

**SERGEY GRIGORENKO, B.Sc.**  
CISSP AMBCI CCSP  
CCNP CCNA CCSA/CCSE MCSA/MCSE Security+

Toronto, Ontario, M2M3W1, Canada  
Tel # 416 705 4156  
Email: Infosec@sergri.net

---

---

**OBJECTIVE:**

Highly motivated, enthusiastic and performance driven Information Security Professional with more than twelve years of successful experience in Information Technology in all phases of Strategic Planning, Implementation, Operations and Management is looking for an IT Security position in a progressive organization where he can utilize his skills and knowledge, ability to add a value by aligning technology strategy with organization's goals and objectives.

**SKILLS SUMMARY**

**Security Architecture and System Engineering**

- Strong understanding of security mechanisms, experience in the determination of security vulnerabilities, weaknesses, threats and related risks that exists within an IT Infrastructure or business processes.
- Working knowledge in Project Manager Competency Development framework including of planning, organizing, and managing resources to bring about the successful completion of specific project goals and objectives, PMBOK.
- Demonstrated knowledge of current IT security strategies, methodologies/tools/techniques, concepts/practices and industry trends associated with LANs, WANs, wireless networks, servers, firewalls, routers, switches, network protocols, applications and databases.
- Capable of effectively build strong relationships with the management of business units supported and communicate Information Security matters to various organizational levels including business units, technical staff and senior management.
- Experienced in transforming and negotiating business, privacy and legal requirements into security and technical specifications.
- More than 10 years of experience in network design, remote computing, desktop and server hardening, virtualization, compliance auditing, penetration testing, security monitoring and response.
- Experience in planning and conducting a network, application, database vulnerability assessment and controlled penetration testing.
- 5 years in SQL, VBasic, VBA, HTML, C/C++, Pascal, Assembler programming.

**Information Technology Risk Management**

- 8 years in development and execution of governance processes to support strategic direction and transformational changes. Organizational Security Program development including policies, procedures, standards and guidelines. Threat Risk Assessment, Penetration Testing and Information Systems Security Audit.
- Adhering processes needed to ensure compliance with legislation that affects Information Security and Privacy (PIPEDA, PHIPA, MFIPA, FISMA/ NIST, HIPAA, Sarbanes-Oxley (SOX 404), PCI DSS 1.2).
- Practical Knowledge of Information Systems Security and Management standards, frameworks and best practices (CobIT 4.1, ISO 17799/27001-27002, ITILv3 Foundations, Common Criteria).
- Ability to analyze and communicate needs and requirements for security architecture and standards to all stakeholders. Clearly express technical information and concepts to a non-technical audience and vice versa.
- Effectively work with senior management, influence decision makers. Monitor and manage projects to ensure accurate project time. Strong understanding of security operations challenges including key performance monitoring and audit.
- Understand the importance of effective technical documentation in identifying and managing IT security risks.

**Personal Qualities**

- Able to lead, manage and coordinate projects and operations, work without supervision both independently and within a team, effectively manage tasks, time and resources.
- Responsible, sociable, accurate, adaptable, self-sufficient, self-directed, detail and results oriented.
- Learn very fast and able to understand areas unfamiliar to me independently.
- Easily adaptable to new systems and tools.
- Always opened for constructive dialogue and suggestions.

## SYSTEMS / TOOLS / TECHNOLOGIES EXPERIENCE

- **Security technologies:** Defense-in-depth methodology , ACL filtering, Checkpoint, Cisco Pix and ASA, IDS/IPS, Barracuda, systems, honeypots, sniffers, network performance and monitoring utilities, vulnerability scanners and penetration testing utilities, forensic and auditing tools, malicious code containment - Antivirus, and Antispam defense.

**Platforms:** MS DOS, NT3.51/4.0/2000/2003, XP, S/390, AIX 5.3, HP-UX 11, SUN 9, Vista, AS400, SCO, CentOS Linux

- **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, VPN, VLAN, NAT, PAT, QoS, Wireless networks.
- **Encryption and authentication:** IPsec, L2TP, PAP, CHAP, WEP, WPA2, EAP, TKIP, DES/3DES, AES, SHA-1, MD-5, PKI, RSA, RADIUS, TACACS+.
- **Databases and Servers:** SQL, Oracle, VMware ESX, WSUS, SMS, MOM, Websense, Smart Filter, Citrix, ISA, IIS, HP Openview, BMC Identity Management, Terminal Server, Apache, Exchange, MDAemon, Veritas, FTP, TFTP, CA, VPN, Cisco ACS, RAS.
- **TOOLS:** Nessus, MBSA, Microsoft Security Assessment Tool, GFI LANguard Network Security Scanner\ Event Log Monitor, Nsauditor, Solarwinds tools, Checkpoint SmartDefense, Encase, Hyena, DameWare, Knoppix, Kismet, Cybercop, Metasploit, IISXploit, WebInspect, SuperScan, N-Stalker Web Application Security, L0pht, Brutus, Nmap, Netcat, Ethereal, Retina, Iris, Cain, Ciscoworks, Snort, Outpost, PGP, McAfee, Norton, Kaspersky, NOD, Acronis, Chost, Communications software, Access, Microsoft Office, Corel, Adobe, Symantec, Macromedia.

