



Security & Threats CSR Balance of Power **Obsolescence** Democratic Peace International Regime World
Government State-Sponsored Terrorism Substitution **Geopolitics** National Decentralisation Cyberterrorism Supply Chain
Stability Diplomatic Sanctions Warfare Security Cooperation Developing Countries Nationality Narcoterrorism Non-State Nations
Transnational Relations **Analysis** Terrorist Attacks Spheres of Influence Market Awareness Acquisition Illegal
Trade BRIC Countries Import Controls and Restrictions Interdependence **Protectionism** Nuclear and Radiological Terrorism
Black Market National Boundaries and Borders Regional Conflict Barriers to Market Market share Clash of
Civilizations **Technology Investment** Political & Ideological Terrorism **Consulting** Industrial Espionage
Transnational Crime Multinational Companies Armaments Policy Defence **Budgets and Spending** Bilateral
Defence Cooperation **Risk** Regional Security Structures Multilateral Defence Cooperation
Military-Industrial **National Debt** Trade Sanctions Defence Reform Terrorist Financing **Competition**
Commoditisation Stability Pricing Strategy Security Policy **Cyber Fraud** Corporate Fraud Security Dilemma e-Business Realpolitik
Client satisfaction **Workshops** Emerging Markets **Intelligence** Transition Economies
Military Threat Perceptions Balance of Payments Consumption Corporate Espionage Consumer
Confidence **Economic Recovery** Chemical and Biological Terrorism Capital Market Readiness Military
Sanctions **Equity** Economic Sanctions Polarity Stakeholder value Monopolies & Cartels Defence
Cooperation.....**AEROSPACE DEFENCE SECURITY**

The Solomon Barnes Consultancy

Threat Modelled Risk



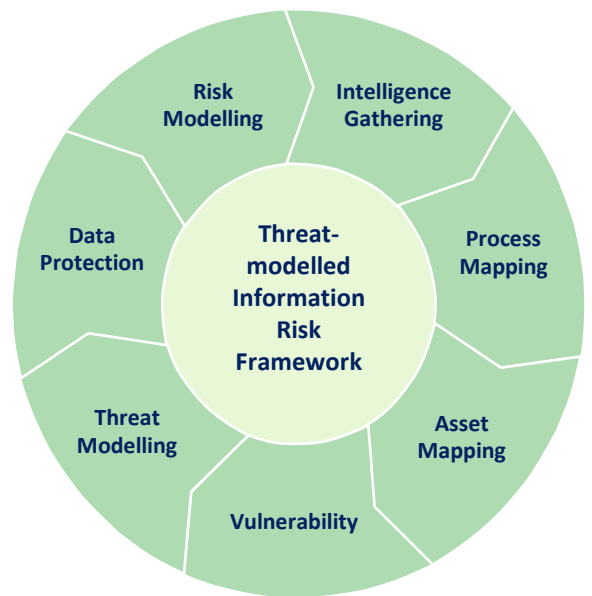
Threat-Modelled = Risk-Informed Management

The Risk Modelling Cycle - 1

The methodology describes a framework for creating and maintaining a threat-modelled information risk framework.

The risk framework is used to enable decision making for security related issues for organizations, based on accurate threat modelling, a quantifiable asset valuation, and 'what if' scenarios that consider both the deterrence factors of a security measure or process, as well as their cost.

The methodology is not a point-in-time solution, but rather a continuous practice in evaluating the current posture based on past experiences, up-to-date intelligence feeds, recognition of trends, and a valuation of the organizational assets (tangible and intangible) along with their transient value (i.e. marketing/reputation/legal implications of it on top of the actual base value).



Intelligence Gathering

The intelligence-gathering phase is performed on two levels – informational and human. The informational layer is focused on gathering data from outside the organization from forums, blogs, social media sites and other public resources that have any relation to the organization, its employees, partners, suppliers, customers and products. This phase, usually based on 'open' sources [OSINT], requires the correlation of all the collected raw data after it has been standardized and sanitized.

The human layer is composed of intelligence gathered from, conversations, meetings with customers/partners/competitors/stakeholders, conferences & exposure to public or private events, and other resources that do not have a technological feed directly available from them.

Business Process Mapping

The business process mapping phase is the first step in identifying all the data flows in the organization, every aspect of the business operations, and any interactions that the business has is required for its ongoing operations with external resources (3rd party suppliers, partners, resellers, etc.).

The mapping should take into account primary the critical processes (money generating, or critical to the business operations from an intellectual property usage/protection perspective), and then the rest of the operations.

This phase should also create an initial identification of critical information assets, and critical data-flow paths to be used later in the threat modelling and risk management process.





Threat-Modelled = Risk-Informed Management

Asset Mapping

The asset-mapping phase is designed to provide the organization a clear view of all its assets, and the participating business processes that relate to these assets.

