



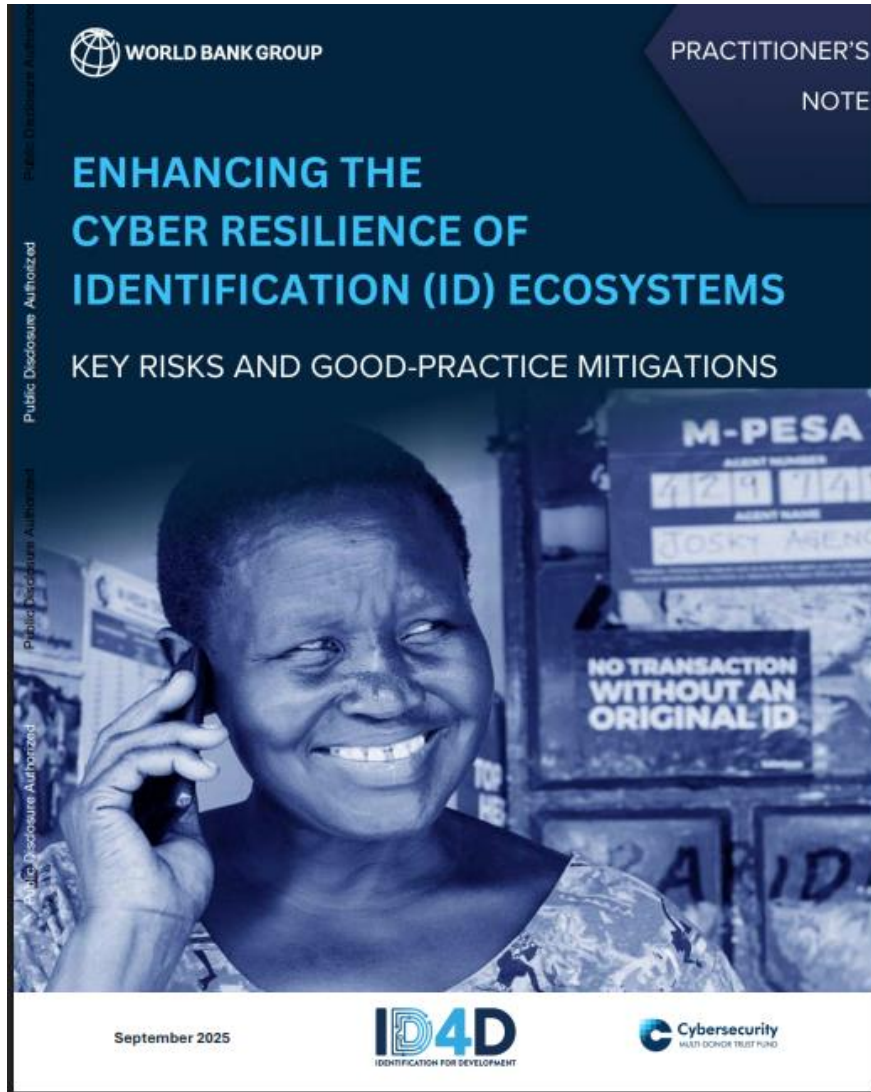
Enhancing the cyber resilience of digital ID ecosystems

ID4Africa
May 2026



WORLD BANK GROUP

World Bank Group and the Turing Institute published a joint knowledge product



Three key trends are reshaping cybersecurity worldwide

Increasingly large ransomware incidents



Economic impact [up to 2.4% of GDP](#) for developing countries

AI-driven sophistication of cyberattacks



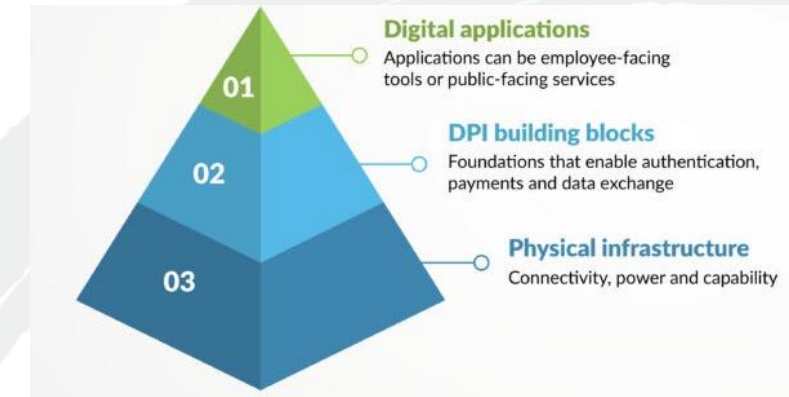
South African Railways Lost Over \$1M in Phishing Scam

Just over half of the stolen funds have been recovered.

