



Top Down Management Approach To Information Security

Presented by
Beth Chiaiese - Foley & Lardner LLP
Eric Maher – Foley & Lardner LLP
Jamie Herman – Ropes & Gray LLP
Robert Weaver – Blank Rome LLP

#SPEC5



Presenter:

Beth Chiaiese

*Dir, Prof Resp & Compl
Foley & Lardner LLP*



Presenter:

Rob Weaver

*Dir, Information Security
Blank Rome LLP*

Thank you for being here today

August 19, 2014



Presenter:

Jamie Herman

*Mgr, Information Security
Ropes & Gray LLP*



Presenter:

Eric Maher

*Mgr, Information Security
Foley & Lardner LLP*

Thank you for being here today

August 19, 2014

Program Goals



Here's What We Hope to Do Today:

- Give you three different road maps of how to get executive buy-in to make information security a priority
- Will use Foley & Lardner as the case study
- Other panelists from Ropes & Gray and Blank Rome will provide counterpoint
- Lots of time for audience input and questions

Polling Questions



Question # 1 – Use ILTA mobile app or <http://ilta.cnf.io> and use session code: 319

POLL: Where does Information Security report in your firm?

- General Counsel
- Information Technology
- Compliance / Risk Management
- Other

First - Why Now?



The Time Is Ripe To Focus Management's Attention On Information Security

- More:
 - Regulation
 - External risk
 - Internal risk
 - Client pressure
 - Data dispersion
 - Cost pressure
 - Productivity issues

Polling Questions



Question # 2 – Use ILTA mobile app or <http://ilta.cnf.io> and use session code: 319

POLL: How supportive is your firm's management of Information Security?

- Very
- Somewhat
- Slightly
- Not at all

The Foley Case Study



How Foley & Lardner is making Information Security the centerpiece of its Information Governance program

Foley

- Who are we?
- What is Information Governance?
- Is IG a Department or a Function?
- IG v. IT?
- Security as a risk management model
- Executive support for IG and security
- Managing change

Blank Rome and Ropes & Gray

- As we talk, panelists will each provide their firms' approach to these issues
- Why IT and the business should see eye to eye
- Lifecycle, lifecycle, lifecycle...everywhere
- Shadow IT to islands of data

Foley & Lardner LLP



Who we are and where Information Security reports

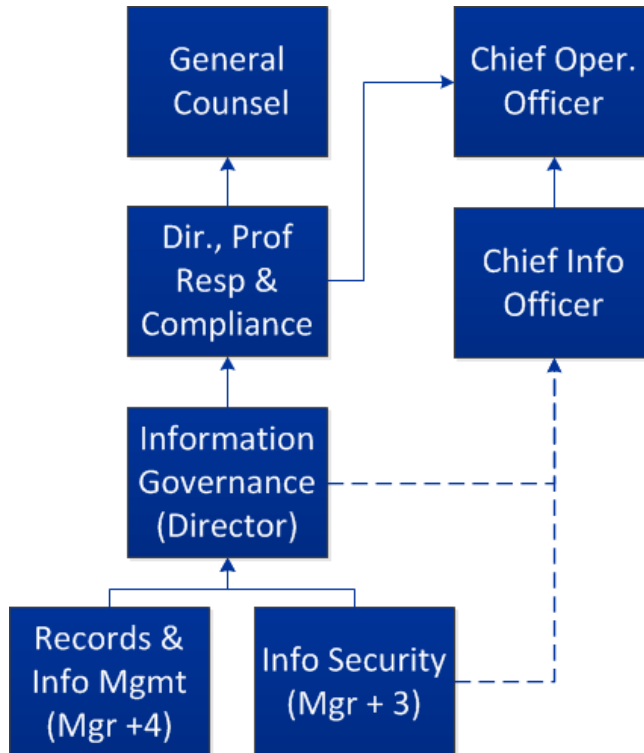
- 17 US offices and 3 international offices
- 847 attorneys (422 partners)
- 3 law departments
 - Litigation
 - Business Law
 - Intellectual Property
- Information Security has a dual reporting structure



Foley – Information Security Reporting



Compliance AND Technology



Polling Questions



Question # 3 – Use ILTA mobile app or <http://ilta.cnf.io> and use session code: 319

POLL: How many personnel are dedicated to Information Security in your organization?

- None – It is “part” of a couple people’s jobs
- 1
- 2
- 3
- 4 or more

Foley Takes An Information Governance Approach



IG is the strategy for making Information Security and Information Management part of the culture

What is Information Governance?

An enterprise-wide approach to the management and protection of a law firm's client and business information assets. An effective IG Program enables lawyers to meet their professional responsibilities regarding client information, recognizes an expanding set of regulatory and privacy requirements that apply to firm and client information, and relies upon a culture of participation and collaboration within the entire firm.

- *Iron Mountain Law Firm Information Management Symposium (2012)*

IG Is Principle-Based



Foley developed 10 Guiding IG Principles. Information Security is at the top.

1. Manage confidential, sensitive or Personal Information as required by law, agreement or Firm Policy
2. Understand third party access requirements
3. Respond promptly to IG Compliance notices
4. File email records regularly
5. Maintain the Firm's Official Records in electronic form, unless hard copy is required
6. Store Official Records in a FLARR¹
7. Organize Official Records by correct client/matter number
8. Retain and destroy records as permitted by Firm Policy
9. Avoid making multiple copies of records
10. Don't handle file transfers (in or out) on your own

¹ Foley & Lardner Approved
Recordkeeping Repository

Is IG A Function Or A Department?