## CAREER HISTORY

**May, 2008 – December 2008** (contract)

IT Security Analyst /Toronto Transit Commission (TTC)

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

- Involved in development, implementation, operations and maintenance of a Security Program and Security Architectures. Conducted security policy gap analysis, revised existed and created new IT security policies and standards within defined framework in accordance with ISO17799 and NIST 800 series documents.
- Recommended new Information Security Policies development guide.
- Performed Threat Risk Assessments TRA (adopted RCMP and ISO/ IEC 27001) , Privacy Impact Analysis, Penetration Tests and Security Audit for numbers of projects.
- Provided Technical Assistance and Security Solutions consulting including assessment of Project Orders, RFP's, Business Case's and Service Level Agreements.
- Maintained management reporting system environment.
- Researches, monitors and communicates business and IT technology trends.

### Projects:

- **(GIS)** Enterprise Geographic Information System: Provided input to ensure that the technical solution is in compliance with appropriate privacy legislation, TTC policies and standards.
- **(CSDN)** 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.
- **(NTAS)** Next Train Arrival System: Involved in Threat/Risk Assessment, recommend remedial actions for risk reduction.
- **(NBAS)** Next Bus Arrival System (NBAS): Performed security assessments of detailed design requirements, RFP, Implementation and Test Plans on the infrastructure and system components during pre-production and production stages.

**Environment:** Supervisory Control and Data Acquisition (SCADA), Unicenter ServicePlus Service Desk (USPSD), IBM ClearCase, OS/390, AIX 5.3, HP-UX, DELL, CISCO ASA, PIX, Aeronet, CheckPoint NGX, SQL, Oracle, Veritas, Symantec, BMC IM, Microsoft Office, Exchange, Citrix, MS 2000/2003, XP, Office, Visio, Retina, Websense, Metasploit, VPN, SFTP, SSL.

**February, 2004 to May 2008****Sr. Security Analyst \* Team Lead / Bendix Foreign Exchange**

- Involved in the development of corporate wide IT Governance and implementing operational strategies, policies, standards to meet business strategic goals using ISO 17799 and CobiT frameworks.
- Determined business and operational requirements identified and recommended technology opportunities including, feasibility options, functionality and cost benefit analysis. Infrastructure Strategy, architecture, and operations, including networking, security, server platforms, desktops, laptops, remote access, storage, disaster recovery, business continuity.
- Conducted security risk assessments and defined security controls to support business needs and objectives. Developed foundations of the corporate security program including information security policies, procedures, standards, and guidelines.
- Conducted Business Impact Analysis on a regular basis, evaluated risks to operational facilities, and identified the technical requirements that meet or exceed the recovery requirements of mission critical business functions.
- Designed LAN and WAN infrastructure, Access Control Management, administered and supported various operating system platforms, network capacity planning and general network management.
- Successfully upgraded legacy systems from old terminals to centralized network environment, role based access control and perimeter protection.
- 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 .Net custom application development and implementation from the security perspective.
- Performed vulnerability assessment to ensure appropriate protection has been utilized for the systems.
- Participated in the incident response team in a hands-on, technical role.
- Network traffic monitoring and analysis for suspicious activities.
- Corporate Antivirus and antis spam protection, backup control.
- Provided guidance and administration for the Patch Management program.
- Worked with the different Business groups to ensure technical requirements are met.
- Provided training for the company's Management and Users.
- Established working relationships with vendor partners.
- Provided leadership role to IT staff in the BFX team.

**Projects:**

- Provided analysis of system, subsystem and elements requirements.
- Conducted BIA, security reviews of core systems, network and operational infrastructure and analysis of the state of information security.
- Enhanced corporate network security by performing various security audits. Introduced and implemented new security architecture model.

