What All CXOs Need to Know About Risks in IT

Why don't all organisations actively control operational risk? Recently a number of global and local IT incidents were reported that most likely had negative financial consequences:

- 15 July **United Airlines** stopped all flights for three hours due to a faulty network router. The same morning **New York Stock Exchange** halted all trades for almost four hours. New York Times reported that the problem was due to a software update.
- After **Ashley Madison** website was hacked 37 million email addresses were leaked. Financial Times reported that CEO Biderman finds himself with a dilemma; his business has two key assets: its data and its customers' trust. It has lost the first, and risks losing the second.
- In the UK, **NatWest** suffered another IT fiasco admitting it could take until the weekend for customers to receive 600,000 payments that failed to enter accounts.
- Thousands of **The co-operative** customers who used their cards in the retailer's stores may have been charged twice. A spokesman said a "processing error" had affected its food stores and petrol stations.
- In **Manchester** many businesses lost electricity for hours after a local power cut caused by flooding in a substation. Restaurants and bars forced to close, with shops facing losing money in stock without refrigeration and restaurants their evening takings.

Similar IT failures could often be avoided or the effects significantly reduced. We are also reading about the tip of an iceberg, as many glitches are not made public.

CXOs should develop an understanding how to identify and reduce operational risks in IT
How can we better identify, manage and reduce operational risks that, worst case, otherwise might develop into Black Swans[1]. Is there an efficient way to avoid or limit financial losses, churn and negative media reporting due to materialised operational risks in IT?

Why don't all Boards of Directors and CXOs take a strategic approach to operational risk mitigation? Even though many excel in this field (because of regulatory requirements, due to the 'nature' of the business, or both) such as financial institutes, emergency services and airlines, a number of organisations would, based on my experience, benefit from investing in risk control.

What about the CIO role and Operational Risks in IT?
Boards recognize that IT has a value and is of a strategic nature, however IT is perceived as complex. If the CIO is not on the executive team, focus may be on cost, and cost alone, rather than considering IT from a business value and risk optimization perspective.

When analyse?
Always conduct an operational risk assessment:

- Before strategic decisions (e.g. transformations, ERP projects or Cloud/outsourcing IT)
- As part of M&A due diligence
- As newly appointed (externally recruited) Chairman or CXO
- If the Board don't know the organisations' ability to control operational risks

[1] *Why Your IT Project May Be Riskier Than You Think by Flyvbjerg and Budzier. Harvard Business Review, Vol. 89 (2011), No. 9, pp. 23-25.*

A practical approach to operational risk control

Management and IT should work together reducing operational risks over time. SMEs and public sector may benefit from a simple methodology consisting of a few steps:

1. Identification of relevant risk areas to be investigated (examples below)
2. Analysis, compilation and assessment of current risks
3. Evaluation of risk levels including financial implications
4. Decisions about actions (activity plans, mitigation projects and budgets)
5. Introduction of governance model and reporting

By asking the right questions, we may quickly (often within one to two weeks) get a good understanding about the general risk situation. Here are a examples of areas and questions:

IT

HW / System redundancy
Network redundancy
Disaster recovery
Roles and processes
History of IT failures
IT performance management

STRATEGY

Risk awareness
Governance
IT strategy
Architectural road map
IT target picture

FINANCE

P2P
O2C
R2R
IT support during critical periods

CHANGE

Project management / PMO
Testing / Go-live / Fall-back

SUPPLIERS

SLAs
Contracts
Damages paid out

SECURITY

Information security
Premises
Cyber and penetration testing
IT security (e.g. Sys admin)
Policies and training

HR

Key individuals
Succession planning

OTHER

Business continuity planning
Crisis communication

Subsequently, risks can be mitigated by reducing the most prioritized risks and by planning future risk reduction. In some areas (e.g. Cyber security) I recommend using a 3rd party specialist.

Finally, introduce a governance model, a risk committee plus basic reporting and monitoring templates. The risk committee should report to management / Board at least once per year.

Benefits from improved risk control

Board and Management may now take control by following risk metrics and setting specific risk reduction goals. By shifting focus from IT costs, IT can be steered towards a more effective delivery with reduced operational risks, improved quality and lower overall costs as a result.

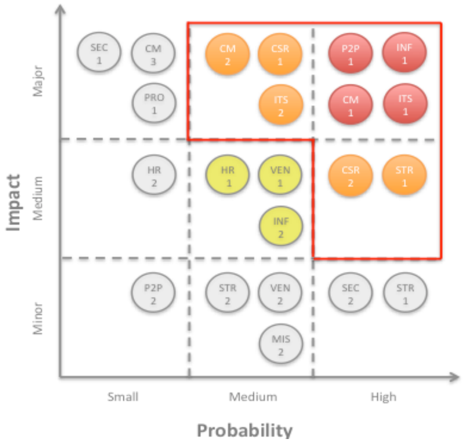

Illustration: Example of risk index report

> *Operational risk is the risk of monetary losses as a result of faults and errors in process, technology or skills or due to external factors (after Basel II definition). Operational risk may also include other risks such as fraud, legal-, physical-, and environmental risks.*

About the author:
Bjorn Ovar Johansson is the Founding Director of Senior IT Executive Limited and active as interim CIO in UK / EMEA. Based in Manchester, he also works as advisor on Operational Risk Mitigation and Performance Management in IT.

M: +447884838102 *E: boj@senioritexecutive.co.uk* *W: senioritexecutive.co.uk*