Archives and Manuscripts
Vol. 40, No. 2, July 2012, 73–83

Records guardianship: security and protection in the workplace

Coralee Louko*

Coralee Louko is currently completing the Master of Archival Studies program at the School of Library, Archival, and Information Studies, University of British Columbia, in Vancouver, BC, Canada. She has fifteen years of experience in records management and administration at a financial planning firm in Calgary, Alberta, Canada. Ms Louko has earned Bachelor degrees in Theology at Eston College in Saskatchewan (2005) and in Art History, with a minor in Museum and Heritage Studies, at the University of Calgary (2010). The latter included a practicum at the Library and Archives of the Military Museums in Calgary.

Ensuring the proper protection of records presents numerous challenges. The archival community has adequately addressed how to recognise, and deal with, threats to the conservation and preservation care of records, but security risks in the workplace are often not given appropriate attention. The identification of potential sources of risk, at all stages of a record's existence, and the discovery of solutions to prevent or mitigate these risks is crucial to guaranteeing the ongoing care and complete protection of records of all types.

Keywords: records protection; workplace security; security breach; risks; threats; transparency; corporate espionage; employee screening; cloud security

The role of an archivist, or records manager, entails multi-faceted responsibilities, but perhaps none more important than upholding the principle of protection. According to the Generally Accepted Record Keeping Principles (GARP®) developed by ARMA International (formerly known as the Association of Records Managers and Administrators) a 'recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity'.[1] This protection encompasses not only preservation, in terms of physical or chemical composition, or even of intellectual, heritage or personal value, but also security, with respect to preventing damage, loss, corruption, tampering, unauthorised use or access and theft. Such a program must also ensure a safe working environment is maintained for those charged with record guardianship, it must cover the records from genesis to disposition, and it must identify potential sources of risk and solutions for dealing with them.

Why does the protection of records merit attention? Aside from potentially containing sensitive information, records often possess significant historical, or other, value. ARMA International claims that records are 'a key resource in the operation of any organisation', crucial not only for their everyday functions, but also for 'answering questions about past decisions and activities' and supporting planning, budgeting, decision-making and regulatory compliance (and proof thereof) and, consequently, must be

*Email: cjlouko@alumni.ubc.ca

ISSN 0157-6895 print/ISSN 2164-6058 online

http://dx.doi.org/10.1080/01576895.2012.712829
http://www.tandfonline.com

guarded carefully.[2] The GARP® principle of integrity, which associates the reliability of a record with that of its recordkeeping system ('including hardware, network infrastructure and software'), stresses the importance of ensuring proper security measures are in place and maintained, in order to ensure trustworthiness.[3] The essential value of an organisation's records, therefore, warrants a formal plan, to ensure their continued protection and uninterrupted security.

What motivates organisations to implement proper records management and protection programs? Richard J Cox – Professor in Library and Information Science at the University of Pittsburgh, School of Information Sciences – has identified seven categories of motivations, given by corporations, for doing so:

(1) a developmental landmark or significant anniversary;
(2) individuals or groups that 'function as champions or advocates' of such programs;
(3) awareness of standards, whether professional or technical;
(4) applicable laws and threatened legal, criminal, or financial penalties for non-compliance;
(5) the desire to increase efficiency, productivity, and corporate competitiveness;
(6) a crisis, ranging from human error, the inability to find requested records, and natural disasters (such as hurricanes) to terrorist attacks and computer hackings; and
(7) the positive spin that public relations and marketing teams believe proper management can put on an organisation's public image.[4]

The fourth and sixth motivations are often interrelated, as a crisis generally precipitates legal action and vice versa. Catastrophes may, in turn, be usurped, to increase awareness of standards (third on the list). No matter the motivation, every organisation should have a proper management system in place to ensure uninterrupted security and protection of their records.

