Cyber Crime Risk Management, *by Marios Kyriacou, Managing Director at MNK Risk Consulting (www.mnkriskconsulting.com)*

The landscape of cyber crime threats is increasing; it's a very broad risk area, involving large quantities of information and highly technical and specialised knowledge.

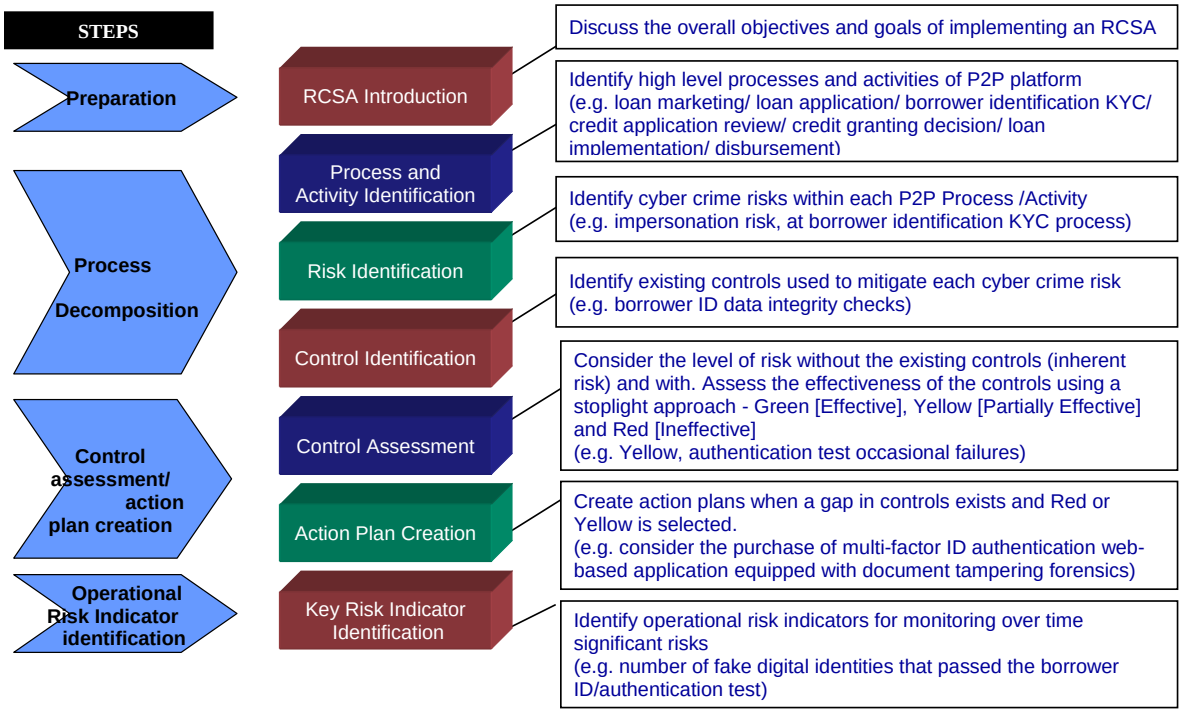
As a result, cyber security management becomes increasingly more complex for financial institutions. Can cyber crime be managed effectively and in a cost efficient manner?

Cyber crime is just another type of operational risk. In fact it is included in the operational risk event types defined by Basel under External Fraud. External fraud and cyber crime risk can be managed through the implementation of a risk management framework that relies on the following components:

- Risk and Control Self Assessment (RCSA)
- Capturing and management of historical risk incidents related to cyber crime
- Scenario Analysis using external data of similar incidents occurred to peer institutions
- Setting up a Key Risk Indicator monitoring program
- Modelling the occurrence and loss severity of cyber crime risk.

RCSA

An example on cybercrime is illustrated below:



Historical Risk Incidents

An incident is broken down into three elements: cause, event, effect. Recording historical incidents on cyber crime risk means understanding the event, what factors have led to that event and its financial or other impacts. Institutions should maintain internal incident databases using a preset taxonomy, recorded cyber crime threats could be categorized into the following event types for instance: Human error, Theft/loss, Insider Misuse, Social, Malicious software, Hacking, Product flaws.

Once events have been identified with respect to their type, the analysis of the cause and impact follows. The cause of events is necessary if a manager wants to track down the root of the problem in a business process; preventing other events with similar cause from occurring in the future.

What about the effect and the loss impact in particular? Managers need to prioritise the types of operational risks they should manage and mitigate. The ranking of risks would depend on the financial impact, and or other indirect impacts such as reputational damage.

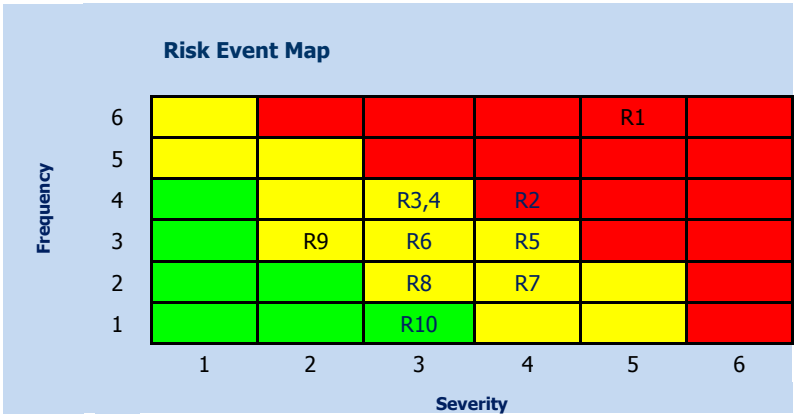
Incident statistics such as the single most severe loss event, the total loss amount per year, the most frequent cause, the top-ten most severe events, enable management to identify any patterns and have a better understanding of the risk profile. In addition it helps the Risk Manager to initiate corrective measures, follow up on their timely implementation and monitor their effectiveness.

Scenario Analysis and External Data

Potentially disastrous scenarios could be identified using internal incident data as well as external actual loss data; the latter may be sourced from either commercially available public loss databases or industry-pooled consortia (e.g. the Operational Riskdata eXchange Association ORX).

Key Risk Indicators (KRIs)

KRIs are dynamic data indicating the level and trend of specific risks. They focus on the significant risks which typically emerge from the analysis of RCSA results, historical cyber crime incidents and scenario losses described earlier. For example, with reference to the ten risks depicted in the heat-map below a Risk Manager could assign KRIs for the two risks (namely R1, R2) which scored high.



Modelling cyber crime risk

There are two stochastic processes that drive the measurement of cyber crime risk: the severity of losses and the frequency of events. Compounding these two stochastic processes results into the simulated distribution of possible future annual losses from cyber crime risk. From the simulated annual loss distribution one can then derive risk measures such as the annual Expected Loss (EL), the Value-at-Risk (VaR), and Expected Shortfall (ES). EL arises on a continuing basis in the 'normal' course of doing business and as such could be absorbed through P&L either by provisioning or (risk based) pricing. VaR looks at unexpected losses, whereas ES at catastrophic losses. Unexpected losses, although unusual, still need to be anticipated and covered through Tier 1 and Tier 2 capital reserves. Catastrophic losses (which are the largest in size of the unexpected losses) could be covered by insurance or other risk transfer techniques.