



THOUGHT LEADERSHIP | CYBERSECURITY

Beyond the Breach

How to Build Unshakeable Cyber Resilience in a
Digital-First World

We live in an era of unprecedented convenience. From automated reporting systems to frictionless global transactions, digital technology has transformed daily business operations into agile, highly efficient workflows.

However, rapid digital transformation carries a fundamental caveat: as technology advances, cyber threats evolve in parallel. Every system hosting organisational or personal data becomes a prime target. A single security breach can compromise sensitive intellectual property, destroy hard-earned trust, and inflict catastrophic financial and reputational damage.

This environment raises a critical question:

How can organisations confidently leverage technology when systemic risks are constantly mounting?

The answer requires a fundamental strategic shift: moving from reactive defence to proactive cyber resilience and deliberately engineering trust into every digital workflow.

The Trust Dilemma: Speed vs. Security

Security is often misperceived as an operational bottleneck: a series of tedious passwords, multi-factor authentication (MFA) prompts, and disruptive updates. However, genuine digital trust is not achieved by ignoring risk, but by managing it strategically.

To maintain operational integrity in an interconnected ecosystem, organisations must anchor their security posture on **three foundational pillars**:

1

Zero Trust Architecture (“Never Trust, Always Verify”)

A perimeter-based security model operates on the flawed assumption that internal traffic is inherently safe. Modern cyber resilience assumes that threats already exist inside the network. By deploying a Zero Trust Architecture, organisations continuously validate user identity, context, and privilege levels at every access point, ensuring that even if a perimeter is breached, lateral movement to core systems is prevented.

2

Proactive Security Engineering

Waiting to respond to an incident is no longer a viable defence strategy. Sustained resilience demands proactive measures:

- **End-to-End Encryption:** Protecting sensitive assets both in transit and at rest.
- **Continuous Threat Monitoring:** Leveraging AI-driven security tools to identify anomalous network behaviour before exploitation occurs.
- **Immutable Data Backups:** Maintaining isolated, tamper-proof data backups to guarantee rapid operational recovery following an attack.

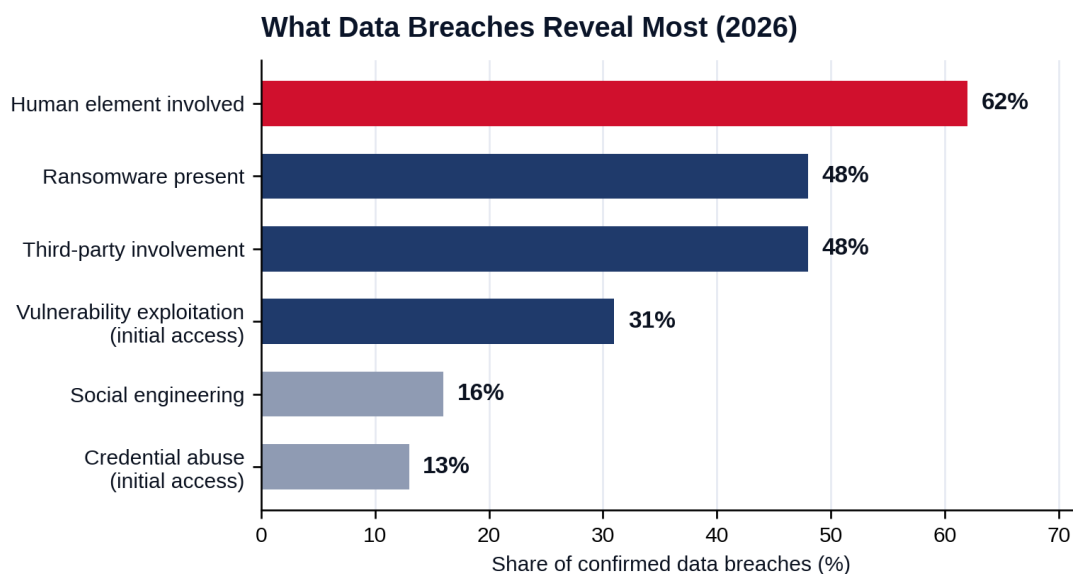
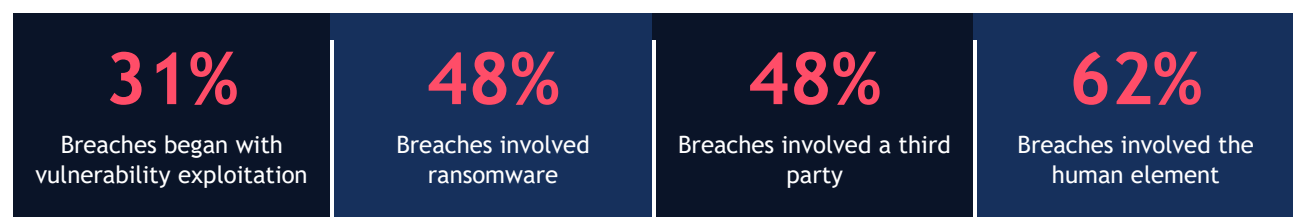
3

