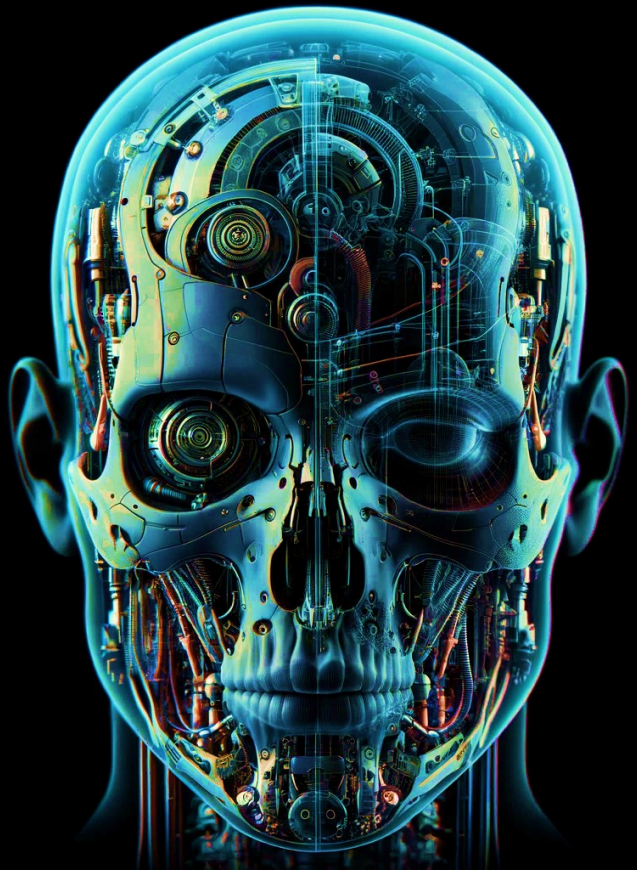
Data Security in the Future-Proofed Practice



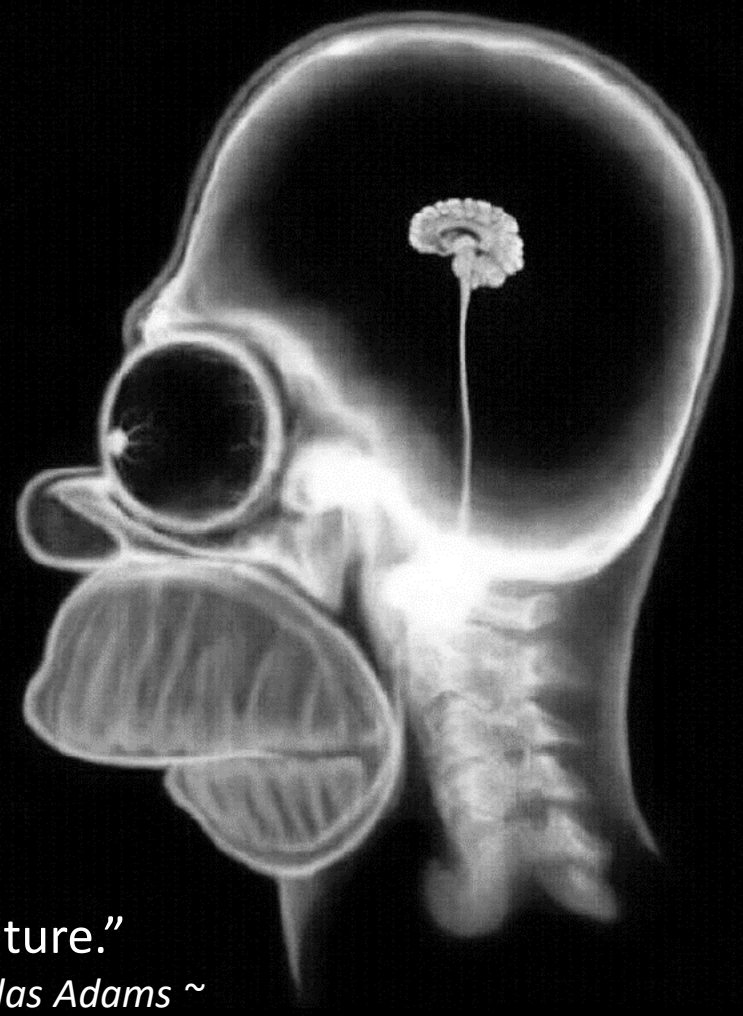
SUREN GOVENDER

Chief Operating Officer

iGUARDSA

suren@iguardsa.net -- 083 626 2229

FILE FOR TECHNICAL BANKRUPTCY



"Let the past hold on to itself and let the present move forward into the future."

