Market Perspectives on Governance, Compliance, and Identity Management

Marne E. Gordan
GRC Market Manager
Tivoli Software
Agenda

- State of the GRC Market
- Why Compliance?
- Why Governance?
- Insider Threat
- IBM Security Framework
- Summing Up
- Q&A
A “Sudden Interest” in Governance ??

- **Sarbanes-Oxley**
  - “Reactive” Legislation
    - Caused by corporate hijinx
    - Sought to hold C-level management responsible for corporate behavior
  - Regulation by inference
  - SOX made “governance” a part of everyday business
    - Previously the domain of large scale corporations
    - Level the playing field in terms of policy and behavior
  - International derivatives
    - EuroSOX
    - J-SOX

- **BASEL II**
  - For the financial services industry
  - Adequate capitalization
  - Estimation and protection against loss
Governance Has Been Around Forever

The concept of "governance" is not new. It is as old as human civilization. Simply put "governance" means: the process of decision-making and the process by which decisions are implemented (or not implemented).

-- UN Economic and Social Commission
Compliance v. Governance

- Not interchangeable
- Compliance
  - Practical
  - Tactical
- Governance
  - Strategic
  - Behavioral

- Compliance is a key component of Governance
Defining Governance in Terms of Business

**Governance** (in business) is the action of developing and managing consistent, cohesive policies, processes and decision rights for a given area of responsibility. For example, managing at a corporate level: privacy, internal investment, the use of data.

A reasonable or rational purpose of governance is to see to it (assure), sometimes on behalf of others, that the organization produces a worthwhile pattern of good results while avoiding an undesirable pattern of bad circumstances.

-- Wikipedia
Defining Governance in Terms of IT

Information Technology Governance, IT Governance or ICT Governance, is a subset discipline of Corporate Governance focused on information technology (IT) systems and their performance and risk management. The rising interest in IT governance is partly due to compliance initiatives (e.g. Sarbanes-Oxley (USA) and Basel II (Europe)), as well as the acknowledgement that IT projects can easily get out of control and profoundly affect the performance of an organization.

A characteristic theme of IT governance discussions is that the IT capability can no longer be a black box. The traditional handling of IT management by board-level executives is that due to limited technical experience and IT complexity, key decisions are deferred to IT professionals. IT governance implies a system in which all stakeholders, including the board, internal customers and related areas such as finance, have the necessary input into the decision making process. This prevents a single stakeholder, typically IT, being blamed for poor decisions. It also prevents users from later complaining that the system does not behave or perform as expected:

*A board needs to understand the overall architecture of its company's IT applications portfolio ... The board must ensure that management knows what information resources are out there, what condition they are in, and what role they play in generating revenue...*

There are narrower and broader definitions of IT governance. Weill and Ross focus on "Specifying the decision rights and accountability framework to encourage desirable behavior in the use of IT."

In contrast, the IT Governance Institute expands the definition to include underpinning mechanisms: "... the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives."

-- Harvard Business Review, October 2005
Relationship to Other IT Disciplines

- IT governance is supported by disciplines
  - IT Asset Management
  - IT portfolio management
  - Enterprise architecture
  - Project governance
  - Project management
  - Program management in the enterprise IT context
    - including software engineering where appropriate
  - IT service management
  - Business Technology Optimization
State of the GRC Market
Governance, risk management, and compliance (GRC) is a global issue comprising many different initiatives—some regulatory, many policy driven—that cut to the core of every business, regardless of geography or industry. AMR Research’s annual survey of over 420 line-of-business and IT executives paints a new GRC picture for 2008, as operational and enterprise risk management moves out of the shadow of compliance.
A Global Perspective on GRC

- A Detailed Survey
  - 420 IT and Line-of-Business (LOB) leaders
  - United States, Germany, and Japan
  - Spending plans
  - Adoption
  - Growth
  - Business drivers

Governance, risk management, and compliance (GRC) spending will exceed $32B for 2008, up 7.4% from 2007, as companies shift toward identifying, assessing, and managing risk across numerous business and IT areas.
Findings

- 2008 GRC spending will expand to $32.1B, up 7.4% from 2007.
  - Average GRC spending exceeds $2.44M per organization.
  - Risk management is now the new compliance, equaling or exceeding financial governance in influence and spending.
  - IT risk is clearly a separate buying center.
  - Environmental concerns are on the rise.
Figure 2: Most influential issue driving investment in GRC

