IMS Risk Management

Legal K.I.S.S
Keep Information Security Simple

By: Gary Sheehan
Moderated By: Erin Kromann
Agenda

• About IMS
• Today’s Security Issues
• Security Approach - Frameworks
• IMS Project Approach
• Questions
About Integrated Management Services

20+ Years of Client Experience in...

Solving Problems
Creating Solutions
Clarifying Needs
Identifying Environments
IMS Risk Management

SECURITY
- Holistic
- Physical
- Information

BUSINESS CONTINUITY
- ERP
- EPP
- BCP
- Full cycle mgt, training & maintenance

REGULATION & COMPLIANCE
- Including HIPAA, SEC, SOX, FINRA, COBIT, ITIL and more...

DECISION MANAGEMENT
- Strategic Coaching
- Real Options Analysis
- Data in Decision Models

MANAGED SERVICES
- Staffing
- Maintenance
- Cyclical Assessments
Security Issues
# TODAY’S SECURITY ISSUES

<table>
<thead>
<tr>
<th>When</th>
<th>What</th>
<th>Who</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 31, 2010</td>
<td>An unauthorized party obtained the law firm’s login information and accessed consumer credit reports and client information.</td>
<td>Samuels, Green, and Steel, LLP Irvine, California</td>
</tr>
<tr>
<td>September 22, 2010</td>
<td>Mr. LaRocque's home was burglarized on the evening of July 25, 2010. A laptop with names, Social Security numbers, tax identification numbers and other personal information from his family law clients was stolen.</td>
<td>Private Legal Practice Hudson, New Hampshire</td>
</tr>
<tr>
<td>July 27, 2010</td>
<td>An attorney left legal files in a public dumpster. The attorney thought it was appropriate to dispose of the files in this way since the accounts were old and closed. The documents contained names, addresses, bank account information, Social Security numbers, driver's license numbers, and dates of birth.</td>
<td>Private Legal Practice San Antonio, Texas</td>
</tr>
</tbody>
</table>
TODAY’S SECURITY ISSUES

The FBI issued an advisory in November 2009 and again in 2010 that more hackers were using complex e-mail schemes, known as spear phishing, to go after information held by U.S. law firms.

The FBI indicated that network defenses against these attacks could be difficult because they appeared to come from a trusted source and “the subject lines are spoofed.”

Data Security Takes a Backseat At Law Firms
Erin Coe
06/2010
MORE ISSUES FOR LEGAL FIRMS

• It hasn’t happened to us yet
• Law firms are now targets
• Resource issues
• Law firms have the gold
SO WHERE ARE THE ISSUES?

Biggest areas of concern for law firms:
- Technical infrastructure
- Web application security
- Mobile data devices
- Social media sites
- Security Documentation
- Training / awareness
- Client Communication

Stephen Surdu,
Vice President of Professional Services
Mandiant Corp.
ADDRESSING ALL THE ISSUES WITH GRC

**Solution:** Using frameworks to build a GRC program to protect your assets and achieve business goals and objectives.

**Governance:** A risk-based process by which policies are set and decision making is executed.

**Risk Management:** The process for addressing risk with a balance of mitigation through the application of controls, transfer through insurance and acceptance through governance mechanisms.

**Compliance:** The process of adherence to policies, requirements and decisions in order to reduce risk. Includes both voluntary and mandatory requirements.

**Frameworks:** an extensible, risk-based structure for documenting and implementing a set of concepts, processes, methods, technologies, procedures and cultural changes necessary for a complete product.
ADDRESSING THE ISSUES WITH GRC

Using frameworks to build a GRC program and achieve business benefits by driving efficiencies in:

- Knowledge management
- Accountability & responsibility
- IT and business process and workflow
- Security and compliance efforts
- Technology usage
- Managing risk
- Performance management
GRC STRATEGY

Phases

Education  Communication  Documentation  Platform / Application  Measurement
GRC STRATEGY - EDUCATION

- Education leads to Documentation
- Documentation leads to Awareness
- Awareness leads to Interest
- Interest leads to Confidence
- Confidence leads to Action
- Action leads to Ownership
- Ownership leads to Accountability
- Accountability leads to Governance
- Governance leads to Compliance
- Compliance leads to Risk Reduction
- Less Risk leads to Better Security
GRC STRATEGY - COMMUNICATION

• Assemble an IT GRC Steering Committee

• Define what GRC means to your organization.

• Survey your organization's regulatory and compliance landscape.

• Determine the most logical entry point and develop a phased approach.

• Establish a clear business case, considering both short-term and long-term value.

• Determine how success will be measured.
GRC STRATEGY - DOCUMENTATION

Regulations

Best Practices

Frameworks

Audits

Policies

Industry Requirements
Platforms / Applications:

- Enterprise GRC products tend to be all about workflow, with little depth in the area of IT risk assessment and compliance management

- IT GRC products tend to have a lot of depth in terms of very specific controls and requirements that relate directly to regulations and standards. Good ones will include IT process workflow

These two categories represent different products, solving different problems, being sold to different audiences.
IT GRC STRATEGY – PLATFORM / APPLICATION

- IDS / IPS
- Measurement
- Compliance Workflow
- Scanning
- Policy, Standards & Procedures
- Risk
- Awareness
- Learning Management System
- Logging & Monitoring
- BCP Incident Response Disaster Rec.
IT GRC STRATEGY – MEASUREMENT
SUMMARY – K.I.S.S.

Security Issues
Addressing those issues with GRC

“Top-performing companies have enabled competitive differentiation, cost reduction, and organizational growth by implementing IT GRC through a strategic combination of business process integration, education & awareness and software supported analysis”.

Aberdeen Group 2010
IMS Risk Management

Approach
Security Approach

**Spot Assessment**
On-site assessment to gauge firm’s status in terms of desired outcomes, industry standards and best practices at a chosen point in time.

**Impact Analysis**
Identify and measure the potential for, frequency and impact of targeted risks with both binary and relative perspectives.

**Planning & Prioritizing**
Prioritize risks based on severity of impact and importance to the firm’s strategic objectives. Plan remediation or implementation.

**Remediate & Implement**
Remediate risks and implement management plans while maintaining performance within the organization.

**Testing & Maintaining**
Test new systems or processes and develop a plan for monitoring and maintenance.
Complimentary Assessment

The purpose of IMS Complimentary Assessment is to gain a greater understanding of the client’s legal security environment. The objective is to develop an overall assessment of the legal security SWOT.

Next Steps:

- Each party signs an NDA
- Survey and/or interview key stakeholder
Erin E Kromann
Director, IMS Risk Management
ekromann@integratedmgt.com
917-656-7911

Gary Sheehan
Senior Consultant, IMS Risk Management
Sources


• Databreach.com

• http://www.abanet.org/media/youraba/200705/article06.html

• Peter Weill, Director, Center for Information System Research, MIT Sloan School of Management