Practicable Backup Arrangements for Small Organisations and Individuals

Roger Clarke
Australian National University
Roger.Clarke@anu.com.au

Abstract

The last thirty years of computing has resulted in many people being heavily dependent on digital data. Meanwhile, there has been a significant change in the patterns of data storage and of processing. Despite the many risks involved in data management, there is a dearth of guidance and support for individuals and small organisations. A generic risk assessment is presented, resulting in practicable backup plans that are applicable to the needs of those categories of IT user.

Keywords: Recovery; Security risk assessment; Micro-organisation; Prosumer

1 Introduction

Large and medium-sized organisations manage their backup and recovery mechanisms within the context of broader disaster recovery and business continuity planning. So do some proportion of small and micro-organisations and even individuals, where they recognise the importance of their data, and have access to sufficient technical and professional expertise. However, in the fourth decade of widespread computer usage, in Australia alone, more than half-a-million small organisations and some millions of consumers are highly dependent upon data, and remain at risk if their data suffers harm.

Yet straightforward guidance on how micro-organisations and individuals should address those risks is surprisingly difficult to find, with multiple searches in such venues as AIS eLibrary and Google Scholar delivering relatively few sources of significant relevance. Only a minority of text-books contain segments, in most cases brief, e.g. Slay & Koronios (2006, p.23), Boyle & Panko (2013, pp. 487-502). Backup appears to be too prosaic a topic to attract attention from IS researchers. For example, in over 500 articles published in AJIS during its first 23 years, not one has the word 'backup' in the title and only 17 (3.5%) even contain the word. In the entire AIS eLibrary, whose collections date back in many cases for 20 years, and in the case of MISQ 40 years, 3 articles have the word in the title, and a further 7 have it in the Abstract, in a corpus of over 30,000 entries. Moreover, none of those papers offered any important contribution to the research reported in this paper. Relevant sources found during the course of the research are cited in the particular sections in which their contributions are relevant to the analysis.

A possible reason for the absence of a visible literature is that academics have assumed that backup and recovery are old problems, long since solved. That is not a tenable proposition, however, because the now three decades of 'personal' computing have involved significant changes in a variety of areas. Organisational hierarchies have been giving way to networks of smaller entities, with a great deal of activity outsourced. Many workforces have been subject to casualisation. Desktops and laptops have been giving way to handheld devices. Organisation-provided devices have been complemented and then to some extent replaced by Bring Your Own Device (BYOD) arrangements. The location of data and application software has switched from the desktop and nearby servers to distant service-providers, initially in a defined physical place but now 'in the cloud' (Clarke 2011).

These changes have brought with them an increased range of threats (e.g. phishing, ransomware) and increased intensity of existing threats. The low quality of software has brought with it an increased range of vulnerabilities. Devices are more opaque than before, particularly smartphones and tablets, where Apple has driven the industry away from general-

purpose computing devices and towards supplier-controlled and -limited 'appliances'. Most users have little interest in understanding the complexities involved, and limited capacity to comprehend them. Human-computer interfaces increasingly reflect a strong emphasis on hedonism, with convenience and excitement as the primary objectives, and little attention paid to risks. In the new context, a re-visit to the topic of backup is essential.

The problem addressed in this paper is the absence of up-to-date guidance for micro-organisations and individuals in relation to the design and conduct of backup and recovery.

Large and medium-sized organisations have access to specialist expertise. A proportion of small and micro-organisations also employ information technology (IT) professionals or contract them on an intensive basis. The focus of this research, however, is on individuals, and on micro-organisations and small organisations, that (rightly or wrongly) do not perceive IT and computer-readable data as being central to their work, and that have modest or very limited competence in IT matters.

A particular focus is on individuals who make relatively sophisticated use of computing facilities for such purposes as the management of personal finance, tax and pension fund, and correspondence, databases of images, videos or audio, or family-trees. The notion of the 'prosumer', coined by Toffler (1970, 1980), has progressively matured (Tapscott & Williams 2006, Clarke 2008). A prosumer is a consumer who is proactive (e.g. is demanding, and expects interactivity with the producer) and/or a producer as well. In the context of computer usage, a third attribute of relevance is professionalism, to some extent of the person themselves but also in relation to their expectation of the quality of the facilities and services they use. A second focus in this work is on very small organisations that involve one or two individuals. Such micro-organisations are within-scope whether they are incorporated or not, whether their activities are stimulated by economic or social motivations, and whether they are for-profit or otherwise. Some categories of small organisation with up to 20 staff or contractors have similar characteristics and needs to micro-organisations.

The relevance of this work extends further, however. During the last two centuries, workers were mostly engaged full-time by organisations under 'contracts of service', and a large body of employment law developed. The last few decades have seen increasing casualisation of workforces, with large numbers of individuals engaged through 'contracts for services'. This requires them to take a far greater degree of self-responsibility. To the extent that large organisations depend on sub-contractors' use of computing and management of data, the sub-contractors' security risks impact upon the organisations that engage them.

The scope of the work is defined as 'backup and recovery'. This excludes broader security issues such as firewalls and the encryption of communications, except to the extent that they have a potential impact on the values that the individual perceives in data. The prosaic-sounding and somewhat dated terms 'backup and recovery' have been used intentionally. Larger organisations may benefit from applying the broader concepts of business continuity planning and disaster recovery strategies, whereas the horizon of the majority of small organisations and individuals is unlikely to extend that far.

The purpose of the research was defined as:

> *to develop practical guidance on how small organisations and individuals can use backup techniques to address data risks*

Reflecting that purpose, this paper is not addressed exclusively to researchers. The emphasis is on practicality, and the expression is intended to be accessible to professionals as well, with unnecessary intellectualisation of the issues avoided.

The following section examines a key determinant of appropriate backup strategy, namely the pattern of data-storage and processing that the prosumer or micro-organisation adopts. A description is provided of how the design science approach was applied in order to address the problem. There is considerable diversity among the categories of users targeted by the research, so it is necessary to define a test-case to which the method can be applied. The main

body of the paper summarises the outcomes of the risk assessment process. This enables three Backup Plans to be presented, corresponding to three different patterns of IT use.

2 Patterns of Data-Storage and Processing

Considerable changes have occurred during the last three or four decades in the locations in which data is stored, and in which it is processed. In order to provide guidance in relation to backup arrangements, it is therefore necessary to first identify the key distinctions among the alternative patterns.

As Table 1 depicts, the original pattern was for processing to be performed locally, with the data stored within the device, or on a nearby computing device. Soon afterwards, the alternative emerged of using a storage-device attached to the local area network and commonly referred to as networked-attached storage (NAS). Within-device and NAS approaches are categorised here as 'Self-Sufficiency', in order to convey the substantially independent nature of the person or organisation.

The need to maintain 'off-site' or 'fire' backups is one particular challenge arising from the Self-Sufficiency model. A second pattern emerged, whereby another party provides support for the functions of creating and managing off-site backups. This is identified in Table 1 using the term 'Backup Service'.