**Environment:** VMware ESX 3.1, Windows 2003, 2000, XP, SCO (UNIX), CentOS (Linux)

- AD, File, DNS, DHCP, Print, Application, Telnet Servers, IIS, SQL, ZIM, WSUS, FTP, TFTP, SNMP, SSH.
- CheckPoint NGX (R60), Cisco IDS 4210, Cisco routers 2600, 2811, switches 2950, Pix 506E, 515E, ASA 5505, RS232, RAS, VLAN, Remote VPN, Site-to-Site VPN, Cisco ACS (AAA), TACACS+, PAT, NAT, ACL, Websense, Cisco SDM, Dell Wireless AP. Nessus, MBSA, Nmap, Solarwinds Engineering, LANsurveyor, EnCase Forensic, L0phtcrack, Netstumbler, CyberCop. PGP, DameWare, VNC, VERITAS Backup Execute 10, UPS Manager, Citrix (Reuters), PC Quote, MS Office, Smart Draw, Visio, Kaspersky enterprise, Cash Plus Reports, Acronis, Privilege Manager, Made Easy, MS AD, Group Policy and Security Manager. MS Office, Maximizer (CRM), Cash+ Accounting, Access.

**September, 2001 to December 2003****IT Manager / EUROVENT**

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 newly formed information security division within this business unit, assisted in development and implementation of the information security management system, with particular emphasis on developing,

implementing and effectively managing the information security risk management function.

- Performed requirements analysis and architecture design.
- 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.
- Regular security checks, risk and vulnerability assessment.
- Implemented SSH, VPN solution to ensure data confidentiality and integrity. Implemented Cisco Firewall and router package filtering technology.
- Utilized network management tools (Retina, EtherReal, NISSUS, Snort, etc.) to analyze, monitor and troubleshoot network related problems.
- Direct supervision, technical coaching and monitoring of two System Administrators and Data Manager. Built and maintained professional relationships with clients and vendors.
- Created virtual lab environment using VMware to educate staff in counter hacking and various security tools and techniques.
- Implemented Security Awareness Campaign - Clean Desk, Clean Screen Policy. Developed Communication Strategies.
- Documented reports summarizing findings and recommendations.

#### Projects:

- Defined system level architecture and detailed design for defense-in-depth solutions for corporate wide network and telecommunication systems.
- Performed technical risk mitigation for newly designed and implemented features through research, modeling, simulation and/or prototyping.
- Created Audit program, Business continuity plan, vulnerability assessment and penetration testing, incident response procedures and change control management guidelines.
- Secure design and locked-down implementation for servers, desktops and laptops (Dell/Windows2K/2K3/XP)

**Environment:** Windows NT, 2000, 98, FreeBSD, Red hat (MySQL), File, DNS, DHCP, Print, Application Servers, IIS, MS SQL, MS MOM, Exchange Server, Sharepoint Portal Server.

- CheckPoint FW-1, Outpost, 2600 Routers, Remote VPN, Snort, Nessus, GFI Security Analyzer, GFI log server, Nmap, Iris Scan, Cain & Abel, Solarwinds tools, MS Visual Studio, Ethereal, RemAdmin, AutoCAD, 1C (sql), MS Office, MS Project, Visio, McAfee, Access.

#### September 1999 to August, 2001

##### System Engineer / North-West Timber Company

Responsible administration and maintenance of local network infrastructure. Provided IT services for over 5000 users. Performed design, configuration, and life cycle support for critical systems. Enhanced monitoring and reporting process.

- Administered and supported Multi-platform Operation systems.
- Provided leadership and implementation assistance for various security-related projects.
- Monitored, inspected and analyzed logs, audit trails, network traffic and payload.
- Maintained various applications and offered technical support to customers.
- Responsibilities included managing clients' NT 4.0 and 2000 networks, troubleshooting and repairing hardware and software issues for both onsite and drop off services, and handling telephone helpdesk support.
- Monitored system tasks and resources, optimized and tuned up system and performed backup/restoration.
- Responsible for maintaining departmental internal web site.
- Installed, configured and maintained SQL database, MS Exchange Server.
- Developed system to ensure compliance with organization's security policy.
- Evaluated and installed computer, networking hardware and operating system software.
- Troubleshooting of LAN and system problems, Cisco Switches and routers, T1 and frame relay, developed and documented standardized troubleshooting methodologies.
- Implemented Secure VPN connections for remote branches across country.
- Standardized desktop throughout the organization. Field-repair times reduced by 75%.

- Assess and review current technology infrastructure to identify key risk areas, and ensure adequate levels of controls are in place to address those risks. Evaluated system, network and application security.
- Provided assistance in network and system design for new opened offices.
- Member of team worked on company security policies and procedures, awareness program design, and implementation.
- Applied security patch management systems.
- Created documentation and offered presentation and training to end users.

