Information Governance and Cybersecurity: Framework for securing and managing information effectively and ethically

Dr Elizabeth Lomas, Associate Professor in Information Governance, University College London. ORCID ID: 0000-0001-5619-6725.

ABSTRACT

Over the last 30 years new technologies have enabled many new uses and possibilities for information/data widening the stakeholder pool. As such it has become increasingly commoditized with greater recognition of a range of information value(s). In tandem with the growing potential, value and social significance of information, the online management of a wide range of data has opened up information/data to new forms of theft and attack including information subversion, cybercrime and cyber warfare. To deal with these complex information world dynamics, it is the field of information governance (IG) which has emerged as the solution for individuals, organizations and nations to manage information. Cybersecurity is a subcomponent of IG. IG provides the holistic solution to dealing with information challenges in terms of both opportunities and dangers that are implicit within information creation. It deals with the management of information assets legally and ethically as well as providing guarantees around information confidentiality, integrity and availability through time. This chapter sets out IG considerations, tools and frameworks for securing and managing information effectively and ethically.

INTRODUCTION

Over the last 30 years the value of information/data has increased as new technologies have made it more accessible, enabled it to be reused, and to add new uses for example through linked data, aggregated data or big data. As such data has become increasingly commoditized with greater recognition of a range of information value(s). New technologies have created new forms of digital assets. An example is blockchain which has underpinned developments in cryptocurrency such as bitcoin. Another example is personal data, which in 2011 the World Economic Forum defined as a new asset class that it predicted will increasingly spur a host of new personalized services and applications with incredible velocity and global reach.

In order to take advantage of new information possibilities provided by technology, including the capacity for workers to connect 24/7, and new communication channels with enhanced audience reach, organizations have moved from a world in which they have been able to control information within internal boundaries to one in which the organizational boundaries are permanently perforated. New forms of data storage distribute and manage data in different ways, e.g. the Cloud. In addition, there are new demands and expectations for organizations to interface and actively interact or even co-create information with external stakeholders. Moreover, the digital world connects to and manages the physical world creating the 'Internet of Things'. Information now acts as the latest form of oil driving economies and societal living requirements.

In tandem with the growing potential, value and social significance of information, the online management of a wide range of data has opened up information/data to new forms of theft and attack. New channels and the proliferation of information have led to new types of misinformation and subversion. The threat and reality of cybercrime and cyber warfare has significantly increased. A 2018 report by the security company Norton reported that in the

year of 2017 alone, 44% of consumers were impacted by cybercrime. At an international level we see increasing reports that cyber warfare is ongoing. Denardis (2014) highlights the alleged 2010 use of the USA/Israeli Government to undermine the Iranian nuclear programmes through the deployment of the Stuxnet Worm and the Russian Denial Of Service attacks on the Estonian Government in 2007. Such attacks can cause both national reputational damage and tangible impacts. It has moved the focus of Internet/World Wide Web, telecommunication infrastructures and mobile usage into an arena of open international dispute. For example, in 2018 the USA National Defense Authorization Act resulted in the Chinese company Huawei being banned from the 5G networks due to concerns over spying. Huawei are bringing a legal case to attempt to overturn this decision. This further evidences the complexity of international information and infrastructure control.

To deal with these complex information world dynamics, it is the field of information governance (IG) which has emerged as the solution for individuals, organizations and nations (Lomas 2010; McLennan 2014; Smallwood 2014) to manage information. IG provides the solution to dealing with information challenges in terms of both opportunities and dangers that are implicit within information creation. It deals with the management of information assets legally and ethically as well as providing guarantees around information confidentiality, integrity and availability through time. It raises information to Government and Board level as an area for regulation, oversight and active strategic management. IG is multidisciplinary drawing on a range of expertise to deliver information agendas. Embedded within IG are other governance components which form smaller parts of the IG framework delivery. These include, but are not limited to, cybersecurity and governance, computer/IT governance, data governance, information assurance and Internet governance. Importantly IG provides frameworks that align people, processes and technology in accordance with the law and best practice.

THE INFORMATION GOVERNANCE CONTEXT AND ITS RELATIONSHIP WITH CYBERSECURITY: A HISTORICAL PERSPECTIVE

IG has grown out of corporate governance thinking which has been legislated and regulated for and applied across public and private sector settings. Governance provides for governing, controlling and regulating good order to deliver societal values including protection. As such, the term governance has developed to require a system of leadership and management that balances societal goals and is in essence 'ethical'. The system of governance may be applied to a nation, business, charity or some other body. In 2000, a leading proponent of corporate governance, Sir Adrian Cadbury, described the complex balance which corporate governance should deliver in terms of providing for the delivery of economic and social goals which consider individual and communal needs. He stated that the aim of governance in this context is to align the interests of individuals, corporations and society as nearly as possible (Cadbury 2000). This therefore includes the organizational management of relationships across organizational boundaries to sustainably deliver employment and prosperity whilst promoting, integrity, openness, value and diversity for a wide range of interests (Financial Reporting Council 2018).

As such, governance is not a fixed concept but is dependent upon the ethical values of society and the governments in place, which inform and dictate the format for leadership, societal accountability and trust. Within this context of corporate governance, information plays a critical dynamic role. As noted by Willis, information delivers; transparency, accountability, due process, compliance, the delivery of statutory and common law requirements, stewardship, systems and processes, and security of personal and corporate information (Willis 2005, 86-87). As technologies have advanced, the role of information within governance agendas has expanded and over time, becoming a distinct activity

particularly as information as an asset has been better recognized (Lomas 2010). In 2010, Deborah Logan (2010) wrote a Gartner blog post defining IG as the specification of decision rights and an accountability framework to deliver 'desirable behaviours'. She wrote the blog under an article titled, "What is information governance and why is it so hard?" Clearly to provide a holistic framework is not simple and the scale of this endeavour is not to be underestimated in terms of the support and resources required. In 2012, Barclay T. Blair, a founder member of the Information Governance Initiative think tank, defining IG, again emphasized this complexity in terms of the need to deal with information through comprehensive IG programs which deliver the value of information assets whilst minimizing risk and cost (Blair 2012).

