CSIR INFORMATION AND **CYBERSECURITY CENTRE**

The CSIR Information and Cybersecurity Research Centre developed, piloted and commercialised the innovative VeristicPrint Biometric System. This marks the first such achievement for the centre since its inception. The system is a contactless fingerprint recognition software solution that enables any digital device, such as a smartphone or webcam, to function as a fingerprint scanner.

The system is made up of three modules:

1. *Contactless Acquisition Module;*
2. *Feature Extraction Module; and*
3. *Hash Matching Module.*

CSIR
Touching lives through innovation

ABOUT THE CSIR INFORMATION AND CYBER SECURITY RESEARCH CENTRE

Established in 2019, the CSIR Information and Cyber Security Research Centre is a consolidation of all CSIR research and development (R&D) capabilities in cybersecurity, information security and identity authentication. These capabilities were developed over decades of working for the Department of Defence and, over the last ten years, for government departments and agencies, such as the Department of Communications and Digital Technologies, state-owned enterprises and private sector players.

The centre aims to support industry, contribute to an efficient, secure and capable state and grow cybersecurity capacity and capabilities in the country. It also develops systems and solutions that are relevant to the local context and makes them available for commercialisation, which is in line with CSIR's strategic focus on industrialisation.

The CSIR has a recognised track record locally and abroad, based on its work with and support for numerous stakeholders and institutions. Since the nineties, as cyberspace became everyone's playground, several technologies were brought to local users. These include antivirus software and an early warning detection system for small businesses encompassing both software and hardware components. A major achievement was a CSIR-developed encryption solution (encoder/decoder) that led to the creation of the pay-TV giant M-Net.

Innovation is homegrown. Initiated by the CSIR and collaborators in the public and private sectors, test and evaluation platforms and cybersecurity educational and training packages have been prototyped, and some have been implemented in operational environments.

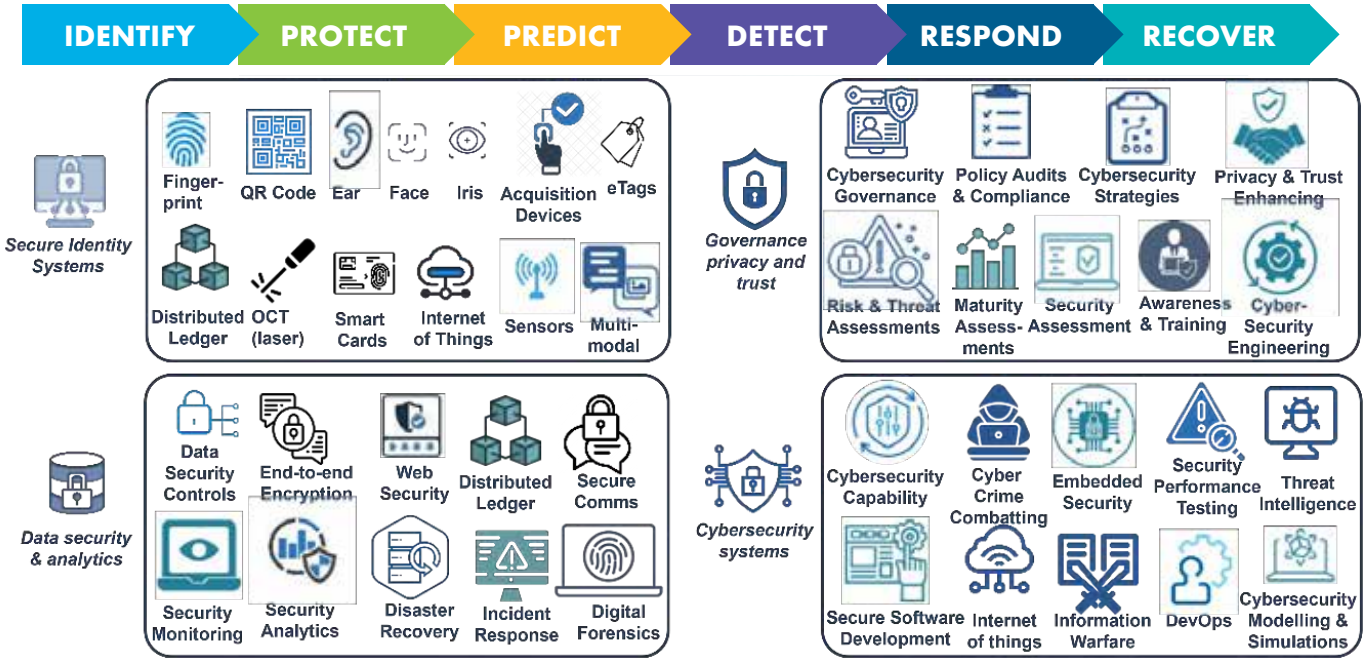
With significant experience in R&D, product innovation and capability development, the CSIR is well positioned to lead the building of a robust, agile and formidable national cybersecurity capability and capacity, as well as to foster innovation for a thriving future industry.