An additional benefit of implementing a proper records protection program is the minimisation of the risk of corruption within the organisation. This has several facets related to transparency, scope and verification. The GARP® principle of transparency calls for documenting an organisation's 'processes and activities … in an understandable manner [that is] available to all personnel and appropriate interested parties'.[5] Ideally, policies promoting transparency will be complemented by routine external scrutiny and will assist with securing the records, by deterring unauthorised access and tampering, thus reducing the opportunity for records to provide 'a mask for improper or illegal activities', such as money laundering and bribery.[6] For example, the Heiner Affair in Australia in the 1990s proved the necessity of transparent practices and external auditing of even the highest levels of authority. The government allegedly attempted to 'cover up [its] misdeeds under the guise of records disposition', by gaining the consent of the state archivist to violate policies and destroy records relevant to 'charges of physical and sexual abuse in Queensland's Institutions for teenagers and children'.[7] Records at any point of the records continuum may provide valuable evidence of corruption and, therefore, merit protection.

In order to facilitate transparency, records managers and archivists must ensure their records cover the full scope of relevant activities. For example, a side effect of the financial market crisis in North America at the turn of the millennium was that it brought to light numerous 'off the books' instances, in which financial advisors had lent their personal money to mutual fund clients.[8] Such transactions not only violate the requirement for transparency and arouse suspicion, due to the apparent secrecy with which they are conducted, but they also create an administrative nightmare, in which the money trail is easily lost, due to the lack of documentation, creating a vulnerability to corruption. Ensuring proper coverage may involve recruiting records from appropriate sources and various departments of the organisation or it may require a new policy, mandating the creation of records for important activities that would otherwise go undocumented. For example, the valuation and capture of significant emails and other electronic messages is an ongoing challenge, yet important decisions may transpire in such ephemeral media. In many cases, no amount of protection, given to the records that do exist, will compensate for the lack of the unrecorded information.

On the other hand, practicing the principles of both protection and transparency will only be effective if the records contain proper documentation to begin with. The priority is quality, rather than quantity, as the reliability of the information contained within the records must also be verified and maintained. The dangers of failing to do so are demonstrated by the Bernie Madoff fiasco in the United States, in which Bernard L Madoff Investment Securities LLC was able to produce copious amounts of highly detailed, but falsified, records for numerous audits and investigations over many years – records which 'withstood scrutiny' and hid the operation of a Ponzi scheme.[9] No amount of protection given to these records would have undone their falsity. Thus, it is important to ensure that the appropriate records are being captured and properly verified, as well as securely maintained.

With respect to the security of records, there are a multitude of other reasons for concern, ranging from identity theft and personal privacy issues to corporate survival and national security. A security breach occurs any time data is accessed or acquired without authorisation, and it is most calamitous, when it 'materially compromises the security, confidentiality, or integrity' of the information.[10] In this era of computers and technology, the number of new vulnerabilities and areas of risk that must be guarded against is growing exponentially; it is difficult to keep fully abreast of all new developments within the electronics industry, not to mention in software and the online world. Yet keep up-to-date we must – it is unacceptable to respond with the excuse 'we didn't think about that', when faced with a crisis caused by a breach in security. The number of people victimised by identity theft, or by having their personal data compromised, is increasing at an astronomical rate. The US Federal Trade Commission estimates that nine million new cases of identity theft occur each year – a number supported by the continuous flow of news stories related to security breaches, which range from the shockingly common incidences of records being thrown into dumpsters to the notorious WikiLeaks 'CableGate' to the stunning cyber attacks on security giant RSA and Sony Electronics' PlayStation Network, which put millions of sensitive personal and financial records in jeopardy.[11] In Australia, the Office of the Information Commissioner investigated new major data breaches at a rate of two a week 'in the last financial year'.[12] The saddest part is that such crises are, at least partially, preventable, yet policies to protect records against infiltrations, attacks, thefts, loss and corruption are generally reactionary, enacted and enforced only after the disaster has occurred, and the damage has been done.

