TYSON MACAULAY, CISSP, CISA

CANADIAN SECURITY CLEARANCE: Top Secret SA – PWGSC File number 95156550-0000145082

LANGUAGES: English   (Speaking, Listening, Reading, Writing)
                         French   (Listening, Reading)

EDUCATION:

Hon BA, Political Science, Carleton University, Ottawa, Ontario, Canada, 1992

PROFESSIONAL DESIGNATIONS:

- CISSP (Certified Information Systems Security Professional)
- CISA (Certified Information Systems Auditor)

AFFILIATIONS:

- International Standards Organization (ISO) – Standards Council of Canada
- International Society of Automation (ISA)
- Cloud Security Alliance – Vice Chair, Canada
- Professional Engineers Ontario – Emerging Technology Task Force

PROFILE:

Tyson Macaulay is the Security Liaison Officer (SLO) for Bell Canada. In this role, he is responsible for technical and operational security solutions across Bell's major product lines: connectivity (fixed/wireless), cloud-services, IP Voice, and unified communications. Tyson's experience encompasses a broad range of industry sectors from banking to defence to healthcare. His expertise includes risk and security management programs, security and privacy standards, security architecture and product development.

Tyson is the author of several security patents filed with the USPTO between 2001 through 2011, and supports the development of engineering and security standards through the Professional Engineers of Ontario (PEO), the International Standards Organization (ISO), the International Society of Automation (ISA) and the Internet Engineering Task Force (IETF).

Tyson is a respected speaker with peer-reviewed publications starting in 1993. Topics include regulatory and risk management issues, wireless security, critical infrastructure protection, industrial control systems security, converged IP networks, carrier-based (Upstream) security and much more. Tyson's publications and practice areas can be found on-line at **www.tysonmacaulay.com**.

QUALIFICATIONS AND EXPERIENCE:

<u>Security Liaison Officer (SLO) / National Security Strategy Lead – Bell Canada, Ottawa, Ontario - November 2004 – Present</u>

Bell Canada Security Liaison functions: product definition and development, publication and research, public speaking, mentoring of internal staff, marketing support, internal risk management, direct management of teams of engineers. (Nov 2004 to present)

- Security architecture and compliance for enterprise clients: Sarbanes – Oxley (SOX) risk-management tools are required for compliancy purposes by the SEC in order to maintain Bell's NYSE listing.   Role required the design of architectures and processes for assessing security-related risks within Bell Canada client-base. Role also involved the training and supervision of 2 staff members responsible for reviewing all Bell opportunities and outbound proposals containing security services or stipulations of any type. Current involvement is a advisor and consultant to full-time SOX staff in Bell.   (Nov 2006 to present).

- Development and documentation of next-generation security products. Work includes patent development in the area of carrier-based security services; IPv6 product definition and IPv6 security services; the validation of market demand for new products and services; interfaces with technology vendors to ensure that performance metrics map to client requirements – as they are currently understood; presentation of next-generation security product offering sot clients for refinement; budgeting and planning development efforts for trials and prototypes of next generation security products. (Nov 2004 – present)

- Though leadership, to highlight Bell's capabilities in the IT Security Industry. Work includes; international standards development, the generation of original written works in the area of IT Security for publication and distribution to clients, peers and the public at large; public speaking and presentation of Bell value proposition and competitive differentiators in forums such as conferences, tradeshows, , corporate boards and post-secondary lectures. (Nov 2004 – present)

National Security Strategy lead functions: functional responsibility for strategy and business development of $150 Million annually in ICT security consulting, managed services and product solutions. Duties include: development of ICT security solutions, delivery methodologies and standardized templates, use of scheduling tools, cost control measures, risk management techniques, Q&A protocols and best practices related to project management in all examples described below. (March 2010 to present)

- Product definitions and development: developed and trained engineering staff in the delivery of a portfolio of distinct professional service products. Work includes: the development of detailed sales and marketing collateral; awareness and education campaigns supporting staff and clients, the development of specific delivery methodologies utilizing international standards and representing international best practice.

