Where the Rubber Meets the Road
In Risk Management


Agenda

• Introductions – The Players
• How was Information Security and Business Continuity defined for the project?
• How was the solution formulated?
• What were the outcomes?
• What were the lessons learned on trying to integrate these programs?

Introductions: The Players

• Bridgestone Americas Holding, Inc. – Nashville, TN
• Bridgestone Firestone Information Services (BFIS) – Akron, OH
• Deloitte & Touche LLP
• Begins with appropriate policies, standards, guidelines and procedures.
• Progresses through logical and physical tools and techniques to protect data from various threats.
• Incident management at its most serious level is where disaster recovery and business continuity meet the operations of the business.

How was the solution formulated?

• Needs:
  – Create world class information security program from a program that was evolving and somewhat distributed
  – Expedite the development of a business continuity management program to support existing DR strategies
• Solution:
  – Integrate a comprehensive information security architecture with proven business continuity management approach into a single unified information protection program
Information Security Architecture

Perimeter Network
- Security
- Applications
- Facilities
- Specialized Architectures

Internal Network
- Security
- Applications
- Facilities
- Specialized Architectures

Applications
- Security
- Applications
- Facilities
- Specialized Architectures

Facilities
- Security
- Applications
- Facilities
- Specialized Architectures

System Development Lifecycle
- Process Enhancement
- Project Management
- Change Control
- Production Readiness
- Architecture Standards
- Help Desk
- Incident Response
- Compliance

Security Foundation
- Strategic Business Drivers
- Security Strategy
- Policy
- Legal/Regulatory Requirements
- Desired Risk Profile

Privacy Blueprint
- Information & Asset Baseline
- Physical & Environmental
- Systems & Network Infrastructure
- Logging, Monitoring & Reporting
- Infrastructure Blueprint

Identity Management Blueprint
- Information & Asset Baseline
- Physical & Environmental
- Systems & Network Infrastructure
- Logging, Monitoring & Reporting
- Infrastructure Blueprint

Application Integrity Blueprint
- Information & Asset Baseline
- Physical & Environmental
- Systems & Network Infrastructure
- Logging, Monitoring & Reporting
- Infrastructure Blueprint

Infrastructure Blueprint
- Information & Asset Baseline
- Physical & Environmental
- Systems & Network Infrastructure
- Logging, Monitoring & Reporting

Business Continuity Management Blueprint
- Resource Acquisition & Implementation
- Training
- Testing

Customizable, Yet Standards-Based BCM Approach

Approach to Business Continuity Management

Analyze
- Current State Assessment
- Risk Assessment
- Business Impact Analysis

Develop
- Governance
- Availability & Repeatability Strategies
- Procedures

Implement
- Resource Acquisition & Implementation
- Training
- Testing

Continuous Improvement/Quality Assurance

Roadmap to an Effective Security Capability

Strategic Alignment
- Security Governance
- Risk Management Framework

Physical Resource Protection
- Physical Security

Information Resource Protection
- Information Security

Business Continuity Management
- Security Management
- User Management

Policies & Standards
- Executive Policies

Awareness & Training
- Employee Training
- Executive Briefings

Business Strategy, Business Continuity
- Business Strategy
- Business Continuity

User Support
- Help Desk

Management & Operations
- System Development

Compliance
- ISO/IEC 17799

TAILORED BEST PRACTICES
Who: IT Oversight Committee

- Purpose: This committee will provide direct accountability to the top of the organization for IT strategic, control and operational decisions that affect more than a single unit of the Bridgestone Americas (BSA) organization.

- Membership (2005):
  - Controller and VP Finance, (BSA)
  - VP IT, BSA
  - G.M. BFIS (Akron Data Center)
  - Director BFIS (Nashville Infrastructure)
  - IT Development Director, BFNT
  - IT Development Director, BSAH
  - IT Director, BFRC
  - General Counsel, BFDP (non-voting)
  - Director of Internal Audit, BSA (non-voting)

Information Technology Security Program (ITSP) - Approach

- Governance
  - Risk Assessment: Identification and prioritization of threats and vulnerabilities.
  - Threat Impact: Analysis of the potential impact of threats on the organization.
  - Security Controls: Selection and implementation of controls to mitigate risks.

- Security Controls Implementation
  - Define Security Strategy: Planning and aligning security initiatives with business goals.
  - Security Controls: Implementation of security measures to protect against threats.
  - Testing: Validation of security controls through testing and evaluation.

- Monitoring & Maintenance
  - Compliance & Audit: Ensuring adherence to security policies and regulations.

The Enterprise Security program needed to ...