What are the potential areas of risk? The list of vulnerabilities is a long one. Perhaps one most often overlooked by archivists and records managers is that of corporate espionage – a risk which is far higher for companies that specialise in research and development, but which may affect any organisation and its records at any point in the continuum.[13] The Canadian Security Intelligence Service (CSIS) claims that 'state-sponsored espionage is a problem "being conducted today at levels equal to – or greater than – those witnessed during the Cold War"'.[14] The methods used by industrial spies range from dumpster-diving to asking the office secretary seemingly innocent questions to actually gaining employment within the targeted company, and the buyers of this information range from competitor companies to foreign nations.[15] Ron Myles – a former CSIS operative and main speaker at the Criminal Intelligence Service Canada (CISC) 2011 conference, 'Protecting Your Company Against Corporate Espionage', in Gatineau, Quebec – estimated the cost to Canadian companies at about C$10 billion per year.[16] According to Myles, the steep price for companies in Canada is higher than necessary, because Canadians are so easy to get along with, and they 'don't believe that people would spy on [them]'.[17] However, Canadians are not alone in their naïve belief in immunity to a practice that is common worldwide, and the lack of awareness is alarming, creating an enormous gap in security policies and inhibiting effective protection plans.

The existence of corporate spies brings attention to the fact that an organisation's own employees are also an enormous source of risk to the protection of its records. Policies to ensure accountability are necessary, even for those in positions of authority. For example, Leslie Charles Waffen, former head of the audio-video branch of the National Archives in the US, was recently convicted of stealing nearly 1000 historical audio recordings, over a period of, at least, ten years, during his 41 years of employment.[18] Waffen sold many of them online, and it took a decade before his activities caught the attention of one of the original donors. This internal risk to records applies not only to theft and espionage, but also to vandalism, corruption and destruction, so organisations need to take precautions, regarding the people who are given access to their records, particularly during the pre-hiring procedures for new applicants. This means background and criminal records checks, proper investigation into prior employment and potential personal or family issues (including filing for bankruptcy or being involved in a civil lawsuit) and drug screening.[19] It may involve psychological scrutiny, but note that personality 'profiling does not necessarily work', as criminal tendencies and perpetrators of workplace violence cross 'all racial, economic, and social lines'.[20] Ensuring a safe environment also entails enforcing appropriate policies and procedures regarding relationships, grievances, termination of employment, physical security measures and workplace safety training.[21] Ideally, the careful selection and monitoring of employees will result in better records protection.

There are a number of reasons why employees may become so disgruntled as to take destructive action against their employer in ways that put records in jeopardy, including sabotage, arson and bombings. Personal vendettas over rejections of requests for raises or vacations, or even due to criticism or a poor review, are all enormous issues, as are substance abuse and workplace romances that go sour or involve marital infidelity.[22] Fundamental disagreements with colleagues or with the organisation's identity, mission, policies or actions and differing religious or political views are also cause for alarm, as is the desire to 'go out in a "blaze of glory," or be infamous'.[23] No matter the motivation, such events not only put lives at risk, but also compromise the safety and security of all proximal records.

The circumstances that instigate such actions may develop after the hiring of the problem individuals, and a person may nurse a grudge for years, before exploding in a way that threatens an organisation, when he or she finds a way to gain access.[24] Therefore, it is important that all employees are trained at spotting high-risk behaviour and that security personnel are kept apprised of developing situations. Warning signs include mood swings, hostility toward other employees or the organisation, changes in personality or work habits (including punctuality), sudden or frequent address or name changes, possession of weaponry (including mace and pepper spray, brass knuckles, handcuffs, knives, handguns), substance abuse and evidence of domestic violence or physical abuse.[25] The latter, in particular, is due to the fact that current employees are not the only risks, but, rather, family members (particularly spouses and former significant others), acquaintances and terminated employees are the leading sources of violence in the workplace.[26]

Non-employees that enter the premises, with or without authorisation, are a huge source of risk to an organisation's records. While this category includes former employees and relations, as mentioned above, it also encompasses break-and-enter thieves, contractors, vendors, delivery people and even clients. For example, an incident that occurred in Canada, in 2004, served as a grave reminder that no one should be trusted: a financial advisor in Calgary, Alberta, momentarily left his client alone in the meeting room, while he went to find a colleague to witness a signature, and, upon returning to the room, he was shocked to discover his client had taken his file on her and escaped out the back door. The hammer fell heavily, and, as a result, new security measures were rapidly implemented in that office. Another common vulnerability to outsiders is the computer screen: a single glance from an unauthorised person can compromise an enormous amount of data. Monitors need to be installed at the appropriate tilt and angle to prevent passers-by from reading sensitive data that may be displayed there – this is particularly true for reception desks – and screen savers requiring passwords ought to be activated. It is shrewd business practice to occasionally take a walk through the workplace, in order to evaluate how records are exposed and where they are vulnerable to unauthorised access.

