where nearly 25,000 email addresses and passwords were leaked.

***Advice:* Check your vulnerabilities and do not rely on antivirus software or blindly trust in new software.**

It is important to perform penetration tests regularly. Relying on professionals can help your business to identify new vulnerabilities.

WannaCry 2017

In 2017, a global ransomware attack known as WannaCry affected a number of countries and sectors. This type of malware encrypts user data and demands a ransom. Despite the fact that it started spreading around the world in 2017, this ransomware worm is still live on the internet and can also be found under the names WannaCrypt, WanaCrypt0r, WRrypt, and WCRY. WannaCry combines two malicious software components — a worm that spreads rapidly without user interaction, and a ransomware that encrypts user files and then asks for money in order to decrypt the files.

Advice: Update and protect your systems.

Having backups and storing work on a network share can minimize the losses. Ensure your Enterprise updates systems and don't allow personal emails to be opened on work laptops or PCs.



MODULE 3

BEST PRACTICE RECOMMENDATIONS



Some best practice recommendations

- ✓ Establish strong passwords
- ✓ Strong Firewall
- ✓ Antivirus protection
- ✓ Secure Systems (like encryption)
- ✓ Disaster Recovery
- ✓ Secure Mobile Phones too
- ✓ Backup regularly
- ✓ Monitor & Evaluate (reporting)
- ✓ Surf Safely
- ✓ Do not leave your hardware unattended / unlocked



Condition 8: Data subject participation

- Data subject may contact the responsible party to access details of their information being processed by responsible party including the 3rd parties that have access to it.
- Responsible party may decline to provide this information should it fall under the conditions of exemptions - see Chapter 4 of the Act

See further reading attached as Section 38

MODULE 4

COMPLIANCE SAFEGUARDS



SAFEGUARDS

What does Google reveal about Data Security?

Data Security is a process of protecting files, databases, and accounts on a network by adopting a set of controls, applications, and techniques that identify the relative importance of different datasets, their sensitivity, regulatory compliance requirements and then applying appropriate protections to secure those resources.

Similar to other approaches like perimeter security, file security or user behavioral security, data security is not the be all, end all for a security practice. It's one method of evaluating and reducing the risk that comes with storing any kind of data.

[What is data security and privacy?](#)

Data Privacy vs Data Security

Data Security and **data privacy** are often used interchangeably, but there are distinct differences:

Data Security protects **data** from compromise by external attackers and malicious insiders.

Data Privacy governs how **data** is collected, shared and used.

What does Google reveal about Data Security? *(continued)*

How do you protect data?

Securing Your Devices and Networks

- **Encrypt your data. ...**
- **Backup your data. ...**
- **The cloud provides a viable backup option. ...**
- Anti-malware **protection** is a must. ...
- Make your old computers' hard drives unreadable. ...
- Install operating system updates. ...
- Automate your software updates. ...
- Secure your wireless network at your home or business.



What does Google reveal about Data Security? *(continued)*

What are the types of data security?

Types of Data Security Measures

- **Data Backup. ...**
- Firewalls. ...
- **Data Encryption. ...**
- Use Strong Passwords. ...
- Use Antivirus Software. ...
- Secure Your Computer. ...
- Up to Date Operating System and Security patch. ...
- Digital Signature.



"So who is this *First* pet?"

What does Google reveal about Data Security? *(continued)*

[What are the 2 types of data encryption?](#)

There are **two types** of **encryption** in widespread use today: **symmetric** and **asymmetric encryption**.

[Which cryptography method is more secure?](#)

Advanced Encryption Standard (AES) - The Advanced **Encryption** Standard, AES, is a symmetric **encryption algorithm** and one of the **most secure**. The United States Government use it to protect classified information, and many software and hardware products use it as well.

[What is the most secure type of data?](#)

One of the most secure encryption types, Advanced Encryption Standard (**AES**) is used by governments and security organizations as well as everyday businesses for classified communications. **AES** uses “symmetric” key encryption. Someone on the receiving end of the data will need a key to decode it

[Why AES algorithm is used?](#)

AES is the Advanced **Encryption** Standard, a standard for cryptography that is **used** to encrypt data to keep it private. ... **AES** is a symmetric, block **cipher** which means that blocks of text of a certain size (128 bits) are encrypted, as opposed to a stream **cipher** where each character is encrypted one at a time.

What does Google reveal about Data Security? *(continued)*

What is the difference between 128 and 256-bit encryption?

The level of encryption reflects the number of possible key combinations. ... A 128-bit level of encryption has 2¹²⁸ possible key combinations (340,282,366,920,938,463,463,374,607,431,768,211,456 – 39 digits long) and 256-bit AES encryption has 2²⁵⁶ possible key combinations (a number 78 digits long).

Has AES been cracked?

