COMPUTERS & SECURITY 65 (2017) 77–89

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Introducing cybernomics: A unifying economic framework for measuring cyber risk

Keyun Ruan *

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

ARTICLE INFO

Article history:
Received 28 January 2016
Received in revised form 1 October 2016
Accepted 25 October 2016
Available online 11 November 2016

Keywords:
Cybernomics
Cyber risk unit
Economic modelling
Risk analytics
Enterprise risk management

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 and medicine 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 are 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).

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 (World Economic Forum, 2016). 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 (Allianz., 2016) with significant economic implications for businesses. Companies' cyber security ratings (BitSight cyber security rating) are now being considered in investment assessments (Bloomberg, 2014). 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 (General Data Protection Regulation). As cyber security enters boardroom discussions worldwide and fills senior executives with fear, billions of investment dollars have been allocated to strengthening security controls (Forbes, 2016) 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

* *E-mail address:* sci@ruankeyun.com.
http://dx.doi.org/10.1016/j.cose.2016.10.009
0167-4048/

business issue, formally integrating it into Enterprise Risk Management (ERM) frameworks such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Data are one of the cornerstones of any risk measurement methodology. The current lack of quantification and consistent measurement of cyber risk is a direct result of insufficient quality data points and data sharing. Cyber risk is the likelihood of economic loss from cyber incidents, but data about such losses have not been adequately collected statistically. There are a wide range of incidents that can cause economic loss, but data breach is the only incident that has been tracked for more than a decade. The availability of breach loss data in different jurisdictions is correlated to when mandatory breach reporting schemes were introduced. More data breaches have been recorded in the U.S. than in the E.U. (Privacyrights.org; Reported data breaches in Europe 2005–2015). California has seen the largest amount of data breaches according to publicly available sources, because it was the first state in the U.S. that introduced mandatory breach reporting[1]. Nevertheless, regulatory support is not the only reason why public access to quality incident and loss data sources is still limited. Security and monitoring companies hold incident and loss data as proprietary competitive advantage. Companies suffering losses prefer to cover them up, while forensic investigators are forbidden from sharing details of incidents.

A robust cyber risk databank not only requires adequate data points, but also significant improvement of data quality. Despite a large number of cyber risk management frameworks, risk assessment methodologies, quantitative risk models, industry surveys and security analytics tools in the market, little has been done to standardize the measurement unit for cyber risk. While more established fields such as mortality risk management and financial risk management measure risk against defined risk units, the absence of a common point of reference for cyber risk makes it difficult to compare different approaches in reducing exposure, assess cost-effectiveness of countermeasures, optimize return on cyber risk spending, and most importantly, structure the risk databank in a consistent and statistically robust manner.

Adequate data collection should occur on the entity level, portfolio level and global level. This is evident from the challenges faced by the cyber insurance industry today. Although cyber insurance premiums are estimated to triple to $7.5 billion in annual premiums by 2020 (Insurance Business, 2015), 98% of businesses in the U.K. are still "under-insured" (Marsh, 2015). The lack of quality risk data is a key challenge (World Economic Forum, 2015) and a key reason why this market opportunity is still under-exploited. For the insureds, there is a need to articulate entity-level cyber risk appetite into monetary value in order to determine how much residual risk should be transferred to insurers. For insurers and reinsurers, firstly, there is a need to profile risk exposure of entities. Secondly, there is a need to quantify accumulated risk on a portfolio of entities caused by use of a shared technology platform (such as cloud computing) and hyper-connectivity in the digital supply chain (Centre for Risk Studies and Risk Modeling Solutions, 2016).

[1] California S.B. 1386 was enacted in 2002 and became effective on July 1, 2003.

By integrating cyber risk management and economics into cybernomics, this paper aims to conceptualize a unifying economic framework to better address data challenges in cyber risk measurement discussed above. This will also be the first academic paper to formally propose measurement units for cyber risk.

The remainder of this paper is organized as follows: Section 2 covers related work in areas of research that are relevant to the cybernomic framework. Section 3 introduces novel methodologies used to develop components of cybernomics. Section 4 formalizes the theory of cybernomics. Risk calculation methods are demonstrated in Section 5, and discussions are presented in Section 6. Finally, the last section offers some concluding comments and suggests future work.

2. Related work

2.1. *The financial valuation of digital assets*

Valuation is the process of estimating the value or worth of an asset or an investment. It is a fundamental subject of study in philosophy, economics, finance and risk management. Currently there is no generally accepted approach to measuring the value of digital assets, the major barrier being a lack of understanding of the nature of information as an economic good. Ad-hoc valuation methods are in use for the valuation of tangible and intangible assets including estimations based on cost of production, cost of replacement, impact analysis etc., but digital assets are far from being fully integrated into general economic laws.

ISO/IEC 27002 defines an asset as anything that has value to an organization. Moody and Walsh (1999) argue against the legacy categorization of digital assets, i.e., software and hardware are merely mechanisms used to create and maintain information. Information has become the underlying business asset that is producing value and has both service potential and economic benefits to the asset owner. Unlike traditional economic goods and services which are classified by internationally recognized standards such as the NICE Classification (NCL) (Nice Classification), there is no universally accepted taxonomy for digital goods and services that can be used to monitor their production cost and market value. The categorization of digital assets has to reflect their economic functions first before their value can be properly assigned.

2.2. *Cyber risk management*

Cyber security is a risk management discipline (Blakley et al., 2001; Spears, 2005), and information security risk is a part of an entity's total risk (Finne, 1996). All risks can be calculated as:

$$Risk = Likelihood \times Consequences, \tag{1}$$

And cyber risk is a function of:

$$R = \{s_i, p_i, x_i\}, i = 1, 2, \ldots, N, \tag{2}$$

where

Table 1 – Qualitative and quantitative risk management methodologies.

Qualitative methods	Quantitative methods
• The IT Infrastructure Library (ITIL) • Control Objectives for Information and Related Technology (COBIT) • ISO/IEC 27005:2011 • Information Security Forum (ISF) Simplified Process for Risk Identification (SPRINT) and Simple to Apply Risk Analysis (SARA) • Operational Critical Threat and Vulnerability Evaluation (OCTAVE) • NIST Special Publication 800-53 • NIST Special Publication 800-37 • ISO/IEC 31000:2009 • Consultative, Objective and Bi-functional Risk Analysis (COBRA) • Construct a platform for Risk Analysis of Security Critical Systems (CORAS) • Business Process: Information Risk Management (BPIRM)	• Information Security Risk Analysis Method (ISRAM) • Central computer and Telecommunication Agency Risk Analysis and Management Method (CRAMM) • BSI Guide- RuSecure- Based on BS7799 Standard • Cost-Of-Risk Analysis (CORA)

R – risk;
s – the description of a scenario (undesirable event);
p – the probability of a scenario;
x – the measure of consequences or damage caused by a scenario;
N – the number of possible scenarios that may cause damage to a system (Kaplan and Garrick, 1981).