~ Douglas Adams ~

PATIENTS COME SECOND?

"Employees come first. If you take care of your employees, they will take care of the clients."

~ Richard Branson ~

DIGITAL TRANSFORMATION IS NOT ONLY ABOUT TECHNOLOGY

"Data that is loved tends to survive."

~ Kurt Bollacker ~

"Design is not just what it looks like and how it feels. Design is how it works."

~ Steve Jobs ~

DESIGN = CARE

"Truly successful decision-making relies on a balance between deliberate and instinctive thinking."

~ Malcolm Gladwell ~

BE DELIBERATE WITH CHANGE

LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:

If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser

THIS HIDDEN SITE HAS BEEN SEIZED

This server has been seized by The National Crime Agency (UK) working in close cooperation with the FBI and international law enforcement partners under 'Operation Cronos.'

NCA National Crime Agency

South West ROCU

Metropolitan Police

Europol

SH Schleswig-Holstein Landeskriminalamt

Kanton Zürich

Gendarmerie nationale

Poliisi Keskusrikospoliisi Centralkriminalpolisen National Bureau of Investigation

86%

of South African companies have experienced more than one cyberattack in 2023

84%

of businesses cannot find skilled security employees

78%

of SA organisations experienced ransomware attacks in 2023 (2022 = 51%)

R14mil

The average cost of ransomware remediation in SA

93%

of employees update social media when they get a new job

13%

of organisations pay the ransom after a cyberattack

77%

of employees reuse passwords across multiple services

80

The number of SaaS applications an average organization uses

REUTERS®

UnitedHealth could take months to fully recover from hack

npr

Health industry struggles to recover from cyberattack on a unit of UnitedHealth

MARCH

FROM KFF Health News

BREAKING NEWS

21 February 2024 – UnitedHealth (ALPHV Ransomware)

- 50% of medical claims in the U.S.
- 15 billion transactions a year
- 33,000 pharmacies
- 1 in 3 U.S. patients
- 600 laboratories
- 900,000 doctors
- 5,500 hospitals
- $22m ransom

SM

UnitedHealth Group®

The Register

White House and lawmakers increase pressure on UnitedHealth to ease providers' pain

US senator calls cyber attack 'inexcusable,' calls for mandatory security rules

WSJ PRO CYBERSECURITY

UnitedHealth Aims to Restore Change Healthcare Systems Within Two Weeks

Testing of medical claims systems will begin on March 18, parent company says

USA TODAY

A medical tech company that handles billions of records was hacked. What you should know.

THE JOURNEY TO RECOVERY

Cyber Incident Response

- Contain threat
- Data inventory
- Patient Zero ID
- Inventory of Affected Systems

1 ASSESS

RECOVER 2

Incident Response & Recovery

- Implement Emergency SOC **(24 hrs)**
- Rebuild Servers
  - Full Scan
  - Install AV and Patch
  - Test
  - Install Apps
- Audit of Security Controls (CSPA)

Security Hardening & Remediation

- Historic Vulnerabilities
  - Learn from past events
  - Remnants of previous attacks
  - Vulnerability reports
  - Maintain “cleaned” status
- Real-Time Vulnerabilities
  - Current and forward looking
  - Predictive analytics to identify threats
  - Highlight trends as they take shape
  - Enable quick response from SOC
- Establish Security Controls BASELINE

4 HARDEN

RESILIENCE 3

Business Restoration & Business Continuity

- Restore all services
- Build for resilience
- Implement 24x7 Managed Services
- Continuous Monitoring and Response

IOL

IOL | BUSINESS REPORT | COMPANIES | ECONOMY | ENERGY | MARKETS | ENTREPRENEURS

BUSINESS REPORT COMPANIES

Life Healthcare hit by cyber attack

EYEWITNESS NEWS

LIFE HEALTHCARE GROUP HACKED AMID COVID-19 FIGHT

In a statement, the healthcare organisation said it was still investigating the extent to which sensitive data has been compromised.