Employee awareness and empowerment to deny access to unauthorised persons (whether to a computer, a fax printout, a room or the premises in general) are key to ensuring records are adequately protected. As seen with employee screening, there are no scientific absolutes regarding the types of people that pose the greatest risk, but there are some warning signs. Employees should be suspicious of people making unscheduled or unusually long or frequent visits (particularly delivery or service people, who generally have routes and timetables to keep), asking too many questions, making enquiries either that concern matters beyond their security clearance or that target a specific employee, and being found in an unauthorised area.[27] Personnel must also be vigilant in identifying unknown people and ensuring they have the proper security clearance and rights of access to be where they are and doing what they are doing. In larger businesses, this may require employees and visitors to wear identification cards and have special pass-keys or other means of controlling computer access, but companies must be diligent in retrieving all of these items upon termination of the visit or employment (including when an employee transfers to a different department), along with all keys and passwords – otherwise, all locks and passwords must be changed, each time someone leaves the employ of the organisation.[28] In the example above, the client who absconded with her file was able to flee the office unquestioned by other employees, not merely because she left unseen by the back door, but also because she had been verified as a legitimate client by the advisor's acceptance of her into his office, and, in those days, it was unthinkable to consider her a threat. This highlights the need for employees to be properly trained and made aware of potential sources of risk, and, when something goes wrong, it is important to figure out what could have been done differently.

Increasing staff awareness of potential dangers should decrease the risks caused by employee behaviour. An enormous vulnerability as simple as leaving doors unlocked or even propped open during smoke breaks can be prevented, by ensuring the participation of every employee.[29] Security policies and procedures should be discussed with new personnel immediately after the hiring process, and written acknowledgement of staff having read the appropriate policies and manuals ought to be obtained. This is particularly pertinent in this era of technology, which permits employees to work from anywhere on the planet. The ability to work remotely, to transfer data from 'a secured network to an unsecured computer' and to remove sensitive data from a safe workplace via laptops and smart phones has exponentially increased the potential for security breaches.[30] For example, in Calgary, in 2006, the sensitive personal and financial data for hundreds of clients was put in jeopardy when an office laptop, which a financial advisor had left unsecured and readily visible in a parked vehicle, was stolen in a smash-and-grab robbery. The theft of either records themselves or of their electronic storage devices is of immense concern, and it is estimated that 'over 350 million records containing sensitive personal information have been involved in security breaches in the United States [between] January 2005' and June 2010.[31] However, the lack of control over the environment where the data will be viewed is perhaps a more significant and under-recognised issue, as prying eyes may not be simply the person standing nearby, but may also be on the other end of a hidden surveillance camera or a keystroke logger, for example. Concerns regarding eHealth – the Australian 'Government project to give citizens access to an electronic health record' – largely stem from the use of unsecured computers to access the data.[32] The potential for unauthorised access and theft is far greater when records are taken outside the organisation, and the lack of supervision outside the workplace also means the records are at risk of tampering, corruption and destruction. It is, therefore, necessary for all employees to be apprised of potential dangers and trained to take precautions to prevent such opportunities.

When are records vulnerable to security breaches? The answer is simple, yet frustrating: records are always at risk, at every point in the records continuum, even during the creation process, when the records are, as yet, incomplete. According to GARP®, an organisation's 'recordkeeping program must ensure that appropriate protection controls are applied to information from the moment it is created to the moment it undergoes final disposition'.[33] There is always the threat of potential tampering, loss, theft or sabotage, due to corporate espionage, and organisations must be vigilant in protecting their records electronically, as well as physically. For example, precautions must be taken to prevent fax printouts from being accessible to passers-by, including the cleaning crew and the night watchman, if they arrive after hours. The destination (even if the speed dial function is utilised) of outgoing faxes, and receipt by the intended individual, should both be confirmed. From the outset, the principle of protection must be adhered to in anticipating future uses of the records, and appropriate precautions and controls must be applied to both the physical and digital environments which will host the records. As a result, 'every system that generates, stores, and uses information should be examined', particularly computer systems and network connections, but also physical systems and operational processes, to ensure appropriate access restrictions (based on job function and security clearance) are applied at all times.[34]

