IT'S NOT THE CONTRACTED FOR RISKS, IT'S THE RISKS OF CONTRACTING

A Risk Driven View of Electronic Contracting

Charles J. Miller, Esq.
ZEFER Corporation
275 Brannan St., San Francisco, CA 94107
(415) 762-3439//cmiller@zefer.com

A. Please Welcome Our Old Friend, FUD[1]…

An essential purpose of the recent laws and regulations addressing electronic signatures[2] is to affirm that electronic writings and signatures have the same legal force as their paper and ink predecessors. Many legal commentators believe this is (finally!) one area where the law has anticipated business practice. But an unfortunate miracle of chemistry has occurred: though legislatures are having the champagne parties, working lawyers are suffering the morning after hangover of mapping electronic-based contracting processes to their paper based parents. Though either process must yield the same end result – enforceable agreements – nearly everything about the two processes is different and the differences are pervasive, deep and difficult, supported by entirely dissimilar risk models.

A cook will tell you that the proof is in the pudding: conclusive evidence of the cook's ability can be tasted in the dessert prepared. Contracts are contrary. We write down agreements against future disputes. Recollections dim or people lie and writings may be good evidence of what was agreed to at the earlier point. Unlike dessert, in the litigation kitchen the pudding is in the proof.

But proof must be produced, authenticated and explained, and therefore must be available, comprehensible and not cost more to produce and explain than the value of the case itself (unless, of course, you have a favorable cost shifting provision, but it will exist in the very electronic agreement you are trying to prove….). Given that computers and computerized records are no longer new, an alarm bell right here may seem extreme. But the Internet newly connects everyone to everyone, and particularly the mal-intentioned to us all. And try explaining public key cryptography, a species of electronic signature, to a jury of our non-engineer peers.

Transactional attorneys, whose typical role is to create the right to enforce, may believe these issues are on the other side of the fence: the enforcement side handled by their knuckle dragging cousins, the litigators.[3] But clients will have you advise on their e-contracting system requirements and capabilities as well as the policies, processes and roles necessary to support the systems they wish to use. Moreover, new capabilities and processes require understanding new laws and duties, creating new conventions, and providing for new warranties, indemnities and standards.[4]

---

[1] Fear, Uncertainty and Doubt

[2] A partial listing is: the Uniform Electronic Transactions Act ("UETA"), the Electronic Signatures in Global and National Commerce Act ("ESIGN"), the Health Insurance Portability and Accountability Act's proposed electronic signature standard ("HIPAA"), the Uniform Computer Information Transactions Act ("UCITA"), the Government Paperwork Elimination Act ("GPEA") and FDA regulation 21CFR Part 11.

[3] The author confesses to having been a knuckle dragging litigator.

[4] For example, should denial of service attacks be called out in force majeure clauses.

Lawyers advise on legal or compliance risks, informed by an understanding of how their clients do business. When goods moved by covered wagon, attorneys were concerned with the effect of bandits, trail problems and wagon wheel construction. The role of counsel as a risk advisor mutates over time. Electronic contracting occurs on-line, so we must know about those risks, the operational or system risks[5] that affect computers and networks.

Convergence is occurring in contracting, not between televisions and computers, rather between signing and system, leading to greater legal conflation between contract and negligence. To enable electronic contracting, lawyers must not only understand the law, but also how the law drives requirements for new e-contracting systems. Through legislation we may have brought the e-commerce horse to the e-contracting water, but getting it to drink the Internet Kool Aid™ requires more than just law.

B. We Are All Trust Engineers Now

As a generic category, contracts are often thought of as risk management tools. Contracts allocate rights and obligations among the parties, describing who has what risks and when. This allocation allows the parties to engage in further risk management practices such as obtaining cargo insurance or initiating timely production runs to meet delivery dates. Many companies develop risk management strategies around their business operations which may include payment or performance guarantees, insurance, long term agreements with unions, or other types of programs or agreements that help assure the trains do run, run on time, and run to the right place, while also addressing what happens if Snidely Whiplash unexpectedly ties poor Nell to the tracks again and the trains have to shut down for a day (e.g. insurance, alternate carriers, alternate suppliers, etc.).

Many elements of a risk management strategy find expression in contracts. Because paper contracts have been around for so long they have become an old familiar. Consequently, we don't always recognize that the contracting process itself has a risk management substrate consisting largely of: paper and writing (fixedness); conventions (form and meaning); settled legal concepts and duties (interpretation); envelopes (confidentiality); post, fax or FedEx (transport); and locked file cabinets (storage, retrieval and security). These well-worn wagon tracks lend a certain confidence to the process, if not any particular swagger. But together they constitute the unspoken set of practices, the ghost in the machine, that animates the contracting process and make us reasonably confident in our ability to marshal evidence as required.

