RISK!
Building an Effective GRC Function in a Hostile World

MacDonnell Ulsch
Gerard Kane
ZeroPoint Risk Research, LLC

© Copyright 2012. ZeroPoint Risk Research, LLC. All rights reserved.
Topics for Discussion

• The Need for GRC
• Current Status of GRC
• What’s at Stake (it’s not just compliance any more)
• What Can be Done?
• Wrap up, Discussion
The following three slides contain passages from the book “THREAT! Managing Risk in a Hostile World,” by MacDonnell Ulsch, published by The IIA Research Foundation.

“THREAT!” examines the need for change in how we manage risk in a post-911 world.
Now Is The Time To Change

“An executive is in a sailboat, deep at sea. The sky is stunningly blue. The sun is bright. The water is calm and clear .... The soft breeze is like a friendly song, warm, comforting, familiar. All seems well and an easy smile settles into his salty face. Life seems good.

“But conditions can change – and change quickly... the executive, lulled into a false sense of security ... could fall overboard and discover in horror that the calm above is hiding hungry, circling sharks below. Or the winds could pick up, instantly changing from comfortable and warm to gale force and perilous, the blue sky giving way to dark, ominous clouds, the bright sun hiding in the distance, out of sight. Water that moments ago was deadly calm is now just ... deadly.”
“The executive never expected change. Yet change came, and without warning. Or did it? Were there signs of impending danger? Did he check the weather forecast before setting sail? Did he have experience in those waters, knowing the likelihood of prevailing conditions at that time of year? Did he know the waters were infested with sharks? Did he anticipate the risk of falling overboard and prepare for that possibility by wearing a life jacket? Or, given advances in technology, did he have shark repellent and an electronic locator beacon? If not, he should have!

“Change is almost never neutral in its impact. This is particularly true when it is either unanticipated or when those experiencing it are not prepared.... Managing risk has always been important.... But the world has changed dramatically... and the impact of change can be devastating....”
“We should treat emerging technology like fire, not air. With fire, we know that a flame can burn and kill indiscriminately. Under controlled circumstances it can be used to prepare food, heat our homes and offices, fuel the power plants that provide electricity, and create the combustion that powers much of our transportation.... We think about weapons technology in this way, but not information technology.”
The Need for GRC

• Expanding Threat Environment
  – Emerging
  – Advanced Persistent Threat
  – Geopolitical influences
  – Organized Crime
  – Money Laundering
  – Insiders
  – Third Parties

• Technology advances introduce new threats
  – Cloud
  – BYOD

• Changing Targets
  – NPPI
  – Intellectual Property/Trade Secrets
  – Critical Infrastructure
The Need for GRC

- With changes in threats come changes in risk, and perhaps more importantly **Risk Impact**
  - Financial
  - Legal
  - Regulatory
  - Reputational
  - Cascading

- It’s not about security, it’s about RISK
Current Status of GRC

- Compliance has attempted to force information risk management into the C suite.
  - The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - The Sarbanes-Oxley Act of 2002 (SOX)
  - 201 CMR 17.00 (2010)
  - Other state requirements

- While some have reconsidered and adjusted their approach to risk management, many are still simply “checking the box.”
Current Status of GRC

- Compliance efforts tend to be fragmented and scattered.
- Lack of a common approach may lead to complexity and redundancy.
- The message from risk reporting loses its gravitas
- 15+ years of compliance has not made upper management smarter about, or more interested in, addressing risk.
  - “there is ‘limited or no understanding of the difference between sensitive information and other data’ at nearly a quarter of the companies participating in its survey.
  - “Today’s companies, clearly very good at collecting data, seem “less savvy when it comes to how to classify and manage it.” (CFOworld 3/7/12)
Current Status of GRC

“...boards and senior management still are not exercising appropriate governance over the privacy and security of their digital assets.”

“There is still an apparent disconnect between boards and senior executives understanding that privacy and security and IT risks are part of enterprise risk management.”

“...less than two-thirds of the Forbes Global 2000 companies surveyed have full-time personnel in key roles responsible for privacy and security in a manner that is consistent with internationally accepted best practices and standards. Moreover, the common practice of assigning security personnel both privacy and security responsibilities creates segregation of duties issues at line responsibility levels.”

## Current Status of GRC

<table>
<thead>
<tr>
<th>Best Management Practice</th>
<th>Regularly</th>
<th>Occasionally</th>
<th>Rarely or Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board reviews &amp; approves top-level policies on privacy &amp; IT security risks.</td>
<td>23%</td>
<td>28%</td>
<td>42%</td>
</tr>
<tr>
<td>Board reviews and approves roles and responsibilities of lead personnel responsible for privacy and IT security</td>
<td>19%</td>
<td>18%</td>
<td>66%</td>
</tr>
<tr>
<td>Board reviews and approves annual budgets for privacy and IT security programs</td>
<td>28%</td>
<td>10%</td>
<td>54%</td>
</tr>
<tr>
<td>Board regularly receives reports from senior management regarding privacy and IT security risks</td>
<td>38%</td>
<td>34%</td>
<td>25%</td>
</tr>
</tbody>
</table>
Has breach activity abated as a result of compliance?

www.privacyrights.org

- 559,878,914 RECORDS BREACHED
- from 3,065 DATA BREACHES made public since 2005
Current Status of GRC

Breaches

2005 2006 2007 2008 2009 2010 2011 2012

0 100 200 300 400 500 600 700

Breaches
Current Status of GRC

Records

© Copyright 2012. ZeroPoint Risk Research, LLC. All rights reserved.
What’s at Stake?