In part, the complexity of the IG endeavour relates to the wide-ranging nature of information assets which may be marketable resources but in addition represent something more. As Desouza (2009, 35) states, resources can be traded being purchased and sold in the marketplace but in contrast assets are things that organizations care deeply about. Such assets have a more strategic and complex set of values. In essence, information can be a product or service, it can deliver influence, a competitive edge, education, enrichment and entertainment. It can have a monetary sales value and/or a cost to recreate it. However, it can have other wider societal values in terms of national, organizational, personal or cultural memory and identity. It can be something to share or keep private. It is important to note the complexity and multiple realities of information value to different stakeholders through time. Reliable authentic information, delivered by systems with integrity, develop trust, accountability and the potential for democracy and/or open systems of government. In this context, cybersecurity helps provide protection and strategies for authorised access to information. IG provides a wider vision of information needs.

Today IG has evolved to straddle four key domains each of which is underpinned by risk management processes; information economics recognising the value(s) of information assets, information laws and ethics, information management, and information security (which extends to cyber security and other information security including the management of paper records). IG balances stakeholder needs to provide access and information use in addition to protection. In terms of managing information, IG is the framework of choice as the broadest and most comprehensive. As noted by Eugen and Petrut (2018), IG encompasses data governance and IT governance. ENISA set out that cybersecurity is one aspect of a bigger governance delivery picture (2015, 12), with cybersecurity focusing on the specific protection required for information rather than a wider information picture which is required for organizational and national level delivery more generally. Cybersecurity does consider national and international safety but does not address citizen requirements in terms of other information needs. IG requires holistic thinking, experts and collaboration to ensure successful information delivery for society. As defined by Lomas et al (2019, 4), IG provides a holistic ethical framework, "which takes into account a range of societal and individual stakeholder information needs. It enables a just process of information co-creation, sharing, management, ownership and rights." In line with social justice concepts all can be invested in the IG system. It takes into consideration individual, family, community, organizational and societal needs supported by practitioner experts but in addition citizens more generally.

NATIONAL LAWS AND ETHICAL EXPECTATIONS FOR MANAGING AND PROTECTING INFORMATION

Key in managing IG is ethical delivery and compliance with law and local expectations. Where there is ethical consensus there is law. However, there is limited consensus and few international information rights laws exist even though we live in a world

where information delivered through technology transcends international boundaries. There are differing national expectations for information ownership, publication, defamation, libel, sedition, computer misuse, confidentiality, privacy and personal data. In a seminal article, Mason (1986, p.5) sets out four key areas of ethical dispute with key questions of contention as summarized in Table 1 below.

Area of Contention	**Questions**
Accuracy	• Who is responsible for the authenticity, fidelity and accuracy of information? • Similarly, who is to be held accountable for errors in information and how is the injured party to be made whole?
Property	• Who owns information? • What are the just and fair prices for its exchange? • Who owns the channels, especially the airways, through which information is transmitted? • How should access to this scarce resource be allocated?
Accessibility	• What information does a person or an organization have a right or a privilege to obtain, under what conditions and with what safeguards?
Privacy	• What information should one be required to divulge about one's self to others? Under what conditions and with what safeguards? What information should one be able to keep strictly to one's self?

Table 1: Mason's Four Ethical Issues of the Information Age with associated questions

These issues have been widely debated. The complexities surrounding these issues exist because it is not always possible to balance these differing dimensions and there are very different national and cultural perspectives. Van Den Hoven (2008, pp.52-57) discusses the different approaches to understanding the practice of applying ethical principles. Generalists see the possibility for there to be agreed overarching ethical principles whilst particularists see the importance of specific contextual circumstances. Reflective equilibrium moves back and forth between these perspectives to reach a balanced perspective which is potentially more suited to a complex world.

The closest thing to an agreed global or 'generalist' agenda on ethical IG is established in the *Universal Declaration of Human Rights* which was adopted by the United

Nationals General Assembly in 1948 in order to set out a global agenda for fundamental human rights. Whilst setting out a global moral agenda one can see the need for a reflective equilibrium approach to apply these into practice. Article 12 and 17 set out rights in terms of privacy and property. Information property rights have emerged and developed through patents, trademarks and copyright laws which over the past century have evolved into relatively agreed international frameworks. The World Intellectual Property Organization has provided a focal point for such discussions. However, in 2019, the EU has moved to protect intellectual ownership to a far greater degree than other Western counterparts. The 2019 Copyright Directive places increased responsibilities on social media platforms to regulate their content and take responsibilities for copyright infringements. Article 13 has been termed the 'meme ban', which makes online platforms responsible for removing copyrighted content. Article 11 delivers what has been termed a 'link tax', preventing news outlets reproducing content. Article 12 of the Copyright Directive prevents filming and sharing at events such as sports venues.

In terms of the Human Rights Declaration, Article 12 sets, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." This thus enshrines privacy principles. Building on human rights legislation in 1980, the Organisation for Economic Co-operation and Development (OECD) passed the *OECD Guidelines on the protection of privacy*. This established key principles for managing personal data or 'data protection'. Within the *Universal Declaration of Human Rights,* Article 20 asserts a further information related right that, "Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

