

GREAT FOR PROTECTING: IMPORTANT EMAILS • CLIENT FILES • SCANNED PAPERS • TAX DOCUMENTS • REGULATED CORRESPONDENCE • HR DOCUMENTS

Demand proof – for you and your business

Proving authenticity of electronic records and digital events is emerging as a significant business, legal and IT issue. In fact, following the past decade of corporate scandals, the courts and regulators are increasingly requiring companies to demonstrate the authenticity of their business records.

The burden of proof... is on you!

The legal system is transforming how businesses must manage electronically stored information (ESI) and prove its authenticity. Under the December 2006 amendments to the Federal Rules of Civil Procedure.

The Sedona Conference, a prominent group of leading judges, litigators and e-discovery experts, are in the process of developing commentary and guidelines regarding the fundamentals of authenticity for ESI and the technical underpinnings affecting qualifying ESI-based evidence, as required by the Federal Rules of Evidence. But until those guidelines come out, you're on your own.

"The security industry has been running backwards in our view — starting at the edge (perimeter) and working its way to the data itself. The availability and protection of the data is the core need... but trying to block sessions at the firewall or stripping out malignant emails... completely missed the insider threat problem. Perhaps closest to the core is a small company (ProofSpace) we've seen trying to establish the integrity of the data itself with the non-debatable tag of time."

— Peter Kuper,
Internet Security Analyst,
Morgan Stanley Research Brief, March 15, 2007

Case in point

The authenticity issue is becoming a pivotal one in cases across the country. In two separate cases, American Express and Markel American Insurance company both lost lawsuits because of their inability to prove their own electronic business records as pristine and authentic, and thereby get them admitted into evidence.

Amex tried, and failed, three times to demonstrate the authenticity of its electronic records and eventually lost the case. The winning defendant — a client who didn't have a lawyer — never even showed up for the court date!

The judge from the Markel case, in an opinion letter from May 4th, 2007 wrote, "although 'it may be better to be lucky than good,' as the saying goes, counsel would be wise not to test their luck unnecessarily. If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied. If less is required, then luck was with you."

This scenario is recurring with increasing frequency as lawyers, clients and regulators become more cynical about the validity of electronic documentation. This growing cynicism is based on an awareness of the vulnerability of virtually all applications to their "administrators", even in the context of modern content management solutions and other managed systems.

Inadequate defense

Magnetically stored data can be easily and undetectably changed, especially when it travels across application and control boundaries. Currently available solutions (PKI based time-stamping systems) are expensive, difficult to implement and can be unreliable. Additionally, most perimeter-based solutions today don't protect email, attachments, spreadsheets, or PDF files from tampering by people inside the organization, or while those documents are in the custody of clients or other third parties.

So how can you prove that you haven't tampered with your own records? How do you prove to a judge that a client did, in fact, instruct you to take a specific action at a specific point in time? How do you comply with SEC regulations to preserve the integrity of data? How can you ensure that your drug applications to the FDA won't be refused?

More to the point — how do you protect yourself? How do you generate this proof while operating your day-to-day business with minimal staff and documentation that proliferates endlessly?

