

INFORMATION TECHNOLOGY

Southern's Approach to IT Compliance

Russ Elder, IT Risk Mgt and Compliance Mgr

Agenda

- Southern Company Overview
- Target Zero
- Risk Identification
- Risk Management
- Regulatory Environment
- GRC Tools
- Focus Areas
 - SOX
 - Critical Infrastructure Protection (CIP)
 - E-Discovery / Email Archive

Southern Company Overview

- One of the largest producers of electricity in the United States
- Service territory of 120,000-square-mile area spanning over
 - Georgia
 - Alabama
 - Southeastern Mississippi
 - The panhandle region of Florida.

Target Zero Message



A safety poster with a green and yellow gradient background. At the top left is a logo of a cross with a heart inside, labeled "Safety and Health". The main text reads "Buckle up. It's the law." in yellow, followed by "SEATBELTS" in large black letters and "SAVE LIVES" in large yellow letters. At the bottom left is the "target ZERO" logo with the tagline "Every day, every job, safely." and at the bottom right is the "SOUTHERN COMPANY" logo.

Safety and Health

Buckle up. It's the law.

SEATBELTS

SAVE LIVES

target
ZERO
Every day, every job, safely.™

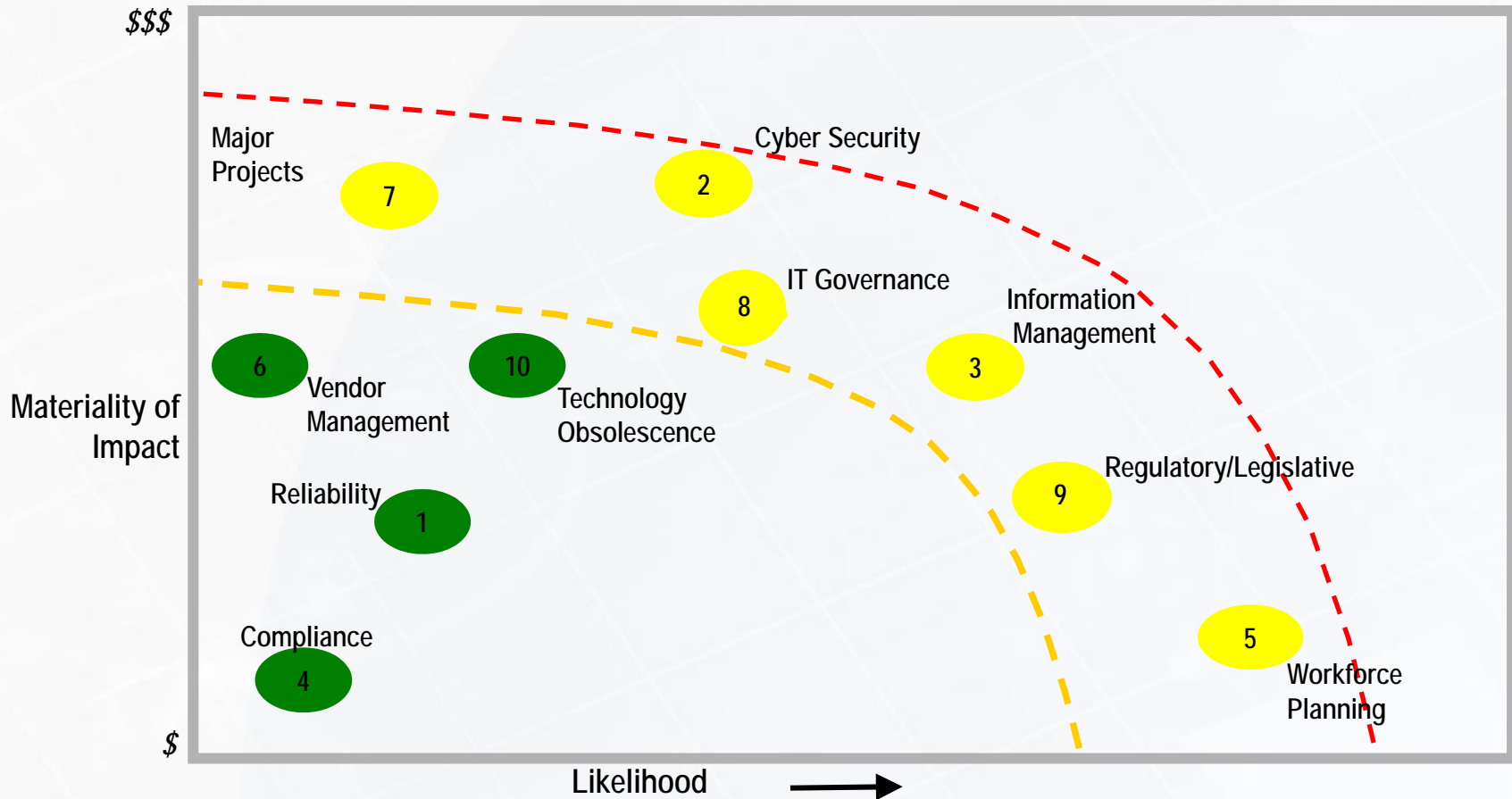
SOUTHERN
COMPANY

Risk Identification

- Partner with Enterprise Risk Mgt Group
- Interview Senior IT Management
- Review with Internal and External Audit
- End product is the IT Risk Profile, which is updated twice a year
- Compliance viewed as a risk category

