

**LIFE AFTER SARBANES-OXLEY:
THE MERGER OF INFORMATION SECURITY
AND ACCOUNTABILITY**

**Bruce H. Nearon, Jon Stanley,
Steven W. Tepler, and Joseph Burton***

ABSTRACT: This Article explores the connection between the Sarbanes-Oxley Act of 2002 and information security. Although the statute and implementing regulations do not address information security explicitly, the authors argue that compliance is incomplete without an adequate information-security regime in place. If necessary, laws should be amended to make documenting, assessing, and testing information security compulsory. The cost of compliance is likely to be less than losses investors will suffer if the security laws and rules remain silent regarding information security.

CITATION: Bruce H. Nearon, Jon Stanley, Steven W. Tepler, and Joseph Burton, *Life After Sarbanes-Oxley: The Merger of Information Security and Accountability*, 45 *Jurimetrics J.* 379–412 (2005).

On July 30, 2002, the Sarbanes–Oxley Act of 2002,¹ a massive piece of federal legislation, was signed into law. The Act was a direct reaction to the series of financial scandals at corporations like Enron, WorldCom, and Arthur Andersen.² The Act addresses corporate governance in general and adequate disclosure in particular. The Act places squarely on the shoulders of senior corporate management the responsibility for assuring the fairness and accuracy of its publicly filed reports. It also establishes guidelines, in some cases very

*Bruce H. Nearon is a CPA with J.H. Cohn LLP. Jon Stanley is an attorney practicing in Maine. Steven W. Tepler, Esq., is CEO of TimeCertain LLC. Joseph Burton is an attorney with Duane Morris LLP. The authors thank Stacy Stanford for technical editing and Candida deFonseca for helpful citation research assistance.

1. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of 15, 18 U.S.C.).

2. See Mary Kreiner Ramirez, *Just in Crime: Guiding Economic Crime Reform After the Sarbanes-Oxley Act of 2002*, 34 *LOY. U. CHI. L.J.* 359, 360–61 (2003).

detailed ones, and added responsibilities for those professionals who work most closely with corporations in the area of governance: attorneys and accountants.³ Finally, to give teeth to these new responsibilities, it has defined some new offenses and penalties for activities related to a corporation's reporting and disclosure responsibilities.⁴

Two of the core provisions of the Act, Sections 302 and 404, raise the issue of information-security (InfoSec) practices for public companies within the scope of the statute.⁵ Section 302 requires that a public company's principal executive officer and principal financial officer certify the accuracy and fairness of the company's periodic reports.⁶ In addition, Section 302 requires these same officers to certify that they are responsible for establishing and maintaining "internal controls,"⁷ that they have disclosed to their auditors and audit committees any significant deficiencies in the design and operation of the internal controls,⁸ and that they have disclosed in required periodic reports any significant changes in the internal controls that might affect those controls subsequent to the date of their evaluations.⁹

Another key provision of the Act is Section 404, which directly implicates information-security practice and procedure. Section 404 mandates that the annual report filed by a public company contain an "internal control report."¹⁰ Sections 302 and 404 of the Act apply to any company (referred to as "issuer" in the Act and Rules) that files periodic reports pursuant to sections 13(a) or 15(d) of the Securities and Exchange Act of 1934.¹¹ Both sections 302 and 404 of Sarbanes-

3. Section 307 of the Act establishes specific rules of professional responsibility for attorneys:

Not later than 180 days after [the date of enactment of this Act], the Commission shall issue rules, in the public interest and for the protection of investors, setting forth minimum standards of professional conduct for attorneys appearing and practicing before the Commission in any way in the representation of issuers, including a rule—(1) requiring an attorney to report evidence of a material violation of securities law or breach of fiduciary duty or similar violation by the company or any agent thereof, to the chief legal counsel or the chief executive officer of the company (or the equivalent thereof); and (2) if the counsel or officer does not appropriately respond to the evidence (adopting, as necessary, appropriate remedial measures or sanctions with respect to the violation), requiring the attorney to report the evidence to the audit committee of the board of directors of the issuer or to another committee of the board of directors comprised solely of directors not employed directly or indirectly by the issuer, or to the board of directors.

15 U.S.C.A. § 7245 (West 2005).

4. For a helpful summary of these new offences and penalties, see Robert J. Saville et al., *Sarbanes-Oxley Act of 2002: Summary and Analysis of Criminal Provisions*, THELEN REID & PRIEST, LLP (Aug. 22, 2002), at http://www.thelenreid.com/articles/article/art_138.htm.

5. 15 U.S.C.A. §§ 7241, 7262 (West 2005). These provisions are not the *only* provisions within the statute that raise InfoSec issues. Section 802, among others, does as well. See 18 U.S.C.A. §§ 1519, 1520 (West 2005).

6. 15 U.S.C.A. § 7241.

7. 15 U.S.C.A. § 7241(a)(4)(A).

8. 15 U.S.C.A. § 7241(a)(5)(A).

9. 15 U.S.C.A. § 7241(a)(6).

10. 15 U.S.C.A. § 7262(a) ("(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) contain an assessment, as of the most recent fiscal year of the company, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.").

11. Securities Exchange Act of 1934, 15 U.S.C.A. §§ 78(m)(a), (o-6) (West 2005). Section 405 of Sarbanes-Oxley, however, specifically excludes registered investment companies from the

Oxley require the SEC to issue regulations implementing the commands set forth in these sections. Since enacting Sarbanes-Oxley, the SEC promulgated rules according to the Act's requirements.¹²

This Article takes the position that sections 302 and 404 logically mandate that entities covered by the Act¹³ must have a reasonable and appropriate information-security policy designed to assure the integrity of their "internal controls and procedures for financial reporting" as that term is defined by the statute in Section 404.¹⁴ It places an affirmative duty upon public companies and the principal executive officers to establish and maintain effective information-security policies and procedures.

This InfoSec regime, once realized and accepted, will result in improved and more reliable overall information security, which in turn will lead to improved "financial reporting" from publicly traded companies, which ultimately will assist the public in regaining a measure of confidence in the corporate environment. In short, the Act will come to be seen as the most significant piece of information-security legislation passed to date and will bring about a fundamental change in how corporations view and respond to information security.

requirements of Section 404. 15 U.S.C.A. § 7263 (West 2005). Thus, with the exception of registered investment companies, all other "issuers" must comply with the provisions of these two sections. This includes foreign private issuers, asset-backed issuers, small business issuers, and (perhaps) bank and savings associations. Securities and Exchange Commission (SEC) filings affected by sections 302 and 404 are the 10-K, 10-KSB, 20-F, 40-F, 10-Q, and 10-QSB.

12. 17 C.F.R. §§ 240.13a-14, 15d-15 (2005) (for section 302); Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, 68 Fed. Reg. 36,636, 36,642 (June 18, 2003) (for Section 404) [hereinafter *Final Rule on Management's Report*].

These rules originally required compliance with their provisions as of the end of a company's first fiscal year ending on or after June 15, 2004, for "accelerated filers," and for all others filers by their fiscal year ending on or after April 15, 2005. Because of the extensive amount of work needed by preparers and their auditors to comply with the Act, on February 24, 2004, the SEC extended the effective dates for accelerated filers to fiscal years ending on or after November 15, 2004, and for nonaccelerated filers for fiscal years ending on or after July 15, 2005. Final Rule; Extension of Compliance Dates; Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, 69 Fed. Reg. 9,722, 9,722 (Mar. 1, 2004). Under pressure from issuers, the SEC extended the compliance dates for nonaccelerated filers a second time on March 2, 2005, to the first fiscal year ending on or after July 15, 2006. Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports of Non-Accelerated Filers and Foreign Private Issuers, 70 Fed. Reg. 1,528, 11,528 (Mar. 8, 2005).

In addition, the recent Section 404 rules issued by the SEC made procedural and substantive changes to the previously established certification requirements under the Section 302 rules. These changes in the certifications required under Section 302 must be complied with in quarterly, semi-annual, or annual reports due on or after August 14, 2003. *Final Rule on Management's Report, supra*, at 36,644.

13. *Final Rule on Management's Report, supra* note 12, at 36,640 (stating that entities covered by the Act are those "companies subject to the reporting requirements of the Securities Exchange Act of 1934, other than registered investment companies.>").

14. *Id.* The statutory definition is long and quite complex. It will be covered in depth in this Article.

I. THE CHANGING NATURE OF INFORMATION

A. Information Assets

Webster's New Twentieth Century Dictionary defines "information" as "knowledge acquired in any manner; facts; data; learning; lore"; "asset" is "anything owned that has exchange value." Companies subject to SEC regulations and the Sarbanes-Oxley Act prepare financial statements according to Generally Accepted Accounting Principles (GAAP). GAAP's definition of "assets" differs from *Webster's*. According to GAAP, "[a]ssets are probable future economic benefits obtained or controlled by a particular entity as a result of past transactions or events."¹⁵ Therefore, it is possible, and even likely, that many valuable corporate information assets are not reported in the financial statements. Sophisticated investors know that the present accounting rules were developed during the mercantile and industrial ages. With the exception of a few specific intangible assets such as goodwill, the financial statements recognize only assets that were important during those times—namely, financial and physical assets. Even though information assets are generally excluded from corporate financial statements, investors are aware of them and compound their estimated values and prospective cash flows in security prices.¹⁶

Much of our analysis is based upon the presumption that information is not only an asset but also the primary asset of most enterprises. Without information, the exchange value of other assets (including information) becomes suspect, if not functionally worthless. Accordingly, information plays three roles in day-to-day enterprise function. First, it provides the infrastructure for the exchange of assets. Second, it can be considered a "meta-asset" in that the infrastructure facilitating the exchange of assets has intrinsic asset value itself. Third, it provides the records and forensic histories for management, audit, compliance, records retention, and other functions.

Even though GAAP may ignore it, the importance of information is so firmly rooted in our transactional global society that we now turn our discussion to the changing nature of information.

B. The Emergence of the Concept of Source Information or Source Data

Webster's defines "source" as "first cause; place of origin from which something comes or develops; that which gives rise to anything." The transactional information used in the day-to-day functions of public and private enterprise ultimately derived from events that are the source of business records. These source data are generally presumed to be authentic, unchanged (or

15. FINANCIAL ACCOUNTING STANDARDS BOARD OF THE FINANCIAL ACCOUNTING FOUNDATION, STATEMENT OF FINANCIAL ACCOUNTING CONCEPTS NO 6: ELEMENTS OF FINANCIAL STATEMENTS 6 (1985), available at <http://www.fasb.org/pdf/con6.pdf>.