Cultivating a Security-First Organisational Culture

Technology is only as resilient as the people operating it. Over 60% of security breaches involve human oversight, including social engineering and phishing schemes. True resilience requires empowering employees through continuous security awareness, transforming them from potential vulnerabilities into an active first line of defence.

Data Breach Landscape: Evidence-Based Insights

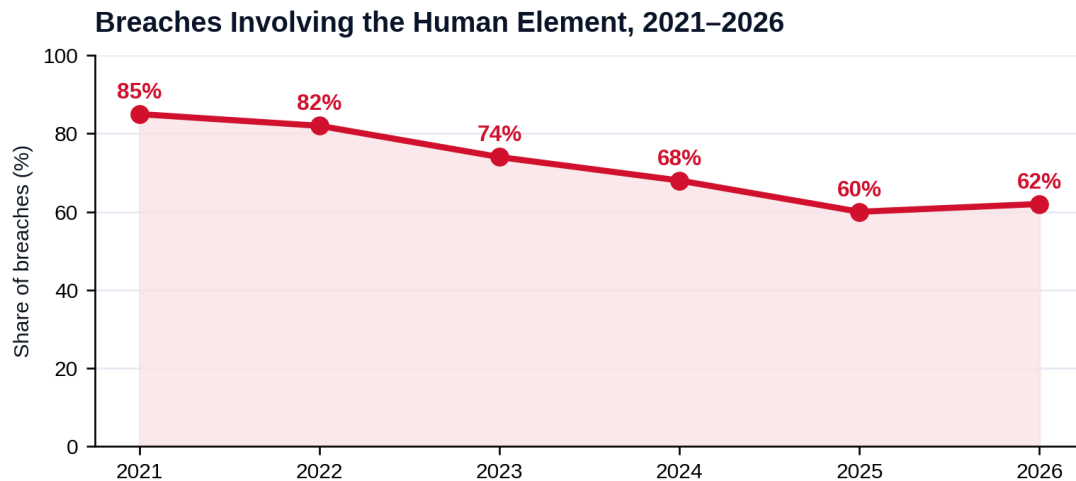
The necessity for continuous cyber resilience is underscored by empirical market data. According to Verizon's 2026 Data Breach Investigations Report (DBIR), which analysed over 22,000 confirmed breaches across 145 countries, several striking trends have emerged:



Source: Verizon 2026 Data Breach Investigations Report (22,000+ confirmed breaches, 145 countries)

Figure 1. Share of confirmed breaches involving each factor. Categories overlap, so a single breach can appear in more than one bar.

Three findings stand out. First, vulnerability exploitation (31%) has overtaken stolen credentials (13%) as the most common way attackers break in, for the first time in the report's history. Second, ransomware now appears in nearly half (48%) of all breaches. Third, breaches involving a third party rose by 60% in a single year, also reaching 48%, which means an organisation's security is now only as strong as its weakest supplier.



Source: Verizon DBIR editions 2021–2026. Verizon refined its human-element definition over this period.

Figure 2. The human element (phishing, social engineering, mistakes and misuse) in breaches, by DBIR edition.

People remain the single most common factor. Although the share has eased from 85% in 2021, the human element was still involved in 62% of breaches in 2026, which is why the security-first culture described above matters so much.

