

CAREER OBJECTIVE:

Highly motivated and performance driven Information Security Subject Matter Expert with more than fifteen years of successful experience in Information Assurance, Risk Management and Compliance is looking for a leadership position in a progressive organization where he can utilize his skills and knowledge in discovering the organization security needs, designing and developing, with economy and elegance, an information security infrastructure, architecture and systems that ensures an appropriate level of **confidentiality, integrity, availability, authentication, and non-repudiation** that is based upon valid **risk management** decisions, and ensuring the entire organization can securely resist the forces to which it may be subjected and meet the organization's business goals and objectives.

SKILLS SUMMARY

Information Technology Risk Management

- Proven experience defining governance principals, policies, procedures and leading business /or IT transformation initiatives to support business strategic direction;
- Practical Knowledge and experience of Information Assurance, Audit and Management standards, IT Governance frameworks and best practices **CobIT 4.1, ISO/IEC 27002/27001 | 13335, ITILv3, NIST, CC- Common Criteria ISO/IEC 15408, CBK, OSSTMM 2.0, OWASP** methodologies, and manuals;
- Strong in business security/privacy related legislation: **PIPEDA, PHIPA, FIPPA, HIPAA Sarbanes-Oxley (SOX 404), Bill 198, PCI-DSS;**
- Solid knowledge and experience in Risk Analysis (**HTRA**), Business Impact Analysis (**BIA**), Privacy Impact Analysis (**PIA**), Information Systems Audit, Vulnerability assessment and Penetration Testing;
- Ability to analyze business needs and translate them into requirements defined in policies and standards including communication of these needs to all stakeholders and executives;
- Strong understanding of security operations challenges including key performance monitoring and audit.

Security Architecture, Engineering and Project Management

- Strong understanding of security models and mechanisms, experience in determination of security vulnerabilities, weaknesses, threats and related risks that exists within an Enterprise including IT Infrastructure or business processes;
- More than 10 years of experience in Project Manager Competency Development framework including strategic planning, organizing, and managing resources to bring the successful completion of project goals. **PMBOK & PRINCE2** knowledge areas and methodologies to achieve an effective project management;
- Familiar with Enterprise architecture principles and frameworks(**TOGAF, IATF, GRC**) and models to ensure effective Information Security governance and risk management;
- Capable of effectively build strong relationships with executives, business and IT management;
- Experienced in transforming and negotiating business, privacy and legal requirements into security and technical specifications;
- Knowledge of leading information security vendors and products, multiple information security technologies and their strengths and shortcomings;
- Strong ability to see the big picture, prioritize and work successfully within an Enterprise environment.

Personal Qualities

- Result-oriented, able to lead, manage and coordinate workflow independently and within a team, effectively manage tasks, time and resources;
- Responsible, sociable, accurate, easily adaptable to new systems and tools;
- Clearly express technical information and concepts to a non-technical audience and vice versa;
- Opened for constructive dialogue and suggestions.

CAREER HISTORY

November 2008 -present

Toronto Star & Metroland Media Group

Torstar Corporation is a broadly based media company listed on the Toronto Stock Exchange (TS.B) including Metroland Media Group, publishers of community and > 140 daily newspapers in Ontario; and Harlequin Enterprises.

Information Security, Risk Management and Compliance Consultant

Delivered Results:

Planned and executed strategies to ensure effective oversight of information security program by applying complex Information Security Architecture and system engineering principles;