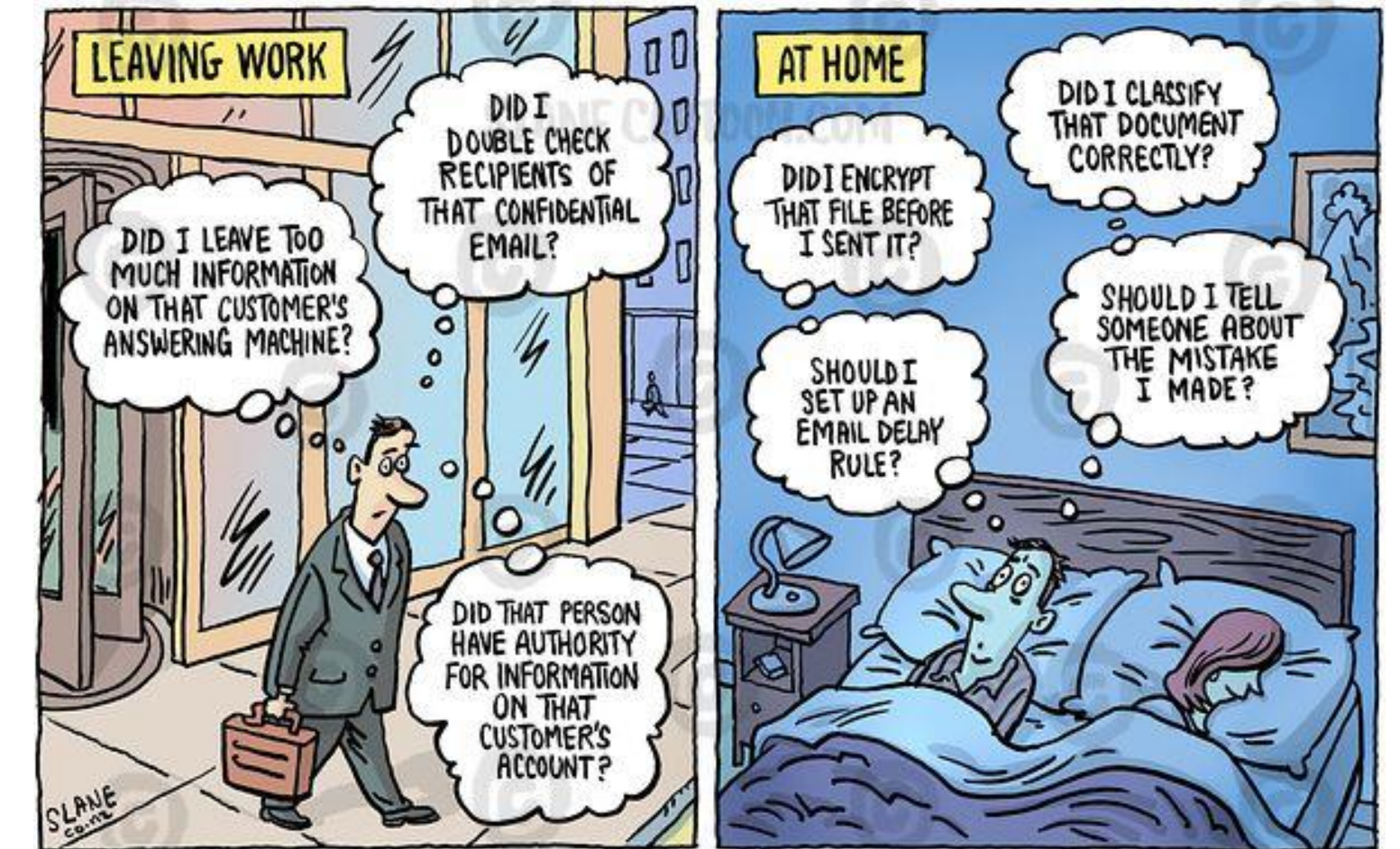
The bottom line is that if **AES** could be compromised, the world would come to a standstill. The difference between **cracking** the **AES-128** algorithm and **AES-256** algorithm is considered minimal. ... In the end, **AES** has never been cracked yet and is safe against any brute force attacks contrary to belief and arguments

Is AES 128 faster than 256?

There is a technical sense in which AES 256 is enormously stronger than AES 128, but in every sense that actually matters for security there is no difference.

How long does it take to break AES 128?

- Even with a supercomputer, it would take 1 billion billion years to crack the 128-bit AES key using brute force attack. This is more than the age of the universe (13.75 billion years).



Avoid the afterthought – think before sending our information.

Some Considerations to ensure Data Security

1. Store your information in a local and secure environment
2. Back up in an environment you can quickly & efficiently restore
3. Be able to provide evidence of the stored data (reporting)
4. Be able to delete / de-identify your data
5. Be able to transfer information among staff / departments securely
6. Be able to run a compliance audit
7. Provide POPIA training for staff



Current Backup Challenges

- **Tape Backups**
 - **Switching** of tapes
 - **Migration** challenges
 - **No 24/7/365 accessibility**, time to request
- **File Synchronization / One Drive / Drop Box / Google Drive**
 - Not a backup but a **Duplicate copy** of data.
 - **RansomWare** attacks primary source it replicates to synchronized server.
 - No **point in time** recovery
 - No **secure Chinese wall** between time stamped copies
- **Insufficient Technical Skill & Reporting**
 - **Time delay** in presenting backup reports
 - **No history** recordings on amount of data backed up **by devise**
 - **No BI** on data growth or problem environments
- **No flexible costing and pricing models**
 - No **Tiered costing** incentives
 - No **Pay as you use**
 - Complex Capex models e.g. quantity end point, data upload



Montana have the Solution you need ...