- Better manage and mitigate risks in the business: 31%
- Reduction in overall cost of GRC: 18%
- Automate/repeatability of GRC activities: 17%
- Provide internal and external transparency: 12%
- Risk/cost of noncompliance: 11%
- Establish a legally defendable information environment: 10%

Source: AMR Research, 2008
Figure 3: Most influential issue driving investment in GRC—by country

- Better manage and mitigate risks in the business: United States 27%, Germany 23%, Japan 31%
- Reduction in overall cost of GRC: United States 16%, Germany 17%, Japan 20%
- Automate/repeatability of GRC activities: United States 17%, Germany 17%, Japan 20%
- Provide internal and external transparency: United States 14%, Germany 13%, Japan 11%
- Risk/cost of noncompliance: United States 7%, Germany 5%, Japan 11%
- Establish a legally defensible information environment: United States 9%, Germany 10%, Japan 16%

Source: AMR Research, 2008
Figure 4: Largest single GRC Investment for all countries and buyers

- IT-specific risk management: 23%
- Sarbanes-Oxley or other financial governance initiatives: 15%
- Operational and general risk management: 14%
- Manufacturing process approval/certification and traceability: 8%
- Environmental factors: EH&S compliance: 6%
- Customer compliance: 5%
- Security and privacy rules, including HIPAA or PCI and other: 5%
- Document and record retention requirements: 5%
- Basel II or solvency requirements: 3%
- Overall SEC or other financial market regulations: 3%
- FDA or other food and drug regulations: approval/certification: 2%
- Legal discovery issues and/or evidence: 2%
- Corporate / industry sustainability initiatives: 2%
- Supply chain traceability: 2%
- Code of conduct/training requirements: 2%
- Import/export/trading regulations: 1%
- Other: 2%

Source: AMR Research, 2008
Figure 1: Additional business areas supported with GRC investments

- Streamline business processes: 55%
- Better visibility to operations: 54%
- Better quality: 54%
- More secure environment: 48%
- Support globalization efforts: 24%

Source: AMR Research, 2008
Why Governance??

System Governance

- Cost
- Quality
- Change
- Compliance
- Alignment
- Service
Is Governance Important?

Jérôme Kerviel: Société Générale's €5bn fraudian slip

As the trading books were being squared off for the day at Société Générale's Paris headquarters 10 days ago, a sharp-eyed compliance officer spotted something awry. Somehow or other, one of the bank's clients had gone over its trading limit - by billions and billions of euros. Or so it seemed.

French Premier Chides Noyer on Societe Generale Delay (Update2)

By Stephanie Bodoni and Helene Fouquet

Jan. 25 (Bloomberg) -- French Prime Minister Francois Fillon chided Bank of France Governor Christian Noyer for failing to inform him sooner that Societe Generale SA had suffered a record trading loss.

Bank scandal a blow to French pride

By Marcel Michelson Reuters

PARIS: The $7 billion equities derivatives loss at Societe Generale has dealt a sharp blow to French pride, not least because of the international reputation in financial markets of its mathematically trained technical traders.

Rogue French trader accused of hacking

Bank says man blamed for $7 billion loss used 'several techniques of fraud'
What Happened??

- January 2008
- Rogue Trader Jerome Kerviel accused of fraud
  - Trusted insider
  - Hacked into the accounts of other users
  - Falsified authorizations
  - Falsified trades and positions
- \(~€5B (~£4B or $7B)\) in losses
  - Built a position of €50B ($73.5B)
  - Bank valued at €34B ($49B)
- Global Impact
  - “Controlled” sell off in European markets
  - Associated sell off in Asian markets
  - US Federal Reserve cut interest rates \(\frac{3}{4}\)%
Some Perspective on the Issue

- The investigation continues
  - What was the real motive?
- French Finance Minister’s probe will focus on why the bank's internal checks failed and whether financial companies should be forced to impose more controls on their businesses.
- “These were trades that should never have happened, conducted by someone who had no authority to make them, on systems he was not supposed to have access to. “
- "You just need to look at the likes of the Rusnak case and the Leeson case to see that these people have always been subjected to control procedures, they have just gone out of their way to get round them."
- Quotable Quote: “[If left alone to trade himself out of this position, he ] would make the bank billions”. *
This Has Happened Before

A look at some major bank frauds

2008: French bank Societe Generale uncovers an alleged $7.21 billion fraud by a futures trader who fooled investors and overstepped his authority.

