UIC John Marshall Journal of Information Technology & Privacy Law

Volume 12
Issue 3 *Journal of Computer & Information Law - Fall 1993*

Article 3

Fall 1993

Security Requirements And Evidentiary Issues In The Interchange Of Electronic Documents: Steps Toward Developing A Security Policy, 12 J. Marshall J. Computer & Info. L. 425 (1993)

Peter N. Weiss

SECURITY REQUIREMENTS AND EVIDENTIARY ISSUES IN THE INTERCHANGE OF ELECTRONIC DOCUMENTS: STEPS TOWARD DEVELOPING A SECURITY POLICY

by PETER N. WEISS*

I. INTRODUCTION

It is widely expected that the impact of computerization on commerce will be as great as that of the industrial revolution.[1] Electronic messaging techniques, particularly Electronic Data Interchange (EDI), hold great promise to become the preferred methods of communicating administrative and business information. But widespread use of these techniques of electronic commerce will occur only if they have, and are perceived to have, the same or similar level of security as paper-based systems. The concept of security focuses on ensuring the integrity and availability of communications and, to the extent necessary, guaranteeing confidentiality.

Electronic and paper media share many of the same security risks. However, the security protections associated with the traditional use of paper and signatures are so transparent to users and so customary that little thought is given to whether particular transactions require their use. Thus, statutory and regulatory provisions commonly specify that communications be "in writing," "signed," "verified," or "acknowledged." These have become so ubiquitous that most routine paper-based communications, particularly forms, contain a facial requirement for a signature—even in the absence of any specific legal or administrative directive that an original autograph signature actually be affixed.

---

* The views set forth are those of the author and do not necessarily represent those of the Office of Management and Budget. I would like to acknowledge the assistance of Thomas A. Connelly, a student at The John Marshall Law School, Chicago, Illinois. His help in the preparation of this article is greatly appreciated.

1. INTERNATIONAL CHAMBER OF COMMERCE, UNIFORM RULES OF CONDUCT FOR INTERCHANGE OF TRADE DATA BY TELETRANSMISSION [hereinafter UNCID RULES], ICC Pub. No. 452 (1988).

In electronic communications environments using techniques such as EDI, however, these security characteristics are no longer "automatic," but must be designed into each particular application. The Computer Security Act of 1987[2] provides a framework for determining what security characteristics are appropriate for particular applications. Although the Act only directly addresses Federal computer systems, its principles should be generally accepted. The Act defines sensitive information as including "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy [of] individuals. . . ."[3] It requires each agency to consider the risk to such sensitive information and to "establish a plan for the security and privacy of each Federal computer system . . . that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system."[4]

As the Computer Security Act recognizes, the goal of information security is to manage and minimize risk. The same information which has monetary or other value requiring risk management also may be called upon as evidence to prove the facts associated with particular transactions. A paper purchase order or invoice may become evidence in a contract dispute, and the information in a regulatory filing may be required for enforcement proceedings. In the evidentiary context, the focus is on whether the information is generated in the normal course of business in a manner which maximizes the likelihood that it is reliable and trustworthy.[5] Little consideration has been given, however, to the particular mix of elements which will effectuate the goals of the Act in the EDI context:

> What is needed, then, is a security policy. Various techniques are available to authenticate the source and verify the content of and to control access to electronically transmitted documents. However, there is little jurisprudential guidance as to whether and, if so, under what circumstances these security techniques will provide the requisite assurance of reliability. This lack of guidance concerning security techniques is reflected in the multiplicity of current security and authentication practices within the EDI community.[6]

---

2. 40 U.S.C. 759 (1987).

3. *Id.*

4. *Id.*

5. *See* U.S. DEP'T OF JUSTICE, ADMISSIBILITY OF ELECTRONICALLY FILED FEDERAL RECORDS AS EVIDENCE (1991) [hereinafter JUSTICE DEP'T GUIDELINES], *reprinted in* INFORMATION RESOURCES MANAGEMENT PLAN OF THE U.S. GOVERNMENT (1991); ASS'N FOR INFOR. AND IMAGE MGMT., PERFORMANCE GUIDELINE FOR THE LEGAL ACCEPTANCE OF RECORDS PRODUCED BY INFORMATION TECHNOLOGY SYSTEMS, AIIM TR 31 (1992) [hereinafter PERFORMANCE GUIDELINE].

6. A.B.A. Res. 115 (Tentative Draft No. 3, 1991). The resulting ABA resolution did

II. STEPS TOWARD DEVELOPING A SECURITY POLICY

The purpose of this paper is to present three preliminary steps toward the development of a security policy for the interchange of electronic documents. Its underlying thesis is that issues of legal admissibility and computer security are intertwined and must be considered together.

First, this paper briefly reviews basic principles of the law of evidence in order to identify the characteristics of electronic records which maximize the likelihood of their admissibility as evidence. This review suggests that the characteristics associated with the evidentiary value of electronic documents are essentially the same as those associated with maintaining the security of the information. It concludes that the provision of adequate security under the risk-based standard of the Computer Security Act also serves to ensure that the electronic records may be admissible as evidence.