The period of active use that follows the genesis of a record presents numerous challenges. This is partly because the documents are often both accessed and kept in the open, rather than behind locked doors. Records are, then, more likely to be neglected by absent-minded and busy employees, especially when being transferred between personnel. Paper files and electronic storage devices may be left on the desktop, on the photocopier, in the fax room, in the staff meeting or reading room and even on top of the water cooler in the break room. While there is always the chance that smaller slips of paper will escape the folder and be lost, records are also vulnerable to unauthorised access by co-workers, administrative staff, cleaners, delivery and service people, clients and anyone else who happens to walk by. Whether in the cubicle or in the hallway in transit, employees need to be aware of potential hazards and take conscious precautions to prevent them. That being said, there must also be procedures and controls in place for when exceptions to the security policy occur, such as for external auditors, attorneys handling litigation and the 'declassification of confidential and privileged information', and these must be 'clearly defined and understood' by all employees.[35] Once again, employee awareness is instrumental to ensuring records protection.

The inactive phase offers the greatest degree of control for records protection, but this does not necessarily hold true for disposition, which poses a unique set of challenges for records protection plans. Generally, this stage occurs at the completion of a retention schedule and results in records being either sent to the organisation's permanent archive (in which they must retain their security clearance classifications and limitations of access), transferred to another organisation (where proper security protocols must continue to be followed) or destroyed beyond hope of reconstruction.[36] All steps must be carried out, while maintaining the security of the records, and, as such, only employees with appropriate security clearances should have access to them, even while in transit to the final location. When shredding is employed as the means of destruction, it is important for organisations to remember to not only ensure that the documents are cross-cut to appropriate size specifications, but also that the shredded output still needs proper protection. If the shredding is contracted out to a third party, an employee should be designated to accompany the bins of documents to be shredded, from the workplace to the shredding machine, and to witness their destruction personally. The use of destruction certificates should also be used to keep track of what has been shredded, who authorised it and who witnessed it. When destroying records, it is also important to ensure that all copies of all versions are being properly disposed of in a timely manner and this includes the old formats and media for records that have been migrated or reformatted. In this marvellous age of technology, there are so many items that require consideration, from mobile phones to computers to digital camera cards, and one must realise that even fax machines and photocopiers now contain hard drives that may retain sensitive data. The US National Institute of Standards and Technology (NIST) has produced a helpful manual, titled *Guidelines for Media Sanitization* (2006), which explains the necessary steps in clearing, purging and destroying electronic media, in order to ensure that it is irreversible, and all sensitive data is rendered unrecoverable.[37] As an added precaution, lawyers William C Martucci and Jennifer K Oldvader recommend performing 'vulnerability scans regularly' on sanitised or destroyed media.[38]

The use of technology, digital media and electronic records is dangerous for multiple reasons, other than the difficulty of ensuring total destruction of all versions. Aside from the vulnerability of hacking and electronic thievery, technological corruption, physical loss and tampering, electronic records require constant transitions between formats and media, as technology progresses and some forms become obsolete. The transfer process must be performed with extreme caution, as it puts the integrity of the records in jeopardy, and the more copies that are produced, the higher the chance that one will be accessed without authorisation. However, despite that risk, back-up copies are a wise necessity to ensure future access is maintained, even in the event of any crises, including natural disasters, 'system malfunctions, or [in case] the data becomes corrupted'.[39] Adequate records protection thus entails ensuring data integrity.

