Abacus TECHNOLOGIES

BMSS Family of Companies

CYBER SECURITY IN 2026

Threat Landscape, Vulnerability Management, and Securing AI

February 19, 2026

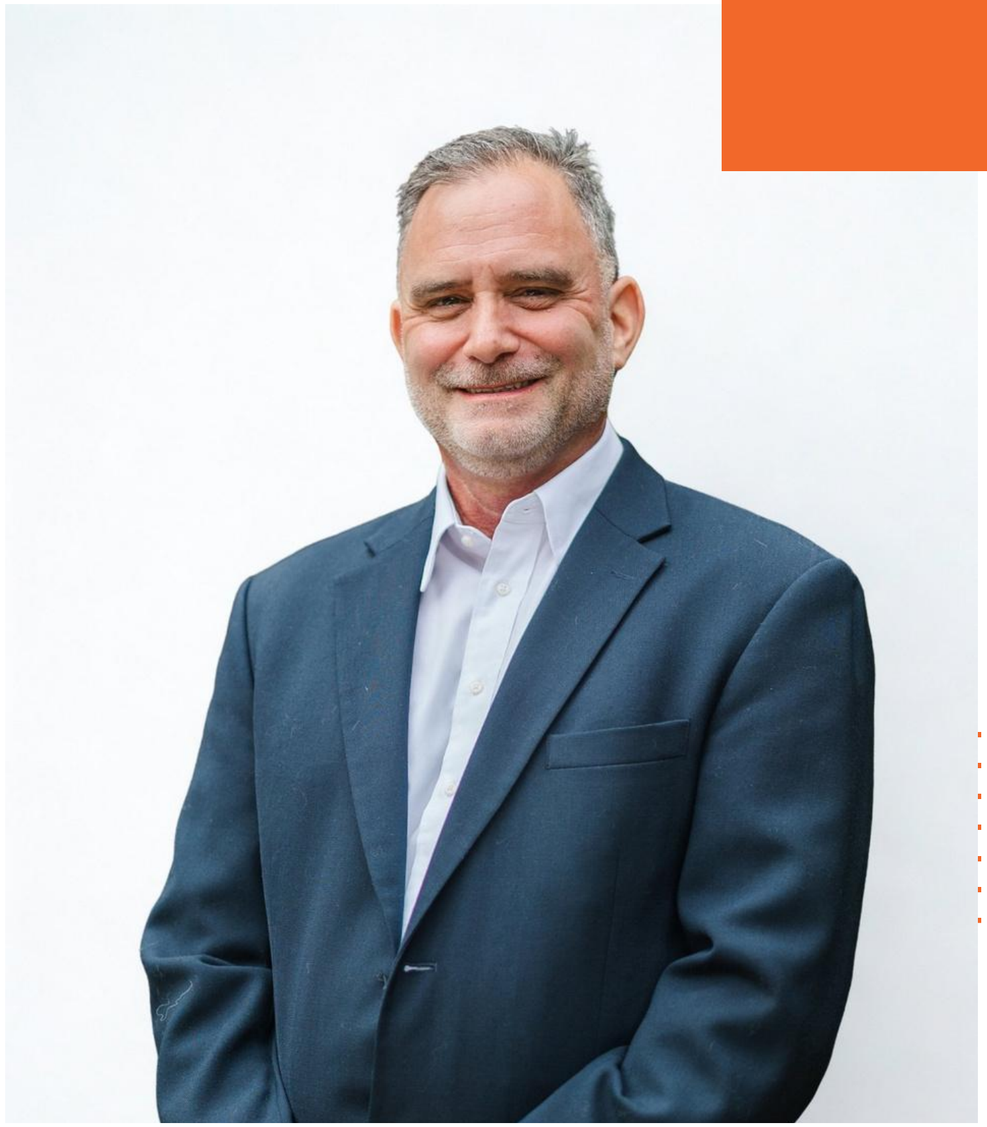
BRIAN JACKSON

- Brian Jackson is the CEO of Abacus Technologies.
- In his role, he oversees all executive decisions and operations of the company along with providing client solutions and development.
- He began his career in technology by implementing accounting systems, business intelligence solutions and developing system integrations and now uses that experience to help clients implement and support business applications, computer hardware, network infrastructure, cloud solutions and cybersecurity processes.

Abacus
TECHNOLOGIES

JONATHAN PERZ

- Manages Abacus Technologies' Information Security practice
- In his role, he engineers and manages security solutions for a wide array of organizations of all sizes in almost every vertical.
- Bachelor degree in Computer Science and Masters degree in Cybersecurity from University of Alabama at Birmingham (UAB).
- Teaches a graduate level course on Penetration Testing at UAB.