- Skills strategy development and implementation: developed comprehensive set of PS skills management tools and process to mange resources of both internal practitioners and partner resources. Work includes the development of software-based tracking and control tools, use of tools in streamlining bid response and improving quality overall; development of training strategy and budget to address

challenges associate with skills and mapping to forecasted requirements around market demand and technology drivers and trends.

- Support to Professional Services delivery teams. Work includes provision of mentoring and leadership on a project by project basis; quality control and project management support to maintain client expectations and align with budgets; customer interviews and meetings to define service requirements for the existing portfolio and support bid and proposal development based upon the articulated needs.

Sample projects

- Bell Canada Product and technology development: Product design, architecture and business cases assessment of cyber-intelligence and IPv6 security services. Work includes the development of requirements-definitions tools and processes, technical specifications related to security and performance, patent development, sales collateral creation, customer interviewing and focus-testing, and significant public speaking. (Jan 2009 to present)

- The Ottawa Hospital C-CISO / Security Liaison Officer: The Ottawa Hospital is Canada's largest, with a $1Billion annual budget and 4 campuses supporting over a million Canadians. This role involved provision of management-level and technical consultation services associated with the developing cyber (ICT) security program TOH. Work includes the delivery of security documents compliant with international standards (ISO 27002), enterprise security architecture, enterprise risk management, regulatory compliance support (PHIPA, PCI), program planning and budgeting, and support to education and awareness campaigns. Data assets covered by this work include a full range of converged IP assets in addition to business data including: telephony/VOIP, SCADA, transaction processing, physical security and video conferencing. (May 2009 – Jan 2011)

- Canadian Department of National Defense – Converged cyber security risk management – Project lead: This role included the analysis of Voice over IP (VOIP) and Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems for cyber threats and vulnerabilities, including recommendation for remediation and mitigation. Work also included the development of reference architecture to support national defensive operations in country, in-theatre and with allies. This work builds upon previous work with critical infrastructure sectors (see below) and research into evolving methodologies for assessing and treating cyber threats against converged IP assets using carrier-network elements as a new layer of security. See Research and Publications section. (Jan 2009 – Aug 2009)

- Critical Infrastructure Protection for Government of Canada – Bell Canada practice lead. Bell Canada was engaged by the federal government of Canada to undertake detailed investigations into Critical Infrastructure risks and security interdependencies. Work involved the coordination of a large team of subject matter experts working across all CI sectors (Telecom, Finance, Health, Energy, Water, Safety, Transportation, Manufacturing, Food and Government). Work included writing and developing all methodologies, based upon work from NIST and Wharton Business School. RAND Corporation was engaged in the verification and validation of all methodologies. Results are interdependencies matrixes for the 10 defined critical infrastructure sectors, and state-of-readiness matrixes for the same 10 sectors. Information collection involved both face to face interviews and on-line surveys, with respondents coming primarily from across Canada but also U.S. sources. This work include a full

range of converged IP assets (business data, telephony, SCADA, transaction processing, physical security and video conferencing) and a full range of telecommunications delivery technologies including MPLS, Ethernet, wireless (satellite/802.11/802.16/CDMA/GSM/EVDO/GPRS).   (Feb 2006 to Jan 2009)

- Bank of Montreal / Harris Bank: C-CISO/Security Liaison Officer between Canada's third largest bank and Bell Canada. Position involves management of SAS70 and CICA 5970 compliance audits to support the Sarbanes-Oxley assurance requirements of the bank under ISO 17799/27002. Additional work includes the management and performance of threat and risk assessments associated with converged ICT networks (data and voice) against physical and cyber threats, technical assessments of enterprise security architecture and large scale telecoms networks (MPLS/Ethernet/IP), presentations to client staff and overall responsibility for development of security remediation plans to support bank assurance requirements. (March 2006 to June 2008)

