XBRL-Trail: A Model for Introducing Digital Forensic Readiness to XBRL

D. Kotze and M.S. Olivier

Information and Computer Security Architecture Research Group, University of Pretoria, Pretoria, South Africa
e-mail: djjkotze@kroon.co.za, molivier@cs.up.ac.za

Abstract

Business is reliant on Information Technology to process and share financial data. Proprietary formats often hinder the sharing of financial data as stakeholders can not uniformly read or access the data. As a result, XBRL (The eXtensible Business Reporting Language) was developed to address the information sharing issue, and is rapidly becoming the standard format for financial data. XBRL does however pose a significant fraud risk, as it is trivial to edit the financial records in an unauthorised manner. Typically such a case requires investigation by digital forensic experts, whose duties are in turn complicated by XBRL's scant retention of forensic evidence (lack of forensic readiness). This article addresses XBRL's lack of forensic readiness and proposes a model to enhance the forensic readiness of XBRL. Using a mediator, placed between the users of the XBRL data and the XBRL data itself, we show that forensic evidence can be captured in real time, which would significantly reduce the investigation time.

Keywords:

Digital Forensics, Forensic Readiness, XBRL

1. Introduction

The eXtensible Business Reporting Language (XBRL) was developed in response to the challenge of sharing financial information. XBRL, like XML, is a mark-up language that uses specialised tags to delineate financial structures or elements.

Although XBRL facilitates information sharing, its approach is not without problems. XBRL is vulnerable to information misuse and unauthorised tampering because of its easy-to-share, human-readable format. Unauthorised tampering with financial data is commonly known as fraud (Oxford English Dictionary, 2007).

Due to the digital nature of the financial statements and the absence of physical evidence, a digital forensic investigation is required to solve these crimes. A cyber investigation is complicated by the difficulty in accurately assessing the reliability of evidence found, due to the ease with which digital evidence can be modified (Casey, 2002). Casey states that forensic examiners have "a duty to estimate how closely ... the data approximates reality". In essence, the conscientious investigator must apply some form of rating to the certainty and reliability of his/her evidence.

Casey (Casey, 2002) further proposes such a rating scale, called the Casey Certainty Scale (CCS). It rates evidence from the lowest level of certainty (C0 — erroneous evidence that contradicts known facts) to the highest level of certainty (C6 — evidence that is absolutely certain, tamper-proof and unquestionable).

Despite the best certainty of evidence, digital forensics investigations are time consuming, costly and disruptive to business. It is worthwhile to apply forensic readiness principals to facilitate the easy collection of forensic evidence, as this decreases investigation time and cost, and minimises disruption to business (Baryamureeba and Tushabe, 2004).

As XBRL does not record evidentiary meta data, one is reliant on applications that fulfil the role of mediator for most digital evidence. This evidence is usually not sufficient for proper investigation. Casey rates this type of evidence as C1 (highly uncertain) as it originates from only one source and may be manipulated in any way. As a result, the authors conclude that XBRL in its current state is *not* reliable and *not* forensically ready.

XBRL is human readable, allowing for data exchange. The research problem is thus defined as follows: In the case of fraud and/or illegitimate tampering with a company's XBRL financials, how can usable digital forensic evidence be extracted?

At this point in time, the authors would like to point out that the research problem has a wider application than XBRL — the entire XML family is plagued by the problems outlined above. The authors chose to utilise XBRL as an illustration vehicle as it provides a very clear instance of critical information which is likely to fall victim to manipulation and/or fraudulent intervention. Furthermore, due to the mathematical rigour of financial statements and their unique characteristics, XBRL forensics provides a multi-faceted research problem with unique features that exceeds that of mere XML forensics.

This article aims to contribute a scientifically-based approach to enhance the forensic readiness of XBRL, accomplished by suggesting a pluggable model to provide relevant evidentiary meta data that ranks highly on the Casey scale in terms of certainty and reliability. This model is called *XBRL-Trail*.

A number of the concerns in the problem statement are addressed by Forum Systems (Business Wire, 2004), in their Firewall and Security Gateway products. Forum Systems provides secure XBRL communications for network devices, by means of encryption, audit logging, access control, digital signatures and integrity checks.