INFORMATION TECHNOLOGY

Risk Profile Example



Risk Management

- IT Risk Management Steering Committee (Monthly Meeting)
- Each risk category on the Risk Profile is discussed
 - Metrics
 - Initiatives
 - Controls
- Other topics include operational incidents, internal audits, SOX, internal policy compliance, etc.

Compliance Risk

- Philosophy: Manage risk appropriately and be able to demonstrate it.
- Challenge: Knowing what requirements are applicable to your operations and staying abreast of changes
 - Legal
 - Compliance
 - Auditing
 - External Affairs
 - Unified Compliance Framework

What will be the next compliance issues?

- New technologies
 - Cloud computing
 - SmartGrid
 - Virtualization
- Changing regulations
- New threats

Potential Regulatory Impacts - Example

Regulation	Business Units Impacted						Timeframe	Scope		Summary	
	IT	Generation	Nuclear	Transmission	Distribution	Customer Svcs		LINC	Physical Security		Cyber Security
Reliability / Generation											
GRID Act (Grid Reliability and Infrastructure Defense Act) Alias: H.R. 5026; Markey Bill (replaces H.R. 2165) <i>Origin: Congress</i>	✓	✓	✓	✓	✓			Apr2010: In Committee	✓	✓	This is an amendment to the Federal Power Act, section 215, granting the President and FERC new authority to address threats and vulnerabilities to the grid. Authority provisions are included for multiple threats to the grid, including physical security, cyber security , electromagnetic pulses, and geomagnetic storms. The act also requires expansion of transformer sharing programs and grants FERC authority over distribution for facilities deemed critical to the nation's defense by the President. <u>IT Impact: FERC will issue Cyber Security standards for systems that support the transmission of electricity.</u>
National SmartGrid Development Plan <i>Origin: Congress</i>	✓			✓	✓			Unknown	✓		Numerous proceedings, drafts and bills regarding standards, management practices, customer data issues and access to spectrum, etc. associated with the enhancement of the energy grid. Includes: Smart Grid Facilitation Act of 2007 H.R.3237; Energy Independence and Security Act (EISA) of 2007 H.R.6; Energy Storage Technology Advancement Act of 2007 H.R.3776; Renewable Energy and Energy Conservation Tax Act of 2007 H.R.3221; American Clean Energy and Security Act of 2009 H.R.2454. <u>IT Impact: Several initiatives that will deal with protecting and storing Customer Data as well as Cyber Security standards for energy related systems.</u>

Significant events can drive regulation

- Northeast Blackout of 2003
- Started around 4:00 P.M., August 14, 2003. Power restoration takes from hours to days.
- The blackout affected an estimated 10M people in Ontario and 45M people in 8 states.
- The main cause was high-voltage lines coming into contact with "overgrown trees".



Blackout of 2003

- The cascading effect resulted in the forced shutdown of more than 100 power plants.
- The failure highlighted certain power grid vulnerabilities.
- Led to changes in U.S. and Canadian energy policy
 - Increased emphasis on Reliability.

GRC Tools

- Our goal: Manage all key Risks in a single tool that maps the risk to controls and applicable regulations
- Spreadsheets not manageable
- Currently , Bwise used for Enterprise SOX reporting
- Evaluating using Bwise for IT GRC tools vs. IT specific GRC tool

Examples of Specific Compliance / Control Activities

- SOX
- Critical Infrastructure Protection
- E-Discovery / Email Archive
- Post Critiques

INFORMATION TECHNOLOGY

Sarbanes Oxley

IT SOX Control Breakdown

There are 18 General SOX Controls to which IT attests. These controls are tested across several areas.

