



**Minnesota Information Professional Society
2006 Education Seminar
Hamline University
May 3, 2006**

Risk Management

**Presentation Outline
and
Speaker Information**

MIKE BENKOVICH
Keynote Speaker
Perzel and Associates

STEVE QUIGLEY
Positioning IT for Success in Disaster Recovery Planning
Clear North

OUTLINE:

Disaster Recovery (DR) & Business Continuity (BC) practice

- ?? We proceed from the assumption that everybody's business is different in terms of their operations (e.g., retail vs. manufacturing vs. financial), customer 'touches', costs of downtime, available IT & other infrastructure, importance of data, etc.)
- ?? Critical - work with IT and the business to define Recovery Time Objectives (RTO) **and** Recovery Point Objectives (RPO)
- ?? Define DR versus BC for the business and demonstrate the variance in costs between modest vs. aggressive RTO & RPO
- ?? Define critical applications and critical users
- ?? Define probability of various disasters (helps focus on potential solutions)
- ?? Understand that most DR/BC solutions are different in some way between companies - not trying to apply a single solution
- ?? Will develop the plan & implement
- ?? Flexibility to work with other partners as needed
- ?? Test, test, test

BIO:

Steve Quigley has been in the information technology industry for over twenty years. He's spent the majority of the past decade providing infrastructure support & technology consulting for medium and small businesses with Clear North Technologies.

Steve began his career with IBM back in 1985 and worked with various business units that included the IBM PC Company, EduQuest (K-12) and the Federal Systems Division. He later worked with other local technology companies in a variety of areas that included software distribution, application hosting, and one of the early Application Service providers. BlueCross BlueShield of Minnesota also provided experience aligning an IT services group to help select BCBS business units meet their business goals.

In partnership with two other IBM co-workers, Steve was also a principal in an auto service business. Collectively, these experiences have helped Steve develop the ability to recommend & apply technology solutions that make business sense to clients while also reinforcing the importance of technology to the senior leadership of those businesses.

DARLENE TESTER
Regulatory Compliance and Liability – Who Goes to Jail and When?
Carlson Marketing



OUTLINE:

Regulatory Compliance and Liability – Who Goes to Jail and When?

1. Introduction
 - a. What are the most common regulatory and statutory requirements around security and privacy
 - b. What requirements are/should be easy to implement
 - c. Which requirements are more complex to implement
2. Liability
 - a. What are compensating controls
 - b. What proof of liability is there
 - c. What caselaw may be used to point the finger of liability
3. Compliance
 - a. What should be done
 - b. What is most likely being done
 - c. Where the gap is between the two
4. Summary
 - a. What are the requirements
 - b. What needs to be done at a minimum
 - c. What may be on the horizon

BIO:

Darlene Tester has been in the information security field for 28 years. She is currently the Director of Information Security & Controls at Carlson Marketing. She has developed and implemented sound security programs for banks, brokerage firms, healthcare companies, and other organizations managing confidential consumer information. She is a certified information security professional with CISSP, CISM, CHSS certifications as well as certifications in ITIL and the international security standard ISO17799. She has written a book on building sound security practices and she is an attorney with a background in regulatory compliance and IT law.

In this age of personal information exchange in electronic format, Tester brings expertise in financial fraud investigations and identity theft awareness. She has been a national speaker on legal liability and security implementation, financial fraud issues, and has held consumer seminars on how to reduce the risk of identity theft. She has written college curriculum for degree programs in e-crime, computer forensics and information security and given seminars to law enforcement on e-crime identification and investigation.

JAMES DANBURG
PCI, SOX, HIPAA, and et al.:
How to integrate these mandates with present & future IT/IS initiatives.
A philosophy of “Continuity of Compliance**” (or How IT/IS gets a real Business Mission).**

OUTLINE:

- 1) A brief on timeline of events, threats & various mandates
 - a) SSS
 - b) SOX, HIPAA, PIPEDA,
 - c) PCI-DSS
 - d) Basel II
- 2) PCI-DSS
 - a) PCI: Merchant Mandate
 - b) Potential impact
 - c) Requirement of compliance
- 3) Common IT/IS Initiatives & their potential “collisions with the mandates”
 - a) System Interoperability (SOA tools)
 - b) Mobile Enablement of Applications
 - c) VOIP
- 4) Continuity of Compliance (a new Business Mission for IT/IS)
 - a) Using Mandates as Templates
 - b) Creating Synergy with CXO's
 - c) IT/IS as the ongoing “Watchdog's of the Enterprise”
- 5) Summary

BIO:

Mr. Danburg is a **Business Process Solutions Architect**, with over 25 years experience in the technology field and with over 20 years Business Development experience in various industries. With the following areas of specialization: Business Process Analysis, Infrastructure Planning (all elements) and the Fulfillment of Business Needs via Technical Solutions. With his broad understanding of technology, and the ability to communicate successfully with both Executives and Technical Specialists, Mr. Danburg has been consistently recognized as some one who not only can “Connect the Dots”, but also “who can bring everyone in the equation” to a workable and agreeable solution. Most recently he was with a firm that was heavily involved in Data Privacy issues and Risk Mitigation technology.

Mr. Danburg served in the USAF as an Operations & Data Flow Analyst in a National Defense Class One Data Center, which was the hub of a Global Data Gathering Network. Performing real time Data Flow Analysis and reacting to National Command Authority Information Requirements 24 by 7. Also, as a shift lead, COMSEC NCO he was responsible for actually building and routing all data via the MDL (Message Distribution Library).