The centre's focus areas are:

- Securing ICT systems;
- Combating cybercrime;
- Cyberwarfare;
- Identity management;
- Awareness and human capital development
- Governance, risk and compliance, and
- Embedded security.

www.csir.co.za

FOREWORD



Local is best: Why home-grown technologies and capabilities are needed to protect and secure the mining sector in the digital realm

In an era of rapid digital transformation and increasing automation within the mining industry, cybersecurity has emerged as a paramount concern. As the digital landscape evolves, so do the sophisticated threats targeting critical mining infrastructure. To maintain operational resilience, safeguard valuable assets and ensure long-term competitiveness, mining companies must prioritise the adoption of home-grown cybersecurity technologies and capabilities.

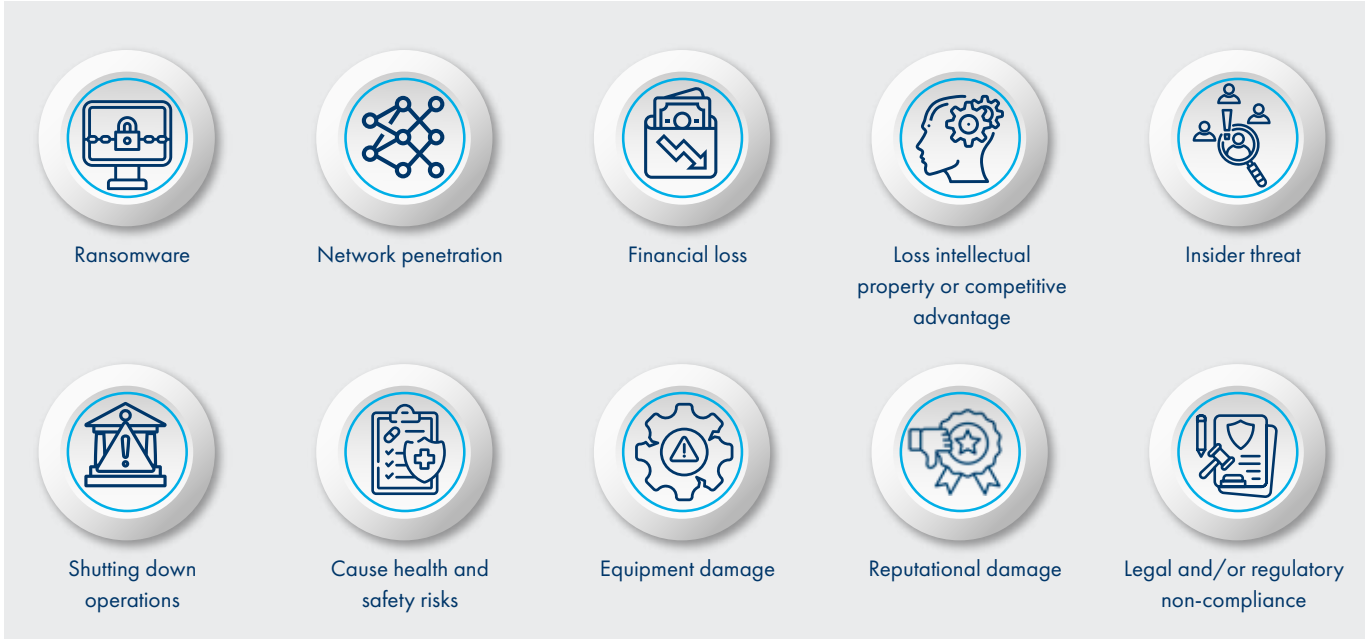


Figure 1: Threats and Risks in the Digital Realm of the Mining Sector

The CSIR Information and Cybersecurity Centre, in collaboration with the South African Department of Science, Technology and Innovation (DSTI), is actively investing in the development and nurturing of local cybersecurity capabilities. This strategic initiative aims to enhance the cybersecurity posture of critical sectors, including mining, by fostering a robust and innovative ecosystem of home-grown solutions.