2002: Former currency trader accused of hiding $691 million in losses at Allfirst bank of Baltimore, at the time under parent Allied Irish Bank, pleads guilty to one of the largest bank fraud cases in U.S. history.

1995: Collapse of Britain’s Barings Bank after a trader in Singapore, Nick Leeson, lost 860 million pounds (then worth $1.38 billion) on futures trades. The fraud prompted banks worldwide to tighten internal checks.

1991: Bank of Credit and Commerce International (BCCI), operating in nearly 70 countries, is seized by bank regulators, acting on auditors’ reports of huge losses from illegal loans to corporate insiders and from trading transactions. Some 250,000 depositors left without funds. Claims exceeded $10 billion.
Why Compliance??

IGNORE

Security Laws & Regulations
at Your Peril!
Why is Compliance Important??

- At the Seattle Cancer Care Alliance
- Patient Eric Drew’s identity stolen by phlebotomist Richard Gibson
  - Gibson had access to patient record
  - Obtained Drew’s SSN, date of birth, and primary address
  - Used it to obtain credit
  - Ran up over $9k USD in debt
    - Clothing
    - Jewelry
    - X-Box
    - Porcelain figurines

Drew Began Receiving Unsolicited Mail Collection Notices

- **Contacted major credit bureaus**
  - Placed fraud warnings on legitimate credit cards
  - Begged major issuers not to issue any new cards
  - Contacted local law enforcement

- **Nothing happened, until**
  - Local reporter Chris Daniels at KING-5 NBC TV reported the story
  - Daniels and Drew continued the investigation
  - Forensic trail led to Gibson

- **Gibson plead guilty**
  - 16 months in jail, plus restitution
  - First documented “HIPAA conviction”
  - Convicted of unlawful use of IIHI
Great Story, But . . . .

- What Does it Have to do with Compliance?
  - When faced with a compliance “checklist”, we
    - Become overwhelmed by tasks and deadlines
    - Focus on “minimum necessary” to pass the audit
    - Focus on “beating” fines and penalties
    - Forget what can happen when data is misused
    - Overlook “harm” to
      - Customers
      - Business Partners
      - Employees
      - Any individuals who entrust us with their data
Comparing the Two Incidents

- In the case of Seattle Cancer Care Alliance
  - The organization was held harmless
- Although SocGen is still under investigation
  - The organization is being held responsible
- Even though one incident was considered a failure of governance, and the other a compliance violation . . . . .
- In both cases
  - The organizations were in compliance with industry requirements
  - Appropriate policies and procedures existed to protect sensitive data
  - The individuals specifically violated established policy
  - Both “had a good reason”
  - Neither considered their actions a crime
- Keyword = INDIVIDUAL
  - One person
  - Deliberate action
  - Malicious intent
Isolated incidents

- Not necessarily...
- Recent Novell research indicates
  - More than half the UK workforce* would be prepared to seek revenge on former employers by exploiting continued access to corporate systems if they lost a job
  - 55% would continue to use their company laptop if it were not taken back; 58% would continue use of company mobile phones.
  - 6% said that they would delete important files
  - 4% would let a virus loose in the corporate email system
  - 67% would be prepared to steal sensitive information that would help in their next job
  - 38% said that they would steal company leads

*2007 article did not indicate how large the polling group was, nor if it were a scientific poll
Insider Threat

There's just something fishy about that guy

(c) M. FLYNN
The reason insider attacks “hurt”

- Two important rights
  - Trust
  - Physical Access

- In general, users and computers accessing resources on the local area network (LAN) of the company are deemed trusted.

- Practically, we do not draconically restrict their activities – revoke trust -- because an attempt to control these trusted users too closely will impede the free flow of business.

- Once an attacker has physical control of an asset, that asset can no longer be protected from the attacker.
Why does the audit community care about the enemy inside?

- While viruses, worms, Trojans and DoS are serious, **attacks perpetrated by people with trusted insider status pose a far greater threat to organizations in terms of potential cost per occurrence and total potential cost** than attacks mounted from outside.
Who is an “Insider”?