	Short Description	Indicative Timeframe	Location of the Primary Copy	Location of the Backup Copy	User Experience
1	Self-Sufficiency	1980-	Local	Local	Demanding
2	Backup Service	1990-	Local	Remote	A Little Easier
3	File-Hosting	2000-	Remote	Local	Easier Still
4	SaaS	2010-	Remote	Remote	Easiest

Table 1: Alternative Data-Storage Patterns

A third pattern became common, referred to in Table 1 as 'File-Hosting'. This arose as the capacity of wide area networks increased, and transmission costs decreased. Another important factor was the proliferation of device-types, with desktops and laptops (variously personal and/or employer-provided) complemented by PCs in Internet cafés, airport lounges and customers' premises; and more recently the user's own smartphone and tablet. Increasingly, individuals used multiple devices, and in multiple locations. The use of file-hosting services represents outsourcing of the operation of the NAS. Users draw down copies of files when they need them, onto whichever device they are using at the time. Changes made to the user's copy need to be uploaded to the file-host. Where copies of files are maintained permanently on users' devices (e.g. address-books and diaries / calendars), processes variously referred to as replication, mirroring and synchronisation need to be implemented.

A fourth pattern has since become increasingly common, indicatively from about 2010 onwards. Whereas, with the 'File-Hosting' approach, processing continues to be performed locally to the user, the fourth pattern involves the service-provider not only hosting the user's data, but also performing much of and even all of the processing. Currently conventional terms for this include cloud computing and (Application) Software as a Service (SaaS – Armbrust et al. 2009, Clarke 2011).

The scope of the research conducted extends to all four of these patterns. This paper, however, reports on the outcomes of the research in relation to only the first three patterns. A companion paper considers appropriate backup approaches in the context of SaaS (Clarke (2016).

The three patterns of use identified in Table 1 need to be articulated further, in order to establish a firm foundation for the analysis and design of backup plans. A preliminary decision

of relevance is the means that the individual uses to achieve sufficient synchronisation among their multiple platforms. In a multi-platform environment, there are likely to be multiple copies of files. Clarity is needed as to which file is the primary copy.

A basic arrangement involves the designation of one computing device as the master - typically the desktop - with the others managed as slaves. The primary copy of the data is on the master-device, and this is mirrored forward from the master to the slaves at convenient times. This is generally done when they have a suitable connection to the master, and there is little or no conflict with other activities, e.g. when all are on the local network overnight. Where a slave device is used to create a new file or amend an existing file (e.g. while the user is away from the office), special care is needed to achieve disciplined backloading to the master-device.

A second arrangement utilises as the primary storage-medium a NAS on the individual's local area network. Any of the computing devices may create new files and amend the primary data, with a file-locking mechanism used to ensure that at any time only one of the computing devices has the capability to amend each file. Where a new or amended file is stored on one of the devices (e.g. because a network connection to the NAS cannot be achieved at the time), special care is needed to achieve disciplined backloading to it.

A step beyond NAS is a Redundant Array of Independent Disks Level 1 (RAID), of which RAID1 is the form relevant to the present discussion. This is essentially a NAS containing two disks, with all write activities occurring on both disks. RAID1 addresses the specific risk that one disk will be lost (in particular, because of a disk crash).

All of the master-slave, NAS and RAID approaches are part of the first, Self-Sufficiency pattern. A further development is to arrange for someone else to host the NAS or RAID. This enables access from multiple devices in multiple locations, and delegates the device management to a specialist organisation, but it means that all of the individual's platforms become slaves to the server operated by the outsourced service-provider, and it brings with it a heavy dependency on reliable telecommunications links. Care is still needed to deal with the risks of multiple, inconsistent copies of files. Additional data risks arise in the forms of exposure to second-party access (i.e. by the service-provider), and of more circumstances in which third-party access to or corruption of the data may occur, in particular because of the increased extent of file-transmission over external networks, and the greater attractiveness of service-providers to hackers (the 'honeypot effect').

A master-slave arrangement may be easier for a small organisation to understand and manage, whereas storing the primary copy on a NAS or RAID1 device requires additional understanding and infrastructure. The use of a remote file-hosting service requires further understanding, may increase costs, and creates a dependency on a provider, but if the service is well-designed and communicated, reliable and cost-effective, it can relieve the user of a considerable amount of effort.

The choice of file-synchronisation approach influences the decision as to which pattern to use for backups. This leads to the following further articulation of the first three patterns outlined in Table 1:

1. **Self-Sufficiency**
   The Primary copy is held locally.
   File-synchronisation is achieved using master-slave arrangements, or local NAS or RAID.
   Backups are managed locally.
   Because both the Primary and the First-Level Backup are subject to similar threats and vulnerabilities, it is essential that a Second-Level Backup (popularly referred to as 'fire backup'), be established at a remote location.
2. **Backup Service**
   The Primary copy is held locally.
   File-synchronisation is achieved using master-slave arrangements, or local NAS or RAID.
   Backups use a service provided by another party.

The Primary and First-Level Backup copies are in different places, and hence a Second-Level Backup might be considered superfluous. On the other hand, additional risks arise, such as the service-provider defaulting on their undertakings.
Hence a Second-Level Backup, in particular one stored locally, remains highly advisable.

3. **File-Hosting Service**
The Primary copy is held remotely.
File-synchronisation is achieved by means of the remote server.
The supplier may offer a backup service as part of the arrangements or additionally, in which case reliance might be placed on that backup service. On the other hand, further risks arise, such as service-provider default, and storage of the First-Level Backup co-located with the Primary copy and hence subject to the same threats.
Hence a Second-Level Backup, in particular one stored locally, remains highly advisable.

3 Method and Test-Case

The work reported in this paper adopted the design science approach to research (Hevner et al. 2004, Hevner 2007). In terms of the research method described by Peffers et al. (2007), the research's entry-point is 'problem-centred'. The process commences by applying risk assessment techniques in order to develop an articulated definition of the problem and of the objectives. An artefact is then designed – in this case a set of backup plans applicable to three patterns of IT use. In terms of Hevner (2007), the article's important contributions are to the requirements phase of the Relevance Cycle, and the Design Cycle, drawing on existing theory in the areas of risk assessment, data management, and data security. The paper makes more modest contributions to the evaluation phase of the Relevance Cycle, but lays firm foundations for application and field testing.

In this section, the existing literature is applied in order to define terms and specify a risk assessment process to support the analysis. Within the scope declared above, a target-segment is defined that is both realistic and sufficiently rich to provide both a test of the method and an outcome that is useful in its own right. The risk assessment process is then applied to the test-case, to produce a sufficiently deep understanding of the needs of that category of users. Practicable backup plans are presented, for each of the three patterns of IT use.

The assessment of risk, and the development of guidance for backups, needed to be based on a model of security, including a set of terms with sufficiently clear definitions. A substantial literature provides the framework for the analysis. This includes OECD (2002), Firesmith (2004), ISO 27002:2005, IETF (2007), CC (2012, pp. 38-39) and Clarke (2015). Appendix 1 provides a depiction of the conventional computer security model, and a glossary of terms. A brief summary of the model is that:

- threatening events impinge on vulnerabilities, resulting in security incidents that may give rise to harm to assets
- safeguards provide protections against threatening events, vulnerabilities and harm; and
- security is a condition in which harm is in part prevented, and in part mitigated, because adequate safeguards are in place

A suitable backup and recovery plan can only be established if alternative designs are outlined and compared with a set of requirements. A process is needed, comprising a series of steps that apply the conventional security model in order to unfold an understanding of the needs of the entities within the project's scope.

