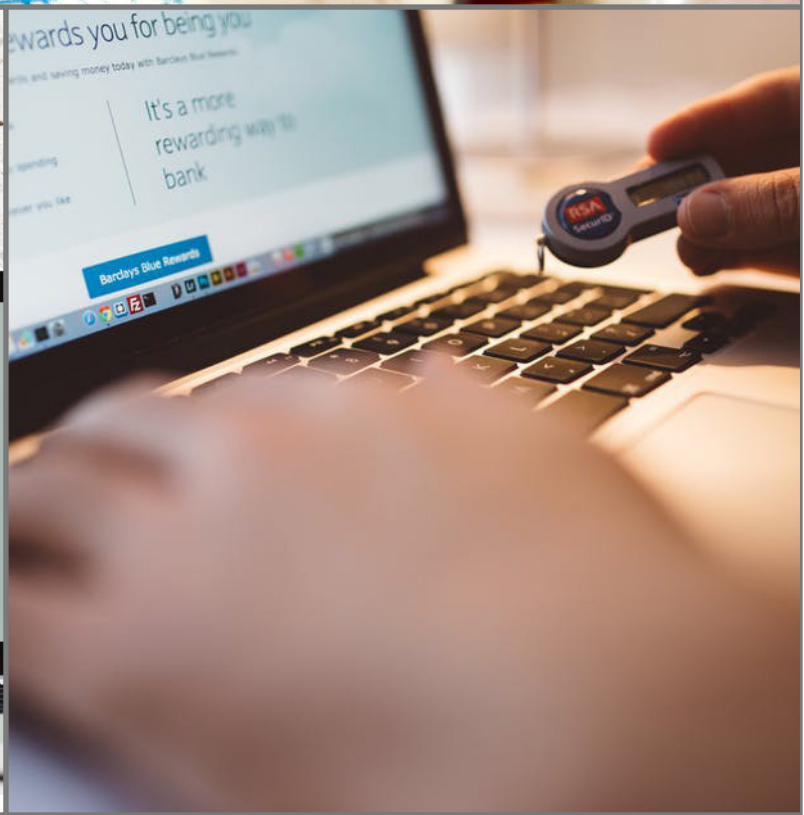
INTRODUCTION TO RISK



There are three types of threat to information assets facing organisations today[1]. There is the insider threat. There is the cyber threat. Thirdly there is the cyber threat that feeds off the low cognisance of being a target, otherwise termed the low 'threat IQ', of the insider[2]. What needs to be established is which one threatens the organisation. Inside these three threats are many variants that feed off whichever vulnerabilities an organisation has at any particular time. And they vary increasingly if that organisation becomes a target, because it has something others want, financial, commercial or political, or because it represents something others find offensive.

Analysing which particular threats are risks to an organisation requires knowledge of the cyber variants and how they exploit vulnerabilities. Managing that risk requires particular skill to balance the most effective defences needed for the ongoing successful business of the organisation. IL7 has the technical knowledge to build perimeter defences against the cyber threat, to employ analytics and monitoring against the cyber threat and to utilise communication and consultancy to galvanise a corporate culture and reduce the threat IQ. The key is to understand the business and what business assets are valuable. Identify vulnerabilities and introduce controls to eliminate or mitigate them. IL7 has the experience to assess risks that a business can take to exploit a business opportunity and the expertise to identify measures to mitigate any effect if the risks taken become reality.

While successful risk management affects the likelihood and consequences of risks materialising, CESG are right to acknowledge that risk management in HMG has become tired and stale over the last few years. It is agreed that, as well as delivering benefits related to better informed strategic decisions, it facilitates successful delivery of change and increased operational efficiency. Other benefits might include reduced cost of capital, more accurate financial reporting, competitive advantage, improved perception of the organisation, better marketplace presence and, in the case of public service organisations, enhanced political and community support. However, methodologies can, and have been, be too restrictive and need more business focus. IL7 recognises the value of risk management and will seek to inject new positivism and energy into its practice.