- Established the facility's first Enterprise Security Program and Information Assurance Framework and created best practices to resolve critical security issues;
- Responsible for all aspects of information assurance within the enterprise including risk analysis, policies, standards and procedures development and enforcement preventing unauthorized access and usage of the Torstar sensitive assets which may result in disclosure, destruction or removal of critical data or interruption of the TORSTAR business processes;
- Serve as the in house security subject matter expert to project teams for new architecture and design initiatives including working with project managers, peers and business unit management to ensure that information security is not compromised throughout the change management process;
- Advises on the planning, budgeting, direction, co-ordination and evaluation of the program to meet the requirements of the Corporate IT Security Strategy and plans;
- Information Security and Compliance Working Committee (**ISCWC** chairmen); Information Security Steering Committee (**ISSC** Member)
- Activities include Bil198, PCI-DSS compliance, enterprise security governance and strategic planning with strong emphasis on security risk management, education & awareness, automated security control acquisition and implementation, security management dashboard development, and end-user security training programs;
- Established and maintained ongoing liaison with Corporate Security and senior executives and program management to ensure cooperative working relationships on all security planning and implementation;
- Conducted sophisticated Threat Risk Assessments of core infrastructure and analyzed current state of information security including high-level security reviews to very tightly focused examinations of specific security concerns;
- Collaborated with other Stakeholders to identify opportunities for delivering effective business solutions and improve performance of the business outcomes;
- Improved methods, tools and techniques to establish best practices, process efficiencies and to surpass service level agreement measurements;

Projects:

- PCI DSS compliance program
- Information Security, Risk Management and Compliance Program

IT Infrastructure Security Architect

Provided specialized leadership, expertise, and coordination in development and implementation of the Corporate Network and systems Security Architecture and design to support the Torstar mission critical systems;

- Responsible for designing and implementing solutions that combine information security best practices, methodologies, processes and technologies that ensure compliance to the Corporate Information Security Policy, SOX, PCI DSS and other regulatory requirements;
- Researched and evaluated many security tools such as firewalls, IPS/IPS, SEIM, automated security management products, application firewalls and vulnerability scanners;
- Successfully implemented the Enterprise wide Network Access Control system, Corporate Edge Firewalls, Wireless Networks and Access Control system from the concept to detailed technical design and specifications including testing, and implementation plan;

- Performed internal and external penetration tests (network and application testing,) and managed regular third-party penetration testing studies, including network, application and social engineering tests
- Direct a 6-person IT Security and Compliance Team responsible for the safeguarding of IT assets (120 remote sites; 3 Data Centers, 1040 servers, > 9,000 users for the Digital Media organization across Canada;
- Monitored intrusion detection and prevention systems, scans and attacks, analyzed and resolved security breaches and vulnerability issues;

Projects:

- 4 years IT Infrastructure Stabilization Plan
- PCI compliance program
- Unified Treat Management Project (NAC,SEIM, ASM, IDS/IPS)

June, 2008 – November 2008 (contract)

Toronto Transit Commission (TTC)

The TTC is owned and operated by the City of Toronto and is responsible for the consolidation, co-ordination and planning of all forms of local passenger transportation within the urban area of Toronto.

IT Security Consultant

Provided assistance to Project Management Group with security issues directly related to requirements and deliverables of TTC projects and recommend remedial actions for risk reduction to acceptable level;

- Improved efficiency and effectiveness of information security governance and security architecture. Instituted security policies, standards, metrics, and guidelines aligned with the business requirements
- Provide analysis and consulting regarding threats, vulnerabilities, and privacy to ensure that new and existing systems, products and services are planned, implemented, operated and maintained to suitably safeguard both the TTC and clients` information
- Analyzed numbers of projects and proposed solutions architectures to identify potential threats and vulnerabilities
- Created remediation action plan that enhance the security of solutions and business processes
- Conducted Information Assurance Gap Analysis, revised existed and created new IT security policies and standards within defined framework in accordance with ISO17799 and NIST 800 series documents.
- Reviewed numbers of Threat Risk Assessments and Privacy Impact Analysis reports
- Maintained management reporting system environment.

Projects:

- **Customer Service Disruption Notification Service:** Performed security testing to ensure systems will contain necessary security controls required to protect information assets and resources from unauthorized access.
- **Next Train Arrival System:** Involved in Threat/Risk Assessment, recommend remedial actions for risk reduction.
- **Internet Trip Planning:** Performed security assessments of detailed design requirements, RFP, Implementation and Test Plans on the infrastructure and system components during pre-production and production stages.