Thus we understand when a court interpreting the UCC's Article 2 finds a letterhead on a purchase order to be a signature, a finding clearly based on understood concepts of authentication in the context of a trade usage or course of dealing. But when one court decided that the printed output of a fax machine wasn't a "document" because the machines communicate by "chirps and beeps," we are conclusively notified that some jurists believe the aliens have arrived with technology beyond the ken of our carbon based life forms, salting the legal mine with unworldly processes we can no longer trust. (Well, for a moment, anyway; the case was later reversed.)

Unlike letterheads as signatures, which represent merely an incremental change in practice, electronic contracting is far more like what the "chirps and beeps" judge prematurely

[5] Risk taxonomies are not standardized. The categories above draw upon standard banking risk categories. See, for example, http://www.occ.treas.gov/ftp/bulletin/98%2D3.txt from the Office of the Comptroller of the Currency. Netrisk suggests a slightly different taxonomy in its chart found at http://www.netrisk.com.

feared: it is a fundamental shift in paradigm in which many of the rules change leading to a period of uncertainty and, consequently, uncalibrated risk. Businesses, which run to the refrain of ROI, are attuned to risk, striving to work within acceptable tolerances based on anticipated returns that drive shareholder value. But in "times like these," when the reverberations of the Internet cataclysm continue to roll through the base economy, risk calculations are upset and ROI must be seen through an increasingly concave risk adjusted lens.

Though the law clearly and emphatically enables electronic contracting, it does so with practically no guidance as to sufficient process, starting with legal understanding and moving through conventions and standards. That is, while the law is pulling for us, even cheerleading for us, to contract electronically, the argument is that it does not, and cannot, provide us with the most important and fundamental element of all: **trust in the outcomes the underlying process generates**. The parties' legal comfort requires not only binding agreements, but, as a practical matter, agreements they can reliably enforce through the production of evidence. Without understood conventions and practices that provide reasonably sure outcomes, favorable law, though necessary, is woefully insufficient.

C. A Selection of Compliance Risks[6]

1. Which Law Applies Anyway?

The first place to look is ESIGN, which applies to all transactions in interstate commerce except for the following: trusts and wills; family law; the UCC (but does apply to Articles 2 and 2A); court pleadings and documents; utility service cancellations; residential defaults; health insurance cancellations; product recalls; hazardous material transportation; state enacted electronic signature laws[7] consistent with ESIGN and that do not provide any greater status for a particular type of signature and which are enacted after ESIGN and specifically reference it; other federal, state or self regulatory agencies that impose performance standards so long as consistency with ESIGN section 101 is maintained, or nothing at all if a state adopts the NCCUSL version of UETA, which in turn permits knockouts of UCITA. (ESIGN sections 102, 103(a) and (b), 104) ESIGN does not prevent states from passing laws that cover the areas it omits (e.g. court filings) and one may assume that some states will do so (or have done so).

Moreover, there is some question regarding the extent to which ESIGN pre-empts preexisting digital signature laws.[8] While everyone agrees that such laws are pre-empted by

---

[6] The discussion below does not pretend to be exhaustive. For instance, ESIGN provides for consumer protections through the use of agreements and notices, the lack of which may or may not affect enforceability. This thorny set of issues, as well as many others, is not discussed.

[7] The law firm of McBride, Baker and Coles maintains excellent tables showing which states have passed what laws at http://www.mbc.com/ecommerce/legislative.asp. International powerhouse Baker & Mackenzie also has excellent global electronic signature and PKI news and links at http://www.bakernet.com/ecommerce/.

[8] Some states adopted "digital signature" laws in the mid-1990s. Digital signatures are a species of electronic signature based on public key cryptography, typically implemented in a public key infrastructure ("PKI"). What law professor Jane K. Winn has accurately panned as the mind numbingly complex explanations of private keys, public keys, x509v3 certificates, extensions, critical flags, ASN.1, Alice and Bob, CRLs and OCSP responders along with a very non-lawyerly concept of "non-repudiation," among other things, no doubt negatively influenced wide-spread adoption. However, a number of states did enact such laws (some with my participation), and in doing so gave certain favorable evidentiary presumptions to persons who reasonably relied on a digital signature to his or her eventual detriment. Some states (i.e.