LOCAL CYBERSECURITY CAPABILITIES FOR THE MINING SECTOR

By developing and deploying home-grown cybersecurity technologies, the mining industry can enhance its control over critical systems and data. This autonomy is crucial for safeguarding sensitive mining operations that increasingly rely on advanced technologies, ensuring business continuity and mitigating the risks associated with reliance on foreign vendors.

ECONOMIC BENEFITS AND JOB CREATION

Investing in the development of home-grown cybersecurity technologies and capabilities offers significant economic and strategic benefits for the mining sector. By nurturing a thriving local cybersecurity industry, we can:

- **Create high-skilled jobs:** Foster the growth of a skilled national workforce capable of developing and maintaining advanced cybersecurity solutions for the mining industry.
- **Stimulate innovation:** Drive innovation within the South African technology sector, leading to the development of cutting-edge cybersecurity solutions tailored to the unique needs of the mining industry.
- **Enhance economic growth:** Establish a competitive cybersecurity industry that can not only serve the domestic market but also compete successfully in the global market, generating export revenue and attracting foreign investment.
- **Strengthen national security:** Enhance the overall cybersecurity posture of the nation by reducing reliance on foreign technologies and building a more resilient and independent cybersecurity ecosystem.

PROMOTING INNOVATION AND RESEARCH

Localising technology development drives innovation and research. Thus, it encourages academic institutions, research councils, public and private industries to invest in the development of advanced cybersecurity technologies and capabilities, pushing through to new levels of ingenuity.

WHAT ROLE DOES THE CENTRE PLAY IN THESE OBJECTIVES?

The CSIR Information and Cybersecurity Centre, with support from the DSTI, has over the past five years, embarked on a focused research and development (R&D) programme to address the critical cybersecurity needs of the industry and government. This programme encompasses key areas, which have relevance in the mining sector, such as:

- **Secure identity and access management (IAM) for mining operations:** Developing and implementing robust IAM solutions to protect critical infrastructure and sensitive data within the mining environment.
- **Data security and analytics:** Enhancing data security and privacy measures, including advanced data analytics and threat intelligence capabilities, to detect and respond to cyber threats effectively.
- **Industrial control system (ICS) cybersecurity:** Developing and implementing secure and resilient ICS solutions to protect critical mining operations from cyberattacks.
- **Cybersecurity governance, risk and compliance (GRC):** Assisting mining companies in developing and implementing effective cybersecurity governance frameworks and compliance programs.

The centre actively seeks impactful collaborations and partnerships with mining companies. We are committed to assisting the sector in enhancing its cybersecurity posture and mitigating the emerging digital risks and threats that pose a significant challenge to operations and business continuity.

Dr Jabu Mtsweni
Head of the CSIR Information and Cybersecurity Research Centre:
Email: JMtsweni@csir.co.za
012 841 4319


FLEXTILT HEAD
CSIR
THORLABS

CYBERSECURITY THREATS AND RISKS TO THE MINING SECTOR

The mining sector is considered a 'physical' operational environment and is assumed to be immune to cybersecurity threats and risks. However, in recent years, due to the drive to automate and digitalise operations, remote access operations technologies (OT) systems such as Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCS) centralised the gathering, analysis and dissemination of critical information. Additionally, with the need to provide monitored safety and health, the mining sector has increasingly become the target for cybercriminals. These ageing OT systems were developed to help companies operate efficiently but not necessarily securely by default.

In a recent survey by PricewaterhouseCoopers (PWC) conducted among CEOs of organisations, it was reflected that cybersecurity and cybercrime have risen to the position of the third most concerning risk to organisations. According to the Council for Scientific and Industrial Research (CSIR), one contributing factor to this rise is the estimated cost of cybercrime in South Africa, which is around R2.2 billion annually as of 2024, with the estimated cost of a single data breach being R53.1 million. Given the significant cost of a single data breach, cyber criminals are increasingly targeting organisations as they streamline their operations through automation and managing facilities and assets remotely with the aid of internet-connected technologies.

In the mining sector, these cyberattacks primarily target IT systems, OT systems and internet of things (IoT). Similar to other industries that rely on IT, the mining sector faces a range of risks associated with IT systems. However, the desired need to merge the OT systems and the IoT systems into visualisation dashboards under the IT systems and the overlap between OT and IT systems has further expanded the threat landscape for the mining sector. In addition, there are more legacy systems that are crucial for operational scenarios under the OT umbrella, further increasing their vulnerabilities.

