Promoting an Effective InfoSec Program to Senior Management

Law & Liability Track
Session LAW-303
Thursday February 8, 2007
10:40 AM - 11:50 AM

RSA®CONFERENCE2007
FEBRUARY 5-9 | MOSCONE CENTER | SAN FRANCISCO

Promoting an Effective InfoSec Program to Senior Management

Moderator - Ben Rothke, CISSP CISM

Senior Security Consultant, INS, Inc.

Panelists

- Lawrence Dietz – Research Director, The Sageza Group
- Usha Karne - Information Technology Specialist - Office of Systems Security Operations Management (OSSOM)
- Pamela Fredericks - Director, Security Advisory Services - Forsythe Solutions Group

Ben Rothke

Promoting information security

The bitter truth about information security.

- Management often doesn't
  - have time for or truly care about information security
  - understand their infrastructure
  - know how to deal effectively and pragmatically with risk
  - know how to deploy the security software and hardware they just spent a fortune on

Promoting information security

- The challenge:
  - Promoting information security with management who may be inexperienced in the ways of information security
  - Especially when they won’t give you enough staff or budget

Spaf's Law

- Professor Gene Spafford - Purdue University
- Spaf's first principle of security administration:
- *If you have responsibility for security but have no authority to set rules or punish violators, your own role in the organization is to take the blame when something big goes wrong.*

Conclusions

- Promoting selling security requires good selling skills, something most people lack.
- Focus on the business issues, not exclusively on the technical issues.
  - Consider getting an MBA to talk to the CxO's and management in a language they can relate to
- Think outside of the security box

Usha Karne

How you approach?

- Research
- Speak their language
- Incentives

Research

- Why we need the new program
- What are they benefiting
- Similar organizations who are using this approach

Speak their language

- Do not talk about technology
  - Performance
  - Ease of use

- Organizational benefits
  - Increasing customers
  - Publicity

Incentives

- Increase Revenues
  - Systems will not go down because of worms & attacks
  - Employees can process more transactions
- Save Money
  - No more system repairs because of attacks or viruses
  - No system down time compensation
- Publicity
  - Attract more customers
  - Competition edge with similar organizations

Summary

- What they want to hear
- Show indirect gain
- Show possible new business opportunities
- Customer satisfaction