ESIGN to the extent they make digital signatures the only acceptable electronic signature type,[9] many commentators believe the favorable evidentiary presumptions for digital signatures often contained in such laws may nevertheless survive. And if the favorable evidentiary presumptions are not worth the difficulty and expense of installing a PKI, you may still find that your European or Asian trading partners only accept digital signatures, and only ones that have been issued pursuant to particularly stringent standards.

As mentioned above, if UETA has been enacted so as to pre-empt ESIGN, UETA collegially exempts another NCCUSL product, UCITA, from its purview if so desired by a particular state. (ESIGN is less charitable if other exceptions are made, i.e. those exceptions that states add under UETA section 3(b)(4).) Moreover, the many sets of federal regulations, such as HIPAA's proposed electronic signature standard, the SEC regulations governing electronic filings posted on EDGAR, and FDA regulation 21 CFR Part 11 (more on that below) covering certain submissions to the FDA also apparently do not suffer pre-emption. A United States Code search using the words "electronic signatures" pulls up many other statutory cites as well. It can be so difficult to know which law a particular electronic signature implementation must comply with or benefit from that you need a lawyer to figure it out on a state-by-state and country-by-country basis. So, some champagne for the lawyers, please.

2. By Encrypting That Hash Table I Did What?

It is practically a matter of judicial notice that consumers are, well, morons. And we are all consumers. Thus the law bends over backwards to provide us with special protections, often against our own inabilities to figure things out. At a recent demonstration of a digital signing room one of the purported signers (truly signing a legally operative document on the same day ESIGN went live) couldn't enter a user name and password even with extensive coaching and a whispering assistant standing by to help. (The assistant ended up entering both pieces of information.)

Only relatively recently have courts largely stopped protecting consumers who signed contracts they failed to understand and then wanted out from under their terms. But there are few people of legal age who don't understand what it means to "sign on the dotted line."[10] With paper processes we universally understand the basic conventions underlying the signing ceremony.

It is not a far leap, we think, to click an "I Accept" button. We reasonably believe that even consumers should understand that by "clicking" the "button" on our computer (or PDA or phone) screens we are agreeing to the very legal terms we scroll impatiently past without reading a word.[11] But the actions that constitute manifesting an intent to be bound continue to move farther in form from what we understand to be dotted line signing. Anticipate howling complaints from people who didn't understand that pressing their new broker-provided cell phone's flashing button meant they agreed, with finality, to permit their broker to debit funds to pay for a stock trade (especially if the trade dives immediately under financial water).

Washington) even made a digital signature the equivalent of a notarized signature, ill advisedly letting the confirmed identification function obsolete the remainder of the notary's purpose.

[9] Except when a government by regulation may duly prescribe performance characteristics for dealing with itself that leave room only for a particular technological solution.

[10] Of course, dotted line signing is a time-dated concept too. As various people have pointed out, new paradigms are often not successful until those vested in the old paradigm die.

[11] I leave it to others to opine on the legal consequences of the adhesive nature of such contracts, particularly if imposed by predatory monopolists.

And this is only one dimension of the problem. We don't always sign to be bound; sometimes we sign to acknowledge having read or received something, to claim authorship or to assert authenticity. A mechanical process like applying a digital signature does not inherently differentiate among possible intents. Take, for example, Secure Sockets Layer ("SSL") technology. Because SSL uses the same public key cryptography processes that make up a digital signature, there was serious discussion whether the underlying data stream protected by an SSL connection would merely be considered secure or digitally signed as an intent to be bound.

UETA considers the hallmark of a signature its manifestation of the signer's intent. But intents can't be seen, only deduced, and then only within a greater construct of social convention, understood as usage or custom. Convention, then, requires a high degree of prior coordination like ducks in a row or quail in a covey. Changing the rules, changing the form factors of signing, means changing the way we understand the world. When the rules change, the conventions fly, requiring what consultants call "change management," a fairly innocuous phrase under which lurk the sharpest shoals that break the most ships. Just ask any company that has sunk cash into "transformational" projects.

Convention allows its parties to have certain understandings without having to discuss them each time the convention is called. Perhaps one knows that if Joe misses the meeting time he will look for you in the closest bar, so that is where you should go, even if today you feel like visiting a restaurant instead. Or, if Bob places mail on the table by the door, Alice should know to mail it on her way to work. Yet we feel certain Bob will one day place the envelopes on the end table or Alice will be distracted, and the mail will sit. Conventions fail even in the most tightly coupled situations.

