MICHAEL YANDRISCHOVITZ

INFORMATION SECURITY LEADER

Falls Church, VA | 571-214-7119 | mike124@gmail.com | mikewhy.com | https://www.linkedin.com/in/mikewhy443/

CISSP, PMP, CISM

PROFESSIONAL SUMMARY

Strategic and execution-focused Information Security Leader with 20+ years of experience driving enterprise security programs, risk management, and cloud/SaaS security architecture across regulated, public and private, client-facing environments including financial services, consulting, higher education, and technology sectors. Trusted advisor to executive leadership and Boards, with a proven track record of maturing enterprise security posture, achieving audit readiness (SOC 2, ISO 27001, SOX), and enabling business growth through transparent, resilient security operations. Combines executive-level strategy with deep hands-on expertise in areas including SaaS governance (Microsoft 365, Purview, Salesforce), firewall and VPN architecture, endpoint hardening, vulnerability remediation, and incident response. Adept at aligning security controls with business priorities to reduce risk, accelerate sales, and ensure compliance. Recently expanded focus to include AI governance and emerging technology risk management.

CORE COMPETENCIES

- Enterprise Security Strategy & Roadmap Development
- Security Architecture (Cloud, Hybrid, Zero Trust)
- SaaS Security Governance (Microsoft 365, Microsoft Purview, Salesforce)
- Risk Management & Regulatory Compliance (SOC 2, ISO 27001/22301, NIST)
- Client Assurance, Executive Communication & Thought Leadership (SIG, CAIQ, RFPs)
- Third-Party Risk Management & Contract Security Reviews
- Security Governance, Policy Management & GRC
- Incident Response, Root Cause Analysis & Playbook Development
- Security Awareness & Behavioral Risk Reduction
- Board & Executive-Level Reporting & Stakeholder Engagement
- Team Leadership, Staff Development & Cross-Functional Collaboration
- AI Governance & Responsible Use Oversight

PROFESSIONAL EXPERIENCE

Director, Information Security
TRELIANT (now Huron)

Aug 2015 – Present
Washington, D.C.

(Promoted from Senior Security Engineer to Director in recognition of leadership in security architecture, governance, and client assurance)

- Lead Treliant's enterprise-wide information security program for 2,500+ global users across hybrid remote/cloud environments, building strategic roadmaps to reduce risk, achieve audit readiness, and drive client trust and retention
- Directed security governance lifecycle managing 200+ policies, procedures, and control documentation while consistently achieving clean audit reports and establishing accountability across all business units
- Led enterprise risk strategy and governance including BCP/DR planning and compliance programs; provided executive leadership with risk intelligence for strategic business decisions
- Presented security performance metrics and risk insights to executive leadership regularly; influenced control improvements and investment strategies that reduced organizational risk by 18% annually through data driven decision making
- Delivered 8 consecutive years of exception free SOC 2 Type 2 attestations through comprehensive control management and auditor engagement; strengthened client confidence and supported business expansion
- Owned end-to-end security questionnaire process for 500+ annual client engagements (SIG, CAIQ, VSA, custom assessments), developing reusable response libraries and streamlining turnaround times; enabled successful onboarding, renewals, and new business wins by articulating complex security posture in client-appropriate language
- Led customer facing security initiatives including sales enablement, brand evangelism, and thought leadership to strengthen client trust, accelerate new business acquisition, and position security as a competitive differentiator
- Executed vendor security program for 100+ third parties annually, reducing risk exposure by 50% through assessments, contract controls, and remediation tracking
- Governed enterprise SaaS security for 2,500+ users through Microsoft 365 and Purview implementations including Conditional Access, DLP policies, and data classification; secured sensitive data and reduced exposure while maintaining user productivity
- Designed enterprise data classification and retention policies covering PII, confidential, and financial data in alignment with NIST and ISO standards; decreased data spillage incidents by 40% through improved handling practices and controls

- Managed enterprise vulnerability program and security operations, ensuring rapid remediation of critical exposures and maintaining hardened configurations across all systems
- Architected security infrastructure including firewall design, VPN deployment, and cloud security controls; delivered high availability and compliance across hybrid environments through deep technical expertise
- Oversaw network team and infrastructure including Cisco network systems, Palo Alto firewalls, and GlobalProtect VPN, achieving 99.9% uptime for global offices while ensuring secure remote access and resilient core systems
- Drove enterprise security projects including SOC 2 preparation, firewall upgrades, and VPN deployments from initial scoping to successful delivery; ensured on time completion through strategic resource planning and stakeholder alignment
- Drove enterprise security awareness training to 100% completion rate while reducing phishing clicks by 70% through targeted awareness campaigns and targeted content
- Built first generative AI governance program establishing secure usage policies and client data protection controls; enabled innovation across the organization while preventing data leakage and ensuring compliance
- Led incident response program including biannual tabletop exercises across Legal, IT, HR, and executive teams; reduced response time by 30% and minimized business impact through improved escalation procedures and lessons learned implementation