- Link the necessary organizational, technical, administrative, and physical security controls
- Include a strategic combination of business drivers, legal and regulatory requirements, and threat scenarios
- Ensure that all tools and techniques are operationally integrated within the overall IT architecture, business processes and business culture.
**Strategic Alignment**

**Key Components**
- Executive Level Sponsorship
  - Risk Tolerance workshop
  - Chief Security Officer
- Risk Profile
  - Threat orientation
  - Current state assessment
  - Risk Tolerance
  - Change readiness assessment
- Security Strategy
  - Business and IT strategies
  - Business and regulatory drivers
  - “To Be” security framework
  - Business driven improvement portfolio
  - Roadmap
  - 3 year operating model

**Key Considerations**
- Active executive participation
- Owner, custodian, stakeholder alignment
- Assigned responsibility, accountability and authority
- Security Life Cycle
- Business and IT alignment
- Security process and management fundamentals/standards/lifecycle versus “wants”
- Compliance with regulatory requirements and initiatives

**Business Enablement**

**Key Components**
- Security Solution Diagnostic
  - Policy and Standards
  - Organizational Alignment
  - Technical Control Architecture
  - Process Alignment
  - Awareness and Training
  - Compliance and Assurance
- Security Solution Methodologies
  - Information Security Risk Assessment
  - System Analysis and Design

**Key Considerations**
- People, process and technology driven requirements
- Cognitive application of solutions models
- Security Blueprints practically applied to relevant aspects of a business operation – network, processes, etc.

**Corporate Security Policy Framework**

<table>
<thead>
<tr>
<th>Policy</th>
<th>Standards &amp; Guidelines</th>
<th>Procedures</th>
</tr>
</thead>
</table>

**Definition**
- Policies are high level statements communicating management’s guidance on issues of security and business risk.
- Security standards and guidelines provide detailed mandatory (mandatory) and discretionary/optional (optional) guidance to personnel in protecting company information and carrying out their job responsibilities.
- Security procedures provide prescriptive guidance on steps to take in order to comply with security policies, standards and guidelines.

**Characteristics**
- Mandatory
- High-level statements
- Vendor and product independent
- Modified infrequently

- Mandatory (Standards)
- Discretionary (Guidelines)
- Detailed statements
- May include vendor and product names
- Modified more frequently than security policies

- Discretionary or Mandatory
- Detailed
- Modified frequently

© 2006 Deloitte Development LLC. All rights reserved.
KEY COMPONENTS

- Security Management Blueprint
  - Program, Organization, Administration
- Business Continuity Management Blueprint
- Infrastructure Security Blueprint
  - Information and Asset Baseline
  - Physical and Environmental Systems & Network Infrastructure
  - Logging, Monitoring & Reporting
- Application Integrity Blueprint
- Identity Management Blueprint
- Privacy Blueprint

KEY CONSIDERATIONS

- Active executive participation
- Owner, custodian, stakeholder alignment
- Assigned responsibility, accountability and authority
- Security Life Cycle
- Business and IT alignment
- Security process and management fundamentals/foundations/baseline versus with 'wants'
**Business Continuity Management Program (BCMP) - Approach**

<table>
<thead>
<tr>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Assessment</strong></td>
</tr>
<tr>
<td>MRI - BMAC - NCSC - NIST - VA</td>
</tr>
<tr>
<td><strong>Business Impact Analysis</strong></td>
</tr>
<tr>
<td>Using regional/market intelligence and information management to determine what services and resources are needed to support critical business activities</td>
</tr>
<tr>
<td><strong>Recovery Strategy</strong></td>
</tr>
<tr>
<td>Identification of recovery techniques and solutions, and development of contingency plans</td>
</tr>
<tr>
<td><strong>Recovery Planning</strong></td>
</tr>
<tr>
<td>Identifying recovery techniques and solutions for use in the event of an interruption and strategies for limiting damage</td>
</tr>
<tr>
<td><strong>Testing</strong></td>
</tr>
<tr>
<td>Development of testing and exercise procedures and availability of the BCM function</td>
</tr>
<tr>
<td><strong>Maintenance</strong></td>
</tr>
<tr>
<td>Continuous development and maintenance of the BCM program</td>
</tr>
</tbody>
</table>

**Compliance & Audit**

**Overall Business Continuity Objectives**

- **Viability**
  - Keeping the company in business
- **Earnings/Profit Protection**
  - Protecting the Enterprise' Financial Commitments
- **Continuing New Business**
  - Preserving the ability to sell in the marketplace
- **Brand Protection**
  - Avoiding public embarrassment and loss of credibility