Building a bilateral convention can be difficult; imagine building a global one. Yet building global signing conventions around the myriad of new form factors for signing is exactly what we must do. Flashing lights on cell phones, I Accept buttons on web sites, Sign tabs on pull down menus, your typed name at the bottom of an electronic record, your yes vote on a document drafted collaboratively on a portal, and tens or hundreds of other artifacts will now become signatures, and have to be accurately understood as such by all relevant parties every time. And then you will have to convince a judge or jury of the other party's intent, or lack thereof, at the time the artifact was created.

3. So We Don't Know Which Law May Apply and We Don't Know What We Did When We Pushed that Button, But We Do Know What an Electronic Signature Is, Right?

UETA and ESIGN provide nearly identical definitions of the term "electronic signature."

UETA	ESIGN
UETA Section 2, Definitions: (8) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.	**ESIGN Section 106, Definitions:** (5) ELECTRONIC SIGNATURE- The term `electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

The definitions are commendably functional, but at the price of form. They continue the trend of counting letterhead as signatures, where it's the intentful authenticating heart that matters, and not a stupid formal rule that fails to look at what is really occurring. As a society we don't like springing criminals on technicalities or exonerating parties on formalities. But determining which forms signified intent was easier when the conventions formed a clearer baseline. It will be the relying party's risk to decide whether any particular manifestation of intent is so clear that the signer likely can't successfully claim confusion.

But, there is a problem lurking in the definitional language that may work against the all-things-being-signatures standard that UETA seemingly intended. There is a minimum requirement that whatever composes the signature be "attached to or logically associated with" whatever is composed as the record.

In the paper world it's easy to imagine what it means to attach or logically associate a signature with a record. We might not be able to say in what chemical sense ink attaches to paper when you sign, or identify the precise locus of logicality when we associate through incorporation, but we grasp these things intuitively and don't typically fear for our ability to convince the court. We know the arguments to make and how a court is likely to receive them.

If we look to the UETA comment to help us understand these terms as applied to the electronic world, we are disappointed at its circularity. The comment states:

> Another important aspect of this definition lies in the necessity that the electronic signature be linked or logically associated with the record. In the paper world, it is assumed that the symbol adopted by a party is attached to or located somewhere in the same paper that is intended to be authenticated, e.g., an allonge firmly attached to a promissory note, or the classic signature at the end of a long contract. These tangible manifestations do not exist in the electronic environment, and accordingly, this definition expressly provides that the symbol must in some way be linked to, or connected with, the electronic record being signed. This linkage is consistent with the regulations promulgated by the Food and Drug 21 CFR Part 11 (March 20, 1997).

The conundrum is clearly stated: the law's language assumes a world of tangible manifestations – a signature at the end of a contract or an allonge stapled to a promissory note – in a world where tangible manifestations don't exist, taking on faith that attachment or logical association can be called into existence, like Bullwinkle pulling a cartoon lion out of a cartoon hat. In the absence of any guidance, we need to figure out this trick on our own.

"Attached to" or "logically associated with" are not legal terms *per se*, so we turn to dictionary definitions. Webster's Seventh New College Dictionary (1969) provides:

attach	1: to take by legal authority esp. under a writ; 2: to bring (oneself) into an association; 3: to bind by personal ties; 4: **connect, tie;** 5: ascribe, attribute
associate	1: to join as a partner friend or companion; 2 (obs): to keep company with: ATTEND; 3: **to join or connect together; COMBINE**

	4: to bring together in any of various ways; ~vi 1: to come together as partner, friends or companions; 2: to combine or join with other parts: UNITE syn. see JOIN.
logical	1a: relating to, in accordance with, or skilled in logic; b. formally true or valid: ANALYTIC, DEDUCED; 2: **that is in accordance with inferences reasonably drawn from events or circumstances**

The UETA comment quoted above clearly calls out the linking/connecting function, and the dictionary provides analytic support. But that linking/connecting aspect does not differentiate the disjunction (that is, if "attach" and "associate" are largely similar, what work is "logically" doing?), so we must make another conjecture. Consider this informal comment on a legal mailing list by a law aware security specialist addressing "I Accept" buttons:

> First I made the point that the law did not legitimize point-and-click - it says one can't disallow it just because it is not a traditional signature. Then I said that point and click could be acceptable but that if there was a challenge, then one might be forced to explain that the transactions written on the log were processed during an authenticated session and that even though the log records contained messages that could have been generated by any one, a review of all the code involved would prove that the messages could have only been written by the user who was authenticated by his password. And while yes it is true that someone could have modified the logs after the fact, there are procedures in place that block outsiders from accomplishing such tasks. And although people in the company could have modified the logs, this company doesn't do that sort of thing.[12]

The point, perhaps, is to distinguish between linking or connecting that is apparent from the face of the electronic record ("attached to") and that which must be deduced from the totality of the circumstances, such as a review and interpretation of log records; the manner of their manufacture, maintenance and review; policy surrounding; and audit procedures in place ("logically associated with"). But as one colleague was inclined to comment, electronic data is just billions of bits.