A range of qualitative and quantitative cyber risk management methodologies as used in industry or proposed by academia are listed in Table 1:

Currently, qualitative methods lack granularity, objectivity and ability to assist in cost–benefit analysis, while quantitative methods lack efficiency, statistical robustness and reliable asset valuation (Suh and Han, 2003). In general, current cyber risk management methodologies have the following limitations:

- Current methods focus on technology and are limited in covering people, process and socio-economic risk factors (Spears, 2005).
- More accurate estimates often require access to data and knowledge that a single entity does not possess (Gerber and Von Solms, 2005).
- Predominant risk assessment frameworks such as ISO/IEC 27002 are structured based on security control domains. These methods comprehensively assess an entity's security posture but are not effective enough in assessing an entity's preparedness towards a set of high risk loss scenarios developed around critical digital assets.
- More fundamentally, the proliferation of risk assessment methodologies in the absence of a common point of reference has caused undesirable inconsistency in measuring cyber risk. This is unlike other risk fields such as finance and medicine.

2.3. *The economics of information security*

Many argue that an entity should not approach information security with a compartmentalized focus (Caralli et al., 2004; Cavusoglu et al., 2004; Chen, 2008; Gordon and Loeb, 2002; Hoo, 2000) with budget managed only by the IT departments (Neubauer et al., 2006). The economics of information security is a relative new area of research (Anderson and Moore, 2006) that emerged to align security investment with wider business processes (Neubauer et al., 2006).

Economics is the study and social science of human behaviour in relation to how scarce resources are allocated and how choices are made between alternative uses (Hackett, 2010). Economics studies mankind's activities, which are production, distribution, exchange, and consumption of goods and services that are capable of satisfying human wants and desires. The economic perspective of information security means providing maximum protection of assets at the minimum cost (Geer, 2004; Gordon and Loeb, 2002). If the budget is fixed, it then becomes an economic optimization problem (Geer, 2004). To integrate economics and information security, Gordon and Loeb (2002) propose an economic modelling framework for assessing the optimal amount of security as shown in Fig. 1. The optimal security level is when the sum of the cost of security control and losses from security incidents is at a minimum (Gordon and Loeb, 2002). Entities should not wish to continue applying security controls beyond this point because it is less costly to live with the situation (Courtney, 1982), thus it is cheaper to accept security risks (Mizzi, 2005).

Another economic perspective of information security is assessing cost-effectiveness of security controls. Given a fixed budget, entities should be able to spend in the most cost-effective manner to reduce its information risks (Gordon and Loeb, 2002). The cost-effectiveness justification approach attempts to justify each security control's costs and benefits to arrive at an optimal mix of security controls (Cerullo and Cerullo, 2005; Frosdick, 1997).

When it comes to the evaluation of information security investment, some financial methods of evaluation have been proposed (Anderson and Moore, 2006; Gordon and Loeb, 2002; Mercuri, 2003; Rodewald, 2005) based on Return on Investment (ROI) and Net Present Value (NPV), but none has been successfully validated with real-world data. Determining the reduction in the probability of a particular breach taking place is extremely difficult to estimate (Gordon and Loeb, 2006; Ryan and Ryan, 2006).

The main limitation of all methods analysed above is the lack of data points to gather and continuously maintain cost and loss information. Furthermore, cyber risk is a broader discipline than information security therefore an overarching framework must be in place to directly integrate cyber risk with economics.

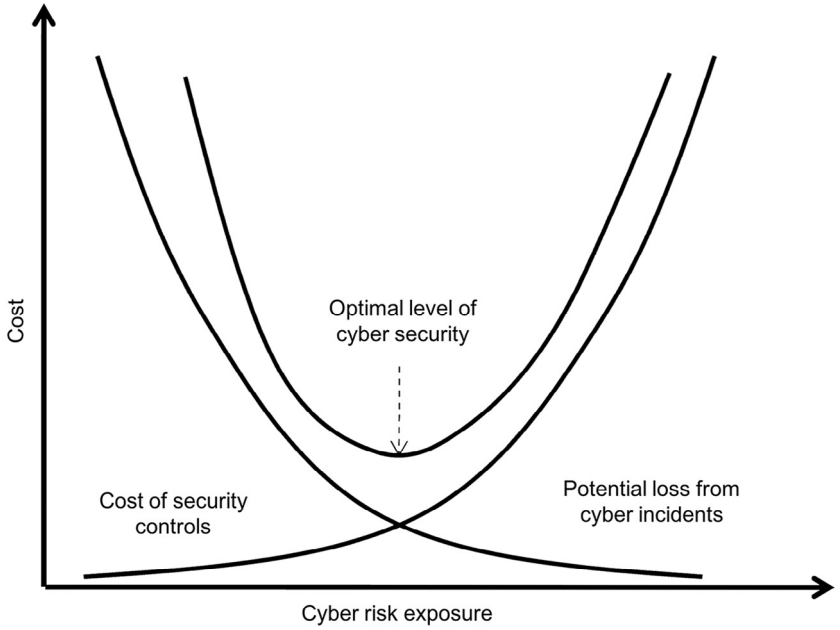

Fig. 1 – Optimal information security level (El Aoufi, 2009).

2.4. *Risk units and risk measurement*

The current state of cyber risk measurement is similar to the dawn of market risk measurement in the late 1980s (TLinsmeier and Pearson, 2000), which eventually gave birth to the profession of "quant" (quantitative analysts). In 1995, J.P. Morgan introduced an analytical tool, RiskMetrics, to compute *VaR* (Guldimann, 2000) using data points established in the bank.

> VaR is a measure of the maximum potential change in value of a portfolio of financial instruments with a given probability over a pre-set horizon (RiskMetrics, 1995). For a given portfolio, time horizon, and probability p, the p VaR is defined as threshold loss value, such that the probability that the loss on the portfolio over the given time horizon exceeds this value is p.

Also in the late 1980s in a different field of risk, Ronald A. Howard created a unit called MicroMort (MM)[2] to help inform patients about the risks of medical conditions or treatments and to consider those risks in making medical decisions (Howard, 1989). MM is a unit of microrisk.

> *1 MM is defined as 1 in 1 million probability of death.*

This description of risk has helped to place various daily activities in perspective. For example, people are exposed to 270 MMs from riding motorbikes in the U.S. in 1989. A person can be exposed to 1 additional MM from eating 40 tablespoons of peanut butter or smoking 1.4 cigarettes.

Another application of the MicroMort framework is to measure people's "willingness-to-pay" to avoid them.

> *The value of 1 MM is defined as the amount of money a person is willing to pay to avoid 1 MM.*

Of course, depending on risk appetite and financial affordability, different individuals can price the same risk differently. Today, MM has also been used to measure cost-effectiveness of countermeasures. Governments around the world price the reduction of 1 MM differently, e.g., U.K. Department of Transport prices the reduction of 1 MM at £1.60 (Department for Transport GMH), while U.S. Department of Transport prices the same at $6.20 (US Department of Transportation, 2011).

Coincidently in late 1988, the Morris Worm exploited buffer overflow vulnerabilities and became the first Internet worm. It caused an estimated economic loss between $100,000 and $10,000,000[3], opening a new chapter of risk. Yet, there has been no academic proposal of cyber risk units to date. This is the gap this paper aims to fill.

