The Bottom Line: Helping Information Security Specialists Develop a Head for Business

LYNN McNULTY, CISSP

2010 FISSEA Conference

Agenda

- Discuss how information security is being leveraged as a business enabler
- Talk about the relationship between the security professional and the bottom line manager
- Provide thoughts on how to prepare for the role of business enabler
- Discuss the role of certifications

Background

- IT security people have historically occupied the position of being the disabler or Mr./Ms. NO!
- We have couched our arguments too often in in technical terms—not business terms
- Part of the problem is that security people have been organizationally placed as to be ineffective

Today's Environment

- IT is viewed as the "great silver bullet" that will solve most of society's problems
- Quick review of representative programs:

  --Preventing terrorism

  --Healthcare reform

  --Smart grid

  --Government reinvention at all levels
- The challenge of security professionals is how to get out in front of the leadership curve

Security as a Business Enabler

- We operate in fire fighting mode—focused on the last breech, the last malware problem, the last intrusion, last years FISMA report, etc
- Meanwhile the business leadership is focused on the future—the strategic plan, next year's budget, the opportunities created by new technology, etc.
- Need to integrate a forward looking, holistic approach to security management into existing program

How to Achieve This Objective

- Need to adopt a forward looking and thinking approach to the other parts of the enterprise
- Start reading the strategic plan, looking at the future budget documents, reading the publications that the senior managers are reading, go to future oriented conferences—i.e. get involved with the future
- Reach out to the change agents/line of business managers in your organization

Risk Management as the Common Language

- Risk management as a concept has been discussed and advocated for many years without a lot of success
- New emphasis on RM provides security people with the opportunity to engage the business side of the enterprise
- 800-53 and related documents provide a common basis for addressing enterprise-wide business applications
- Need to evolve from security guys and gals to risk management professionals

Benefits of a Risk Management Approach

- Get out of the application silo approach to security—focus on big picture and talk in management terms
- Provide a forward looking view of the enterprise security environment
- Provide an analytical framework for addressing and SOLVING security problems inherent in future programs in a cost effective manager

Individual Preparation

- Avoid the "Tastes Great, Less Filling" debate about whether security is a technical or a managerial issue—it's both
- Take some business oriented classes at your local college or university
- Read the business oriented publication—HBR, Business Week, Fortune, etc.
- Attend business/strategic program focused conferences
- Talk to your line of business managers

What is Going on in the Development of a Federal RM Workforce

- Various initiatives underway with respect to the federal IT security workforce
- Seem to be focused on differentiating the more technical aspects of the profession—some mention of risk management
- I would argue that greater emphasis on risk management is needed
- Need to look at 800-53 and related documents and determine if we have the requisite skills
- Need to differentiate between tactical and strategic risk management

Role of Certifications

- Nice to have if you work in field, but mandatory if you work at DoD
- No one certification is going to qualify you to validate your ability to work effectively with the business leaders in the enterprise—MBA is not a certification
- (ISC)^2 CAP certification is evolving towards a RM approach—based on NIST body of doctrine
- Look at other certs in fields of project management, privacy, etc.

Personal Note

- It has been my pleasure to watch FISSEA grow and develop over the years.
- I was involved with the beginnings of this organization during my tenure at NIST
- I will be moving into full retirement over the next few months.
- As you know I have been involved with (ISC)2 for a number of years. Marc Noble, CISSP, former CISO at FCC, is the new Director of Government Affairs.