WENDALL REIMER
Integrating Security into Software Development Lifecycle
Midwave



OUTLINE:

- Why do we care?
 - Integrating security into SDLC
 - What are the benefits?
 - Microsoft Principle
- Project conception/initialization
- Requirements gathering
- Design
- Build/Test
- Implementation/Ongoing Support

BIO:

Mr. Reimer is an experienced information security executive with extensive experience in developing and leading enterprise information security programs for Fortune 500 class companies. He has broad and deep knowledge of information security risks and solutions, as well as regulations that impact how companies approach security and audit compliance. Mr. Reimer developed and implemented successful information security programs at two large, international companies. These programs were directly aligned with overall business objectives and reviewed regularly by executive management and the Board of Directors. He has implemented processes that were aligned with company culture, environment and tolerance levels. He brings strong leadership and communication skills across all areas and levels of an organization. Mr. Reimer has leadership experience in multiple areas of information technology with a successful track record of mentoring and coaching employees and peers.

JAMIE BJERKE
OCTAVE Risk Management Methodology
IST



OUTLINE:

Security Risk Assessment: OCTAVE Methodology Overview

Introduction: Threat and Vulnerability State

OCTAVE Defined

- Founding Principles

- Objectives of the Initiative

OCTAVE In Action

- Preparing for an OCTAVE Assessment

- OCTAVE Assessment Process

- Outcomes

Conclusion/Q & A

BIO:

Jamie Bjerke is a Senior Security Consultant at Information Security Technology, Inc. (IST) located in St. Paul, MN. Jamie's focus is delivering security services to IST clients. Prior to joining IST, Jamie worked as a Senior Technology Consultant at Accudata Systems Inc. There he served as the technical lead in security consulting engagements in the areas of security assessments, security architecture and design and security technology deployments for enterprise customers.

Jamie's earlier security work included team leader for Exxon Mobil's External Connections team, leading a group of security engineers. This team was responsible for global external connection standards and practices concerning third party network connections to Exxon Mobil, including Internet connectivity. While at Exxon Mobil, Jamie also served as a technical team lead for Exxon Mobil's global remote access infrastructure, as well as an engineer in the global data-networking group.

BRAD PINT
The Role of Insurance In Risk Assignment
AsteRisk Managers, Inc.

AARON MOLENAAR
Hennepin County DR/BCP Planning
Hennepin County



OUTLINE:

Aaron Molenaar will describe several large continuity and recovery efforts underway at Hennepin County, how their interaction will lead to better overall service for the county, and the key technologies that IT is implementing to provide greater continuity and recoverability of county information systems

BIO:

Aaron Molenaar is a Business Continuity Planner and Consulting Security Specialist for Hennepin County, where he leads IT Continuity efforts and lends his expertise to enterprise projects like security policy, awareness, architecture, and implementations. He has spent 14 years in the IT field, the last 8 of which have been dedicated to information security, disaster recovery and business continuity.

Aaron has an A.A. degree from North Hennepin Community College, is a board member for the Minnesota chapter of the Information Systems Security Association (ISSA) and a general member of the Business Continuity Planners Association (BCPA).

DEB DOFFING
Data Risk and Internal Security
Nextel

OUTLINE:

Protecting Data - Where to start?

5 Risk Management Steps

--1 Identify Critical Information

--2 Conduct a Threat Analysis

--3 Conduct a Vulnerability Assessment

--4 Assess the risks discovered

--5 Recommend and implement countermeasures

Risk Management and Control (Cobra model)

--Deterrent Controls

--Detective Controls

--Preventative Controls

--Corrective Controls

Managing Change

BARRY CAPLIN
Lifecycle Management Risk
State of Minnesota – DHS

OUTLINE:

Information Security Risk Management through the Information Lifecycle Management Process (ISM in the ILM)

A mature Information Security Management program handles many issues and areas of risk within the Enterprise. Information Lifecycle Management refers to the process through which information traverses the Enterprise from conception, through development, operations and maintenance, and to disposal. When these two disciplines collide, opportunities abound to advance the profile of the Information Security program, engage business areas in Information Security processes and provide Senior Management with the documentation they need to make informed Risk Management decisions. This presentation will examine the phases of the Information Lifecycle Management process and provide examples of appropriate Information Security programs, tools and techniques, including Risk Analysis, Vulnerability Analysis and IT Audit.

BIO:

Barry is the Chief Information Security Officer for the MN Dept. of Human Services. He joined DHS in mid 2003 and is responsible for information security department-wide and the security technologies operating within the department, including the development and implementation of department-wide security policy, security architecture, and consistent standards and procedures. This is a balancing act, supporting the department's business objectives with the many difficult security challenges and compliance efforts relating to federal and state statutory and regulatory requirements, such as HIPAA and the MN Data Practices Act.

Barry has more than 20 years of experience in information technology and security. He has worked in information technology positions at US Bank, US West/Qwest, Boeing Computer Services and United Technologies. He holds a master's degree in applied mathematics from Virginia Polytechnic Institute and a bachelor's degree in mathematics and computer science from the State University of New York at Binghamton. He is a certified information systems security professional (CISSP), an information systems security management professional (ISSMP), a certified information systems auditor (CISA), a certified information security manager (CISM) and is active in the Minnesota chapters of InfraGard, the Information Systems Security Association (ISSA), and the Information Systems Audit and Control Association (ISACA).
