

Canadian ISO 17799 User Group Conference

Sun Life Financial's Experience with Security Governance & ISO 17799

Deloitte & Touche, 79 Wellington West, 20th Floor
Toronto, ON 30 January 2004

D.A. Stolovitch, CD, CPP, CISSP, CISM
Director - IT Security Governance
Sun Life Financial

2

Aim

- To present a brief overview of Sun Life Financial's experience with security governance & ISO 17799:
 - what we are doing & why; and
 - key lessons we have learned.

Topics

- The Company
- Corporate Information Security Mission & Roles
- ISO 17799 & Security Governance
- BS 7799-2 Certification
- Security Programme Architecture
- Security Governance Framework
- Security Strategy
- Approach to Security Governance
- Key Lessons Learned



The Company

- A leading international financial services organisation providing a diverse range of wealth accumulation and protection products and services to individuals and corporate customers.
- Founded in 1865.
- Operations in key markets world-wide.
- One of the largest North American life insurance companies.
- As at 30 September 2003 - total assets under management of CDN \$348.5 billion.
- Publicly traded on the Toronto (TSX), New York (NYSE) and Philippine (PSE) stock exchanges under ticker symbol "SLF".



The Company

- We are a finance company - we live or die by our computers!
- 15,000+ users on our world-wide network
 - employees, contractors, outsourced service providers, subsidiaries, Joint Ventures, & thousands of external sales agents!
- Senior executives and other employees constantly travelling world-wide
- Business operations in Canada, US, UK, Bermuda, Ireland, India, Hong Kong, China, Philippines, & Indonesia
 - Different Financial Regulators = different/inconsistent regulatory requirements
 - Different, inconsistent, or non-existent laws
 - Local law enforcement, emergency and medical services may be corrupt, ineffective, or non-existent
 - Regional Risks – insurrection, terrorism, natural disasters, disease



Current & Emerging Risk Issues

- Legal & Regulatory
 - Privacy
 - Financial Services regulations (OSFI, FSA, etc.)
 - Corporate Governance (e.g. Sarbanes-Oxley)
- Technology
 - Vulnerabilities – bad software, bad installation/configuration
 - Malicious Code – viruses, worms, etc.
 - Hacking – Denial of Service, Intrusion, exploit code
 - Rapid evolution & increasing complexity of IT
- Customer Expectations & Independent Assurance
- Media & Reputation – Public Expectations
- External Risks – Crime, Terrorism, War, Natural Disasters, Disease Outbreak, etc.
- Insider Attacks
- Ignorance & Complacency



Corporate Information Security's Mission & Roles

8

Mission

Corporate Information Security contributes to the success of Sun Life Financial, and the creation of shareholder value, through security and enterprise continuity:

- leadership;
- corporate governance; and
- strategic services

enabling the effective management of risks to the protection, privacy, confidentiality, availability, and integrity of sensitive information and IT resources throughout the Corporation.

We do this in support of the EVP – CIO and in partnership with Business Group CIOs, Business Leaders, Privacy, IT Security and Business Continuity organisations and other security stakeholders.



Roles

- Security Governance
- Strategic Security Services
- Oversee Security Operations



Security Governance

- Develop, maintain, and communicate
 - Enterprise Information Security Programme Architecture & Governance Accountability Framework
 - Security & Enterprise Continuity:
 - Policies and Standards
 - Procedures for processes requiring enterprise-wide standardisation
- Monitor and report to SLF Board and executives on governance implementation & compliance



Strategic Security Services

- Enterprise Security & Continuity Leadership & Strategy
- Guidance & support – Security & Enterprise Continuity related operating plans and execution
- Security Consulting:
 - Threat, Vulnerability & Risk Assessment
 - Security Reviews & Compliance Support
- Security Awareness
- Security Control Development & Standardisation
- Crisis Management Programme development & maintenance
- Business Impact Analysis
- Crisis Management, Business Continuity & Disaster Recovery Plan development and testing



Oversee Security Operations

To ensure governance requirements are met, we oversee:

- Firewall Management
- IDS Management
- Security/Virus Incident Response & Management
- Security Intelligence & Strategic Threat Monitoring
- Vulnerability Testing & Management
- Security Administration:
 - General (e.g. user ID set up & termination)
 - Privileged Access
 - System Access & Logical Security
- SPAM Control
- Internet Web Blocking



ISO 17799 & Security Governance

14

What is Security Governance?

