Cybersecurity in 2026: KEY TAKEAWAYS

A PRACTICAL GUIDE TO UNDERSTANDING TODAY'S IDENTITY-DRIVEN THREAT LANDSCAPE.

Brian Jackson (CEO), Jonathan Perz (Manager of Information Security), and Lauren Pankey (Manager of Technology Risk) of Abacus Technologies explain why cybersecurity in 2026 demands an identity-centric strategy focused on identity protection, cloud discipline, and rapid response to reduce financial, operational, and reputational risk beyond what traditional perimeter defenses can address.

What's Driving Security Risk in 2026

1. Credential Theft & Multifactor Authentication (MFA) Bypass

- Phishing remains the primary entry point.
- MFA fatigue attacks pressure users into approving login prompts.
- Attackers steal session tokens, which can remain valid for up to 90 days.
- Token theft allows access even if passwords are changed.
- Implication: MFA alone is no longer sufficient.

2. Cloud Misconfiguration

- Many cloud environments are not secure by default. Excessive permissions and weak configuration allow attackers to install malicious applications, maintain persistent access, and avoid detection.
- Implication: Identity and access management must be actively governed.

3. Business Email Compromise (BEC)

- Identity-based attacks frequently lead to wire and ACH fraud, payroll diversion, invoice manipulation, and reputational damage
- Unlike ransomware, these attacks often occur quietly and can go unnoticed until funds are lost.

4. Ransomware Still Matters

- Ransomware continues to exploit unpatched firewalls, outdated VPNs, and internet-facing systems.
- Organizations without tested backups and response plans face prolonged downtime and operational disruption.

Emerging Risk: AI Security & Governance

- AI adoption introduces new cybersecurity considerations. Organizations must address AI governance frameworks, data leakage risks, model access controls, alignment with compliance requirements, and responsible use policies.
- AI increases productivity but also expands attack surfaces, accelerates attacker capabilities, and introduces regulatory risk if unmanaged

Executive Priorities

Enforce conditional access policies

- Monitor abnormal login behavior
- Reduce session token exposure
- Restrict third-party app permissions
- Conduct regular configuration reviews
- Enable enhanced logging and monitoring

Improving Response Readiness

- Implement continuous monitoring
- Test incident response plans
- Maintain offline, recoverable backups

AI Governance & Strategy

- Define a clear AI strategy aligned to business goals
- Implement company-wide AI training and usage policies
- Maintain an evolving policy framework as technology and regulations change

AI Security & Risk Management

- Ensure secure configuration of AI platforms
- Manage third-party AI risk through due diligence
- Strengthen data risk management to prevent leakage or misuse

STAY INFORMED:

Sign up for our BMSS newsletter and contact us at www.bmss.com and www.abacustechnologies.com

https://www.bmss.com/newsletter-signup/

BMSS Family of Companies

Abacus TECHNOLOGIES