Safeguarding National Identification Ecosystems against Cyber Risks

May 2026

ECOWAS CEDEAO

smart africa
CONNECT. INNOVATE. TRANSFORM

WORLD BANK GROUP

Introduction

Objective

Understand Cyber threats for ID ecosystems

Identify and understand the evolving threat landscape, including AI-driven attacks and the persistent challenge of ransomware.

Showcase Best Practices

Highlight international examples of robust digital ID security operations from leading nations such as India, Estonia, and Singapore, offering valuable insights and models.

Cyber Risk Assessment Framework

Show a tool to assess the risks across the pillars and propose mitigations in accordance.

Enhancing Cyber Resilience for National Digital ID Ecosystems.

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

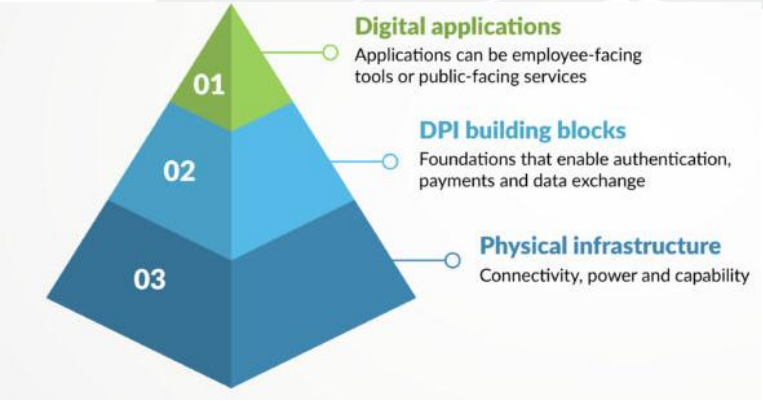
Just over half of the stolen funds have been recovered.

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.

Things That Can Go Wrong

Your Data Gets Stolen

Confidentiality Breach

Criminal or foreign actors access your citizen database and extract personal or biometric records. Often undetected for months.

Your Data Gets Changed

Integrity Breach

An insider or attacker modifies enrollment records: creating fake identities, changing identity attributes, potentially enabling welfare fraud at scale.

Your System Stops Working

Availability Breach

A ransomware attack or deliberate flood of traffic takes your infrastructure offline. Citizens cannot use their identity to access health, finance, or social services.

The scale, scope, and sophistication of attacks is growing significantly — particularly across Africa and South Asia.

What Is a Digital ID Ecosystem?

Understanding what governments are responsible for protecting

A country's ID ecosystem is the complete set of institutions, laws, technologies, and processes that establish and verify people's identities - both in person and online.

Civil Registration and Identification Management Systems

National population registers, birth records, ID number databases. The core store of citizens' identity data.

Digital Credentials & Cards

National ID cards, e-passports, mobile IDs. The physical or digital tokens people carry.

Authentication / Identification / Verification Services

Systems that verify identities, allow for data sharing between entities and platforms.

Institutions and Users of Digital ID systems

From the government authority(ies) responsible for ID, to relying parties using credentials, all the way to the citizens who need to prove their identity.

Laws & Governance Frameworks

Data protection laws, cybersecurity mandates, privacy regulations, liability rules.

Cybersecurity risks arise from vulnerabilities across the entire digital ID lifecycle

Main stages

Examples of risks

Design and Procurement	Registration	Authentication	Data Sharing
Low-cost biometric sensors *Backdoors in the software*	*Fake breeder document* *Face-morphing* *Synthetic IDs*	*Presentation attacks* *Credential theft*	*Biometric or biographic data breaches*

The Most Common Weaknesses

Field experience across national ID programs shows the same weaknesses appearing repeatedly

People & Access

- Government employees can access data they should not. No enforcement of who sees what
- Enrollment agents bribed to register false identities — no monitoring of agent behaviour
- No background checks for staff handling sensitive biometric systems

Data & Systems

- Citizen databases not encrypted - anyone who breaks in can read everything
- Records can be changed or deleted without leaving a trace
- The same ID number shared across multiple systems - one breach exposes all

Devices & Connectivity

- Lost or stolen enrollment devices can still be used - no remote shutdown
- No backup systems - a single failure takes down all ID services
- APIs hand over complete personal records on a simple ID number query

The good news: most of these weaknesses are cheap to fix. They require decisions, not large budgets.

Vulnerabilities: System Design, Authentication & Data Sharing

Beyond the registration pathway, foundational vulnerabilities recur across system design choices, authentication flows, and data-sharing integrations in implementations.