The advent of Cloud computing (including the Infrastructure, Platform and Software and Service as Service models (IaaS, PaaS and SaaS, respectively)) has introduced new challenges for recordkeepers.[40] Any information that is stored online is vulnerable, not only to hacking, but also due to the security level of the party providing the physical storage of the media or the network. Determining who has access – both physical and electronic – to the data may not be simple or transparent, but is essential to ensuring a secure Cloud environment. It is also prudent to seek clarification on the roles and responsibilities of each party and to carefully examine terms of service and the Service Level Agreement (SLA), before signing with a Cloud Service Provider (CSP). For example, clearly delineate who is in charge of encryption and managing routers and firewalls and who is responsible for ensuring operating systems, applications and antivirus programs are updated and maintained.[41] In addition to this, disaster plans and guidelines for response procedures in the event of a security breach must also be in place. Gaps, due to misunderstandings, create vulnerabilities – a high risk when dealing with multiple parties, as in the Cloud environment. For example, if responsibilities are not clearly laid out, the lack of critical software updates may leave records exposed to cyber-attacks, simply because each party believed the other would install the updates. Ensuring sufficient records protection necessitates transparent communication and coordination between all entities with access to the data.

Also, with regard to technology, one of the biggest security risks is now employee use of social media, such as Facebook, Twitter and chat rooms. Organisations must develop and enforce digital policies regarding what employees may post and discuss online, in order to protect their records and sensitive information from '"leaking" outside the organisation', just as they must have policies and procedures in place regarding the removal of physical files.[42] Such an electronic policy should cover how smart phones, laptops and even voicemail should be protected and it should determine which information can be emailed, downloaded and printed. Effective computer protocols should be put in place to ensure that the limitations are obeyed.

Some of the problems in implementing proper protection policies depend upon the inability to anticipate all areas of vulnerability; others depend upon the employees charged with implementing them. For example, many older financial planners are truly struggling with attempts by mutual fund regulators to ensure that records are properly protected, particularly with respect to digital media. In most cases, this is a result of the fact that the older people get, the more adverse they are to change, and many refuse to adapt to new technology; in other cases, it is a result of technological illiteracy. In still other cases, it is simply a matter of forgetting about the institution of new policies which prohibit doing things the way that they have always been done. For example, in the past, financial advisors built relationships with their clients based on trust and did not think twice about leaving a client alone with their files for a few minutes, in order to make a photocopy or recruit a signature witness. Similarly, having a client come in to pick up a cheque for the proceeds of a redemption did not require a signature and photo identification. In particular, many older advisors balk at the need to make detailed notes on every interaction with clients, even after being subjected to litigation and falling short in the documentation aspect. However, the threat of legal action is usually enough to scare most employees into compliance with protection policies.

When an organisation's worst fears do come to pass, and a breach in security is discovered, there should be policies in place dictating how to deal with the aftermath. Of course, this will depend upon local legislation, which is currently not formalised in Australia, although the Office of the Australian Information Commissioner has published guidelines.[43] In North America, generally, notification must legally be sent by a reasonable method (either written via mail or courier, by telephone or electronic means, or via public media) to those whose personal information was affected, describing the incident and scope of the security breach, and usually within 30 days of the occurrence.[44] And, of course, the organisation would be remiss to not examine the incident carefully and evaluate what could have been done differently, to assess whether or not (and how) such a breach could have been avoided. The development, as well as the implementation, of policies is important, in order to prevent such events from happening again in the future and to ensure records security.

The guardianship of an organisation's records is an essential part of ensuring business continuity. Identifying threats to records security is crucial to any protection plan, which must take into account both internal and external risks and all points in the records continuum. The development of appropriate policies to prevent security breaches must be accompanied by implementation and enforcement; employee awareness and participation is a necessity. Adhering to the principle of protection in all aspects will result in efficacy and prosperity for organisations of all types and sizes.