Abacus TECHNOLOGIES

TODAY'S AGENDA

- Cybersecurity 2026 Threat Landscape – Jonathan Perz
  - The Real Threat Landscape
  - Shifting from Reactive to Proactive Security
  - Why 24/7 Monitoring and Vulnerability Discipline Matter

- Securing AI – Lauren Pankey
  - Governance Frameworks, The Engine and the Blueprint, Third-Parties, Liability and Access, Future Trends
- Conclusion
  - Wrap Up and Q&A

Abacus TECHNOLOGIES

THE REAL 2026 CYBERSECURITY REALITY

- Cybersecurity in 2026 is not about *if* you are targeted. It is about how fast you detect and respond.
- The macro shifts…
  - Identity is the perimeter
  - Speed and skill of exploitation are compressing
  - AI is accelerating both attackers and defenders
- Most breaches begin with a compromised identity — not a zero-day vulnerability.

Abacus TECHNOLOGIES

ORGANIZATIONAL THREAT REALITY: Where Damage Actually Happens

What are we seeing?

- MFA fatigue attacks
- Token theft and session hijacking
- Credential harvesting via advanced phishing kits
- Comprised accounts through malicious app permissions
- Ransomware remains active and adaptive

Abacus TECHNOLOGIES

ORGANIZATIONAL THREAT REALITY: Where Damage Actually Happens

- Business Impact of Identity Compromise:
  - Business Email Compromise (BEC)
  - ACH / wire fraud
  - Vendor payment redirection
  - Malware distribution to clients
  - Reputational damage
  - Regulatory exposure

A compromised Microsoft 365 account is not just an email problem. It is a business continuity problem.

Abacus TECHNOLOGIES

BIG PICTURE QUESTIONS

Ask Yourself:

- Do I know who is logging into my environment — in real time?
- How long could an attacker stay in an account without re-authenticating?
- If access occurred at 2:00 AM Friday, would we know before Monday?
- Would our first alert come from a client?

Abacus TECHNOLOGIES

AI IS COMPRESSING TIMELINES AND SKILLSETS

- AI Is Compressing Timelines
  - Exploit code appears within days of disclosure
  - Ransomware groups weaponize vulnerabilities rapidly
  - Attackers scan continuously and automate targeting
- AI Is Compressing Skillsets
  - Hackers are ‘smarter’
  - Lower entry point for threat actors to be impactful

Quarterly patch cycles are outdated thinking.

Attackers use AI with great effect to make their attacks more effective.

Abacus TECHNOLOGIES

24/7 MONITORING IS A NECESSITY

- Most organizations have tools. Few have:
  - Continuous log ingestion
  - Correlated alerting
  - After-hours monitoring
  - Defined response playbooks
  - Containment authority
- An alert at 2:13 AM Friday is useless if no one acts until Monday.

Cybersecurity is about closing the gap between compromise and containment.

Abacus TECHNOLOGIES

VULNERABILITY MANAGEMENT: THE DISCIPLINE MOST ORGANIZATIONS UNDERESTIMATE

- Vulnerability management is not patching. It is risk prioritization.
- Common Gaps:
  - Incomplete asset inventory
  - Unknown internet-facing services
  - No context-based prioritization
  - CVSS-only decision making
  - No validation of remediation

If you do not know what you have, then you do not know what you are exposing.

Abacus TECHNOLOGIES

VULNERABILITY MANAGEMENT: THE DISCIPLINE MOST ORGANIZATIONS UNDERESTIMATE

- Modern vulnerability management Requires:
  - Continuous asset discovery
  - Risk-based prioritization (exploit in the wild + business criticality)
  - Clear remediation ownership
  - Compensating controls when patching cannot happen
  - Validation and executive reporting

Attackers automate discovery.
Your defense must be at least as disciplined.

Abacus TECHNOLOGIES

WHAT ABOUT AI AND CYBERSECURITY?

AI is an acceleration engine.

- ATTACKERS Use AI To…
  - Improve phishing realism
  - Automate reconnaissance
  - Scale social engineering
  - Evade traditional detection patterns
- DEFENDERS Use AI To…
  - Improve anomaly detection
  - Enhance SOC triage
  - Improve risk prioritization

AI can be a business multiplier, but we cannot ignore the real threat to your organization in 2026.

AI does not eliminate governance risk. It multiplies it.