Whilst not necessarily contradictory, the boundaries between these rights have not been consistently interpreted at a global level. Within Europe, legislation has placed an emphasis on strengthening privacy and personal data rights. In 1995 the European Union (EU) passed a Data Protection Directive (Directive 95/46/EC). This Directive regulated for a minimum standard for managing personal data across the 28 EU member states and those additional nations within the European Economic Area (Iceland, Liechtenstein and Norway). In 2016, the EU passed the General Data Protection Regulation (GDPR) with even stronger requirements for managing personal data (European Parliament and Council of the European Union 2016). This came into force in May 2018. It provides strict requirements for managing European citizens data even if the service is provided by a non-EU entity. The fines for personal data failings are significant and can cost an organization up to 20 million Euros or 4% of turnover whichever is greater. There are six key principles at the heart of the Regulation which requires organizations to build in 'privacy by design' when developing any system with personal data elements. This concept was first advocated for in the 1990s by the Ontario Privacy Commissioner, Ann Cavoukian. As such organizations are encouraged to undertake privacy impact assessments. This approach allows for the legislation to remain relevant as the needs for managing cybersecurity evolve. Under the term of the legislation, personal data must be protected. The full range of protections are not defined but the privacy impact assessment requires that threats are identified and reviewed as new security dangers emerge. The recommended standard to build compliance in this regard is the International Standards Organization's *ISO 27000* standard series which aligns IG and cyber security considerations. If personal data is breached then, in the GDPR context, the relevant EU regulatory authorities must be notified within 72 hours and penalties may be applied. Those individuals impacted should also be informed and the risks of the breach explained.

This legislation has evolved out of a recognition that personal data has become both a valuable asset which provides revenue streams, not least for harvesting marketing information, as well as a resource capable of costing an organization where it is not properly managed. In 2018, a number of high-profile companies received fines for data breaches and data misuse, for example the two USA corporations Facebook and Uber. Whilst these laws are sensible and pragmatic in principle, they are not necessarily easy to deliver into practice when considering competing personal data rights and demands for wide ranging information use. Businesses have continued to push the boundaries. For example, Amazon's Alexa records all conversations within its range regardless of whether the device is being actively used. As discussed by Day et al (2019), the justification for this is that then Amazon staff can use the data to improve speech recognition. However, the information on this functionality and the ability to change it within Alexa privacy settings is limited. These instances happen because of the increasing possibilities of technology and the reality that the emphasis on protecting personal data is not interpreted uniformly at a global level. Within the USA context there has been a greater emphasis on fundamental freedoms of speech in contrast to privacy. This aligns the Human *Universal Declaration of Human Rights* Article 20 with the USA Constitution wherein freedom of speech is the First Amendment.

Whilst there may be a need to protect personal data, the balance of this is contested across nations. The USA enacted freedom of information legislation in 1966 and as such was an early proponent of providing citizen access to public sector information. Sweden has been a pioneer of freedom of speech and the press with censorship abolished as long ago as 1766. It is therefore not a coincidence that Wikileaks, which campaigns for open data, is based in Sweden. Ironically, the USA has been a significant target for Wikileak attacks. More generally, open data campaigners have called for Open Government Manifestoes with data more automatically made publicly available.

Globally national governments have legislated for different approaches to privacy and freedom of information particularly in respect of the parameters of the work of the security services. In 2013, Edward Snowden, who had been a USA Government employee within the Central Intelligence Agency, leaked classified information from the National Security Agency (NSA). The leaked information revealed a significant level of surveillance across citizens' digital lives including their usage of cell phones, social media such as Facebook, and other software such as Skype. The intelligence gathered was deemed to provide a 'pattern of life' which provided a detailed profile of individuals and their networks of association. The UK's intelligence service was implicated in the surveillance. The targets of the surveillance were not limited to USA and UK citizens. The USA argued that all surveillance was in accordance with USA law and certainly legislation such as the Patriot Act 2001 allow far reaching powers to be exercised to allegedly keep the USA safe from terrorist attack. Snowden is seen by some as a traitor, given that it is argued the intelligence services do need to operate in secrecy to be successful and keep the nation safe. However, others see Snowden as a valiant whistleblower and freedom fighter, as his leaks have been claimed to expose a significant level of snooping on all citizens. Following this incident, the German Chancellor Angela Merkel famously condemned the USA and UK surveillance stating in response to the incident that there should be "no spying among friends". The USA Patriot Act has been challenged in other ways. In 2005 the so called 'Connecticut Four' (four librarians) filed a lawsuit Doe v Gonzales to challenge the powers of the Federal Bureau Agency under the Act, which was claimed to provide for access to libraries' patron reading records. In essence, this debate was about whether an individual should be judged and in part tried based upon what they read. In 2006 the USA Government gave up this battle and in 2007 the 'Connecticut Four' were honored for their stance by the American Library Association.

The expectations for state intervention in overseeing citizens' lives through monitoring of their digital data is highly contested; it is at the heart of the moral agenda delivered by IG in terms of ensuring balanced information delivery. Recently there has been international criticism of China by freedom campaigners regarding so called 'Sesame credit' which scores citizens for their online behaviours including providing points for not only personal behaviour but the behaviours of those within a citizen's digital networks. Good behaviours, such as the purchase of Chinese goods or online educational study, may be rewarded whilst bad behaviours, such as online gaming, may be punished, for example through either travel rewards or travel bans.

The Chinese Government does take a differing stance on some aspects of state control. As cited by Zeng et al (2017), the Chinese President Xi Jinping's address to the Beijing sponsored World Internet Conference in Wuzhen in 2015 indicated China's position that the Internet should be governed according to the same principles as other fields of international relations whereby Internet sovereignty is provided for and respected. As such nations would in accordance with this, control and regulate their own cyberspace. In a world where cyber warfare presents real challenges, the ability to manage boundaries in cyber space may become more accepted. Cybersecurity relies on national values for determining the protections and processes put in place around different types of information as opposed to opening up and creating trust across boundaries.