TimesLIVE

Hackers strike at Life Healthcare, extent of data breach yet to be assessed

09 June 2020 - 08:07

the doj & cd
Department:
Justice and Constitutional Development
REPUBLIC OF SOUTH AFRICA

experian

iWeb

Life Healthcare Group hit by cyber attack amid COVID-19

LAW SOCIETY OF SOUTH AFRICA

TransUnion

DAILY MAVERICK

defence
Department:
Defence
REPUBLIC OF SOUTH AFRICA

DBSA

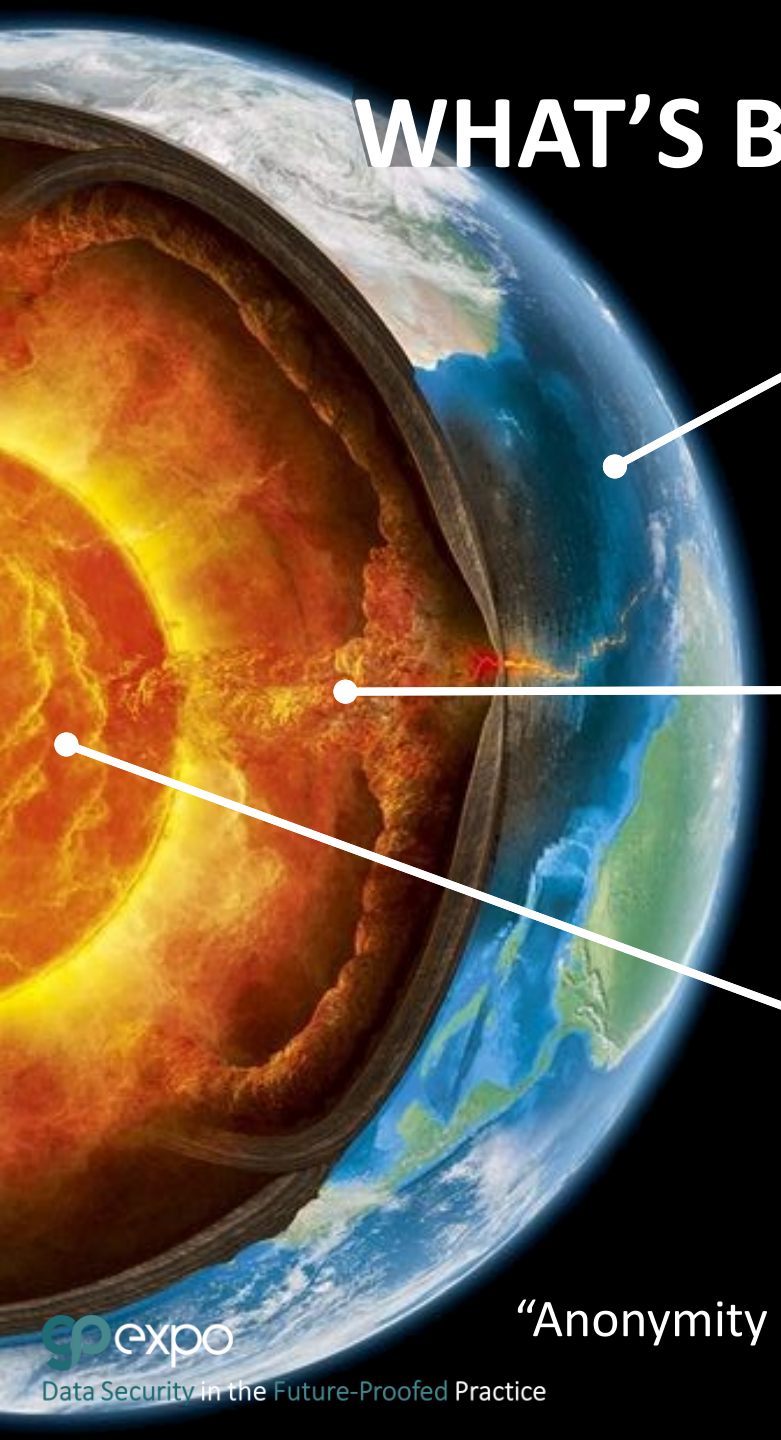
Tshwane University of Technology

Companies and Intellectual Property Commission

NEWSDECK

Life Healthcare Group hit by cyber-criminals

WHAT'S BELOW THE SURFACE OF THE INTERNET?