System Design

- Vendor lock-in
- Single points of failure
- Unique identifiers (UIDs)

Authentication

- Replay attacks and session hijacking
- No risk-based / step-up authentication
- No liveness detection

Data Sharing & APIs

- Over exposed APIs
- Weak or absent access logging
- Consent management absent

Good practice: address these foundational vulnerabilities first strong basic information security (encryption, RBAC, logging, redundancy) eliminates the attack surface that enables even sophisticated AI-driven exploits.

Foundational Capabilities Every Government Needs

1 Strong Legal & Governance Frameworks

Pass data protection and cybersecurity laws. Set minimum security standards for all agencies handling identity data. Assign clear accountability.

Reference: EU NIS2, GDPR, UNCITRAL Model Law 2022

2 Incident Response Capacity (CSIRT)

Establish a national team to detect, respond to, and recover from cyberattacks. Only 20% of low-income countries have a fully operational CSIRT.

Only 17 of 54 African nations have registered incident response teams

3 Digital Trust Infrastructure

It ensures that identity credentials are genuine and cannot be faked or tampered with. Can be scaled from simple national certificate authorities models (e.g., the EU Digital COVID certificate) to complex chain-of-trust models (e.g., traditional PKI approaches).

A Digital Trust Infrastructure is the backbone of all secure digital identity systems

4 Critical System Protection (CIP)

Treat digital ID databases as critical national infrastructure. Require security certifications. Western & Central Africa: <250 ISO-certified organizations vs. Japan: 5,500+.

Target: mandate ISO/IEC 27001 for all identity data controllers

5 Cybersecurity Skills Development

Invest in training government staff, building local expertise, and public awareness campaigns. Without skilled people, no technical system stays secure.

Fund cyber education and public-private workforce partnerships

High-level overview of stakeholders in ID ecosystems

National ID ecosystem

Systemic cyber risk

Public or private body responsible for CRVS and foundational ID systems

Public agencies issuing IDs
(e.g., tax, social security, police, passport)

Service providers using IDs
(e.g., hospitals, clinics, judiciary)

Trust Service Providers
(e.g., national CAs, digital signature providers)

Users
(e.g., individuals enrolling in or using national ID services Citizens and Residents)

Digital Wallet ecosystem

Wallet Providers

They will build the wallet on behalf of member states and offer to its citizens, residents and businesses. They will also provide ongoing technical support

Issuers

Any trusted organization that can issue digital ID and/or trusted digital documents like an education certificate, or mobile driving license

Service Providers

Any public or private organization that relies on information from the wallet and requests identification and authentication from wallet users in order to offer a service. Eg. A car rental business that requires a mobile driving license from a customer's wallet before lending them a car.

Trust Service Providers
(e.g., QTSPs — issuing qualified certificates, eSeals, timestamps)

Users / Citizens
(Holders of the EUDI wallet)

Cyber Risks Assessment Framework

Cyber Risks Assessment Framework

Good practices per pillar, grounded in country experience

Cybersecurity foundations

National level

National Computer Security Incident Response Team (CSIRT)
(FIRST member)

Robust legal framework for cybersecurity, data protection and digital IDs
(EU: Directive on Security of Network and Information Systems (NIS2), eIDAS 2.0; Malabo Convention)

National PKI
(CA root, CP/CPS, HSM)

Security-by-design

ID-specific

Leveraging international standards for cybersecurity throughout procurement
(e.g., ISO/IEC 30107, 27034)

ISMS certification for the national ID agency
(e.g., ISO/IEC 27001)

Resilient architecture (decentralized and/or redundant)
(e.g., back-ups, multi-cloud approach)

Operational resilience

ID-specific

Government Security Operations Center (SOC) or ID-SOC

Core technical controls such as Multi-factor authentication (MFA)

Credentials recovery (e.g., forgotten password)

Use of tokens (vs. « unique identifiers ») for transactions and data sharing

Innovative risk management

ID-specific

Leveraging security researchers to harden the digital ID platform (e.g., India, France)

Partnering with Application Stores to badge official government applications (e.g., Vietnam)

Using AI to facilitate fraud detection and response

Resilient Architecture for ID systems

Decentralization

- Split systems and data across multiple environments / locations
- Avoid a single point of failure or compromise
- Limit attacker lateral movement

If one component is breached, the entire ID system is not exposed

Redundant IT Architecture (High Availability)

- Multi-site infrastructure (primary + backup / failover)
- Real-time replication and tested backup & recovery
- Defined RTO/RPO for ID services (enrollment, verification)

Services remain operational even during incidents

A resilient ID system is not just secure; it is designed to contain attacks, minimize data exposure, and continue operating under disruption.