XBRL-Trail however differs from the Forum Systems solution in the fact that it addresses the novel concept of forensics for XBRL/XML documents and provides a novel solution for XML/XBRL forensic readiness problem. It is less concerned with XBRL security, as a forensically-based solution implies a measure of XBRL security to support the forensics requirements, but does not attempt to provide an explicit security solution. The *XBRL-Trail* model makes a thought-provoking contribution by combining a forensic investigation with a version control system in order to provide a step-by-step history of actions as evidence. This article further contributes the identification of a number of existing technologies for forensic use, combining them to suggest a solution that provides forensic readiness. Examples of existing technologies include digital signatures and watermarks for tamper-proofing; version control for step-by-step *detailed* meta data (or logging of actions) and the ability to revert back to previous versions of a XBRL document; and username/password authentication (for non-repudiation).

The rest of this paper is structured as follows — in section 2 we supply a brief overview of XBRL and Forensic Readiness, continuing in section 3 with the development of the XBRL model. We introduce the idea of XBRL version control and tamper-proofing in section 4 and conclude with a discussion of *XBRL-Trail*'s characteristics and implementation in section 5

2. XBRL and Forensic Readiness

As with any system, there are drawbacks to the mark-up and human readability components of the format. XBRL has been criticised for many things, but it is beyond the scope of this article to determine XML/XBRL's suitability to its purpose. Instead, we accept XBRL as a solution for information exchange and focus on the forensic issues inherent to XBRL. For a discussion of the merits of XBRL, refer to Ward's article on enhancing the credibility of audited financial statements (Ward, 2004).

Looking at XBRL forensically, there are a number of serious concerns. The XBRL human readability requirement introduces the risk of fraud by means of editing the financial information stored in a system. In addition, XBRL lacks inherent support for the extraction of detailed forensic evidence in the event of fraud, which is necessary for the successful prosecution of the fraudsters.

For standard XML documents, forensic evidence extraction is not important, but considering that XBRL is intended to handle very sensitive data and allows for modification through its human-readability, this situation calls for some form of remediation.

This problem is exacerbated by the lack of certainty (as explained in the introduction) pronounceable over the evidence that *can* be extracted from XBRL data. Casey establishes two types of uncertainty, namely temporal uncertainty and uncertainty of origin. These uncertainties deal with some aspects of the very core of a forensic investigation, namely the *who* and the *when* properties of the crime. These uncertainties form the main basis for the criteria of the CCS. Casey (Casey, 2002) attributes XBRL evidence's lack of certainty to flaws in its temporal certainty and certainty of origin.

The only way to address the lack of certainty is to obtain evidence from a third-party solution i.e. that which is independent of XBRL. Such a solution provides the advantage that evidence is gathered from an independent source, which enables a higher certainty rating according to the CCS. Such evidence also has temporal and origin certainty

Continuous evidence collection is required from the third-party solution, as evidence cannot be retrieved from the XBRL source data. The technique of having forensic data pre-gathered is a major component of forensic readiness. Forensic readiness is defined by Rowlingson as the "ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation" (Rowlingson, 2004).

Tan states that the default existence of relevant evidence in digital crime scenes is rare (Tan et al., 2003). Typically, extensive investigation is required in order to discover relevant evidence. Such an investigation takes exponentially longer than it took the perpetrator to commit the crime (Tan, 2001). The more time-consuming an investigation is, the longer is the down-time incurred by the business.

Coupling long investigation time with a strong priority on business continuity[1] is a recipe for a failed investigation. It is thus clear that an emphasis on forensic readiness within an organisation is crucial to the success of an investigation.

We continue to develop a model to address these concerns in the next section.

3. Development of the XBRL model

As mentioned earlier, forensic readiness in XBRL is of crucial importance. Rowlingson (Rowlingson, 2004) defined a process to establish forensic readiness in a corporation, aimed at demarcating the applicable business problems and addressing them. The authors now utilise a reduced version of this process to develop requirements for the *XBRL-Trail* model.

The first step is "*the definition of a business scenario that requires digital evidence*" (Rowlingson, 2004). In the case of XBRL, the scenario is the *collection and processing of financial information*, posing the risk of fraudulent modification of financial information.

To address this risk, we need to monitor the financial data transactions in some manner. This is achieved by using a mediator that records all actions in the form of meta data.

[1] Business continuity is the ability to continue with business as usual. This is typically impaired by an investigation as the business cannot use their systems and generate new data whilst an investigation is in progress.

The second step is the "*evidence collection requirement*" (Rowlingson, 2004). The evidence collection requirement is that of the collection of meta data, due to the insufficiency of the evidentiary data available in the XBRL environment. Meta data constitutes details about file changes, the instigator and date of change, the actual change and the effect of the change.