February, 2004 to June 2008

Bendix Foreign Exchange

Currency-related products and services including Electronic Funds Transfer, Money Orders, Bank Drafts, Notary Services, Collection Services, Correspondent Services, Euro-Dollar Transactions, Money Transfer Anywhere, Blocked Accounts.

Manager, Information Security

Founded and led all aspects of the Corporate IT including Security governance and strategic planning with strong emphasis on security risk management, education & awareness, dashboard metrics, project management, incident investigations and associated management reporting to various levels of the organization

- Managed group of highly experienced information technology professionals. Developed and maintained appropriate staffing levels, resources and budget, through deliberate organization and planning.
- Defined architectures and solutions based on defense-in-depth concept to satisfy system requirements and support business needs and objectives

- Provided leadership working with corporate project teams in areas such as Mission Critical threat/risk assessments, disaster recovery plans and business continuity plans. Conducted numbers of Threat Risk assessments and Privacy Impact Assessments and appropriate level of security controls have been established including policies, standards, procedures
- Defined overall tactics and strategy for corporate information security program for short, mid, and long term
- Implemented Role Based Access Control (RBAC) through authentication, authorization and accounting process to preserve and protect the confidentiality, integrity, and availability of information, systems, and resources
- Acted as a subject matter expert for solution delivery in the areas of Firewalls, IDS, VPN, and Authentication
- Implemented Disaster Recovery plans to protect IT Assets against future and operational interruptions
- Supervised the process of new application development and implementation from the security perspective
- Conducted regular vulnerability assessment to ensure appropriate protection has been utilized for the systems
- Provided guidance the Patch and Configuration Change Management
- Worked with the different Business groups to ensure all requirements are met
- Provided training for the company's Management and Users
- Established working relationships with vendor partners.

September, 2001 to December 2003**EUROVENT**

European Association of Air Handling Engineering and Manufacturing

Director IT

Ascertained business requirements of the entire organization and creating a strategy to implement a technology infrastructure to meet these needs. Responsibilities include the overall management of all information services, data processing, client support and security functions

- Lead development and implementation of the information security management system, with particular emphasis on developing, implementing and effectively managing the information security risk management function
- Prepared various research, evaluation and statistical reports for client management including Enterprise statistical security incident reports, management reviews and technology assessments
- Vulnerability assessment and security evaluations within the network and server infrastructure as well as working to build up new security products and improving flaws in current systems
- Delivered IT strategic plans, systems development and network infrastructure solutions
- Reviewed general support system and major application controls to determine gaps and identify technical, operational, and procedural refinements
- Implemented SSH, VPN solution to ensure data confidentiality and integrity. Implemented Cisco Firewall and router package filtering technology
- Direct supervision, technical coaching and monitoring of two System Administrators and Data Manager. Built and maintained professional relationships with clients and vendors.

September 1999 to August, 2001**North-West Timber Company**

The large-scale producer of paper and paper stationery. More than 400 items of productions heading the vertically-integrated group of the industrial enterprises, consisting of Neman Pulp-and-Paper Mill (Kaliningrad area), Kamennogorsk Offset Paper Mill (Leningrad area), Velsk Glued Timber Structures Mill (Arkhangelsk area) and the group "Basis".

Sr. System Engineer

Design implementation and maintenance of IT infrastructure (over 5000 employees). Provided leadership for various security-related projects and training to end users.

1996 – 1999**System Engineer / LENIMS**

Responsible for design, implementation, and management of complex network infrastructure and servers in the production, development and hosted application environments.