3. Methodology

3.1. *Applying economic theory of value to digital asset valuation*

An entity's digital value composition is like its digital DNA. It is the underlying attribute that determines the entity's inherent cyber risk. In this paper, digital assets are defined as assets

[2] MicroMort comes from the words *micro* and *mortality*.

[3] During the Morris appeal process, the U.S. Court of Appeals estimated the cost of removing the virus from each installation was in the range of $200–$53,000. Possibly based on these numbers, Harvard spokesman Clifford Stoll estimated the total economic impact was between $100,000 and $10,000,000.

in binary format the compromise of which will cause economic loss to its owning entity. Digital assets include Intellectual Property (IP), Personally Identifiable Information (PII), Mergers and Acquisitions (M&A) data, customer records, access credentials, encryption keys, business critical IT services, cloud services among others.

Similar to traditional goods and services, value of digital goods and services should be quantified and actively monitored while traded in global markets. A kilo of apples is sold for different prices in Germany and in Argentina. Similarly, a gigabyte of PII is sold for different prices in the U.S. and the U.K. (Intel Security, 2015). Monitoring the market value of digital goods and services requires an International Digital Asset Classification (IDAC) to be developed on the global level, similar to or as a sub-class of NCL established by the Nice Agreement in 1957. NCL is an international classification of goods and services, the tenth edition of which came into force on January 1, 2016, composing of 34 classes of goods and 10 classes of services.

To reflect the economic functions of digital assets, the categorization method below is used in this paper. Two subcategories are defined under core value assets to differentiate value conversion from digitization of traditional economics and value creation from intrinsic digital innovation.

Category 1 Core value assets. Digital assets which are directly part of goods or services that the entity profits from or is about, i.e., what the entity "is" digitally.
Category 1a Digitized assets. Goods and services digitized from traditional goods and services.
Category 1b Assets born digital. Goods and services that are intrinsically digital, e.g., software, bitcoin.
Category 2 Operational assets. Digital assets that support the creation, consumption and distribution of goods and service, i.e., how the entity is being "run" digitally.

An entity E's digital composition can be described by the ratio of its core value assets to operational assets:

$$CA : OA = \{c_i, p_i\} : \{o_j, q_j\} \quad i = 1, 2, \ldots, N_c,\ j = 1, 2, \ldots, N_o \tag{3}$$

where

CA – E's core value assets in bytes;
OA – E's operational assets in bytes;
c – a type of asset listed in IDAC which is of core value to E;
p – E's core digital asset c in bytes;
o – a type of asset listed in IDAC which is of operational value to E;
q – E's operational asset o in bytes;
N_c – the number of core value assets in entity E;
N_o – the number of operational assets in entity E.

Similarly, entity E's DA (digitized assets in bytes) to AD (assets born digital in bytes) ratio can also be calculated. An entity's digital value composition describes its nature of innovation. For example, a global retail company selling traditional goods will have a high OA:CA ratio, while a software development company will have a high CA:OA ratio and a high AD:DA ratio.

Theory of value is a generic term that encompasses all the theories within economics that attempt to explain the exchange value or price of goods and services. Intrinsic theories hold that the price of goods and services is objectively determined by labour, cost of production, etc., and not a function of subjective judgement (Marx, 1865; Smith, 1776). Subjective theories hold that for an object to have economic value it must be useful in satisfying human wants and must be in limited supply (Stigler, 1950). In neoclassical economics, the value of goods or services is seen as nothing but the price it would trade in an open and competitive market (Marshall, 1890). Using the above digital asset categorization, the existing theory of value can be applied to assets under Category 1:

Intrinsic value. The value of the digital asset is determined through fundamental analysis without reference to its market value, e.g., replacement cost or cost of production including labour, capital, infrastructure, taxation, etc. For example, the value of a piece of software is the amount of man-days, technology cost, intellectual property, and other costs that put into the development of it.
Market value. The value of the digital asset is the price at which the digital valuable would trade in a competitive market. For example, currently payment card numbers with CVV2 and date of birth are sold at $15 per record in the U.S. and at $30 per record in the U.K., respectively. Payment card numbers with full personal information are sold at $30 per record in the U.S. and at $35 per record in the U.K. (Intel Security, 2015).
Subjective value. The price of the digital asset is determined by the importance the entity places on it. For example, the value of sensitive email transactions is often subjective to how much the company values the content of the communications.

The value of Category 1a assets can be directly converted from their physical equivalents whenever possible, while the value of Category 1b assets requires their own valuation analyses.

Business Impact Analysis (BIA) can be used for asset valuation in Category 2. Business Consequences (BC) can include financial, legal, reputation and regulatory impact (Information Security Forum, 2000). For example, Amazon's 2013 service down time cost Amazon as a cloud service provider $66,240 per minute (Forbes, 2013).

A list of sample digital assets and their valuation are listed in Table 2.

Applying the existing economic theory of value to digital assets, digital theory of value is defined in this paper as:

The digital value of an entity is the sum of the aggregated value of its core value assets and the aggregated value of its operational assets.

Entity E's total digital value can be calculated as:

$$V = \sum_{i=1}^{Nc} cv_i + \sum_{j=1}^{No} ov_j \tag{4}$$

where

Table 2 – Sample digital assets and valuation method.

Digital valuables	Category			Valuation method
	Core value assets		Operational assets	
	Digitized assets	Assets born digital		
IP documented in digital format	✓			Based on intrinsic/market/subjective value
Digital IP such as software		✓		Based on intrinsic/market/subjective value
Critical business application			✓	Based on BIA
Encryption key			✓	Based on BIA, i.e., equivalent to the digital asset being encrypted
Login credential			✓	Based on BIA, i.e. equivalent to the digital asset it grant access to
Cloud services of a cloud provider		✓		Based on intrinsic value
Cloud services of a cloud consumer			✓	Based on BIA
3D printing design files		✓		Based on intrinsic/market/subjective value
Digital diary	✓			Based on subjective value
Bitcoin		✓		Based on market value
Digital photos	✓			Based on subject value/market value
Emails	✓			Based on subjective/market value
Scientific research data	✓			Based on intrinsic/market/subjective value
Metadata used for analytics		✓		Based on market value
Payment card number with CVV2	✓			Based on market value
Cyber-physical systems (e.g. drones) of a producer		✓		Based on intrinsic/market/subjective value
Cyber-physical systems (e.g. drones) of a consumer			✓	Based on BIA
Patented navigation software in self-driving cars of a producer		✓		Based on intrinsic/market/subjective value
Navigation software in self-driving cars of a customer			✓	Based on BIA

V – total digital value of entity E;
cv – value of core value asset c of entity E;
ov – value of operational asset o of entity E;
N_c – the number of core value assets in entity E;
N_o – the number of operational assets in entity E.

Taking into consideration the economic lifespan of digital assets, i.e., the expected period of time during which the digital asset is useful to its average owner, the valuation process of an entity's digital asset inventory should also help identify its "digital crown jewels".

3.2. *Applying medical risk factor categorization scheme to holistic modelling of cyber risk*

One of the purposes of a cybernomic databank is to identify Key Cyber Risk Factors (KCRF) correlated with an entity's risk profile. Cyber risk exposure of an entity is influenced by a wide range of dynamic technological and non-technological profiling factors, internal vulnerabilities and external threats. Motives of the attackers, in particular, are largely determined by non-technological factors (Huq, N. and TrendLabs Research, 2015).