As technologies have advance there have been new areas of contention. The ability for humans to understand and account for new technologies is complex. With the advancement of robotics, autonomous vehicles, machine learning and Artificial Intelligence (AI), who holds responsibility for the actions of technology is being gradually defined in law. In the context of these technologies the role, decisions and

accountability in terms of human interventions are being further worked through. As new forms of technology emerge with biological components and increasingly sophisticated systems the boundaries between human rights and 'personhood' are a further area of contest. In 2017, the EU Legal Affairs Committee argued for the potential for AI and robots to have the status of personhood. However, this concept is as much about assigning responsibility away from individuals. Limited companies have legal personhood with legal responsibility. Nevertheless, there are boards of people with culpability for decisions if not financial payment. We are still working out:

1. What is a person and what are the rights that assign to 'personhood'?
2. What are the responsibilities that assign to 'personhood'?
3. Where are the boundaries and laws required between human and machine?
4. How are robots and AI understood and accountable?
5. How can/should these technologies be deployed.

In the latter context we see already the debates around surveillance but also in regards to AI predictive technologies and what they should be allowed to calculate or assume.

The link between information rights/data law link to education, consumerism and networks are a contested ground globally. IG seeks to underpin and enforce good ethical information behaviours but in part relies on legislation as the ultimate boundaries for delivering these frameworks. Where moral behaviours are agreed, IG provides for whistleblowing to call out bad behaviours and in some instances, this has changed engrained national norms. However, the complexity of navigating information boundaries is not insignificant.

INFORMATION GOVERNANCE FRAMEWORKS

There is no one single approach to delivering IG. There are a wide range of frameworks that have been developed to put in place systems for managing, protecting and leveraging information value through IG frameworks. The ARMA International's *Information Governance Maturity Model* developed in 2010 established eight key principles against which to measure IG delivery within an organizational context which include accountability, transparency, integrity, protection, compliance, availability, retention and disposition. These principles have been largely developed from records and information management paradigms and whilst providing a strong internal framework they nevertheless potentially require some development to take account of managing information across complex boundaries. A critical component within the framework is the delivery of retention/disposition schedules. In a cybersecurity context it is important not to retain redundant information which might pose risks to an individual or organization if accessed by an unauthorized party. Equally key data, as established under a retention schedule, must be protected to ensure its continued availability and integrity through time to authorised parties. Equally there is a need to ensure information remains available. Cyber attacks have sought new ways to cause damage and unethical profit. For example, ransomware attacks take control of a system and deny access to core data by organizations or individuals subject to the payment of a ransom. Bitcoin has enabled ransoms to be paid with minimal potential for the payment to be tracked. The proliferation of new forms of attack continue each year. In this regard it is the International Standard's Organization's family of information security standards *ISO 27000* (see http://www.27000.org/) that builds a strong framework aligning IG and cybersecurity.

ISO 27000 is legislated for as the recommended standard for information security best practice, for example to deliver personal data security under the EU's GDPR and to meet the

requirements of the USA's Federal Information Security Management Act. The key requirements of the standard series are to deliver an 'Information Security Management System (ISMS)' which provides for information as an asset to be managed to deliver:

- protection of organisational assets, ensuring both their ongoing availability for business purposes and their protection against unauthorised access;
- privacy of personal information;
- maintenance of intellectual property rights.

Critically it delivers (ISO 2012, 2 and 5):

- Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
- Integrity: The property of safeguarding the accuracy and completeness of assets.
- Availability: The property of being accessible and usable upon demand by an authorised entity.

These defined characteristics are not synonymous and may sometimes need to be balanced with choices made through risk management decision processes. However, importantly they provide for the delivery of a system which is not dealing with a narrow definition of security which locks down information but rather one which delivers information in accordance with organizational/national needs. The framework is established through (ISO 2013a):

- a policy, objectives and activities that reflect business objectives and can include whistleblowing processes;
- asset classification and control;
- physical and environmental security;
- personnel security;

- an approach and framework to implementing, maintaining, monitoring (including incident reporting systems), improving systems consistent with the organisational culture;
- systems development and maintenance protocols;
- business continuity management;
- legal compliance frameworks;
- visible support and commitment from all levels of management;
- effective marketing of the requirements to all managers, employees and other parties to achieve awareness;
- distribution of guidance on policy and standards to all managers
- provisions to fund key activities;
- provision of appropriate awareness, training and education;
- implementation of a measurement system to evaluate performance and feedback suggestions for improvement.

It aligns to the ARMA International IG principles but places the delivery of a potentially wider scoped risk management framework. Some of the most effective implementations of an *ISO 27000* system may be very simple systems as it is argued these can enable individuals to engage with, understand, remember and implement the system requirements. Key to successful IG delivery is human engagement with the values delivered by the frameworks.

The standard requires than an organisation understands what information assets it holds and then ascertains the value of these assets. The starting point for evolving the ISMS is the information asset register which records the asset, its value, location and owner in

terms of assigning responsibility for the asset. Information assets are wide ranging and include the knowledge that individuals hold if it is significantly valuable and the future potential lack of availability of that knowledge presents a risk to organisational processes. In essence, *ISO 27000* links knowledge management concepts (which focus on human knowledge of organisational value) and records and information management. Furthermore, any other key components that are part of the delivery of information assets value must be listed, including software suppliers, systems hardware and other non-technological information components.

RISK ASSESSMENT AND TREATMENT

Risk assessment and risk frameworks are a mandatory part of the *ISO 27000* framework. The risk methodology requires the development of the information asset register to ensure that the threats and vulnerabilities for each information asset's confidentiality, integrity and availability are managed. Risk assessment should involve the identification of information opportunities in addition to potential negative consequences from system failures. Thus, Cloud computing services provided by a third party may result in some loss of organizational control. However, working with a Cloud service that operates at a larger scale may provide additional expertise to mitigate against new and emerging software threats. Key to decision making in terms of the whole infrastructure deployed is to understand the value(s) of information and the competing requirements and threats/vulnerabilities.

The overarching risk management process requires the understanding of strategic objectives, the establishment of risk appetite (i.e. the level of risk exposure which is acceptable), risk assessment, analysis and evaluation, risk reporting, decisions and treatment and then ongoing monitoring and review. In the simplest of systems, the information asset is provided with a value which aligns to the scored impact should the information be

compromised in any way. In the context of *ISO 27000* compromise may mean that the information is:

- disclosed to unauthorised parties, for example if the information is stolen for the purposes of identity theft or other forms of cybercrime;
- unavailable, for example through loss, data corruption or as occurs in the instance of a ransomware attack,
- no longer trustworthy, for example if a system has been tampered with.