1985 – 1993 Air Force / Pilot – Engineer**TECHNOLOGIES EXPERIENCE SUMMARY**

Security technologies: Defense-in-depth concept , Firewalling , Network Access Control (NAC) and user provisioning, System hardening, Intrusion Detection and Prevention, SEIM, Automated security management , vulnerability and penetration testing, content filtering and forensic analysis

Platforms: MS: DOS, NT3.51/4.0/2000/2003, XP; Unix: HP-UX 11, Solaris 8/9, SCO, BSD; Linux: RH, CentOS

Network Protocols: TCP/IP, UDP, ICMP, SNMP, FTP, TFTP, SFTP, FTPS, HTTP, HTTPS, SSL, TELNET, SSH, LDAP IPX/SPX, NetBEUI, SMTP, POP3, IMAP, DNS, DHCP, WINS, RIP, IGRP, EIGRP, OSPF, ISIS, BGP

Network technologies: Routing, Firewalling, LAN, WAN,VNS, VPN, VLAN, NAT, PAT, QoS, Wireless

Encryption and authentication: IPsec, L2TP, PAP, CHAP, WPA2, TKIP, DES/3DES, AES, SHA, MD-5, PKI, RSA, PGP, 802.11i, 802.1x, EAP, PEAP

Databases and Servers: SQL, Oracle, Cisco ACS, MS IAS, RADIUS, TACACS+ , VMware ESX, WSUS, SMS, MOM, WEB, Exchange, Veritas, Websense, Citrix

TOOLS: Nessus, Qualys, MBSA, GFI LANguard, CA SPECTRUM, NETWORK INSTRUMENTS –OBSERVER, MangeEngine, MRTG, PRTG, Nagios, Snoopy, Nsauditor, Solarwinds , Encase, Hyena, DameWare, Knoppix, Kismet, Iperf, Cybercop, Metasploit, IISXploit, WebInspect, SuperScan, N-Stalker Web Application Security, LOpht, Brutus, Nmap, Netcat, Ethereal, Retina, Iris, Cain, Ciscoworks, Snort, Triwire HIDS, McAfee, Norton, Kaspersky, Acronis, Communications software, Access, Microsoft Office

Appliances: CISCO: Pix 401/515/525, ASA 5505/5520/5540, IDS/IPS 42035/ Netranger, MARS V6, Routers 7200/2800/2600 Switches 6500/3400/2950, VPN 3000, Enterasys: C3/B3/N7Matrix, IDS Dragon 7, DSCC, Netsight Console, 4110 Wireless Gateways, HiPath APs, HiGuard Wireless IDS/IPS, NAC Gateways, SIEM, Iron Port, F5 BiG IP, CITRIX NetScaler, Gigastore, RiverBed, SUN,DELL Blades

CERTIFICATIONS

CISM (Certified Information Security Manager) -2009

CISA (Certified Information Systems Auditor) -2008

CISSP (Certified Information Systems Security Professional) - 2007

ISSAP (Information Systems Security Architecture Professional) - 2010

CCSP (Cisco Certified Security Professional) -2006

CCNP (Cisco Certified Networking Professional)-2007

CCNA (Cisco Certified Network Associate)-2005

CCSE (CheckPoint Security Expert NGX)-2008

MCSE: Security (Microsoft Certified System Engineer)-2007

CompTIA Security +

CNSS 4011 INFOSEC Certification by NSA (National Security Agency) / CNSS (Committee on National Security Systems)

AMBCI (Associate Member of the Business Continuity Institute)

CISSP-ISSEP (in process)

EDUCATION

1999-2001 **Saint-Petersburg Polytechnic University**, B.Sc., System Engineer for the specialty “System Software Development”

1999- 2001 **Saint-Petersburg Polytechnic University**, Diploma in “Personal computer and local networks”

1984-1989 **Yeisk Air Force Military School**, B.Sc., Pilot-Engineer

COURSES AND TRAINING ATTENDANCE

Gartner: Security & Risk Management Summit, June 21-23, 2010 (Washington, DC)

VISA: "PCI-DSS Training Seminar" June 15-17, '09 (Toronto)

Enterasys: "Network Access Control Architecture and Design" November 23-25, 2009 (Toronto)

Skybox Security: "Protect the Critical Infrastructure using Firewall Compliance & Network Analysis" Dec., '08 '09