The table below summarises some of the threats faced by organisations in the mining sector. These threats are then classified according to the probability and severity of their potential impact. Once the threat is realised, the resulting impact is assessed for companies affected by the threat in relation to their sector.

Table 1: Top 10 risks and threats faced by the mining sector

#	Threat or Risk	Probability	Severity	Impact
1	Ransomware	Low	High	Medium
2	Network penetration (IT, OT and/or IoT)	Low	High	High
3	Financial loss	Low	Medium	Medium
4	Loss of Intellectual Property or competitive advantage	Medium	Medium	Medium
5	Insider threat	Low	High	High
6	Shutting down operations	Low	High	High
7	Cause health and safety risks	Low	High	High
8	Equipment damage	Low	Medium	Low
9	Reputational damage	Low	High	High
10	Legal and/or regulatory non-compliance	High	High	High

To support organisations in the mining sector that face the above-mentioned risks and threats, the Information and Cybersecurity Centre at the CSIR offers the following cybersecurity services:

- Qualitative cybersecurity risk assessments (questionnaire-based risk assessment);
- Quantitative cybersecurity risk assessments (vulnerability assessment and penetration testing);
- Cybersecurity gap analysis;
- Design cybersecurity architecture (roadmap);
- Managed security services (design, tool selection, deployment, configuration, maintenance of all security tools such as firewalls, internet proxy, email gateway, endpoint detection and response, security information and event management, security orchestration automation and response, deploying data loss prevention tools as well as other security tools);
- Managed security tools that are deployed on-premises and/or in the cloud;
- Data classification and labelling;
- Managed security operations centre (identify, protect, monitor, respond, recover); and
- Provide digital forensic investigations (mobile phones, email, computers, laptops, servers and so on).

VSOC CAPABILITY FOR THE MINING SECTOR

In South Africa, the increasing trend in data breaches is also observed through breach notifications to the Information Regulator. By June 2023, the Information Regulator in South Africa had received over 1 021 cyber data breach notifications, which is double the number reported in the previous five months of the same year.

The CSIR Information and Cybersecurity Centre is well equipped with systems engineers, cybersecurity researchers, analysts and cybersecurity engineers to assist organisations dealing with cybersecurity incidents.

The virtual security operations centre at the CSIR operates 24/7, providing real-time monitoring, response and recovery as part of its Computer Security Incident Response Team (CSIRT). It is capable of designing, deploying, configuring, maintaining and operating various security operations centre technologies, such as Endpoint Detection and Response, Security Orchestration Automation and Response, Security Information and Event Management, among others.

The CSIR's capabilities include:

- Governance, risk and compliance such as policies, procedures, quantitative risk assessments (penetration testing and vulnerability assessment) and qualitative risk assessments (survey questions to system administrators);
- Guidance and hands-on support on cybersecurity incident response;
- Incident management according to NIST SP 800-61;
- 24x7x365 managed security operations centre according to NIST SP 800-137;
- Awareness training for employees and contractors;
- Digital forensics investigations for computers, servers, mobile phones, emails and report generation for court cases;
- Security tool administration (firewalls, load balancers, internet proxy, email gateway, SIEM tool, SOAR tool, Endpoint Detection and Response, and others).
- On-call for certified senior cybersecurity professionals; and
- Human capital development on the above services.

CSIR CYBERSECURITY TECHNOLOGIES FOR THE MINING INDUSTRY

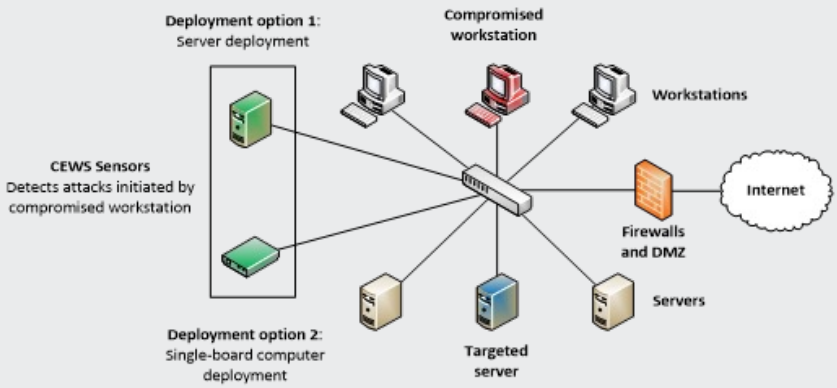
CYBER EARLY WARNING SYSTEM

ICT systems in the mining sector enable informed decision making and the streamlining of business processes, thereby leading to increased process efficiency and productivity, the reduction of operational costs and improved employee, customer and investor satisfaction. However, the mining industry is under threat from targeted and highly coordinated cyberattacks launched by hacktivists, hostile governments and organised criminals. The consequences of successful cyberattacks in this domain range from the disruption of mining operations to the disclosure of sensitive information that could potentially be used to manipulate share prices. Incidents such as the Sibanye-Stillwater cyberattack in July 2024, which led to global outages in ICT systems, have demonstrated the critical importance of securing networked ICT systems in the mining industry from cyberattacks.