Surface Web

- 5% of total internet content
- Sites indexed by search engines
- .com, .net, .org, .co.za

Deep Web

- 90% of total internet content
- Not indexed by traditional search engines
- Requires sign-in (e.g. online services, Gmail)

Dark Web

- 5% of total internet content
- Only accessible through Tor, I2P, or Freenet
- Hidden pages, unregulated, used for illegal activities

"Anonymity breeds a sense of invincibility."

~ Jamie Bartlett ~

INSIDE THE MIND OF A HACKER

“power at your fingertips”

“the hard part isn’t getting in”

“harmless exploration”

“serious lack of security”

“could have escaped detection”

“tech voyeurism”

“strictly for financial profit”

~ anonymous ~

THE ART OF HUMAN MANIPULATION

A “friend” sends you a strange message

Emotions are heightened

Request is urgent

Offer is too good to be true

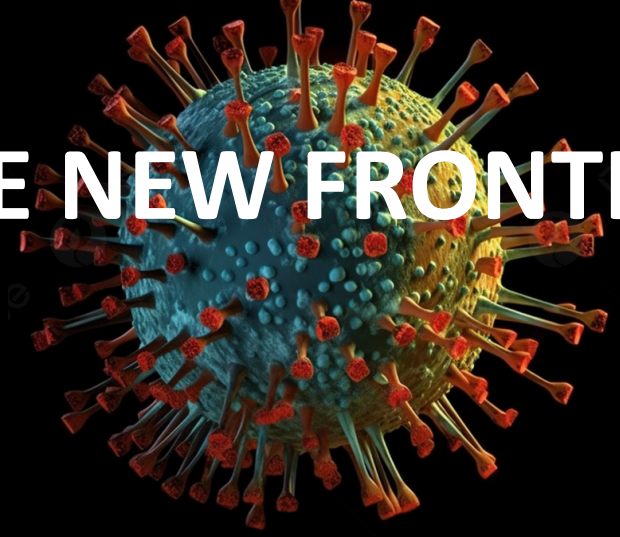
Receive help you didn’t ask for

Sender can’t prove their identity

“Social engineering bypasses all technologies”

~ Kevin Mitnick ~

CYBER HYGIENE: THE NEW FRONTIER IN HEALTHCARE



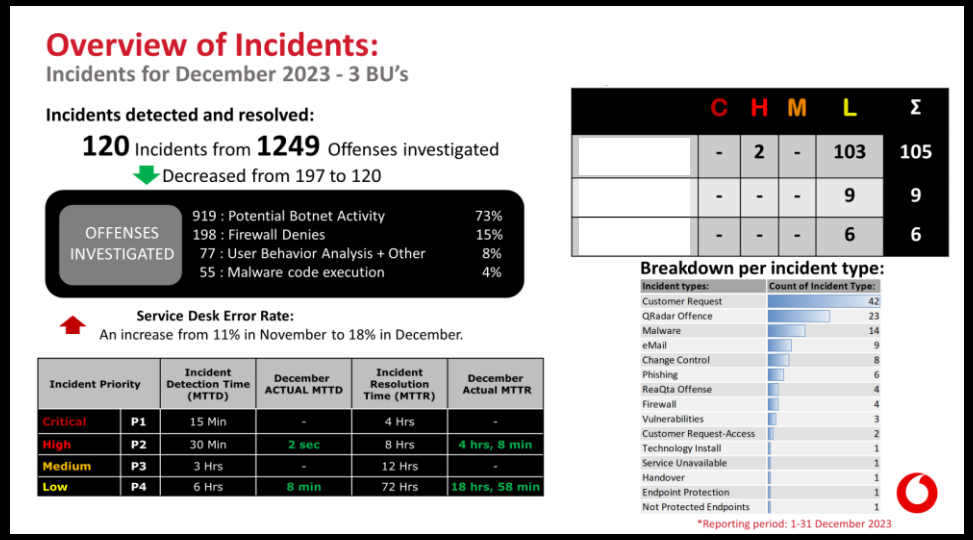
HEALTHCARE		CYBER SECURITY
Regular health **check-ups** to detect **anomalies**	EARLY DETECTION	Regular **checks** for **abnormal** behaviour and vulnerabilities
Immune system **identifies and isolates** pathogens	CONTAINMENT	**Identify and isolate** threats to prevent spread of attack
Medical treatment to **remove** pathogens, **healing** the body	TREATMENT & RECOVERY	**Removing** threats, **patching** vulnerabilities, **restoring** data