Higher level interpretations of state, i.e. the "meaning" of the position of switches etched in micron wide lines of silicon, are just that, and many such interpretations need to be combined to form the letters that you are reading, the "document" they exist in, the stored form in memory, and all of the operations that go into finding and retrieving it locally, on the network or over the internet. On top of that you must provide that another something, a signature indicator, itself made of interpreted bits, is combined with the file – and whether it is, or when it was, or what either of those statements means, may in some cases be questions that can only be proved by technical analysis of the sort done by down in the code engineers. One good guess is that all electronic signatures will have to be logically associated, but ultimately it will not only be the fact of association, but the "strength" of that association, measured in metrics that have not yet been established, that will make a difference in court.[13]

---

[12] Analysis by computer scientist and security expert Hoyt L. Kesterson II.

[13] Certain signature types, e.g. digital signatures – when properly implemented, are widely recognized to provide good signer authentication and durable message integrity. But even with digital signatures, much proof will go to the system's implementation and the conditions of its use to determine whether the outcomes should really be trusted.

Strong recognition of the strength problem is found in the only external reference the UETA comment, quoted above, provides on this topic:

> 21 CFR Part 11 states:
>
> Sec. 11.70 Signature/record linking.
>
> Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

We are faced with a dilemma. UETA's comments are clear that almost any form that either party purports manifests intent is worthy of an evidentiary battle to settle the question. The comments leave little room for any preliminary examination asking whether a particular manifestation should be considered a signature as a matter of law. But the comments curiously reference a "consistent" statute that is quite clear that an electronic signature also provides a security function, just like the biometric aspect of a wet signature. Under 21 CFR Part 11, signatures must not only ostensibly exhibit an intent to be bound, but must do so with a certain level of certainty, which in the computer world means security. And this security will have to address not only the linkage between signature and record but also, ultimately, the systems surrounding the record, and the policies, procedures and organization surrounding the systems.

A minimal security function is also consistent with the demands of evidence law. Federal Rule of Evidence 901(a) provides that establishing the authenticity of evidence is a condition precedent to admissibility.[14] As pointed out in *Ricketts v. City of Hartford* (2nd Cir., 1996) 74 F3d 1397, 1407, the requirement of authentication is one of the purest examples of a rule respecting relevance: evidence has no probative value if it is not what its proponent purports it to be.

The party offering the evidence has the burden of showing authenticity. *U.S. v. Almonte* (2nd Cir. 1992) 956 F.2d 27, 30.[15] Though authentication hearings may require determination of factual questions, a judge hears them. FRE 104 sections (a) and (b); *U.S. v. Ladd* (1st Cir. 1989) 885 F2d 954, 956. The burden at this stage is slight, requiring the judge only to make a finding, i.e. that there is a reasonable likelihood the evidence is authentic. *U.S. v. Holmquist* (1st Cir. 1994) 36 F.3d 154, 168. However, given the complexity of these issues, particularly since they will be matters of first impression in many courts for quite a while, perhaps these will turn into mini-trials like *Markman* hearings in patent cases.

Winning the authentication battle to obtain admissibility is only the first step. Authenticity for purposes of admissibility can be found even in the face of conflicting inferences. *U.S. v. Reilly* (3rd Cir. 1994) 33 F.3d 1396, 1409. So getting the evidence in does not mean you

---

[14] FRE 902(b)(10) provides that if evidence depends on the outcome of a process or system to produce a result, then authentication might be comprised of evidence showing the process or system produces an accurate result. Various types of electronic signatures, from digital signatures to the stylus and writing pad signatures required by UPS or K-Mart, are the results of a process or system subject to this rule.