Privacy-Preserving Identity Architecture & Core Security Controls

Strong digital identity systems combine **privacy-by-design architecture** with **enforced security controls** - minimizing data exposure while preventing fraud

Privacy-Preserving Systems & Technologies

Verification APIs return yes/no answers; wallets support selective disclosure. ZKPs are advanced, not baseline.

Minimal Data Flows

Architecture must enforce minimization. Every data flow should be purposeful and legally grounded.

Strong Authentication & MFA

MFA blocks most fraud. Require it for high-risk transactions. Make mandatory, not optional.

Credential Recovery

Use identity re-proofing, not SMS resets, so recovery paths do not become attack vectors.

Logging & Anomaly Detection

Monitor recovery flows for suspicious patterns. Behavioral signals reveal stuffing and social engineering.

Robust IAM for Internal Staff

Staff accessing identity data need strict RBAC, MFA, and complete audit trails.

Strong Authentication: Real-World Implementations

UK GOV.UK One Login

Mandatory MFA enforced for high-risk transactions across government services.

Estonia Smart ID

Multi-factor authentication via smart ID, mobile ID, and hardware-based credentials.

Canada GCKey

Controlled identity recovery with step-up verification and re-proofing workflows.

Unique Identifiers: Implications and Risks

What Are Unique Identifiers?

A unique identifier (UID) like a national ID number is a persistent, system-wide number assigned to every individual in a national ID system. UIDs enable cross-system linkage and are fundamental to digital identity architectures, but they also concentrate risk. Once compromised, they cannot be changed like a password.

Risks of Persistent UIDs

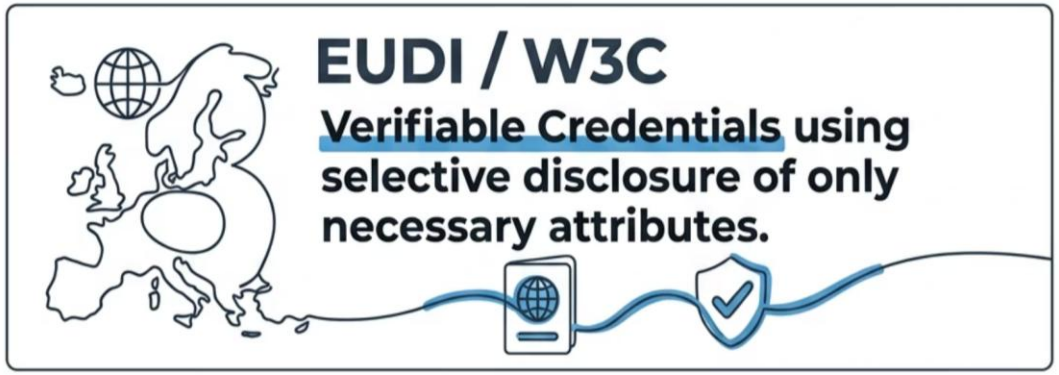
Exposed UIDs enable aggregation attacks, identity theft, and systemic fraud. Sharing UIDs amplifies breach scale.

Tokenization & Pairwise Identifiers

Use transaction-specific tokens or pairwise pseudonymous identifiers.

Operational Best Practices

Use revocable, time-bound tokens; limit sharing to yes/no responses; store real data in isolated systems.



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).

Using AI for fraud detection and response in ID systems

AI strengthens detection and response across the identity lifecycle

- Detects anomalies in authentication & usage (unusual patterns, impossible travel)
- Identifies fraud at enrollment (duplicate / synthetic identities, biometric inconsistencies)
- Supports real-time response (risk scoring, step-up authentication, alerts)

Key use cases in ID ecosystems

- Fraud detection in eKYC / enrollment processes
- Behavioral analytics (user, device, transaction patterns)
- Biometric fraud detection (liveness, spoofing attempts)
- Adaptive authentication (risk-based MFA triggers)

AI must be used responsibly in identity systems

- Bias audits --> ensure models do not discriminate against certain groups
- Human oversight --> no fully automated high-impact decisions (e.g., denial of identity services)
- Explainability & transparency --> decisions must be understandable and auditable
- Data governance --> training data must be representative, secure, and compliant

AI enhances fraud detection, but trust in ID systems requires human oversight, fairness controls, and accountability.

Case Studies

PILLAR 2- CASE STUDY

Security-by-Design

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

State-controlled Certificate Authority

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.