Recognising the need for improved cybersecurity in industries such as mining, the CSIR developed a novel technology, referred to as the Cybersecurity Early Warning System (CEWS), for securing ICT infrastructure from cyberattacks. The CEWS is deployed on the intranet and reliably detects and reports cyberattacks that have breached the network boundary via avenues such as phishing and social engineering. This creates a window of opportunity for the network administrator to halt the attack and prevent information theft and service disruption. The competitive advantages of the technology are its low total cost of ownership and its reliability. It is anticipated that the widespread deployment of this technology in the mining sector will curtail successful cyberattacks in this industry, thus preventing disruption to operations and reputational damage.

CEWS provides the following features:

- Scans for cyberattacks in the traffic passing through the connected network switch. It alerts the network administrator to potential threats via email, user interface messages or Security Information and Event Management (SIEM) tie-ins;
- Creates a window of opportunity for responding to and stopping the cyberattack; and
- Prevents network downtime, service disruption, lost revenue and recovery costs.



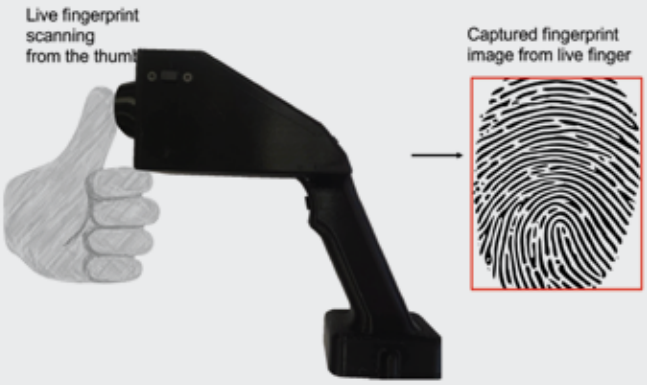
HANDHELD FINGERPRINT SCANNER DEVICE

An active mining site can be a very complex environment with numerous machines for various operations and people performing different tasks. The complexity can be exacerbated by operating underground, which usually increases the risk of injury. The CSIR has developed a contactless lithium-ion battery-powered fingerprint device that can be updated with a dataset of fingerprints in an instant. The device can be used to optimise resource utilisation in a mining operation. It can be used to optimise personnel mining time, verify presence or assist in the allocation of tasks. Since a dataset of personnel on a shift can be loaded instantaneously, the device can play a critical role in safety and emergencies. All these are enabled by the ability to identify a person against a loaded dataset, along with coding their specific locations or intended areas of work. The Fingerprint Scanner Device is a technology capable of uniquely capturing fingerprints and using them to identify or verify a person.

Features:

- Uses a digital camera to capture fingerprints directly from a finger or paper;
- Verifies and identifies individuals quickly and accurately;
- Counts the number of people who have been identified; and
- Determines and records the locations where it was used.

An illustration of the fingerprint device capturing a live fingerprint



An illustration of the fingerprint device capturing a fingerprint from paper

SELECTED RESEARCHERS

ICSC RESEARCHERS PROFILES

Researcher Profile:

Dr NNP Mkuzangwe

Dr Nenekazi Mkuzangwe holds a PhD (Electrical and Electronic Engineering) from the University of Johannesburg and a MSc (Mathematical Statistics) from Rhodes University. She obtained her first degree in 2001. Mkuzangwe has taught mathematical statistics and statistics to science, commerce and health science students at Nelson Mandela University. She joined CSIR in August 2013 under a PhD Studentship Programme and was permanently employed as a network and data security researcher in January 2018. In July 2020, Dr Mkuzangwe became a member of the CSIR's Data Security and Analytics Research Group.

Research Interests: Predictive modelling, intrusion detection, data security/privacy

Masters Students:
Currently mentoring Hombakazi Ngenjane on a research project, "Digital Forensics Supported by Machine Learning for the Detection of Online Sexual Predatory Chats."