Second, this paper analyzes the security characteristics associated with traditional paper-based communications and compares the functions performed by each with the security services available in electronic data interchange and similar technologies. It demonstrates that although the transition from paper-based communications to electronic techniques poses some unique risks, the essential security requirements are the same.

Finally, this paper presents a possible security classification scheme for various EDI applications, and suggests presumptively adequate security techniques for each to serve as a starting point for the development of the security plans required by the Computer Security Act and good practice. Each security plan must evaluate the risks associated with the loss, misuse, or compromise of the information against the costs associated with the various techniques available to mitigate those risks. Its purpose is to identify those techniques which achieve a reasonable risk/cost balance under the circumstances.

---

not, however, articulate a substantive security policy, but rather encouraged its development:

> The [ABA] supports action by federal and state governments, international organizations, and private entities to: (a) facilitate and promote the orderly development of legal standards to support and encourage the use of information in electronic form, including appropriate legal and professional education; (b) encourage the use of appropriate and properly implemented security techniques, procedures and practices to assure authenticity and integrity of information in electronic form; and (c) recognize that information in electronic form, where appropriate, may be considered to satisfy legal requirements regarding a writing or signature to the same extent as information on paper or in other conventional forms, when appropriate security techniques, practices and procedures have been adopted.

A.B.A. Res. 115 (1992).

Questions of legal admissibility and computer security are but two sides of the same coin. For example, if a systems manager retained the services of a component litigator to help design an EDI application in a cost effective manner which would assure a high degree of likelihood that the outputs of the system would be admissible, the system manager would, in the process, have met the requirements of the Computer Security Act. On the other side, had the systems manager retained the services of a security specialist versed in the risk/cost methodology of the Computer Security Act to perform the same task, the outcome should be precisely the reverse—a high degree of likelihood that the outputs of the application would be admissible as evidence would be assured. Recognition of this essential unity between system integrity and the evidentiary value of system outputs should help to alleviate unfounded, but often expressed, concerns regarding whether electronic documents and their various signature analogues are "legal."[7]

III. EVIDENTIARY REQUIREMENTS FOR ELECTRONIC DOCUMENTS

Although the law is sometimes criticized as slow to keep pace with progress,[8] the reality of the information revolution has been recognized by the courts:

> . . . [N]o court could fail to notice the extent to which business today depends on computers for a myriad of functions. Perhaps the greatest utility of a computer . . . is its ability to store large quantities of information which may be quickly retrieved on a selective basis. Assuming that properly functioning computer equipment is used, once the *relia-*

---

7. Indeed, these concerns should by now have definitively been laid to rest. In general, signature and writing requirements are not legal barriers to electronic commerce:

> *The concern with electronic signatures . . . is a red herring.* A variety of techniques for authenticating electronic documents exist that are as good or better than traditional handwritten signatures . . . There is growing agreement . . . that authentication and signature concerns can be addressed by existing legal concepts in conjunction with adequate audit and record keeping controls.

Henry H. Perritt, Jr., *The Electronic Agency and the Traditional Paradigms of Administrative Law*, 44 ADMIN. L. REV. 79 (1992) (emphasis added). *See also*, A.B.A. Res. 115, *supra* note 6; *Signature Requirements under EDGAR*, Decision of the SEC General Counsel, (Jan. 13, 1986) ("requirements for 'signatures,' . . . may be satisfied by means other than manual writing on paper . . . or the use of Personal Identification Numbers (PINs). In fact, the electronic transmission of an individual's name may legally serve as that person's signature, provided it is transmitted with the present intention to authenticate."); *National Institute of Standards and Technology—Use of Electronic Data Interchange Technology to Create Valid Obligations*, 1991 WL 315248 (G.C.), 71 COMP. GEN. 109 (1991) (Contracts formed using EDI satisfy statutory writing and signature requirements so long as technology used provides same degree of assurance and certainty as traditional "paper and ink" methods of contract formation).

8. *See* Peter N. Weiss, *Law and Technology: Can They Keep Abreast?*, 8 GOV'T INFO. Q. 377 (1991).

> *bility* and *trustworthiness* of the information put into the computer has been established, the computer printouts should be recieved as evidence of the transactions covered by the input.[9]

As a general matter,[10] computerized records are admissible as evidence provided that they are authenticated and can withstand challenges regarding their genuineness and reliability. The authentication requirement is satisfied "by evidence sufficient to support a finding that the matter in question is what its proponent claims."[11] This is done in legal proceedings by laying a foundation that will qualify the evidence as being what it is purported to be (e.g., a record prepared in the ordinary course of business).

Challenges to an offer of electronic documents as legal evidence usually take the form of objections on the basis of a violation of the "best evidence" or "hearsay" rules. A refresher on these rules might be helpful at this point.