In medicine, "modifiable risk factors" are factors that can be treated or controlled, including lifestyle factors such as cigarette smoking, physical inactivity and excessive alcohol use (Derby et al., 2000). "Non-modifiable risk factors" refer to any risk factor for a particular condition which cannot be modified. Age, for example, is the most important non-modifiable risk factor for stroke (Sacco, 1995). Cybernomics borrows this established risk categorization scheme, and categorizes cyber risk factors under the Cyber Risk Quadrant within four types of factors:

Technological factors .Attributes that are related to the usage of technology.
Non-technological factors. Attributes that are not related to the usage of technology, including people, process, socio-economic, geo-political factors.
Inherent factors. Intrinsic attributes based on nature of business, industry, core operations, goods and services the entity provide, or macro trends and attributes that have pan-industry impact on entities in certain geo-regions or even global impact. Inherent factors determine an entity's inherent cyber risk exposure, and are factors the entity cannot easily change.
Control factors. Attributes of the entity that are non-intrinsic and can be changed or improved. Control factors are a reflection of an entity's control effectiveness against cyber loss, and are the subject of investment when it comes to risk mitigation.

Some examples of various cyber risk factors are shown in Table 3.

An entity's residual cyber risk is calculated as:

$$\textit{Residual cyber risk} = \textit{inherent risk} \div \textit{control effectiveness}, \quad (5)$$

So the cyber risk factor categorization scheme above makes the calculation of an entity's residual cyber risk very straightforward. It can also help the entity holistically identify, monitor

Table 3 – Cyber risk quadrant.

	Technological factors	Non-technological factors
Control factors	Implementation of firewall Implementation of anti-virus applications Level of application security Deployment of Security Operations Center (SOC) Percentage of workload in the cloud Design of security architecture Network segregation	Business process design and criticality Cross-function incident response competencies Training and awareness Location of business Cyber risk team structure Outsourcing strategy Appointment of a Chief Information Security Officer (CISO)
Inherent factors	Digital customer base Usage of industry-standard applications (e.g. Bloomberg for banking industry) Industry digitization index Pace of digitization (e.g. Moore's law)[a] Smartphone penetration rate Digital economy and society index (Digital economy and society index) Cloud adoption rate (Cloud computing statistics on the use by enterprises) Number of reported vulnerabilities (Common Vulnerabilities and exposures (CVE)) Depreciation rate of digital devices Number of companies certified with ISO/IEC 270001 (ISO Survey, 2014) Total records breached (Dataloss DB; ID Theft Center) Size of digital universe	Regulatory requirements Data protection legislations Nature of business Core goods and services Motivation level for inside threat Likelihood of human error Unemployment rate Average age of suspected cyber attackers (U.K. National Crime Agency, 2015) Crime rate Cultural perception of privacy Country risk Political risk Geo-political climate Global risks

[a] As of 2016, Moore's Law is no longer valid after half a century of accurate projection: http://www.telegraph.co.uk/technology/2016/02/25/end-of-moores-law-whats-next-could-be-more-exciting/.

Table 4 – Digital assets and associated cyber loss events.

Digital valuables		Cyber loss scenarios
Core value assets	IP of a critical product	IP theft, industrial espionage, etc.
	Regulated PII	Data breach, data leakage, etc.
	Sensitive financial data	Cyber fraud, data corruption, malfunction of trading algorithms, ransomware, etc.
Operational assets	Business critical IT services	System downtime due to technical malfunction, human error, etc.
	Payment website	Denial-of-Service (DoS) attack, insider attack, etc.

and benchmark on both technological and non-technological factors. Traditional threat and vulnerability analyses still apply. Vulnerabilities can fall under both inherent factor (when they are inherent to the business and cannot be mitigated) and control factor (when necessary security measures are not in place).

KCRF can be identified only with consistent monitoring and correlation of risk factors and cyber loss. In order to standardize incident data collection, an International Classification of Cyber Incidents (ICCI) also needs to be developed in conjunction with the IDAC, similar to the International Classification of Disease (ICD) (International Classification of Diseases). The first attempt to classify diseases systematically was made by Sir George Knibbs (Knibbs, 1929), who credited François Boissier de Sauvages de Lacroix (1706–1777). At the beginning of the 19th century, the classification of disease in most general use was developed by William Cullen (1710–1790) (Cullen, 1780). The statistical study of disease began a century earlier with the work of John Graunt on the London Bills of Mortality[4] in an attempt to estimate the proportion of children who died before reaching the age of six. Therefore, the current scientific robustness in quantifying a person's medical risk is a result of 400 years of standardized risk data collection. The lessons learned should be applied in cyber risk management whenever possible.

3.3. *Using scenario analysis for control assessment and loss quantification*

In order to identify controls that will be the most effective in reducing an entity's cyber risk exposure in cybernomics, scenario analysis[5] is used to assess the entity's controls against its most damaging cyber loss events. Once the entity has identified its most valuable digital assets, a cyber loss scenario inventory can be developed around those assets. These are the loss events the entity's is "genetically" most exposed to. A basic example is shown in Table 4.

Then, microeconomic loss can be quantified using the loss categories listed in Table 5. Monetary loss estimation under each loss category can come from historical incidents, industry reports, forensic reports, expert judgement, external studies, statistical database, etc.

[4] Bills of Mortality were the weekly mortality statistics in London, designed to monitor burials from 1592 to 1595 and then continuously from 1603.

[5] Scenario analysis is a process of analysing possible future events by considering alternative possible outcomes. As a main method of projections, scenario analysis does not try to show one exact picture of the future.

Table 5 – Microeconomic loss quantification method.

Loss category	Microeconomic loss quantification method
Direct loss (financial loss, physical asset damage, death and bodily injury)	Loss based on valuation of the digital valuable affected, direct losses on expenses, etc.
Incident investigation and response	Cost of paying internal forensic team and external consultants for investigation and response to the incident, including technical tools and applications required for purchase and installation.
Reputational damage (applicable after incident has gone public)	Estimated economic loss correlated to the size of the readership of the media the incident is publicized on, and through reputation rating agencies, e.g., bizrate (BizRate).
Legal liabilities	Liability (e.g., per record in case of PII breach) as defined in laws, regulations, contracts and agreements.
Regulatory penalties	Regulatory fines e.g., 5% of revenue.
Impact on share price	From implicit market value (estimates) and explicit market value (observed).

With increasing sophistication and interdependency of IT outsourcing, and the usage of cloud computing in particular, quantifying macroeconomic losses in IT supply chain has become a main obstacle for cyber insurers and reinsurers. Detailed process for macroeconomic loss quantification is out of scope for this paper, but the Cambridge Center of Risk Studies has proposed two stress test scenarios for cyber catastrophes to quantify macroeconomic losses (Centre for Risk Studies, 2014; Ruffle et al., 2014).

