

Information Security

Not Just for Geeks Anymore

Carol M. Johnson

Corporate Vice President & Associate General Counsel

Massachusetts Mutual Life Insurance Company

MassMutual Financial Group

cjohnson@massmutual.com



The content of this presentation represents the opinions of the presenter and does not necessarily reflect the positions or policies of any of the MassMutual Financial Group companies

Information Security – Business Critical

- Being able to demonstrate that computer logs are complete, accurate and verifiable is imperative, even for the most basic electronic systems, such as voicemail and email
- Tying the “signature” to the transaction
- Preventing identify theft and fraud
- Protecting confidentiality of customers’ and employees’ nonpublic personal information
- Responding to Regulators’ Audits (Insurance Department Privacy Questionnaire)
- Enforcement Agency Inquiries
- Civil Litigation
- Consumer Complaints

Legal / Business Requirements

Legal

- There is a thicket of federal and state laws / regulations that have an impact on eSignature processes and information security (see Buckley Kolar presentation)
- The number & complexity of the laws / regulations is growing
- Companies need to be able to document integrity of information systems
- The potential liability and “reputation cost” of a security breach is enormous

Business: Internal – Governance and Management

- Boards of directors and executive management of financial services companies:
Information security is key to fulfilling their responsibilities

Business: External

- Customers’ expectations
- Inspiring the public’s trust is more important than ever

MassMutual Financial Group Companies – An Overview

Global, diversified financial services organization (Year end 2003):

- Over 31,000 employees and representatives worldwide
- Assets under management: \$285 billion
- Worldwide insurance in force: \$415 billion

Companies include

- Massachusetts Mutual Life Insurance Company

Founded 1851

52 U.S. jurisdictions – Over 80 agencies and 1,500 additional sales offices

Ranked 84 on the *Fortune* 500 (*Fortune* March 2004)

www.massmutual.com

- MML Investors Services, Inc.

Broker-Dealer

- MassMutual International, Inc.

Subsidiaries' operations in Asia, South America, Europe

- The MassMutual Trust Company, FSB

Serves fiduciary accounts – complements insurance products and estate-planning services

- Babson Capital Management LLC

Investment adviser – services institutional and individual investors

- OppenheimerFunds, Inc.

Over 7 million mutual fund shareholder accounts

Companies' Products / Services

- Life insurance, disability income insurance, long-term care insurance, annuities
- Retirement:
 - Defined contribution / 401(k), defined benefit, nonqualified deferred-compensation plans and services
- Structured settlements
- Trust services
- Mutual funds and other investments
- Asset management for individuals, institutions and corporations

Insurance and Financial Services Companies – Multiple Regulators

- State
 - State-by-state insurance laws (All 52 jurisdictions)
 - Other laws not pre-empted by federal law (California SB 1)
- Federal
 - SEC
 - NASD
 - ERISA – U.S. Department of Labor
 - Other: Gramm-Leach – Bliley, Fair Credit Reporting Act, HIPAA
- International

LET'S BE PRACTICAL

Some Components of an Effective Information Security Program

BASELINE: INFRASTRUCTURE & PROCESS IS IMPERATIVE

-- Board and Executive-level sponsorship

-- Chief Compliance Officer / Chief Information Security Officer

-- Legal advice – identify current and changing requirements

-- Resources to establish, communicate, and enforce policies and practices

Not enough to write the policies and procedures

Need to be “in the bones” in the corporate culture

Build in to business processes

Challenges: staff turnover, organizational structure, geographical diversity, complex subject matter

-- Processes to respond appropriately to internal and external demands

INFORMATION SECURITY POLICIES

- Applied across the enterprise
- Developed by Information Security staff
- Reviewed by legal and compliance staff
- Stay ahead of the curve – but remain within normative business practices
- Buy-in by business side
- Build in to business practices
- Communicate and educate throughout the organization
- Checks / audits to determine compliance

Representative Information Security Policies

Encryption

- All portable computing devices must employ encryption and password protection methods approved by Information Security.
- Only company-approved encryption algorithms may be applied to data owned by the company.

External Network Interfaces

- All network services and connections to the company network from the outside must be pre-approved by Information Security.

Malware (Viruses and Worms)

- Virus checking programs approved by Information Security must be continuously enabled on all servers and networked personal computers (PCs), including home devices when connected to or sharing data with company information systems.