In terms of valuing information, it is important to note that the value of information may not be static. Some information relies on immediacy, for example information relating to financial markets may be highly significant at a very particular point in time. Other information accrues value. In the context of big data, data gains value by virtue of the scale of information held. The same piece of information or data may have multiple significances to different stakeholders. Against each asset, any threats/vulnerabilities relating to the asset are identified, described and estimated. A threat itself cannot be managed but the vulnerabilities the threat can exploit can be dealt with. As risk seeks to mitigate the "effect of uncertainty on objectives" (ISO 2018) organizations will then determine an approach to risk. The risk exposure is calculated by multiplying the asset value/impact by the likelihood of the vulnerability being exploited.

In addition, to assessing the organizational and legislative context a number of models can help with understanding risks. One such model is the STEEPLE model. This has seven factors which provide domains for considering risks. The seven factors are (Lomas and McLeod 2017) socio-cultural factors (S), technological factors (T), economic factors (E), environmental impacts (E), political factors (P), legal factors (L) and ethical factors (E). These enable information values to be considered in a diverse way and to take into account

risks including social agendas more widely. For example, the factors take into account environmental considerations considering the power resource implications of managing information through time. One case is that of bitcoin. Alex de Vries, a bitcoin specialist at PwC, has estimated that the servers required to run bitcoin consume almost as much power as that taken to run Ireland (De Vries 2018). Equally many individuals now have multiple devices running and consuming power for a wide range of non-essential uses. As such IG does encompass environmental considerations which may score differently in terms of an impact as opposed to economic impacts.

Whilst the approach of quantifying risk by multiplying the asset value/impact by the likelihood of the vulnerability being exploited is one of the more common approaches it is not the only one. Another approach commonly used in an Information and Communication Technology (ICT) context relates to analysing the single loss expectancy (SLE) for a single event which is calculated by the asset value multiplied by the likelihood or exposure factor. An annualized loss expectancy (ALE) can then be calculated by multiplying the annual rate of occurrence (ARO) by the single loss expectancy (SLE). This can be a useful approach in an ICT context where, as an example, power outages may influence ICT service delivery on multiple occasions or in regards to cybersecurity where there may be numerous cyber attacks.

Where there is legislation in place, the organization must act to manage and mitigate vulnerabilities. However, in many instances there will be a balance to be struck in terms of the action required. There is often no one right response to the risk choices to be made, as to share information will have benefits but may mean opening up information to some additional security risks. An organization may have an agreed risk appetite that will be critical to evaluating and implementing the appropriate risk approaches. The risk appetite can simply be set at a defined level whereby the risk score, if above the defined risk appetite, must be dealt with. This is typically dispensed with by terminating the process and thus

erasing the risk, treating the risk through applying controls or transferring the risk to another party. In the latter context it is important to note that not all risks can be transferred. For example, an EU organization that captures personal data can outsource the management of that personal data but nevertheless it retains data protection responsibilities under EU data protection laws. In considering risk in an opportunistic context there will be certain calculations where the risk must be taken to leverage an advantage. In addition, risk can be tolerated. It remains impossible to negate all information vulnerabilities if the range of information values are to be leveraged.

Societal expectations for risk in different national and organizational contexts do differ. The financial sector is highly regulated to ensure confidence and consumer protection within the financial system. The public sector contains large quantities of diverse personal data sometimes sensitive in nature. There is an expectation, in this context, that the information will be protected and that public-sector organizations will be accountable and transparent regarding their actions. The retail sector now often has large amounts of customer data which needs to be managed to provide customer assurance and maintain reputational confidence. Within this context information is key for managing supply chains.

Within the *ISO 27000* standard are a list of 114 controls divided between process controls such as policies and procedures, physical controls, technical controls, legal and regulatory controls and human controls including HR processes, education and training (ISO 2013b). Organizations can also adopt their own additional controls. Controls can be preventive, detective or corrective. It is a requirement of the standard to create a 'statement of applicability'. This is defined as a "documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS" (ISO 2013b). Where a control is not selected then it is necessary to justify within the statement of applicability why the system does not require that control. This process helps put in place a structure of

linked information security responsibilities, e.g. ICT will be responsible for network access controls and operating system access controls, HR for all employment recruitment and contracts including vetting, undertakings of confidentiality etc. Whilst individual controls may fall within pre-existing frameworks some will require new partnerships and the programme of reviewing these controls therefore builds an information management framework of responsibilities (Lomas 2010). This is critical for IG and cybersecurity successful delivery. For example, HR may decide on homeworking policies, but these will also rely on ICT to facilitate access to online working spaces that do not compromise other network security considerations. As cyber attacks increase, it is important that training occurs with appropriate penalties for noncompliance. A bank may dismiss an employee for clicking on a link in an email that may contain a virus or responding to a phishing attack whereas a University is not likely to take such severe action. ICT will identify the risks and work with HR on training employees but HR will determine any dismissal procedures.

Organizations must have approaches to handling incidents, including accidents, as well as full scale crises including internal and external attacks. Business continuity planning provides for pre-empting such situations. One of the listed controls relates to change management. In this regard *ISO 27000* requires that information systems continue to be continuously monitored, through the cycle of planning, checking, doing, acting and monitoring to make sure all aspects remain up-to-date and appropriate. All information security incidents, including near misses, must be recorded, reviewed, assessed and new processes established as appropriate.