Challenge 1 – Tape Backup

- No longer require a manual process for backup's. Our Backup Agent automatically take care of the backup process

Challenge 2 – File Synchronisation / One-Drive / Dropbox / Google Drive vs Backup

- Montana's solution is not a Replication or Duplication of your data – it's a POPIA compliant **BACKUP**
- Montana's Back-up **Version Control** and multiple copies allowing point in time restores and protection against Ransomware and Viruses
- So, what happens when your environment is faced with Ransomware?
 - The ransom attach will automatically create a new “copy” of all your data. The copy prior to the ransom attach is still securely stored in our Data Centre. We simply re-install the copy of your data prior to the ransom attack.
 - Is the hacked/ransomed data still secure? Yes, it is, because the Ransomer will require the ENCRYPTION key to decrypt the data and that key is NOT stored with the data. It is unique to each customer and his/her business environment.

Challenge 3 – Insufficient Skills

- Montana's Back-up Engineer can assist
- Full training on how to recover data in the event it is lost

Flexible Costing

- Pay as you Use Costing Model – only pay for the data that are backed up
- Allocate data costs to departments/staff in your organisation

Montana Value Proposition

- **Mature and Reputable Enterprise Backup solution**, used by SA banks and Insurance companies.
- Version Control and multiple copies allowing point in time restores and protection against RansomWare and Viruses.
- Can backup and restore data **Hundreds of Times Faster** than other solutions
- **Address POPI and PAIA Act** requirements on security and off site backups
- **Unified view** of companies backup environment, results and costs.
- **Utility billing**, pay for what you backup
- **Enterprise class** infrastructure
- **Tier 4 Data Centers** with an **uptime of 99,995%**,
- **Access** to backed-up data **24/7/365**
- **Personal** support
- High performance **DR** if required

Happy Owner



Happy Staff



Happy Customer



Support when required



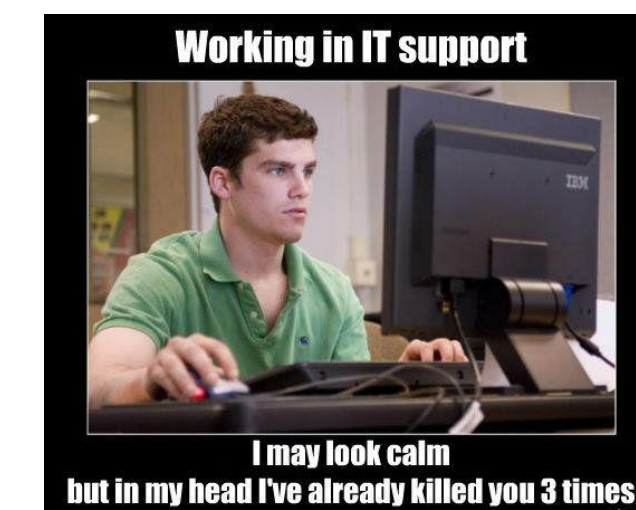
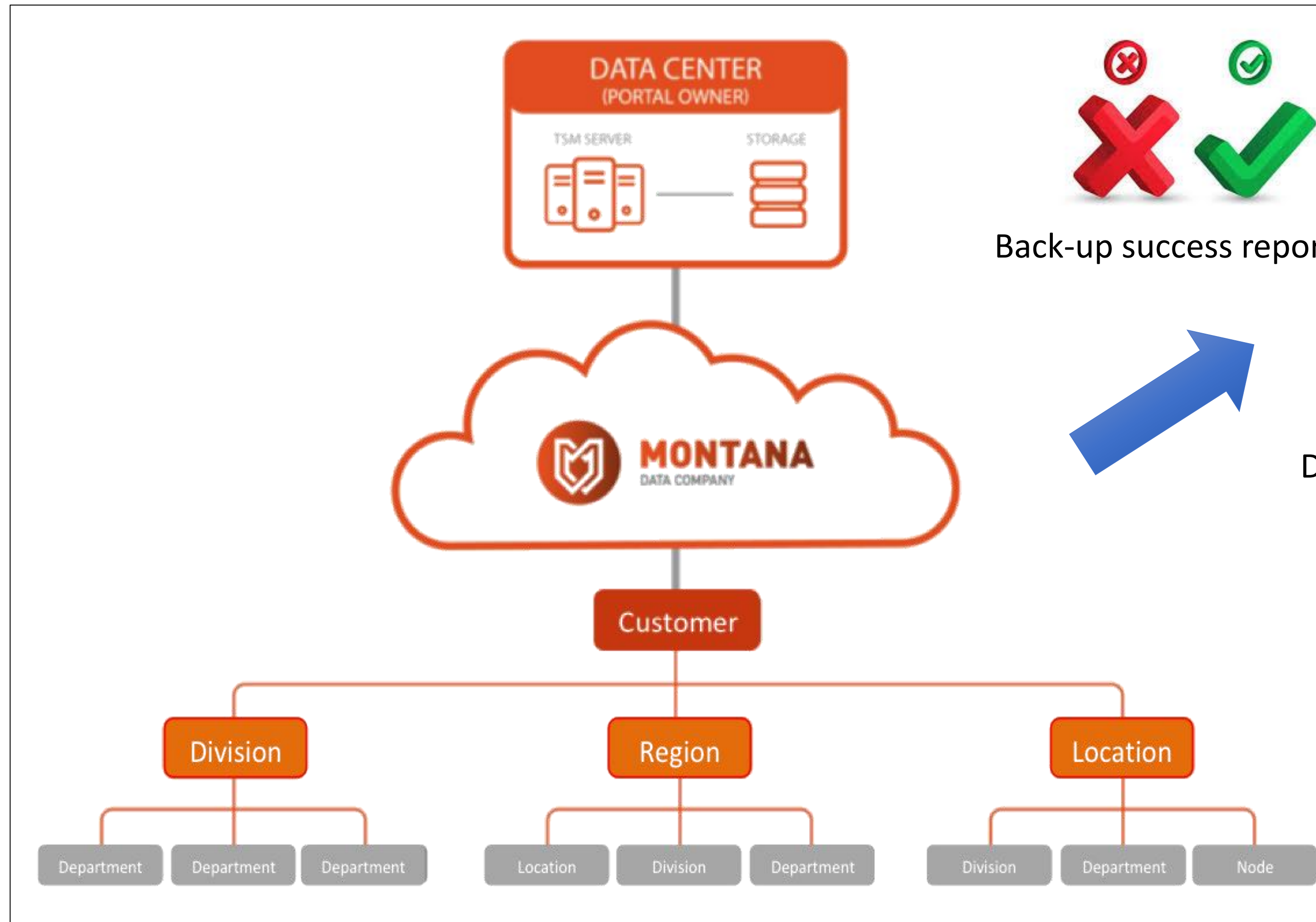
Security & Reliability:

Should IT need to know how it's done ?

- **Complete Built-in Security**
 - In use and accredited for **SIPRNET and JWICS, plus is FIPS 140-2 compliant.**
 - software has been thoroughly **vetted by the intelligence community** for large data transfers over even **the most difficult military networks** and is deployed in support of **mission-critical operations**, transferring terabytes of data every day.
 - Secure endpoint authentication, data encryption on-the-fly and at rest, and per-packet integrity verification
 - FIPS 140-2 compliant, built on the open ssl libraries
- **Secure User/Endpoint Authentication**
 - Authentication via secure SSH mechanisms: interactive password or public key
 - LDAP, Active Directory user authentication
 - Native File System Access Control support across all operating systems
- **AES-128 Cryptography**
 - On-the-fly data encryption
 - Data encryption in transit and (optionally) **256bit encryption** at rest (secured storage of transferred content)
- **Data Integrity Verification**
 - Each transmitted **data block is verified with a cryptographic hash function**
 - Protects against **man-in-the-middle**, re-play, and UDP denial-of-service attacks
- **100% Reliable Data Transmission**
 - Session semantics guarantee **100% bit-for-bit identical data copy at the destination**
 - **Automatic resume** of partial or failed transfers
 - Automatic HTTP fallback in highly restrictive networks