Originally, the best evidence rule allowed only an original writing to be admitted into evidence for the purpose of proving the contents of that writing; any copy or duplicate was excluded.[12] The requirement proved to be unworkable and gradually the rigid application of the rule was relaxed.[13] Today, the rule is considered a rule of preference rather than exclusion,[14] with the aim being to obtain the most reliable evidence concerning the contents of a writing or document when those contents are in dispute.[15]

The Federal Rules of Evidence (FRE) incorporate this modern stance. First, FRE 1001(1) defines a "writing" to include any "mechanical or electronic recording, or other form of data compilation."[16] Sec-

---

9. United States v. Russo, 480 F.2d 1228, 1239 (6th Cir. 1973) (emphasis added).

10. For a more in-depth treatment of the subject of the admissibility of computerized information, see generally Rudolph J. Peritz, *Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence*, 80 NW. U.L. REV. 956 (1986); Richard M. Long, Comment, *The Discovery and Use of Computerized Information: An Examination of Current Approaches*, 13 PEPP. L. REV. 405 (1986); Mark A. Johnson, Comment, *Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability*, 75 MARQ. L. REV. 439 (1992).

11. FED. R. EVID. 901(a).

12. JUSTICE DEP'T GUIDELINES, *supra* note 5.

13. *Id.*

14. 2 MCCORMICK ON EVIDENCE § 237, at 76 n.2 (4th ed. 1992).

15. *Id.* § 243, at 87.

16. FED. R. EVID. 1001(1). The Advisory Committee notes to this rule make it clear that electronic documents are to be considered writings:

> Traditionally the rule requiring the original centered upon accumulations of data and expressions affecting legal relations set forth in words and figures. This meant that the rule was one essentially related to writings. Present day techniques have expanded methods of storing data, yet the essential form which the information ultimately assumes for usable purposes is words and figures. Hence

ond, FRE 1001(3) defines as an "original" writing "any printout or other output readable by sight," if that printout accurately reflects data stored in a computer or similar device.[17] Third, FRE 1002 states that "[t]o prove the content of a writing, recording or photograph, the original writing, recording, or photograph is required . . . ."[18] This third requirement poses no great difficulty for admitting computer documents, including EDI documents, into evidence since such documents are by definition original writings.

Of course, satisfying the best evidence standard does not make a computer generated document automatically admissible. There is still the hearsay hurdle to jump. A computer generated document offered to prove the truth of its contents is hearsay,[19] therefore, an exception to the hearsay rule must exist to provide grounds for the admission of the document into evidence.[20] This hurdle can be cleared with relative ease.[21]

While several possible hearsay exceptions may exist (depending upon the circumstances) to provide a basis for the admission of a computer generated document into evidence,[22] the most commonly applicable basis is the business records exception. The business records exception is founded on the premise that certain records are routinely

---

the considerations underlying the rule dictate its expansion to include computers, photographic systems, and other modern developments.

Id. Advisory Committee's note.

17. FED. R. EVID. 1001(3). The advisory committee clarifies that "practicality and usage confer the status of original upon any computer printout." *See id.* Advisory Committee's note.

18. FED. R. EVID. 1002.

19. *See* FED. R. EVID. 801(c). "Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." *Id.*

20. FED. R. EVID. 802 states: "Hearsay is not admissible except as provided by these rules or by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress." *Id.*

21. Recent court decisions have required a less stringent foundation for computer records under the Federal Rules of Evidence than was previously required under the Federal Business Records Act. *Compare* United States v. Vela, 673 F.2d 86 (5th Cir. 1982), *reh'g denied*, 677 F.2d 113 (1982) (presumption of trustworthiness of computerized records under Federal Rules of Evidence) *with* United States v. Scholle, 553 F.2d 1109 (8th Cir.), *cert. denied*, 434 U.S. 940 (1977) (Federal Business Records Act requires a unique, detailed foundation for computerized business records).

At least one commentator has recommended a return to greater foundational showings for computer generated records. Peritz, *supra* note 10.

22. For example, a computer record made by a party to the suit may be admissible against that party as an admission by a party-opponent, FED. R. EVID. 801(d)(2); or it may be admitted as a past recorded recollection, FED. R. EVID. 803(5). Additionally, a computer record which is against the declarant's interest is admissible as an exception to the hearsay rule. FED. R. EVID. 804(b)(3).

kept and relied upon by a business to carry out its activities and practices. There presumably are built-in safeguards insuring the accuracy and integrity of the information kept in those records. As a result, such records are considered to be trustworthy and reliable, thereby making them admissible as an exception to the hearsay rule.

Under the Federal Rules of Evidence,[23] the proponent of a computer generated record must show that the record is (1) kept pursuant to a routine procedure designed to assure its accuracy, (2) created for motives that tend to assure accuracy (e.g., not simply for the purposes of litigation), and (3) not itself an accumulation of hearsay.[24]

Electronically filed federal records are almost invariably offered as business records prepared in the ordinary course of business.[25] During the process of laying the foundation, the proponent of the evidence seeks to demonstrate the authenticity and reliability of the information, and the opponent tries to challenge those assertions:

> [T]he foundation for admission of computerized records consists of showing the input procedures used, the tests for accuracy and reliability and the fact that an established business relies on the computerized records in the ordinary course of carrying on its activities. The . . . opposing party then has the opportunity to cross-examine concerning company practices with respect to the input and as to the accuracy of

---

23. The federal business records exception was codified in the Federal Business Records Act prior to the enactment of the Federal Rules of Evidence. *See* 28 U.S.C.A. § 1732(a) (West 1966 & Supp. 1993), *repealed by* Pub. L. No. 93-595, 1974 U.S.C.C.A.N. 2251.