The refereed literature provides references on the discipline and practice of risk assessment and risk management, with particular reference to ISO 27001:2005, NIST (2012), IASME (2013), Clarke (2013) and Clarke (2015). There are, however, relatively few sources that formally articulate risk assessment and risk management processes in particular contexts relevant to the present analysis. An exception is Shedden et al. (2011), which provides a case

study of a complex data backup process. The above literature was drawn on in order to establish the process declared in Table 2. Its purpose is to avoid subtleties and complexities in order to scale the process to the contexts of the target organisations and individuals. The test-case excludes individuals likely to be subject to targeted attacks, so the analysis pays little attention to countermeasures that may be adopted by attackers to circumvent the individual's safeguards.

In principle, this process needs to be applied to the specific context facing a particular organisation or individual. In practice, most of the intended clientele would still find the process far too demanding. A practical compromise is to define a small set of client segments, apply the process to each of these segments, test the resulting recommendations in the field, and publish the outcomes to organisations and individuals in those segments.

Stratification of the broad domains of organisations and individual users could be performed in a variety of ways. Industry sectors have varying needs, and hence analyses could be undertaken for a garden designer, a ceramic artist, a technical writer, a structural engineer, a motor vehicle repairer, a marriage-celebrant, a genealogist, and a cause-based advocate. However, many of these have similar assets and values, face similar threats, are afflicted with similar vulnerabilities, and trade off various factors in similar ways. It therefore appears feasible to define a smaller number of categories than would arise with a sector-based analysis, by focussing on the nature and intensity of the risks that the client faces.

Analyse
1. Define the Objectives and Constraints
2. Identify the relevant Stakeholders, Assets, Values and categories of Harm
3. Analyse Threats and Vulnerabilities
4. Identify existing Safeguards
5. Identify and Prioritise the Residual Risks
Design
1. Identify alternative Backup and Recovery Designs
2. Evaluate the alternatives against the Objectives and Constraints
3. Select a Design (or adapt / refine to achieve an acceptable Design)
Do
1. Plan the implementation
2. Implement
3. Review the implementation

Table 2: The Process

This paper presents a single such test-case. The criteria used in devising it were:

- simplicity, in order to keep the scale of the work and its presentation within bounds
- representative value, i.e. including a moderate proportion of the elements that arise in more complex cases, such that it can reasonably be used as a proxy for prosumers more generally, and for micro-organisations; and
- familiarity to the author, in order to take advantage of existing knowledge and obviate the need for field-work during this phase of the project

The selected case is a person who is a moderately sophisticated user of computing devices, but has limited professional expertise in information technology matters. They use their

computing devices for personal activities and/or in support of one or more organisations. The functions performed are primarily:

- preparation and amendment of documents
- maintenance of data-sets and databases in a variety of formats, including text, structured data, image, sound and video
- exchange of communications with other people
- access to web-sites
- maintenance of their own web-sites
- the use of Internet Banking and eCommerce, but only as a purchaser, not as a merchant

The person operates out of a home-office that is equipped with a desktop device. When travelling, the person carries a portable / laptop / clam-shell device. The person has a handheld device, and uses this to access messages and send messages using a variety of channels (voice, SMS, email, IM), and to access web-sites. The laptop and handheld device may also be used within the home-office.

The person copies files between the desktop and the other devices as needed. Many of the files that the person creates are sent to other people, so if a file is accidentally deleted or damaged, it may be possible to rescue a copy from somewhere else. But the person has experienced several instances in which important files were simply lost, and needs to avoid that happening.

Use of services offered by third parties (Internet Service Providers, ISPs) is within-scope for such mainstream activities as the hosting of email and web-sites. Use of cloud computing, on the other hand, has been excluded from the case, because of the many additional factors this gives rise to. For example, the person might use cloud services for messaging, for storage of the primary copies of photographs, for storage of their address-book and appointments diary, for their log of past dealings with each contact in their address-book, or for their accounting records. Analyses of the risks involved in consumer uses of cloud computing, and approaches to dealing with them, are in Clarke (2011, 2013, 2016).

The test-case excludes circumstances in which the individual is likely to be a specific target for attackers, as distinct from being just another entity subjected to random unguided attacks by malware and social engineering techniques. Hence the trade-offs selected during this analysis are not appropriate to, for example, private detectives, and social and political activists who are likely to be directly targeted by opponents and by government agencies.

4 Application of the Process to the Test Case

This section applies the process outlined in Table 2 to the test-case defined immediately above. The discussion in the sections below reflects relevant sources on risk assessment and risk management. References are not cited in a single, consolidated exposition of existing theory. It is more appropriate to the progressive analysis presented in this paper to provide references in the particular sections to which they make contributions.

4.1 Analysis

This section follows the steps specified in the first segment of Table 2.

4.1.1 Objectives and Constraints

As a reference-point, the following definition is proposed of the individual's purpose and the constraints within which the design needs to work (Clarke 2015):

> *To avoid, prevent or minimise harm arising from environmental incidents, attacks and accidents, avoiding harm where practicable, and coping with harm when it arises, by balancing the reasonably predictable financial costs and other disbenefits*

> *of safeguards against the less predictable and contingent financial costs and other disbenefits arising from security incidents*

On the other hand, the target audience needs a simpler formulation, such as:

> *To achieve reasonable levels of security for reasonable cost*

4.1.2 Stakeholders, Assets, Value, Harm

Literature searches found no refereed sources or Standards documents that articulate the process of stakeholder analysis. In the case of an individual, the stakeholders comprise the individual themselves, the individual's family, any employees and sub-contractors, and any clients, whether of an economic or a social nature. In the case of micro-organisations, there may be additional stakeholders, such as employees, customers, suppliers, and perhaps an advisory committee. Also within-scope are some categories of associations with membership and committee structures and small, multi-member enterprises such as investment clubs. In some contexts, regulatory agencies may loom at the level of stakeholder, e.g. for accountants, financial planners, marriage celebrants and health care professionals.

The assets on which this study is focussed are data. A useful resource in this area is ISO 27005 (2012, Annex B). IT equipment and services on which the individual depends are only within-scope to the extent that they play a role in the protection of data assets. Relevant categories of assets are listed in Table 3.

- **Business-Related Content**
  such as databases, transaction files, reports, work-in-progress, sources of data and information, customer information, details of outstanding debts
- **Financial Data** – such as records of assets and transactions, insurance details
- **Payment Authenticators** – such as PINs, credit-card details
- **Identity Authenticators** – such as passwords, passport, driver's licence details
- **Funds** – such as bitcoin wallets
- **Personal Data**, in some cases of a sensitive nature:
  - of an individual – e.g. diaries, address-books, music collections, health-related data
  - of the individual's family – e.g. family albums, family history, tax return data
  - of other people – e.g. if the individual performs counselling, mentoring or coaching
- **Infrastructure Configuration Data**
  such as settings, parameters and scripts that support computing operations

Table 3: Relevant Data Assets

The values that stakeholders attribute to Assets derive from a variety of sources (Clarke 2013), in particular:

- **Intrinsic Value**, as arises from debtors ledgers, share registers and bitcoins
- **Operational Value**, as arises from the data's usefulness in performing a function, such as publishing images and scheduling meetings
- **Competitive Value**, as arises both from the data's usefulness to the individual and its potential usefulness to other parties, including economic competitors and strategic competitors
- **Reputational Value**, as arises from the data's capacity to influence the perceptions that other parties have of the individual or of some other party
- **Compliance Value**, as arises from obligations, e.g. in relation to the protection of the data

- **Psychic Value**, as arises from personal associations, particularly with image, video and music collections, and family trees
- **Privacy Value**, as arises from the concerns of a person to whom data relates (particularly health and financial data), whether or not the concerns are rational, and whether the value is associated with economic, social, psychological, political, religious or philosophical factors

Values associated with data involve a considerable set of attributes referred to in the literature using various terms, such as 'properties'. One concept of long standing is the 'CIA' list, which stands for Confidentiality, Integrity and Availability (Saltzer & Schroeder 1975). This convention is much-criticised, and many alternatives and adjuncts have been offered. For example, Parker (1998) added Possession, Authenticity and Utility; and Cherdantseva & Hilton (2013) add instead Accountability, Auditability, Authenticity, Trustworthiness, Non-repudiation and Privacy.