John Leyden, Contributing Writer
February 2, 2024

3 Min Read Editor's Choice

DPI investments expand the attack surface



Fraud, identity theft and financial scams are on the rise

As a result, the scale, scope and sophistication of cybersecurity incidents affecting ID ecosystems are growing significantly, in particular in Africa.

Cybersecurity risks arise from vulnerabilities across the entire digital ID lifecycle

Main stages



Examples of risks

Low-cost biometric sensors
Backdoors in the software

Fake breeder document
Face-morphing
Synthetic IDs

Presentation attacks
Credential theft

Biometric or biographic data breaches

Four pillars to assess the cyber readiness of ID ecosystems

**Cybersecurity
foundations**

National level

**Security-by-
design**

ID-specific

**Operational
resilience**

ID-specific

**Innovative
risk
management**

ID-specific

Cybersecurity Foundations

Togo | CDA

Rapid CSIRT Capacity Through Public-Private Partnership

Shared capital investment

Setup costs split between government and Asseco (Poland), reducing upfront public expenditure

Self-financing model

Free CSIRT services to government; revenue from regional private-sector SOC clients

Rapid local skills transfer

Team almost entirely Togolese nationals with structured knowledge transfer

FIRST membership achieved

First low-income country in West & Central Africa to gain FIRST registration

Ghana | NIA & CSA

Building the Institutional & Legal Foundation for a Secure ID Ecosystem

Dedicated legislation

Cybersecurity Act (CSA, 2020) established with 100+ professionals overseeing critical infrastructure

Active CERT-GH / FIRST membership

Only country in West & Central Africa with more than one FIRST-registered team

Data protection framework

Data Protection Act (2012) + Cybersecurity Act govern identity data storage and sharing

Political commitment

Inter-Ministerial Advisory Council elevates identity infrastructure protection to whole-of-government priority

Security-by-Design



Estonia | RIA & PPA — Embedding Security into Digital Identity Architecture from Day One



State-controlled PKI

RIA retains direct control of the root Certificate Authority. Core security governance is never outsourced.



Multi-credential Resilience

Three credential channels (eID card, Mobile-ID, Smart-ID), all PKI-based. If one compromised, others remain.



ISO/IEC Standards in Procurement

ICAO and ETSI standards embedded in all procurement — independently verified benchmarks before deployment.



Transparency as Control

Citizens view their full data access history online at any time, deterring unauthorized access.



Rapid Vulnerability Response

Critical 2017 flaw affecting ~800K eID cards resolved through mass revocation and re-issuance within weeks.

A Gov-SOC or ID-SOC is essential for cyber resilience

India (UIDAI)

Dedicated Security Operations Center (SOC, i.e., network security monitoring) for Aadhaar, with continuous log analysis and anomaly detection (e.g., authentication events success/fail, bulk queries, privilege changes)

Estonia

Centralized SOC for X-Road and ID infrastructure, with strong logging and traceability.

Singapore

The government SOC monitors critical digital services, including identity platforms.

Monitoring **key variables** across the ID platform enables early warnings (e.g., spikes / patterns in authentication)

Early detection reduces risk of **systemic** compromise (credential theft, API abuse, database breach).

The Gov or ID SOC can **escalate** major incidents to the national CSIRT



Operational Resilience

India | UIDAI — Aadhaar: Continuous Security Operations at Billion-Person Scale

1.3B enrollees | **Billions** of monthly authentication transactions



Dedicated 24/7 SOC

Tuned to Aadhaar's threat profile, monitoring unauthorized access to CIDR



Encrypted Biometrics

Biometric data encrypted within certified devices before transmission



Layered Access Architecture

CIDR access only through mandatory ASA and AUA intermediary layers



Tokenization (Virtual ID)