Additionally, meta data collection requires that all data modifications should occur through a single point, confirming the use of a central mediator.

The penultimate step is that of "*establishing a capability for securely gathering legally admissible evidence*" (Rowlingson, 2004), addressing the question of where to store the recorded meta data. If one stores it together with the source data, it might simply be removed or altered by a malicious agent. This is a complex problem, requiring separate discussion and is addressed in section 4.

The final step to establish forensic readiness is to "*ensure that monitoring/auditing ... will detect major incidents*" (Rowlingson, 2004), achieved by silently logging all XBRL changes by means of the mediator; and restricting access to the data through the use of a mediation agent.

In the next section we discuss the complex problems of tamper-proofing data and recording forensic data by means of version control.

4. Version control and tamper-proofing

We can infer two main requirements for XBRL data integrity from the previous section, namely the recording all access requests to the source data; and the protection of the XBRL financial data from unauthorised access. As this article proposes a high-level overview of the model, the authors shall refrain from discussing any implementation specifics, instead opting for a broad discussion of the technologies that can be used to achieve XBRL data integrity.

In order to record all access to the XBRL financial data, there are two fundamental pre-requisites: 1) All data modifications should take place through a central point at which monitoring occurs; and 2) Meta data capturing should be enforced at the central point.

Meta data capturing should not be computationally intensive, as it is inferred for all editing operations. For fraud detection, we only log edit operations (create, update and delete)[2]. For the purposes of forensic evidence, *who modified the data*, *what was modified* and *when it was modified* is crucial. This dictates an approach of storing the exact edit operation, the date and time and details of the user who made the change.

[2] If the financial data is sufficiently sensitive, access operations should be recorded as well.

A Version Control System (VCS) is intended to record changes to data and is defined as “a mechanism that allows one to audit changes to a particular document or a source by being able to see who changed what” (Pfleeger and Pfleeger, 2003). Furthermore, it allows for roll-back to previous versions, making this approach suitable for evidence collection.

As a result, one can *interpret changes* in addition to merely keeping a record of the changes. Investigators can thus determine *who* changed *what*, instead of only being able to prove that user *x* had access to the files. This level of detailed evidence will significantly shorten the investigation time and greatly aid in its success. Furthermore, this approach bolsters the CCS rating of the forensic evidence as it establishes a multiplicity of elements that compose evidence and addresses the concern of uncertainty of origin.

This brings us to the second requirement, namely preventing unauthorised access and direct modification of the data, known as *tamper-proofing* (Kundur and Hatzinakos, 1999). Casey (Casey, 2002) states that evidence should be “protected against tampering” in order to be reliable, making tamper-proofing[3] another requirement for a high rating on the CCS.

XBRL tamper-proofing is subject to three requirements, namely: 1) the source data must be human readable; 2) tampering must be virtually impossible; and 3) tamper-proofing must be computationally cheap.

Tamper-proofing is traditionally enforced through access restriction through means of password protection (Gollman, 2005). This approach is not successful, as the raw XBRL data is editable and password protection will not negate the risk of direct access to data.

Another popular choice for tamper-proofing is that of encryption (Gollman, 2005), which addresses the risk of direct data access. For this solution, the authors considered the encryption options available in the standard XML security extensions (Hirsch, 2002; Lautenbach, 2004) as well as the IBM XML security suite (Tidwell, 2000). These solutions were however found unsuitable for use, as encryption contravenes the XBRL criteria of being human readable.

Let us now consider Digital Rights Management (DRM). DRM refers to “the control and protection of digital intellectual property (content)” (Commonwealth of Australia, 2008). The purpose of “protecting digital property” is in close alignment with our objective of ensuring that XBRL data is protected from direct access and editing, and is mainly achieved by content encryption and affixing a digital watermark to the content (Jupitermedia Corporation, 2008).

[3] The authors do not use the term tamper-proofing in the absolute sense as no system will ever be completely perfect, but rather as a reference to a sufficiently tamper-resistant system.

Instead of restricting the usage of XBRL data, *XBRL-Trail* requires *restriction of access to the contents*. The strategy of affixing validation to a document by means of *digital watermarking* is also quite promising.

A digital watermark is defined as “a piece of information which is embedded in the digital media and hidden in the content so that it is inseparable from the data” (Bansal and Singh-Bhadouria, 2007). Bansal and Singh-Bhadouria further note that watermarks are used for various tamper-proofing applications, such as *digital signatures*, *fingerprinting* and *authentication*.