16. MARGARET M. BLAIR & STEVEN M.H. WALLMAN, UNSEEN WEALTH: REPORT OF THE BROOKINGS TASK FORCE ON INTANGIBLES 10–11 (2001); BARUCH LEV, INTANGIBLES: MANAGEMENT, MEASUREMENT, AND REPORTING 5, 79 (2001).

appropriately documented and logged if changed), and trustworthy enough to be relied upon not only by contracting parties or auditors, but also by the enterprise itself, to protect and defend its assets and increase shareholder wealth. Accordingly, what enterprises provide to the auditor—and, in theory, what auditors should be auditing—is source data. But are covered enterprises generating reliable source data for audit purposes and providing source data to auditors for examination?

C. The Data-Generating Event

To help explain the auditing and Sarbanes-Oxley compliance challenges presented by electronically generated information or data, the term *data-generating event* (DGE) can be used. A DGE robustly associates time with content (or information) and is comprised of two elements. The first element is the time of the event. The second element is the content associated with the event. In the physical world, a DGE can be a sunrise with 7:00 a.m. being the time of the event and the sunrise itself being the content associated with the event. It is critical to note that in the physical universe, the time and the content of a DGE cannot be dissociated. We cannot cause a sunrise on a particular day at a particular geographical coordinate not to occur at its appointed time. Using a 7:00 a.m. sunrise as a typical example, it is clear that for events occurring in nature, DGEs are trusted as to both time and content. For physical media created by human artifice, establishment of a DGE is somewhat more attenuated. An inventor's dated ink entry into a paper-based logbook does not create a DGE unless there is some way to establish that the event (that is, time asserted on the log) and the content (the entry in the inventor's log) occurred contemporaneously.¹⁷ In other words, the mere recitation in the content of the date of the written entry does not, by itself, prove the date of the entry, and therefore also does not prove the content's existence at a unique and "non-recreatable" point in time. Human-created physical recordings are thus nearly always susceptible to challenge. In this instance, supporting, corroborating, or authenticating information by way of human testimony and forensic analysis conducted on the physically recorded media is generally necessary to establish a robust association between the event (that is, the time) and content (that is, the log entry).¹⁸

D. The Data-Generating Event, Source Data, and Audit Process

A DGE should give information a strong or irrefutable time reference to unaltered content, and it is in this manner that it imbues data with reliability and "auditability." The generation of Sarbanes-Oxley compliant data, as well as the

17. For example, a plaintiff-inventor seeking to enforce a patent claim had his patent invalidated when, following a forensic analysis involving the testing of the chemical composition of the ink used to write his inventor's logbook, it was determined that fraudulent material was later added to a once-genuine notebook. *Aptix Corp. v. Quickturn Design Sys., Inc.*, No. C 98-00762 WHA, 2000 U.S. Dist. LEXIS 3408, at *71 (N.D. Cal. June 14, 2000).

18. FED. R. EVID. 1002 requires the production of an original so that its contents can be proved.

conduct of a Sarbanes-Oxley compliant audit examination of those data, critically depends on (1) the creation of reliable DGEs by covered enterprises and (2) audit processes that permit examination only of reliable DGEs, which support the financial statements and management's internal control assertions.

As discussed above, the reliability of a DGE depends upon the nature and extent of human interaction involved in its creation.¹⁹ There has been significant recognition of this issue as it relates to the creation of paper-and-ink records, and the principles espoused by GAAP, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), and the Generally Accepted Auditing Standards (GAAS) provide some measure of reliability to human-created financial information.²⁰ As a result of the evolution of decades of such accounting and auditing guidelines and principles, the paper-based source data universe of financial information is subject to laws and regulations designed to ensure reliability and integrity of content.

E. The Concept of "Control" as It Relates to the Data-Generating Event

The reliability of electronically generated source data is significantly more diluted, attenuated, and suspect for all enterprise purposes, including financial audits, than physically generated data. This is because the reliability and auditability of a DGE is directly dependent on issues of control.²¹ If there is human control over a DGE, this control reduces the DGE's reliability and auditability. Take the 7:00 a.m. sunrise, which is a naturally occurring DGE. No human effort can control the time of the sunrise nor can it stop the event (or content) from occurring. This renders the DGE indisputable, and courts would be able to take judicial notice of this fact under Rule 201 of the Federal Rules of Evidence.²² A critical, but generally unarticulated, supporting element for the

19. The probative frailty of a purported DGE where it is even partially dependent upon human-based activity has been tacitly acknowledged for decades, as evident in a law prohibiting liquor retail dealers from possessing liquor bottles that have been refilled after they were originally filled and stamped. While generally viewed as revenue-producing measures, this law has been tacitly understood and accepted by the courts and others to mean that a stamp or seal on an alcoholic product authenticates the contents of the container (the bottle) and assures that (1) the contents are what they purport to be; (2) that the contents have not been altered, substituted, or otherwise tampered with; and (3) that a reliable authority (such as a government agency) has attested to this authentication by affixing a tax-stamp or wax seal over the bottle's cork or cap. *See, e.g., United States v. Milstein*, 401 F.2d 51 (7th Cir. 1968).

20. GAAP, COSO, and GAAS are well known standards in the accounting community.

21. Indeed, it could well be argued that the reliability and auditability of a DGE is inversely proportional to the degree of human control.

22. FED. R. EVID. 201 provides that a federal court may take judicial notice of an adjudicative fact that is both "not subject to reasonable dispute" and either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. "[T]he effect of taking judicial notice under Rule 201 is to preclude a party from introducing contrary evidence and in effect, directing a

finding of indisputability is that a DGE not be under human control. Indeed, the closest language in the Rule that could be said to address issues of control over the DGE refers to facts whose “accuracy cannot reasonably be questioned.”²³

In the case of the inventor’s paper-and-ink logbook, we are presented with a dramatically different schema. Here, we must somehow deal with a purported DGE, which is actually hybrid in nature. A human factor could exert control over the time or content. In the case of the inventor and the logbook, the inventor could alter time or alter, substitute, or delete the content of a document associated with time. Thus, the rules of evidence generally require that there be some extrinsic testimony offered to authenticate records.²⁴ They are not presumed to be valid and may be rebutted by testimonial or documentary evidence.

Fortunately, the development of ever more accurate and wide-ranging technology-based testing methods has aided immensely in ascertaining the provenance of a DGE. By applying scientific techniques (such as testing the age of ink and paper or determining that an ink or paper did not exist at the time it was alleged to have been used), we add natural elements to support or refute the existence of a DGE. The finding will ultimately reveal whether some control could have been exerted on a DGE’s time or content.

Control over time provides the easiest and most complete control over the DGE. If a data generator (such as the inventor who keeps a log) could exert control over the DGE, such control compromises the reliability of any associated content because of the significant potential for time-based data manipulation. For DGEs that occur purely as a result of natural events (for example, sunsets), human control is impossible, and therefore the DGE is completely reliable. This is not the case with physical or electronic data recorded by humans. The following sections will provide an analysis of DGE reliability as it relates to physically created recorded media, electronically generated source data, and issues relating to “auditability” and Sarbanes-Oxley Section 404 compliance.

F. Physical Information or Data

Physical information includes paper and ink, celluloid (that is, film), and other human-readable media. Until a few years ago, most enterprise information and nearly all source data were recorded using paper and ink. Records of all kinds were stored in paper- or celluloid-based media format. Audits were conducted based largely upon observations of physical assets and examinations of paper-and-ink documents, which were often bound in large, tamper-evident and tamper-resistant journals and ledgers. Paper-and-ink documents were a substantial part of the “source data” used by auditors to support opinions and attestations.

verdict against him as to the fact noticed” *United States v. Jones*, 29 F.3d 1549, 1553 (11th Cir. 1994). The example of an event and time of a sunrise would necessarily be categorized as an adjudicative, and not a legislative fact. *See, e.g., LaDuke v. Nelson*, 560 F. Supp. 158, 162 (E.D. Wash. 1982).

23. FED. R. EVID. 201(b).

24. FED. R. EVID. 901.

G. Physical Information and the Data-Generating Event

In the physical world, chemical, spectrographic, and other tests provide reliable and accurate tools to ascertain the time-based legitimacy of a DGE in written media. For example, an inventor seeking to assert a patent infringement claim in federal court produced his inventor's notebooks in compliance with a discovery request.²⁵ A forensic examination of that notebook's entries showed that ink used by the plaintiff-inventor to write a 1988 entry was not commercially available until 1995, and the court invalidated the patent of the plaintiff. In this case, the defendant's experts were able to disprove the creation of a DGE. The time of the inventor's log entry of 1988 could not be associated with the content of the event (that is, the physical composition of ink, which was not released commercially until 1995). As this case illustrates, DGEs are often relatively easy to establish in the world of physically recorded data or information.

H. Physical Information and Source Data

The concept of source data as it relates to physical data, such as paper and ink, is relatively easy to understand and incorporates the concepts of the DGE. At or around the time an event occurs, information is recorded on a physical medium such as paper and ink. This medium is preserved and archived to provide the source information or data about a business process or other transaction involving the creation of information (that is, time and content). In the physical world, these source data are used for auditing, compliance, and evidence production in any legal or regulatory challenge.²⁶

As discussed above, the integrity of paper-and-ink source documents has been significantly enhanced by the development of physical forensic tests to detect forgeries, alterations, deletions, or substitutions. Indeed, many forgeries and scams have been detected by the use of such forensic tools.²⁷ It is nevertheless clear that the generation of paper-and-ink records does not necessarily create DGEs. Indeed, the recent \$16 billion corporate bankruptcy of Parmalat was largely the result of the creation of forged and altered financial documents. This is a clear example of control over a DGE. In fact, Parmalat SPA executives controlled both the time of forged data creation and the content to effectuate a \$5 billion fraud of Parmalat investors worldwide.²⁸

25. See *supra* text accompanying note 17.

26. If the length of time between the event and the recording of the event is protracted, it becomes a recollection. Generally speaking, a recollection is not considered to be source data.

27. See Katherine Ramsland, *The Hitler Diaries*, COURT TV'S CRIME LIBRARY, at http://www.crimelibrary.com/criminal_mind/forensics/literary/6.html?sect=21; Mike Tone, *Brazen Fossil Hunters Are Cleaning Out U.S. Dinosaur Heritage*, THE ATLANTA JOURNAL-CONSTITUTION (Aug. 24, 2001), available at http://news.nationalgeographic.com/news/2001/08/0823_wiredino_hunters.html.