- Manulife Financial / John Hancock financial: C-CISO/Security Liaison Officer between Canada's largest insurer and Bell Canada. Position involves management of SAS70 and CICA 5970 compliance audits to support the formalized security program of the company under ISO 17799/27002. Additional work includes the management and performance of threat and risk assessments associated with converged ICT networks (data and voice) against physical and cyber threats, technical assessments of enterprise security architecture and large scale telecoms networks (MPLS/Ethernet/IP), presentations to client staff and overall responsibility for development of security remediation plans to support assurance requirements. (March 2006 to June 2008)

- TD Waterhouse Bank: C-CISO/Security Liaison Officer between Canada's second largest bank and Bell Canada. Position involves architecture and specification of all security components associated with large scale converged network-deployment (VOIP, Data, Presence technologies). Management of SAS70 and CICA 5970 compliance audits to support the assurance requirements of the bank under ISO 17799/27002. Work includes business and technical requirements definition and documentation, architecture, threat and risk assessments associated with converged ICT networks (data and voice) against physical and cyber threats, technical assessments of enterprise security architecture and large scale telecoms networks (MPLS/Ethernet/IP), presentations to client staff and overall responsibility for development of security remediation plans to support bank assurance requirements. (March 2006 to Aug 2007)

Director, EWA-Canada Ltd, Ottawa, Ontario - June 2001- November 2004

EWA-Canada is the Canadian branch of Electronic Warfare Associations (EWA), a U.S. defence contractor based in Herndon, Virginia. Functional responsibility for Threat and Risk Management services, PKI Managed Services and Wireless Security (satellite/802.11/802.16/CDMA/GSM/EVDO/GPRS). Duties include: project management according to ISO 9001 standards, technical architecture, policy development, systems integration and crypto-applications development. Use of scheduling tools, cost control measures, risk management techniques, Q&A protocols and best practices related to project management in all examples described below. All projects performed at EWA-Canada are ITS projects.

<u>General Network Services - GNS (acquired by JAWZ Canada Inc), Founding Partner / CTO, Ottawa, Ontario - Feb 1996 to May 2001</u>

Responsible for PKI and Wireless Security and Managed Services including: project management, architecture, security program and policy development, systems integration and crypto-applications development. Use scheduling tools, cost control measures, risk management techniques, Q&A protocols and best practices related to project management in all examples described below. All projects performed at JAWZ/GNS are ITS projects.

<u>Internet Consultant, Self-employed, Ottawa, Ontario - April 1992- Jan 1996</u>

Development and Project Management of early TCP/IP / Internet services for Federal Government on the CA*Net network. Designed and offered Internet training courses to business and government. System administration and project management on internet sites including support of system confidentiality, availability and integrity. Responsible for the application of document management methodologies and federal identity program procedures to all services delivered through the projects under management. Use scheduling tools, cost control measures, risk management techniques, Q&A protocols and best practices related to project management. Specific clients included:

TECHNICAL SKILLS:

Management / Administration	Technology/Standards
- Operational Risk Management - Threat-Risk Assessment - Privacy Impact Assessment - Disaster Recovery / Business Continuity - Security Audit and Evaluation - Project Management and cost control - Secure Electronic Archival Systems - Certification Practice Statements and Certificate Policies - Electronic Workflow Design and Improvement - PKI Architecture Development - Critical Infrastructure Protection (CIP) - Information Sharing Analysis Centers (ISAC) - Enterprise Security Architecture - Managed Security services	- ISO 17799/2700x, ISO 21827, NIST 800-26, NIST 800-55, NIST 800-82, ISA-99, CoBIT, ISO 25999, NPFA 1600 - SAS 70 / CICA 5970 auditing - IP Convergence security (VOIP, SCADA) - WAN/LAN Topology and Architecture (MPLS, ATM, Ethernet) - ICS/SCADA: MODBUS, Devicenet - IPv4 and IPv6 - X.500 and X.509 - Wireless: GSM, CDMA, 1xRTT, GPRS, EDGE, EVDO, UMTS, Bluetooth, IEEE 802.11, IEEE 802.16, IEEE 802.20, Satellite, Mobile IP - Public Key Infrastructure (PKI) - Digital Signatures and File Encryption - Session Encryption / VPN - SMIME / Secure e-mail