Control Breakdown

	General Controls	Gen IT	SNC IT	SCS IT	LINC IT	Total
Change Management	3	6	3	8	3	20
Logical Access	9	38	0	54	15	110
Operational	6	5	2	8	3	18
Total	18	49	5	70	21	145

Operational Environments

Windows Unix Mainframe

Batch Job Schedulers

Autosys Cron (SCS) Opalis DTS
Jobtrac Cron (GEN) INFORMATICA

Key Financial Tools

Cool Comp. Netcool BiztalkMMS-Reporting MKS
GemAuth PVCS Firecall Lumigent Audit DB
Networker Clarify Tripwire Remedy Endeavor
VSS HPPM

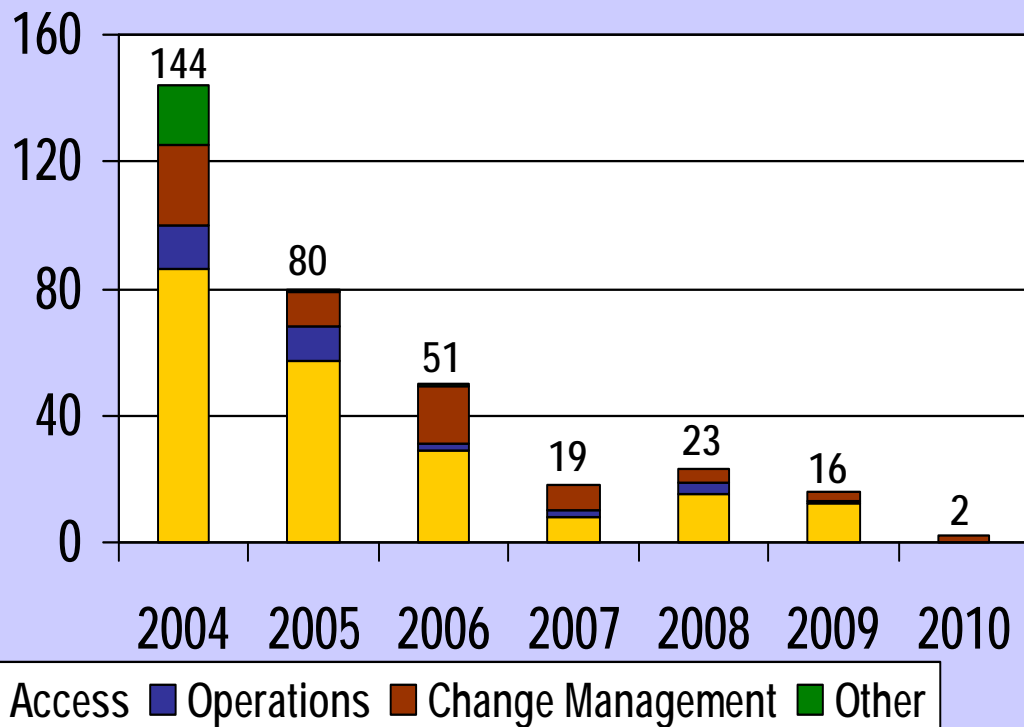
Database Management Systems

Sybase IDMS DB2
Oracle IMS SQL

IT SOX Deficiencies

As of 07/08/10

IT SOX Deficiencies



Note: Quarterly Monitoring began in 2006.

IT Deficiencies

	2006	2007	2008	2009	2010
Management	15	6	8	8	0
D&T	19	4	6	4	0
Quarterly Mont.	17	9	9	4	2
Total	51	19	23	16	2

IT Deficiencies Open at Year End

	2006	2007	2008	2009
Access	1	1	2	1
Operations	0	0	0	0
Change Mgmt.	0	1	1	0
Total	1	2	3	1

INFORMATION TECHNOLOGY

Critical Infrastructure Protection

What is CIP?

In 2008, the Federal Energy Regulatory Commission (FERC) approved mandatory *Critical Infrastructure Protection* (CIP) reliability standards to protect the nation's bulk power system against potential disruptions from *cyber security* breaches.

CIP

- Critical Infrastructure Protection (CIP) is part of the reliance framework.
- Standards detail Cyber Security requirements...examples:
 - CIP-002 — Critical Cyber Asset (CCA) Identification
 - What is a Critical Cyber Asset?
 - CIP-006 — Physical Security
 - What is a security perimeter?
 - CIP-007 — Systems Security Management
 - What does this mean?