24. United States v. Sanders, 749 F.2d 195, 198 (5th Cir. 1984) (citing Capital Marine Supply, Inc. v. M/V Roland Thomas II, 719 F.2d 104, 106 (5th Cir. 1983)); 12 FED. PROC., L. ED. § 33:418 (Matthew J. Canavon et al. eds., 1988).

25. *See* JUSTICE DEP'T GUIDELINES, *supra* note 5 ("[e]lectronically filed Federal records are invariably offered as business records prepared in the ordinary course of business."); *see also* United States v. Croft, 750 F.2d 1354 (7th Cir. 1984) ("[i]t is well-settled that computer data compilations may constitute business records . . . and may be admitted at trial if a proper foundation is established.").

The business records exception exists at common law or in statute in most states. The exception also exists in federal law and is codified in the Federal Rules of Evidence. *See* FED. R. EVID. 803(6). Federal Rule of Evidence 803(6) states:

> The following are not excluded by the hearsay rule, even though the declarant is available as a witness:
>
> . . .
>
> (6) *Records of regularly conducted activity.* A memorandum, report, record or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method of circumstances of preparation indicate lack of trustworthiness.
>
> . . .

FED. R. EVID. 803(6).

> the computer as a memory bank and retriever of information. . . [T]he court must "be satisfied with all reasonable certainty that both the machine and those who supply its information have performed their functions with utmost accuracy." . . . [T]he trustworthiness of the particular records should be ascertained before they are admitted and the burden of presenting an adequate foundation for receiving the evidence should be on the parties seeking to introduce it rather than upon the party opposing its introduction.[26]

Federal records management regulations also incorporate these evidentiary principles and provide similar guidance to federal agencies in carrying out their responsibilities.[27]

In sum, the law of evidence does not rest on inflexible paper-based rules which should pose a barrier to the use of electronic commercial practices. Rather, it is concerned with the underlying integrity of the information on which a judge, jury, arbitrator, or mediator can reasonably rely in reaching a just conclusion to a particular controversy. Modern rules of evidence and court decisions appear to have come to terms with the realities of business and professional practice—the ever-growing dependence on information technology systems for records production and maintenance.[28]

> The essential questions posed by the law of evidence in this context can be summaried as follows:
>
> Electronic messages present four distinct evidentiary problems:
>
> 1. Proving that an electronic communication actually came from the party that it purports to come from;
> 2. Proving the content of the transaction, namely, the communications that actually occurred between the parties during the contract formation process;
> 3. Reducing the possibility of deliberate alteration of the contents of the electronic record of the transactions;
> 4. Reducing the possibility of inadvertent alteration of the contents of the electronic record of the transactions.[29]

The key evidentiary issue is the weight that a court will give to electronic records. "This will primarily be a question of agreeing to, and implementing, adequate security procedures."[30] These concerns with the identification of the originator, with the integrity of the con-

---

26. United States v. Russo, 480 F.2d 1228, 1241 (6th Cir. 1973) (quoting United States v. De Georgia, 420 F.2d 889, 895 (9th Cir. 1969)).

27. *Judicial Use of Electronic Records*, at para. 11, Federal Information Management Regulation (FIRMR) Bulletin B-1, *Electronic Records Management*; 36 C.F.R. § 1234.24.

28. PERFORMANCE GUIDELINE, *supra* note 5, at § 2.4.

29. MICHAEL S. BAUM & HENRY H. PERRITT, JR., ELECTRONIC CONTRACTING, PUBLISHING AND EDI LAW, § 6.23, at 344 (1991).

30. Ian Walden, *EDI and the Law*, INFORMATION TECHNOLOGY & THE LAW 239, 241 (2d ed. 1990).

tent of the communication, and with reducing the likelihood of alteration, which are at the heart of the law of evidence, are precisely the concerns which must be addressed in the context of EDI security. Thus, any combination of security controls which provides assurance that these characteristics have not been compromised will also provide a high degree of confidence that the contents of the communications will be admissible as evidence. The following sections of this paper will examine the security characteristics associated with both paper and electronic media, and will suggest a security classification scheme which may be of assistance in determining the appropriate mix of security techniques for particular EDI applications.

IV. SECURITY CHARACTERISTICS OF PAPER-BASED COMMUNICATIONS

Traditional paper-based communications accompanied by handwritten signatures provide three essential security characteristics: *message integrity, originator authentication,* and *non-repudiation.* Depending on the nature of the communication, an additional security characteristic, *confidentiality,* may be desired. The efficacy of the various techniques used to ensure the desired level of security in turn depends on the adequacy of the *administrative controls* associated with their use.