RESEARCH AND PUBLICATIONS:

Books

1. <u>Security Converged IP Networks: New requirements for information and Communications Technology Security and Assurance</u>, 300 pages, Auherbach publishing, June 2006 ISBN: 978-0849375804
2. <u>Critical Infrastructure: Understanding its Component Parts, Interdependencies, Vulnerabilities and Operating risks</u>, 400 pages Auherbach publishing, Aug 2008 ISBN: 978-1420068351
3. <u>Official ISC2 Guide to the CISSP CBK</u> (2009 revision), ISC2, Auherbach publishing ISBN: 978-0849382314

4. <u>Industrial Automation and Process Control Security: SCADA, DCS, PLC, HMI</u> - Auherbach publishing ISBN: 978-1439801963

Periodicals and papers

1. Bell Canada whitepaper, <u>Computing cloud Security</u>, November 2011
2. Bell Canada whitepaper, <u>IPv6 Security</u>, June 2011
3. US DOD IATAC Newsletter, <u>Upstream Intelligence: Use cases and Case studies</u> Jan 2011
4. US DOD IATAC Newsletter, <u>Delivery technologies for Upstream Intelligence</u>, Oct 2010
5. US DOD IATAC Newsletter, <u>Upstream Intelligence</u>, Aug 2010
6. US DOD IATAC Newsletter, <u>Anatomy of Upstream Intelligence</u>, Aug 2010
7. US DOD IATAC Newsletter, <u>Business Models for Upstream Intelligence</u>, Aug 2010
8. Bell Canada whitepaper, <u>ICT threats and mitigating controls under pandemic response conditions</u>, Aug 2009
9. Big Medicine EM Journal, <u>Critical Infrastructure Interdependency Wheel - Summary U.S. Version</u>: July 2009
10. Bell Canada whitepaper, <u>Upstream Security</u> June 2009
11. Big Medicine EM Journal, <u>Critical Infrastructure Interdependency Wheel - U.S. version</u>: July 2008
12. Big Medicine EM Journal, <u>Critical Infrastructure Interdependency Wheel - Canadian version</u>: July 2008
13. <u>Critical Infrastructure; proceedings from IFIP 11.10 Conference March 2008</u>, Journal of Critical Infrastructure Protection, Elsevier Publishing

14. Frontline Security Magazine, <u>Critical Infrastructure Interdependency: How does we measure it?</u> Q3 2008
15. <u>Additivity of Operational Risk</u>, RFC, Feb 2008
16. Information Systems Security Journal, <u>Risk Conductors,</u> Jan 2007
17. CSO Online magazine, <u>Operational Risk management</u>, Nov 2006

18. Dalhousie Technology Law Journal, April 2005, <u>The Case for Review of CRTC Wireless Jamming Regulations</u>, , Dalhousie University Law School
19. Information Assurance Journal, April 2005, <u>Commodity Absence</u>, US DoD
20. Bell Security Solutions Inc whitepaper, February 2005, <u>Managing Assurance: IT Security on converged networks</u>
21. CSE Security Symposium proceedings, May 2003, <u>IEEE 802.11 Counter-measures</u>,
22. Information Assurance Journal, February 2002, <u>Hardening 802.11 Wireless Networks,</u> US DoD
23. AFCEA Newsletter, Fall 1999: <u>The Bumpy Road to PKI Implementation</u>
24. Computing Canada, September 1999: <u>Digital Signatures: How far down the road</u>?

25. Journal of Government Information: May 1997: <u>Cutting Off Access to Government Information: Loop-holes in the Access to Information Act Generated by the Internet</u>
26. Policy Options, <u>The Development of Electronic Commerce in Canada: Using Networks for a Competitive Advantage</u> May 1993