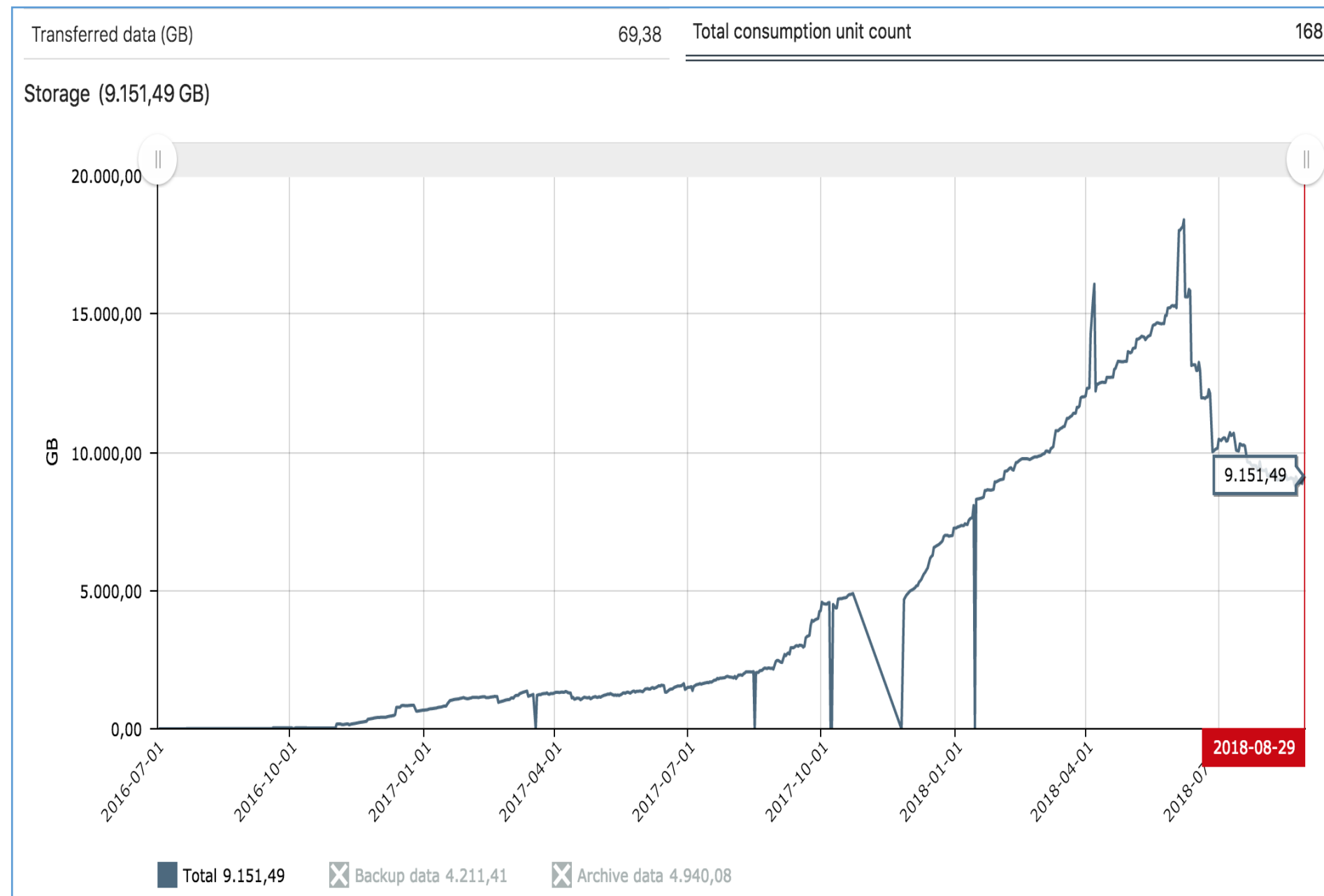
Backup Portal

- **Reporting and costing allocation** from individual device, consolidated to department, regional, location and company.



Ease of back-up
technical support

Backup Portal for Monitoring



Storage type	Size (GB)
Backup data	208,69
Archive data	4940,08
Total storage	5148,77

Transferred (GB)	1,34
------------------	------

Status	Consumption unit count
OK	0
OK (warnings)	2
Error	1
Ignored error	0
Total consumption unit count	3

Backend server summary

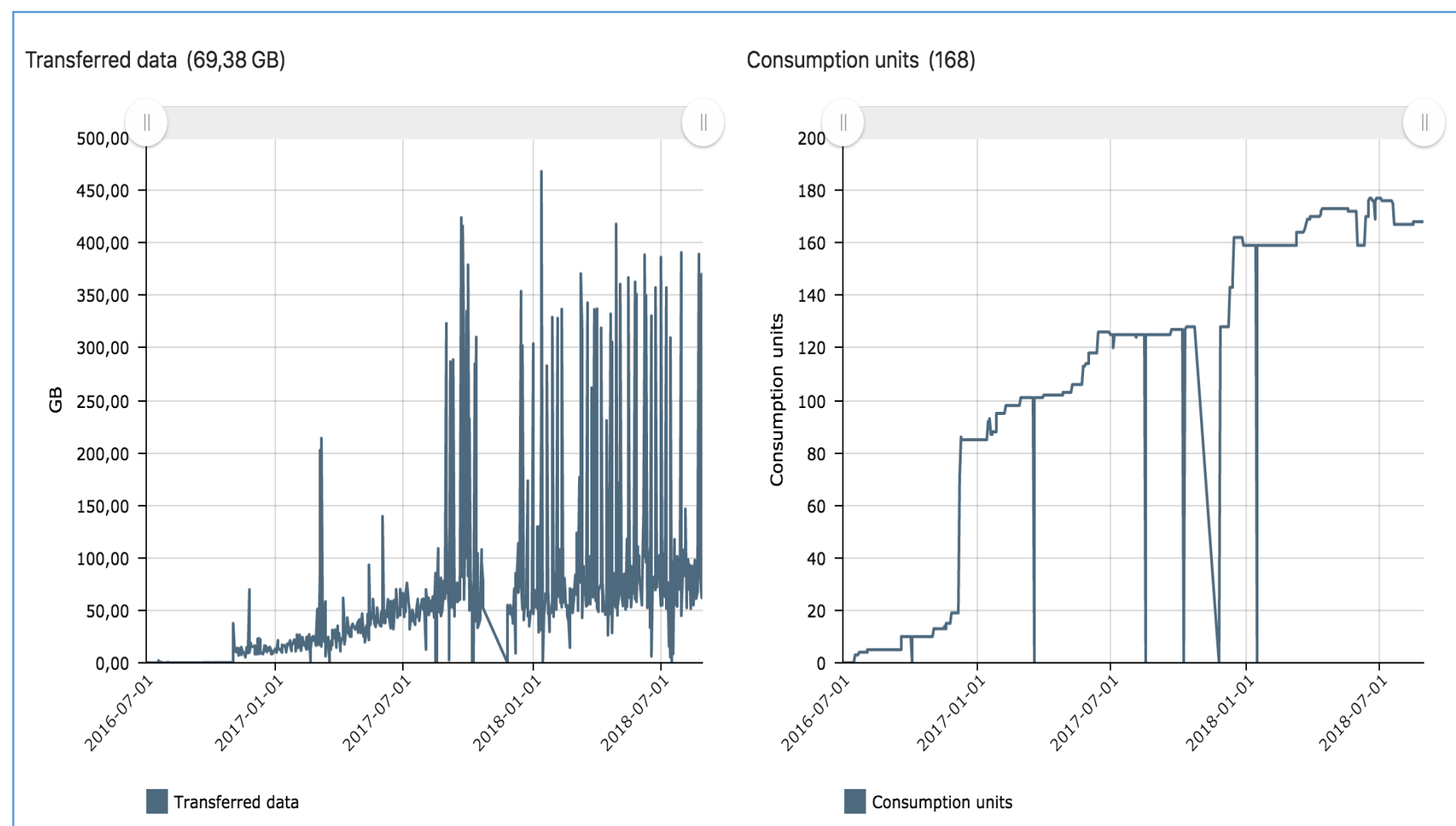
Servers from reporting time zones:

1. NRSSTSM101 (SP: MDCTSM1) in time zone (GMT+02:00) Harare, Pretoria

Consumption units

Current business unit (BCX SAP Services PCoE (Partner Center of Excellence))

Name	SP name	Client version	Server	Status	Errors	Size (GB)	Transferred (GB)
SAPGW1_File	SAPGW1_FILE	6.3.2.0	NRSSTSM101	OK (warnings)		14,06	0,27
SAPsolman_File	SAPSOLMAN_FILE	7.1.6.2	NRSSTSM101	Error	1. Newest event failed (8)	158,77	0,00
SAPsolman_Maxdb	SAPSOLMAN_MAXDB	7.1.6.2	NRSSTSM101	OK (warnings)		4975,94	1,07



Status report: Wednesday, 2018-08-29 today

Overview

Storage type	Size (GB)
Backup data	4.211,41
Archive data	4.940,08
Total storage	9.151,49

Transferred data (GB)	69,38
-----------------------	-------

Storage (9.151,49 GB)

Subscription types & Billing

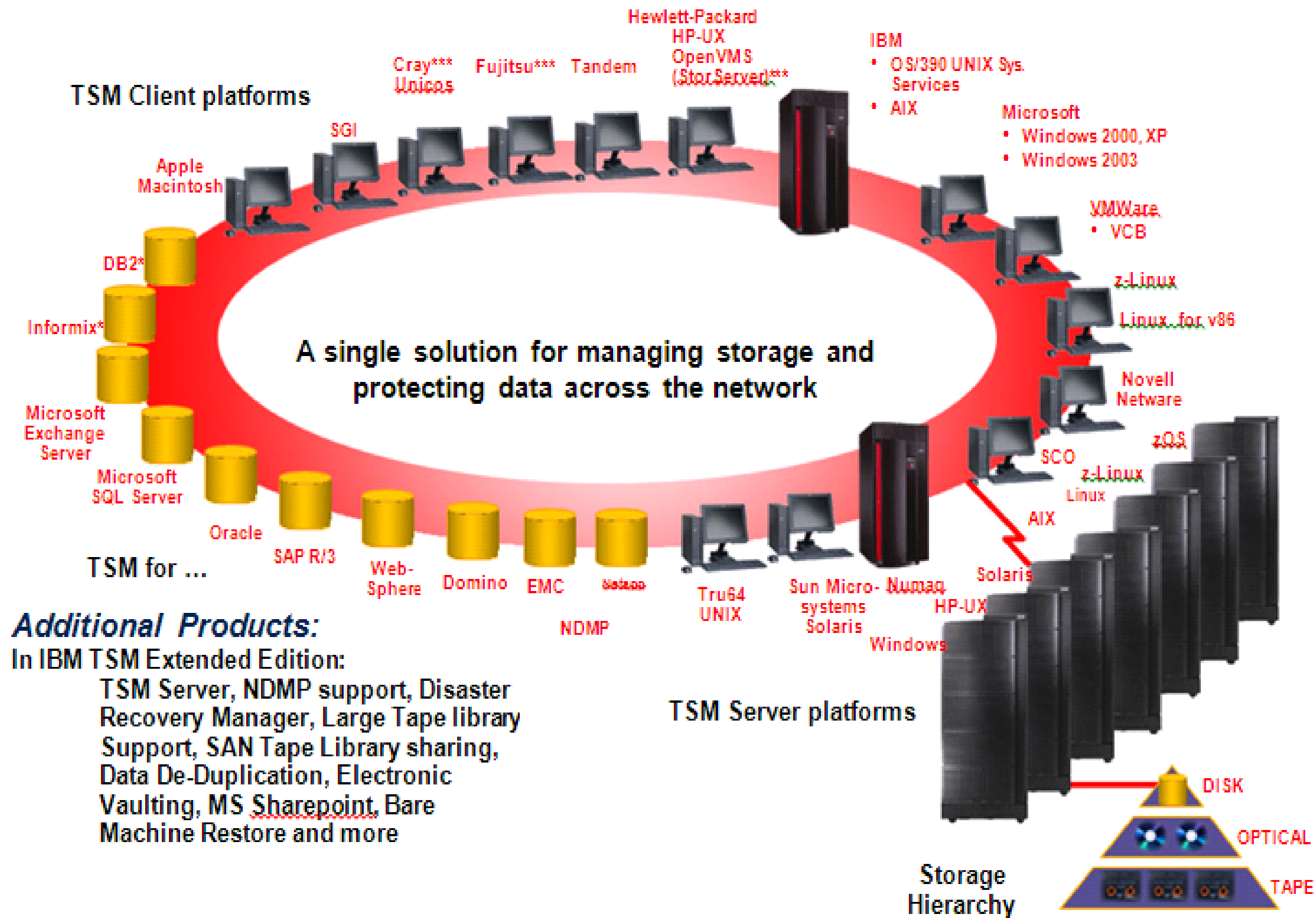
- The portals **Billing Engine** defines how you invoice your various divisions or departements for **correct cost allocations**.
- Billing info can be **exported via CSV or API** into Financial systems

