Robert Hayden, CISSP

Multi-skilled security professional

Bob@BobHayden.org linkedin.com/in/robert-r-hayden 585.755.2139 Rochester, NY

TECHNICAL SKILLS

Strategy and Planning: Capability and benefit roadmaps, Tool and service optimization, Security strategy, Architecture, Program management

Information Security: IT Security domain expertise, Policy development and management, Security awareness & training, Risk assessment & compliance, Technical security team leadership, Platform engineering

Cloud: AWS: CloudFront, S3, Route53, IAM, Lambda, SES, SNS, API Gateway, CloudFormation (Infrastructure as Code), Config, GuardDuty, Automation, M365, Scalr (Cloud management platform), Cloud security architecture

Frameworks: NIST 800-53, CIS, ISO 27xxx, NIST CSF, CSA Cloud Control Matrix, cross-framework mappings, policy alignment, Mitre ATT&CK

Software Engineering: SQL, Java, JavaScript (Programming), PowerShell (Scripting), Security code reviews

PROFESSIONAL EXPERIENCE

Planned Career Break | Rochester, NY

Personal growth, rejuvenation and family support *10/2023 - Present*

- Sector Chief, FBI Buffalo InfraGard. Providing sector-specific security expertise and service for critical infrastructures.
- Acting as temporary primary caregiver for a family member and managing real estate investments.
- Continuing my lifelong learning, I am pursuing new certifications including FINRA SIE and AWS Solution Architect.
- Active in the InfoSec community with InfraGard, ISSA, certification maintenance and SANS Advisory Board.

Bausch Health Companies / Bausch + Lomb | Rochester, NY

IT Security Manager *11/2021-10/2023*

- Streamlined IT and Security policy lifecycle, training, and document management processes, **reducing overhead and reducing time to approval, publish, and train by 75%.**
- Acted as Incident Response Manager, coordinating response actions. Exceeded closure metrics 100% of the time.
- Partnered with external SOC to refresh IR runbooks, **reducing unnecessary incident escalations by 70%.**
- Quantified primary root cause of priority security events, generating and implementing mitigation plans.
- Executed enhancements to global IT Security communications, security intranet, LMS, document repositories and monthly newsletters **increasing workforce contact hours for security content 25% YOY.**
- Formalized the testing of workforce susceptibility and response to attack scenarios, **achieving 15% YOY reduction in employee phishing failures.** Incorporated lessons learned from incidents into future attack scenarios.
- Integrated security systems to remove manual burdens and workforce effort including SSO, AD feeds.
- **Expanded the frequency of phishing assessments by 200%, introduced attack simulations in 12 languages and achieved a 30% YOY increase in employee completion rate of assigned security awareness training**.

Security Program Manager *10/2019-11/2021*

- Initiated a comprehensive security awareness program consisting of an information hub, assessments and phishing simulations, newsletter content, training modules and a rich set of materials and activities that together increased workforce contact hours over 41%.

- Instituted program success indicators including workforce completion rates, topic comprehension, ability to detect attacks and proper reporting mechanisms **resulting in evidence of program success in all categories.**

Xerox Corporation | Rochester, NY

Cloud Security Architect *1/2016 – 5/2019*

- Initiated the cloud security design for the virtual data centers on the Amazon AWS platform, **removing platform compliance concerns for migration and engineering teams.**
- **Engineered solutions to monitor and alert on changed AWS configurations** in support of security event detection using Infrastructure as Code (CloudFormation) resulted in a repeatable functioning solution.
- Represented the security function on the cloud capabilities team at scrum milestones.

Manager, Global Information Security Strategy, Architecture and Policy *6/2008 – 5/2019*

- Transformed malware protection capabilities resulting in **improved malware prevention by 40%+ for 6,000 devices and drove $6M in potential productivity savings** related to device slowdown, re-imaging, and response costs.
- Harmonized the policies of Xerox and an acquired large business services organization **enabling minimal risk posture change for each organization while removing disparate policy sets** as a barrier to integration success.
- Enhanced the protection strategy for the corporation to address blind-spots or protection gaps resulting in the **successful deployment of secure web gateway, CASB, MFA replacement, next gen firewall, and application control** all meeting the value propositions identified in the strategy.
- Aligned security policies with industry frameworks, **reducing audit load and eliminating customer RFP concerns** associated with internal policy conformance with these frameworks.
- Introduced an adaptive enterprise-wide security architecture with associated policies and standards to set engineering and deployment expectations that **enabled the significantly accelerated development of a secure cloud consumption capabilities** in support of cloud-ready workload migrations.
- Established the security implementation and governance models for Xerox's multi-cloud data centers (Azure, AWS), providing **management and audit assurance of policy, framework, and regulatory compliance**.

Manager, Architecture, Policy and Strategic Investment Portfolio *5/2005 – 6/2008*

- Devised a methodology to review tools, contracts, and processes to identify overlap, misalignment, unused capacity, features or entitlements, and ineffective designs or configurations, resulting in the development of **9 optimization projects with cost-saving opportunities of $2M+ and 25% reduction in deployed vendor footprint**.
- Generated security priorities relative to M&A activities that address architectural gaps.
- Delivered the architecture, alignment, and sequencing of information security investments.
- Launched technology and capabilities strategy and multi-year roadmaps to document and justify the recommended actions to address internal/external threats and challenges and to show alignment to business priorities.
- Guided programs to advance roadmap initiatives, **successfully implementing 100% of priority roadmap go**als while securing funding for 85% of the entire security roadmap.

CERTIFICATIONS / CREDENTIALS

Certified Information Systems Security Professional
(CISSP) (12/2003 - Present) *Credential ID: 52179*

More Certifications:
https://www.credly.com/users/robert-hayden/badges

EDUCATION

Bachelor of Arts, Computer Science (*Magna Cum Laude)*
State University of New York at Potsdam

PUBLICATIONS

Defensible Networking and Blue Team WMI
2016, SANS Institute
PowerShell Security, Ransomware, and DevOps
2020, SANS Institute