

BENJAMIN L. TOMHAVE, MS, CISSP

9106 Omar Ct • Fairfax, VA 22031 • tomhave@secureconsulting.net • +1 703-282-8600

SENIOR SECURITY PROFESSIONAL

Progress-oriented Senior Security Professional with demonstrated success driving proactive security initiatives in a variety of organizations while participating in the development of progressive secure architecture and security policy framework solutions in direct support of business objectives.

- ♦ Track record of improving enterprise risk resiliency through secure architecture design, holistic risk management, business requirements development, and full security policy lifecycle management.
- ♦ Demonstrated competency in designing and implementing innovative security programs that promote awareness, decrease risk, and enhance the overall business.
- ♦ Adept at developing effective security policies, standards, guidelines, and procedures that blend with the corporate culture and incorporate business priorities and requirements.
- ♦ Outstanding leadership abilities; able to coordinate and direct all aspects of project-based security efforts; able to initiate and deliver security enhancements for a wide range of project-based work.
- ♦ Hands-on experience leading compliance and remediation efforts for SOX and PCI DSS, including requirements definition, design, and architecture, with specific experience in policy development, security requirements definition, and enterprise key management.
- ♦ Recognized, published author with public speaking experience, actively involved in industry committees within the American Bar Association and OWASP. Publications include the cover story in the September 2009 issue of The ISSA Journal.

CORE COMPETENCIES: Information Security Management; Secure Architecture Design and Assessment; Policy Framework Design & Development; Education, Training, and Awareness Program Development, Management, & Delivery; Secure Business Solutions; Encryption Key Management; Security Innovation

PROFESSIONAL EXPERIENCE

Independent - Various, Fairfax, VA

December 2009 to Present

Consultant / Author / Speaker

Working through a variety of sources, provided security professional services to clients. Engagements and expertise include security and risk assessment, policy development, security program development and management, encryption key management, and secure application development. Client organizations have ranged in size from small to larger.

Key Contributions:

- Developed and maintained client relationships.
- Generated business leads, created work proposals, and reached agreements.
- Executed statements of work in accordance with client requests.
- Assisted a large enterprise client with the build-out of a security program for a subsidiary.

Foreground Security, Fairfax, VA

October 2009 to December 2009

Senior Security Engineer

Team lead for implementation and project management of a complete security infrastructure upgrade for a large civilian government agency. Helped manage deployment of SIEM, NIDS, HIDS, FISMA tool, and network monitoring tool. Utilized products from Nitro Security, Trend Micro (formerly Third Brigade), Relational Security, and NetWitness.

BENJAMIN L. TOMHAVE, MS, CISSP

Key Contributions:

- Provided leadership within the project team, including documentation of weekly status reports.
- Assisted other project engineers as necessary and applicable.
- Built Windows Server 2008R2 servers to support various product rollouts.
- Analyzed network monitoring tool output and developed automated alerts and reports.

Highwinds, Phoenix, AZ

January – September 2009

Technical Director of Information Security & Compliance

Recruited to serve as the first full-time security resource for the organization. Objectives included shepherding Payment Card Industry Data Security Standard (PCI DSS) compliance efforts for one Level 2 and two Level 3 merchants. Activities included addressing policy development, data cleanup, security scanning and testing, incident response management, network security, logging and monitoring, identity and access management, training and awareness, and application security.

Key Contributions:

- Developed and executed against a roadmap to ensure PCI DSS compliance.
- Provided reactive guidance as needed for guiding management and operations to better practices.
- Developed a comprehensive roadmap for establishing and growing a comprehensive enterprise assurance management program.

BT Professional Services, Reston, Virginia

2007 – 2009

Senior Security Consultant

Recruited to serve as a regional security practice lead to assist with the development, qualification, and execution of client opportunities. Led and participated in information security consulting engagements covering the full spectrum of information security, information security management, business consulting, information assurance, risk and compliance, and governance. Developed and delivered internal training programs that enhanced internal capabilities to support and promote the security portfolio. Provided pre-sales support for security-related engagements.

Key Contributions:

- Led successful security consulting engagements that directly led to more than \$300k in repeat business.
- Introduced technical security solutions to clients that reduced their overall risk exposure while improving bottom-line performance.
- Assisted account managers and managing consultants in qualifying opportunities and writing proposals for more than \$500k in new opportunities.
- Developed and delivered internal training the directly enhanced the ability of consultants, managers, and sales to qualify and close opportunities. Topics included consulting skills, information security fundamentals, and descriptive courses around services offered (Ethical Hacking and the TrustCheck assessment tool).
- Interfaced with a multitude of vendors, including: NetWitness, Cloakware, Cyber-Ark, Veracode, Sentrigo, Venafi, StrongAuth, nCipher, RSA Security, and SafeNet/Ingrian.