Create new subscriptiontype

Name	<input type="text"/>
Fixed price	<input type="text"/>
GB Included	<input type="text"/>
Price per extra GB	<input type="text"/>
Archive price per GB	<input type="text"/>
NO of nodes - File server	<input type="text"/>
Price per extra node	<input type="text"/>
NO of nodes - Wrk. st.	<input type="text"/>
Price per extra node	<input type="text"/>
NO of nodes DB/Mail	<input type="text"/>
Price per extra node	<input type="text"/>
Description for partner	<input type="text"/>

A Single Solution for all environments

TSM – Supported Environment



Additional Products:

In IBM TSM Extended Edition:

TSM Server, NDMP support, Disaster Recovery Manager, Large Tape library Support, SAN Tape Library sharing, Data De-Duplication, Electronic Vaulting, MS Sharepoint, Bare Machine Restore and more

Data Security Breaches are real...

Are you protected?

Recent Data Breaches
On January 22, 2020, a customer support database holding over 280 million Microsoft customer records was left unprotected on the web (IdentityForce).
On February 20, 2020, Over 10.6 million hotel guests who have stayed at the MGM Resorts have had their personal information posted on a hacking forum (IdentityForce).
On April 14, 2020, the credentials of over 500,000 Zoom teleconferencing accounts were found for sale on the dark web (IdentityForce).
On July 20, 2020, An unsecured server exposed the sensitive data belonging to 60,000 customers of the family history search software company, Ancestry.com (IdentityForce).
On August 20, 2020, Researchers at Comparitech uncovered an unsecured database with 235 million Instagram, TikTok, and YouTube user profiles exposed online belonging to the defunct social media data broker, Deep Social (IdentityForce).
On November 5, 2020, a database for Mashable.com containing 1,852,595 records of staff, users, and subscribers data was leaked by hackers (IdentityForce).
On December 10, 2020, an undisclosed number of users of the audio streaming service, Spotify, have had their passwords reset after a software vulnerability exposed account information (IdentityForce).
On February 18, 2021, the California Department of Motor Vehicles (DMV) alerted drivers they suffered a data breach after billing contractor, Automatic Funds Transfer Services, was hit by a ransomware attack (IdentityForce).

COVID-19 Specific
Remote work during COVID-19 increased data breach costs in the United States by \$137,000 (IBM).
54% of organizations required remote work in response to COVID-19 (IBM).
76% of participants said remote work would increase the time to identify and contain a data breach (IBM).
Estimates show there have been as many as 192,000 coronavirus-related cyberattacks per week in May 2020 alone, a 30% increase compared to April 4 (Unisys).
In 2020, 98% of point of sale data breaches in the accommodation and food services industry were financially motivated (Verizon).
Confirmed data breaches in the healthcare industry increased by 58% this year (Verizon).
Web application breaches account for 43% of all breaches and have doubled since 2019 (Verizon).
33,000 unemployment applicants were exposed to a data security breach from the Pandemic Unemployment Assistance program in May (NBC).

Breaches by the Numbers
How Breaches Happen
An average of 4,800 websites a month are compromised with form-jacking code (Symantec).
34% of data breaches in 2018 involved internal actors (Verizon).
71% of breaches are financially motivated (Verizon).
Ransomware accounts for nearly 24% of incidents where malware is used (Verizon).
95% of breached records came from the government, retail, and technology in 2016 (Tech Republic).
36% of external data breach actors in 2019 were involved in organized crime (Verizon).

Average Response Time and Lifecycle
The average time to identify a breach in 2020 was 228 days (IBM).
The average time to contain a breach was 80 days (IBM).
Healthcare and financial industries spent the most time in the data breach lifecycle, 329 days and 233 days, respectively (IBM).
The data breach lifecycle of a malicious or criminal attack in 2020 took an average of 315 days (IBM).
48% of malicious email attachments are Microsoft Office files (Symantec).
From 2016 to 2018, the most active attack groups targeted an average of 55 organizations (Symantec).

Crucial Information
The global number of web attacks blocked per day increased by 56.1% between 2017 and 2018 (Statista).
The number of data breaches in the U.S. has significantly skyrocketed within the past decade from a mere 662 in 2010 to over a thousand by 2020 (Statista).
Office applications were the most commonly exploited applications worldwide in Q3 of 2018 (Statista).
There was an 80% increase in the number of people affected by health data breaches from 2017 to 2019 (Statista).
By stealing only 10 credit cards per website, cyber criminals earn up to \$2.2 million through formjacking attacks (Symantec).

Cost of a Data Breach
Healthcare is the most expensive industry for a data breach at \$7.13 million (IBM).
The global average cost of a data breach is \$3.86 million (IBM).
The average cost per lost or stolen record in a data breach is \$150 (IBM).
A breach lifecycle under 200 days costs \$1 million less than a lifecycle over 200 days (IBM).
39% of costs incurred more than a year after the data breach (IBM).
In 2020, the country with the highest average total cost of a data breach was the United States at \$8.64 million (IBM).
A mega breach of 50 million records has an average total cost of \$392 million, a growth of almost 12% from 2018 (IBM).
Hospitals spend 64% more annually on advertising over the two years following a breach (American Journal of Managed Care).

