Resume of Siva Ram (CISA)

Email: siva.x.ram@gmail.com   Website: www.maravis.com

I currently manage cyber security, compliance and fraud risk for globally deployed corporate banking platforms. Previously, I managed a global information security team that provided architecture/security design consulting and performed threat modeling/penetration testing on globally deployed applications.

I started and managed the application security/PCI compliance practices at two organizations prior to joining HSBC and was a co-founder of a security services company, based in California. I have interacted extensively with clients (senior management and technical) and managed vendor and client relationships.

My experience includes enterprise application development and performing threat modeling, penetration tests and vulnerability assessments, developing secure coding guidelines and delivering security training in addition to performing PCI-DSS and PA-DSS assessments.

I am a Certified Information Systems Auditor (CISA), an ex-PCI Qualified Security Assessor (PCI-QSA), ex-Payment Application QSA (PA-QSA) and an IBM Certified Specialist (IBM Rational AppScan).

Professional Experience

Head, Cyber Security& Fraud Risk, GLCM Digital Channels,

HSBC Bank Plc.

September 2014 – Present

My role is to block cyber-attacks/fraud earlier in the cyber kill chain, by planning and delivering the best possible attack detection and prevention capabilities. To this end, I focus on defense in depth, with multiple overlapping controls and building security into infrastructure and applications from the beginning.

Responsibilities

- Develop and implement cyber security and fraud management strategy for online and mobile channels for platforms that did _USD12Trillion_ in transactions in each of the last 4 years
- Advise senior management on the bank's security posture
- Manage privacy/compliance/security related regulatory requirements in 50+ countries for globally available platforms
- Ensure appropriate security/fraud incident handling/response
- Identify and prioritize security and fraud controls to be implemented, balancing budget and security requirements
- Provide training to customers and internal technology teams on cyber security and fraud controls

Achievements

- Deployed a security solution (identifying vendors, PoCs, finalizing selection, procurement, implementation), resulting in enhanced capabilities that have resulted in reducing phishing and malware related fraud by 70%
- Implemented "_shift left_" security model, resulting in a significant reduction in the number and severity of new security risks. This resulted in the closure of all High and most Medium security issues.
- Created a cyber security risk matrix to identify risks and existing controls based on the NIST Cyber Security Framework

- Drove an incremental roll out of technical and procedural controls to detect, prevent and respond to cyber-attacks resulting in tangible improvements in the security posture
- Conducted cyber-attack simulations for the security response teams and business response teams. Fed back lessons learned into training to improve future response.
- Provided significant input to multiple group security policies and standards.
- Drove multiple regulatory compliance projects successfully under tight deadlines.
- Currently driving several initiatives in the security and fraud space: Biometrics, Risk Based Authentication, Anomaly Detection, User Behavior Analysis, Network enhancements, Mobile Security
- Delivered presentations on cyber security and fraud risk to internal staff and customers.

Manager, Global Information Security, HSBC Bank Plc.

June 2012 – August 2014

I managed a global team of Security Consultants that worked with software development teams to ensure security risk was managed appropriately for all group-wide applications. This entailed understanding the functionality provided by applications, reviewing architecture and design, identifying the data that is handled, performing threat modeling, evaluating the risks and recommending mitigating controls/solutions.

I was responsible for the security of several core banking applications that handle trillions of dollars in transactions every year and customer/employee facing Mobile applications. A key task was to explain the security risks to the business, enabling them to make informed decisions on mitigation and risk acceptance. This required finding the right balance between the need for security and functionality.

Managerial responsibilities included supervising other security engineers, ensuring risk assessments are delivered on time and mentoring junior engineers.

Other Responsibilities

- Performed security reviews on internet and mobile applications (architecture and design).
- Provided security recommendations for architecture and design of products.
- Created/Reviewed security policies and procedures.
- Increased efficiency of risk assessment engagements.
- Researched new attack vectors and mitigating solutions.
- Provided guidance to regional security teams.
- Provided analysis/opinions to senior management/project teams on "hard-to-solve" problems that pop up from time to time.
- Engaged with development teams and promote secure design/development early in the SDLC.