She has mentored university students in applying statistics-based machine learning techniques to analyse real-life data to inform decision making in a project called Data Science for Impact and Decision Enablement sponsored by the Department of Science, Technology and Innovation. She has reviewed an international journal article in the field of intrusion detection.

Researcher Profile:

Dr Moses Dlamini

Dr Moses Dlamini is a senior researcher with a focus on information security, cybersecurity, cloud computing security, security of the internet of things, securing artificial intelligence and machine learning classification models, security of operational technology and industrial control systems, securing Industry 4.0, digital deception, context-aware and behavioural authentication, privileged access management, identity and access management, conflict-aware access control, digital forensics and chaos-based cryptography.

Dr Dlamini publishes his research work both at national and international fora. He is also a reviewer of several information security and privacy journals and conferences. He is passionate about technology that serves the needs of society and industry.

He holds a PhD (Computer Science) from the University of Pretoria (2020), a MSc (Computer Science) from the University of Pretoria (2010), a BSc Hons. (Computer Science) from the University of Pretoria (2007) and a BSc (Computer Science and Mathematics) from the University of Swaziland (2002).

Research Interests: Information and cyber security analytics, detection and prevention of adversarial artificial intelligence and machine learning attacks, design of future-proof and zero-trust cybersecurity architectures, detection of digital deception, and fourth industrial revolution security.

Researcher Profile:

Sipho Ngobeni

Sipho Ngobeni is a senior researcher and plays a leading role in assisting industry and government in developing and implementing cybersecurity governance instruments (strategies, policies, processes, procedures, frameworks and standards), cybersecurity assessments, security configuration reviews, threat modelling and operationalising computer security incident response teams. He has authored and co-authored numerous peer-reviewed papers.

Ngobeni holds a MSc (Computer Science) from the University of Pretoria (2016), a BSc Hons. (Computer Science) from the University of Zululand (2007), and a BSc (Computer Science) from the University of Zululand (2006).

Research Interests: Cybersecurity Governance; Cybersecurity Assessments and Audits; Data Privacy and Protection; Digital Forensics and Security Operations.

Researcher profile:

Rethabile Khutlang

Rethabile Khutlang's interests are biological image analysis, exemplar and latent fingerprint acquisition and 3D image analysis using optical coherence tomography. Khutlang has a (MSc Biomedical Engineering) from the University of Cape Town. His experience at the CSIR includes working as a biological and biometrics engineer. Khutlang leads teams working on embedded tokens, data analytics platforms, fingerprint analysis software development kits and a biometrics suite platform. He also leads a team using OCT to address fingerprint spoofing, usage of fingerprints inside skin and lifting fingerprints none destructively from crime scenes.

Research interests: Image processing, machine learning, biometrics and data analysis

Researcher profile:

Dr Namosha Veerasamy

Dr Namosha Veerasamy Is a senior cybersecurity researcher. She is an experienced senior researcher with a demonstrated history of working in the research industry. Skilled in management, networking, security, cyber awareness, and cyber defence.

She holds a BSc (IT Computer Science), a BSc Hons. (Computer Science), a MSc (Computer Science) with distinction and a PhD (Computer Science). She is also a Certified Information System Security Professional (CISSP) and a Certified Information Security Manager (CISM).

Research interests: Financial technology threats, cybersecurity policy, cybersecurity skills assessment, cybersecurity awareness creation and the knowledge of cyber threats.

Researcher profile:

Dr Andre Mcdonald

Dr Andre McDonald is an experienced technology specialist with a demonstrated history of working in the research industry—a strong professional skilled in dynamic systems, chaos theory, signal processing, information theory and cybersecurity.

He holds a BEng (Computer), a BEng Hons. (Electrical Engineering) and MEng (Electrical Engineering).

Research interests: Dynamical systems, chaos theory, signal processing, information theory and cybersecurity.

CONTACTS

DR JABU MTSWENI
Head of the Information and Cyber Security Centre
JMtsweni@csir.co.za
+27 12 841 4394

DR MOSES DLAMINI
Research Group Leader (Acting): Governance, Privacy and Trust
tdlamini1@csir.co.za
+27 12 841 5018

BILLY PETZER
Research Group Leader: Cybersecurity Systems
bpetzer@csir.co.za
012 841 7313

RETHABILE KHUTLANG
Research Group Leader
rkhutlang@csir.co.za
012 841 2257

MUYOWA MUTEMWA
Research Group Leader
mmutemwa@csir.co.za
012 842 7326

CSIR
Touching lives through innovation