Other codes also assist with defining specific data governance and ICT security and management requirements. Examples include *DoD 5015.2* (Department of Defense 2002) as a specific security sets of measures, *COBIT 5* for audit approaches (Information Systems Audit and Control Association 2012), and *ITIL* for maintenance purposes (Office of

Government Commerce 2011). In a technology context, vulnerability disclosure is required to enable organizations to identify and patch weaknesses within ICT software and hardware that can be exploited by cyber criminals. A recent report by ENISA (2018) sets out the different actors within a vulnerability disclosure process and the significant role of economic considerations and incentives that may influence their behaviour. The report concludes that it is often due to economic protection that some vulnerabilities are disclosed responsibly whilst others are not. As such it is important for Governments to hold software and hardware suppliers to account for such notifications and for the complex network of information relationships to be understood to provide IG.

Too simplistic risk profiling has increasingly been called into question (Gilb 2005, Lomas 2010). In the wake of the 2008 banking crisis, risk profiling was shaken to its roots. The complexity of managing risk and better understanding networked risks was given greater recognition. This involves more sophisticated approaches to planning and considering a range of scenarios and future outcomes.

Risk management needs to take on board new realities of information creation and thus management. As information growth and variety expands, the ethics and realities of information value, ownership and placement across legislative regimes need to be negotiated and risk assessed. *ISO 27000*'s central focus on frameworks with risk management processes at their very heart provide one tool which can assist. Nonetheless and critically is international cooperation and collaboration at a Government and citizen level.

INFORMATION GOVERNANCE SUBCOMPONENTS

As noted, IG provides an overarching framework but within it there are component parts of the 'technical' governance delivery which are sometimes isolated to focus on a specific aspect of the IG delivery. These include, but are not limited to data governance,

information assurance, cyber security and governance, information security, Internet governance and IT governance. Where governance is aligned it implies board level oversight and a broader ethical consideration of the delivery.

Information must be reliable to deliver value and this process is delivered through data governance. One way of providing greater assurance of information value is to break down the information into its smallest component parts (i.e. data) in order to ensure that each piece of data is reliable. This is termed data quality. Sarsfield (2009, 38) defines data governance as guaranteeing that data can be trusted, and people made accountable for any adverse event that happens when the data quality is poor. In this context ownership and responsibility for preventing issues with data and fixing any issues that occur. Reliable data governance can provide powerful intelligence to impact on decision making and direction.

Data governance is delivered by the provision of data quality linked to the process of data curation and stewardship including the provision of metadata. Metadata encompasses a wide number of elements. The Dublin Core Metadata Initiative defined 15 core metadata elements, which have now been incorporated into the international standard *ISO 15836* (ISO 2017a) and are wide ranging including for example metadata about the author, creation date and data format. These elements can be separate, encapsulated, tagged, hidden or explicit, automated or manually applied. The international standard *ISO 23081* (ISO 2017b) defines six types of metadata including metadata about records, agents, business activities or processes, records management processes, business rules or policies and mandates, and metadata about metadata.

Metadata is also a critical component of information assurance which seeks to ensure the evidential value of information delivery. The five information assurance pillars are availability, integrity, confidentiality, authentication and non-repudiation. The first elements traditionally align to information security delivery and are at the heart of IG

frameworks. So too are the additional components of authentication and non-repudiation which refer to the application of processes which will assure that an author's statement or documentation cannot be disputed in terms of its validity. As such it is often associated with legal processes, for example the delivery of a contract. Aligned within this aspect of legal delivery is e-discovery which provides a framework for the discovery and production of information in a legal suit.

IT governance looks specifically at the technical delivery (Weill and Ross 2004), "the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives." Another IG component is cyber governance which deals with organizational cyber risks at a board level engaging key stakeholders. Von Solms (2016) sets out a maturity model for this one IG subset. This has been built on the PwC's global security surveys (PwC 2015). This surveys the budget, roles and responsibilities of the security within an organization, security policies, security technologies, overall security strategy and finally the review of the current security and privacy risks. Based on this data set, Von Solm has developed a maturity model that sets out 4 categories against which maturity is measured:

- Category 1: Understanding the strategic role of Cyber Risk in the company
- Category 2: Understanding and providing guidance on the Cyber Strategy of the company
- Category 3: Understanding and reviewing the Cyber Security budget for the company
- Category 4: Understanding and evaluating the Cyber Security policies of the company

The categories have further sub-categories and against each, the level of maturity is assessed through a scale of nothing existing at all, to a very basic position, to a progressed position, and finally a stable position. The maturity levels evidence that, in this context,

security is locked down but there is no greater ambition than stability. Strategic and opportunistic ambition for information more widely is set into the bigger IG framework.

Cyber security systems seek to keep information safe from a wide range of attacks within a cyber context. Information security provides for the management of security risks across all platforms and information formats including technology and people with assets including knowledge, paper documentation and online data formats. To harness the value of information/data whilst providing protection, sophisticated approaches to information creation and management are required. It is an oft quoted maxim that a security system is only as strong as its weakest link. In this regard, Kooper et al denote the limitations and inadequacies of relying on only smaller parts of governance delivery, such as IT governance (Kooper et al 2011). To deliver on information value, opportunistic and negative risks must be balanced. Kooper et al, discuss the balance of actors and the wider dimensions of delivering on information value. To deal with this complexity, holistic systems are needed that manage a wide range of information considerations not least the human factor.

Furthermore, as technology is driven globally, these systems must take account of information rights legislation at a global scale and regional difference in law and citizen expectations must be navigated. As such it is IG, which has emerged as a multidisciplinary field, that provides for holistic thinking and frameworks to protect and enhance the management of information. The 2017 survey delivered by the Information Governance Initiative and published in 2018, which claimed to have reached 100,000 practitioners globally, stated that 48% of practitioners saw IG as essential for successful cyber security delivery even though cyber security is narrower in delivery as it cannot exist without broader underpinning. IG provides for a wider and more comprehensive approach.