Scenario analysis is currently recommended in all cases of cyber loss quantification to compensate for the lack of quality historical loss data. Going forward, both the statistical approach and scenario analysis should be used. The statistical approach involves forecasting an entity's cyber loss using probability and statistical models with the aid of the cybernomic databank. It should be used to monitor risks continuously. Scenario analysis, especially stress scenario analysis, does not necessarily require the use of a probability or statistical model. Instead, the conditions of a cyber incident can be arbitrarily chosen or based on major incidents in crisis situations. Scenario analysis should be used on a case-by-case basis to estimate risk in unique circumstances.

3.4. *Applying VaR and MM to define cyber risk units*

Cybernomics applies attributes of established risk measures VaR and MM to the definition of cyber risk units. In Table 6 a comparison is made between the needs for cyber risk measurement and the applications of MM.

Class D asset is any type of digital asset as listed in IDAC, and it is one type of valuable asset in entity E's digital asset inventory.

Based on this comparison, MM attributes can be borrowed to define a cyber risk measurement. However, there are differences between the nature of human mortality risk and "digital mortality" risk. Firstly, MM was created on the basis that human death is a certain event with a probability of 1. It has been applied based on statistics of all causes (both natural and non-natural) to human death, including suicides. In comparison, the economic lifespan of digital assets can be eternal with the recent breakthrough in digital storage capability (The Daily Beast, 2016).

> *"Digital death" is defined as a binary condition when a digital asset loses all of its economic value.*

Currently, the majority of digital assets will eventually "die" either "naturally" through retirement or replacement, or "non-naturally" due to external threats such as the compromise of its Confidentiality, Integrity and Availability (CIA). The impact of economic lifespan is further analysed in the discussion section. In this paper, cyber risk measures are defined based on the following assumption:

Assumption 1. All classes of digital assets will eventually reach a state of "digital death" and lose all of their economic value.

Secondly, different classes of digital assets are exposed to different inherent risks. So each class of digital assets should have its own set of microrisks, similar to if we were to track microrisks for all organisms and not only humans. We have not yet tracked microrisks of any other organisms so we cannot draw any comparisons. Nevertheless, all digital assets are made of bits, just like all organisms are made of cells. How different fundamental

Table 6 – Comparison between needs for cyber risk measurement and applications of MM.

Needs of cyber risk measurement	Applications of MM
To measure the effect of control factors on the probabilities of class D assets losing their value	MM measures the effect of day-to-day activities (modifiable risk factors) on the probability of human death
To articulate entity E's "willingness-to-pay" for the reduction of risk of class D assets	The value of MM reflects the "willingness-to-pay" for the reduction of risk
To measure cost of controls to reduce risk exposure of class D assets	The cost of reducing 1 MM reflects the cost-effectiveness of countermeasures to reduce risk

inherent factors are for different classes of digital assets is left for further discussion. In this paper, cyber risk measures are defined based on the following assumption:

Assumption 2. The inherent differences between different classes of digital assets are distinct enough for their risks to be monitored and analyzed separately.

Based on the two assumptions above, $BitMort_D$ (BM_D) is defined as follows for class D assets:

$BitMort_D$ (BM_D) for a given class D digital assets is 1 in a million probability of its digital death, i.e., a binary condition when the asset loses all of its economic value. The value of 1 BM_D is the amount of money an entity is willing to pay to reduce 1 BM_D for its class D assets.

The same scale of Million is chosen for BM based on the following facts:

- There were 707,509,815 data records lost globally in 2015 (2015 Data Breach Statistics, 2015) out of an estimated population of 95,100,000,000 total records (3.17 billion Internet users in 2015 (Number of Internet users worldwide from 2005 to 2015) with an average of 30 online records per person[6]), which is roughly a probability of 0.0074.
- There were a total number of 499,331 recorded deaths in England and Wales in 2012 out of a population of 56,567,000 (Deaths Registered in England and Wales (Series DR), 2012), which is a probability of 0.0088.

Because there is no way to decide what scale to use without substantial loss data collected for different types of digital assets, the scale of Million is sufficient as a start. It can always be scaled up or down, similar to byte–megabyte–gigabyte and metre–centimetre–millimetre.

When residual risk measured in BM becomes statistically available for various types of digital assets, it is possible to aggregate them along with asset value to generate a cyber VaR curve, representing the entity's residual cyber risk:

$$VaR = \sum_{i=1}^{n} V_i f_{Di}, \tag{6}$$

where *VaR* is Value at Risk for all digital assets of an entity E; entity E's digital asset inventory $D = \{D_1, D_2, \ldots, D_n\}$; the value of each asset $V = \{V_1, V_2, \ldots, V_n\}$; and f_{Di} is the amount of residual risk D_i is exposed to measured in BM_{Di}s.

To compute the cyber VaR curve, historical simulation and Monte Carlo[7] simulation can be used. Under historical simulation, BMs are extracted under a number of different historical time windows which are defined by the entity. While historical simulation measures risk by replicating one specific historical path of cyber risk ecosystem, Monte Carlo simulation attempts to generate a large number of paths using repeated random sampling to produce a probability distribution.

The risk measure *hekla* is defined as follows:

hekla is a probability, where a 12-month hekla VaR is the loss limit an entity can afford from cyber incidents. The value of hekla is the amount of money the entity is willing to pay to reduce its hekla by 1% for the same loss limit.

The time horizon of 12 months is chosen to reflect cyber risk exposure over one financial year, which should be considered in budget planning and integrated with ERM frameworks.

4. Theory of cybernomics

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. It has three views: the entity view, the portfolio view and the global view.

4.1. *Entity view*

In the entity view of cybernomics as shown in Fig. 2, for entity E: E's digital value is the sum of the aggregated value of its core value assets and aggregated value of its operational assets. E maintains a digital asset inventory with economic value assigned to each asset. Each asset listed in E's digital asset inventory follows standard classification in IDAC. E maintains a microeconomic loss scenario inventory developed around its critical assets.

E uses microcybernomic databank and modelling to optimize its capital modelling for managing residual cyber risk. E monitors its cyber risk factors, which are categorized under Cyber Risk Quadrant as technological, non-technological, inherent and control factors. E reads measures of these risk factors from its entity-level interface with the cybernomic databank. It uses a combination of statistical modelling and scenario analysis to quantify cyber loss, and uses scenario-based control assessment to optimize its investment on measures that are the most cost-effective for risk reduction. E also gets the most relevant entity-level simulation scenarios from the cybernomic databank. In return, E feeds its incident and microeconomic loss information back to the cybernomic databank.

For a given class of asset D in E's asset inventory, BM_D is defined as 1 in a million probability of its digital death. The value of 1 BM_D is the amount of money E is willing to pay to reduce 1 BM_D for D type of asset. Following this process, risk exposure of all assets in E's asset inventory, cost of risk reduction of each type of asset, and E's "willingness-to-pay" to reduce their risk exposures can be measured and aggregated into a 12-month VaR curve.

[6] Based on expert judgement.

[7] Monte Carolo method is a technique in which a large quantity of randomly generated numbers are studied using a probabilistic model to find an approximate solution to a numerical problem that would be difficult to solve by other methods.