Director, Information Security
GARTNER (formerly CEB)

Aug 2012 – Aug 2015
Arlington, VA

(Promoted from Senior Security Engineer to Director following successful delivery of enterprise-wide security initiatives)

- Completed global multi factor authentication rollout to 8,000+ users across 60+ locations in under six-months; transformed credential security and remote access infrastructure
- Pioneered firm's BYOD and access control framework for 10,000+ employee devices using posture-based security policies; reduced unmanaged device risk by 90% through automated compliance checks
- Led cybersecurity assessments for M&A due diligence and integration, evaluating acquisition targets and harmonizing inherited systems with enterprise controls to ensure secure transitions without business disruption
- Eliminated 95% of malware infections by removing local admin privileges from 4,000+ endpoints and enforcing least privilege access, drastically reducing enterprise attack surface
- Established SIEM and logging architecture reducing mean detection time by 45% and response time by 35%; implemented vulnerability management program that accelerated remediation and improved security posture visibility
- Implemented enterprise web filtering and user activity monitoring, increasing policy adherence by 60% through improved visibility and automated enforcement
- Optimized security questionnaire responses reducing client onboarding time by 5 to 7 days while strengthening buyer confidence and accelerating renewals
- Provided strategic guidance on ISO 27001/22301 compliance and security posture improvements; aligned organizational priorities to fast-track certification readiness
- Supported SOX audits by implementing and validating ITGCs for access provisioning, privileged account management, audit logging, and change control; partnered with Internal Audit to close control gaps and streamline evidence collection
- Led vendor risk assessments evaluating third party security controls and contracts; ensured alignment with enterprise standards while mitigating supply chain risks across critical partnerships
- Led secure software development initiatives embedding security controls throughout the SDLC; ensured secure coding practices met compliance mandates and client expectations
- Directed incident response and root cause analysis across the enterprise; enhanced playbooks and containment strategies that strengthened organizational resilience and minimized business impact
- Embedded security reviews within change management workflow; assessed risks and provided mitigation strategies that ensured secure compliant implementations
- Advised Enterprise Architecture Board on security implications of technology decisions; ensured alignment between new deployments and enterprise security standards

Information Security Officer
GEORGETOWN UNIVERSITY | McDonough School of Business

Jun 2009 – Aug 2012
Washington, D.C.

- Led security program for Georgetown's McDonough School of Business, building foundational policies, conducting risk assessments, and maturing controls that protected critical faculty, research, and operational systems
- Developed and delivered targeted awareness training for faculty, staff, and students, improving policy adoption and reducing reported incidents by 40% while strengthening protection of academic and institutional data
- Led risk assessments for academic systems, identifying high priority vulnerabilities and securing funding for critical controls while improving alignment between IT and school leadership on threat mitigation
- Improved access governance by leading periodic reviews with department heads, remediating 85% of permission discrepancies and reducing unnecessary access to sensitive systems
- Supported academic incident response and post-incident reviews, refining containment strategies and improving cross-departmental coordination to accelerate resolution
- Led investigations into policy violations, providing senior leadership with actionable recommendations that mitigated risk and improved accountability
- Led and developed 6 junior staff members, strengthening their security analysis and project delivery skills through direct coaching and performance guidance

- Selected to lead McDonough School of Business's first Salesforce implementation as a special project alongside security program leadership; directed cross-functional team from requirements through go-live, establishing role-based access, FERPA-compliant data protection, and governance controls that enabled broad academic and administrative adoption

Network Security Manager
GEORGETOWN UNIVERSITY

Jul 2006 – Jun 2009
Washington, D.C.

(Promoted through multiple roles—from Network Security Manager to Information Security Officer—reflecting strong technical execution, risk leadership, and program development)

- Led network security operations including intrusion detection, incident response, and hardening efforts, improving system resilience and reducing downtime by 60%
- Conducted penetration tests and vulnerability assessments to identify system weaknesses; led rapid malware response efforts that reducing containment time by 50%, reducing exposure and preventing system compromise
- Served as digital forensics expert for cross functional investigations with legal, audit, and law enforcement teams, resolving policy violations and misuse cases

EDUCATION & CERTIFICATIONS

Master of Science
Technology Management – Georgetown University

Master of Science
Computer and Information Sciences – DeSales University

Bachelor of Science
Computer Science – Alvernia University

CISSP PMP CISM

ITIL