Abacus TECHNOLOGIES

LAUREN PANKEY, CISA

- Manager, Technology Risk
- Performed 500+ SOC audits for companies of all sizes, ranging from start-ups to fortune 500 companies across a wide range of industries, including fintech, healthcare, insurance, manufacturing, B2B services, and cryptocurrency.
- Help companies navigate AI governance through policy development, third-party AI vendor risk assessments, and more.
- Auburn University: Bachelor of Science in Business Administration – Information Systems Management
- University of Alabama at Birmingham: Master of Science – Information Systems Management

Abacus TECHNOLOGIES

THE 2026 THREAT LANDSCAPE: GOVERNANCE

- Agentic Risk: AI agents acting autonomously can bypass traditional firewalls.
- Data Leakage Risk: Employees inadvertently feeding proprietary code or PII into public models.
- Shadow AI Risk: The rise of unvetted AI tools used across departments without IT oversight.

Abacus TECHNOLOGIES

THE 2026 THREAT LANDSCAPE: GOVERNANCE

What is Agentic AI and What are AI Agents?

- An AI Agent handles a single, well-defined task. On their own they are not designed to manage complex task or adapt to changing business conditions without an agentic unifying layer. Example: Personal Shopping Assistant or 24/7 Chatbots.
- Agentic AI is the system that coordinates many of these to execute broader, multi-step workflows that span teams and systems. Agentic AI adapts as the system changes. Example: Uber's Enhanced Agentic RAG.

Abacus TECHNOLOGIES

THE 2026 THREAT LANDSCAPE: GOVERNANCE

What is Shadow AI and How Does it Relate to Data Leakage?

- The unauthorized, unapproved, and often unmonitored use of AI-powered tools, applications, and services within an organization, usually by employees attempting to increase productivity without following IT security protocols or Company policy.
- Employees may enter confidential, proprietary, or personal data into public AI models, which can then be used to train those models further, exposing the Company's information.

Abacus TECHNOLOGIES

GOVERNANCE FRAMEWORKS (ISO 42001 AND NIST AI RMF)

- Key Points:
  - ISO 42001: The new gold standard for AI Management Systems (AIMS).
  - NIST AI RMF: Focus on the four functions: Govern, Map, Measure, Manage.
  - Audit Readiness: Integrating AI security into existing SOC 2 or ISO 27001 cycles.

Abacus TECHNOLOGIES

THE BLUEPRINT: ESTABLISHING A CORE AI POLICY

- Key Points (Policies):
  - Acceptable Use: Defining "Green" (allowed), "Yellow" (restricted), and "Red" (prohibited) AI tools.
    - Data Sensitivity: Explicitly banning the input of PII, trade secrets, or client data into non-enterprise-grade AI.
    - Ethical Guardrails: Setting standards for bias mitigation and fairness that align with corporate values.
    - Control and Accountability: Defining who is responsible for AI outcomes and decisions and requires human review for critical decisions.

Abacus TECHNOLOGIES

THE ENGINE: OPERATIONAL PROCEDURES AND PROCESSES

- Key Points (Processes):
  - AI Use Case Inventory: A mandatory registry for every AI tool used in the company (crucial for ISO 42001).
  - Algorithmic Impact Assessments (AIA): A formal procedure to score the risk level of a new AI tool before deployment.
  - Human-in-the-Loop (HITL): Procedures requiring a human "sign-off" on high-consequence AI outputs.

Abacus TECHNOLOGIES

THE SUPPLY CHAIN: THIRD-PARTY AI GOVERNANCE

- Key Points (Procedures):
  - Vendor Due Diligence: Updated SOC 2 and ISO questionnaires that ask specifically about model training data.
  - Model Provenance: Verifying where the data came from (avoiding "poisoned" or copyrighted data).
  - Contractual Liability: Procedures to ensure vendors assume liability for model hallucinations or security breaches.

Abacus TECHNOLOGIES

LIABILITY AND ACCESS: CONTROLLING THE “KEYS”

- Key Points:
  - Identity for AI: Treating an AI agent like a user with a unique ID and limited permissions (Least Privilege).
  - Audit Trails: Maintaining immutable logs of every action an AI agent takes for legal and compliance reasons.
  - The "Kill Switch": A formal procedure for emergency deactivation of a rogue or compromised AI system.

Abacus TECHNOLOGIES

FUTURE TRENDS: AI GOVERNANCE

- Key Points (Future Trends):
  - Audit Your Shadow AI Now
    - You cannot govern what you cannot see
  - Continuous Auditing: Shifting from "once-a-year" audits to real-time compliance monitoring.
  - Cross-Functional AI Council

Abacus TECHNOLOGIES

QUESTIONS?

BMSS
Family *of* Companies