We now briefly discuss the impact of the above applications in relation to the problem of tamper-proofing:

- **Digital Signatures (DS)** — A digital signature is defined as “extra data appended to a message which identifies and authenticates the sender” (Howe et al., 2001). Digital signatures in the form of watermarks serve to identify the owner of the content and can also be used to indicate the originator of the data.
- **Authentication** — Watermarks can be applied in authentication, when designed in such a manner that alteration of the data results in either the destruction of the watermark or a mismatch between the watermark and the content.
- **Fingerprinting** — Fingerprinting uses a hidden watermark to establish the creator or owner of the content or data.

One can now ask whether simply applying a DS to data will render it tamper-proof? Combining an encrypted hash of the file with the credentials of the author should technically be enough to fulfil the tamper-proofing requirement.

Research by Kundur and Hatzinakos (Kundur and Hatzinakos, 1999) and Johnson et al (Johnson et al., 1999) suggests that a DS implementation is not sufficient, as signatures can be forged. This is addressed by combining DS with an authentication watermark. Authentication involves applying a watermark which has the property that alteration to the document either *destroys the watermark* or creates a *mismatch* between the content and the watermark. The latter is easily achieved by combining a hash of the XBRL data and the digital signature in the watermark. Should the data or the signature change, the XBRL copy will be rejected by the requesters of the XBRL data as the watermark becomes invalid.

As the implementation of watermarks is outside of the scope of this article, refer to Kundur and Hatzinakos (Kundur and Hatzinakos, 1999), Johnson et al. (Johnson et al., 1999) and Bansal and Singh-Bhadouria (Bansal and Singh-Bhadouria, 2007) for more information.

It should be noted that using digital watermarks for tamper-proofing is a novel application of the watermarking concept (Kundur and Hatzinakos, 1999). Our research suggests that using the watermarking technique to secure XBRL source data is the first application of the tamper-proofing qualities of digital watermarks for non-image related data.

In the above sections we have derived a set of criteria to address the concerns with XBRL data and we have formalised a process for dealing with version control and the tamper-proofing of data. This was necessary in order to establish a tamper-proof method of capturing meta data that may be used as forensic evidence. Both of these strategies succeeded in establishing a greater degree of certainty with regards to the evidence as per the guidelines set by Casey (Casey, 2002).

We proceed by supplying an overview of the characteristics of the model that embodies these criteria and processes in the next section.

5. Characteristics and implementation of *XBRL-Trail*

As noted in section 3, there are three core components that give rise to the *XBRL-Trail* model: 1) The recording of all data transactions, using a central mediator; 2) Recording of meta data to serve as forensic evidence — requiring a central mediator, a version control system and an authorisation system; and 3) The need for tamper-proofing evidence and source data — requiring techniques such as digital signatures and digital watermarks.

Let us now examine each of these components and focus on how they can be applied and implemented in the *XBRL-Trail* environment.

Firstly, let us examine the central mediator. Due to the criticality of the financial data that is dealt with, the mediator should be *trusted* to report *all* transactions that occur. These transactions should be reported in an *accurate*, *valid* and *complete* manner. Pfleeger and Pfleeger (Pfleeger and Pfleeger, 2003) define such a trusted mediator as "a system that meets the intended security requirements; is of high quality; and justifies the user's confidence in that quality".

We now introduce the concept of a reference monitor. A reference monitor is defined as "a portion of code that controls accessibility of objects" (Pfleeger and Pfleeger, 2003). As per this definition, the central mediator is in fact the same as a trusted, two-way reference monitor. This is due to the fact that both these constructs function as trusted intermediaries that regulate the flow of data. As such, the authors will from now onwards refer this concept as the reference monitor.

Pfleeger and Pfleeger (Pfleeger and Pfleeger, 2003) further state that each reference monitor should comply with three requirements in order to be effective: 1) it should be *tamper-proof*; 2) it should *always be invoked* when access to protected information is required; and 3) it should *be small enough* to be subjected to thorough analysis and testing, in order to ensure that all components are functioning correctly and can be trusted.

Secondly, we discuss the retention of meta data. It should be the responsibility of the reference monitor to record all edit operations and log the data as it forms the central point of access to the data. For this purpose, meta data is defined to consist out of three components, namely: 1) details as to *who performed the change*; 2) details as to *when the change was performed*; and 3) details as to *what was changed*. For the last component, we make use of a version control system in the reference monitor (discussed in section 4).