THE HUMAN FACTOR

As noted by Rubino et al in 2017, key to good governance is to have leadership throughout an organization in order that others take on the significance of managing and protecting information ethically. This applies at Government levels too. In addition, IG needs to be understood and engaged with by multiple parties if it is to be successfully implemented and maintained. The Information Governance Initiative's (IGI) 2018 report further defines areas of information delivery and aligns these to a requirement for people with professional expertise to provide IG frameworks including analytics, audit, big data, business intelligence, business operations and management, compliance, data curation and stewardship, data governance, data science, data storage and archiving, e-discovery, enterprise architecture, finance, informatics, information security and protection, IT management, knowledge management, legal, master data management, privacy, records and information management and risk management (IGI 2018, 17). The report (IGI 2018, 37) defines the roles of the:

- Accountable (the boss)
- Responsible (the doers) including professionals which encompass records and information management professionals, information security, legal and compliance business operations and management, risk management, data storage and archiving and privacy.
- Consulted (the advisors) including expertise from the above professions and in addition audit.
- Informed (the dependents).

In the latter context, this looks largely internally. However, in accordance with evolving governance principles, organizations must look outside their boundaries to consider wider engagements with all information stakeholders. As a social construct, the concept of systems with human design and societal needs at their centre are critical to IG delivery. In

addition, humans need to be provided with skill sets to better navigate new digital realities. The United Nations Educational, Scientific and Cultural Organization (UNESCO 2013) recognizes the human right and requirement for all citizens to receive a media and information/digital literacy education to navigate information in order to access reliable information/data and use it successfully. In a world of 'fake news' and social media subversion this has become more critical. These boundaries are becoming further complicated by technological advancement. Artificial intelligence and algorithms are delivering new decision making into society; it is important that these remain controlled, understandable and relatable for human needs. The potential for robots to have legal personality and rights is becoming a new and complex space of ethical debate. Human and societal needs must remain at the centre of IG as it expands and proliferates. Individuals do need wide ranging training and education to fully engage with the potential risks and opportunities associated with creating, sharing and using information. As noted within the World Economic Forum personal data has an economic value due to the new potential to connect it to and profile individual service and consumer needs. The complexity of human needs will need to be better framed in terms of ethical considerations that can then be enshrined into international law. To date the Human Rights Declaration has developed fundamental moral tenets pertaining to information governance but their complex balancing and application in law is only partially evolved and not globally agreed. In a digital era legal responsibilities and accountability are not properly agreed and accounted for. Setting human moral agendas in place is key for information governance to have effect.

CONCLUSION

The pervasiveness of information and technology with interdependencies between digital and physical spaces have created a world in which information and its governance impact on all aspects of society.

Key components of IG delivering are:

- Putting the human dimensions at the heart of IG processes to ensure an ethical delivery which is framed in accordance with societal needs;
- Contextual understanding of national and organizational information needs;
- Greater global agreement on information rights laws;
- Developed and mature IG professionalism with interlinking expertise from across a wide range of professional domains;
- Understanding of information assets, their (co)creation, ownership, sharing and evolution;
- IG frameworks around assets with Government/board oversight on policies, strategies and risk management including audit and regulatory underpinning.

The threats to our world through cybercrime and warfare are increasing. IG with its capacity to deliver a multidisciplinary and holistic response to contested and complex challenges is essential for successful cyber security and the bigger issues of organizational management, Government leadership, national security and international cooperation. Locking down all information is not possible as it creates alternative risks. Navigating, managing, mitigating and taking risk is essential for human evolution and survival. However, it important that in so doing the moral needs of society/humans remain at the heart of an information governed world.

REFERENCES

Adesemowo, Adjeniji., Rossouw von Solms, and Reinhard Botha. 2016. "Safeguarding Information as an Asset: Do We Need a Redefinition in the Knowledge Economy and Beyond?" *South African Journal of Information Management*, 18(1).

ARMA International. 2010. *Information Governance Maturity Model*. Kansas: ARMA.

Arquilla, John. 2012. "Cyberwar Is Already Upon Us. But Can It Be Controlled?" *Foreign Policy*, 27 February 2012. Available from: https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/. Accessed April 22 2019.

Blair, Barclay. 2012. "Advancing a Definition of Information Governance." *Essays in Information Governance*. Washington: IGI. Available from: http://barclaytblair.com/2012/02/24/advancing-a-definition-of-information-governance/ **.** Accessed April 22 2019.

Cadbury, Adrian. 2000. *Global Corporate Governance Forum.* Washington DC: World Bank 2000.

Day, Matt, Turner, Giles and Natalia Drozdiak. 2019. "Amazon Workers Are Listening to What You Tell Alexa", *Bloomberg News*, 10 April 2019. Available from: https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio. Accessed April 22 2019.

Denardis, Laura. 2014. Cybersecurity Governance. In *The Global War for Internet Governance*, 86-106. Connecticut: Yale University Press.

Department of Defense. 2002. *DoD 5015.2 Design Criteria Standard for Electronic Records Management Software Applications.* DoD. http://dtic.mil/whs/directives/corres/pdf/501502std.pdf. Accessed April 22 2019.

Desouza, Kevin. 2009. "Securing Information Assets: The Great Information Game." *Business Information Review*, 26(1).

De Vries, Alex. 2018. "Bitcoin's Growing Energy Problem", *Joule*, 2(5), p801-805.

ENISA. 2015. *Governance Framework for European Standardisation.* https://www.enisa.europa.eu/publications/policy-industry-research. Accessed April 22 2019.

ENISA. 2018. *Economics of Vulnerability Disclosure*. Athens: ENISA. https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure Accessed April 22 2019.

Eugen, Petac. and Duma. Petruţ. 2018. "Exploring the New Era of Cybersecurity Governance." *Ovidius University Annals, Economic Sciences Series*, *18*(1), 358-363.

European Commission. 2008. *On Promoting Data Protection by Privacy Enhancing Technologies.* Brussels: European Commission.

European Parliament and Council of the European Union. 2016. *Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (Data Protection Directive). The General Data Protection Regulation*. *L119*, 1-88. Brussels: European Parliament and Council of the European Union.

Financial Reporting Council. 2018. *UK Corporate Governance Code*. London: Financial Reporting Council.

