

Cybersecurity in Oil & Gas

Safeguarding Namibia's Digital Infrastructure



Elizabeth Simon CEO
Green EcoTech International (GETI) NGO

Namibia Oil and Gas Conference

12 - 15 August 2025

Introduction: The Digital Transformation Challenge

Digital Transformation in Namibia's Oil & Gas

- ✔ Embracing digital systems for core operations
- ✔ Improved efficiency in drilling, transportation, logistics
- ✔ Enhanced payment systems and financial processes

Cybersecurity Vulnerabilities

- ⚠ Interconnected systems create complex attack surfaces
- ⚠ OT/ICS systems often lack modern security features
- ⚠ Critical infrastructure exposed to disruption

The High Cost of a Breach

\$ 5.04 Million

Average cost of a data breach in the energy sector

- IBM Security 2024 Report

Protection is not optional

It's essential for national revenue, economic stability, and sovereign integrity

What Is at Stake?



Production Disruption

A breach in control systems can halt operations from rigs to refineries, bringing critical infrastructure to a standstill.



Financial Loss

Companies lose an average of \$84 million per day when operations are down due to cyberattacks (Deloitte analysis).



Environmental Disasters

Hackers can manipulate safety systems, causing spills, leaks, fires, or well blowouts with catastrophic environmental impact.



National Security

Energy infrastructure is a strategic asset. Unsecured systems expose Namibia to foreign interference or sabotage.

⚠️ Case Study: Colonial Pipeline Attack (USA, 2021)

The Attack

Ransomware group gained access to IT network, forcing shutdown of the largest fuel pipeline in the U.S.

The Impact

Fuel shortages across 12 states, widespread panic buying, price spikes, and national emergency declaration.

The Entry Point

A single, compromised employee password for a VPN account with no multi-factor authentication.

Resolution: \$4.4 million ransom paid in Bitcoin

Threat Landscape for Oil & Gas

Ransomware

66% of energy companies targeted by ransomware (2023)

Disruptive attacks targeting operational systems

Phishing

91% of attacks begin with phishing email

Tricks employees into revealing credentials

OT Vulnerabilities

- Decades-old legacy systems
- No encryption between components
- Blind to intrusions

Supply Chain Risk

Targeting smaller vendors to gain foothold
Lateral movement to OT systems

Insider Risk

 Malicious insiders

 Unintentional mistakes

Case Study: Saudi Aramco (2012)

Not ransomware: A destructive act of sabotage

Wiping malware known as "Shamoon"

Entry point: Employee with privileged access

Clicked malicious link in email

Impact: 30,000+ workstations affected

Hard drives partially or totally wiped

Aftermath: Weeks of manual operations

Fax machines and typewriters used for supply chain

“ Demonstrated how cyberattacks on IT systems can threaten core industrial operations ”

Namibia's Digital Infrastructure Challenges



Infrastructure Gaps

- > Cybersecurity treated as an afterthought
- > Limited SIEM and IDS deployment
- > Security blind spots from siloed operations



Skill Shortage

- > Critical shortage of cybersecurity experts
- > OT security expertise particularly acute
- > Heavy reliance on costly foreign expertise



Regulatory Framework

- > No specific cybersecurity regulations
- > No national incident response plan
- > No mandated security standards



Operational Silos

- > Lack of integration between entities
- > No unified threat intelligence
- > Difficulties in coordinated responses

Global Cybersecurity Readiness



0.37/1.0

Namibia's score on the 2024 Global Cybersecurity Index

Below average in Africa for critical infrastructure protection

Regional Case Study - West Africa



- ▶ West African Refinery Cyber Incident (2023)
- ▶ A ransomware group successfully attacked a refinery in West Africa, encrypting its systems, causing operational disruption.

Cost Impact Analysis



🕒 Impact

- 🕒 9 days of production stoppage
- 💰 \$2.3M ransom demand
- 📈 Local fuel price surge

🔍 Root Causes

- 🛡️ Outdated firewall
- 🏗️ No IT/OT segmentation
- 💾 No backup policy

🔧 Recovery Costs

After recovery, the refinery spent an additional **\$1.5 million** on security upgrades.



💡 Key Lessons

- ✅ Even newer African energy infrastructure is highly exposed
- ✅ Internet-facing devices often have no defense layers
- ✅ Recovery costs exceed ransom payment

❑ For Namibia: Build resilience before a similar crisis occurs

Best Practices for **Securing Oil & Gas Infrastructure**

Proactive defense is no longer optional but a prerequisite for survival in the cyber landscape.

Asset Visibility

- ✓ Inventory all connected systems
- ✓ Map IT and OT environments

Network Segmentation

- ✓ Separate IT and OT networks
- ✓ Prevent lateral movement

Multi-Factor Authentication

- ✓ Require two verification factors
- ✓ Protect remote access points

Employee Training

- ✓ Focus on phishing awareness
- ✓ Build security-conscious culture

Incident Response

- ✓ Create detailed IRPs
- ✓ Test twice a year

System Backups

- ✓ Regular, encrypted backups
- ✓ Stored offline or immutably

“Cybersecurity in energy is not about if you'll be attacked, but whether you'll survive it.”

- Dragos CEO, 2024

National and Sector-Level Solutions

A cohesive approach involving government, industry, and educational institutions to build a resilient digital ecosystem for Namibia's oil and gas sector.



Cybersecurity Framework

- ✓ Aligned with NIST or ISO 27001 standards
- ✓ Mandatory for all operators and vendors



Mandatory Requirements

- ✓ Compulsory cybersecurity standards
- ✓ Applied to vendors and contractors



Emergency Coordination

- ✓ Specialized coordination unit
- ✓ Facilitates information sharing



Capacity Building

- ✓ Train 500+ Namibians in OT cybersecurity
- ✓ Partnerships with universities



Incentive Programs

- ✓ Tax incentives for security investments
- ✓ Reduces financial barriers



Benefits

- ↑ Proactive security posture
- ↑ Reduced breach costs
- ↑ Increased operational resilience

Standard Bank's Role in Energy Cybersecurity

Standard Bank supports Namibia's energy sector with comprehensive cybersecurity solutions.

Advisory Services



- ✓ Risk audits for energy clients
- ✓ Cybersecurity consulting

Secure Digital Products



- ✓ Encrypted banking platforms
- ✓ Secure payment solutions

Sector Engagement



- ✓ Policy support for digital resilience
- ✓ Industry collaboration

Capacity Building



- ✓ Cybersecurity training programs
- ✓ Partnerships with training institutions

The Path Forward: Acting Before Attackers Do



Cybersecurity as a Core Component

Cybersecurity is now integral to Namibia's oil and gas success. A single breach could halt operations and reverse years of progress.



Cost-Efficient Defense

Securing digital infrastructure is cheaper than recovering from an attack. Proactive investment yields better returns than post-breach recovery.

The Time to Act is Now



Government

Develop and implement national cybersecurity framework



Financial Partners

Support capacity building and provide incentives



Industry

Adopt best practices and prioritize security investments

"Before attackers do."

THANK YOU



Elizabeth Simon
CEO

Green EcoTech International NGO

Cell: +264 817512823

Email: getiwbgys@gmail.com



"Before attackers do."