- *Message integrity* is the assurance that the content of a communication is complete and has not been changed prior to receipt. This is accomplished by a number of features, the primary ones being those associated with the use of the writing itself: inks which make erasure and alteration easily perceptible, salutations and closings which constrain the length of the message, and even the size of the paper which may limit the addition of text. For applications requiring additional security, techniques such as the use of engraved backgrounds, chemically treated papers, or lamination in plastic are used to make alteration particularly difficult.

- *Originator authentication* provides assurance that the communication originated from the named source. This is most commonly provided by the handwritten signature, or historically, by the seal of the author. The authentication purpose of the signature or the seal has two conceptual parts. First, they add a degree of formality, increasing the likelihood of actual assent to the terms contained in the document. Second, they serve to identify the document with the originator, because signatures and seals tend to be unique. In most commercial transactions today, these functions are served primarily by the use of letterhead or pre-printed forms, and in formal documents of a routine nature such as checks and negotiable instruments, printed signatures or "autopens" are often used to fulfill legal and customary requirements for signatures. Higher levels of originator authentication can be provided by the use of

watermarked or other special paper such as those generally used for negotiable instruments.

• *Non-repudiation* is a stronger form of authentication which relates to the ability of a disinterested third party to reasonably conclude that the identified originator intended to be bound by the substance of the communication. This function is most commonly performed by the original autograph signature affixed to a document having facially adequate message integrity. During the early development of contract law, primary reliance was placed on the individual's seal as indicating an intent to be bound. Only in the 20th Century did the signature gain its present prominence, and the special status accorded contracts under seal only disappeared as states enacted the Uniform Commercial Code. Enhanced forms of non-repudiation have generally involved the use of witnesses. Even after the use of written records of business and other transactions became common in the later Middle Ages, the most important enhanced form of non-repudiation remained witnesses. This formal reliance on witnesses is carried over today in the attestation of wills and the use of notaries public.

• *Confidentiality* is the ability to limit access to the information contained in a communication. This has generally been accomplished with some combination of security markings, envelopes, seals, trusted messengers, and by the use of codes and ciphers.

Administrative controls utilized adequately are central to the efficacy of message security. As paper-based communications took on forms more diverse than the handwritten document with affixed signature, communicating entities had to establish internal procedures to assure the efficacy of the various security techniques they wished to utilize. These ranged from limiting access to the official seal, and later to the letterhead and autopen, to ensuring the trustworthiness of message carriers and witnesses.[31]

As explained below, these same security characteristics and procedures are associated with electronic communications, particularly EDI. The primary difference is that the ubiquity of these techniques in paper-based systems and their transparency to users results in their being given little attention. It is generally only when cost becomes a relevant factor (e.g., the costs associated with special papers, autopens, or bonded couriers) that attention is given to the risk/cost equation. In EDI systems however, no intrinsic security "baseline" analogous to the forensic characteristics provided by paper, ink and signatures exists. Rather, each technique as applied to any particular application carries a price.

31. OFFICE OF MANAGEMENT AND BUDGET, REVISED "INTERNAL CONTROL SYSTEMS," OMB Circular A-123, 48 F.R. 38560-02 (1983) sets forth the present requirements for administrative controls in federal agencies.

V. SECURITY CHARACTERISTICS OF ELECTRONIC DATA INTERCHANGE

> "[E]ach time a new system or tool is produced, our more or less conscious attachment to tradition leads us to expect guarantees which were previously not only never fulfilled but were not even asked for."[32]

The use of electronic commerce techniques does not necessarily increase transactional risk beyond that experienced in a paper-based environment, but in some ways can actually reduce the likelihood of legal disputes ever arising. This is in spite of the fact that, unlike paper-based communications, electronic communications can theoretically be changed without a trace. For example, relevant communications protocols (e.g., X.25 and X.400) and the EDI standards themselves contain headers, password fields, and control information relevant to security and admissibility concerns. These characteristics, coupled with the speed of communication afforded by EDI and the decreased likelihood of transcription errors, may well lessen the frequency of disputes caused by the transmission of erroneous information. It is significnt to note that with electronic contracting starting to come into its own, there is as yet no reported case of disputes turning on the authenicity of the underlying electronic communication.

A common sense corollary to the risk-based standard set forth in the Computer Security Act is that, except where the use of computers increases risk, the use of computers should not create new requirements for the conduct of business beyond those that exist in a paper environment, unless the additional security obtained from those measures is worth the additional cost.[33] Looked at from the standpoint of potential threats, "[s]uch controls should make the cost of obtaining data greater than the potential value of obtaining or modifying the data."[34]

Security characteristics of paper-based media (hand or typewritten signatures and letterhead) are relatively easy to defraud, yet we use them unless the particular transaction is of such value that the cost of additional precautions seems justified. Certain electronic techniques can provide security beyond that available in a paper environment, and should be used when they will cost-effectively control new or previously uncontrollable risks. The point is that security is not an absolute, but must be tailored to the particular circumstances in order to be "com-

---

32. Walden, *supra* note 30 (quoting A.A. Martino).

33. Bruce W. McConnell, *Electronic Data Interchange in the U.S. Government: An Active Ingredient of Electronic Commerce*, 1 EDI FORUM 17 (1991), *reprinted from* OFF. OF INFO. & REG. AFF., EXEC. OFF. OF THE PRES., A FIVE YEAR PLAN FOR MEETING THE AUTOMATIC DATA PROCESSING AND TELECOMMUNICATIONS NEEDS OF THE FEDERAL GOVERNMENT (1990).