- The aspect of corporate governance that applies to an organisation's security
- So, what is corporate governance?
 - Many different definitions – none universally accepted
 - ISF's definition:

“A demonstrable framework for operating an organisation to acceptable levels of risk, fully compliant with regulatory and legislative requirements, and ensuring the protection of stakeholder value.”
 - ISF Workshop Report *Information Risk in Corporate Governance*, December 2003

What is Security Governance?

- Gives life to Security Strategy
- Includes several key activities:
 - Risk Identification, Assessment & Management
 - Knowing about current & emerging risks, their significance (likelihood & impact), and how best to manage them
 - Risk-based Rule-Making
 - Making & maintaining policies/standards/procedures to deal with risks
 - Directs the delivery of security programmes & services
 - Communicating & Implementing Rules
 - Awareness, training, communicating, implementing
 - Monitoring & Reporting on Compliance
 - Adjusting
 - Correcting non-compliance
 - Addressing new/changed risks



Role of ISO 17799

- A primary source for SLF's security governance
- Not the only source!
- ISO 17799 is not enough – it can't stand alone!
- SLF also uses:
 - Information Security Forum *Standard of Good Practice: The Standard for Information Security, Version 4.0*
 - ISACA/IT Governance Institute *Control Objectives for IT (COBIT), 3rd Edition*
 - CICA *IT Control Guidelines, 3rd Edition*
 - CERT/CC *System and Network Security Best Practices*
 - applicable US NIST Security Standards



Value of ISO 17799

- It is an INTERNATIONAL STANDARD
- Far from perfect, but good enough in many/most areas of security
- A security management standard – not a technical standard
- Helps us deal with regulators and international business partners
- Hard to argue with – after all, it’s an ISO standard
- Helps justify direction taken in SLF’s security policies & standards



Limitations of ISO 17799

- Does not cover all aspects of security
- Some parts of it aren’t relevant to SLF
- High-level “what to do” – does not have enough “how to do it” for implementation and compliance assessment
- Needs to be supported by more detailed direction – can’t stand by itself



Where ISO 17799 Fits as a Source for Security Governance

- Overall IT Governance Framework
 - COBIT – security covered in PO9, DS4, & DS5
- High-level Security Programme Framework
 - ISO 17799
 - CICA *IT Control Guidelines*
- Intermediate-level Detailed & Comprehensive Guidance for Security
 - ISF *Standard of Good Practice*
- Detailed Guidance for Specific Aspects of Security
 - CERT/CC *System and Network Security Best Practices*
 - applicable US NIST documents



BS 7799-2 Certification

BS 7799-2 Certification

- No interest in BS 7799-2 certification at this time
- Reason – lack of business value
 - High cost & no benefit
 - Not harmonised with other certifications (e.g. SysTrust, WebTrust, CICA s.5900/SAS70, Sarbanes-Oxley)
- BS 7799-2 is a UK standard, not an International one
 - Not internationally accepted/recognised
 - No ISO certification equivalent to BS 7799-2 at this time
- Our customers and regulators aren't demanding it
 - They are interested in security & privacy
 - They ask us to:
 - complete detailed questionnaires describing our security programme; or
 - supply a copy of a certificate from our External Auditors (CICA s.5900 or SAS 70 in the US)



Enterprise Information Security Programme Architecture

Enterprise Information Security Programme Architecture

- Define SLF's Information Security Programme
- Not a technology architecture – a business programme architecture
- Describes and maps out all components of the Information Security Programme
 - How they relate to each other
 - How they align to SLF's business
- Written in business language
- States at a high level
 - what is to be done; and
 - who is to do it



Enterprise Information Security Programme Architecture

- 14 key components
- Integrated and work together to provide an effective Information Security Programme.
- Overall model of the architecture and the components are based on the approach used in
 - ISO Standard 17799 *Code of Practice for Information Security Management*
 - the Information Security Forum *Standard of Good Practice*
 - the Ernst & Young Security Architecture
 as adapted to meet SLF business needs.