- Current or former employees, consultants, and outsourcers who:
  - Intentionally or inadvertently exceeded or misused an authorized level of access to networks, systems, or data in a manner that
  - Targeted a specific individual or affected the security of the organization’s data, systems, and/or daily business operations

<table>
<thead>
<tr>
<th>User</th>
<th>Access Type</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super/Privileged User</td>
<td>VPN</td>
<td>Executive logging in remotely to review personnel files</td>
</tr>
<tr>
<td>Super/Privileged User</td>
<td>LAN</td>
<td>IT administrator using the LAN to administer desktop</td>
</tr>
<tr>
<td>Trusted User</td>
<td>Dial-up</td>
<td>Salesperson logging in via remote access to manage accounts</td>
</tr>
<tr>
<td>Trusted User</td>
<td>LAN</td>
<td>Employee using a directory on the file server to save critical files</td>
</tr>
<tr>
<td>Semi-Trusted User</td>
<td>Extranet</td>
<td>Client or partner accessing account information</td>
</tr>
<tr>
<td>Semi-Trusted User</td>
<td>LAN</td>
<td>Consultant using the LAN to conduct daily business</td>
</tr>
</tbody>
</table>
Who are these privileged users?

- DBAs
- Sys Admins
- Network Admins
- In certain circumstances
  - Data entry personnel
  - Customer Service Representatives
The Mind of the Insider

- **Good intentions**
  - Toyota Belgium – an exec took a CD home to work on data, lost it on the bus

- **Or evil**
  - UK – a former sales representative at a high tech firm continued to access customer database from his previous employer; within a one month period poached over 1300 clients

- According to CSI 2008 Study, the majority of perpetrators don’t consider their actions illegal
- Consider their actions justified
More About the Study

- **CERT**
- **Carnegie Mellon University (Pittsburgh, PA)**
  - Software Engineering Institute
- **United States Department of Defense**
  - With contributions from the US Secret Service
- **2008 Insider Threat Study:**
  - Illicit Cyber Activity in the Information Technology and Telecommunications Sector
    - Research conducted across 13 critical infrastructure sectors
    - Focus mainly on private industry
The Insider Threat Profile

- A frightening 87% of those perpetrating harm were those we would consider as having the “keys to the kingdom”

- Current and former employees carry out illicit insider activities in nearly equal numbers.

- Most insiders were either previously or currently employed full-time in a technical position within the organization.

- Thirty-eight percent of the insiders had been arrested previously.
43.5% of global security incidents (inside & outside) can be attributed to the privileged user

SUMMARY:

• The number of attacks attributed to the inside vs. outside is approximately equal (Source: CSI/FBI Survey 2008)

• 43.5% of the total number of security incidents experienced globally can be attributed directly to the privileged user group.

• The privileged user group generally represents < 5% of any given organization.
These attackers planned ahead

- 62% percent of the attacks were planned in advance.
- 57% percent of the attackers surveyed would consider themselves “disgruntled.”
- 80% exhibited suspicious or disruptive behavior to their colleagues or supervisors before the attack.
- Only 43% had authorized access (by policy, not necessarily via system control).
- 64% percent used remote access to carry out the attack.
We Are Not Proactively Monitoring

- Most insider attacks are only discovered through manual (non-automated) detection of an irregularity or failure of an information system.
  - System logs were the most prevalent means by which the insiders were identified.
  - The majority of the insiders took steps to conceal their identities and their activities.
We Find Out After the Fact !!!

- Most of the incidents were detected by non-security staff
- The majority of attacks were accomplished using company computer equipment.
- 86% of the incidents were detected only after there was a noticeable irregularity in an information system or a system became unavailable.
  - 80% of incidents were detected through manual procedures only
  - 16% were identified using a combination of automated and manual procedures.
  - 24% of incidents are detected through observation and notification by others.
Then We Become Reactive

- The various mechanisms used to identify the perpetrators included
  - system logs (67%)
  - forensic examination of the targeted networks, data, or systems (35%)
  - the insiders’ own source IP addresses (33%)
  - username (25%)
  - phone records (22%)
  - forensic examination of the insiders’ home computer equipment (18%)
We Need to Become More Proactive