Endnotes

1. ARMA International, 'Generally Accepted Recordkeeping Principles ® (GARP®) 2009', available at <*http://www.arma.org/garp/garp.pdf*>, accessed 10 September 2011. ARMA International (<*www.arma.org*>) is a not-for-profit professional association and the authority on managing records and information. Formed in 1955, ARMA International is the oldest and largest association for the information management profession, with a current international membership of more than 10,000. It provides education, publications and information on the efficient maintenance, retrieval and preservation of vital information, created in public and private organisations in all sectors of the economy. It also publishes *Information Management* magazine and the 'Generally Accepted Recordkeeping Principles ® (GARP®)'. More information about GARP® can be found at <*www.arma.org/garp*>.
2. ibid., p. 2.
3. ibid., p. 4.
4. Richard J Cox, 'Seven Paths to Developing or Sustaining RIM Programs', *The Information Management Journal*, vol. 40, no. 2, March/April 2006, pp. 48–57.
5. ARMA International, p. 1.
6. ibid., p. 2.
7. Randall C Jimerson, 'Archives for All: Professional Responsibility and Social Justice', *The American Archivist*, vol. 70, no. 2, Fall/Winter 2007, pp. 252–81 (258).
8. Common excuses given by the advisors for such actions included the desire to maximise leveraging power and assisting clients with responding to unexpected margin calls in a timely manner.
9. John C Montaňa, 'Apples and Oranges: Recordkeeping Principles for Transforming Business Practices', *Information Management Journal*, vol. 43, no. 3, May/June 2009, pp. 26–32 (28). Also, see Aaron Knapp's series of 2009 articles in *Legalisms*, titled 'The SEC Fiddled While Rome Burned', for a more in-depth explanation of the Madoff disaster. Part 1 of 3 available at <*http://legalisms.wordpress.com/2009/02/20/the-sec-fiddled-while-rome-burned-part-1-of-3/*>; Part 2 available at <*http://legalisms.wordpress.com/2009/02/22/the-sec-fiddled-while-rome-burned-part-2-of-3/*>; Part 3 available at <*http://legalisms.wordpress.com/2009/03/08/the-sec-fiddled-while-rome-burned-part-3-of-3/*>, accessed 23 November 2011.
10. William C Martucci and Jennifer K Oldvader, 'Workplace Privacy and Data Security', *Employment Relations Today*, vol. 37, no. 2, Summer 2010, pp. 59–66 (60).

11. ibid., p. 59. For a concise explanation of the WikiLeaks incident, see Christian Stöcker, 'A Dispatch Disaster in Six Acts', *Spiegel Online International*, 1 September 2011, available at <*http://www.spiegel.de/international/world/0,1518,783778,00.html*>, accessed 16 September 2011. For more on the RSA security breach, see Ben Grubb, 'Hacked Security Firm Leaves Aussies Vulnerable', *The Sydney Morning Herald*, 21 March 2011, available at <*http://www.smh.com.au/it-pro/security-it/hacked-security-firm-leaves-aussies-vulnerable-20111216-1oxzx.html*>, accessed 25 June 2012. For a brief overview of the Sony PlayStation breach, read 'PlayStation Privacy Breach: 77 Million Customer Accounts Exposed', *The Sydney Morning Herald*, 27 April 2011, available at <*http://www.smh.com.au/digital-life/games/playstation-privacy-breach-77-million-customer-accounts-exposed-20110427-1dvhf.html*>, accessed 25 June 2012.
12. Lia Timson, 'One Data Breach a Week: Australia', *The Sydney Morning Herald*, 30 April 2012, available at <*http://www.smh.com.au/it-pro/security-it/one-data-breach-a-week-australia-20120430-1xulv.html*>, accessed 25 June 2012. Timson claims that the 'Office of the Australian Information Commissioner was notified of 56 data breaches' and 'opened a further 59 investigations into other breaches, taking the number of investigations to 115'.
13. Daniel Proussalidis, 'Canadians Naïve About Corporate Espionage: Ex-CSIS Agent', *Toronto Sun*, 29 November 2011, available at <*http://www.torontosun.com/2011/11/29/canadians-naive-about-corporate-espionage-ex-csis-agent*>, accessed 4 December 2011. Not only records managers, but also archivists need to be aware of the sources of their holdings, as not only corporate records, but also employees' private papers are at risk for corporate espionage.
14. ibid., paragraph 8.
15. ibid., paragraph 7.
16. ibid., paragraph 1.
17. ibid., paragraph 2.
18. See Jessica Gresko, 'Amateur Sleuth Helps Stop National Archives Thefts', *Associated Press*, 4 May 2012, available at <*http://news.yahoo.com/amateur-sleuth-helps-stop-national-archives-thefts-081112038.html*>, accessed 5 June 2012; Ruben Castaneda and Lisa Rein, 'Former Employee Admits Stealing Recordings from National Archives', *Washington Post*, 4 October 2011, available at <*http://www.washingtonpost.com/local/former-employee-admits-stealing-recordings-from-national-archives/2011/10/04/gIQAB1kzLL_story.html*>, accessed 4 October 2011.
19. Larger companies may outsource employee screening and background checks to reputable experts, such as BackCheck in Canada. Companies with financial constraints or non-profit organisations may require candidates to pay screening costs, although this will not be appropriate in all cases. Others may choose the 'do it yourself' method, using 'how-to' resources, such as Linda L Graff's *Beyond Police Checks: The Definitive Volunteer and Employee Screening Guidebook*, Linda Graff and Associates, Dundas, 1999, or Edward C Andler and Dara Herbst's *The Complete Reference Checking Handbook: The Proven (and Legal) Way to Prevent Hiring Mistakes*, American Management Association, New York, 2003, to navigate the delicacies of the procedure. Look for local resources to ensure that you comply with the legal intricacies of your particular jurisdiction.
20. Rita Jackson, 'Security in the Workplace: Protecting Employees while Open to the Public 24 Hours a Day, 7 Days a Week', *Health Care Food and Nutrition Focus*, vol. 20, no. 4, April 2003, pp. 1, 3–7.
21. ibid., pp. 4–5. Also, see Peter Piazza, 'Security Trumps Privacy Concerns', *Security Management*, vol. 46, no. 8, Aug 2002, p. 37. One of the side-effects of the terrorist attacks of 9-11 in the US was an increase in employee acceptance of being monitored by their employers in the workplace and, in many cases, support for more stringent security measures, including 'more thorough pre-employment background investigations' and the development and communication of a policy, regarding 'privacy and security issues at the workplace' (Piazza, p. 37).
22. Jackson, pp. 1, 3. According to Rita Jackson, contributing author to the *Health Care Food and Nutrition Focus* journal, 'Very often, a person is either intoxicated or high at the time of an incident' involving violence in the workplace (p. 3).
23. ibid., p. 1.
24. ibid., p. 3.
25. ibid.