Enterprise Information Security Programme Architecture

- Security Strategy
- Security Governance
- Security Risk Management
- Security & IT Organisation
- Security Awareness
- Infrastructure & Technology Security Architecture



Enterprise Information Security Programme Architecture

- Security Operations
 - Intelligence Monitoring, Analysis & Warning
 - Security Incident Detection & Notification
 - Crisis Alert Notification
 - Firewall & IDS Management
 - Vulnerability Testing & Management
 - Anti-Virus Deployment & Management
 - SPAM & Web Filtering
 - VPN & Remote Access Management
 - Security Administration



Enterprise Information Security Programme Architecture

- Security & BC/DR Incident Response & Management
- Business Continuity, Disaster Recovery & Crisis Management
- Physical Security
- Personnel Security
- Security Performance/Posture Metrics, Monitoring & Reporting
- Security Audit & Compliance



Worldwide Security Governance Framework

World-wide Enterprise Security Governance Framework

- Signed by the President & COO – last updated in December 2003
- States that our Information Security Programme must align to relevant aspects of ISO 17799 (and some other named sources of best practice)
- A matrix that covers
 - Governance - who authorises/issues what level of Governance
 - Services - who delivers what type of service
- Provides basis for co-ordinated effort across the enterprise
- Delineates security roles & responsibilities
 - Line Management & Users
 - National CIOs & IT Security
 - Physical Security
 - HR - Personnel Security
 - Audit & Compliance



Security Governance

Business Needs/Drivers Supported by Governance

- Integration of Clarica
- Outsourcing
- Centralise Security Administration in Ireland
- Maintain uptime of vital SLF IT systems (BCP/DR)
- Enable privacy of personal information - customers, policy holders & employees
- Safeguard sensitive/confidential information owned by or entrusted to SLF
- Enable regulatory compliance (OSFI, FSA & Other Canadian, US, UK, & Asia-Pacific Financial Regulators)



Governance Documents

- POLICY - statements of SLF's direction/position
 - What must be done & the business rationale for doing it
- STANDARDS
 - Supporting the policy with more detailed direction
 - Performance or technical requirements
 - Who, what, when, where, frequency, quality, level of performance, etc.
- PROCEDURES
 - Supporting the standards
 - How to do it



What is Covered in Governance?

- Enterprise-wide protection of:
 - Sensitive/confidential information
 - IT systems - critical IT infrastructure
- Enterprise-wide continuity of business:
 - Business Continuity Planning & Disaster Recovery
 - Crisis Management
- All of this is based on risk & due diligence



Our Approach to Governance (1)

- EVP - CIO approves
 - Governance development priorities
 - Policies & Standards
- Key Policies (e.g. Information Security, BCP/DR, E-Mail Retention, Acceptable Use)
- Approximately 30 Security Standards:
 - **BUSINESS SECURITY STANDARDS** -
 - Product/technology neutral
 - Aligned to & covering key areas of Information Security Forum & ISO Standard 17799 Framework
 - **TECHNICAL SECURITY STANDARDS** -
 - Product neutral, unless otherwise required
 - Covering the platforms/technologies SLF uses



Our Approach to Governance (2)

- Technical Security Standards:
 - do not specify/prescribe products
 - do set requirements - enabling Systems Engineering to select the right security product/solution
- Developed in consultation with key stakeholders
 - e.g. Business Groups, Systems Engineering, Legal Counsel, Privacy, Physical Security, Audit, etc.
- Corporate Information Security develops and issues
 - All policies & standards
 - A few procedures - where enterprise-wide standardisation needed (e.g. incident reporting/management)
- Business Groups develop and issue their own procedures to cover applications & local security issues
 - Reviewed by Corporate Information Security to prevent conflict with Corporate Governance



Governance of Outsourced Service Providers, Vendors & Other 3rd Parties

- Must comply with SLF Security Governance:
 - When given access to SLF IT systems/resources;
 - When physically present at SLF facilities; or
 - When delivering contracted services to SLF
- Specific expectations are documented in relevant contracts or service agreements
- Performance/compliance:
 - Monitored via normal contract monitoring/management processes
 - Subject to audit at any time by SLF auditors



