Accepted Manuscript

Title: Introducing cybernomics: a unifying economic framework for measuring cyber risk

Author: Keyun Ruan

PII: S0167-4048(16)30140-7
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2016.10.009
Reference: COSE 1052

To appear in: *Computers & Security*

Received date: 28-1-2016
Revised date: 1-10-2016
Accepted date: 25-10-2016

Please cite this article as: Keyun Ruan, Introducing cybernomics: a unifying economic framework for measuring cyber risk, *Computers & Security* (2016), http://dx.doi.org/doi: 10.1016/j.cose.2016.10.009.

Introducing cybernomics: a unifying economic framework for measuring cyber risk

Keyun Ruan, sci@ruankeyun.com

Address: EY, Harcourt Centre, Harcourt Street, Dublin 2, Dublin, Ireland

Abstract

This is the first in a series of papers on the risk measures and unifying economic framework encompassing the cross-disciplinary field of 'Cybernomics'. This is also the first academic paper to formally propose measurement units for cyber risk. In this paper, multidisciplinary methodologies are used to apply proven risk measurement methods in finance, medicine and economics to define novel risk units central to cybernomics. Leveraging established risk units – MicroMort (MM) for measuring medical risk and Value-at-Risk (VaR) for measuring market risk – BitMort (BM) and *hekla* (named after an Icelandic volcano) are defined as cyber risk units. Risk calculation methods and examples are introduced in this paper to measure cost-effectiveness of control factors, articulate an entity's 'willingness-to-pay' (risk pricing) for cyber risk reduction, cyber risk limit, and cyber risk appetite. Built around BM and *hekla*, cybernomics integrates cyber risk management and economics to study the requirements of a databank in order to improve risk analytics solutions for: 1) the valuation of digital assets; 2) the measurement of risk exposure of digital assets; and 3) the capital optimization for managing residual cyber risk. Establishing adequate, holistic and statistically robust data points on the entity, portfolio and global levels for the development of a cybernomics databank is essential for the resilience of our shared digital future. This paper explains the need to establish data schemes such as International Digital Asset Classification (IDAC) and International Classification of Cyber Incidents (ICCI).

Keywords

Cybernomics, cyber risk unit, economic modelling, risk analytics, enterprise risk management

1. Introduction

The trading of innovative digital goods and services has become so critical to economic competitiveness that it is the reason why over half of the companies on the Fortune 500 have disappeared since the year 2000 [1]. While advancements such as cloud computing and Internet of Things (IoT) are reshaping the backbone of infrastructure and supply chains, breakthroughs in Artificial Intelligence (AI), 3D printing, crypto-currency, and virtual reality are transforming Information Technology (IT) from a supportive operational role into the business critical role of core value creation. In the meantime, cyber risk has also become one of the top three global risks [2] with significant economic implications for businesses. Companies' cyber security ratings [3] are now being considered in investment assessments [4]. After the General Data Protection Regulation (GDPR) comes into effect in 2018 in the E.U., companies can be fined a maximum 20 million euros or 4% of global turnover for data breaches [5]. As cyber security enters boardroom discussions worldwide and fills senior executives with fear, billions of investment dollars have been allocated to strengthening security controls [6] with limited measurement on returns. The economic implications of cyber risk have to be quantified into monetary value for cyber risk management to transform from a compartmentalized technical issue into a business issue, formally integrating it into