28. Mark Landler et al., *The Rise and Fall of Parma's First Family*, N.Y. TIMES, Jan. 11, 2004, at 3-1.

I. Electronic Information or Data

Virtually all source data now generated by enterprises are electronic or digital, not physical. A University of California study conducted in 2000 showed that 99.993 percent of the three billion gigabytes of data produced worldwide is computer generated.²⁹ Electronic (or digital) data are found in binary notation (ordered sets of zeroes and ones). These binary data are now the source data used by enterprises worldwide to record, store, and use information.

Enterprises currently rely on digitally created data as if they were a naturally occurring DGE, such as a sunrise, or at worst, a hybrid DGE for which traditional evidentiary and forensic techniques are sufficient to establish authenticity. Nothing could be further from the truth. The problem with electronic (or digital) data is that they are, by design, ephemeral in nature. The digital form of data was created in large part to allow for ease of recording, manipulation, substitution, and deletion. Indeed, electronic data are completely human artifices and, as such, provide untrammelled access to DGE manipulation. Without effective internal information-security controls, electronic data content can be created, changed, substituted, or deleted by human hands, often without ways to detect who made the changes and when. Further, in current DGEs, the time associated with data is just as easily manipulated.

Current scientific and evidentiary techniques to detect or weed out DGE manipulations range from inadequate to nonexistent. First, no one can ascertain the "age" of the zeroes and ones that comprise source binary data because these zeroes and ones are volatile and unstable. Second, evidentiary techniques fall far short of providing any real tool for determining either the authenticity or credibility of data content because manipulated data will be the only data available for a trier of fact to consider. The vulnerabilities inherent in digitally generated data leave wide open the potential for undetected (or late-detected) DGE manipulation. In the current data-generating environment, a presumption by enterprises that electronic data are reliable would be invalid.

J. Source Electronic Data Views and Audits

The migration of enterprise source data generation from physical to electronic media is nearly complete.³⁰ However, nearly all current digital data-generating enterprises are exposed to the DGE vulnerability inherent in digital data.³¹ These vulnerabilities call into question the ability of an enterprise to create auditable data. Consequently, they also call into question the ability of an auditor to attest that financial information is presented fairly when issuing an opinion. This problem is pandemic. If a human factor can control either the time or content

29. Peter Lyman & Hal R. Varian, *How Much Information?*, at <http://www.sims.berkeley.edu/how-much-info-2003> (last visited Aug. 24, 2005).

30. *Id.*

31. There has been substantial recognition of the potentials for time-based data manipulation by the banking and finance industry. The ANSI X9F4 standards workgroup published its draft trusted timestamp standard for the banking and finance industry. Copies of the published ANSI Trusted Timestamp Standard are available for purchase at www.x9.org.

element of a DGE, we can no longer be assured that the electronic records offered for audit are reliable within the definitions in Concepts of Financial Accounting³² or in compliance with the new internal controls provisions of Sarbanes-Oxley Section 404.

K. The Distinction Between Electronic Source Data and “Views”

An additional complication is intrinsic to electronic data used for audit and compliance purposes. Binary source data may appear as something like the following:

```
000100101010101111010101001010101011110100000101001
10101001010101010101000000101011011111010101001010101
1010101111110100001010010010100101001010110111010101011
```

They are not easily read by humans. The data above could be from a spreadsheet, a word-processed memorandum, an audit log, or a recipe for dog biscuits.

Examination of the original underlying source records (data) provides more persuasive audit evidence than an examination of copies, summaries, or distillations prepared by clients. The enterprise may not present—and the auditor may not examine—reliable data, and both parties may be unaware of this. Why is this so? To make binary data human (and therefore auditor) readable, the zeroes and ones must be processed at least once and perhaps many times by other computer processes, which create not source data, but a “view” or a distillation of data. A distillation rendering is not the same as source data. Views, which can be read and examined by auditors, are not source data. A view can be a printout of a file or a screen or a human-readable rendering of a spreadsheet, word-processed document, or digital image. This view can be intentionally altered to provide a more favorable picture of the financial condition and operation of the

32. FINANCIAL ACCOUNTINGS STANDARDS BOARD, STATEMENT OF FINANCIAL ACCOUNTING CONCEPTS NO. 2, at 6 (1980):

Reliability

- The reliability of a measure rests on the faithfulness with which it represents what it purports to represent, coupled with an assurance for the user that it has that representational quality. To be useful, information must be reliable as well as relevant. Degrees of reliability must be recognized. It is hardly ever a question of black or white, but rather of more reliability or less. Reliability rests upon the extent to which the accounting description or measurement is verifiable and representationally faithful. Neutrality of information also interacts with those two components of reliability to affect the usefulness of the information.
- Verifiability is a quality that may be demonstrated by securing a high degree of consensus among independent measurers using the same measurement methods. Representational faithfulness, on the other hand, refers to the correspondence or agreement between the accounting numbers and the resources or events those numbers purport to represent. A high degree of correspondence, however, does not guarantee that an accounting measurement will be relevant to the user’s needs if the resources or events represented by the measurement are inappropriate to the purpose at hand.

company. Unfortunately, without information about the security controls around this view, the auditor has no basis to evaluate its reliability.

Thus, the auditor might not be auditing original documents. Even more dangerous, without appropriate information-security controls, no auditor, CEO, or computer expert can examine these zeroes and ones and state, with any reasonable assurance, that they represent a spreadsheet, a digital image, or a record of an actual transaction that occurred in the real world. The views the auditors see are more like the world of the *Matrix*³³ and its characters; the auditors have no way of knowing whether the views they see are reality or illusions created to control them.

An auditor must have some way to determine that the view he or she sees is reliable, and an enterprise must have some way to prove it. If an enterprise merely assumes views of electronic data are reliable, such reliance constitutes a *prima facie* case for a potential violation of the internal controls provisions of Section 404 of Sarbanes-Oxley. In our view, an auditor who relies on views without understanding, documenting, and testing the internal controls over the reliability of such views is also in violation of the provisions of Sarbanes-Oxley.

L. Electronic Data and the Data-Generating Event

Compounding the “source data” versus “view” issue is a related vulnerability unique to digital data. In the digital universe, the binding of time with content to create a DGE is very weak and inherently unreliable. What has been formerly considered inseparable in nature (that is, the time of a sunrise and the sunrise itself) or established for physically recorded media by ink and paper testing is no longer inseparable. In the digital world, *both time and content are under the control of the enterprise generating the data*. Therefore, both the time and the content of digital data can be “unlocked” and readily manipulated by resetting the system or network clock. If the control of time in a digital data-generating environment is under enterprise control, the ability to bind time strongly with content is missing. Therefore “when” and “what” have no meaning because data can be created *nunc pro tunc*, or “now for then.”

M. Electronically Produced “Hard Copies”—Paper-Based Records Now at Risk

With the cascading revelations of the high-profile, time-based data manipulation schemes of the past few years, it has become increasingly apparent that paper printouts produced as records are as unreliable as the electronic data from which they are derived. If the source data from which a paper record is produced is not auditable, we are again looking at examining and relying upon a view, albeit physically produced. Paper-based records generated from digital data are as suspect of DGE manipulation as the digital data from which they are produced. Witness the Parmalat debacle, where the CEO and CFO scanned Bank

33. *The Matrix* (Warner Brothers Studios 1999) (“The Matrix is the world that has been pulled over your eyes to blind you from the truth.”)

Nearon et al.

of America letterhead and the signatures of officials to create a paper document that attested to the existence of a nonexistent Cayman Island bank account containing \$5 billion.³⁴ Parmalat declared bankruptcy.

N. Time-Based Data Manipulation and Sarbanes-Oxley Section 404

The potential for time-based manipulation is easily realized and therefore significantly reduces the reliability and auditability of electronically generated source data. This creates a material weakness that could affect internal controls sufficiently to create a material misstatement or misrepresentation, which in turn could trigger Sarbanes-Oxley Section 404 liability for the executive level of the reporting enterprise as well as its auditors.

O. Sarbanes-Oxley Implications

The Sarbanes-Oxley Act outlaws, among other things, fraud by CEOs or auditors of covered public companies. The implications for both CEOs and auditors as they relate to electronic data-generating environments are grave. First, it may be argued that the provision by the enterprise of views for audit, and the corresponding audit of views by auditors, constitute *prima facie* violations of Sarbanes-Oxley Section 302. This is because certifications are not being made on reliable business documents but on unreliable views. Second, the government and the courts traditionally have recognized that internal control requirements apply to electronic information-security infrastructures.³⁵ If material weaknesses (for example, the ready ability of an insider to reset a system clock and undetectably alter, delete, or substitute digital accounting records) could lead to a material misstatement (as it has in the cases previously cited), a Sarbanes-Oxley violation might ensue.

The emergence of digital accounting records as source data by entities covered by Sarbanes-Oxley presents significant compliance challenges. First, if the premise of this Article is correct, covered entities must document, assess, and test information-security controls as part of the basis for complying with Sarbanes-Oxley. Second, because electronic information is perhaps a covered entity's most important asset, the CEO is now under a heightened burden, pursuant to Section 404, to certify that no material weaknesses of controls exist within the entity's information-security infrastructure that might result in a material misstatement.

34. See Landler et al., *supra* note 28.

35. U.S. TREASURY, TREASURY DIRECTIVE 87-05, ELECTRONIC COMMERCE INITIATIVES (Apr. 21, 2001), available at <http://www.ustreas.gov/regs/td87-05.htm> (last visited Aug. 8, 2005) ("Treasury bureaus should follow the guidance of TD 80-05 and TD P 80-05, which address statutory record requirements. In addition, retention of financial documents should also follow the relevant guidance provided by the General Accounting Office. Unless otherwise stated, these requirements apply to all electronic information systems and should be adhered to by Treasury bureaus.").

II. SECTION 404—ANALYSIS AND REQUIREMENTS

In a mere 173 words, Section 404 of the Sarbanes-Oxley Act gets at the heart of the Act's intent, which is "to protect investors by improving the accuracy and reliability of corporate disclosures."³⁶ It requires the SEC to establish rules requiring public companies to include in their annual filing an internal control report that states management's responsibility for internal control over financial reporting. It also requires management to assess the effectiveness of internal controls as of the end of the issuer's most recent fiscal year. Public company auditors are required to attest to and report on management's assessment of internal control as part of the annual financial statement audit.³⁷ Section 404 attempts to improve the accuracy and reliability of financial reporting by improving the process of recording transactions and preparing financial statements.