## 1996 – 1999

### System Engineer / LENIMS

Responsible for building, monitoring and management of the server infrastructure for production, development, lab and hosted application environments, including all of the following:

- The main focus of my work was on determining the future direction of the computing environment for a group of about 150 technical users within Lenims under a \$1.5 Million budget.
- I was responsible for upgrading and converting of all of the PC's from 386/486's to Pentiums and from Windows 3.1 to Windows 95 (NT would not work here). Included in this was installing and supporting all of the desktop applications.
- Building, configuring, administrating and maintaining of Windows NT 4.0 Servers.
- Configuration and Maintenance of RBAC access control.
- Modifying and securing of security systems (Checkpoint Firewall) based on Linux.
- Performance tuning, building strategy, administration and maintenance of WEB (and all internet based) servers.
- Administration and maintenance of Compaq, Hewlett Packard and Dell Desktops and Servers, as well as Toshiba Laptops.
- Maintenance of network equipment, monitoring of network utilization and capacity planning of network resources (including WAN connectivity and management).
- The Microsoft Proxy Server was configured to use an ADSL connection to the Internet, and the Exchange servers were configured to handle Internet based mail for all users.
- Create and maintain disaster recovery solution and testing the disaster recovery plan.

**1985 – 1995** Served in the Air Force

Pilot – Engineer

## EDUCATION

- **1999-2001** St. Petersburg State University, B.Sc. System Engineer for the specialty “Computing Machinery and Computer-Aided System Software”
- **1999- 2001** Saint-Petersburg State Technical University, professional retraining program  
Diploma in “Personal computer and local network software”
- **1984-1989** Yeisk Air Force Military Academy, B.Sc. Diploma in Electronics

## CERTIFICATIONS

- CISSP (**C**ertified **I**nformation **S**ystems **S**ecurity **P**rofessional)
- CISA (scheduled on December 2008)
- AMBCI (**A**ssociate **M**ember of the **B**usiness **C**ontinuity **I**nstitute)
- CCSP (**C**isco **C**ertified **S**ecurity **P**rofessional)
- CCNP (**C**isco **C**ertified **N**etworking **P**rofessional)
- CCNA (**C**isco **C**ertified **N**etwork **A**ssociate)
- CCSE/CCSA (**C**heck**P**oint **S**ecurity **E**xpert/**A**dministrator NGX)
- MCSE/MCSA:Security (**M**icrosoft **C**ertified **S**ystem **E**ngineer/**A**dministrator)
- CompTIA Security +
- CNSS 4011 INFOSEC (Certification by NSA (National Security Agency) / CNSS (Committee on National Security Systems)
  - Certified Cisco VPN (Virtual Private Networks) Specialist
  - Certified Cisco IDS (Intrusion Detection System) Specialist
  - Certified Cisco Firewall Specialist
  - Certified Cisco Information Security Specialist

---

## PROFESSIONAL MEMBERSHIP

- \* (ISC)<sup>2</sup> - International Information Systems Security Certification Consortium
- \* ISACA - Information Systems Audit and Control Association
- \* BCI - The Business Continuity Institute
- \* IASA - International Association of Software Architects

---

## COURSES AND TRAINING ATTENDANCE

- IBM: "Building a successful security strategy" (Ziff Davis Enterprise Virtual Tradeshows) – Sept 17, '08
- VeriSign: "Crime Story: Bad Guys and what you can do to protect yourself from them", Aug 19, '08
- (ISC)<sup>2</sup>: "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
- BGP: "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)<sup>2</sup>: "Vulnerability Management / Patches" Apr 22 '08
- McAfee: "McAfee 2008 Security Road Show" Apr 16 '08
- Prism Microsystems Inc: "Using Behavior-based Correlation to Detect Threats in Real Time" Apr 16 '08
- InfoSecurity: "IP business communications security under the microscope" Apr 15 '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)<sup>2</sup> - "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)<sup>2</sup> "Securing from the Start: Examining Application Security" Feb 19 '08
- Straight Talk with IDC: 'How to Stay Out of the Headlines with PCI Compliance' Jan 31 '08
- (ISC)<sup>2</sup> - "You're E-mail Inbox Gateway to Danger?" Jan 22 '08
- CISCO – "Essentials of Successful VoIP Migration". Dec 6 '07.
- (ISC)<sup>2</sup> – "on 4 Steps to Security Success". Nov 20 '07
- ISA and McAfee – "Security Risk Management Series - Data Loss Prevention (DLP)". Oct 23 '07
- CISCO - "Security Threat Landscape Session with Patrick Gray". Oct 18 '07
- ISA & 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
- Double- "Take Protecting Microsoft Exchange and Centralized Backup" – Oct., 25 2006
- 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