AOL, LLC, Dulles, Virginia

2003 – 2007

Senior Technical Security Engineer

Recruited as an individual contributor for a joint incident response management and security assurance team. Developed the position to take lead responsibilities for information security management, including security assurance, and the training and awareness program. The success of the information security

BENJAMIN L. TOMHAVE, MS, CISSP

management program, which was later separate from incident response management, resulted in a marked decrease in security incidents and an overall improvement in enterprise risk resiliency.

Key Contributions:

- Managed and performed information security assurance activities, include the review of hundreds of development project designs directly impacting the security posture of dozens of products, primarily in the web services space.
- Managed up to ten (10) third-party consultants performing information security assurance activities in support of SOX, PCI DSS, and internal security policy compliance.
- Led the development of comprehensive assessment methodology and report templates and boilerplates, improving the effectiveness, efficiency, and consistency of information security assurance activities, and thus reducing program costs while increase risk resilience.
- Gained familiarity and expertise with information security models, frameworks, and methodologies, including COSO, CoBIT, OCTAVE, IA-CMM, OSSTMM, SSE-CMM, SIPES, and ISO 17799/27002, by integrating applicable best practices into the information security management program.
- Reduced the impact of security incidents by participating in the incident response management program by responding to incidents as an on-call responder, managing security points of contact across the enterprise and for sister divisions, and coordinating incident communication regarding specific incidents and emerging threats.
- Improved enterprise risk resilience by leading inter-departmental cooperation in securing standard system build images based on approved security standards and assessed through a formal systems vulnerability assessment process.
- Led the development of a comprehensive information security policy framework based on the ISO/IEC 27002 code of practice, working across multiple departments within the enterprise over the course of 2 years.
- Improved the efficiency and effectiveness of new hire transition and integration through the development of supporting documentation and an informal new hire mentorship program.
- Increased enterprise awareness of security concerns through the development and presentation of technical security training.
- Helped achieve compliance with the Sarbanes-Oxley Act of 2002 and make measurable progress toward PCI DSS compliance through supporting and managing assessment and remediation activities.

IP3 Inc., Saginaw, Michigan

2006 – 2007

Instructor

Delivered a podcast titled "Making Sense of Models, Frameworks, and Methodologies" based on Masters thesis work, and then deliver CISSP boot camp training both in person and online.

Key Contributions:

- Taught approximately 20 students material in support of the CISSP exam in an in-person boot camp.
- Delivered training for less than a dozen students over one CISSP module in an online format.
- Presented the results of Masters thesis research on the topic of information security models, frameworks, and methodologies.

BENJAMIN L. TOMHAVE, MS, CISSP

ITT Technical Institute, Springfield, Virginia

2006

Adjunct Professor

Delivered ITT-designed curriculum to approximately 20 post-secondary students on the fundamentals of Linux operation system administration.

Key Contributions:

- Taught approximately 20 post-secondary students how to install and configure Fedora Linux.

I_TECH Corporation, a subsidiary of First Interstate Bancsystem, Billings, Montana

2003

WAN/Security Engineer

Recruited to take over leadership of a comprehensive network security re-architecture project. Responsible for all aspects operational security within supported systems, including OS and router hardening, perimeter and internal firewalls, AV maintenance, etc.

Key Contributions:

- Saved the company approximately \$3 million on a comprehensive network security re-architecture through aggressive negotiation with vendors, by identifying alternative products of equal or superior quality, and by broadening the pool of resellers.
- Designed a multi-vendor solution representing best-in-class products, including firewalls (NetScreen and Cisco PIX), upgraded AV infrastructure (Trend Micro), VPN capabilities (NetScreen, Cisco and Secure Computing), outbound web proxy (BlueCoat) and additional network management capabilities (CiscoWorks VMS, NetScreen GlobalPRO).

Sofast Communications, Great Falls, Montana

2001 – 2002, 2003

Senior Systems Engineer

Served as lead systems administrator and secondary network administrator for national Internet Services Provider. Responsibilities included supporting dial-up, broadband and DSL customers for connectivity, email and web hosting. Also provided systems administration to systems used for web hosting and portal services.

Key Contributions:

- Instrumental in designing, building, implementing, and maintaining clustered and high-availability systems significantly increasing uptime, availability, and risk resilience.
- Decreased enterprise risk exposure through deployment of anti-virus and spam filtering solutions, hardening servers, redesigning secure network architecture, designing and implementing a data backup solution, designing and implementing security policies and procedures, and designing and implementing a productized broadband management solution.

ICSA Labs, Mechanicsburg, Pennsylvania

2002

Network Security Lab Analyst

Hired to conduct comprehensive security testing and certification of firewall products, coordinating the resolution of issues with vendors. Testing was conducted in a process-oriented, scientific environment and involved use of common penetration assessment tools, including Nessus, CyberCop, Nmap, hping, nemesi and tcpdump, among others.