The SEC adopted final rules to implement Section 404 on June 5, 2003, effective on August 14, 2003.³⁸ Section 302 of the Act requires management to certify that they have evaluated the effectiveness of internal controls within 90 days prior to the report.³⁹ The rules adopted by the SEC in August 2003 require companies to disclose in their quarterly and annual filings changes in internal control that could affect controls in future periods, as well as changes made to correct significant deficiencies and material weaknesses.⁴⁰

A. Defining "Internal Controls over Financial Reporting"

Under Section 404, a key issue for management and auditors is the definition of "internal controls." The proposed final rules discuss the development of the theory of internal control: "From the outset, it was recognized that internal control is a broad concept that *extends beyond the accounting functions of a company.*"⁴¹ In developing its definition of "internal control," the SEC considered accounting control as codified in the Foreign Corrupt Practices Act (FCPA).⁴² The FCPA was intended to improve the accuracy of companies' accounting records and the

36. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745, 745.

37. 15 U.S.C.A. § 7262(b) (West 2005).

38. *Final Rule on Management's Report*, *supra* note 12, at 36,636.

39. 15 U.S.C.A. § 7241(a)(4)(C) (West 2005).

40. *Final Rule on Management's Report*, *supra* note 12, at 36,646, 36,647. The compliance dates were June 15, 2004, for accelerated filers and April 15, 2005, for companies that are not accelerated filers and for foreign private issuers. *Id.* at 36,651. Companies considered "accelerated filers" meet the following criteria: (1) those that have a public float of \$75 million or more and that have been a public company for at least 12 months; (2) those that have filed at least one annual report with the SEC; and (3) those that are not permitted to use small business issuer forms. Cooley Godward LLP, *The Sarbanes-Oxley Act of 2002: SEC Issues Final rules Regarding Internal Control Over Financial Reporting Under Section 404*, Cooley Alerts (Aug. 4, 2003), at <http://www.cooley.com/news/alerts.aspx?ID=38005220>. However, in February 2004, the SEC issued a revised rule postponing the compliance dates for accelerated filers to November 15, 2004, and for nonaccelerated filers to July 15, 2005. 69 Fed. Reg. at 9,722.

41. *Final Rule on Management's Report*, *supra* note 12, at 36,638 (emphasis added).

42. Foreign Corrupt Practices Act of 1977, Pub. L. No. 95-213, 91 Stat. 1494 (codified in scattered sections of 15 U.S.C.).

reliability of auditing.⁴³ Not coincidentally, this is almost identical to the intent of Sarbanes-Oxley: both acts were Congress's reaction to national scandals—the FCPA to Watergate in 1973; and Sarbanes-Oxley to Enron, Andersen, WorldCom, and the other infamous spectacular financial frauds and audit failures in 2001 and 2002.

The FCPA requires companies subject to Section 12 of the Securities and Exchange Act or those required to file under Section 15(d) “to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that—

- (i) transactions are executed in accordance with management's general or specific *authorization*;
- (ii) transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for assets;
- (iii) access to assets is permitted only in accordance with management's general or specific *authorization*; and
- (iv) the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.”⁴⁴

The SEC also considered the work done by the Committee of Sponsoring Organizations (COSO) of the National Commission on Fraudulent Financial Reporting (Treadway Commission). Between 1987 and 1992, the committee developed a common definition of “internal control” and a broad framework that companies, auditors, regulators, and others could use to evaluate the effectiveness of internal control. The final document came to be known as “COSO.” In *Internal Control—Integrated Framework*, “internal control” is defined as:

A process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in three categories—effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.”⁴⁵

According to COSO, the key components of internal control are (1) the control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring.

43. Specifically:

The Foreign Corrupt Practices Act of 1977 was enacted principally to prevent corporate bribery of foreign officials. This act had three major parts: 1. It required the keeping by corporations of accurate books, records, and accounts; 2. It required issuers registered with the Securities and Exchange Commission to maintain a responsible internal accounting control system; and 3. It prohibited bribery by American corporations of foreign officials.

MICHAEL V. SEITZINGER, CONGRESSIONAL RESEARCH SERVICE REPORT TO CONGRESS: FOREIGN CORRUPT PRACTICES ACT 1 (1999), available at <http://www.fas.org/irp/crs/Crsfcpa.htm> (last visited Aug. 22, 2005).

44. Securities Exchange Act of 1934, 15 U.S.C. § 78(m)(b)(2)(B) (2000) (emphasis added).

45. COMMITTEE OF SPONSORING ORGANIZATIONS (COSO), INTERNAL CONTROL—INTEGRATED FRAMEWORK 3 (1992).

In considering COSO, the SEC interpreted the five key elements as not limited to traditional financial accounting controls and widened the scope of internal control to “policies, plans, procedures, processes, systems, activities, functions, projects, initiatives, and endeavors of all types at all levels of a company.”

In adopting its final rules, the SEC decided to use the term “internal control over financial reporting,” which is defined as:

A process designed by, or under the supervision of, the registrant’s principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant’s board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that: (1) Pertain to the *maintenance of records* that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant; (2) Provide reasonable assurance that transactions are *recorded* as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the registrant are being made only in accordance with *authorizations* of management and directors of the registrant; and (3) Provide reasonable assurance regarding *prevention or timely detection of unauthorized acquisition, use or disposition* of the registrant’s assets that could have a material effect on the financial statements.⁴⁶

The final rule’s definition of “internal control” excludes two of COSO’s three objectives of internal control: effectiveness and efficiency of operations and compliance with laws, rules, and regulations (except for compliance with laws, rules, and the SEC’s requirements related to financial reporting). To ensure that companies, auditors, investors, and others understand that safeguarding assets is a key element of internal control over financial reporting, it is explicitly included in the final rule.

III. THE INTERRELATIONSHIP BETWEEN SECTION 404 AND INFORMATION SECURITY

To satisfy Section 404, management’s assessment of internal control over financial reporting and the auditor’s audit of internal control over financial reporting should include adequate InfoSec controls. The use of information technology to process and store financial accounting information is nearly universal. Although public companies are not subject to the standards that govern audits of government entities and recipients of public funds, it is significant that these standards clearly recognize the risks that information technology poses to financial information. According to the Generally Accepted Government Auditing Standards, Amendment 1, “[t]he new standard should heighten auditors’ awareness of the risks associated with auditing in the environment of computer-

⁴⁶ *Final Rule on Management’s Report*, *supra* note 12, at 36,640 (emphasis added) (citation omitted).

ized information systems that is *pervasive* today.”⁴⁷ E-mail and Internet access are nearly universal on finance and accounting department workstations that record, process, report, or store financial accounting and insider information. The information-security controls over this information are a material component of internal control over financial reporting. If management and the auditor do not assess and audit these controls, users of management’s certification and the auditor’s attestation may be uninformed of material weaknesses that may affect the reliability of financial reports. If management and the auditor are unaware of these weaknesses, they cannot report them.

A. Maintaining Records

Ninety-three percent of today’s business records are estimated to be in digital form.⁴⁸ The percentage of records that support the transactions and dispositions of the assets of registrants that are digital is probably similar. Maintaining records means keeping the records in existence and preserving them, as well as maintaining equipment capable of accessing them. Because accounting records are most likely created and maintained with information technology, it stands to reason that to assess and audit controls over record maintenance, one would have to understand the information-security controls over them. The objectives of such information-security controls are, at minimum: (1) *integrity*: the information has not been subject to unauthorized change, alteration, or deletion; (2) *confidentiality*: the information is not disclosed to parties that do not have a legitimate purpose to know such information; and (3) *availability*: the information is available to those who have a need to use such information in a timely fashion.

In this regard, the objectives of information-security controls inevitably intersect with the definition of “internal control over financial reporting” in that they seek to provide reasonable assurance that the financial accounting records are maintained in an accessible format (*availability*) and are accurate (*integrity*). Fairness, on the other hand, may not be achieved with information-security controls because the fairness of the supporting records is subject to human judgment and intentional and subconscious bias such as for estimates, valuation, inclusion, exclusion, or recognition. Accordingly, if management and the auditor fail to document, assess, and test information-security controls over the maintenance of digital accounting records that support the financial statement, their work is fundamentally incomplete.

B. Recorded Transactions and Digital Records

Internal control over financial reporting should provide reasonable assurance that transactions are recorded in accordance with generally accepted accounting

47. COMPTROLLER GENERAL OF THE U.S., U.S. GENERAL ACCOUNTING OFFICE, GOV’T AUDITING STANDARDS, AMENDMENT NO. 1: DOCUMENTATION REQUIREMENTS WHEN ASSESSING CONTROL RISK AT MAXIMUM FOR CONTROLS SIGNIFICANTLY DEPENDENT UPON COMPUTERIZED INFORMATION SYSTEMS 2 (1999) (emphasis added).

48. Michele C.S. Lange, *New Act Has Major Impact on Electronic Evidence: Several Provisions of Sarbanes-Oxley Govern Document-Retention Policies*, 26 NAT’L L.J., Nov. 4, 2002, at C8.

principles. The principle of periodicity requires that transactions be recorded and recognized in the proper accounting period. The transaction date field in an accounting record generally establishes the period in which a transaction will be reported. For some entities, such as those that use e-commerce, e-business, and EDI, all evidence of transactions conducted with these technologies is likely to be digital. If management and the auditor test these transactions by merely viewing computer screen shots or inspecting hard copy printouts of digital records, then such tests are not credible without consideration of the information-security controls over the generation of such evidence. Management could easily fabricate a digital view of a transaction and all supporting documentation to make it appear the transaction occurred in any time period⁴⁹ or for any amount.⁵⁰

For other transactions initiated manually and evidenced with a hard copy document, the hard copy may be digitally imaged and destroyed or made otherwise unavailable. Digital evidence is easy to alter, even for a novice, and alterations are difficult to prevent or detect without proper information-security controls. As discussed, the date of recorded transactions could easily be altered to manipulate income. This is not just a theoretical risk; resetting the computer's time clock to commit financial fraud is common. For example, in *Canary*, programmers installed software to automatically record trades made after the market closed but that were made to appear as if they had occurred before the closing bell.⁵¹

Given the importance of the date that revenue is recognized and recorded, the role date manipulation has played in financial fraud, and the ease by which the date can be manipulated, controls over the computer's time-generating device are crucial in achieving the objectives of internal control over financial reporting. As such, management's assessment, documentation, and testing and the auditor's examination are not complete without considering information-security controls over date generation.

The risk of altering digital accounting records is not limited to the date. In fact, alteration of almost any digital accounting data, such as account number, payee name, customer name, customer address, or even board minutes, is as easy as a mouse click. On the other hand, prevention and detection of such alteration is extremely difficult without information-security controls.