Pamela Fredericks

Approach

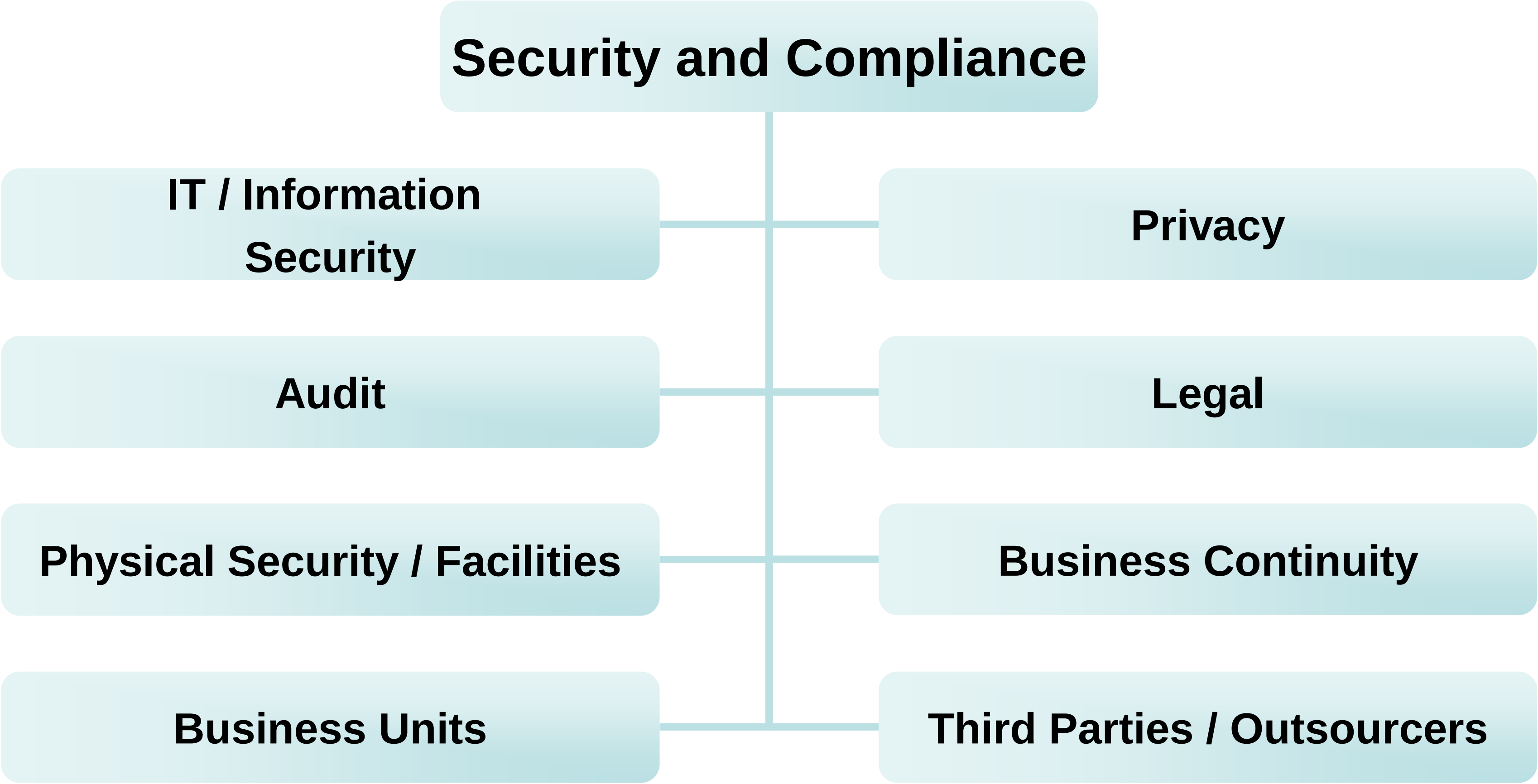
- Management is best reached through a unified approach that links security to privacy, compliance, and audit requirements

Compliance Leads to Security

- Security occupies both the 1st and 2nd priority for technology spending over the next 12 months: Morgan Stanley research
  - Morgan Stanley Equity Research, 1/3/06, Enterprise Technology: Morgan Stanley CIO Survey
- All companies, public and private, resonate on the compliance topic
- Increase in breaches → more legislation → more audits
- Personally Identifiable Information (PII) leads to data classification
- Data protection standards in other countries forcing U.S. to adopt more stringent rules and requirements

Shared Responsibility

Security and Compliance are part of operational risk – a shared responsibility that belongs to many parts of the organization



Security and Compliance

IT / Information Security

Privacy

Audit

Legal

Physical Security / Facilities

Business Continuity

Business Units

Third Parties / Outsourcers

Communicate at the Right Level

Find out where management is in the compliance / audit / security continuum:

Security / Controls Assessment Stage — **set a baseline**

- Define the scope of the security and compliance program
- Identify risks, threats, vulnerabilities, current state

Policy & Processes Stage — **make a statement**

- Document policy, standards, procedures, governance
- Provide awareness and training, user education

Security and Controls Architecture Stage — **apply technology**

- Solutions and products for specific security areas
- Automate manual processes where possible
- Monitoring, detection and incident response

Security Basics

Security & Compliance Requirements for Corporate Data

- Available (BCP)
- Recoverable (DR)
- Confidential (privacy)
- Data Integrity (security controls)
- Accountability (audit & monitoring)

Unifying Approach

- Security is an easy sell if it satisfies **audit** requirements
- Build a model based on commonalities of basic **security and privacy** principles
- Cost savings found by fostering one unified security and **compliance** approach across the organization
- Use standard industry frameworks: COBIT, ITIL, ISO-17799, language auditors are looking for
- Utilize shared responsibility and linkage by involving multiple departments

Lawrence D. Dietz, Esq.