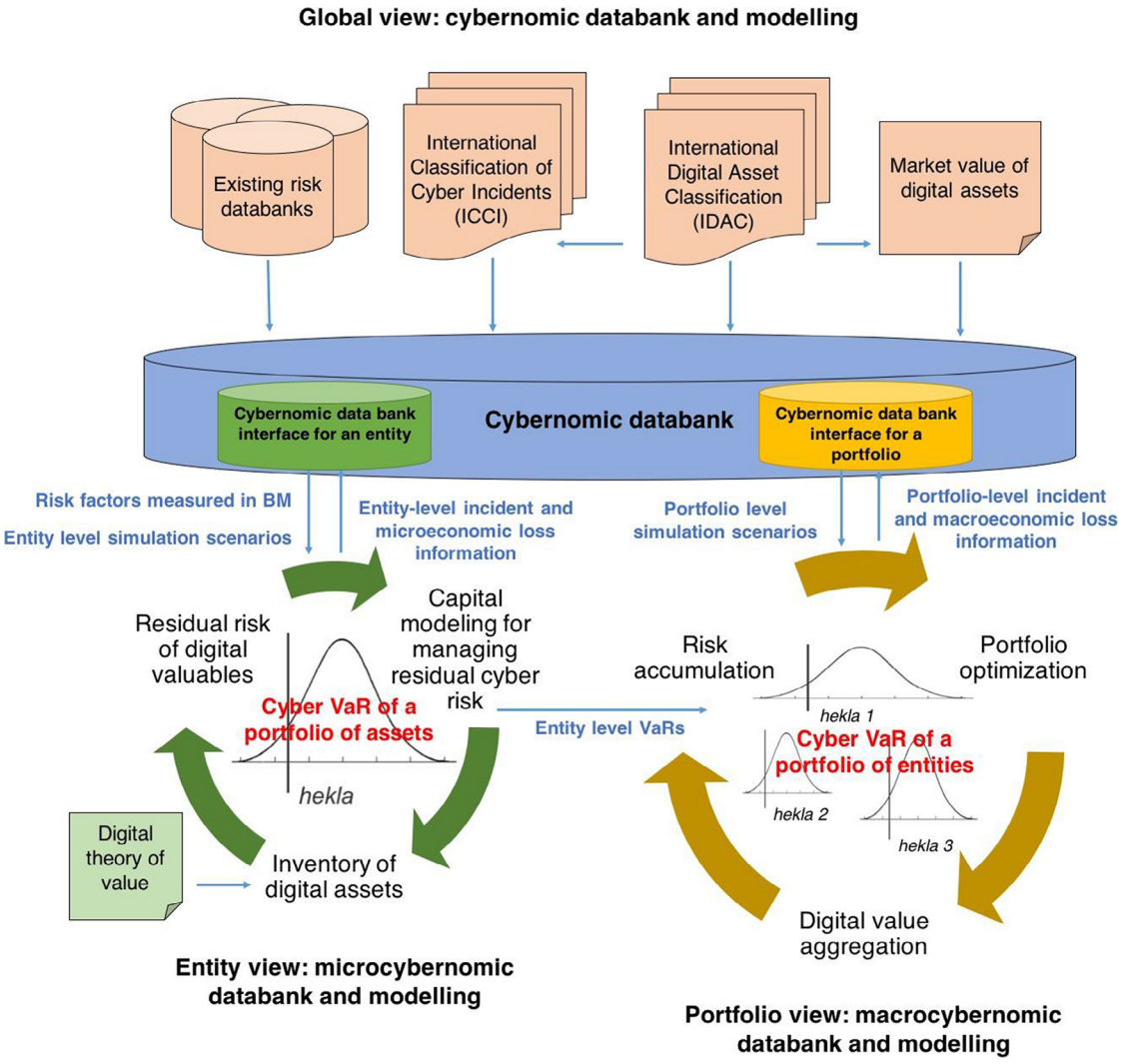

Fig. 2 – Global view, entity view and portfolio view of cybernomics.

hekla is a probability, where a 12-month *hekla* VaR is the loss limit E can afford from cyber incidents. The value of *hekla* is the amount of money E is willing to pay to reduce its *hekla* by 1% for the same loss limit. *hekla* can be used to articulate E's risk limit, risk appetite and risk pricing.

Both BM and *hekla* are stackable on portfolio and global levels.

4.2. *Portfolio view*

In the portfolio view of cybernomics as shown in Fig. 2, for multinational corporations, insurers, investors, or policy makers who manage a portfolio of entities P: P uses macrocybernomic databank and modelling to optimize portfolio returns. P aggregates digital value from its portfolio of entities, calculates portfolio cyber VaR stacked from cyber VaRs of individual entities. Then, it determines portfolio level *hekla* and manages available capital accordingly. The portfolio view reads portfolio level simulation scenarios from its portfolio-level interface with the cybernomic databank. In return, P feeds its incident and macroeconomic loss information back to the cybernomic databank.

4.3. *Global view*

In the global view of cybernomics as shown in Fig. 2, a databank and cybernomic model evolve around the classification schemes of assets (IDAC) and associated incidents (ICCI), and integrates with existing risk databanks to cover socio-economic, geo-political risk factors. Market values of digital assets listed in IDAC are monitored. Risk factors are categorized under Cyber Risk Quadrant. Through public–private data partnership schemes, incident and loss data are collected from both entity and portfolio levels to support statistical modelling. The cybernomic model correlates risk factors and cyber loss to calculate risk exposures measured in BM and identify KCRF. The cybernomic databank feeds risk exposure information and simulation scenarios to entities. It also feeds portfolio-level simulation scenarios to portfolio risk managers based on historical incidents.

5. Risk calculation using BM and *hekla*

Given Company A's digital asset inventory $D = \{D_1, D_2, \ldots D_n\}$, D_1 being regulated PII. Section below demonstrates how BM and *hekla* are used for risk calculation.

1. Measuring strength of controls for digital assets using BM

In company A, the implementation of firewall can reduce risk exposure of D_1 by f BM_{D1}s, and not having appointed a CISO can increase the same by c BM_{D1}s.

2. Measuring cost-effectiveness of controls for digital assets using BM

It costs company A $5000 using solution X and $10,000 using solution Z to reduce risk exposure of D_1 by 1 BM_{D1}. Therefore, solution X is more cost-effective than solution Z.

3. Articulating an entity's "willingness-to-pay" for risk reduction for digital assets using BM

Company A prices the reduction of 1 BM_{D1} from the risk exposure of D_1 in the tens of cents per record.

4. Articulating an entity's cyber risk limit using *hekla*

The maximum loss amount Company A can tolerate from cyber incidents is a 12-month 7% *VaR* of $100 million (or 10% of its total revenue) from cyber loss. This means Company A's cyber loss limit is $100 million (or 10% of its total capital), with a *hekla* of 7%.

5. Articulating an entity's cyber risk appetite using *hekla*

Company A's cyber risk appetite is a *hekla* of maximum 4% where the 12-months *hekla* VaR is $100 million (its risk limit).

6. Measuring an entity's cyber risk pricing using *hekla*

If Company A is willing to spend $10 million to bring its *hekla* from 7% down to 6% with the same loss limit, it means company A prices its own *hekla* at $10 million.