C. Authorizing Transactions

According to the final rules, internal control over financial reporting includes "policies and procedures that: . . . [p]rovide reasonable assurance that receipts and

49. Randall Smith, *Spitzer, SEC Charge Fund-Case Broker*, WALL ST. J., Sept. 17, 2003, at C1.

50. See Landler et al., *supra* note 28.

51. Smith, *supra* note 49; see also DAVID PRIEBE ET AL., *Corporate Governance Reform and Electronic Documents*, in THE ABA INFORMATION SECURITY COMMITTEE'S TREATISE ON DIGITAL EVIDENCE ___ n.7 (forthcoming) (citing In the Matter of Thomas H. Pike, Securities Exchange Act of 1934, Release No. 39793 (Mar. 25, 1998) ("At the end of each quarter, Sensormatic turned back the computer clock that dated and recorded shipments. Based on these computer-generated documents reflecting shipments, Sensormatic then prematurely recognized revenue on shipments made past the end of the quarter.")).

expenditures of the registrant are being made only in accordance with *authorizations* of management and directors of the registrant.”⁵² Documentation of authorization is typically evidenced by sign-off and, in many financial accounting processing systems, may be performed explicitly by a user clicking on a checkbox in an online form or implicitly through access rights granted to certain menu functions. Prior to digital records, authorization was evidenced by a signature, initials made in pen and ink on paper by the authorizers, or a stamp that made a physical imprint on paper. Authorization was difficult to forge, and advancements in certain forensic technologies made detection easier. This is not the case for digital authorizations. Given the nature of digital records, forged authorizations are simple to make and difficult to detect. In fact, without understanding and testing controls over digital authorizations, management and the auditor would have no basis to rely on digital evidence of such authorizations. The concept of authorization is rife with complexities in the case of computers and the Internet.⁵³

Suppose a company has granted all accounting personnel full access rights to all accounting functions. Suppose, too, that such rights allow an employee to establish a vendor, change vendor addresses, print checks, and adjust accounts receivable. If the employee establishes a fraudulent vendor, issues a check to such a vendor, or pockets a collection and makes an adjustment to accounts receivable, has the employee acted “without authorization”? This case involves understanding what authorization means and how it relates to employee misconduct. Kerr analyzed case law involving this issue and finds that in all of these cases, employees have misused their employer’s computers by entering commands and viewing information they were not supposed to, at least in the circumstances (or for the reasons) present.⁵⁴

If the above example were viewed within an agency theory framework, the employee’s actions would be considered “unauthorized”: “Unless otherwise agreed, the authority of an agent terminates, if, without the knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.”⁵⁵

In the case Kerr reviews, *State v. Olson*,⁵⁶ the company did not explicitly limit computer access. In *Olson*, the court concluded, that authorized access to a computer for an unauthorized purpose does not constitute “unauthorized access” in the absence of an explicit workplace rule that conditions computer use on the use of data.⁵⁷ Therefore, if management does not assess controls over information-technology *authorization*, and the auditor does not audit it, they may not have a basis to conclude that controls over receipts and expenditures of the registrant are being made only in accordance with *authorizations*.

52. *Final Rule on Management’s Report*, *supra* note 12, at 36,640 (emphasis added).

53. See Orin S. Kerr, *Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1617–20 (2003).

54. *Id.* at 1632–38.

55. *Id.* at 1633 (citing RESTATEMENT (SECOND) OF AGENCY § 112 (1958)).

56. 735 P. 2d. 1362 (Wash. Ct. App. 1987).

57. *Id.* at 1365.

D. Prevention of Unauthorized Acquisition, Use, and Disposition of Assets

It has been estimated that 70 percent of current market capitalization is derived from information assets.⁵⁸ If reported in the financial statements—which they may not be—the value of these assets is impounded in intangible assets.⁵⁹ Even if not included in goodwill, prospective cash flows derived from these assets are implicitly impounded by investors in share prices. Much of these assets are stored in digital form, including human resource records, customer lists, price lists, vendor lists, proprietary software, and research and development records.⁶⁰ Access, breach, and disclosure of information assets to competitors or other outsiders often impair the value of these assets. One objective of information-security controls—*confidentiality*—seeks to prevent unauthorized acquisition and use of information assets.

Does “unauthorized access” to information assets constitute unauthorized acquisition, use, or disposition of corporate assets? The few courts that have reached these questions have offered inconsistent interpretations.⁶¹ It is clear that an insider who copies the customer database or proprietary software and sells it to a competitor has acquired and used it. However, it is not certain that if the company loses sales or its competitive position as a result of this, that there has been disposition of corporate assets. Companies routinely grant users broad access to information assets, and actual audits have found that management rarely implements adequate preventive and detective information-security controls. Information assets constitute a significant portion of the company’s market value; therefore, management and the auditor’s internal control work is not complete without considering preventive and detective controls over these assets.

Because almost all financial accounting systems control cash disbursements and maintain account receivables with information technology, access to these assets and authorization by management and directors of the registrant is achieved with various information-security controls, for example, user names and passwords, file and information technology resource permissions, firewalls, routers, and virtual private networks (VPNs). Information technology is an integral part of financial reporting and preparing financial statements. Information-security controls are critical to the reliability of financial reporting because of the inherent characteristics of digital records. If these controls are

58. Kevin Kalinich, *E-Business Risk Insurance: Are There Gaps in Your Business Insurance Program?*, Aon FSG Technology and Professional Risks (July 2003).

59. FINANCIAL ACCOUNTING STANDARDS BOARD OF THE FINANCIAL ACCOUNTING FOUNDATION, STATEMENT OF FINANCIAL ACCOUNT STANDARDS No. 142: GOODWILL AND OTHER INTANGIBLE ASSETS 31 (2001) (“the costs incurred to develop intangible assets which are not specifically identifiable [are required to be] recognized as expenses”— this generally means that unless intangible assets are purchased in a business combination, they will not appear on the face of the financial statements. Otherwise, the value of such intangible assets acquired in a merger or acquisition are generally included in the financial statement caption “Goodwill” in the balance sheet.), available at <http://www.fasb.org/pdf/fas142.pdf>.

60. BLAIR & WALLMAN, *supra* note 16, at 25, 52, 54, 62.

61. See Kerr, *supra* note 53.

weak or nonexistent, assets are at risk to unauthorized disposition. For example, the disposition of cash is ordinarily made through issuing checks. To issue a check, a vendor must exist or be established, a payable created, and a check printed and signed. If an individual can gain access to the underlying files or the menus that create these, half the battle is won. In many companies even the signing of checks under a certain amount is done digitally. The preventive control over this process limits access to underlying files and menus. Unfortunately, many companies grant all or many employees complete access to the underlying files and menus. If management and the auditor fail to consider information-security controls over disposition of assets controlled by information technology, their assessment and audit is incomplete.

E. Detection of Unauthorized Acquisition, Use, or Disposition

The previous section discussed the importance of security and control of information and financial assets. Can information-security controls detect unauthorized acquisition, use, or disposition of such assets? Perhaps. Operating systems and applications have the ability to record, via auditing logs, when users access the system and which activities they perform. If there are integrity and continuity controls over the logs and someone independent of the activity being logged reviews them, the probability that unauthorized activity will be detected is increased. However, management often relies on reviews of printed reports, such as payables lists and check registers, to detect unauthorized disbursements. Someone who has access to the underlying records as well as the report masks can alter them. Unless management and the auditors factor in this possible scenario, they might reach false conclusions and be unaware of ineffective detective controls.

IV. SECTION 302 ANALYSIS

Although Section 404 is clearly concerned with processes and procedures that may affect financial reporting, Section 302 can claim an equal or greater role in mandating greater corporate information security. First, Section 302 also contains provisions regarding the adequacy and effectiveness of internal controls over financial reporting. While Section 404 requires affected companies, on an annual basis, to file an “internal control report,”⁶² Section 302 and its implementing rules require establishment of this financial control structure. Thus, with regard to financial controls, Sections 302 and 404 complement and support each other.

Second, Section 302 requires the principal executive and financial officers of public companies to certify that they have taken the required actions with respect to their company’s internal control. Most importantly, Section 302

62. 15 U.S.C.A. § 7262(a) (West 2005) (an internal control report states management’s responsibility for establishing and maintaining an adequate internal control structure for financial reporting as well as management’s assessment of the effectiveness of that internal control structure).

mandates processes to ensure that material information regarding a company's operations and internal controls are appropriately assessed and disclosed in the company's periodic SEC filings. Both financial and nonfinancial information are collected, analyzed, and presented, if appropriate. The information-technology function is implicated in this process not only because any such "information" resides almost exclusively within the confines of the corporate information-technology infrastructure, but also because events which may adversely affect the security of a company's information-technology infrastructure are potentially reportable on the company's periodic reports. Where such information is potentially reportable, Section 302 requires the establishment of policies and procedures that will enable such events to be disclosed.

A. What the Rules Require

Section 302 of the Sarbanes-Oxley Act is sometimes viewed, incorrectly, as merely a certification requirement. However, as implemented by the SEC's rules, Section 302 mandates the establishment of processes, procedures, and controls over all information that is material to the fair and accurate presentation of the company's financial condition and the results of its operations. Section 302 requires that the "principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions" certify six facts concerning a company's "internal controls."

The SEC rules effectuating Section 302 define "internal controls" to cover both "material non-financial information, as well as financial information." The SEC rule implementing Section 302(a)(4) uses the term "disclosure controls and procedures," while the rule implementing Sections 302(a)(5) and (6) uses the term "internal control over financial reporting."⁶³

Under the SEC's rules implementing Section 302, the principal corporate officers must certify that they or the corporation itself has undertaken certain actions.⁶⁴ The terms of the required certification are defined by statute and must be worded exactly as specified. Officers must certify that they are "responsible for establishing and maintaining disclosure controls and procedures . . . and internal control over financial reporting" with respect to internal control over financial reporting paragraphs 4(b), (d), and 5 of the specified certification require the certifying officials to aver that they have "designed such internal control over financial reporting . . . to provide reasonable assurance regarding the reliability of financial reporting . . . disclosed . . . any change in the registrant's internal control over financial reporting that . . . has materially affected or is reasonably likely to materially affect the registrant's internal control over financial reporting"⁶⁵

63. These terms relate to Exchange Act rules 13(a)-15 and 15(d)-15, which define "disclosure controls and procedures" (17 C.F.R. §§ 240.13a-15(e), 15d-15(e) (2005)) as well as the term "internal control over financial reporting" (17 C.F.R. §§ 240.13a-15(f), 15d-15(f) (2005)). See *Final Rule on Management's Report*, *supra* note 12, at 36,638.