Key Contributions:

- Certified approximately a half dozen firewall products based on the ICSA Labs Firewall Certification Criteria.

BENJAMIN L. TOMHAVE, MS, CISSP

Wells Fargo Services Corporation, Minneapolis, Minnesota

2000 – 2001

Information Security Analyst 4

Recruited to provide technical project management to a team of 30+ engineers throughout the continental United States. Responsibilities included design review, workflow management, special project leadership, and point-of-contact for regular work requests.

Key Contributions:

- Reduced enterprise risk exposure, increased operation efficiency, and supported time-critical business projects through the support of approximately 500 firewall, web and application servers, based on Sun Solaris, Compaq Tru64, and Windows NT.

BORN Information Services, Minnetonka, Minnesota

2000

Senior Security Consultant

Recruited to help co-lead a new information security consulting practice that provided clients across multiple industries with technical professional services. Offered services included networking, information security and server administration. Practice development included development of a unique methodology for implementing an information security program. Responsibilities included provided pre-sales support to account executives as well as assisting with the identification, development, and qualification of sales leads.

Key Contributions:

- Represented and promoted the company by speaking at a regional security conference, presenting on the topic of strategic, holistic security, congruent with our unique methodology.
- Supported a client's preliminary deployment of Windows 2000 by developing security policies governing early adoption.
- Helped clients reduce their risk exposure through the completion of critical design reviews, security assessments of critical infrastructure, and providing prescriptive recommendations for remediation identified vulnerabilities,

Ernst & Young LLP, Minneapolis, Minnesota

1999 – 2000

Senior Security Consultant

Recruited to perform and lead IT audits, including documenting and providing expert analysis of system and network security. Audit and security assessment findings, sometimes based on SAS 70, included business-justified recommendations for remediation.

Key Contributions:

- Enhanced the value of clients' annual financial audits by evaluating the security of key financial systems.
- Notable assignments included: National Computer Systems, Fortis Inc., Target Corp., and American Express Financial Advisors.

International Network Services, Chicago, Illinois & Minneapolis, Minnesota

1998 – 1999

Associate Network Systems Engineer

Provided network professional services to a variety of clients in the Chicago, Illinois, and Minneapolis, Minnesota, metropolitan areas. Services included troubleshooting, network design and implementation, and fulfilling numerous other network administration functions on behalf of customers.

Key Contributions:

- Assisted in the operation and maintenance of a Network Operation Center for a major insurance provider.

BENJAMIN L. TOMHAVE, MS, CISSP

- Facilitated the smooth transition to a new office location by serving as the point of contact for move issues and managing design changes and trouble requests.
- Enhanced internal technical training capabilities by designing and implementing a reconfigurable networked classroom, including installation of standardized cabling, Ethernet hubs, Windows NT 4.0 Server with DHCP, and Cisco PIX firewall.

EDUCATION AND CREDENTIALS

Master of Science Degree in Information Security Management

THE GEORGE WASHINGTON UNIVERSITY – Washington, District of Columbia

Bachelor of Arts Degree in Computer Science

LUTHER COLLEGE – Decorah, Iowa

Professional Certifications

CISSP – Certified Information Systems Security Professional #46697

NSA IAM – INFOSEC Assessment Methodology Certified

NSA IEM – INFOSEC Evaluation Methodology Certified

NSTISSI 4011, 4012, 4013, and 4015 Certified

Professional Training and Conferences

BlackHat USA Conference 2009

Security BSides Las Vegas (2009), San Francisco (2010), Austin (2010)

RSA Conference USA 2008, 2009, 2010

ISACA Information Security Management Conference 2005, 2006

NSA INFOSEC Assessment Methodology (IAM) Training (2006)

NSA INFOSEC Evaluation Methodology (IEM) Training (2006)

BSi ISO 17799 Implementation (2005)

“Facilitative Leadership” by Interaction Associates (2007)

“Managing Conflict” by Ridge Associates (2005)

“Intercultural Training: Working with Indian Nationals” by Prudential Financial (2007)

SANS Track 8: System Forensics, Investigations, and Response (2004)

PROFESSIONAL AFFILIATIONS

Member – American Bar Association Information Security Committee

Member – American Bar Association eDiscovery and Digital Evidence Committee

Contributing Author / Core Guide (Practical Security) – Truth to Power Association

Member – Open Web Application Security Program (OWASP)

Member – Information Systems Security Association

Member – IEEE Computer Society

Inactive Member – InfraGard

Former Member – OASIS EKMI and KMIP Technical Committees

Former Member – Information Systems Audit and Control Association