• It’s time to be concerned about more than PII/PHI
• Intellectual Property and Trade Secrets are now the big target.
The principal drivers of economic espionage and trade secret theft are:

- Military force modernization
- Economic competition
- Commercial modernization
- Money laundering
- Cost of capital
- Cost of Research & Development
- Time to market considerations
- Market penetration
Who Steals Trade Secrets?

- Employees
- Foreign or multinational corporations
- Foreign government-sponsored educational and scientific institutions
- Free-lance agents (some of whom are unemployed former intelligence officers)
- Computer hackers
- Terrorist organizations
- Revolutionary groups
- Extremist ethnic or religious organizations
- Drug syndicates
- Organized crime
Trade Secret Theft

- Organized crime is involved in trade secret theft and economic espionage.
- Russia has emerged as a major international influence in organized crime.
- Compare organized crime in the US and Russia:
  - US:
    - 24 crime families
    - 2,000 active members
  - Russia
    - 5,000 – 8,000 groups
    - 100,000 active members
- 108 nations engaged in economic espionage
China: Pursing Global IP

• The People’s Republic of China developed the 863 program to acquire dual use technology—commercial and military application.

• 863 program targets six key areas:
  – Information Technology
  – Advanced Materials
  – Biotechnology & Advanced Agricultural Technology
  – Advanced Manufacturing and Automation Technology
  – Energy Technology
  – Resource & Environment Technology

© Copyright 2012. ZeroPoint Risk Research, LLC. All rights reserved.
What Can Be Done?

- Think “Post-Breach”; Act “Pre-Breach”
- Increase awareness at all levels
- Revisit policies and procedures
- Look inward as well as outward when identifying and assessing threats
- Rethink “insiders”
  - Vendors
  - Contractors
  - Temps
  - Employees
What Can Be Done?

- Create roles, responsibilities and accountability where they do not currently exist
  - CRO
  - CPO
  - CISO
- Make Risk a topic in normal management reporting
- Create Risk Councils, and include the appropriate players
Risk Council Determines Acceptable Risk
Risk Management must become an integral part of Business/Organizational Management.

Traditionally we think of management as:

- *The act of getting people together to accomplish desired goals and objectives using available resources efficiently and effectively.*
- *Planning, organizing, staffing, leading or directing, and controlling an organization (a group of one or more people or entities) or effort for the purpose of accomplishing a goal.*
An alternative management definition:

1. Corporate power elites distinguished primarily by their distance from actual productive work and their chronic failure to manage. (see also suit). Spoken derisively, as in "*Management* decided that ...".

2. Mythically, a vast bureaucracy responsible for all the world's minor irritations.

Need for an Enterprise Approach to Managing Risk

Our view of management:

“Effective management recognizes and takes advantage of opportunities, understands and mitigates risks, and optimally allocates resources, all for the purpose of achieving the organization’s strategic goals.”
Getting Management Involved

- Change the way risk is viewed and discussed.
  - GRC has been “C” driven. Must migrate to being “R” driven.
  - Think “Post-Breach”; Act Pre-Breach.
  - Change the dialog; Speak in terms of *Risk Impact, i.e.*:
    - *Financial*
    - *Legal*
    - *Regulatory*
    - *Reputational*
    - *Cascading*

- Build risk management, privacy and security into budgets.

- Build an Enterprise Risk Management (ERM) program.
Enterprise Risk Management

“... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

The ERM program, using the COSO ERM Framework, is geared toward the achievement of organizational objectives set forth in these categories:

- **Strategic** – high level goals, aligned with and supporting the mission.
- **Operations** – effective and efficient uses of resources.
- **Reporting** – reliability of reporting.
- **Compliance** – compliance with applicable laws and regulations.
Enterprise Risk Management Components

- Internal environment
- Objective setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring
Enterprise Risk Management Components
Enterprise Risk Management
Entities

An effective ERM program:

• establishes a portfolio view of risk at the unit level and entity level;
• Establishes a common language for the discussion of risk across all functions and business units;
• Allows management to see and consider how individual risks interrelate;
• Avoids redundant risk assessment and mitigation efforts;
• Helps to create a culture of risk awareness, beginning with the “tone at the top”.

© Copyright 2012. ZeroPoint Risk Research, LLC. All rights reserved.
Discussion and wrap-up