64. 17 C.F.R. § 228.601(b)(31) (2005).

65. § 228.601(b)(31) ¶¶ 4(b), 4(d), 5.

Finally, the certifying officers must state that they have “disclosed based on [their] most recent evaluation of internal control over financial reporting . . . all significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant’s ability to record, process, summarize and report financial information.”⁶⁶

Taken together, the certifications required by Section 302 impose, at least implicitly, far-reaching and significant responsibilities for the establishment, maintenance, and evaluation of internal controls over financial reporting. The SEC rules go even further. Exchange Act Rules 240.13a-15 and 240.15d-15, which implement Section 302 of the Act, mandate that the public companies themselves, and not merely the certifying officers

must [1] maintain disclosure controls and procedures . . . and internal control over financial reporting . . . [2] evaluate . . . the effectiveness of the issuer’s disclosure controls and procedures . . . [3] evaluate . . . the effectiveness . . . of the issuer’s internal control over financial reporting . . . [4] evaluate . . . any change in the issuer’s internal control over financial reporting . . . that has materially affected, or is reasonably likely to materially affect [internal controls over financial reporting] . . .⁶⁷

Thus, these rules mandate the establishment and periodic evaluation for effectiveness of disclosure controls and procedures as well as processes for internal control over financial reporting.

Given that corporations and their executive officers must implement internal controls, the question becomes, Are information-security practices and procedures encompassed within the definition of either “disclosure controls and procedures” or “internal control over financial reporting”? With respect to internal control over financial reporting, the question is readily answered in the affirmative. As discussed more fully in connection with Section 404, there are both strong historical and interpretive arguments for concluding that corporate information-security practices and procedures are included within “internal controls.” One argument is that “internal control over financial reporting” includes those policies and procedures that:

- (1) Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer; (2) [p]rovide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer’s assets that could have a material effect on the financial statements.⁶⁸

66. § 228.601(b)(31) ¶ 5.

67. 17 C.F.R. §240.13a-15 (2005).

68. 17 C.F.R. § 240.13a-15(f) (2005).

In the modern corporation, information-security practices and procedures not only are implicated in these goals but are essential to them. Additionally, almost all customer and other transactions—from the recordation of sales on the Internet (point of contact sales) to inventory management and control—are computer-driven or controlled. The integrity of the data underlying these transactions can only be assured if effective information-security policies and procedures are implemented.

B. Disclosure Controls

In addition to the requirement that a company establish processes to ensure internal control over financial reporting, which by its very nature implicates information technology and thus information security, the regulations implementing Section 302 of the Sarbanes-Oxley Act also require companies to implement “disclosure controls and procedures.” The policies, procedures, and practices necessary to secure modern corporations’ information assets fall within the regulatory definition of disclosure controls and procedures. Exchange Act Rule 240.13(a)-15(e) defines “disclosure controls and procedures” as “controls and other procedures . . . that are designed to ensure that information required to be disclosed . . . is recorded, processed, summarized and reported” The principal securities laws of the United States require public companies to provide full and fair disclosure of material information to potential investors about their financial condition and results of operations. Under SEC regulations, companies must disclose their evaluation of known trends, demands, commitments, events, or uncertainties that are likely to have a material effect on their financial condition and operations.⁶⁹ Threats to the security of digital information assets carry the potential to cause such a material impact. The generally accepted definition of “information security” is a system or process designed to ensure the confidentiality, integrity, and availability of information.⁷⁰ Effective information-security practices and procedures must therefore be established if related information-security threats can be disclosed.

Should there be any doubt that threats related to information security are “disclosable” under the securities regulations, in 1998, the SEC released *Interpretation: Disclosure of Year 2000 Issues and Consequences by Public Companies, Investment Advisors, Investment Companies and Municipal Securities Issuers*.⁷¹ This publication analyzed the effect of the so-called “Year 2000 problem” on the disclosure obligations of public companies. The SEC set out to answer two questions: (1) whether Year 2000 issues were required to be disclosed and (2) if so, what was the nature of the disclosure to be made. With respect to the first question, the SEC stated: “a company must provide Year 2000 disclosure if:”

69. 17 C.F.R. §§ 228.303(b), 229.303(a)(1) (2005).

70. IBM DICTIONARY OF COMPUTING (George McDaniel ed. 1994) (defines information security as, “[t]he concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use.”).

71. 63 Fed. Reg. 41,394 (Aug. 4, 1998).

(1) Its assessment of the Year 2000 issues is not complete, or (2) [m]anagement determines that the consequences of its Year 2000 issues would have a material effect on the company's business, results of operations, or financial condition, without taking into account the company's efforts to avoid those consequences.⁷²

The SEC reached this conclusion, in principal part, by applying its guidelines for completing Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A). The MD&A requires management to discuss various matters in its periodic reports including matters that might be "forward looking." The definition of "forward-looking information" includes the concept of known material events, trends, or uncertainties.⁷³ Like the Year 2000 threat, current information-security threats (such as viruses, denial of service attacks, hacking, industrial espionage, and fraud) faced by public companies and their information-technology systems are known events, trends, or uncertainties and must therefore be disclosed if management determines that the potential consequence of each event would have a material effect on a company's business.

We do not argue that every information-security event is or should be disclosable, only that events related to information security are potentially disclosable and must be evaluated by management. Under the rules implementing Section 302 of the Sarbanes-Oxley Act, if an event or class of events is potentially disclosable, disclosure controls and procedures must be put into place to collect and analyze information about these events. Moreover, the key factor in determining whether an information-security event should be disclosed is management's determination of the potential consequences of that security event on the company. Without appropriate information-security practices and procedures, including vulnerability and risk assessment procedures, management cannot make a meaningful evaluation on this issue.

In its earlier analysis, the SEC also discussed what information regarding the Year 2000 security problem needed to be disclosed. While concluding that "[t]he disclosure should be specific to each company and quantified to the extent practicable," the Commission determined four categories of information to be discussed for the disclosure to be "meaningful":⁷⁴ (1) the company's state of readiness, (2) the costs to address the company's Year 2000 issues, (3) the risks of the company's Year 2000 issues, and (4) the company's contingency plans.⁷⁵ These categories are characteristic not only of Year 2000 issues but of virtually all information-security threats. That being the case, the nature of the information that must be disclosed is a critical factor in determining the nature of the system needed to collect that information. This kind of information is most efficiently collected and analyzed through the establishment and maintenance of appropriate information-security practices and procedures.

72. *Id.* at 41,396.

73. *Id.* at 41,398.

74. *Id.* at 41,399.

75. *Id.* at 41,399–41,400.

In conclusion, Section 302 of the Sarbanes-Oxley Act and its implementing regulations mandate the establishment, maintenance, and assessment of effective information-security practices and procedures for two reasons: (1) such procedures are an essential component of a public company's internal control over its financial reporting and (2) such practices and procedures constitute the disclosure controls required to evaluate the disclosability of information-security threats.

V. WHAT ARE "UNAUTHORIZED ACCESS" AND "UNAUTHORIZED ACQUISITION"?

As we have repeatedly noted, according to Section 404, entities covered by Sarbanes-Oxley must maintain "adequate internal controls over financial reporting" and "the accuracy and timeliness of financial reporting is . . . heavily dependent on a *well-controlled* information technology environment."⁷⁶ Further, all documents relating to financial reporting produced by an entity's information-technology system⁷⁷ must have, as its core element, "data integrity."⁷⁸ Auditors, directors, and investors, among others, must have reasonable assurance that the records supporting the financial information they use have not been accessed, altered, acquired, or created in an unauthorized manner. This requirement specifically applies to assets, as noted in the SEC's Final Rules: "Provide reasonable assurance regarding *prevention or timely detection of unauthorized acquisition, use or disposition* of the registrant's assets that could have a material effect on the financial statements."⁷⁹ Yet, while it is clear that Section 404 mandates that covered entities prevent "unauthorized" access to a registrant's assets, ascertaining exactly what "unauthorized access" is turns out to be no simple matter.

A. "Unauthorized Access" in a Digital Context

A corporate entity's governance documents and its computer use policy must provide more guidance than simply mandating that there must be no unauthorized access to company assets. Rather, it is in a company's interest to spell out with as much clarity as possible what is meant by "unauthorized access." Its computer-

76. IT GOVERNANCE INSTITUTE, IT CONTROL OBJECTIVES FOR SARBANES-OXLEY: THE IMPORTANCE OF IT IN THE DESIGN, IMPLEMENTATION AND SUSTAINABILITY OF INTERNAL CONTROL OVER DISCLOSURE AND FINANCIAL REPORTING 5 (2004) (emphasis added).

77. *See, e.g.*, 40 U.S.C.A. § 11101(6)(A) (West 2005) ("any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by [an] executive agency").

78. A definition of data integrity is "1. [The] condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [INFOSEC-99]. 2. The condition in which data are identically maintained during any operation, such as transfer, storage, and retrieval. 3. The preservation of data for their intended use. 4. Relative to specified operations, the *a priori* expectation of data quality." ATIX Committee TIAI, *Data Integrity*, Telcom Glossary 2K (Feb. 28, 2001) at http://www.atix.org/tg2k/_data_integrity.html.

79. *Final Rule on Management's Report*, *supra* note 12, at 36,640 (emphasis added).

use policy also should specify that it specifically applies to information assets and electronic accounting records. Such efforts may be rewarded in the event of future disputes, and a company defining “unauthorized access” should seek to stay as close to the courts’ definitions of the term as possible. Unfortunately, the few attempts by courts to define the term “unauthorized access” have produced divergent interpretations,⁸⁰ and little scholarly attention has been directed to the matter.⁸¹

B. Judicial Interpretations of “Unauthorized Access”

In *State v. Allen*,⁸² the Kansas Supreme Court implied that “access” meant *successfully* obtaining data from “inside” the computer.⁸³ The Court declared that “[u]ntil [the defendant] proceeded beyond the initial banner and entered appropriate passwords, he could not be said to have had the ability to make use of Southwestern Bell’s [computer system] . . . as gaining access is commonly understood.”⁸⁴ In *State v. Riley*,⁸⁵ however, the Washington Supreme Court came to the opposite conclusion on similar facts. In both cases, the defendants were charged with computer crime after allegedly connecting with telephone company computer networks.⁸⁶ The statutes of the two states defined “access” almost identically.⁸⁷ Yet, the Washington court found that “Riley’s repeated attempts to discover access codes by sequentially entering random 6-digit numbers constitute ‘approach[ing]’ or ‘otherwise mak[ing] use of any resources of a computer.’ Therefore, Riley’s conduct satisfied the statutory definition of ‘access’ and so was properly treated as computer trespass.”⁸⁸

How a publicly traded company’s information-security policy defines “access” is relevant to, among other things, the standard of monitoring (primarily via reviews of audit logs) to which a company commits itself. The *Allen* interpretation would call for a somewhat lower standard for capturing evidentiary data. Only successful attempts to access the computer need be logged. Under the *Riley* court’s holding, even *attempting* to access the computer could be seen as unauthorized access.

