The last five years has witnessed a significant increase in malware sophistication with the latest being Stuxnet, Flame and Gauss class of worms. Stuxnet being categorised as sabotage worm famously attacking Iranian uranium enrichment industrial processes in 2010. The worm initially spreads indiscriminately, but includes a highly specialized malware payload that is designed to target Siemens supervisory control and data acquisition (SCADA) systems that are configured to control and monitor specific industrial processes. Both Flame (aka Skywiper) and Gauss are categorised as espionage worms although they are reputed to have sabotage capability. In 2012 Flame infected governmental organizations, educational institutions and private individual with the aim of stealing strategically important information including intelligence, banking and intellectual property data, and sensitive private information. Geographically, Flame targeted mainly Middle Eastern countries. Gauss, also from 2012, is thought to be a development of Flame with a primary objective of collecting online banking details. We the advent of these new sophisticated worms with increased effectiveness and functionality, we must be cognisant that major systems such as those that support financial services, critical infrastructure and industry are at risk.

The level of risk of attack from this new sophisticated malware is difficult to quantify as standard risk analysis models lack reality owing to rapidly changing technology and an incomplete view the overall security of target systems involved. An attacker exploits new technologies and strives to discover new routes into target systems for new malware. In order to understand the true malware risk faced by organisations any model developed to support the analysis must be able to address a statistically combination of all feasible attack scenarios as an attacker may chose a combination or routes to enhance a successful attack mission. Moreover, since all parametric aspects of a sophisticated cyber-attack cannot be quantified, a degree of expert judgement must be applied.

In this paper we propose a more functionally effective cyber-attack risk analysis model that can be used by institutions and organisations to identify the most cost-effective counter measures. This identification will be made easier as the model will have attack scenarios at its foundation. Countermeasures can therefore be assessed within an associated scenario in order to understand overall cost-effectiveness as the combinational effect will be carried through to a composite result. The proposed model will also utilise both qualitative and quantitative methods in order to be able to acknowledge the benefits of expert judgement combined with hard analysis.

The structure of this paper follows: an overview to the new espionage malware; a functional description of the proposed model together with scenario identification; direct attack analysis; attack through mules; inside the target organisation; bring it all together; summary and conclusions.