Governance of Subsidiaries & Joint Ventures

- Must comply with SLF Security Governance
- On a case-by-case basis, they may be exempted by VP – Information Security & Enterprise Continuity from a policy, standard or procedure if:
 - the policy, standard or procedure does not apply;
 - relates to a business or IT activity, process or technology that is not used or performed in the subsidiary/JV
 - the subsidiary/JV has its own substantially consistent document that covers the subject; or
 - as confirmed by Corporate Information Security or Business Group IT Security
 - the head (e.g. President or equivalent) of the subsidiary/JV has signed off accepting the risk posed by not implementing or complying with the SLF security policy, standard or procedure.



Implementation & Awareness (1)

- Effective implementation & awareness process is critical
- The job doesn't end once the policy or standard is signed by the boss
- Security Awareness
 - Is a Critical Success Factor for implementation of Security Governance
 - Gives life to Governance!
 - Fosters compliance
 - Enables access to your security programmes and services
 - If done well, gives you more benefit than most other aspects of security



Implementation & Awareness (2)

- Once Governance (policy/standard/procedure) is approved
 - Supporting security awareness tools are developed (e.g. PowerPoint slide briefing on key points, user guides, etc.)
 - New document and any supporting awareness tools are issued to all stakeholders as a package
 - Simultaneous posting on Intranet & internal advertising
 - Stakeholders are given 30 days to report the date by which the new policy/standard, etc. will be communicated and implemented
 - maximum of 12 months allowed for implementation
 - Stakeholders develop and execute their own implementation plan -
 - communication & roll-out to staff & awareness
 - development/implementation of any local supporting procedures, configuration, & management processes



Compliance

- Effective compliance monitoring is critical!
- Security notifies Audit of the implementation dates supplied by stakeholders
 - Audit then knows when a specific aspect of policy/standard can be added to the scope of their audits
- Audit conducts internal audits & reviews
- External auditors do likewise (e.g. CICA s.5900)
- World-wide network of Compliance Officers also can do local compliance reviews
- Security does ongoing security reviews
- Programme of 3rd Party Penetration Testing



Ongoing Care & Feeding

- Governance must be kept up to date so that it keeps pace with business needs and the rapid evolution of technology
- Policies, Standards, and Procedures are reviewed, and if necessary revised:
 - Annually;
 - Following a serious security incident;
 - When significant changes are planned or occur to:
 - SLF business operations;
 - SLF IT platforms & technologies;
 - laws & regulations;
 - security threats, vulnerabilities, & risks; or
 - When requested by a stakeholder.



Key Lessons Learned

Some Key Lessons We Have Learned – so far

- Top Management Commitment is vital!
 - Reporting relationship
 - Budget resources
 - Support when tough decisions are needed
- Keep it simple – don't over-engineer!
- Everything must be risk-based – in business terms!
- Sort out the mandate first – so you don't have to debate it later!
 - Security Governance Framework
 - Security Programme Architecture
- Then develop an Enterprise Security Strategy to implement the above!
- For governance – make prioritised list of policies, standards & procedures for development
 - Based on risk and stakeholder preferences
 - Based on relevant parts of ISO 17799 and other sources of best practice
 - Factor in revision of legacy governance



Some Key Lessons We Have Learned – so far

- Outsource security services when needed – choose service providers with care!
- Choose your internal Security Staff with care!
- Be wary of consultants and service providers – products & services are not always what they seem or claim to be – may not meet your needs!
- Document & publish your programme and your policies/standards/procedures
- Security awareness is vital – gives life to your governance & programme!
 - Bulletins, new hire orientation, Intranet accessible central repository for policies, standards & procedures, etc.
- Develop & monitor metrics
 - security posture
 - security performance
- Have the programme audited – auditors are your friends or at least allies!



Questions?

D.A. (David) Stolovitch, CD, CPP, CISSP, CISM
Director – IT Security Governance

Corporate Information Security
Sun Life Financial

(416) 496-3404
david.stolovitch@sunlife.com

