When Your Identity Security Fails

Patterns, Gaps & How to Fix Them

James Rees

JAMES REES

MD, Razorthorn Security

CISM, PCI DSS QSA, PCIP, ISO 27001 LA

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.

-Sun Tzu

The battlefield has shifted. Attackers are no longer breaking into networks.

Today, they simply log in.

The Reality

- Cloud first
- SAAS everywhere
- Hybrid by default
- Identity now sits in front of every critical system
- We must innovate and reduce costs through rapid AI adoption

What to Watch For

- MFA bypass, token theft, privilege escalation and third party risks
- AI-driven phishing and deepfake impersonation
- Rapid adoption of untested and unfinished AI products
- AI is bypassing traditional controls, introducing new threats

RAZORTHORN

TWO DIFFERENT PERSPECTIVES

The Belief Of The Business

- We have MFA
- We have a strong password policy
- We have conditional access
- We have done the minimum required to meet the standards

The Reality

- MFA enabled but inconsistently enforced
- Privileged accounts exempted for operational reasons
- Service accounts are forgotten
- Identity monitoring is not the most reactive
- Access reviews are performed but not validated

RAZORTHORN

THE IDENTITY CHALLENGE

What does this mean for you?

01 Heavy concentration of financial services and regulated sectors

02 Widespread reliance on Microsoft 365 and cloud SaaS platforms

03 Cross-border access and distributed remote workforces

04 Regulated industries face the sharpest consequences of identity failure

RAZORTHORN

Identity Security Threats

Privilege Creep

- Staff change roles — access never removed
- Admin accounts used for everyday tasks

Overconfidence in MFA

- No phishing-resistant enforcement
- No regular validation testing

No Continuous Validation

- Annual audits and annual pentests
- No visibility in between

Business Process Gaps

- Password resets without strong verification
- Third-party accounts not reviewed

RAZORTHORN

WHAT DOES A GOOD SECURITY PROGRAMME LOOK LIKE?

01 Phishing-resistant authentication for high risk users

02 Regular identity attack simulation

03 Executive impersonation protection strategy

04 Strict privileged access management

05 Formal identity governance reviews

06 Measurable identity risk reporting to the board

RAZORTHORN

We are fighting a constant battle.

We need to be proactive before reactive.

RAZORTHORN

CURRENT TESTING STANDARDS ARE NO LONGER ENOUGH

Identity environments change constantly

- New SaaS apps added monthly
- New integrations and API tokens
- New remote contractors
- New privileged roles
- Annual testing misses drift

Continuous Validation

- Regular validation of identity pathways
- Simulated attacks against authentication
- Privilege escalation validation
- Drift detection over time

RAZORTHORN

HOW RAZORTHORN CAN HELP

Assurance Testing

- Internal & external pentesting
- Web app pentesting
- Mobile pentesting
- Cloud reviews
- Red teaming

Governance Advisory

- Business security review
- Defence in depth review
- Deepfake risk reviews
- Security maturity against ISO27001, PCI DSS, DORA, NIS2, MiCA, etc

Continuous Threat Exposure Management

- Repeatable testing model
- Ongoing exposure tracking
- Evidence for regulators and boards

RAZORTHORN

We don't just tell you
you're compliant.

**We show you whether
you are resilient.**

RAZORTHORN

The next breach you suffer will not be because your security perimeter failed.

They were already in.

TEST IT | **VALIDATE IT** | **GOVERN IT**

RAZORTHORN

THANK YOU

www.razorthorn.com

hello@razorthorn.com

Listen to the Razorwire Podcast

RAZORTHORN