BEN TOMHAVE, MS, CISSP

Herndon, VA • tomhave@secureconsulting.net • +1 703-282-8600

TECHNICAL SECURITY ARCHITECT/LEADER

I am a well-regarded, highly experienced technical security professional with over 20 years of IT industry experience. As a security architect, I am a generalist who has served in nearly all types of security roles ranging from audit and assessment to incident response and forensics to security architecture and DevSecOps. I am currently seeking technical security leadership opportunities such as a security architect, security strategist, researcher, or similar. My most recent experiences include work in IAM and MFA, cloud security, container security, DevSecOps and application security practices, data security, security management, GRC and derivative use cases, policies and KPIs, vulnerability and patch management, system and network hardening, and overall enterprise security architecture.

CORE COMPETENCIES: Security architecture design and assessment (legacy and cloud); application security program management and DevSecOps; data security, data encryption, and enterprise key management; security management; identity and access management (IAM) strategy and architecture; governance, risk management, and compliance (GRC); security education, training, and awareness program development, management, and delivery, including a focus on behavioral information security; security product strategy and market analysis; analyst relations management.

PROFESSIONAL EXPERIENCE

Falcon's View Consulting, LLC   June 2015 to present
Principal

> As a solo consulting practice, providing cybersecurity professional services to multiple industries. Project work includes content development, security architecture, security product strategy and development, high-level security assessment and advisory services, specialized security training, and DevOps/DevSecOps architecture. Engagements include technical security ghost writing, program assessment based on NIST CSF, security advisory services on topics including risk management and container security, and general enterprise security architecture.

Pearson, Centennial, CO (remote)   September 2017 to April 2018
Manager, Security Engineering and Architecture

> Providing front-line management of a team of security engineers and architects responsible for identity and access management (IAM), multi-factor authentication (MFA), cloud security, container security, and data security (including encryption and certificate management). Provided technical leadership for the IAM and MFA initiative, including support for solution design and program communications. Technologies in-scope include ForgeRock, AWS, Cloud Custodian, CloudCheckr, CyberArk, and Vormetric.

New Context, San Francisco, CA (remote)   June 2016 to July 2017
Principal Security Scientist

> Served in a variable role performing research, product management of in-house development projects, and conducting business development. Efforts included creation of materials around the "Lean Security" methodology, development of presentations for conferences, and writing copy for sales collateral, blog posts, and byline articles. New Context has a focus on secure DevOps services and product development.

Ellucian, Fairfax, VA   October 2015 to June 2016
Manager, Information Security Architecture

> Evaluated current security processes, tools, and practices as a member of the information security team reporting directly to the CISO. Charged with evaluating the effectiveness of current solutions and identifying gaps in security protection. Developed a comprehensive security architecture framework to evaluate and manage security architecture strategy for both traditional on-premises and cloud environments. Worked with vendors and cross-organizationally to identify, evaluate, and test (pilot) solutions. Technologies evaluated

included data loss prevention (DLP), endpoint detection and response (EDR), traditional endpoint security, email security solutions (on-premises and Office 365), enterprise mobility management (EMM), network security tools and capabilities, identity and access management tools and capabilities, application security practices, cloud security tools (such as for AWS) and container (Docker) security tools. Technologies in-scope included AWS, Okta, Digital Guardian, IBM BigFix, Symantec EPP, Zscaler, Microsoft Adallom, FireEye, Splunk, Ansible, Rapid7, Tenable, CloudCheckr, StackRox, Jump Cloud, among many others.

K12, Inc., Herndon, VA   March 2015 to October 2015
Security Architect

As a member of the enterprise architecture team, charged with broad responsibilities to inject security practices into the overall application stack. Reviewed overall environment and developed an incremental roadmap for addressing critical gaps and charting a progressive course to more effective enterprise security over time. Included collaborating with the team driving a DevOps initiative, as well as initiating changes to implement and leverage security operations automation.

Gartner, Inc., Arlington, VA (remote)   June 2013 to March 2015
Research Director

As a member of the Security & Risk Management Strategies team within Gartner for Technical Professionals, I conducted research into topics including risk management, security programs, security planning and management, application security, DLP, and SharePoint security. Additionally, I contributed content as a speaker at several Gartner and non-Gartner events and webinars, as well as delivering advisory services to clients and providing direct support to the sales team, both virtually and in-person, in multiple regions.