7. Measuring an entity's cost of risk reduction using *hekla*

If in practice, it takes Company A $15 million to reduce its *hekla* from 7% to 6% with the same loss limit, then the cost of the reducing *hekla* by 1% in company A is $15 million.

8. Measuring an entity's cyber risk ROI using *hekla*

Company B's digital value composition is >95% similar to Company A's, therefore Company B has similar inherent cyber risk exposure as Company A, and it follows the same process to compute its *hekla*. Due to different ways of control implementation, the cost of reducing *hekla* by 1% in Company B is $5 million whereas it costs Company A $15 million to do the same. Thus, Company B is more cost effective than company A in managing its cyber risk. Cyber risk ROI is essentially the reduction of *hekla* per every dollar spend.

9. Using BM and *hekla* on a portfolio of entities

BM and *hekla* are measures that can be "stacked" on the portfolio level. All applications of BM and *hekla* can be applied on a portfolio of entities and on the macroeconomic level.

6. Discussion

6.1. *Accuracy*

It is important to note that it is valuable for cyber risk managers to measure the difference between a $50 million exposure and a $10 million exposure, but it is irrelevant to measure the difference between $10 million and $11 million. It costs exponentially more to reach this level of accuracy that is likely to be counterproductive to improving cost-effectiveness.

6.2. *Analytical capabilities*

The solution conceptualized in this paper relies on advanced data analytics capabilities that is on a trajectory of exponential growth. Compared to the 1990s when J.P. Morgan built the first analytics tool to compute VaR, we enjoy a tremendous advantage today in storing and processing large datasets. As a result, the major obstacle to advancement for this field is not the lack of technological capabilities to compute datasets, but to break down necessary non-technological barriers and establish a wide range of data points under the three views of cybernomics.

6.3. *Testing and validation*

This is the first of a series of papers introducing the discipline of cybernomics. Testing and validation using real-world data is a work in progress and will be published in separate papers. Nevertheless, it is impossible today to validate the entire framework due to the lack of data points. Validation can only be made in parts. The purpose of publishing this paper is also to invite testing and validation from the research community. It took years to validate VaR and decades to validate MM due to the time required for data collection, yet it was important to put forward the definitions first so that data collection can take place in a structured manner.

6.4. *Economic lifespan of digital assets*

It has already been proven technically feasible for digital assets to outlive humanity (Ruffle et al., 2014). In the meantime, we are suffering increasing "data pollution"[8] in the early days of Big Data. The low end tasks of selection, normalization and cleansing of large datasets often cost more than analytics. This will eventually become an overhead that nobody is willing to

[8] Data pollution refers to the generation of a large quantity of low-quality or duplicated data that are never deleted.

pay. The alternative is to set a "self-deletion" date for certain classes of digital assets. Due to the uncertainty of which path will be taken in the future, definitions in this paper are based on the assumption that there will be limited economic lifespans for all classes of digital assets.

6.5. *Fundamental inherent differences of digital assets*

Definitions in this paper require microrisks of different classes of digital assets to be tracked separately based on the assumption that inherent differences of digital assets are distinct enough for their risks to be tracked in separate databanks. However, it does not rule out the possibility of a more unified approach to the definition of this risk unit since all digital assets are fundamentally made of bits.

7. Conclusion and future work

The purpose of this paper is to introduce the unifying economic framework and risk measures of cybernomics. Built around BM and *hekla*, cybernomics integrates cyber risk management and economics to study the requirements of a databank in order to develop 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.

A novel multidisciplinary approach is used to apply established methods in economics, finance and medicine to develop the components of the cybernomic framework and risk measures. Leveraging from risk units MM and VaR, BM and *hekla* are defined in this paper with a number of supporting definitions. This is the first time cyber risk measurement units have been introduced in an academic paper.

Risk calculation methods and examples are introduced in this paper such as using BM and *hekla* to measure cost-effectiveness of control factors, articulate an entity's "willingness-to-pay" for cyber risk reduction, cyber risk limit, and cyber risk appetite.

This paper conceptualizes the requirement of a cybernomics databank under three views: entity view, portfolio view and global view. It argues that international standard classifications must be in place for digital assets and cyber incidents, i.e., IDAC and ICCI, to achieve accurate projection using statistical modelling in conjunction with scenario analysis.

The proposed framework also addresses limitations of existing cyber risk management methods. It holistically establishes risk data points on entity, portfolio and global levels. It uses scenario-based control assessment to prioritize high value control investments.

Much work has yet to be done to develop the theory of cybernomics. In the next paper on this topic, a case study will be provided with real-world data to demonstrate more detailed applications of cybernomics risk calculation.

Acknowledgements

I would like to thank my friend Dr. Fred A. English for introducing medical risk management concepts to me, and also the Cyber Security team at EY (formerly Ernst & Young) for supporting me to further develop my theory on cybernomics.

REFERENCES

2015 Data Breach Statistics. Breach level index findings; 2015. Available from: http://www.safenet-inc.com/resources/data-protection/2015-data-breaches-infographic/.
Allianz. Top business risks 2016. Allianz Risk Barometer, 2016.
Anderson R, Moore T. The economics of information security. Science 2006;314(5799):610–13.
BitSight cyber security rating. Available from: https://www.bitsighttech.com/.
BizRate. Available from: http://www.bizrate.com.
Blakley B, McDermott E, Geer D. Information security is information risk management. In Proceedings of the 2001 workshop on new security paradigms (pp. 97–104). ACM, 2001.
Bloomberg. KKR adds cyber risk score to its assessment of companies; 2014. Available from: http://www.bloomberg.com/news/articles/2014-04-11/kkr-adds-cyber-risk-score-to-its-assessment-of-companies.
Caralli RA, Stevens JF, Willke BJ, Wilson WR. The critical success factor method: establishing a foundation for enterprise security management (No. CMU/SEI-2004-TR-010). Carnegie-Mellon University Pittsburgh PA Software Engineering Institute, 2004.
Cavusoglu H, Cavusoglu H, Raghunathan S. Economics of IT security management: four improvements to current security practices. Commun Assoc Inform Syst 2004;14(1):37.
Centre for Risk Studies. Business blackout: the insurance implications of a cyber attack on the U.S. power grid. University of Cambridge, Cambridge; 2014.
Centre for Risk Studies and Risk Modeling Solutions. Managing cyber insurance accumulation risk, 2016.
Cerullo MJ, Cerullo V. Threat assessment and security measures justification for advanced IT networks. Inf Syst Control J 2005;1:1–9.
Chen T. Information security and risk management, chapter in Encyclopedia of Multimedia Technology and Networking, M. Pagani, 2008.
Cloud computing statistics on the use by enterprises. Available from: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises.
Common vulnerabilities and exposures (CVE). Available from: https://cve.mitre.org/.
Courtney RH. A systematic approach to data security. Com Sec 1982;1(2).
Cullen W. Synopsis nosologiae methodicae (Vol. 2), 1780.
Dataloss DB. Available from: http://datalossdb.org/.
Deaths Registered in England and Wales (Series DR), (2013). Office for National Statistics. Retrieved 2014-06-03, 2012.
Department for Transport GMH. United Kingdom. TAG Unit 3.4: The Safety Objective. Available from: http://www.dft.gov.uk/webtag/documents/expert/unit3.4.1.php.
Derby CA, Mohr BA, Goldstein I, Feldman HA, Johannes CB, McKinlay JB. Modifiable risk factors and erectile dysfunction: can lifestyle changes modify risk? Urology 2000;56(2):302–6.
Digital economy and society index. Available from: https://digital-agenda-data.eu/datasets/desi/indicators.
El Aoufi S. Economic Evaluation of Information Security [Master's thesis] 2009.
Finne T. A DSS for information security analysis: Computer support in a company's risk management. In Systems, Man, and Cybernetics, 1996., IEEE International Conference on (Vol. 1, pp. 193–198). IEEE, 1996.