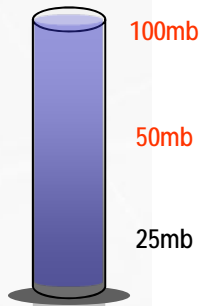
INFORMATION TECHNOLOGY

eDiscovery/Email Archive

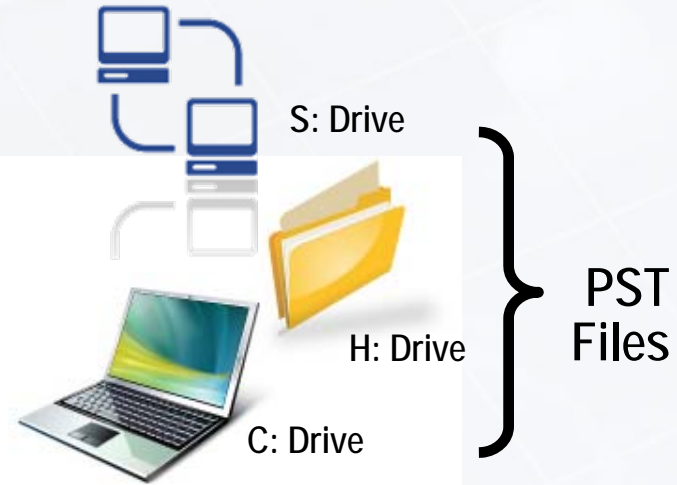
eDiscovery and Data Retention Risk

- E-Discovery continues to be Unpredictable and Expensive.
- The average corporate email user sends and receives 167 messages a day.
By 2013 this number will increase to 219 messages.
 - *Source : Radicati Group Study*
- Where is this data being stored?

Email Environment

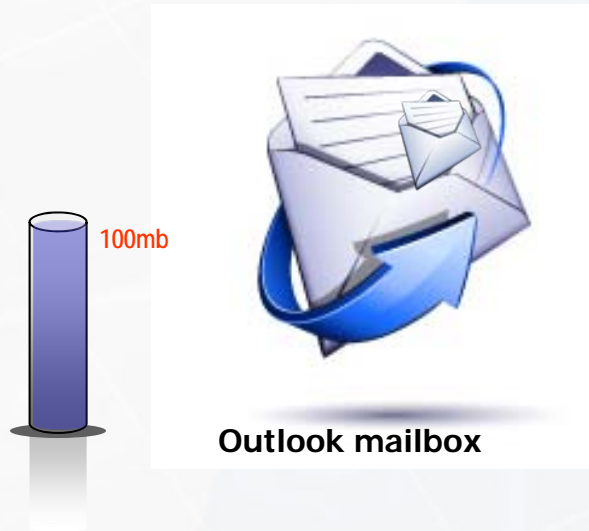


Outlook mailbox



Public Folders

Mail Environment with E-mail Archive



- Help manage mailbox size since archived e-mails are not included in the 100mb limitations;
- Provide an appropriate location to store e-mails for business purposes or retention requirements;



INFORMATION TECHNOLOGY

Post Critiques

INFORMATION TECHNOLOGY

Server Issue Affecting Applications Incident Category: Software Failure

DRAFT - CONFIDENTIAL

Incident Summary

On 03/06/09, as part of the normal process for preparing for a SAN firmware upgrade, SC Gen IT Infrastructure patched the Informatica servers as instructed by Enterprise Storage.

On 03/07/09, the patched Informatica servers began to experience performance issues which affected multiple Trading Floor Applications. As a temporary solution, SC Gen IT brought the Informatica Data Feeds up on UAT servers as a production failover measure.

After investigation by SC Gen IT, Enterprise Storage, UNIX Support, and Veritas, it

Business Impact

- Affected business critical application:
 - Load Forecaster
- Other applications affected:
 - Informatica
 - Trend
- Until the Informatica Data Feed could be brought up on UAT, all impacted applications experienced slow

Sequence of Events

03/06/09 (Friday) ET

- 05:00 PM – SC Gen IT patched the Informatica servers as instructed by Enterprise Storage in preparation for a SAN firmware upgrade.

03/07/09 (Saturday) ET

- 03:00 PM – Trading Floor began experiencing slow response time on multiple applications.
- 04:00 PM – Trading Floor users contacted SC Gen IT; SC Gen IT started troubleshooting the problem; initially focusing on the Informatica Application; decided to shut down the two Informatica Servers; once the Informatica Servers were shut down, the performance/response time of the other applications appeared normal.
- 05:00 PM - SC Gen IT brought up the Informatica Data Feeds on UAT servers to handle the production Data Feed failover.
- 05:30 PM – SC Gen IT requested the IOC page Enterprise Storage.

Process & Control Strengths

- ✓ SC Gen IT monitoring and alerting processes worked as intended.
- ✓ SC Gen IT escalation processes worked appropriately.

Action Items

- Apply new Veritas Patch to Informatica Development and UAT Servers. (Complete – SC Gen IT)
- Research and implement the scripting of the Informatica Data Feed jobs to be enabled on the UAT servers to handle production Data Feed failover in the event of serious problems on production servers. (Complete – SC Gen IT)

What are your threats, trends, issues?

- What regulatory requirements over Infrastructure is your industry facing?
- What initiatives are your companies working on?
- What initiatives should they be working on?
- Questions, surprises, clarifications?

Thank you!

- Feel free to contact me at rtelder@southernco.com