Research Director, The Sageza Group

The Legal Angle On Promoting an Effective Infosec Program to Senior Management

RSA CONFERENCE 2007

FEBRUARY 5-9 | MOSCONE CENTER | SAN FRANCISCO

Executive Management Challenge

- What Do I Need To Do?
  - Organizations everywhere are attempting to cost effectively comply with multiple external & internal mandates
  - In order to protect sensitive customer & personnel data they must understand how to achieve good governance
- How Do I Best Guide My Company To Do It?
  - Employ solid governance and compliance will follow
  - Automatically test controls on a scheduled basis
  - Enforce compliance to prevent data loss
  - Detect failures in security controls in real time
- Who Should I Rely On To Help?
  - Legal
  - Finance
  - Information Security

Legal Position Is Critical

- Legal Exposure is a detriment to market cap
- Exposure of non-compliance with key regulations or the hint of non-compliance will negatively impact the company.
- The Board is personally involved when things go legally wrong.
- Legal liability is increasingly personal liability.
- Understand your international profile and jurisdictions.
  - HP Debacle.

Information Security Not So Critical

- Perceived as a technical problem
- Not generally visible organizationally
- Taken for granted
- Bundled under IT, not considered a part of Governance.
- Isolated from key functional areas: audit, HR, legal, Business Units

How To Break The Log Jam

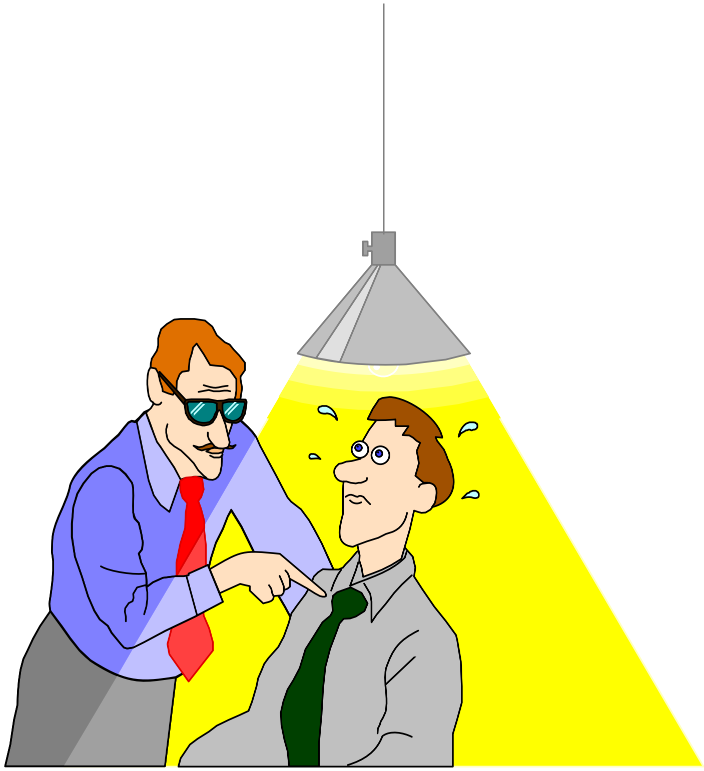
- Relate to the company position as a whole –
  - Where are the intersections between legal and info security?
- Enlist legal as an ally
  - Help them formulate preventative measures.
  - Show how reports in particular can be powerful evidence of compliance.
  - "Coach" legal to showcase information security as a compliance tool.
- Employ the Zig Ziglar philosophy:
  - You can get anything you want if you help others get what they want.

Bad Examples Abound

- HP Board and *Pretexting*
- Sentencing of ex-Worldcom/MCI and Enron executives

Conclusion

- Q&A
- Questions
- Comments



Contact info

- Ben Rothke – ben.rothke@ins.com
- Lawrence Dietz – larry@sageza.com
- Usha Karne - usha.Karne@ssa.gov
- Pamela Fredericks - pfredericks@forsythe.com