34. INT'L ORGANIZATION OF STANDARDS 7498, Addendum 2.

mercially reasonable."[35]

As in a paper-based system, the use of appropriate administrative controls is essential to assuring security in EDI applications. These include organizational arrangements such as separation of duties, physical security, and techniques for message authorization. Adequate administrative controls are central to the ability to effectively make use of the various techniques available to ensure the requisite level of security in the particular EDI application. In an electronic commerce environment, administrative controls also must be agreed upon and followed by trading partners. The International Chamber of Commerce's UNCID rules set forth a code of conduct under which trading partners may agree on such factors as appropriate identifiers, acknowledgments of transactions, confirmation of contents, protection of sensitive data, and data storage and transaction logging.[36]

The following is a description of the various computer security techniques applicable to EDI, followed by an indication of which of the four security characteristics they tend to satisfy. They are listed in a generally ascending order of security strength.[37] However, the strength of each technique depends on how it is integrated into the system and the accompanying administrative controls.

- *Access controls.* The use of logon techniques including passwords, key cards or other tokens, remote job entry protocols, or other unique identifiers such as fingerprint configuration or other biometric characteristics, which identify users and restrict access to an EDI application. (*Originator authentication, non-repudiation, confidentiality*)
- *Imbedded references.* The use of agreed reference numbers of passwords, either generic to the parties or specific to particular transactions, within a message. (*Originator authentication, non-repudiation*)
- *Functional acknowledgment.* A requirement for a confirmation message to be returned each time a message is received, but which does not repeat back the contents of the message. Analogous to a postal return receipt. (*Originator authentication, non-repudiation*)
- *Message repetition acknowledgment.* A requirement for a confirmation message to include the full contents or critical elements of the message sent. (*Message integrity, originator authentication, non-repudiation*)
- *Internal message verification.* Recalculation and verification of real totals and/or hash totals to protect against altered values of essential fields of a message. Hash totals are summations for checking contents

35. *See* U.C.C. § 4A.

36. UNCID RULES, *supra* note 1.

37. For an additional discussion of each computer security technique, see COMPUTER SYSTEMS LAB., NAT'L INST. ON STANDARDS & TECH., SECURITY ISSUES IN THE USE OF ELECTRONIC DATA INTERCHANGE (1991), and sources cited therein.

of similar fields, such as those containing part numbers, which would otherwise not be summed. (*Message integrity*)

- *Trusted Third-Party.* The use of a third-party service provider or value added network (VAN) to provide message status reports, message filing and audit services, and other security services. (*Originator authentication, message integrity (depending on service), non-repudiation, confidentiality*)
- *Cryptographic message authentication.* Techniques which utilize message authentication codes (MAC) and "digital signatures" calculated from all bits in the message using a secret encryption key. May be verified, if desired, by a recipient having possession of a decryption key.[38] (*Originator authentication, message integrity, non-repudiation*)
- *Data encryption.* Encrypts all bits of a message. Keys used for confidentiality must be different than those used for cryptographic message integrity, and both parties must have key access.[39] (*Confidentiality, non-repudiation*)[40]

These security techniques and their functions are summarized in Table 1. Their relative strengths are not indicated in the Table. They comprise a menu of techniques which, alone or in combination, can provide various levels of security.[41] Each, however, has its cost in terms of administrative effort as well as the hardware and software needed for its implementation. The mapping of security techniques to function is for general guidance and is based on expected usage. For instance, access controls and message authentication techniques can provide non-repudiation if the techniques are strong and the application supports it.

---

38. *See, e.g.*, FED. INFO. PROCESSING STANDARDS No. 113 (1992).

39. *See* FED. INFO. PROCESSING STANDARDS No. 46-1 (1992).

40. The practical and cost implications of the use of public key versus private key cryptosystems for message authentication and data encryption are beyond the scope of this paper.

41. *See generally Model Electronic Payments Agreement and Commentary, reprinted in* EDI & INF. TECH. DIVISION, A.B.A. SEC. SCI. & TECH., MODEL ELECTRONIC PAYMENTS AGREEMENT AND COMMENTARY, 32 JURIMETRICS J. 619, 649 (1992), which lists verification techniques of generally ascending strength:

(a) Sequence number consistency;
(b) Comparison of control totals with Remittance Information associated with a payment;
(c) Use and confirmation of a valid password/user ID combination;
(d) Communication call back procedures, and use of private or leased communication lines;
(e) A syntactical check on the Transaction Set as received, together with the subsequent communication of a Functional Acknowledgment to the Transaction Set's originator;
(f) Consistency checking of the payment amount with prior transactions or customer profiles;
(g) Smart cards and 'tokens';
(h) Message Authentication Codes; and
(i) Digital Signatures.

Conversely, cryptography without administrative controls may not provide non-repudiation.

