cyberDNA

IDENTITY INTELLIGENCE

BOARD-LEVEL IDENTITY REPORT · 2026

2026 Identity Risk Index

Understanding how identity exposure defines modern cyber risk.

cyberdna.com.au

Identity · Exposure · Resilience

Identity has become one of the primary attack surfaces of the modern enterprise.

As organisations adopt cloud, SaaS and hybrid work, identity systems increasingly become the path attackers use to gain access. The decisive question is no longer whether the network is defended — it is **who can access what**, and how easily that access can be abused.

This report combines industry research, modern threat intelligence and the CyberDNA Identity Risk Index to help organisations understand where identity risk concentrates and how maturity can be measured.

POSITIONING

This is not a statistical benchmark.

It is CyberDNA's framework for understanding, measuring and improving identity security posture — supported by findings from leading cybersecurity research.

WHAT THIS REPORT COMBINES

Industry research

Established findings from leading global security reports.

Threat intelligence

How adversaries target identity in the current landscape.

Identity Risk Index

CyberDNA's six-domain model for measuring posture.

ABOUT THIS FRAMEWORK

The CyberDNA Identity Risk Index is a qualitative framework designed to help organisations understand identity exposure across six critical domains. This report is not a statistical benchmark of the market and does not claim to represent industry-wide averages or survey findings. The framework is informed by publicly available cybersecurity research and CyberDNA's perspective on identity risk.

What the research consistently shows

Drawn from established, widely-cited industry research. Findings are directional and attributed to their source — not aggregated into a single market statistic.

Verizon

DATA BREACH INVESTIGATIONS REPORT

- Credential abuse remains one of the most common breach techniques.
- The human element continues to play a role in a majority of breaches.
- Privilege misuse remains an important risk factor in both insider and external compromise scenarios.

SOURCE: VERIZON DBIR

Microsoft

DIGITAL DEFENSE REPORT

- Identity attacks continue to be a major concern for enterprises operating in hybrid and cloud environments.
- Password attacks remain one of the most persistent attack methods.
- MFA significantly reduces the risk of account compromise.

SOURCE: MICROSOFT DIGITAL DEFENSE REPORT

IBM

COST OF A DATA BREACH REPORT

- Stolen or compromised credentials remain one of the leading causes of security incidents.
- Credential compromise contributes significantly to breach costs.
- Credential compromise can contribute to longer breach detection and containment timelines.

SOURCE: IBM COST OF A DATA BREACH REPORT

NIST

DIGITAL IDENTITY GUIDELINES

- Strong authentication is foundational to managing identity risk.
- Multi-factor authentication is recommended as a baseline control.
- Identity assurance levels help match controls to the level of risk.

SOURCE: NIST DIGITAL IDENTITY GUIDELINES

CISA

IDENTITY SECURITY GUIDANCE

- Identity and credential attacks are a recurring focus of national guidance.
- Credential theft is highlighted as a common path to compromise.
- Strong identity security practices are emphasised as core defences.

SOURCE: CISA

> **Modern cybersecurity research consistently highlights identity as one of the most critical attack surfaces and a common pathway attackers use to gain access.**

Six domains of identity risk

CYBERDNA FRAMEWORK

The Identity Risk Index measures posture across six domains. Each domain examines a distinct dimension of identity exposure.

01 Authentication Strength

MEASURES

- MFA adoption
- Legacy authentication exposure
- Passwordless readiness

02 Privileged Access Exposure

MEASURES

- Standing privilege
- Admin sprawl
- Access governance

03 Identity Lifecycle Management

MEASURES

- Joiner / Mover / Leaver
- Orphaned accounts
- Deprovisioning

04 SaaS Identity Governance

MEASURES

- SaaS identity visibility
- Shadow IT
- Identity fragmentation

05 Machine Identities

MEASURES

- Service accounts
- Secrets management
- API key governance

06 Third-Party Access

MEASURES

- Vendor identities
- External collaboration
- Access reviews

A maturity path, not a score

Identity programmes progress through four stages — from fragmented and reactive toward an identity-centric security architecture.

01

Emerging

- Fragmented identity visibility
- Reactive controls

02

Developing

- MFA adoption
- Improved governance

03

Managed

- Strong access controls
- Automated lifecycle management

04

Mature

- Continuous identity monitoring
- Identity-centric security architecture

Maturity is a direction of travel — improving visibility and control in each domain moves an organisation toward identity-centric security.

The maturity model is a qualitative guide and does not represent market averages. The CyberDNA Identity Risk Index is intended as a strategic assessment framework rather than a statistical market benchmark.

Identity risk is concentrated, not uniform.

Organisations commonly encounter identity exposure across several recurring areas. Improving visibility and control in these areas strengthens overall resilience.

Privileged accounts	Broad standing access with a high blast radius if abused.
Legacy authentication	Protocols and methods that bypass modern controls.
Dormant accounts	Unused identities that remain active and unmonitored.
Third-party access	External and vendor identities, often over-permissioned.
Machine identities	Service accounts, secrets and API keys at scale.

> **Organisations that improve visibility in these areas are better positioned to reduce exposure and improve resilience.**

What this report is informed by

This report draws on established, publicly available cybersecurity research and national guidance. Findings are referenced directionally and attributed to their source.

01 **Verizon Data Breach Investigations Report (DBIR)**
Breach patterns, credential abuse and the human element.

02 **Microsoft Digital Defense Report**
Identity and password attack trends.

03 **IBM Cost of a Data Breach Report**
Initial attack vectors and breach impact.

04 **NIST Digital Identity Guidelines**
Authentication, identity assurance and MFA.

05 **CISA Identity Security Guidance**
Identity attack and credential-theft defence.

The Identity Risk Index framework and maturity model are proprietary to CyberDNA.

Findings referenced in this report are attributable to the original source and are presented to provide context for CyberDNA's Identity Risk Index framework.

cyberDNA

YOUR NEXT STEP

Understand Your Identity Risk Position

Discover how your organisation aligns with the CyberDNA Identity Risk Index, and identify the areas where identity exposure may concentrate.

Book Your Identity Risk Review →

A 30-minute conversation with a CyberDNA identity specialist.