80. Kerr, *supra* note 53, at 1597.

81. *Id.* at 1598 n.10.

82. 917 P.2d 848 (Kan. 1996).

83. *Id.* at 852–53 (emphasis added).

84. *Id.* at 853.

85. 846 P.2d 1365, 1393 (Wash. 1993) (en banc).

86. *Allen*, 917 P.2d at 850; *Riley*, 846 P.2d at 1368.

87. Compare KAN. STAT. ANN. § 21-3755(a)(1) (Supp. 2004) (“‘Access’ means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or computer network.”) with WASH. REV. CODE ANN. § 9A.52.010(6) (Lexis 2004) (“‘Access’ means to approach, instruct, communicate with store data in retrieve data from, or otherwise make use of any resources of a computer, directly or by electronic means.”).

88. *Riley*, 846 P.2d at 1373.

C. Judicial Interpretations of “Authorization”

Courts have created three tests to determine what is and what is not, according to the Federal Computer Fraud and Abuse Act⁸⁹ (CFAA), unauthorized access: the “intended function” test articulated in *United States v. Morris*,⁹⁰ a criminal case; the employee “misconduct” cases, leading to findings of unauthorized access; and “contractual disputes” where an alleged breach leads to the violation.

An entity covered by Sarbanes-Oxley will have to determine which definition, or combination of definitions, the entity is most appropriate. This decision should not be made without significant input from information-technology specialists. The decision will dictate, among other things, what type of perimeter defense and recording system is set up to guard the company’s digital assets.

D. The Intended-Function Test

Morris was one of the first federal cases to deal with the consequences of damages arising from an “Internet worm.”⁹¹ *Morris* contended that his access was not unauthorized given that he had permission to access and use the network on which the worm was sent.

The court rejected this defense. It noted that *Morris* did not use the software as it was originally programmed to be used. His “unintended use” of the software allowed him to access the network in the first place; therefore, *Morris*’s access to the damaged computers was unauthorized.⁹²

This is a particularly nebulous definition. It presupposes a specific, clearly articulated description of how software—and therefore company policies related to the software—is intended to be used. This definition assumes a community consensus regarding the software and that the employees in question are aware of—and grasp—this consensus. Arguably, this is a rare occurrence in most institutions today.

E. The Employee-Misconduct Definition of Unauthorized Access

In *Shurguard Storage Centers v. Safeguard Self Storage*,⁹³ the court determined that when an employee uses a computer system belonging to an employer in a manner that is adverse to the interests of the employer, the employee is no longer acting as the agent of the principal.⁹⁴ Given that the employee’s access to the computer and computer network was authorized by his

89. 18 U.S.C. § 1030(a) (2000).

90. 928 F.2d 504 (2d Cir.1991).

91. *Id.* at 505.

92. *Id.* at 510.

93. 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

94. *Id.* at 1124–25; *see also* *United States v. Czubinski*, 106 F.3d 1069, 1071–72 (1st Cir. 1997) (IRS employee accessing workplace network for personal reasons); *Fugarino v. State*, 531 S.E.2d 187, 189 (Ga. Ct. App. 2000) (motives for deleting files can create unauthorized status).

Nearon et al.

agency status, the *moment* the agent acted in a manner adverse to the principal, the agent's access to the computer became unauthorized and, therefore, a violation of the CFAA. The court based its holding on the *Second* Restatement of Agency: "Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests, or if he is otherwise guilty of a serious breach of loyalty to the principal."⁹⁵

This definition of "unauthorized access" would seem to be the most promising for Sarbanes-Oxley purposes in that it is relatively simple to articulate and comprehend, compared to the "intended function" definition.⁹⁶ The computer-use policy is presented to the employee. A serious violation (and some case law would say *any* violation)⁹⁷ of the policy results in the revocation of the employee's authorized access. This does, however, put a premium on the policy being clearly articulated to the employees.

F. Breach of Contract As a Gateway to Unauthorized Access

In *EF Cultural Travel BV v. Explorica, Inc.*,⁹⁸ the court determined that the breach of a confidentiality agreement between an employer and former employee could lead to a finding of unauthorized access on the part of the breaching party.⁹⁹ The former employee set up a competing business where he used specially designed software to harvest information from the Web site of his former employer.¹⁰⁰

The district court ruled that search of the employer's Web site was unauthorized because it went against the "reasonable expectations" of the Web site owner.¹⁰¹ The appeals court, however, reasoned that because the employee had used his insider's knowledge in violation of a confidentiality agreement to create the software that accessed the EF Web site, he was liable for unauthorized access.¹⁰²

G. Unauthorized Acquisition of Information and Assets in a Digital Context

What does it mean to steal assets maintained in a digital format? How does an entity ascertain when its digital assets have been stolen? This is not a metaphysical question. According to Blair and Wallman,¹⁰³ and Lev,¹⁰⁴ seventy

95. *Shurguard*, 119 F. Supp. 2d at 1125 (citing RESTATEMENT (SECOND) OF AGENCY § 112 (1958)).

96. *Morris*, 928 F.2d at 510.

97. *See Am. Online, Inc. v. Nat'l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000).

98. 274 F.3d 577 (1st Cir. 2001).

99. *Id.* at 583–84.

100. *Id.* at 578–80.

101. *Id.* at 580.

102. *Id.* at 583–84.

103. BLAIR & WALLMAN, *supra* note 16, at 1, 11, 12.

104. LEV, *supra* note 16, at 8.

percent of the value of public companies is made up of intellectual property. Thus for entities covered by Sarbanes-Oxley and other SEC reporting requirements, a novel question is raised of how and when unauthorized access can, in effect, become a theft of property that would result in an occurrence that likely could have a “material effect on the financial statements”¹⁰⁵ of the company. The courts have offered some guidance on this issue.

In *United States v. Riggs*,¹⁰⁶ the first reported case involving the theft of a text file, a federal district court held that it was “well-settled that when proprietary business information is affixed to some tangible medium,”¹⁰⁷ it meets the statutory definition of property.¹⁰⁸ The *Riggs* court’s holding identified the precise moment the defendant obtained *possession* of the property in question. Essentially, the defendant had stored the stolen property on a computer bulletin board but had not, for the moment, downloaded the file to his computer. Therefore, the defendant claimed, he could not be charged with “possession” of stolen property.

The court held that for purposes of the statute, this distinction was meaningless. It noted that the *potential* was there, at any time, for the defendant to produce the information in an “accessible, even salable form.”¹⁰⁹ The court elaborated:

Although not printed out on paper, a more conventional form of tangibility, the information in Bell South’s E911 text file was allegedly stored on computer. Thus, by simply pressing a few buttons, Neidorf could recall that information from computer storage and view it on his computer terminal. The information was also accessible to others in the same fashion if they simply pressed the right buttons on their computer. *This ability to access the information in viewable form from a reliable storage place differentiates this case from the mere memorization of a formula.*¹¹⁰

*United States v. Ivanov*¹¹¹ goes even further in defining when something of value has been obtained. Ivanov was charged with hacking into a company’s computer system. His intention was, allegedly, to blackmail the company. Ivanov’s defense centered on whether he obtained “something of value” after hacking into the computer system.¹¹² The court rejected this defense holding that, for purposes of a CFAA Section 1030(a)(4)¹¹³ violation, “[a]t the point Ivanov gained root access to OIB’s computers, he had *complete control* over that data,

105. *Final Rule on Management’s Report*, *supra* note 12, at 36,640.

106. 739 F. Supp. 414 (N.D. Ill. 1990).

107. *Id.* at 420.

108. 18 U.S.C. § 2314 (2000) (federal statute prohibiting interstate transportation of stolen property).

109. *Riggs*, 739 F. Supp. at 421.

110. *Id.* at 422 (emphasis added).

111. 175 F. Supp. 2d 367 (D. Conn. 2001).

112. *Id.* at 371.

113. 18 U.S.C. § 1030(a)(4) (2000) reads as follows:

Whoever: . . . (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period.

Nearon et al.

and consequently, *had possession* of it.”¹¹⁴ That Ivanov subsequently transferred the data to Russia “[did] not alter the fact that . . . Ivanov first possessed [the] data” in Connecticut.¹¹⁵

This holding is consistent with the intent of the drafters of the 1986 version of the CFAA. A Senate report noted that “removal” of the data or “transcribing” of the data need not be proven as an essential element of the violation.¹¹⁶ This is a unique finding because, as the report noted, information is essentially “stolen” without being “altered.”¹¹⁷

These authorities may be relevant to determining when assets of an entity covered by Sarbanes-Oxley have been stolen. In certain circumstances information on systems that are merely compromised, particularly where root access is gained, may also be deemed stolen. Thus, holdings in CFAA jurisprudence will have a significant influence on how an entity covered by the Act should define and interpret its information-security policies and processes. The definitions in themselves, particularly with regard to unauthorized access, could be potential triggers for Sections 302 and 404 violations.

For these reasons and numerous others, a digital information-security regime (ISR) seems essential for Sarbanes-Oxley compliance. The next question then is how to design and implement an ISR that would meet acceptable due diligence standards.

VI. ARE INDUSTRY TECHNICAL STANDARDS NECESSARY TO MEET THE COMPLIANCE REQUIREMENTS OF 302 AND 404?

Industry technical standards must be employed by covered entities. The use of open and unbiased technical standards is a logical prerequisite to implementation of Sections 302 and 404, and will allow management and the examining auditor to avoid an ad hoc evaluation framework. A customized evaluation model would call for tremendous effort as management and auditors wrestled to familiarize themselves with unique systems designed in a hit-or-miss framework and maintained at an individual company’s whim. Further, requiring industry technical standards is consistent with the requirements of the Act. The final rules state that management must provide “[a] statement identifying the *framework* used by management to conduct the required evaluation of the effectiveness of the company’s internal control over financial reporting [(ICOR)].”¹¹⁸ While Sarbanes-Oxley does not state what this “framework” must be, it does provide a description of elements that must make it up. The standard measures used to evaluate ICOR should be publicly available. They also should be “free from bias [and permit]

114. *Ivanov*, 175 F. Supp. 2d at 371–72 (emphasis added). “Root access” gives an individual operational control of the computer.