Cyber Security is EVERYONE's problem

Problem Statement

- Lack of security visibility across silos
- Lack of monitoring on environments for compromise
- Lack of vulnerability management
- Lack of security tools within environments
- Limited security skills, knowledge and capacity

ACTIONABLE INSIGHTS
weekly, monthly & ad-hoc reporting



Overview of Incidents:

Incidents for December 2023 - 3 BU's

Incidents detected and resolved:

120 Incidents from **1249** Offenses investigated

Decreased from 197 to 120

OFFENSES INVESTIGATED		
	919 : Potential Botnet Activity	73%
	198 : Firewall Denies	15%
	77 : User Behavior Analysis + Other	8%
	55 : Malware code execution	4%

Service Desk Error Rate:
An increase from 11% in November to 18% in December.

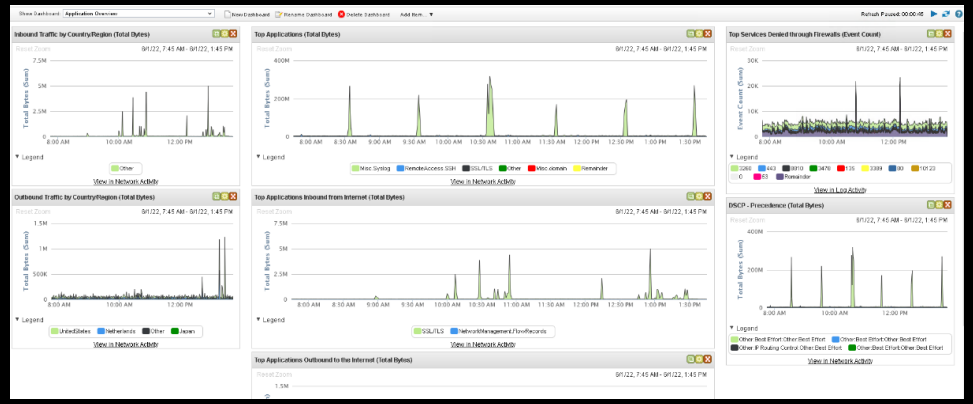
Incident Priority		Incident Detection Time (MTTD)	December ACTUAL MTTD	Incident Resolution Time (MTTR)	December Actual MTTR
Critical	P1	15 Min	-	4 Hrs	-
High	P2	30 Min	2 sec	8 Hrs	4 hrs, 8 min
Medium	P3	3 Hrs	-	12 Hrs	-
Low	P4	6 Hrs	8 min	72 Hrs	18 hrs, 58 min

	C	H	M	L	Σ
	-	2	-	103	105
	-	-	-	9	9
	-	-	-	6	6

Breakdown per incident type:

Incident types:	Count of Incident Type:
Customer Request	42
QRadar Offence	23
Malware	14
eMail	9
Change Control	8
Phishing	6
ReaQta Offense	4
Firewall	4
Vulnerabilities	3
Customer Request-Access	2
Technology Install	1
Service Unavailable	1
Handover	1
Endpoint Protection	1
Not Protected Endpoints	1

*Reporting period: 1-31 December 2023



PRACTICAL STEPS TOWARDS A SECURE FUTURE

Good

A good password will be:

- Long: at least 15 characters
- Complex: a mix of upper- & lowercase letters, numbers, symbols
- Unique: not used for any other accounts
- Unfamiliar: not containing personal info, e.g. birthdate, pet name

Pick a word: Friendship

Modify it: !Fr13nds_$h1P!?