Forbes. Amazon.com goes down, loses $66,240 per minute; 2013. Available from: http://www.forbes.com/sites/kellyclay/2013/08/19/amazon-com-goes-down-loses-66240-per-minute/#405e458a3c2a.
Forbes. 9 figure deals lift cybersecurity investment to an all time high; 2016. Available from http://www.forbes.com/sites/stevemorgan/2016/02/08/9-figure-deals-lift-cybersecurity-investments-to-an-all-time-high/#2a7995a82aed.
Frosdick S. The techniques of risk analysis are insufficient in themselves. Disaster Prev Manag 1997;6(3):165–77.
Geer DE. Security of information when economics matters. Verdasys, May, 2004.
General Data Protection Regulation. European commission. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.
Gerber M, Von Solms R. Management of risk in the information age. Com Sec 2005;24(1):16–30.
Gordon LA, Loeb MP. The economics of information security investment. ACM Trans Inform Syst Sec (TISSEC) 2002;5(4):438–57.
Gordon LA, Loeb MP. Managing cybersecurity resources: a cost-benefit analysis, vol. 1. New York: McGraw-Hill; 2006.
Guldimann TM. The story of RiskMetrics. Risk 2000;13(1):56–8.
Hackett SC. Environmental and natural resources economics: Theory, policy, and the sustainable society. ME Sharpe, 2010.
Hoo KJS. How much is enough? A risk management approach to computer security. Stanford: Stanford University; 2000.
Howard RA. Microrisks for medical decision analysis. Int J Technol Assess Health Care 1989;5:357–70. doi:10.1017/S026646230000742X.
Huq, N. and TrendLabs Research. Follow the data: dissecting data breaches and debunking myths: Trend Micro analysis of privacy rights clearinghouse 2005–2015 data breach records, 2015.
ID theft center. Available from: http://www.idtheftcenter.org/id-theft/data-breaches.html.
Information Security Forum. Simplified process for risk identification (SPRINT) user guide, 2000.
Insurance Business. Warren Buffet enters the cybersecurity insurance market; 2015. Available from: http://www.ibamag.com/news/warren-buffett-enters-the-cybersecurity-insurance-market-25540.aspx.
Intel Security. The hidden data economy: the market place for stolen digital information, 2015.
International classification of diseases. Available from: http://www.who.int/classifications/icd/en/.
ISO Survey. The ISO survey of management system standard certifications, 2014.
Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Anal 1981;1(1):11–27.
Knibbs GH. The international classification of disease and causes of death and its revision. Med J Aus 1929;1:2–12.
Marsh. UK cyber security: the role of insurance in managing and mitigating the risk, 2015.
Marshall A. Principles of economics, 1890.
Marx K. Value, price and profit, 1865.
Mercuri RT. Analyzing security costs. Commun ACM 2003;46(6):15–18.
Mizzi A. Return on information security investment, MBA Dissertation, University of Malta, 2005.
Moody DL, Walsh P. Measuring the value of information – an asset valuation approach. In ECIS, 1999. pp. 496–512.
Neubauer T, Klemen M, Biffl S. Secure business process management: a roadmap. In First International Conference on Availability, Reliability and Security (ARES'06) (pp. 8-pp), IEEE, 2006.
Nice classification. Available from: http://www.wipo.int/classifications/nice/en/.
Number of Internet users worldwide from 2005 to 2015. Available from: http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/.
Privacyrights.org. Available from: http://www.privacyrights.org/data-breach.
Reported data breaches in Europe 2005–2015. Available from: http://cmds.ceu.edu/article/2014-10-07/data-breaches-europe-reported-breaches-compromised-personal-records-europe-2005.
RiskMetrics. Technical document, Morgan guarantee trust company, Global Research, New York, 1995.
Rodewald G. Aligning information security investments with a firm's risk tolerance. In Proceedings of the 2nd Annual Conference on Information Security Curriculum Development (pp. 139–141). ACM, 2005.
Ruffle SJ, Browman G, Caccioli F, Coburm AW, Kelly S, Leslie B, et al. Stress test scenario: Sybil logic bomb cyber catastrophe. Centre for Risk Studies. University of Cambridge, Cambridge; 2014.
Ryan JJ, Ryan DJ. Expected benefits of information security investments. Com Sec 2006;25(8):579–88.
Sacco RL. Risk factors and outcomes for ischemic stroke. Neurology 1995;45(2 Suppl. 1):S10–14.
Smith A. An inquiry into the nature and causes of the wealth of nations, 1776.
Spears JL. A holistic risk analysis method for identifying information security risks. In Security Management, Integrity, and Internal Control in Information Systems (pp. 185–202). Springer US, 2005.
Stigler G. The development of utility theory. Journal of Political Economy 1950;50:307–27.
Suh B, Han I. The IS risk analysis based on a business model. Inf Manag 2003;41(2):149–58.
The Daily Beast. The data that can outlive humanity; 2016. Available from: http://www.thedailybeast.com/articles/2016/04/12/the-data-that-can-outlive-humanity.html.
TLinsmeier TJ, Pearson ND. Value at Risk. Financial Anal J 2000;http://dx.doi.org/10.2469/faj.v56.n2.2343.
U.K. National Crime Agency. Cyber-attack suspects' average age down to 18; 2015. Available from: http://gadgets.ndtv.com/internet/news/cyber-attack-suspects-average-age-down-to-17-uk-agency-775908.
US Department of Transportation. Treatment of the economic value of a statistical life in departmental analyses—2011 interim adjustment; 2011. Available from: http://www.dot.gov/policy/transportation-policy/treatment-economic-value-statistical-life.
World Economic Forum. Risk and responsibility in a hyperconnected world: pathways to global cyber resilience, 2015.
World Economic Forum. Digital disruption has only just begun; 2016. Available from: http://www.weforum.org/agenda/2016/01/digital-disruption-has-only-just-begun.

Pioneered the field of cloud forensics with foundational publications, Dr. Keyun Ruan edited the world's first academic reference book on the topic and spoke widely at leading international conferences. She has contributed to working groups commissioned by the U.S. government and European Commission to advance standards in this area. Accelerated standard developments have resulted in significant improvements in incident management and continuous monitoring capabilities of major cloud providers. Her current work focus is 'cybernomics - quantitative cyber risk analytics for enterprises and cyber insurers. She was named '30 under 30 shaping Ireland's future' in 2014.