[15] This seems to mean that the party relying on an electronic signature must provide evidence of its authenticity. But this may vary, particularly under state law and depending upon the circumstances. In a telephone conversation, Ann Taylor Schwing, author of California Affirmative Defenses, pointed out that under California law the burden might shift to the person best able to provide evidence. She also recommended that defendants denying an electronic contract plead e-signature affirmative defenses as well.

have established a fact for trial. The trier of fact makes its own determination of the authenticity of the admitted evidence and the weight it should be given. *Alexander Dawson, Inc. v. NLRB* (9th Cir. 1978) 856 F.2d 1300, 1302.

The electronic signature definition is a punt. Policy makers balked at making digital signatures the only recognized electronic signature form because of the unknowns in doing so, including rapid technological change obsolescing any codified standard. On the other hand, they apparently recognized their inability to draw a line excluding signature types that are simply not trustworthy. In essence, their policy is to make almost anything **enforceable**, while letting the difficulty of **enforcement** corral the parties into good risk decisions. Caveat naïve early adopters and the case law they will make for us. However, the difficulty in defining what an electronic signature is likely forces the court to make a preliminary determination of exactly the type UETA was trying to avoid.

The absence of clear standards means there will be numerous disputes. They will run from people lying and overreaching, to others simply misunderstanding what a counterparty did or didn't intend. And these are the problems that occur if systems work as intended. There is an entirely different set of problems from the systems side.

D. At the Intersection of Operational and Legal Risk

Two California cases having nothing to do with electronic contracting show why attorneys who practice in this new area best know a little computer security theory, or at least its consequences. *Thrifty-Tel v. Bezenek* (1996) 46 Cal.App.4th 1559, presents the dreary facts of teenage hackers breaking into a phone system. They were eventually found liable for trespass and fraud. The fraud, however, was not committed against a person; it was committed against the company's "computerized network" which the court, in finding liability, characterized as the plaintiff's "agent or legal equivalent." *Thrifty-Tel* at 1568.

The second case involved a real estate transaction. In *Shapiro v. Sutherland* (1998) 64 Cal.App.4th 1534, a broker paid the seller for property (without taking title) and then resold it to a buyer. The original seller failed to state certain facts in its disclosure form and the broker passed on the (false) disclosure unaltered to the ultimate buyer. The buyer sued both the seller and the broker for fraud.

The *Shapiro* court held the seller liable under the "indirect deception doctrine" because an indirect misrepresentation – one made to a person (here, the broker), intended to be repeated to a known class of people (the ultimate buyer) – is equivalent to a misrepresentation made directly by the seller to the indirect buyer. *Shapiro* at 1548. In a computer-contracting context, if Alice were to break into Bob's network and use it to defraud Charlie by appearing to be electronically contracting as Bob, Alice would be liable to Charlie for fraud. But that is not what scares us.

The *Shapiro* court, in what is arguably indicative dicta, exonerated the broker who passed on the fraudulent disclosure, but only because the court found no independent negligence on the broker's part. *Shapiro* at 1547. Independent negligence on the broker's part may have resulted in its liability to the end buyer as well. If these rules are applied to electronic contracting, then a network owner whose network is used to defraud a third party may be liable to that third party along with the fraudster. And security professionals believe that most networks are pretty insecure.

E. I Am Sure *Your* Network Runs Like a Well Oiled Machine

In his latest book on computer security, *Secrets & Lies: Digital Security in a Networked World,* noted expert Bruce Schneier famously states:

> If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology,

This is not a happy message as it speaks to the task's difficulty. Other commentators are even gloomier: the risk of computer intrusion cannot be stopped; only managed. The problem cannot be solved technologically, and perhaps won't be solved even with the addition of appropriately trained people following well-crafted policy. If the task is impossible[16] then failure should not always constitute negligence. But some teams make better efforts than others, and a line must be drawn between those who tried and failed and those who didn't try.

Attack typology is finite, but the variations on type continue to expand as increased system complexity allows more possibilities. The categories include bad passwords, buffer overflows, failures to encrypt, Trojan horses, undiscovered system bugs,[17] exploitable trust relationships, failure to install security patches, viruses, human engineering and insecure reliance on shared libraries. And even savvy companies fall prey because good security is difficult.

Microsoft Corporation was recently hacked. The attacker reportedly exploited a security hole in Microsoft software for which Microsoft had issued a patch. Had Microsoft installed its own patch for its own software running on its own server, it may not have suffered this incident. As it turns out, it was an ethical hack performed by someone counting the coup of successfully penetrating security and getting credit for the scalp. Not all hacks are so benign.