However, such lists lack clarity because they confound properties of data with properties of the infrastructure used to achieve access to the data. Particularly for such purposes as backup and recovery strategies, the following areas are only indirectly relevant:

- the availability of infrastructure, including computing and networking hardware and systems software
- the availability of services, including application software, data and supporting services, whether it is full availability, degraded availability (as occurs with a business continuity plan that involves fallback arrangements), or complete unavailability (during interruptions to communications and while disaster recovery procedures are being undertaken)
- the integrity of services
- the robustness of services, i.e. their ability to withstand shocks
- the resilience of services, i.e. their ability to quickly recover and resume service, following shocks

This analysis is concerned specifically with the value attached by stakeholders to data. It accordingly applies the set of factors in Table 4. The primary three values encompass the relevant aspects of the lists referred to in the previous paragraph, but separate out the confusing effects of multiple purposes. The third value is then disaggregrated into its constituents. This reflects sources on data quality and integrity in the information systems and related literatures, including OECD (1980), Huh et al. (1990), van der Pijl (1994), Clarke (1995, pp. 601-605), Wang & Strong (1996), Müller & Freytag (2003, pp. 8-10), English (2006), Piprani & Ernst (2008) and the ISO 8000 series emergent since 2009.

Harm to values in data needs to be considered at two levels. A useful resource in this area is ISO 27005 (2012, Annex B, pp. 39-40). Categories of harm to data itself are listed in Table 5, and the forms of consequential harm to stakeholders' values are listed in Table 6.

- **Accessibility**
  The data is accessible to appropriate entities in appropriate circumstances
- **Inaccessibility**
  The date is otherwise not accessible
- **Quality**
  The data adequately satisfies all dimensions of data integrity:
  - **Accuracy**
    The degree of correspondence of the data with the real-world phenomenon that it is intended to represent, typically measured by a confidence interval, such as 'accurate to within 1 degree Celsius'
  - **Precision**
    The level of detail at which the data is captured, reflecting the domain on which valid contents for that data-item are defined, such as 'whole numbers of degrees Celsius'
  - **Timeliness**, which comprises distinct elements:
    - **Currency**
      The absence of a material lag between a real-world occurrence and the recording of the corresponding data
    - **Temporal Applicability**
      The absence of ambiguity about the date and time when, or the period of time during which, the data represents or represented a real-world phenomenon. This is important in the case of volatile data-items such as total rainfall for the last 12 months, marital status, fitness for work, age, and the period during which an income-figure was earned or a licence was applicable
- **Completeness**
  The availability of sufficient contextual information that the data is not liable to be misinterpreted. Of particular concern are provenance, and the data's syntax and semantics

Table 4: Relevant Values Associated with Data

- **Accessibility**
  The data is not accessible to appropriate entities in appropriate circumstances
    - Data Loss
        - Data in volatile memory is dependent on continuous functioning of the CPU and electrical power
        - Data in non-volatile memory is at risk of being over-written, in many cases at file-level and in some cases at record-level within databases
        - Data storage-media and data storage-devices containing storage-media are subject to theft, destruction and malfunction
    - Data Unavailability at a relevant time, e.g. due to shortfalls in infrastructure performance
- **Inaccessibility**
  The data is otherwise accessible. This takes several forms:
    - Data Access, whereby data in storage is accessed by an inappropriate person, or for an inappropriate purpose
    - Data Disclosure, whereby data in storage is communicated to an inappropriate person, or for an inappropriate purpose
    - Data Interception, whereby data in transit is accessed by an inappropriate person, or for an inappropriate purpose
- **Quality**
  The data does not adequately satisfy all dimensions of data integrity:
    - Data Quality is low at the time of collection
    - Data Quality is low at the time of use, due to Data Modification or Loss of Data Integrity
- **Completeness**
  The data does not adequately satisfy the requirement, in particular the availability of the data's provenance and the definitions of the data's syntax and semantics

Table 5: Harm to Values Associated with Data

• **Reduced Asset Value** e.g. loss of a debtors ledger or prospects database with intrinsic value
• **Degraded Operational Capacity** Tasks cannot be performed
• **Degraded Service Quality** Tasks cannot be performed well
• **Reduced Revenue or Amenity** (depending on whether the purpose is economic or social)
• **Cost, Time, Effort and Economic Loss Incurred during Recovery** incl. the acquisition of backup data, the performance of recovery procedures, transport and communications, and the replacement of payment or identity authenticators
• **Damaged Reputation** incl. the confidence of family, employees, customers, investors or regulators
• **Negative Privacy Impact on Individuals** e.g. through unauthorised access to personal data, or disclosure or interception of personal data
• **Non-Compliance with Obligations or Commitments** e.g. through loss of tax records

Table 6: Harm to Stakeholder Values Arising from Harm to Values Associated with Data

4.1.3 Threats and Vulnerabilities

This section follows convention by identifying lists of threats and of vulnerabilities, although the distinctions can be challenging to make, and hence it is often more practicable to consider threat-vulnerability combinations. Catalogues of threats and vulnerabilities are available from a variety of sources, most usefully ISO 27005 (2012, pp. 42-49) and NIST (2012, pp. 65-76). These are reflected in Table 7 and Table 8. All elements within these Tables can of course be analysed in greater detail. For example, a deeper treatment of malware is in Clarke (2009), and of social engineering in Mitnick & Simon (2003).

A means is needed to invoke the range of Threats but in a simplified form that is easier for the target-audience to grasp and to remember. A convenient approach is to adopt a single instance of each category of Threats as being representative of the category, and to contrive the first letter of each to build a word. One such mnemonic is 'FATE':

F - Fire (for Environmental Events)

A - Attack

T - Training (for Accidents caused by Humans)

E - Equipment (for Accidents within Infrastructure)

The term 'FATE' is in no sense a theoretical construct. Its purpose is merely to provide prosumers and people in micro-organisations with a readily-remembered basis for imposing a degree of organisation on the wide variety of threats that may result in harm to their interests.

4.1.4 Existing Safeguards

Before conclusions can be reached about what risks need to be addressed, it is necessary to take into account factors that already exist and that intentionally or incidentally mitigate risks. Common patterns of human behaviour such as habit, caution and loyalty have the effect of protecting stakeholders' interests, and can be reinforced through training and reminders. Longstanding practices in relation to physical security help as well, such as locks and smoke

alarms. Aspects of infrastructure assist, such as those resulting from contractual terms and 'fitness for use' conditions imposed by the laws of contract and consumer rights. Suppliers have a self-interest in delivering goods and services of reasonable quality, in order to sustain their reputation. Logical security precautions are widely used, particularly in the form of accounting controls. Insurance provides monetary recompense for financial losses, but also imposes requirements for some level of safeguards to be established and maintained.

