Security & Risk Mindedness in Corporate Organisations

Stuart Osborne QPM MSc

Stuart.osborne@outlook.com

Career Observations

Investigated and responded to many incidents ranging from traditional crime, terrorism, environmental impact, commercial espionage, fire and protest activity that caused death, injury, damage to property, harm to reputations and effected the ability for organisations to continue to operate with substantial cost to both the public and private sector.

Often these events:

- Could have been prevented
- Should have been identified and managed sooner & better
- Injury, damage and commercial impact could have been reduced
- Recovery achieved sooner
- Lessons learned on a cross sector basis

Context

- *Threats continue to grow*
- *Becoming more diverse and complex*
- *Increasing No. of tools, techniques, technology*
- *Organisations & industry are still vulnerable*
- *Significant and costly incidents still happening*
- *Calls for further regulation from some*
- *Desire for greater flexibility from others*

“What is required to get awareness and consideration of security issues by the Board or Executive and where necessary, the embedding of security measures”

Security covered risks to:

People Assets Information Infrastructure

and the ability to:

Prevent Protect Respond Recover

from any event

Methodology

- Documentary review of past incidents
- Assessment of education courses in security, risk & business
- Impact of legislation and regulation
- Bench marking ‘best practice’
- Interviews with:
  - Security and operational risk practitioners
  - Members of main company boards
  - Non-executive directors
  - Members of the company executive - C’ Suite
  - Industry trade, security and risk organisation’s
  - CPNI, regulators and oversight bodies

Common Themes

- Security and Risk management not recognised as a ‘key board function’
  - Legal, Finance, Human Resources, Communications, Business Development, Audit
- Organisational structures frustrated internal communication
  - Inconsistent management lines, seniority levels, access to Board, financing and reporting
- Different cultural appreciation of issues and priorities
  - Educational pathways, career experience and personal motivations
- Timeliness of risk management practitioners in processes
  - Strategy, planning, design, build and implementation and operations
- History of an Organisations experience of a significant adverse incident
  - Post event reactive, isomorphic learning, untested or realised vulnerability
- Inconsistent impact of legislation and regulation
  - Corporate Vs. personal liability, reputation, increasing profit, reducing costs
- Compliance driven Vs. Risk managed
  - Tick box, embedded, license to trade, cost center Vs. business enabler

Hierarchy of Influence

Tier 1. **The Board**

‘ To ensure the company’s prosperity by collectively directing the company’s affairs, while meeting the appropriate interests of it’s ***shareholders and relevant stakeholders****’*

(Standards of the Board, IoD)

Tier 2. **The Executive**

Reports directly to the board and is accountable for delivering the strategy, implementing the structure and managing and overseeing the day-to-day business of the organisation.

Tier 3. **Management and Operations**

Reports to the executive and delivers the functionality and operations of the business

Considerations for Security & Risk Mindedness in the Future

- Legislation, Codes and Regulation
  - *Companies Act 2006, UK Corporate Governance Code 2018*
- Knowledge, Understanding and Communication
  - *Top Down and Bottom Up*
- Competence and Standards
  - *Tactical, Procedural and Strategic*
- Recognition and Visibility - *Reputation*
  - *Capability, Reward and Review*
- Motivation and Incentive – *Shareholder Value*
  - *Reputation, differentiation, commercial advantage*

Thank You

Stuart Osborne QPM MSc

Stuart.osborne@outlook.com