Attributing the change to a specific user however requires an extra piece of functionality, called an authorisation system. Such a system requires the definition of two concepts, namely authorisation and authentication. Gollman (Gollman, 2005) defines authentication as “ensuring that the credentials are valid”. Authorisation, in turn, is defined as “ensuring that the user has access to the information requested” (Gollman, 2005).

Authentication and/or authorisation should be used to restrict access from within the reference monitor, allowing only authorised users to access the financial source data. The advantages are three-fold: 1) a reduction in the fraud risk, as only trusted parties can modify the XBRL data; 2) a comprehensive evidentiary record, allowing investigators to deduce who had access to the financial data in the event of fraud; and 3) providing certainty as to the origin of evidence, which in turn boosts the evidence certainty as per Casey (Casey, 2002).

Authentication and authorisation still however does not enable us to tell *when* data was changed. We recommend that timestamps should be kept to establish an evidentiary chronologic timeline of events (Baryamureeba and Tushabe, 2004). Our final component is that of the safe-keeping of evidence and source data. This is embodied by the requirement that meta data should be stored in a tamper-proof format. This is accomplished by watermarks, as discussed in section 4. By employing this methodology, forgeries are eliminated and consistency with XBRL’s requirement of human readability is maintained.

Let us now determine the effect of our model components and requirements on the certainty rating of our available forensic evidence. Due to our strategy of tamper-proofing the evidence, we have increased the certainty of the evidence to a very high degree, securing either a C4 (Probable) or C5 (Almost certain) rating. Furthermore, multiple evidence sources are available, namely authorisation and authentication information, version control information and standard meta data information, thus further increasing the certainty rating of evidence gathered from *XBRL-Trail*.

We thus conclude that evidence gathered from *XBRL-Trail* is worthy of a high degree of certainty as it contains evidence from multiple sources that are protected against tampering (Casey, 2002), which is a major enhancement over the relatively low level of certainty afforded to evidence gathered without *XBRL-Trail*.

We conclude with an illustration of the *XBRL-Trail* and how it operates in Figure 1.

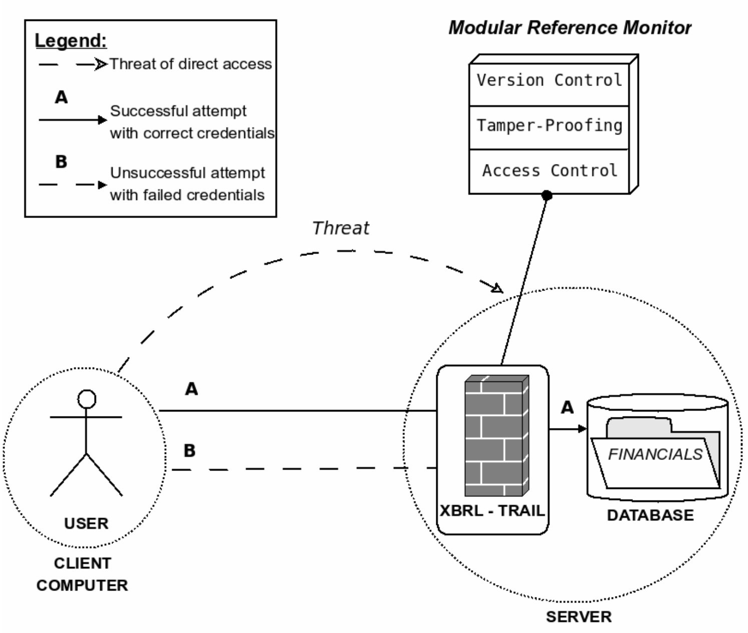

Figure 1: A graphical representation of how the reference monitor restricts and regulates access to the financial data in XBRL format.

6. Conclusion

We investigated XBRL and its impact on business, and noted that it is well-suited to the sharing of financial information between various business stakeholders.

XBRL's inherent characteristics cause it to be easily modified in an unauthorised manner, introducing a fraud risk. Fraud in turn leads to a reputational and financial risk as financial statements often determine a company's market perception and they are also used to indicate a company's financial health.

In the event of fraud involving XBRL, digital forensics experts will be required to investigate the crime. In turn, these experts need to rely on forensic evidence gathered from the scene in order to solve the crime. XBRL's basic mark-up structure however complicates this task significantly, as very little forensic information is available to the investigators. We found that XBRL is not forensically ready and that some mediator for XBRL transactions is required to facilitate forensic readiness.