- Look at the behavior of our individuals before the fact
- Particularly our privileged users
  - Assign unique user IDs and network credentials
  - Apply the principle of least privilege
    - To network resources
    - To critical data
  - Establish baseline activity for the environment
  - Examine trendline activity within the environment
  - Analyze all anomalous activity
Can Compliance Help Us

Top 5 control deficiencies derived from last 2 years of SOX Section 404 filings

- **Improper Change Management**
  - Lack of formal program change procedure
  - Lack of understanding of system configurations
  - Oversight of changes and review of change logs

- **Insufficient Segregation of Duties**
  - Separation of requestor, approver, implementer
  - Separation of developers and operators

- **Excessive Access to Systems / Databases**
  - Developer / programmer / DBA /Admin access to production environment
  - Developer / programmer DBA /Admin access to production data

- **Lack of Access Controls**
  - User provisioning and administration
    - Changes in responsibilities
    - Changes in organization
    - Terminations
  - No documented access policies and standards

- **Lack of general monitoring of the security infrastructure**
## Top 5 Failed PCI Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Associated Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 3: Protect stored data.</td>
<td>Unencrypted spreadsheet data; unsecured physical assets</td>
</tr>
<tr>
<td>Requirement 11: Regularly test security systems and processes.</td>
<td>POS/shopping cart application vulnerabilities; most data compromises attributed to Web application vulnerability</td>
</tr>
<tr>
<td>Requirement 8: Assign a unique ID to each person with computer access.</td>
<td>Weak or easily guessed admin account passwords</td>
</tr>
<tr>
<td>Requirement 10: Track and monitor all access to network resources and cardholder data.</td>
<td>Lack of log monitoring and IDS data; poor logging tools</td>
</tr>
<tr>
<td>Requirement 1: Install and maintain a firewall configuration to protect data.</td>
<td>Card numbers in the DMZ; segmentation flaws</td>
</tr>
</tbody>
</table>

Source: [http://www.verisign.com/static/PCI_REASONS.pdf](http://www.verisign.com/static/PCI_REASONS.pdf)
Reinventing IT Security to secure business processes

IBM elevating IT Security to a risk mgt. discipline that secures business processes

IBM broadening IT Security to cover security operations within every IT resource domain and drive synergies among them
Think access to assets and individuals
Figure 4: Largest single GRC Investment for all countries and buyers

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT-specific risk management</td>
<td>23%</td>
</tr>
<tr>
<td>Sarbanes-Oxley or other financial governance initiatives</td>
<td>15%</td>
</tr>
<tr>
<td>Operational and general risk management</td>
<td>14%</td>
</tr>
<tr>
<td>Manufacturing process approval/certification and traceability</td>
<td>8%</td>
</tr>
<tr>
<td>Environmental factors: EH&amp;S compliance</td>
<td>6%</td>
</tr>
<tr>
<td>Customer compliance</td>
<td>5%</td>
</tr>
<tr>
<td>Security and privacy rules, including HIPAA or PCI and other</td>
<td>5%</td>
</tr>
<tr>
<td>Document and record retention requirements</td>
<td>5%</td>
</tr>
<tr>
<td>Basel II or solvency requirements</td>
<td>3%</td>
</tr>
<tr>
<td>Overall SEC or other financial market regulations</td>
<td>3%</td>
</tr>
<tr>
<td>FDA or other food and drug regulations: approval/certification</td>
<td>2%</td>
</tr>
<tr>
<td>Legal discovery issues and/or evidence</td>
<td>2%</td>
</tr>
<tr>
<td>Corporate / Industry sustainability initiatives</td>
<td>2%</td>
</tr>
<tr>
<td>Supply chain traceability</td>
<td>2%</td>
</tr>
<tr>
<td>Code of conduct/training requirements</td>
<td>2%</td>
</tr>
<tr>
<td>Import/export/trading regulations</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
</tbody>
</table>

Source: AMR Research, 2008

Risk-based spending against the most prevalent threats!!
Just Remember . . .

- For both Compliance and Governance
  - It is critical that we understand “who” had access to “what”
  - Restrict access to critical resource based upon the principle of least privilege

- Monitor activity
  - Know the baseline performance of your network
  - Study trendline activity
  - In order to accurately determine anomalous activity
    - It could signal an insider breach

- Don’t forget about “harm” !
Contact Information:

Marne E. Gordan  
GRC Market Manager  
megordan@us.ibm.com  
+1 703 960 9536