Environmental Event

- Electrical Event (interruption, surge)
- **F**ire Event
- Water Event
- Impact Event

Attack

- On Data Storage
  - Sabotage
  - Theft
  - Seizure
- On Traffic
  - Interception
- On a Business Process
  - Abuse of Privilege, e.g. unauthorised disclosure by an insider
  - Masquerade, e.g. access by adopting an authorised identity
  - Social Engineering
- On a Computer-Based Process
  - 'Hacking' / Cracking
  - Malware, incl. Ransomware

Accident, i.e. Unintentional Error

- **By A Human**
  - Business Process Design Error
  - Inadequate **T**raining in a Business Process
  - Business Process Performance Error
- **Within Infrastructure**
  - **E**quipment Failure (Processor, Storage Device, Infrastructure, Power)
  - Storage-Medium Failure
  - Network Malfunction
  - Data Incompatibility

Table 7: Threats to Data

Infrastructural Vulnerabilities

- Dependence on the availability, reliability and integrity of:
    - **Power Supply**, subject to the Threats of blackouts, brownouts, voltage variability, UPS failure
    - **Computing Facilities**, subject to the Threats of planned and unplanned downtime, unavailability of a storage-device that can read a particular storage-medium, seizure powers
    - **Networking Facilities**, subject to the Threats of outages, congestion, DOS attack
    - **Storage-Media**, subject to the Threats of disk crash, corruption, encryption/hostage/ransom, loss, online accessibility of live and backup data at the same time, seizure powers, unreadability due to humidity, dust, magnetic disturbance, corrosion, etc.
    - **Ancillary Services**, e.g. air-conditioning, fire equipment, subject to the Threats of outages and malfunctions
    - **Automated Processes**, subject to the Threats of design and coding errors, malware, wrong versions of software or data, erroneous recovery of software or data, overwrite of valid backups with corrupted backups
- Dependence on the effectiveness of **Access Controls** over:
    - Authenticators
    - Software Execution
    - Remote Access
    - Message Transmission
    - Encryption and Decryption

Human Vulnerabilities

- Dependence on the availability, reliability and integrity of individuals, subject to the Threats of:
    - Inadequate **Performance**
    - Inadequate **Training**
    - Inadequate **Loyalty**
    - Insufficient **Wariness and Scepticism**

Table 8: Data Vulnerabilities

4.1.5 Residual Risks

The final step in the assessment process is the identification and prioritisation of the 'residual risks', i.e. those that are not satisfactorily addressed by existing safeguards. The conventional approach to prioritisation is to assign to each residual risk a severity rating and a probability rating, and to then sort the residual risks into descending order, showing extreme ratings in either category first, followed by high ratings in both, etc. This is most comprehensively presented in NIST (2012, Appendices G, H and I). In principle, these are context-specific judgements that need to be made by the responsible individual, or by someone closely familiar with the individual's needs and circumstances. The analysis conducted here, however, assigns severity and probability ratings on the basis of the test-case described earlier. The results are summarised in Table 9.

Risk	Severity Rating (E, H, M, L)	Probability Rating (H, M, L)
Storage-Media Failure denying access to all files	Extreme	High
Environmental Event, Destruction, Theft or Seizure denying access to the Storage-Medium	Extreme	Medium
Malware or Hacking Attack denying access to all of the data	Extreme	Medium
Malware or Hacking Attack resulting in inability to access a file	High	Medium
Mistaken Amendment, Deletion or Overwriting of a file	High	Medium
Individual File-corruption: • discovered within-cycle • discovered after more backups have been run	 High High	 Medium Medium
Environmental Event resulting in inability to access a file	High	Medium
Software Error resulting in inability to access a file	High	Medium
Unavailability of Networking Facilities resulting in inability to access a file	Medium	Medium
Technological Change causing a Storage-Medium to be unreadable	Low	Low

Table 9: Priority Threat-Vulnerability Combinations

4.2 Design and Implementation

This section applies the remaining steps defined in Table 2. A range of alternative approaches to backups exists. Drawing on the literature, most usefully Chervenak et al. (1998), plus Lennon (2001), Gallagher (2002), Preston (2007), de Guise (2008), Strom (2010), TOB (2012) and Cole (2013), Appendix 2 identifies relevant characteristics of backup data, and of backup processes, and Appendix 3 describes each of the various categories of backup procedure.

Key considerations in designing a backup regime include the frequency with which full backups are performed, whether incremental backups are performed and if so how frequently, whether copies are kept online or offline, and whether second-level archives are kept and if so whether they are later over-written or archived. One of the most critical choices, however, is whether the first-level backup is stored locally or remotely.

In Appendix 4, a summary is provided of the extent to which different backup techniques address the various risks that afflict both individual files and the primary storage-medium as a whole.

The information generated by the preceding sections enables a judgement to be made about what combination of approaches to platform-management and backups is most appropriate. A scheme that would cover every possible eventuality is highly likely to be too complex and too costly for a micro-organisation or a prosumer. Important factors that need to be considered are identified in Table 10. Commonly, cost and complexity, on the one hand, are traded off against protections against the lower-priority Threat-Vulnerability Combinations.

An individual or small organisation may be able to directly utilise the outcomes from a generic analysis and design process such as that presented above. The responsibility for converting a risk management strategy to a reality, on the other hand, rests on the individual or organisation concerned. Broadly, the following steps are necessary:

- **Plan the implementation**
  Establish policy, procedures, controls and training
- **Implement the Plan**
  Rehearse the procedures, run the procedures, check the results
- **Review the implementation**
  Reconsider the procedures and outcomes after 1 month and 6 months

The discussion of analysis, design and implementation in this section has been framed in a sufficiently general manner that individuals and small organisations confronted by a wide variety of circumstances could apply it. The following section presents the outcome applicable to the test-case defined earlier in the paper.

Risk Management
• The Risks that are safeguarded against
Equipment
• Operational Storage Size
• Backup Storage Size
• Processor, Bus and Local Network Capacity
• External Network Connection and Capacity
Operation
• Batch Backup Run-Times
• (and consequential service unavailability or qualified availability)
• Recovery Run-Time
• Speed of Recovery from a Security Incident
• Complexity of strategy, plan, policies and procedures
• Concentration and Effort needed to implement the plan
Cost
• One-Time Costs of Safeguards
• Recurrent Costs of Safeguards
• Costs of each kind of Security Incident

Table 10: Factors to be Traded Off

5 Practicable Backup Plans

In Table 1, three patterns of use were distinguished. This section applies the assessment conducted above to each of those three patterns. It presents three Backup Plans that address all of the high-priority threat-vulnerability combinations identified in Table 9, and do so in a manner that is not unduly complex or expensive.

5.1 Self-Sufficiency

The first Backup Plan applies to circumstances in which the storage-medium on which the backup is stored is on the premises, and hence co-located with the primary copy. This may be by direct connection to the master-device, typically the desktop, or over a local area network. A review of Wintel-oriented backup software is in Mendelson & Muchmore (2013), and another for Mac OSX environments is in Preece (2016). Examples of products that satisfy a significant

proportion of the requirements are Acronis (Wintel, Mac and Linux) and Chronosynch (Mac only).

To address on-site risks (typified earlier as FATE – Fire, Attack, Training and Equipment), it is necessary that a second-level backup be maintained at a sufficiently remote location.

This Backup Plan is outlined in the first column of Table 11. Because the test-case encompasses some diversity of needs, a list of essential elements is provided, supplemented by a further set of recommended actions. The actions are further sub-divided into Infrastructure Features, File-Precautions, Backup Runs and Business Processes. Full detail of the Plan is provided in Appendix 5, in a form designed as a checklist for micro-organisations and prosumers who want to apply the technique.