Data Breach Risk
A financial services employee has access to 11 million files (Varonis).
The average distributed denial-of-service (DDoS) attack grew to more than 26Gbps, increasing in size by 500% (Nexusguard).
In the first quarter of 2020, DDoS attacks rose more than 278% compared to Q1 2019 and more than 542% compared to the last quarter (Nexusguard).
9,637 attacks were between 10Mbps and 30Mbps (Nexusguard).
Over 64% of financial service companies have 1,000+ sensitive files accessible to every employee (Varonis).
On average, 50% of user accounts are stale (Varonis).
58% of companies found over 1,000 folders that had inconsistent permissions (Varonis).
Only 5% of a company's folders are protected (Varonis).
38% of all users sampled have a password that never expires (Varonis).

Largest Recorded
Yahoo holds the record for the largest data breach of all time with 3 billion compromised accounts (Statista).
In 2019, First American Financial Corp. had 885 million records exposed online including bank transactions, social security numbers and more. (Gizmodo)
In 2019, Facebook had 540 million user records exposed on the Amazon cloud server (CBS).
In 2018, Marriott International data breach affected roughly 500 million guests (New York Times).
In 2016, for reasons of poor security, Adult Friend Finder Network was hacked exposing 412 million users private data (Zero Day).
Experian-owned Court Ventures sold information directly to a Vietnamese fraudster service involving as many as 200 million records (Forbes).
In 2017, data of almost 200 million voters leaked online from Deep Root Analytics (CNN).
In 2014, Ebay was hacked, accessing 145 million records (Yahoo).
In 2008 and 2009, Heartland Payment Systems suffered a data breach resulting in the compromise of 130 million records (Tom's Guide).



TO OUR GUEST PRESENTERS!

NAH, I'M NOT
WORRIED ABOUT CLOUD
SECURITY. MY STORED
DATA IS SO DISORGANIZED
THEY'D NEVER BE ABLE TO
FIND ANYTHING!





In closing...

- ✓ Remember, you and other businesses in SA must be able to prove compliance as from 1 July 2021
- ✓ Assess where you are in your compliance action plan, consult where necessary & take action
- ✓ Safeguards must include PHYSICAL security too...
- ✓ **Safety isn't expensive...it's priceless!!!!**

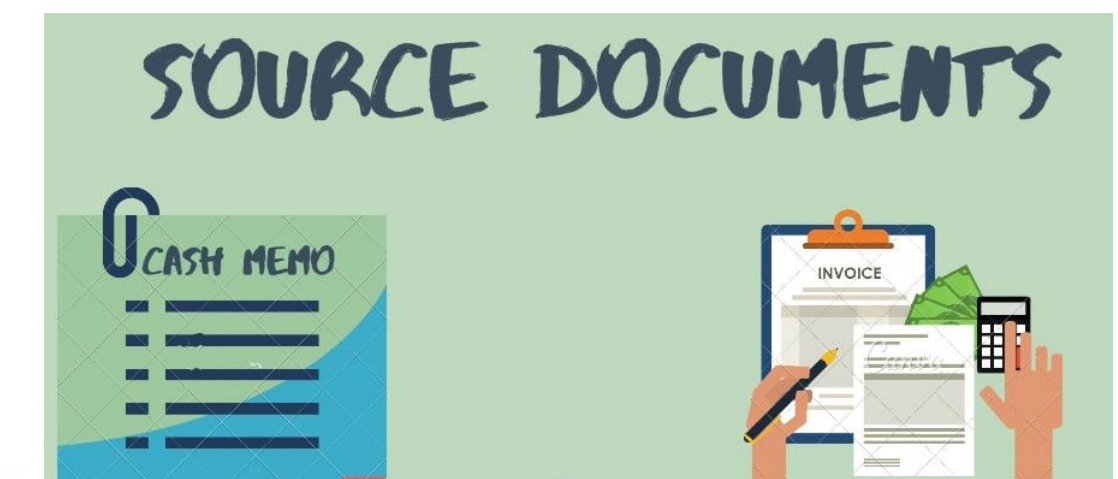


S Search for Hazards
A Analyse the risk
F Find the cause
E Eliminate the cause
T Tell others
Y You are safe

Source Documents

The following Source Documents are available to you:

- Section 19 of POPIA - Security measures**
- Section 22 of POPIA - Notification of security compromise**
- Section 38 of POPIA - Exemptions for processing**



What's Next???

Dates for the remainder of the 2021 instalments of the POPIA Compliance Series:

- ❑ **6 May 2021: Latest guidance for Information Officers**
- ❑ **3 June 2021: How to solve POPIA challenges facing Financial practices**
- ❑ **24 June 2021: POPIA Readiness check**

Refer to SAAA website to book in advance for the rest of the webinar series



QUESTIONS



Formal Q&A Session

We will now take a **quick comfort break** before we discuss some questions received during the webinar.

- Please use the chat sidebar to the right of the video / presentation on the screen to ask your questions.

Remember: A Q&A summary will also be uploaded to your profile, where applicable

If you would like to e-mail a question please use:

technicalquestions@accountingacademy.co.za

E-mail general comments to info@accountingacademy.co.za

Contact our POPIA Experts



MONTANA
DATA COMPANY

Suite 51
377 Rivonia Boulevard
Rivonia
2128
South Africa.
<http://www.montanadc.com>

Karabo Letlhaku

Data Governance Account Executive

+27 84 550 9798

karabol@montanadc.com

Stephane Geldenhuys

Sales Executive

+27 76 411 5089

Stephaneg@montanadc.com



for your participation!