Achievements

- Contributed to group-wide security policies, standards and processes.
- Championed the adoption of industry standard encryption algorithms across the group resulting in several regions around the world upgrading to stronger algorithms.
- Implemented process that resulted in improving on-time completion of security review engagements from about 25% to about 98% within one year.
- Championed the need for early engagement with development teams and providing security input into design, resulting in a significant reduction in the number of issues raised during coding and deployment stages.
- Cross-trained security consultants across application streams resulting in increased productivity.
- Contributed to expansion of world-wide regional security teams by developing screening processes and interviewing candidates.

- Standardized risk ratings across the security teams to ensure consistent response to risk.
- Created security patterns that enabled better and effective utilization of valuable security consultants.

Manager – Security Services and Compliance, SPIguard Security Solutions, Inc.

December 2009 – May 2012

I managed security services and the PCI DSS/PA DSS compliance practices at SPIguard, which includes managing the consulting team, services and delivery for clients. My role required close interaction with both technical and management personnel at clients through all stages of the engagement.

In addition to performing PCI assessments and PA DSS validations along with associated services, I also managed the development of several online tools that help clients obtain and maintain PCI compliance.

Achievements

- Added new security services (Threat modeling/Penetration testing/Security Risk Assessments) to the company's portfolio.
- Doubled revenues by streamlining processes, increasing client satisfaction and response times.
- Developed processes for performing PCI and PA DSS compliance verification efficiently.
- Created and delivered PCI DSS and PA DSS awareness courses.
- Designed online tools for managing ongoing PCI compliance management.
- Delivered presentations on security topics at industry events.

Co-Founder/VP Security Services, AppSec Consulting, Inc.

May 2005 — December 2009

My primary responsibility was managing engagements and ensuring on-time/on-budget service delivery. I was also responsible for identifying what services to deliver and create processes and procedures for successful delivery of those services. Another significant responsibility was managing the training practice; developing and delivering security courses for web application developers and QA engineers. I designed and developed an online platform to deliver training that is still in use.

I also performed application risk assessments, penetration tests and security certifications in addition to PCI DSS assessments.

Achievements

- Set up the application security practice (primary business).
- Set up and managed the company's infrastructure for the first 4 years of the company's existence.
- Identified and implemented cost saving measures which were very important to a self-funded startup company.
- Set up and managed training services. Developed and delivered training courses for clients. Managed the conversion of all courses to online format for scalability.
- Designed and developed a Learning Management System (LMS) to host online training courses. Features included user tracking and reporting, bookmarking, auto-resume and automated registrations.

- Designed and managed development of an online application that enabled clients to verify skills of contractors and employees. Features included randomized questions and customizable tests.
- Developed and refined processes for application security assessment engagements.

Sr. Security Consultant, Port2Web/SiegeWorks

December 2001 — April 2005 (3 years 5 months)

I contributed significantly to starting and building the application security practice at SiegeWorks. My responsibilities included performing penetration tests and vulnerability assessments for various Fortune500 clients. Since the application security practice was new at SiegeWorks, I also created all related procedures and checklists. Many of my engagements involved creating platform specific secure coding guidelines and standards. I also developed and delivered courses on secure web application development for developers. Part of my responsibilities involved identifying security tools and evaluating them.

Achievements

- Created procedures and processes associated with performing penetration testing and vulnerability assessments.
- Created checklists for providing security certifications to clients' software.
- Standardized threat modeling and vulnerability rating methods to promote consistency.
- Designed an online asset management system and oversaw development.
- Spoke on web application security at various industry events.

Sr. Software Engineer, ITC, IT Solutions

July 1996 — December 2001 (5 years 6 months)

I developed client-server and web applications on various platforms for international clients. The applications included online credit card approval and credit card monitoring systems, order entry and asset management systems. I performed code-reviews to identify performance bottlenecks and security issues. I also helped develop a hotel management system that was sold as a product.

Education

I have a Master's degree in Computer Applications and a Bachelor's degree in Computer Science.

Interests

My interests include security, technology, electronics, computers and software. I am also interested in martial arts and am training in Aikido, a Japanese martial art.