The asset mapping should include as a minimum the following components: description and identifier, classification and categorization, owner, location, access rights and handlers, business processes that use/relate to the asset. Additionally, a valuation of the asset is required for every aspect of the business that the asset relates to: including “replacement” value, and additional intrinsic values from a compliance standpoint, and a marketing/competitive damages value. Values may differ with each threat scenario and as such they all need to be defined and available for the threat modelling and risk modelling.

Vulnerability and Exposure Analysis

Based on the asset mapping, and the technological and business process architecture of the data-flows relevant to the organization, a vulnerability & exposure analysis is performed. This phase is not limited to technical vulnerabilities of some application or server, but also includes risks to business processes, 3rd party providers involved in the process, and any other aspect of the asset lifecycle.

The human factor can be usually evaluated based on the level of education in relation to the criticality of the assets, and the general awareness to risks related to the business process at stake. In either case – technical or human, it is important to realize that location and access are ubiquitous, and again – both logical as well as physical ones.

Each vulnerability should include as much information on the ability to exploit such opportunity to gain access to the information assets, as well as the current countermeasures placed in order to mitigate such incident.

The protections should also be identified and classified accordingly. At this phase, the key technical evaluations should be focused on the less standard devices such as mobile equipment, custom systems and applications, control systems, embedded devices, etc. This is to ensure that the entire infrastructure have been reviewed – just as if a motivated attacker would approach it.

Threat Modelling

In the threat-modelling phase, the relevant threats for each asset are identified, correlated to the intelligence gathered, and evaluated on the basis of the threat’s exposure frequency to the asset, and its capability to successfully attack the asset.

This modelling should be expressed in statistical terms that can be repeated independently even when based on different subject matter expert opinions.

Dataflow Protections

The last element of the base evaluation phase is the analysis of any means that are designed to detect incorrect data flows.

This includes DLP systems (Data Leak Protection/Prevention), as well as business processes that are in place to prevent information from getting to the wrong places inside the organization and outside of it. All the communication systems should be included in this phase – data, voice, image, and physical.





Threat-Modelled = Risk-Informed Management

Risk Modelling

Based on all the prior phases, a risk model can be calculated based on the expected frequency for a security incident (based on the threat modeling, protections, vulnerabilities and exposures), and the severity of such an incident (based on the threat capability, the asset valuation and data protections).

A risk model should be created for all the identified assets, and a quantitative compound score applied to it, based on the expected liability it yields and the probability/frequency.

What-If Modelling

A what-if scenario can be analyzed for both incident handling, as well as placing, removing, & modifying controls over information assets. This modelling is critical in the decision making process for organizations who need to adapt to a changing landscape, or when an acquisition of new technology is evaluated. Both infrastructure, as well as security measures can be modelled to see how they reflect on the overall future risk posture of the business.

Closing the Cycle

The full cycle from intelligence gathering through risk modelling to risk management is ongoing

It should be updated as a basic risk management practice, and used to support informed decision-making for both technologies, as well as business processes.

The model should be challenged and assumptions adapted from different areas of the organization and refined in order to reflect the most accurate status:

- In technological terms the threat landscape is always shifting
- In business terms competitors adopt new strategies, markets evolve, economic and fiscal factors impact the business, and as social trends & regulatory factors change.

Risk Management and Decision Making

Having established a profound risk model, decision-making and risk management can be more confidently business-oriented. Senior management needs to define its tolerance to risk for each one of the assets or processes it owns.

This is achieved by analysing the risk capacity provided by the risk model, identifying the resources & capabilities that the organization already possesses to mitigate the risk, and any applicable regulation that may contribute to defining the risk tolerance.

Additionally, at this phase, any value propositions that would affect the risk model should be identified and analysed, and the overall impact to the risk posture should be calculated for these, along with the required internal and capital resources of such a proposition.

Finally, the organization can view the comprehensive risk model along with all the alternatives for impacting the risk posture and their cost & resource impacts in a way that allows informed decision-making processes.





A Security Risk Diagnostic sets the foundation for a more comprehensive full-day assessment of your security risk profile. In an exploratory meeting, our experts review the following issues with you to prioritise focus areas, and raise your awareness of the following key parameters for evaluating security risk.

Security Awareness – How do you evaluate your internal processes & procedures for physical & IT security.

Risk Monitoring Processes – How do you identify & characterise potential threats and risk

Management of Security Risk – How do you integrate assessment of threat and vulnerability when considering options for investment & innovation

Are you aware of the number, nature and source of the security incidents you have suffered to date

Have you identified what are your business's key assets, at risk from attack

Have you assessed the business impact from the compromise of information assets

How would you describe your strategy to manage, mitigate and minimise security risk

Do you feel confident in the processes and technologies in place to execute your security strategy

How have you earmarked the level investment to ensure they remain effective

Do you conduct an rolling reassessment of security risk, and a regular review of strategy

Have you been aware of new & emerging threats from industrial espionage, or cyber crime

Are you confident that there is appropriate training of staff to recognise and respond to security risk

Where does responsibility for security risk 'sit' within the senior management team