We introduced evidence certainty (Casey, 2002) — a measurement of the reliance that can be placed on evidence. We noted that a diligent investigator should detect, quantify and compensate for loss and error in evidence. We further highlighted the need of introducing a measure of reliance to the court, together with the evidence.

Lastly, we established that XBRL's default evidence certainty is almost negligible, making it unsuitable for presentation in a court of law.

We then derived the foundation for the requirements needed for a model to successfully solve the problem of evidence availability, by addressing several core needs, namely: 1) the need for recording all transactions to data; 2) the need for recording meta data as forensic evidence; and 3) the need for the safe-keeping of evidence and source data.

The derived model addressed the risks by utilising a reference monitor that controls access to the XBRL source data; version control; timestamps and authorisation. The subsequent evidence is tamper-proof[4] by means of digital signatures and a digital watermark.

In addressing the risks above, we have significantly improved the level of reliance that can be placed upon forensic evidence that is gathered from the *XBRL-Trail*. This is due to our model's addressing of temporal uncertainty and uncertainty of origin, as well as establishing evidence from multiple sources and a reliable time-line. At this point it should be noted that this solution is still in the concept phase and has not yet been implemented. It is not possible at this time to present empirical results regarding *XBRL-Trail*'s practicality.

The resulting model presented in this article seems to adequately address the identified research problem, in turn motivating further work in refining the *XBRL-Trail* concept.

7. References

Bansal, A. and Singh-Bhadouria, S. Network security and confidentiality with digital watermarking. In *IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2007)*, page 325 to 328. IEEE, 2007.

Baryamureeba, V. and Tushabe, F. The Enhanced Digital Investigation Process Model. *Digital Forensics Research Workshop*, August 2004.

Business Wire. Forum Systems Announces Availability of Secure XBRL . Online, January 2004. http://findarticles.com/p/articles/mi_m0EIN/is_2004_Jan_20/ai_112342649/pg_1.

Casey, E. Error, uncertainty and loss in digital evidence. *International Journal of Digital Evidence*, 1(2), 2002.

Commonwealth of Australia. Resources glossary, January 2008. http://www.acma.gov.au/WEB/STANDARD..PC/pc=PC_1498.

[4] As stated earlier, the term is not used in the absolute sense of the word, but rather implying “sufficiently tamper-proof“ to not be tampered with. No system will ever be absolutely tamper-proof.

Gollman, D. *Computer Security*. Wiley and Sons, second edition, 2005. ISBN 0-470-86293-9.

Hirsch, F. Getting started with XML security. Online, November 2002. http://www.sitepoint.com/article/getting-started-xml-security.

Howe, D. Free on-line dictionary of computing. Online, March 2001. http://foldoc.doc.ic.ac.uk/foldoc/Dictionary.gz.

Johnson, N., Duric, Z. and Jajodia, S. A role for digital watermarking in electronic commerce. *ACM Computing Surveys*, 1999.

Jupitermedia Corporation. DRM. Online, 2008. http://webopedia.internet.com/TERM/D/DRM.html.

Kundur, D. and Hatzinakos, D. Digital watermarking for telltale tamper-proofing and authentication. *Proceedings of the IEEE*, 87(7):1167 to 1180, July 1999.

Lautenbach, B. Introduction to XML Encryption and XML Signature. *Information Security Technical Report*, 9 (3):6 to 18, 2004.

Oxford English Dictionary, editor. *Oxford English Dictionary*. Oxford University Press, March 2007. http://dictionary.oed.com/cgi/entry/50088116?

Pfleeger, C. and Pfleeger, S. *Security in Computing*. Prentice Hall, third edition, 2003. ISBN 0-13-0355548-8.

Rowlingson, R. A ten step process for forensic readiness. *International Journal of Digital Evidence*, 2(3), Winter 2004.

Tan, J. Forensic readiness. *Proceedings of the CanSecWest Computer Security Conference*, April 2001.

Tan, T., Ruighaver, T. and Ahmad, A. Incident Handling: Where the need for planning is often not recognised. *Proceedings of the 1st Australian Computer, Network and Information Forensics Conference*, 2003.

Tidwell, D. The XML Security Suite: Increasing the security of e-business. Online, April 2000. http://www-4.ibm.com/software/developer/library/xmlsecuritysuite/index.html.

Ward, G. How XBRL Can Enhance the Credibility of Audited Financial Statements. Online, November 2004. http://www.ifac.org/MediaCenter/? q=node/view/73.