In the case of HMG IS1/2, the structure works, being based on domain based security (DBSy[3]), but the fundamentals have changed. We no longer have the same classifications, or protective markings[4], the business impact levels have passed into obscurity and the prescriptive CESG / CLEF evaluated product lists no longer apply. The calculated outcomes and the controls required at certain levels of classification or risk are unclear and the Baseline Control Set (BCS) is difficult to reference. IL7 has worked with IS1/2 for many years and produced in that time a plethora of Risk Management & Accreditation Document Sets (RMADS) and still does. Even without the BILs the process works as the governance chain are not trained in other methodologies and accept IS1 as the HMG method. Its continuing benefit, as with other methods, is that it makes those involved think about the issues; most

[1] For the purposes of this exercise, acts of God and natural disasters are treated as hazards, insurable risks, treated with back-up, business continuity. This paper concentrates on the risk to information assets.

[2] The 'insider' here is a collective term that includes the privileged user, the normal user, the service provider, service consumer or supplier as all could be duped into being infected in a way that can endanger the target.

[3] Initially called the Domain Based Approach, it was developed alongside Purple Penelope to support the MOD's increasing need for interconnections between systems operating at different security levels.

[4] Government Security Classifications Annex – Controls Framework April 2013, Ref [10].

threats are caused by people and the DBSy model concentrates on threat actors. It is personal or group capabilities and motivations that are featured. IS1's failing is that it does not in itself generate a security management system that communicates across the business, nor does it monitor its own effectiveness. Coupled with the weakness of the calculation parameters, enthusiasm is waning and alternative approaches are being sought.

IL7 intends to help organisations move away from IS1/2 and other inefficient methodologies. They are too cumbersome, not agile enough to defend and attack the twin axis of cyber and insider threats. There is no room in the world for the traditional long winded, trackable risk assessment, the paper trail of questionnaires and worksheets. The world is moving rapidly forward. Putting into place best practice procedures and proven technology eliminates the majority of threat without procrastination and protracted analysis. When the obvious threats are exposed a detailed cost benefit analysis becomes unnecessary. But there is a very real place for risk assessment and organisations still need to account for what they spend on defence against cyber and insider threats. They still need to measure and record the amounts spent if they are to improve. And risk assessment and risk management themselves are countermeasures against these threats. They, together, applied in a consistent framework, provide the communication within the organisation to build a culture where everybody identifies the risk and works together to eliminate it. In order for this to work, the risk management process adopted by an organisation must fit the business model, the business goals of the organisation.

The recent report from the Nation Audit Office (NAO) [Ref 1] recognises the increasing dependencies between central government and the wider public sector. Driven by the increasing information flows, the demands of public service provision and shared technical infrastructure. The report also says that "the NCSC is designed to work with government and the private sector: whether it has the capacity to do so effectively remains to be seen". IL7 would join that group of consultancies to add flexibility to that capacity. IL7 recognises that NCSC, as the technical authority, has obligations beyond the limited fields of central government and can no longer confine its recommendations to standards that suit the HMG community. Even the world of central government has changed widely since the early developments of domain based security. The world is now faced with the digital economy, digital government and the plethora of new threats associated with embracing the opportunities and risks of cyber. Threat actors are different, more organised, more technically proficient and the technology in their hands more powerful and sophisticated. In past experience HMG organisations have static threat models. This was reflected in the IS1 calculations. This results in static controls and one-dimensioned defences that do not change over time. These threat models need to be frequently re-examined by stakeholders who are cogniscient with both the business and the cyber threat landscape.

IL7 recognises the need for more flexibility in getting the risk message across. Whether it's the cyber threat or the insider threat, the risk needs to be quantified and communicated clearly. Areas of local government and health need faster, less bureaucratic methods of risk assessment. Others have different control contexts to address and face different regulations and frameworks of compliance. While HMG IA governance is still underpinned by the accreditation cycle whereby SyAc and Accreditor both know the process, this is not guaranteed to continue. Nor, necessarily, does such governance exist universally outside central government. Stakeholders in the risk decision are no longer IAOs, SIROs or Accreditors. The Business Case for risk, and the Security Case in IS1/2 terms, needs to be

made to the business owner, the one that will pay for the treatment, and suffer the consequences for not doing so. They might not understand IS1 terminology and therefore they need to be addressed in the business language and context they understand. IL7 also recognise that this flexibility in communication needs to be consistent and repeatable so it needs to have a framework. The frameworks offered by ISO 31000, Ref [2], and ISO/IEC 27005, Ref [6], meet these requirements but often methodologies purported to be derived from them are fixated on burdensome, time consuming surveys.