Better

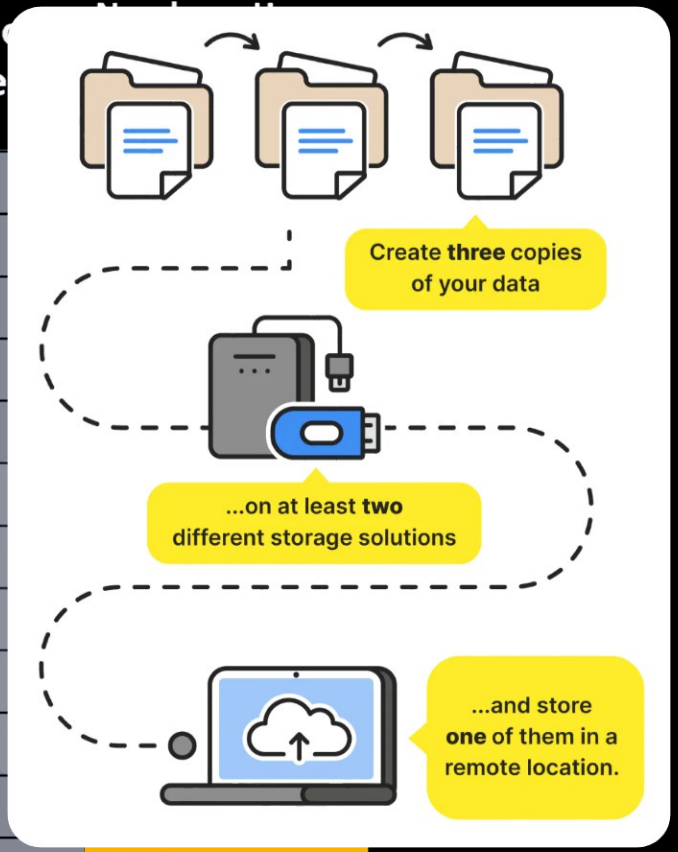
An even better password will be longer, yet easier to remember.

Pick a phrase: There's no place like home.

Modify it: Th3re's_n0-Pl@ce_L!k3-ho^3.

Best

Use a password manager that can generate long, complex, random passwords and store them, making remembering all of those phrases unnecessary. You just have to remember a single master password.



Zero Trust:

Trust no one, verify everyone.

TRUST YOUR GUT

"Intuition does not come to an unprepared mind."

~ Albert Einstein ~

“If you can't afford security, you can't afford a breach.”

~ Suren Govender ~

WHAT ARE YOU LOOKING AT?

Cyber Security is JENNY's problem

How much of your data is out there already?

We're deeply sorry Jenny Alison Richards*, 38

Dear Jenny Alison Richards (F) of **122 Mason Street, Southridge, VIC 3031**, telephone **082 8291 274**, driver's licence no **98465 3422.**

We sincerely regret the recent incident of a cyberattack on our platform which may have impacted your personal data.. We know this is devastating and that we'll need to work hard to regain your trust **Happy birthday for yesterday by the way**. Thirty-eight eh?

We are working closely with authorities to understand how this attack on your privacy - including your Medical Aid number **4512 4932 05521** - occurred. We know how stressful this is, especially given your ongoing battle with **haemorrhoids**.

We know there's a lot of misinformation out there. Rest assured, we're doing everything we can to ensure that your personal details, such as your **password (JennyHatesBen$!*@!!)** are not made public. Thanks for your understanding and all the best for the divorce settlement from your husband **Benjamin Richards** next week . By the way, your suspicions are correct – he has been cheating on you – go Girl Power!

***Names have been changed to protect the innocent ☺**

iGUARDSA


iGUARDSA
exclusive offer to gpexpo
CLAIM YOUR FREE
CYBER SECURITY ASSESSMENT
suren@iguardsa.net
083 626 2229
info@iguardsa.net
GPEXPO OFFER