**Considerations for BCM Program**

- Increased Focus by Regulatory Bodies
- Safeguarding Customer Interests
- Safeguarding Assets
- Rapidly Evolving Technology Capabilities
- Risk Management
  - Continued support available to provide resiliency for primary operations
  - Understanding the need for measuring and monitoring enterprise risk
  - The need to mitigate all critical failures of the BCM Program
  - Attention must be given to all aspects of risk management, including the risk management functions of vendors & suppliers

**Compliance & Audit**

- Viability
  - Keeping the company in business
- Earnings/Profit Protection
  - Protecting the Enterprise’ Financial Commitments
- Continuing New Business
  - Preserving the ability to sell in the marketplace
- Brand Protection
  - Avoiding public embarrassment and loss of credibility

**Risk Management**

- Enhanced view of the business to improve the ability to respond to emerging opportunities
- Continuous review of the need for measuring and monitoring enterprise risk
- The need to mitigate all critical failures of the BCM Program
- Attention must be given to all aspects of risk management, including the risk management functions of vendors & suppliers
**Strategy Development Methodology**

- **Strategy Drivers** are the 4 failed sites. Communications. Emergency. Transportation. Utilities.
- **Impact**:
  - Reduced tolerance for threat from intentional acts of terrorism.
  - Increased regulatory scrutiny.
  - Consolidation and globalization.
  - Integration.
- **Opportunity**:
  - Cost optimization.
  - Scalability.
  - Interoperability.
  - Security.
  - Availability.
  - Performance.
- **Paralysis Point** at risk.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>Communications</td>
<td>Personnel Deployment</td>
<td>Governance</td>
<td>Crisis Management</td>
<td>Testing Strategy</td>
<td></td>
</tr>
</tbody>
</table>

**Process Enhancement**

**Key Components**
- Security Criteria
  - Standards
- Core Enterprise Processes
  - Architecture, Engineering
  - Project Management
  - Risk Management
  - IT Operations Management
- Security Champions
  - Subject Matter Experts
  - Awareness & Training
  - Security Communication Portal
  - Self Service
  - Knowledge Management

**Key Considerations**
- Key security standards, model and criteria proactively championed through existing enterprise-wide management processes.
- Incentive concept to promote security staff as enablers versus roadblocks.
- Roles and responsibilities clearly defined and championed.
KEY COMPONENTS

• Key Performance Indicators
  – High Risk Elements
  – Critical Resources
  – Core Management Processes
  – Customer Satisfaction
• Information Structure
  – Presentation and Reporting
  – Metrics
  – Data Abstraction
  – Source Data
• Compliance Monitoring
  – Internal and External Audit Plans
  – Regulatory
  – IT Scanning / Self-Assessments

KEY CONSIDERATIONS

• Focus on a few critical objective indicators that truly enhance visibility
• Internal audit alignment
• Communication of successes/failures
• Service Level Agreements (SLA) for customer satisfaction
• IT Return on Investment (ROI)
• Critical vendor maintenance contracts
• Metrics for day-to-day operations
• Reporting timelines
• Existing balanced scorecard system

Outcomes

• Complete set of Information Security Policies, Standards and Procedures
• Implementation plans for logical security tools supporting the defined policies and procedures
• Monitoring processes were developed to ensure ongoing compliance
• Risk Assessment/BIA process was implemented
• BCM Strategies and Procedures were documented and stored in Strohl Systems LDRPS

Lessons Learned

• Efficiencies can be gained by combining oversight for information security and business continuity
• Centralizing the policies, standards and guidelines promote effective decentralized implementations of security mechanisms in a consistent manner
• Monitoring is critical, but preventive controls preferred
• IT service providers need their own BCM beyond DRP
• IT can start the process, but the business must own, support and drive the program
• Consultants provide independence, thought leadership and proven methods for expediting what was not getting done internally in both information security as well as BCM
Deloitte, one of the nation's leading professional services firms, provides audit, tax, consulting, and financial advisory services through nearly 120,000 people worldwide, our member firms, including their affiliates, deliver services in four professional areas: audit, tax, consulting, and financial advisory services. Known as an employer of choice for innovative human resources programs, the firm is dedicated to helping its clients and its people excel. "Deloitte" refers to the associated partnerships of Deloitte & Touche USA LLP (Deloitte & Touche LLP and Deloitte Touche Tohmatsu Company) and subsidiaries. Deloitte is the U.S. member firm of Deloitte Touche Tohmatsu. For more information, please visit Deloitte's Web site at www.deloitte.com.