Passwords – Logon Ids

- Each person accessing information and resources within the company's environments will be uniquely identified with a logon ID and corresponding confidential password. Passwords must conform to company standards and must be changed at least once each 90 days.
- Passwords must never be shared or revealed to anyone besides the authorized user. If a user suspects that his or her password has been compromised, or become known to another individual, he / she must change that password immediately and report the incident to Information Security.
- Logon IDs may not be utilized by anyone but the individuals to whom they have been issued. A user must not allow others to perform any activity with his / her Logon ID.

Systems Audit Trail

- Computer systems must produce audit trails that capture events, including Logins, logouts, account creation, account modification, account deletion, changes to access rights or privileges.

Systems Control

- For all business applications and systems infrastructure systems, designers and developers must involve Information Security from the beginning of the systems design process through the production implementation. Information Security approval must be obtained for all new and significantly modified applications.
- Prior to any software evaluation, business areas must contact Information Security for review and approval. It will be the responsibility of Information Security to determine whether or not Information Security needs to be considered during the evaluation of a product.

Traveling with Company Portable Devices

- All company devices such as laptops, notebooks, PDAs, and other transportable computers must not be checked in airline luggage systems. These devices must remain in the possession of the traveler as carry-on baggage. This equipment must not be left unattended.

Reporting Computer Theft

- Any theft of company computing devices or personally owned computing devices that contain company information must be immediately report to Security and Information Security.

VENDOR RISK ASSESSMENT / CONTRACT MANAGEMENT (ENTERPRISE-WIDE)

Vendor Risk Assessment

Determine Data Sensitivity: What data will the vendor have access to?

- None – No data exchanged, no security impact
- Low Risk – Demographic info and projected financial info
- Medium Risk – Names, Addresses, Phone Numbers
- High Risk – Non-public Private Information (SNN, health / medical, financial, proprietary and confidential info, etc.)

Vendor Questionnaire: Does the vendor have policies and procedures? See representative questionnaire attached.

Contract Management

- Include approved language regarding security compliance, privacy safeguarding, intellectual property, and other contract standards in all contracts where risk assessment indicates

SECURE Email

- Use a secure Internet messaging function when transmitting Non-public Private Information
- Outbound email is automatically redirected to a secure, encrypted channel
- Product info: http://tumbleweed.com/products/secure_redirect.html

WEB SITES – ENTERPRISE-WIDE STANDARDS AND GOVERNANCE PROCEDURES

- Apply to all external Web Sites maintained by or for the companies
 - Include all public sites and password-protected sites for external audiences
 - External audiences include customers (individual and institutional), vendors, service providers
- Identify oversight team
 - Include business, legal, and compliance representatives
- Adopt / Update Web Site Standards
- Establish Governance process for compliance with Standards

Representative Standards

- Information Security must be notified of all Web Site projects at the onset of development and must review and approve the information security and privacy safeguarding aspects of the project
- All Web Sites must comply with the organization's Information Security Policies
- "Contact Us" screens and other input forms used by Web Site visitors must be form-based and must be secure (SSL-enabled)
- Web Sites must include approved Privacy / Legal Notices or links to approved Privacy / Legal Notices

SPeRS – STANDARDS AND PROCEDURES FOR ELECTRONIC RECORDS AND SIGNATURES Version 1.0, September, 2003

- Definitive work to date
- Not a technology manual or set of technical standards
- Guidance for conducting business electronically
- A reality check – to identify issues, help with legal compliance, stay within business norms

RESOURCES – INFORMATION SECURITY

Anti-Phishing Working Group, <http://www.anti-phishing.org>

“Committed to wiping out Internet scams and fraud.”

BITS – Financial Services Roundtable, www.bitsinfo.org and www.fsround.org

BITS is a non-profit industry consortium whose members are 100 of the largest financial institutions in the United States. BITS’ mandate: “Facilitate the growth of electronic banking and financial services” and “Sustain consumer confidence and trust by ensuring the safety soundness, privacy, and security of financial transactions,” etc. BITS shares its membership with the Financial Services Roundtable.

CSRC – Computer Security Division: Computer Security Resource Center, <http://csrc.ncsl.nist.gov/>

Sharing information security tools and practices and providing “one-stop” shopping for information security standards and guidelines for the federal agencies and key security web resources to support industry.

RESOURCES – INFORMATION SECURITY

(cont.)

HTCIA – High Technology Crime Investigation Association, <http://www.htcia-ne.org/>

Designed to encourage, promote, aid and effect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership.

ISSA – Information Systems Security Association, <http://www.issa.org/>

A not-for-profit, international organization of information security professionals and practitioners. Provided educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.