VI. PRESUMPTIVE SECURITY LEVELS FOR VARIOUS ELECTRONIC DATA INTERCHANGE APPLICATIONS

The security assessment associated with each EDI application should include an examination of the substantive nature of each transaction type and an analysis of the risks and threats associated with each. Applications range from those which are not sensitive (e.g., reports of order status or questionnaires involving information without privacy or business confidentiality implications), through those with low to medium levels of sensitivity (e.g., procurement transactions and regulatory reporting), to those with high sensitivity (e.g., electronic funds transfer). The desired mix of security techniques will differ for each.

It is also important to recognize that it is the substance of the transaction rather than its form which is critical to the security analysis, as well as to the issues associated with legal admissibility.[42] For example, an EDI purchase order which is of relatively low dollar value and which is part of a routine course of dealings between trading partners would likely have a low level of risk from tampering or other threats. Likewise, it would require a relatively straightforward foundation for admissibility as evidence in the event of a dispute. On the other hand, an identically formatted EDI purchase order which is of a high dollar value and exchanged between parties who have never done business before would likely have a higher level of risk from tampering or repudiation. It would require a more extensive foundation for admissibility in evidence.

Since this analysis focuses on the security of the data interchange process, it does not examine a related issue relevant to admissibility: the security of the storage of messages after receipt. One of the keys to laying a proper evidentiary foundation is the ability to demonstrate that an organization's recordkeeping practices are such that their outputs can be deemed credible reflections of their inputs.[43] Thus, the evidentiary showing regarding records security may also vary based on media and storage techniques. For example, it is likely that electronic records stored on write-once-read-many (WORM) optical media may be considered to have a higher degree of security, and hence be more readily ad-

42. Contrary to some popular belief, use of encrypted message authentication techniques is not necessary to satisfy legal "signature" requirements. *See supra* note 7. Encryption is but one of a number of techniques that can satisfy legal signature requirements.

43. *See* JUSTICE DEP'T GUIDELINES, *supra* note 5.

missible, than records stored on magnetic media.[44] The security characteristics of an organization's data storage methods must, of course, be considered as part of the overall security analysis:

> Good electronic record systems design ensures that archives and records retention needs are designed into the system. While such design features may be difficult to incorporate in PC-based systems, the communications link . . . is an obvious and fail-safe point of capture for maintaining a comprehensive record. . . . Technical means could ensure that nothing gets into the system without being entered in a docket and having an archival copy made. The integrity would be greater than that achievable with human- and paper-based systems.[45]

The following schema is intended to aid in security analyses of EDI applications. It sets forth four general categories, each with increasing levels of security requirements, it suggests a mix of security techniques presumptively appropriate for each level, and it provides examples of applications which generally would be considered to be in the particular security category.[46]

- *Non-Sensitive.* Applications which do not involve the obligation of federal funds and which do not have regulatory or privacy implications. Examples include order status information, material inspection and receiving reports, and some questionnaires. For these applications, reasonable access controls should be adequate with other techniques being optional.
- *Sensitive (Low).* Applications which have no significant incentive for tampering by third-parties. These include most small purchase transactions, orders, invoices, bills of lading, and most regulatory reporting applications. Originator authentication and non-repudiation can generally be satisfied by functional acknowledgments, and the risk of tampering and privacy concerns, if any, can be minimized through access controls. Additional authentication and non-repudiation techniques such as message repetition, internal message verification, and imbedded references are optional.
- *Sensitive (Medium).* Applications which present significant incentives for tampering and/or for which a reasonable level of confidentiality should be maintained. These include responses to Invitations for Bids and Requests for Proposals, as well as applications for valuable benefits or substantial payments. Either of two strategies may be used.

---

44. *Id.* at 50 n.2.

45. Perritt, *supra* note 7.

46. This category may prove controversial. On the one hand, the Computer Security Act's definition of "sensitive" is broad, leading some to say "if it's worth keeping, it must be sensitive." On the other hand, general principles of statutory construction suggest that if some categories of federal data are "sensitive," others, by implication, must be non-sensitive.

> Cryptographic data authentication[47] or similar techniques provide strong protection against tampering. The use of message repetition acknowledgment, or other message verification techniques, in conjunction with a trusted third-party service provider may be adequate provided that the service provider has strong system access controls and adequate recordkeeping and audit mechanisms.
>
> • *Sensitive (High).* Applications where message confidentiality is of particular concern, or where there is a particularly great risk from lack of message integrity, and access related controls are deemed inadequate. These include the protection of particularly sensitive though unclassified information such as electronic funds transfer transactions. Generally, encryption techniques are recommended, either full text encryption for confidentiality or cryptographic message authentication.

These sensitivity levels and their presumptive security techniques, along with examples of each are summarized in Table 2. It should be noted that particular transactions may have varying levels of sensitivity for differing parameters. For example, while encryption may be considered appropriate for an electronic funds transfer, the remittance advice information related to the transfer may have a low degree of sensitivity for originator authentication and message integrity. Depending on the nature of the transaction, there may or may not be confidentiality concerns. Thus, the analysis may at times be multi-dimensional.