Yet a scarier situation arises with Microsoft as well, but others no doubt suffer the same problem. Microsoft uses digital signature technology to sign its code to prove its authenticity to end users downloading on-line. Recently Verisign mistakenly issued two code-signing certificates in Microsoft's name to an imposter.[18] Though a revocation list for the certificates has been generated, how do you assure distribution and use of that list to everyone on the Internet who may be affected?

These types of events are the leading edge of a new generation of legal advice and litigation. As much as any favorable or unfavorable aspects of law, they will drive electronic contracting adoption. And as we read of security failures we will judge whether the company really cared about security or not and form opinions on their culpability.

As society continues its march to complexity, novel situations give rise to new legal analysis as the old theories are stretched and pulled to cover unimagined fact patterns. The California courts, no strangers to new theories and lots of litigation, developed its six factors test to decide whether Gene has a duty to George when no case or statute provides a ready answer.

---

[16] This is not meant to be discouraging; few risks can be reduced to zero forever.

[17] Bugs used to be mere glitches in code that resulted in performance problems; now they are vulnerabilities to be exploited for denial of service attacks.

[18] There have been no public reports of this incident's cause and this article does not mean to imply which of the parties was at fault or whether this risk could have been eliminated through better process.

And whether any other state or nation adopts all or part of these provisions,[19] they seem a good summary and one that should be kept in mind regardless of the rule covering your particular client. The criteria are:

> …(1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness of the connection between the plaintiff's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct and (6) the policy of preventing future harm.
>
> *J'aire Corp. vs. Gregory* (1979) 24 Cal.3d 799, 804.

It might seem that exploited networks should be exempt from liability. And certainly an argument can be made that network owners are faced with a particularly bad problem: software is rarely warranted in any meaningful way, and manufacturers, intent on winning the race to market, often pay scant attention to security. And, even if they are paying attention, it's difficult to catch everything.[20]

In the absence of a blanket pardon based on futility, it seems quite clear that some court will find liability under the *J'aire* factors, cited above. As is often the case, the burden will be placed on those making money and the insurance industry will be called in to take last position. But there will be difficult times in the early days because e-business insurance is in its infancy. The insurance companies are quite clear that most, if not all, e-business risks fall outside of traditional policies and are offering new products into the gap, such as AIG's netAdvantage Suite.(sm) But these coverages come with strings, including a requirement that network defenses be up to a certain snuff.[21]

Moreover, this is not a happy message to your clients. Trying to make money, they exhibit the same behavior as people who have never been burgled: it won't happen to me so I won't spend a lot of money to prevent it. Security companies try to finesse this mind set by claiming that security is an "enabler" and therefore deserves its rightful piece of the corporate budget. While certain security related technologies such as single sign on do have an enablement patina, the fact is that security is not an enabler, it is a value preserver. Just as a home burglar alarm preserves the value of your belongings to you, security does the same thing for the corporate network and website, and any profits derived from them.

The need for security is increasing quickly. Consider the following trends. Most companies don't understand security because the whole doing business on-line notion is so new. Software, even that with so-called security features, is often insecure. There is high growth in the malicious talent pool driven by curiosity, challenge, apparent anonymity, ready availability of

---

[19] For an excellent article analyzing the basis for various theories based on negligent network security, see Erin Kenneally's "The Byte Stops Here: Duty and Liability for Negligent Internet Security," Computer Security Journal, Vol. XVI, Fall, 2000.

[20] There seems to be little difference between proprietary and open source software in this regard. It does no good to have many eyes watching the open source derived code if those eyes do not know what they are watching for, which is all too often the case for security issues. Some people argue that open source is also vulnerable to Trojan horses implanted by skillful fraudster/contributors who mask malicious contributions. Of course, some argue that proprietary code is vulnerable to Trojan horses implanted by skillful fraudster/employees.

[21] AIG currently offers a free network vulnerability assessment to potential insureds, but only offers insurance to those who pass with a sufficiently high score.

computers and phone connections, ease of secret community, computer intrusion as military training, computer intrusion as terrorism or political statement, computer intrusion as war, and poverty. Finally, there is capitalism itself, which, through the value destroying capabilities of technology, forces companies to become more efficient, meaning closer electronic coupling of all members in the global supply chain. While the closest distance between two points may be a straight line, in computer cracking the fastest path to intrusion is rarely a frontal assault, but instead an assault on a supplier with a trusted connection to a supplier with a trusted connection to you.

E. So What Do We Do?

There are no magic bullets. But clients should be informed as to the risks.

