Protective Security Risk Management

CPNI
Centre for the Protection of National Infrastructure

Effective security risk management requires an organisation to have defined **governance** with oversight of **protective security management systems.** As risk owners, senior leaders need to be conversant with the key principles of protective security in order to guide their strategic decision-making.

Stakeholder engagement and security risk assessment support effective decision making. This model highlights some key steps that should be taken when considering the wider process of protective security risk management, rather than a specific format for risk assessment itself.

1. Identify Assets & Systems

All organisational **assets** and **systems** that are necessary for the delivery of effective operations, or are of **specific** organisational value (e.g. commercially sensitive information), should be identified.

These may be: physical items, data stored or transmitted in any format (e.g. hard or electronic copy), personnel with specific knowledge/skills, or crowded places requiring protection. Engaging a suitable organisation-wide stakeholder group to conduct this exercise, and provide ongoing support to the risk assessment/management process, will provide the greatest benefits.

2. Categorise & Classify

In order to ensure that the appropriate level of resource is used in implementing risk mitigations, assets can be **categorised** in relation to their level of criticality in supporting your business. Criticality levels can be based on the level of harm any loss of identified assets may have to both your business and third parties. Information should be assessed and **classified** according to its sensitivity and the impact of compromise, loss or misuse.

In a similar way to levels of criticality, the classification of information can be based on the amount of damage caused to your organisation and/or partners as a result of compromise. Having your assets and information assessed in this way will allow for additional nuance in risk mitigation. For example, the implementation of counter espionage rather than, or in addition to, counter terrorism measures.

3. Identify Threats

Threats to your organisation should be **identified**. These may be national security threats, such as terrorism or hostile state threats, or more local and specific threats. Relevant threat information can be obtained from sources including: organisational knowledge and learning, intelligence agencies, technical authorities such as CPNI, the National Cyber Security Centre (NCSC), the police, other government agencies both in the UK and overseas, partner organisations and peer groups (external stakeholders). Good quality threat assessment data will help to inform your likelihood and impact assessments.

4. Assess Risk

Risks are identified **threats** or vulnerabilities, aligned to assets, that have been **assessed** for their **likelihood** (of the threat event occurring) and **impact** (to the organisation and/or third parties) should the threat transpire. Processes exist for conducting such a risk calculation and your organisation will likely have an accepted preference. The ability to understand the uncertainties and confidence levels of your assessments and to prioritise your focus and resources to those scenarios of greatest assessed risk is the fundamental aspect of this principle. This should be aligned to the expressed risk appetites of senior decision makers.

5. Build Risk Register

All the data gathered in working through these principles should be **recorded in a protective security risk register.** The format of the register is a matter of individual preference, although compatibility with existing organisational risk registers and risk management processes is recommended. It is important to **ensure** sufficient detail is captured as the more detailed the risk register, the more useful the risk assessment will be, thus allowing:

Allowing:

- Senior decision makers to make informed judgements on risk appetite and resource allocation;
- Practitioners and stakeholders to develop and implement appropriate risk mitigation plans;
- Timely review when required;
- Effective audit of decision making;
- The building of the risk register as a **business as usual** mechanism for managing protective security practices.

6. Protective Security Strategy

Developing a **strategy** for mitigating the risks identified will help optimise the implementation process. Starting with highest priority risks, stakeholders should review existing protective measures. Where mitigations are assessed as inadequate, additional measures should be proposed for approval by the decision maker(s). It may be beneficial to align a strategy with any regulatory requirements which necessitate compliance to standards.

7. Development and Implementation

Poorly defined requirements for the implementation of new measures can lead to proposed solutions which do not address the vulnerabilities, are over engineered, or do not represent value for money. Once agreement is reached to mitigate the identified risks, organisations should seek to develop their implementation plans by creating a statement of need, an example of this is **the CPNI operational requirement process**. At the end of the process an organisation should have a clear, prioritised list of protective security mitigations, which span security disciplines, linked to technical guidance needed to implement them.

8. Review

Risk assessment/management is cyclical and reviews should be conducted on a regular basis or when required, such as: on a change in threat; change to operational environment; or to assess the suitability of new measures implemented.

Additional information, including recommended internal stakeholders, and an example methodology for conducting security risk assessment to counter the insider threat, can be obtained at **www.cpni.gov.uk** or via your CPNI Adviser.