Temporary, revocable VID replaces permanent Aadhaar number for services



Yes/No Authentication

Standard auth returns only YES/NO — no identity data transmitted

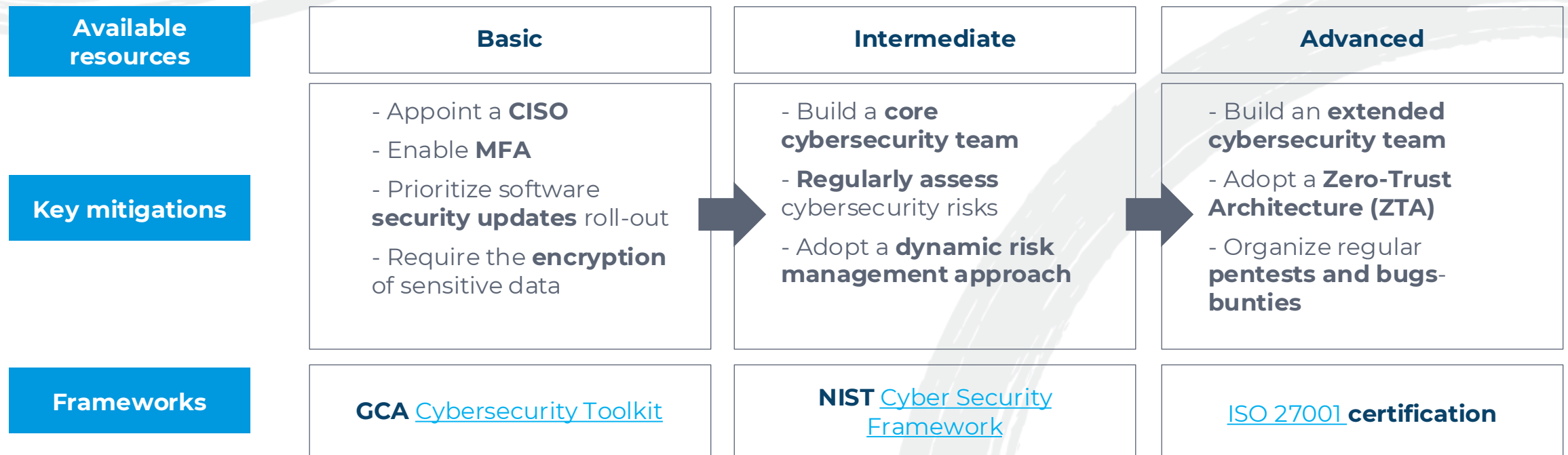


Business Continuity

Geographically distributed data centers with defined recovery objectives

Strengthening cyber resilience for the national ID agency

In Ethiopia, Benin and Nigeria, the World Bank is supporting national ID agencies towards their ISO/IEC 27001 certification (ISMS)



CISO: Chief information security officer.

CISA: Cybersecurity and Infrastructure Security Agency (USA)

GCA: Global Cyber Alliance

MFA: Multi-Factor Authentication (as opposed to passwords only)

NIST: National Institute of Standards and Technology

ZTA: Zero-Trust Architecture (as opposed to perimeter-bound security).



Innovative Risk Management

Singapore | GovTech / Singpass — Proactive Ecosystem Engagement and AI-Driven Identity Security

4.5M users | **2,700+** integrated services | **0** breaches (5 years)



Vulnerability Programs

Three concurrent programs: VDP (public, 2019), GBBP (invited hackers, 2018), VRP (rewards up to USD 150K, 2021)



AI/ML Fraud Detection

Dedicated anti-fraud team monitors real-time anomalies — flagging logins from new devices or inconsistent locations



AI Liveness Detection

Singpass Face Verification matches live scans against biometric records — countering deepfake threats



Law Enforcement Collaboration

GovTech and Singapore Police share threat intelligence; phishing sites blocked immediately upon identification



Legal Deterrence

2024 Computer Misuse Act amendments criminalize sharing Singpass credentials — up to SGD 10K or 3 years

Leveraging security researchers through Vulnerability Disclosure Policies and Bug Bounty Programs

In France and India, the government launched a BBP to identify vulnerabilities on their national digital ID platforms. This enabled the discovery of hundreds of critical vulnerabilities and swift mitigation before they were even exploited.

VDP: A **vulnerability disclosure policy** *gives clear guidelines* on how an organization can be notified of potential vulnerabilities found by external third parties (e.g., email address and or / online form).

BBP: A **bug bounty program** *incentivizes* external third parties to find potential vulnerabilities in a digital platform and notify the organization. In return, the finders are rewarded with social or monetary prizes.

French digital ID's cybersecurity put to the test with bug bounty program

🕒 Jun 14, 2022, 1:46 pm EDT | [Tyler Choi](#)

CATEGORIES [Biometric R&D](#) | [Biometrics News](#) | [Civil / National ID](#)

A global cybersecurity community has announced it will launch a bug bounty program for France's digital ID as an audit of its security and level of trust.

The YesWeHack community is set to scrutinize the [France Identité mobile application](#), a digital ID that was launched as in a beta phase in May 2022. Though France Identité does not biometrically verify its users due to concerns raised by the French public, it can scan national ID cards, which contain a chip that stores biometric data in the form of a photograph and two fingerprints of the card holder.



The Unique Identification Authority of India (UIDAI) has invited 20 candidates from the top 100 bug bounty leader boards like HackerOne and Bugcrowd in its endeavor to secure Aadhaar data hosted in UIDAI's Central Identities Data Repository (CIDR).