115. *Id.* at 372.

116. S. REP. NO. 99-342, at 6–7 (1986), reprinted in 1986 U.S.C.A.N. 2479, 1986 WL 31918.

117. *Id.* at 13.

118. *Final Rule on Management’s Report*, supra note 12, at 36,642.

reasonably consistent qualitative and quantitative measurements of a company's internal controls."¹¹⁹

VII. HOW INDUSTRY STANDARDS AND BEST PRACTICES MAY BE USED TO COMPLY WITH SARBANES-OXLEY REQUIREMENTS

A. Sources for Standards

Employing the term "standards" at the zone where the information-technology world and the legal world meet raises difficult and complex textual issues. It is not enough simply to say that industry technical standards¹²⁰ do not necessarily equal *legal* standards. Rather, it should be shouted so as to serve as a counter-balance for those claiming, directly or indirectly, the opposite.

At present, there has been only one legal opinion addressing the issue of digital information-security standards,¹²¹ and that case failed to provide clear, definitive guidance as to what might be appropriate industry technical standards or best practices for internal controls. There is no "safe harbor" provision in Sarbanes-Oxley regarding industry practices or best practices other than specific mention of the COSO *Internal Control—Integrated Framework*.¹²² COSO, as presently constituted, offers little specificity on industry technical standards for information-security regimes. Extensions of COSO and an update have been proposed, but these too are relatively silent when it comes to information security.¹²³ One can turn, however, to the National Institute of Standards and Technology's (NIST) "security publications."¹²⁴ NIST security standards, are proffered in the Health Information Portability and Accountability Act (HIPAA),¹²⁵ as a possible industry technical standard for implementing the security standards required by HIPAA.

119. *Id.*

120. Some examples, by no means exhaustive, of "industry technical standards" or "best practices" include (1) Generally Accepted System Security Principles (GASSP), issued by the International Information Security Foundation; (2) Guidelines for the Security of Information Systems, issued by the Organization for Economic Cooperation and Development; (3) ISO/IEC 17799:2000; (4) Rainbow Series, issued by the Department of Defense/National Security Agency/National Computer Security Center; (5) OMB Circular A-130; (6) Information Systems Audit and Control Association's Objectives for Information and Technology (COBIT) (to be covered in greater detail later in this work); (7) GAO's Federal Information System Controls Audit Manual; (8) AICPA's SysTrust system; (9) Internet Engineering Task Force's RFC 2196, Site Security Handbook.

121. *Cobell v. Norton*, 226 F. Supp. 2d 1, 127–29 (D.D.C. 2002), *vacated by* 334 F.3d 1128 (D.C. Cir. 2003).

122. *See Final Rule on Management's Report*, *supra* note 12, at 36,642.

123. COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, ENTERPRISE RISK MANAGEMENT—INTEGRATED FRAMEWORK (2004), *available at* <http://www.coso.org/publications.htm> (last visited Sept. 13, 2005).

124. *See, e.g.*, MARIANNE SWANSON & BARBARA GUTTMAN, NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T COMMERCE, GENERALLY ACCEPTED PRINCIPLES AND PRACTICES FOR SECURITY INFORMATION TECHNOLOGY SYSTEMS (1996).

125. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, and 42 U.S.C.).

A second source for a standard is CobiT—Control Objectives for Information and Related Technologies. CobiT was developed by the IT Governance Institute¹²⁶ to provide “good practices for the management of IT processes in a manageable and logical structure, meeting the multiple needs of enterprise management by bridging the gaps among business risks, technical issues, control needs, and performance measurement requirements.”¹²⁷

CobiT, as differentiated from the numerous other industry technical standards, rests on the fact that the IT Governance institute has released a detailed and specific framework on the relationship between Sarbanes-Oxley and information technology.¹²⁸ This document attempts to link the requirements of Sections 302 and 404, the COSO Framework, and information-technology practices.¹²⁹ The CobiT document does not necessarily establish a “safe harbor” for Sarbanes-Oxley compliance, but it is a starting point.

B. The Applicability of the COSO Standard

To evaluate the effectiveness of the company’s internal control over financial reporting, the final rules specify that management must use “a suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment.”¹³⁰ The final rules mention COSO as satisfying this criterion, but any framework may be used provided that it is “unbiased, permits consistent measurement, and does not omit relevant factors regarding internal control over financial reporting.”¹³¹ Questions arise as to whether COSO adequately addresses concerns regarding information security and whether an evaluation of internal control over financial reporting based on COSO is complete if it omits information-security controls.

Prior to 1992, when COSO was being developed, most public companies used mainframe and mid-range computers housed in data centers accessible only

126. IT Governance Institute, <http://www.itgi.org> (last visited Sept. 1, 2005).

127. COBIT STEERING COMMITTEE AND THE IT GOVERNANCE INSTITUTE, COBIT EXECUTIVE SUMMARY 3 (3d ed. 2000), available at www.isaca.org/cobit (last visited Sept. 13, 2005).

128. See *supra* note 76.

129. IT GOVERNANCE INSTITUTE, *supra* note 76, at 7:

In developing this document, the contributors engaged in two activities. IT controls from *Control Objectives for Information and Related Technology* (COBIT®) (see next paragraph) were linked to the IT general control categories identified in the PCAOB standard, and these identified control objectives were linked to the COSO internal control framework.

The Sarbanes-Oxley Act requires organizations to select and implement a suitable internal control framework. COSO, *Internal Control—Integrated Framework*, has become the most commonly adopted framework. Generally, SEC registrants and others have found that additional details regarding IT control considerations were needed beyond that provided in COSO. Similarly, the PCAOB indicates the importance of IT controls, but does not provide further detail. As a result, COBIT, published by the IT Governance Institute, was used in this document as the basis to access further IT control detail.

While COBIT provides controls that address operational and compliance objectives, only those related directly to financial reporting were used to develop this document. Consideration was also given to other IT control guidelines, including ISO 17799 and the Information Technology Infrastructure Library (ITIL).

130. *Final Rule on Management’s Report*, *supra* note 12, at 36,642.

131. *Id.*

by information-technology staff and finance and accounting users through dumb terminals to initiate, record, process, and report financial information. Although some companies had local area networks (LANs), generally only scientific researchers or employees at research institutions had e-mail or access to the Internet. Today, information-technology architecture has changed dramatically. The mainframe has been relegated to data warehousing, mid-range computers have taken over much of the heavy lifting, and clusters of microcomputer-based client servers are increasingly used for processing financial information. Furthermore, corporate networks have been opened to suppliers and customers via extranets; dispersed geographic locations via wide area networks (WANs); and e-commerce, e-business, and ubiquitous employee use of e-mail and the Internet. At the time COSO was published, these technologies were not envisioned for widespread business use (except for WANs at the largest organizations), let alone considered during an evaluation of internal control over financial reporting.

COSO, however, was written as a high-level document and considered information-technology controls—then referred to as “information systems control activities”—as consisting of general and application controls.¹³² COSO categorizes general controls as data center operation, system software acquisition and maintenance, access security, and application system development and maintenance.¹³³ Also, according to COSO, “[t]hese controls apply to all systems—mainframe, minicomputer, and end-user computing environments.”¹³⁴ When COSO was written, access controls typically meant user IDs, passwords, user menu rights, and physical access to the data center.

In today’s information-technology environment, however, corporate networks on which the financial application and accounting records reside have a myriad of access points. Generally Accepted Auditing Standards recognize that compromising a single access point might compromise the entire database (the digital records that support the financial statements).¹³⁵ Networks control access with routers, firewalls, security parameters on servers, and other communication devices through appropriate information-security practices. These practices include information-security policies, procedures, and device-security settings. Given the porous nature of today’s information-technology environment, to understand access controls over financial reporting, management must evaluate information-security controls. In fact, in our networked world, access controls—one of COSO’s four elements of general controls—mean information-security controls. Lacking an evaluation of information-security controls, it is unlikely that management or the auditor has performed a complete evaluation and an audit of internal control.

132. COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), INTERNAL CONTROL—INTEGRATED FRAMEWORK 52 ¶ 4 (1992).

133. *Id.* at 52 ¶ 5.

134. *Id.*

135. AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, STATEMENT ON AUDITING STANDARDS: THE EFFECT OF INFORMATION TECHNOLOGY ON THE AUDITORS CONSIDERATION OF INTERNAL CONTROL IN A FINANCIAL STATEMENT AUDIT 11 (2001).

C. Can Sarbanes Oxley Compliance Be Achieved Without Reliance upon Industry Standards?

It seems clear that a standard that incorporates the “best practices” of information-technology security will guide the way towards implementation of Sarbanes-Oxley. Given that Sarbanes-Oxley activity will become a normal part of the business routine, as opposed to a one-time event (for example, Y2K), it is vital for the public to discuss which standards to employ as soon as possible.



This Article has explored the growing and complex nexus between the Sarbanes-Oxley Act of 2002 and information security. Information-security policies, practices, and controls are a critical element in internal control over financial reporting. Consequently, we have discussed the internal control disclosure and certification requirements for issuers and their auditors in existing security laws and rules. While these specific requirements are silent regarding information security, we believe that issuers’ disclosures and certifications and auditors’ attestations are incomplete without identifying an appropriate information-security regime in the entity being audited. Admittedly, the laws and rules for Sarbanes-Oxley compliance are silent with respect to information security, and this could tempt management and auditors to ignore the issue. In that case, internal controls will be weakened, leading to an inevitable breach of information security, materially misstated financial statements, and investor losses.

The profound shift in business records from pen, ink, and paper to digital media has significant implications for businesses’ and auditors’ reliance on such records. The shift has taken the ground from beneath our feet. When we look at a document that supports financial statements, we are likely looking at only a “view” of it and cannot determine with certainty who created it, when it was created, when a transaction occurred, its authenticity, or its integrity. In light of this fundamental change, we have addressed issues of authorization and access, two central aspects of internal control. Case law on unauthorized access is sparse, and courts have reached inconsistent judgments.

We believe that documenting, assessing, and testing information security by issuers and auditors for compliance with Sarbanes-Oxley will likely reveal material and significant information-security weaknesses. This might cause management to remediate these weaknesses. Amending the SEC laws to explicitly include information security as part of the issuer’s disclosures, the certification process, and the auditor’s attestation might be the only way to achieve this. The cost of proscription would certainly be less than the inevitable losses to investors if the security laws and rules remain silent regarding information security.