PILLAR 3-CASE STUDY

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

PILLAR 4-CASE STUDY

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

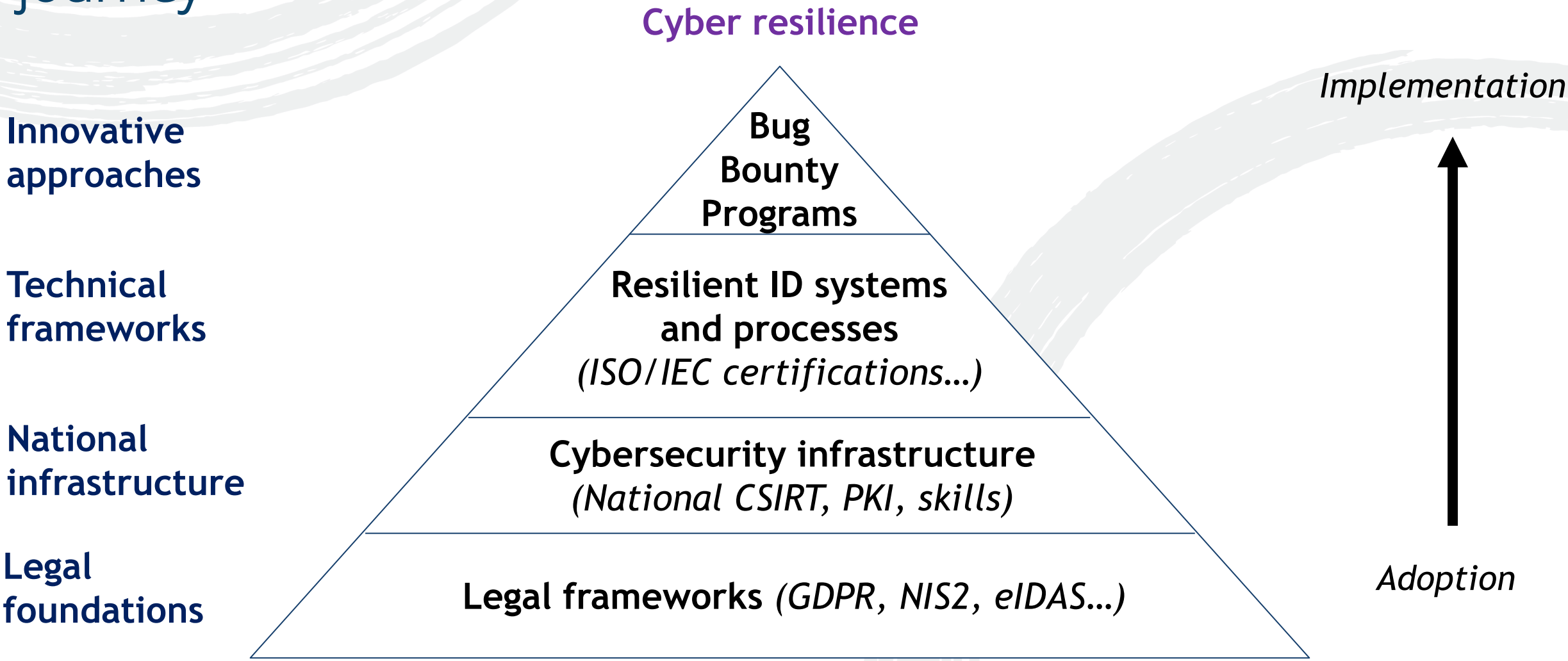
Law Enforcement Collaboration

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

Legal frameworks are just the beginning of your cybersecurity journey



Conclusion

1. **Cybersecurity must be woven into every layer**

   From design & procurement through data sharing and system retirement - not added as an afterthought.

2. **Build foundational national capabilities first**

   Legal frameworks, PKI, CSIRTs, and cybersecurity skills development are prerequisites for long-term resilience.

3. **Adopt Security-by-Design, Privacy-by-Design, and Zero Trust**

   These universal principles must be adapted to local contexts, resources, and technical capacity.

4. **A phased, risk-based approach is essential**

   Start with basic cyber hygiene, progress to advanced controls; avoid overburdening limited resources.

5. **Cooperation builds trust and resilience**

   Engage ethical hackers, technology platforms, and international partners

These are good practices, not best practices. The measures outlined here provide an evidence-based baseline for improvement, serving as a foundation. As the threat landscape evolves, practitioners should enhance this guidance with the latest advisories from national CSIRTs, NIST, ENISA, and FIRST, and adjust their controls accordingly