LockPath, Inc., Overland Park, KS (remote)   August 2011 to May 2013
Principal Consultant

Hired to perform numerous duties as directed, including:

- **Professional Services:** Delivered consulting services supporting customer implementations of the Keylight platform and suite of applications.
- **Customer Training:** Developed and delivered comprehensive customer training across all LockPath products. Curriculum was tailored to multiple learner styles, including use of visual, auditory, and tactile techniques.
- **Writing:** Produced multiple written pieces, including byline articles and white papers, ranging in length from a few hundred to a couple thousand words.
- **Public Speaking:** Delivered presentations at several security-related conferences, including the RSA USA Conference, Secure360, the Rocky Mountain Information Security Conference (RMISC), the ISC[2] Security Congress, and the ISSA International Conference.
- **Partner Enablement:** Worked with partners to ensure that they were well supported and able to fulfill their mission requirements as pertained to delivering services related to LockPath products.
- **Other Duties As Assigned:** Completed other activities as assigned, including performing market analysis, providing input on product design discussions, and assisting with security policy development.

Gemini Security Solutions, Chantilly, VA   May 2010 to August 2011
Sr. Security Analyst, Business Development Management

Experienced consultant hired to develop business relationships and grow client-base. Contributed to billable projects, development of proposals and statements of work, and promotion of the company. Increased company profile through writing and speaking engagements. Provided subject matter expertise in core competencies for use on client projects, internal consulting, contributing to industry groups and initiatives, and overall knowledge development and transfer.

BENJAMIN L. TOMHAVE, MS, CISSP

Independent - Various, Fairfax, VA   December 2009 to May 2010
Consultant / Author / Speaker

> Worked through a variety of sources to provide 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.

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.

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.

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.

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 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.

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.

BENJAMIN TOMHAVE, MS, CISSP

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.

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, nemesis and tcpdump, among others.

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.

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.

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.

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.

EDUCATION AND CREDENTIALS

Master of Science Degree in Engineering Management
Concentration: 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

BENJAMIN L. TOMHAVE, MS, CISSP

Expired / Deprecated
Certified FAIR Basic Analyst and FAIR Certified Trainer
HITRUST Certified CSF Practitioner (CCSFP) #55570
NSA IAM & IEM Certified
NSTISSI 4011, 4012, 4013, and 4015

Papers & Publications
Please See: http://secureconsulting.net/papers-publications.html

PROFESSIONAL TRAINING AND CONFERENCES

AWS: Cloud Practitioner Essentials, Security Fundamentals Online, Well-Architected Training
BJ Fogg Behavior Design Boot Camp (2017)
RSA Conference USA 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017
Rocky Mountain Information Security Conference 2011, 2012, 2013, 2014, 2015, 2016, 2017
ISSA International Conference 2010, 2011, 2012, 2017
MISTI InfoSec World (2017), Cloud Security World (2016), Cybersecurity World (2015)
Secure360 2011, 2012, 2013
ISC² Security Congress 2012
Society of Information Risk Analysts Conference (SIRAcon) 2012
NESCO Town Hall: Security Risk Management Practices for Electric Utilities (May 2012)
OWASP AppSec USA (2010), AppSec DC (2010), Summit (2011)
Security B-Sides – Attendee: Las Vegas (2009, 2015), San Francisco (2010)
Security B-Sides – Austin (Organizer/Co-Founder, 2010, 2011), Ottawa (2010)
EnergySec Summit 2010
Cyber Information Security Conference (CIScon) 2009
BlackHat USA Conference 2009
ISACA Information Security Management Conference 2005, 2006
NRA Range Safety Officer (2013)
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

Senior Member – Information Systems Security Association

Previous Affiliations
Former Member – American Bar Association Information Security Committee
Former Member – American Bar Association eDiscovery and Digital Evidence Committee
Former Member – OASIS EKMI and KMIP Technical Committees
Former Member – Open Web Application Security Program (OWASP) and OWASP Global Conferences Committee
Former Board Member – OWASP Northern Virginia (NoVA) Chapter
Former Contributing Author / Core Guide (Practical Security) – Truth to Power Association
Former Member – SANS Technology Institute Strategic Planning Advisory Committee
Former Board Member – Society of Information Risk Analysts
Former Co-Chair – American Bar Association Information Security Committee