5.2 Use of a Backup Service

The second Backup Plan is for circumstances in which the storage-medium to which the backup is performed is located remotely from the primary copy, and the transfer occurs over an Internet connection. It is desirable to authenticate the remote device and to use channel encryption. The process can be driven either by a device on the local network – typically the desktop – or by the remote device that has direct access to the backup storage-medium.

This Backup Plan is outlined in the second column of Table 11. Full detail of the Plan is provided in Appendix 6, in a form designed as a checklist for micro-organisations and prosumers who want to apply the technique.

The Plans outlined in Table 11 for the Self-Sufficiency and Backup Service patterns are substantially the same. The small, but critical, differences are the logistical arrangements for First-Level and Second-Level Backups, and safeguards for the content of the remote backup.

The remote backup device may be hosted by someone the individual or organisation has associations with (e.g. a business colleague or a relative). Alternatively, the hosting may be performed by a service-provider, such as an accountant, a local provider of Internet services, a specialist backup provider, or a cloud operator. A commercial catalogue of offerings is in Muchmore (2013). A service that appears to score well on many aspects of the requirements is SpiderOak. It is also possible to use major service-providers as a Backup Service. Evaluating their offerings against these requirements is difficult, however, because reliable information may be difficult to find. For example, postings in Mac user fora make clear that Apple's Time Machine offering is unclear to many users.

Elements of the Backup Plan	L	R
ESSENTIAL		
Infrastructure Features		
A. Install power-surge protection and an 'uninterruptible' power supply with battery backup (UPS)	Y	Y
B. Use the desktop as master, and the laptop and handheld as slaves OR Maintain the primary-copy on networked attached storage (NAS)	Y	Y
File Precautions		
C. When creating and amending files, perform continual saves	Y	Y
D. When making significant amendments, first create a new file-version	Y	Y
E. Run malware detection and eradication software		
a. on each storage-device at the time it is connected to any working-device	Y	Y
b. on all incoming files arriving via email, fetches using a web-browser, etc.		
Backup Runs		
F. a. Perform 3-monthly Full Backup to a separate local storage-medium	Y	Y
b. Perform daily Incremental Backup to the same storage-medium	Y	Y
G. a. Perform weekly, fortnightly or monthly Full Backup to a rotating set of 2, 3 or 4 storage-media, as Second-Level Backup	Y	Y
b. Promptly transport Second-Level Backup storage-media to a remote location	Y	-
c. Store the Second-Level Backup storage-media locally	-	Y
d. Store the Second-Level Backup storage-media offline	Y	Y
e. Fetch the relevant Second-Level Backup storage-media shortly before each Backup Run	Y	-
H. a. Annually, and after each significant upgrade to software, perform a complete Disk-Image Backup of all working-devices , including all software and parameter-files	Y	Y
b. Store the resulting Disk-Images remotely and offline	Y	Y
Business Processes		
I. Document and periodically rehearse backup procedures	Y	Y
J. Document and periodically rehearse recovery procedures	Y	Y
RECOMMENDED		
Infrastructure Features – Additional Measures		
K. Implement a Virtual Private Network (VPN) connection from laptop and handheld back to the local network	Y	Y
File Precautions – Additional Measures		
L. Weekly, run malware detection and eradication software on all stored files	Y	Y
Backup Runs – Additional Measures		
M. Ensure that: • the remote online First-Level Backup is encrypted • the decryption key is stored locally • the decryption key is not accessible by the service-provider	-	Y
N. a. Half-yearly, retire a Full Backup to Archive	Y	Y
b. Store successive Archive copies locally and remotely, and possibly also on a third site	Y	Y
O. Annually, spool 3-year-old Archives to new media	Y	Y
P. 5-Yearly, spool all Archives to a new media-type	Y	Y

Table 11: Backup Plans Using Local (L) and Remote (R) Backup

5.3 Dependence on a File-Hosting Service

The third Backup Plan applies where the Primary copy of the files is held by another party. This has some similarities to the use of a Backup Service, addressed in the previous section.

Key differences are, however, that the use of a Backup Service, by its nature:

- ensures that two copies exist – because the backup is in addition to the Primary copy; and
- maintains physical separation between the local Primary copy and the remote First-Level Backup.

In the case of a File-Hosting service, on the other hand:

- there may or may not be a backup copy; and
- any backup copy may or may not be subject to the same risks as the primary copy – and will be if they are in the same location or both are accessible online.

This Backup Plan is outlined in Table 12. Full detail of the Plan is provided in Appendix 7, in fuller form, as a checklist for micro-organisations and prosumers who want to apply the technique.

Much of the Plan in Table 12 is the same as that for the Self-Sufficiency and Backup Service patterns. The differences are as follows:

- because the location of the Primary copy is different, the technique for achieving appropriate synchronisation among multiple copies is different
- malware-checking needs to be performed within the File-Hosting services site on incoming files;
- the daily (or more frequent) First-Level Backup run is a responsibility of the File-Hosting service;
- the daily (or more frequent) Second-Level Backup run is a responsibility of the File-Hosting service;
- malware-checking needs to be performed within the File-Hosting services site on stored files;
- the Primary copy of the data at the File-Hosting service should be encrypted;
- at least one recent backup should be in the possession of the individual or organisation.

File-Hosting services have gone through several generations. Initially services were offered by Internet Access Providers, as a form of value-add. Then came consumer-oriented products typified by DropBox (since c. 2007). A further round has been cloud-based services, typified by Apple iCloud (since 2011) and Google Drive (since 2012). Some are primarily outsourced data-storage services. Others focus on providing their customers with access to their files from multiple devices and from any location, and are sometimes described as 'file-synchronisation' services. Others are primarily to enable files to be provided by one user and made available to others. Yet others are intended to support documents developed collaboratively by multiple people. Some support files generally, and are agnostic about what formats the files are in. Some, however, may use proprietary file-formats, a feature which is hostile to the purpose considered here.

ESSENTIAL

Infrastructure Features

1. Install power-surge protection and an 'uninterruptible' power supply with battery backup (UPS)
2. a. Store the Primary copies of all files with a File-Hosting service
   b. Process the data using software on the desktop, laptop and handheld, working on local copies for as long as needed
   c. Synchronise the copies of files on the individual's devices to the remote Primary copy whenever each device has a suitable connection to the File-Hosting service

File-Precautions

3. When creating and amending files, perform continual saves
4. When making significant amendments, first create a new file-version
5. Run malware detection and eradication software
   a. on each storage-device at the time it is connected to any working-device
   b. on all incoming files arriving via email, fetches using a web-browser, etc.
6. Ensure that the File-Hosting service runs malware detection and eradication software on all incoming files

Backup Runs

7. Ensure that the File-Hosting service maintains a Full Backup to a separate storage-medium no less frequently than daily
8. a. Ensure that weekly, fortnightly or monthly Full Backup is performed by the File-Hosting service to a rotating set of 2, 3 or 4 storage-media, as Second-Level Backup
   b. Ensure the Second-Level Backup storage-media are stored at a different location from the First-Level Backup
   c. Ensure that the Second-Level Backup storage-media are stored offline
9. a. Annually, and after each significant upgrade to software, perform a complete Disk-Image Backup of all working-devices , including all software and parameter-files
   b. Store the resulting Disk-Images remotely and offline