Dealing with confidentiality concerns is particularly challenging. On the one hand, only cryptographic techniques can ensure a high degree of confidentiality. However, in paper-based systems, the business community has accepted that the confidentiality provided by the postal system is adequate and that the risk of their information being improperly divulged is acceptably low. Therefore, it may be that the risk of such disclosure on electronic networks, absent the use of encryption, is also acceptably low. This depends on the strength of the access controls related to the system and the type of transaction.

This may be the case since the private sector routinely transmits confidential business information unencrypted. While it is certainly possible for data to be intercepted while it is on a vendor's network, it is more likely to be improperly accessed while it is still in the hands of the company. When data spies use telecommunications networks, it is usually to gain access to a company's computers.

If parties to particular transactions think that the risk of disclosure from unsecured telecommunications links is too high, then additional levels of security can be added. While the installation costs of a data encryption capability may be low, the maintenance costs (especially at the administrative level) may be an impediment to the use of this tech-

47. For a description of one technique for cryptographic data authentication see FED. INFO. PROCESSING STANDARD No. 113 (1992).

nology, at least in the near term. Moreover, data encryption is not now in wide use for commercial transactions other than for funds transfers. Careful attention must be paid to the risk/cost tradeoffs in these situations.

VI. CONCLUSION

The thesis of this paper is that evidentiary issues and security requirements are two sides of the same coin. In the realm of security, "one size" does not fit all and just as in the law of evidence, the foundational showing will vary with the particular circumstances.

A simple hypothetical case should elucidate the point. Party A sends Party B an electronic purchase order in a standard EDI format. Parties Y and Z do the same. In both cases disputes arise necessitating the use of the two purchase orders as evidence. Here, however, the similarities end. Parties A and B, it turns out, are merchants and established trading partners engaged in a regular course of business involving the routine exchange of electronic purchase orders. The transaction at issue involves a standard commercial product and does not carry an extraordinary dollar value. Parties Y and Z, however, are strangers who, although they possess and utilize EDI capability, have never done business together before. Furthermore, the transaction was of a high dollar value and was for the purchase of a custom manufactured item.

Although the two EDI purchase orders were essentially identical, from an evidentiary standpoint the two transactions were totally different. The burden Party A must carry in order to have its purchase order admitted into evidence is relatively light. The use of basic security techniques (password access control, generally reliable audit capability, probably the use of a VAN) should suffice to have the evidence admitted. Party Y, however, must bear a heavier evidentiary burden. The controls used by Party A might not suffice. Strong originator authentication, message integrity, and non-repudiation (probably using encryption techniques) would have been advisable.

Likewise, from the standpoint of the Computer Security Act's risk-based standard, the two transactions bear little resemblance. For Parties A and B, the use of sophisticated and potentially costly security techniques as a supplement to routine control and audit practices would have been unnecessary to satisfy the Act. For Parties Y and Z, they would probably have been essential.

In sum, the development of security plans as required by the Computer Security Act and good practice involves a common sense approach to risk assessment. Analyzing the security requirements of particular applications can be aided by considering the security characteristics

which the application should possess as well as the sensitivity level for each. As enhanced security techniques become more cost effective and increasingly ubiquitous, the task will become easier. However, careful assessment of the risk/cost tradeoffs must be made as part of this process. Attention to these factors should satisfy applicable legal requirements.

TABLE 1
DOCUMENT INTERCHANGE SECURITY TECHNIQUES
AND CHARACTERISTICS

	CHARACTERISTICS			
Security Techniques	Originator Authentication	Confidentiality	Non-repudiation	Message Integrity
Access Controls*	X	X	X	
Imbedded References	X		X	
Functional Acknowledgement	X		X	
Message Repetition Acknowledgment	X		X	X
Internal Message Verification				X
Trusted Third-Party	X	X	X	X
Cryptographic Data Authentication	X		X	X
Data Encryption		X	X	

* Access controls include a variety of techniques providing a wide range of security strength.

TABLE 2
SECURITY SCHEMA FOR ELECTRONIC DATA INTERCHANGE

Sensitivity Level and Presumptive Security Techniques	Application Examples	
Sensitive (High)	*Procurement*	*Non-Procurement*
Text Encryption per FIPS PUB 46-1	Protection of Logistics Unclassified Sensitive (PLUS)	Regulatory and other reporting with particular confidentiality concerns
EFT encryption	Electronic Funds Transfer	Electronic Funds Transfer
Sensitive (Medium)		
Cryptographic message authentication or Message repetition acknowledgment through trusted third-party	Large Purchases (Bids and Proposals)	Regulatory and other reporting with significant incentive for third-party tampering
Sensitive (Low)		
Access controls, Functional acknowledgment Optional: Message repetition, Internal message verification, Imbedded references	Small Purchases (Quotations) Orders under existing contracts Invoices Government Bills of Lading	Regulatory and other reporting: tax filings customs filings environmental reports Personnel actions
Non-Sensitive		
Access controls	Bidders mailing list information Status of orders Reports on orders received Material inspection and receiving reports	Questionnaires without confidential or proprietary information