Fliegauf, Mark. 2016. "In Cyber Governance We Trust." *Global Policy*, 7(1).

Franks, Patricia. and Nancy Kunde. 2006. "Why Metadata Matters." *The Information Management Journal*, Sep-Oct 2006, 55-61.

Gilb, Tom. 2005. *Competitive Engineering: a Handbook for Systems Engineering, Requirements Engineering, and Software Engineering Using Planguage*. Oxford: Elsevier.

Harmer, Geoff. 2013. *Governance of Enterprise IT based on COBIT5: a Management Handbook.* Ely*:* IT Governance Publishing.

Himma, Kenneth and Herman Tavani. 2008. *The Handbook of Computer Ethics*. Chiswick: John Wiley & Sons.

Information Governance Initiative. 2018. *IGI State of the Industry Report: Volume III.* Washington: IGI.

Information Systems Audit and Control Association. 2012. *COBIT 5 - Control Objectives for Information and Related Technologies*. Illinois: Information Systems Audit and Control Association.

ISO. 2012. *ISO/IEC 27001:2012. Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary.* Chiswick: BSI.

ISO. 2013a. *ISO/IEC 27001:2013. Information Technology – Security Techniques – Information Security Management Systems – Requirements.* Chiswick: BSI.

ISO. 2013b. *ISO/IEC 27002:2013. Information Technology – Security Techniques – Code of Practice for Information Security Controls.* Chiswick: BSI.

ISO. 2017a. *ISO/IEC 15836-1:2017. Information and Documentation – the Dublin Core Metadata Element Set- Part 1: Core Elements.* Chiswick: BSI.

ISO. 2017b. *ISO/IEC 23081-1:2017. Information and Documentation – Records Management Processes – Metadata for Records Part 1: Principles.* Chiswick: BSI.

ISO. 2018. *ISO/IEC* 31000:2018, *Risk Management – Guideline.* Chiswick: BSI.

Office of Government Commerce. 2011. *ITIL*. London: Her Majesty's Stationery Office.

KMPG. 1995. *Hawley Committee: Information as an Asset- Checklist and Explanatory Notes.* London: KPMG.

Kooper, Michiel. Rik Maes, and Edo Roos Lindgreen. 2011. "On the Governance of Information: Introducing a New Concept of Governance to Support the Management of Information." *Information Management Journal*, 31, 195-200.

Logan, Deborah. 2010. "What is Information Governance and Why is it so Hard?", *Gartner blog*. http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/ . Accessed April 22 2019.

Lomas, Elizabeth. 2010. "Information Governance: Information Security and Access Within a UK Context." *Records Management Journa*l 20(2), 182–198.

Lomas, Elizabeth., Basma Makhlouf Shabou, and Arina Grazhenskaya. (2019). 'Information Governance and Ethics - Information Opportunities and Challenges in a Shifting World: Setting the Scene' *Records Management Journal*, 29(1).

Lomas, Elizabeth and Julie McLeod. 2017. "Engaging with Change: Information and Communication Technology Professionals' Perspectives on Change in the Context of the 'Brexit' Vote." *PLoS ONE* 12(11)

MacLennan, Alan. 2014. *Information Governance and Assurance*. London: Facet.

Mason, Richard. 1986. "Four Ethical Issues of the Information Age." *MIS Quarterly*, 10(1), 5–12.

Norton. 2017. *Norton Cyber Security Insights Report Global Results*. Mountain View: Symantec. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf. Accessed April 22 2019.

Organisation for Economic Co-operation and Development. 1980. *OECD Guidelines on the protection of privacy*. Paris: OECD.

PwC. 2015. *Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015*. London: PwC.

Rubino, Michelle, Fillipo Vitolla, and Antonello. Garzoni, A. 2017. "The Impact of an IT Governance Framework on the Internal Control Environment." *Records Management Journal*, 27(1), 19-41.

Sampson. Karen. 1992. *Value Added Records Management: Protecting Corporate Assets, Reducing Business Risks.* Westport: CT.

Sarsfield, Steve. 2009. *The Data Governance Imperative*. Ely: IT Governance Publishing.

Smallwood, Robert. 2014. *Information Governance: Concepts, Strategies, and Best Practic*es. California: Wiley.

United Nations Educational, Scientific and Cultural Organization (2013) *Global Media and information literacy (MIL) assessment framework: country readiness and competencies*. Paris: UNESCO. Available from: http://www.karsenti.ca/archives/UNE2013_01_MIL_FullLayout_FINAL.PDF Accessed April 22 2019

United Nations General Assembly (1948) *Universal Declaration of Human Right.* Paris: United Nations General Assembly. Available from: https://www.refworld.org/docid/3ae6b3712c.html Accessed April 22 2019.

United Nations, General Assembly (2015) *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174). New York: United Nations General Assembly. Available from: https://digitallibrary.un.org/record/799853 Accessed April 22 2019.

Van Den Hoven, Jeroen. 2008. "Chapter 3: Moral Methodology and Information Technology." *In* Himma, Kenneth and Herman Tavani. 2008. *The Handbook of Computer Ethics*. Chiswick: John Wiley & Sons.

Von Solms, Basie. 2016. 'Towards a cyber governance maturity model for boards of directors', *International Journal of Business and Cyber Security*, 1(1), p1-9.

Weill, Peter, and Jeanne Ross. 2004. *IT governance—How top performers manage IT decision rights for superior results*. Boston: Harvard Business School Press.

Willis, Anthony. 2005. 'Corporate governance and management of information and records', *Records Management Journal*, 15(2), 86-97.

World Economic Forum. 2011. *Personal data: the emergence of a new data class*. Geneva: World Economic Forum.

Zeng, Jinghan., Tim Stevens, and Yaru Chen. 2017. 'China's solution to global cyber governance: unpacking the domestic discourse of "Internet Sovereignty"', Politics and Policy, 45(3), 432-464.