Business Processes

10. Document and periodically rehearse backup procedures
11. Document and periodically rehearse recovery procedures

RECOMMENDED

Infrastructure Features – Additional Measures

1. Implement a VPN connection from all of the individual's devices to the service-provider

File-Precautions – Additional Measures

2. Weekly, run malware detection and eradication software on all locally stored files
3. Ensure that the service-provider runs weekly malware detection and eradication software on all stored files

Backup Runs – Additional Measures

4. Ensure that:

- the Primary copy of the data stored at the File-Hosting service is encrypted
- the decryption key is not accessible by the File-Hosting service
- the decryption key is stored locally

5. a. Perform a monthly or quarterly Full Backup of all working-devices to a separate local storage-medium

   OR

   b. Ensure that an equivalent arrangement is in place using a SaaS Data Escrow service or Backup as a Service (BaaS)
6. a. Ensure that, half-yearly, the File-Hosting service retires a Full Backup to Archive
   b. Ensure that the File-Hosting service stores successive Archive copies locally and remotely
7. Ensure that the File-Hosting service, annually, spools 3-year-old Archives to new media
8. Ensure that the File-Hosting service, 5-yearly, spools all Archives to a new media-type

Table 12: Backup Plan Using File-Hosting Services

It is a matter of serious concern that large corporations that offer File-Hosting Services generally make very little information available, which makes it very difficult to perform a satisfactory evaluation against the requirements expressed in Table 12. Even large organisations generally have far less market power than Apple, Microsoft and Google, and hence small organisations and prosumers that value their data, and that use File-Hosting Services provided by such corporations, are subject to unmanaged risk exposures.

6 Conclusions

This paper has presented an analysis of the backup requirements of micro-organisations and prosumers. It has focussed on a test-case, in order to not merely provide general guidance, but also deliver a specification that fulfils the declared objective of developing "guidance on how small organisations and individuals can use backup techniques to address data risks", which balances among multiple, inherently conflicting needs.

The Peffers et al. (2007) research method was applied, commencing with 'problem-centred initiation', through the problem definition, objectives formulation and articulation phases, and into the design phase, resulting in three sets of specifications. Tables 3–9, which declare Assets, forms of Harm, Data Threats, Vulnerabilities and Priority Threat-Vulnerability Combinations, all represent templates or exemplars that can be applied to similar studies of somewhat different contexts. The research has contributed to IS theory in the areas of data management and data security, in particular by articulating risk assessment and risk management procedures.

The project's contributions in relation to the evaluation phase are less substantial. A limited evaluation has been conducted of one of the three Backup Plans. The author's profile has a reasonably close correspondence with the test-case defined in Table 2. In addition, the processes applied by the author for the last decade have been very similar to that derived for the Self-Sufficiency pattern in column 1 of Table 11 and Appendix 5. The backup procedures have been exercised hundreds of times, and the recovery procedures on a modest number of occasions. The author has suffered very few losses of datafiles. The rare exceptions are of two kinds. A few very old files have been discovered to be corrupted (by runs of disk utility software) only after all still-readable backups were similarly corrupted. A somewhat larger number of files (from the period 1984-1992) are no longer accessible because no device is available that can read the storage-medium and/or because no application software is available that can read the data-format. A review of the procedures in light of the analysis reported here highlighted the need for refinements to the author's procedures, and for more assiduous application of them, particularly relating to the periodic rehearsal of recovery processes, and the migration of copies forward from obsolescent to contemporary storage-media. Further, the ease with which the Self-Sufficiency Backup Plan could be applied the author's circumstances represents a useful, if weak, form of evaluation of the Plan's ease of application to the target-segment's needs.

The research has laid a firm foundation for IS professionals to better address the needs of micro-organisations and prosumers. The specific Backup Plans proposed above can be used as a basis for evaluating the capabilities of software products that support local backup management, and for evaluating backup services offered by ISPs. They, and variants of and successors to them, are capable of being productised by providers. These include corporations that sell hardware, that sell operating systems, that sell pre-configured hardware and software, that sell value-added hardware and software installations, that sell storage-devices, and that sell storage services. A further opportunity is for guidance based on the Plans to be distributed by industry associations, user associations and clubs, to assist those organisations' members.

In order for the outcomes to be exploited, it is necessary for the analysis to be subjected to review by peers, and the feedback reflected in the three Plans through the publication of revised versions. The analysis may require adaptation, at least of terminology, in order to be readily applied to specific contexts, in particular the many variants of Microsoft Windows, Apple OSX and iOS, and Linux and Android operating environments, and particularly where the

individual uses multiple such platforms. The analysis needs to be applied to additional test-cases, reflecting the needs of small organisations and individuals whose characteristics are materially different from those addressed by this paper.

Beyond analytical review, the three specific Backup Plans derived from the analysis need to be applied, and their effectiveness and practicality evaluated empirically. The analysis also needs to be applied in circumstances in which the individual accepts (but manages) the additional risks involved in relying entirely on networks and remote services – with all the uncertainties of format-compatibility and geographical and jurisdictional location that the cloud entails. Those circumstances are addressed in a companion paper (Clarke 2016). Both analyses may require further adaptation if and when the target market-segments' usage of general-purpose computing devices (such as desktops and laptops) declines, and datafile creation and amendment comes to be undertaken almost entirely on locked-down appliances (such as smartphones and handheld devices).

As individuals increasingly act as prosumers, they become more demanding, and more aware of the benefits of effective but practical backup arrangements. Meanwhile, many large organisations are becoming concerned about importing subcontractors' security risks. They can be expected to bring pressure to bear on small organisations and individuals to demonstrate the appropriateness of their backup plans, and to provide warranties and indemnities in relation to them. The work reported here accordingly lays a foundation for significant improvements in key aspects of the data security not only of individuals and small organisations, but also of the larger organisations that depend on them.

References

Armbrust M., Fox A., Griffith R., Joseph A.D., Katz R., Konwinski A., Lee H., Patterson D., Rabkin A., Stoica I. & Zaharia M. (2009) 'Above the Clouds: A Berkeley View of Cloud Computing' Technical Report No. UCB/EECS-2009-28, UC Berkeley Reliable Adaptive Distributed Systems Laboratory, February, 2009, at http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

Boyle R.J. & Panko R.R. (2013) *'Corporate Computer Security'* Pearson, 3rd Ed., 2013

CC (2012) *'Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model'* Common Criteria, CCMB-2012-09-001, Version 3.1, Revision 4, September 2012, at http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

Cherdantseva Y. & Hilton J. (2012) '*A Reference Model of Information Assurance & Security*' Proc. IEEE ARES 2013 SecOnt workshop, 2-6 September, 2013, Regensburg, at http://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf

Chervenak A. L., Vellanki V. & Kurmas Z. (1998) *'Protecting file systems: A survey of backup techniques'* Proc. Joint NASA and IEEE Mass Storage Conference, March 1998, at http://www.storageconference.us/1998/papers/a1-2-CHERVE.pdf

Clarke R. (1995) 'A Normative Regulatory Framework for Computer Matching' *J. of Computer & Info.L.* 13,3 (June 1995), PrePrint at http://www.rogerclarke.com/DV/MatchFrame.html

Clarke R. (2008) 'B2C Distrust Factors in the Prosumer Era' *Invited Keynote, Proc. CollECTeR Iberoamerica*, Madrid, 25-28 June 2008, pp. 1-12, at http://www.rogerclarke.com/EC/Collecter08.html