(ISC) 2: "Proving Ground - The Many Flavors of Authentication" November 19, '09

ISACA: "Harmonizing Security and Compliance", June 23, '09

PGP: "Closing the Barn Door - Keeping Your Data from Hopping Fences", June 16, '09

Qualys: "Web Application Security: Intelligent Choices", May 22, '09

Symantec: "Working Intelligently and Protecting Your Windows Infrastructure", April 29, '09

Tripwire: "IT Audit: Challenges and Opportunities", April 28, '09

Symantec: "Working Intelligently and Protecting Your Windows Infrastructure" – April 29, '09

Open Group: "IT Risk Management, overview of Open Group Risk Taxonomy Standard" - April 8, '09

ORACLE-ISACA: "Optimizing Your Enterprise Governance Risk and Compliance Program"- Feb24 '09

CA- IBM-(ISC) 2 "Automation and Compliance - A Partnership for Success" – Jan 20, '09

HP-(ISC) 2: "Application Security. PCI DSS requirements" – Dec 09, '08

IBM: "Building a successful security strategy" (Ziff Davis Enterprise Virtual Tradeshow) – Sept 17, '08

VeriSign: "Crime Story: Bad Guys and what you can do to protect yourself from them", Aug 19, '08

(ISC) 2: "Logging and Reporting: A Foundation for Your Security Infrastructure", Jul 22 '08

IDC: "Configuration and Change Management for IT Compliance and Risk Management", June 15, '08

Tripwire: "Practical Steps to Improving Your Compliance Process", June 03, '08

CISCO: "Cisco Takes the Mobility Network to the Next Level", May 28 '08

Websense: "Protect Against Data Loss from Web or Email", May 22 '08

PGP: "Data Breaches and their Impact". May 20 '08 May

CISCO: "Five Crucial Steps to Deploying a Secure Guest Network" May 13 '08

Websense: "The Webification of the Desktop" Apr 29, '08

(ISC) 2: "Vulnerability Management / Patches" Apr 22 '08

McAfee: "McAfee 2008 Security Road Show" Apr 16 '08

Prism Microsystems: "Using Behavior-based Correlation to Detect Threats in Real Time" Apr 16 '08

CISCO: "Designing Wireless Networks and Mobility Services in Branch Locations" Apr 09 '08

ISSA: "PCI DSS –Your Stepping Stone to a Trusted Security Model" Mar 28, 08

(ISC) 2: "Web Access Management" 18 Mar '08

CISCO: "Network Admission Control Design." Mar 6 '08

University of Bern: Open Source Security Testing Methodology Manual (OSSTMM) Feb 29 '08

(ISC) 2: "Securing from the Start: Examining Application Security" Feb 19 '08

IDC: 'How to Stay Out of the Headlines with PCI Compliance' Jan 31 '08

(ISC) 2: "You're E-mail Inbox Gateway to Danger?" Jan 22 '08

CISCO: "Essentials of Successful VoIP Migration". Dec 6 '07.

(ISC) 2: "on 4 Steps to Security Success". Nov 20 '07

McAfee: "Security Risk Management Series - Data Loss Prevention (DLP)". Oct 23 '07

CISCO: "Security Threat Landscape Session with Patrick Gray". Oct 18 '07

McAfee Security Risk Management: "Protection and Compliance Seminar". Sept 20 '07.

Websense: "Simple, Affordable, Fast and Effective - The new standard in Internet security" - July 2 '07

Microsoft: Energize IT (Lunch of Forefront Security, Ms. Server Code Name 'Longhorn') – June 16 '07

Network General: "Canadian User Forum" – Oct 18 '06

"Live Web Application Hacking" Workshop –Sept 21 '06

"Active Directory Design and Implementation" – April 10 '05

"Effective Patch Management", Feb 17 '04

"Microsoft Security Week", December 1-5, '03

“Network Analysis, Monitoring and Troubleshooting”, January 17 ‘02