The first step is to obtain a clear picture of the client's current risk posture. Determine whether the ability to enforce contracts is significant. Perhaps the client doesn't litigate contract disputes, instead resolving them by referral to collection agencies.

Assuming the client desires to enforce its contracts by litigation, the lawyer's analysis has two particular purposes: convince a judge that electronic evidence is authentic and then convince a trier of fact that the authenticated evidence is persuasive.

In reviewing the electronic contracting process, divide it into zones. Consider each zone an area to be controlled with particular risks that must be managed through acceptance, avoidance, mitigation or transfer. Develop controls to achieve each risk management objective.

In the first zone is the counterparty. Consider and rate the risk that the counterparty will be a source of concern. Areas to consider might include

- Methods of counterparty authentication,
- Appropriate communications channels given the sensitivity of the underlying transaction[22]
- Appropriate signature types addressing party authentication and message integrity
- Network security practices as evidenced by audit statements
- Trading partner agreements outlining risk allocations.

In the second zone is the transport infrastructure. TCP/IP protocols unleash packets promiscuously and they travel many different paths to get to their destination, sometimes through the systems of direct competitors. Determine whether this is acceptable or whether use of encryption or VANs might be prudent.

In the third zone lies your client's systems and processes, which must then be divided into a number of sub-zones. Each sub-zone addresses the issues associated with a single operation from three perspectives: technology; policy and process; organization and enforcement.

In contracting, the operations include:

- Contract drafting
- Approval

[22] For example, this consideration might require that communications originate from a particular computer at particular times, as opposed to PDAs or phones, to assure non-coercion.

- Signing
- Transmission
- Archiving
- Retrieval
- Audit.

Some issues to consider for an operation are:

- Access controls
- Operational integrity
- Data integrity
- Data confidentiality.

The results of the analysis should be incorporated into an overall risk management plan. The plan should also cover macro issues like business continuity and insurance.

F. Some Standards and Services that May Be Helpful

There are standards governing information security management, the most influential being ISO 17799, based on British Standard 7799, incorporating concepts from early security efforts like the Orange Book and the approach of the Common Criteria. There are a growing number of standards governing public key infrastructures such as ANSI X9.79 for use in financial services, the AICPA/CICA WebTrust SM/TM Principles and Criteria for Certification Authorities, and for European implementations, the ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates. The American Bar Association's Information Security Committee will also soon offer its PKI Assessment Guidelines.

Systems exist for identifying counterparties. CertCo, Inc. has a service it calls RMX that provides a simple XML interface to gather information about counterparties from databases such as Dunn & Bradstreet and EDGAR, among others. AIG and Dunn & Bradstreet have teamed up with an offering at Avantrust.com that provides counterparty identification along with trade credit and insurance. Experian provides identity scoring based on information in your credit history, by requiring you to answer certain questions, some of which they characterize as "in pocket" (e.g. social security number or drivers license number) and some characterized as "out of pocket" (e.g. the amount of your mortgage or car payment, or last electricity bill).

Perhaps the most interesting system for B2B contracting is Identrus. Identrus is a closed PKI provided through the global banking system. It currently has over 40 participating banks that cover some 10,000,000 corporate clients worldwide. Its purpose is to provide counterparty identification in aid of global trade.

All participating banks use the same standards for identifying their customers, meaning that the same identification and authentication processes stand behind Barclays Bank's identification of Triumph Motorcars in the UK, Citibank's identification of General Motors in the US, and Sumitomo Bank's identification of Toyota in Japan. When the system goes operational parties may obtain warranties provided by their own bank against counterparty identity fraud and the system comes complete with dispute resolution mechanisms. The result is a homogenous risk environment both in terms of identification risk and identity warranty performance.

PKI based systems will also become easier to implement, should PKI prove to be the electronic signature type of choice. VeriSign, in conjunction with Bank of American, Microsoft

and webMethods is proposing XKMS as an IETF standard that will make private key registration and signing party verification quite simple through XML interfaces. This will allow device providers to simply plug their devices into a trust infrastructure and be PKI enabled.

F. Conclusion

The Internet is in its infancy and many risk issues have yet to be addressed. Companies such as Identrus and VeriSign are working to reduce complexity and increase certainty. But part of the solution requires the legal profession to attack the issues proactively, acting as the risk manager most companies won't hire (relying instead on their insurance brokers to plug leaks while not recognizing that the entire levee may go).

We have all heard of the Chinese curse wishing that an enemy live in exciting times. These are exciting times indeed.