Clarke R. (2009) *'Categories of Malware'* Xamax Consultancy Pty Ltd, September 2009, at http://www.rogerclarke.com/II/MalCat-0909.html

Clarke R. (2011) 'The Cloudy Future of Consumer Computing' *Proc. 24th Bled eConference*, June 2011, PrePrint at http://www.rogerclarke.com/EC/CCC.html

Clarke R. (2013) 'Data Risks in the Cloud' *Journal of Theoretical and Applied Electronic Commerce Research (JTAER)* 8, 3 (December 2013) 59-73, Preprint at http://www.rogerclarke.com/II/DRC.html

Clarke R. (2015) 'The Prospects of Easier Security for SMEs and Consumers' *Computer Law & Security Review* 31, 4 (August 2015) 538-552, PrePrint at http://www.rogerclarke.com/EC/SSACS.html

Clarke R. (2016) *'Backup and the Cloud: Survival Strategies for Users Dependent on Service-Providers'* Xamax Consultancy Pty Ltd, February 2016, at http://www.rogerclarke.com/EC/PBAR-SP.html

Cole E. (2013) *'Personal Backup and Recovery'* Sans Institute, September 2013, at http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_en.pdf

English L.P. (2006) 'To a High IQ! Information Content Quality: Assessing the Quality of the Information Product' *IDQ Newsletter* 2, 3, July 2006, at http://iaidq.org/publications/doc2/english-2006-07.shtml

Firesmith D. (2004) 'Specifying Reusable Security Requirements' *Journal of Object Technology* 3, 1 (Jan-Feb 2004) 61-75, at http://www.jot.fm/issues/issue_2004_01/column6

Gallagher M.J. (2002) *'Centralized Backups'* SANS Institute, July 2001, at http://www.sans.org/reading-room/whitepapers/backup/centralized-backups-513

de Guise P. (2008) *'Enterprise Systems Backup and Recovery: A Corporate Insurance Policy'* Auerbach, 2008

Hevner A.R. (2007) 'A Three Cycle View of Design Science Research' *Scandinavian Journal of Information Systems*, 2007, 19(2):87-92

Hevner A.R., March S.T. & Park, J. (2004) 'Design research in information systems research' *MIS Quarterly*, 28, 1 (2004), 75–105

Huh Y.U., Keller F.R., Redman T.C. & Watkins A.R. (1990) 'Data Quality' *Information and Software Technology* 32, 8 (1990) 559-565

IASME (2013) *'Information Assurance For Small And Medium Sized Enterprises'* IASME Standard v. 2.3, March 2013, at https://www.iasme.co.uk/images/docs/IASME%20Standard%202.3.pdfhttps://www.iasme.co.uk/images/docs/IASME%20Standard%202.3.pdf

IETF (2007) *'Internet Security Glossary'* Internet Engineering Task Force, RFC 4949, Version 2, August 2007, at https://tools.ietf.org/html/rfc4949

ISO 27005 (2012) *'Information Technology - Security Techniques - Information Security Risk Management'* International Standards Organisation, 2012

Lennon S. (2001) *'Backup Rotations – A Final Defense'* SANS Institute, August 2001, at http://www.sans.org/reading-room/whitepapers/sysadmin/backup-rotations-final-defense-305

Mendelson E. & Muchmore M. (2013) 'The Best Backup Software' *PCMag Australia*, 28 March 2013, at http://au.pcmag.com/backup-products/9607/feature/the-best-backup-software

Mitnick K.D. & Simon W.L. (2003) *'The Art of Deception: Controlling the Human Element of Security'* Wiley, 2003

Muchmore M. (2013) 'Disaster-Proof Your Data with Online Backup' *PCMag Australia*, 30 March 2013, at http://au.pcmag.com/backup-products-1/9603/feature/disaster-proof-your-data-with-online-backup

Müller H. & Freytag J.-C. (2003) *'Problems, Methods and Challenges in Comprehensive Data Cleansing'* Technical Report HUB-IB-164, Humboldt-Universität zu Berlin, Institut für Informatik, 2003, at http://www.informatik.uni-jena.de/dbis/lehre/ss2005/sem_dwh/lit/MuFr03.pdf

NIST (2012) *'Guide for Conducting Risk Assessments'* National Institute of Standards and Technology, Special Publication SP 800-30 Rev. 1, September 2012, at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

OECD (1980) *'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data'* OECD, Paris, 1980

OECD (2002) *'OECD Guidelines for the Security of Information Systems and Networks: Towards A Culture Of Security'* Organisation For Economic Co-Operation And Development, July 2002, at http://www.oecd.org/dataoecd/16/22/15582260.pdf

Parker D.B. (1998) 'Fighting Computer Crime' John Wiley & Sons, 1998

Peffers K., Tuunanen T., Rothenberger M.A. & Chatterjee S. (2007) 'A Design Science Research Methodology for Information Systems Research' *Journal of Management Information Systems* 24, 3 (Winter 2007–8) 45–77

van der Pijl G. (1994) 'Measuring the strategic dimensions of the quality of information' *Journal of Strategic Information Systems* 3, 3 (1994) 179-190

Piprani B. & Ernst D. (2008) 'A Model for Data Quality Assessment' *Proc. OTM Workshops* (5333) 2008, pp 750-759

Preece J. (2016) '*Mac Backup Software Review' Top Ten Reviews,* 2016, at http://mac-backup-software-review.toptenreviews.com/

Preston W.C. (2007) *'Backup & Recovery'* O'Reilly Media, 2007

Slay J. & Koronios A. (2006) '*Information Technology Security & Risk Management'* Wiley, 3rd ed., 2006

Saltzer J. & Schroeder M. (1975) 'The protection of information in computer systems' *Proc. IEEE* 63, 9 (1975), pp. 1278-1308

Shedden P., Scheepers R., Smith W. & Ahmad A. (2011) 'Incorporating a knowledge perspective into security risk assessments' *VINE* 41,2 (2011) 152

Strom S. (2010) *'Online Backup: Worth the Risk?*' SANS Institute, May 2010, at http://www.sans.org/reading-room/whitepapers/backup/online-backup-worth-risk-33363

Tapscott D. & Williams A.D. (2006) *'Wikinomics: How Mass Collaboration Changes Everything'* Portfolio, 2006 TOB (2012) 'Types of Backup' typesofbackup.com, June 2012, at typesofbackup.com

Toffler A. (1970) *'Future Shock'* Pan, 1970

Toffler A. (1980) *'The Third Wave'* Pan, 1980

Wang R.Y. & Strong D.M. (1996) 'Beyond Accuracy: What Data Quality Means to Data Consumers' *Journal of Management Information Systems* 12, 4 (Spring, 1996) 5-33

Supplementary Materials

App. 1: The Conventional Security Model
http://www.rogerclarke.com/EC/PBAR.html#App1

App. 2: Backup Characteristics
http://www.rogerclarke.com/EC/PBAR.html#App2

App. 3: Backup Procedures
http://www.rogerclarke.com/EC/PBAR.html#App3

App. 4: How Backup Mechanisms Address Threat-Vulnerability Combinations
http://www.rogerclarke.com/EC/PBAR.html#App4

Acknowledgements

The assistance of Russell Clarke is gratefully acknowledged, in relation to conception, detailed design and implementation of backup and recovery arrangements for the author's business and personal needs, and for review of a draft of this paper. The comments of a reviewer and the Section Editor were of material assistance in clarifying aspects of the analysis and the presentation