Short Answer – At Foley, it’s both

Foley’s IG Department is responsible for:

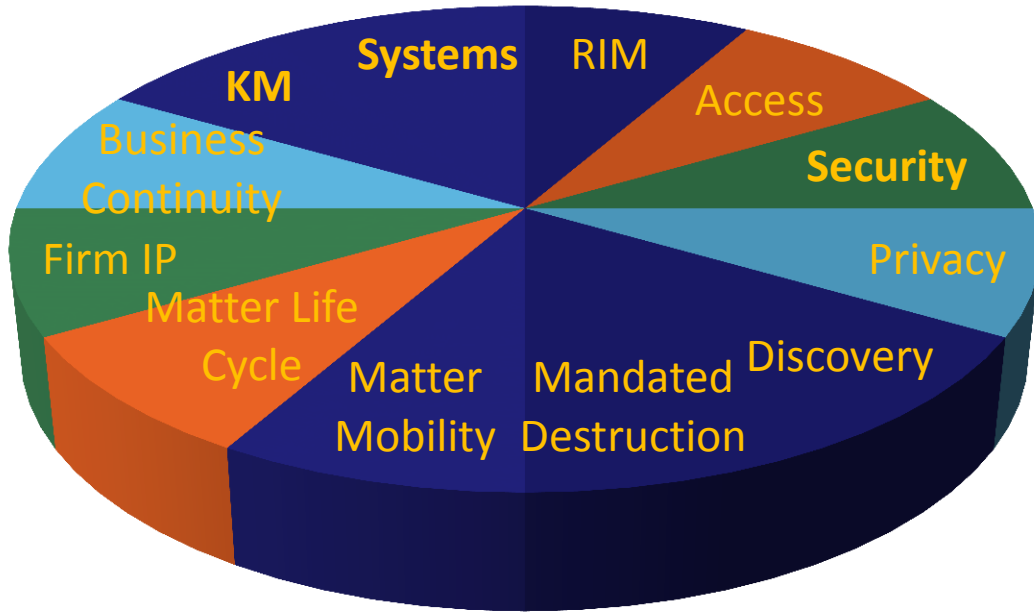
- Importing and exporting information
- Document security, including ethics walls and litigation holds
- Secure retention and disposition of information
- Firm Risk Management
- Vendor Risk Management
- Information Security Infrastructure
- Client Audits

But IG Is Also A Function



IG Principles should be applied to many information management functions

Applies to Client and Business Information



Policies, Auditing, Continuous Improvement

Policies, Auditing, Continuous Improvement

Policies, Auditing, Continuous Improvement

IG v. IT



How is Foley balancing Information Security between IG (Strategy) v. IT (Operations)?

IG – Strategic Goals

- Risk Management Based
- Architectural Role in System and Network Designs
- More Formal Audit Processes
- “Confidentiality and Integrity” Drivers
- Security Consultants to the Firm

IT – Operational Goals

- Operationally Driven
- Project and Break Fix Focused
- “Availability” Motivated

Information Security Risk Model



Foley approaches Information Security as a risk management issue. This helps focus priorities and resources, and the attention of Firm Management.

- ISO 27001 based risk management structure
- Entering year two. First year focused on technology risks, now looking to expand to Firm Data Risk in general.
- Dealing with both successes and challenges.
- Still building the program, and are hoping the move out of IT can help

Risk Management Outside of IT



Separating risk from operations to give Firm Management an accurate picture

Challenges in IT:

- Lack of Firm Management Involvement
- Risk Initiatives Buried in Operational Tasks
- Risk Projects seen as “Security Projects”

Hopes for New IG Structure:

- Risks are Coming from Where Firm Expects
- Separating Risk for Operations
- Firm Management Involvement in Process
- More Mature Model that Clients are Expecting

Polling Questions



Question # 4 – Use ILTA mobile app or <http://ilta.cnf.io> and use session code: 319

POLL: What are your firm's biggest Information Security concerns?

- External hacking
- Internal fraud
- Ethics violations
- Breach of client confidentiality
- Use of personal devices for business purposes
- Visibility into the firm's exposure to risk

Getting Management Support



The real key: Top-down management support for cultural change

Where we are now:

- Very active Information Security Committee
- The GC and the COO support our efforts
- The CEO kind of “gets it”, but helps us communicate
- The Professional Management team also sort of “gets it”
- The message hasn’t penetrated the Management Committee or most lawyers and staff

Where we’re going:

- Information Governance Advisory Group (Policy and Strategy)
 - Executive sponsors: GC and COO
 - Chaired by Director, IG
 - Members include
 - Director, Prof Resp
 - CIO
 - CFO
 - CHRO
 - CMO
 - Key office and practice leaders
- Info Sec Committee remains (Operations)

Polling Questions



Question # 5 – Use ILTA mobile app or <http://ilta.cnf.io> and use session code: 319

POLL: How are you delivering security awareness education at your firm?

- Mandatory classroom training
- Mandatory e-training or educational videos
- Training is optional but strongly encouraged
- Distribute educational materials
- Targeted awareness (email communication) when something comes up
- Not providing any form of security awareness training

Change Management

It's all about education, training and awareness



Principle based awareness programs

- This year: Information Security Awareness Program
 - Monthly theme
 - Stories, articles, case studies
 - SANS videos
 - Presentations (ALAS plus internal)
 - Hands on training (encryption)
 - Connect security to personal life
 - More is better

Audience targets

- Attorneys
- Staff
- Technology Department
- Help Desk
- Everyone

Questions

We'll now open it up for questions

Thank You