Quick Guide: Building Daily Cyber Resilience

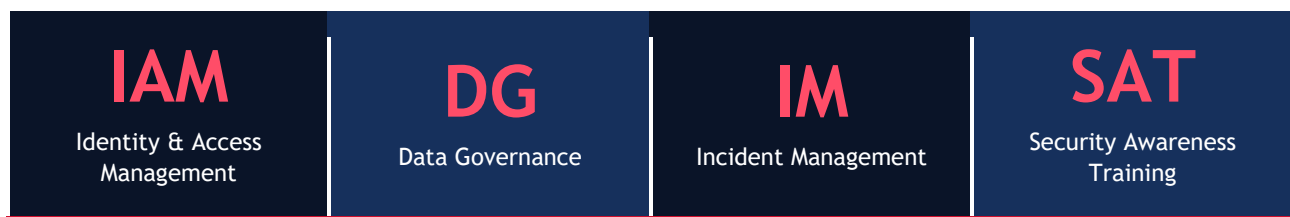
Focus area	Actionable strategy
Data protection	Encrypt data in transit and at rest; keep encryption keys separate from the data; classify sensitive data so the strongest controls protect it first.
Access control	Enforce multi-factor authentication (MFA) on every account, starting with email, admin and remote access; apply least-privilege permissions and review them quarterly; use a password manager.
Vulnerability management	Keep an inventory of all systems and software; patch internet-facing and critical systems first, against a fixed deadline; scan for weaknesses on a regular schedule.
Backups and recovery	Keep isolated, immutable backups (3-2-1: three copies, two media types, one offline); test a full restore on a set schedule.
Continuous monitoring	Centralise logs; alert on unusual logins, large data transfers and privilege changes; name who responds, including out of hours.
Third-party risk	Vet suppliers' security before onboarding; require MFA and breach notification in contracts; give vendors access only to what they need; review them annually.
People and culture	Run short, regular security training and phishing simulations; make reporting a suspicious message easy and blame-free; brief leaders on the top risks.
Incident response	Write a recovery plan with named roles, contacts and decision authority; rehearse it in a tabletop exercise at least twice a year; pre-draft customer and regulator messages.

Securing Tomorrow, Today

Technological advancement should not be hindered; its operational advantages are irreplaceable. However, innovation must never compromise organisational stability. By embedding modern resilience frameworks, enterprises can confidently embrace digital transformation, knowing their data, operations, and market trust are protected.

How BDO Empowers Your Resilience

At **BDO East Africa (Rwanda)**, our Risk Advisory Services practice enables organisations to establish lasting cyber resilience across four key pillars:



Regulatory Compliance & Data Protection

Compliance is both an operational necessity and a statutory requirement. In Rwanda, organisations processing personal data must align with **Law N° 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy**.

We assist clients in navigating these statutory requirements through:

- **Data Protection Impact Assessments (DPIAs):** conducting assessments to identify and mitigate privacy risks.
- **Registration support:** guiding registration as Data Controllers or Data Processors with the Data Protection and Privacy Office (DPPO) under the National Cyber Security Authority (NCSA).

ISO Standards & Management Systems Certification

Through our **ISO Standards Training & Certification Services**, we guide organisations through the end-to-end journey of preparing for, implementing, and maintaining international standards, including:

Standard	Management system
ISO/IEC 27001	Information Security Management Systems (ISMS)
ISO 22301	Business Continuity Management Systems (BCMS)
ISO 9001	Quality Management Systems (QMS)
ISO/IEC 42001	Artificial Intelligence Management Systems (AIMS)

Our advisory team works alongside your workforce to turn compliance and security into an embedded operational culture rather than a periodic audit exercise.

BDO East Africa (Rwanda) | Risk Advisory Services

Partnering with organisations to build unshakeable cyber resilience in a digital-first world.

Authors



Yves Nkaka
Manager IT Advisor



Isabelle Izabayo
Senior IT Advisor



Shami Vanessa Nice
Communication & Client Relationship



Ketty Beriteto
Market Engagement Manager



FOR MORE INFORMATION:

BDO East Africa (Rwanda) Ltd

8th Floor, Career Centre Building

KG 541st

P.O. BOX 6593 Kigali, Rwanda.

Office: (+250) 788 309 225, (+250)738
304 070

Email: rwanda@bdo-ea.com

Service provision within the international BDO network of independent member firms ('the BDO network') is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium with VAT/BTW number BE 0820.820.829, RPR Brussels.

Each of BDO International Limited (the governing entity of the BDO network), Brussels Worldwide Services BV, and the member firms is a separate legal entity and has no liability for another such entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV, and/or the member firms of the BDO network.

BDO is the brand name for the BDO network and for each of the BDO member firms.

www.bdo-ea.com