26. ibid. Note that this statistic is for the United States, but it is likely to be applicable in other nations.
27. ibid., p. 4.
28. Records should identify which keys and passes each employee (including janitors and security guards) has been issued, and an inventory should be conducted regularly, in order to ensure that none are missing or still in the hands of an employee that should no longer have such access.
29. See Jackson, p. 5.
30. Martucci and Oldvader, p. 65.
31. Martucci and Oldvader, p. 59.
32. Brett Winterford, 'Australia's eHealth Record a Security "Disaster"', *iTnews*, 28 November 2011, available at <*http://www.itnews.com.au/News/281216,australias-ehealth-record-a-security-disaster.aspx*>, accessed 25 June 2012.
33. ARMA International, p. 5.
34. ibid.
35. ibid.
36. ibid.
37. See National Institute of Standards and Technology, *Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology: Computer Security*, National Institute of Standards and Technology: Computer Security Division, Gaithersburg, 2006.
38. Martucci and Oldvader, p. 62.
39. ARMA International, p. 7.
40. TechTarget and the Cloud Security Alliance provide an excellent free online resource centre for learning about security and protection in the Cloud (including topics such as identifying if cloud computing fits your needs, evaluating Cloud Service Providers, risk assessment, encryption and handling leaks), available at <*searchcloudsecurity.com*>.
41. See Robert Zigweid, 'Lesson #1 Collision Course: PCI Data and the Cloud', 2012, available at <*http://searchcloudsecurity.techtarget.com/tutorial/Cloud-computing-and-data-protection-Cloud-computing-encryption-tutorial*>, accessed 26 June 2012.
42. ARMA International, p. 5.
43. Timson asserts that in the wake of so many major security crises (115 in the last fiscal year), 'pressure is mounting' on the Australian government to introduce legislation regarding the disclosure of data breaches (Timson, paragraphs 2, 5). See the Office of the Australian Information Commissioner, 'Data Breach Notification', April 2012, available at <*http://www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html*>, accessed 5 July 2012.
44. Martucci and Oldvader, p. 61.