

The danger of exposure to the Internet

Care must be taken when presenting computer data in court to make sure alteration has not taken place through exposure to the Internet

Mike Cherry and Edward J. Imwinkelried

• *LAWSUIT #1:* You are suing a pharmaceutical company which recently released a new drug onto the market. You represent a class of persons who became seriously ill after using the drug. The medical trials for the drug were conducted by a local research institution. When you sue the company, the company attempts to persuade you to drop the suit. The company insists that the trials did not reveal any of the side effects suffered by your clients. As part of the company's effort to persuade you, they voluntarily provide you with the printouts of the trials' data from the institution's computers. Indeed, the printouts indicate that there was no indication of such adverse effects. Moreover, the institution itself allows your forensic computer expert to inspect their system. Your own expert tells you that the printouts are accurate and that the metadata for the files does not indicate that any institution employee tampered with the data. Is that endgame for your lawsuit?

• *LAWSUIT #2:* You are suing a financial institution. You represent a class of customers of the institution. Identity thieves gained confidential information about your clients from the financial institution's computer system. The institution insists that it was not at fault. The institution's IT personnel point out that they use a "state of the art" combination of firewalls, virus scanners and filters. Does the defendant's use of that technology provide a complete defense to your lawsuit?

There is a strong argument that, in both lawsuits, the answer is, "No."

We are entering an era of rampant error in Internet data. It may soon become impossible for the courts to determine the truth based on digital information. In the long term, America should implement a strategy of isolating key computer systems with sensitive data from the Internet. In the short term, the judiciary ought to generally adopt a more skeptical attitude toward computer data proffered in court and, in particular, permit plaintiffs' attorneys to conduct extensive discovery concerning the possibility that the data has been compromised by alteration.

The hard reality is that if you want to keep computerized information safe and secure, the computer system should not be exposed to the Internet. Unfortunately, in practice that reality has been almost universally disregarded. Instead, public and private sector computer systems rely on Internet surfware such as virus scanners, firewalls, spyware detectors, penetration detectors and filters to minimize the risks associated with an Internet connection. Those security measures are helpful, but they are far from foolproof. Internet hacking is so pervasive and effective that, in many cases, it can defeat these measures. In the United States alone, despite the widespread use of such security measures, millions of false identifications are created every year. As a consequence, there are grave and growing doubts about the reliability of even the most critical data maintained in law enforcement and regulatory computer systems. As we shall see, better solutions are available, but they will come at a cost.

Introduction

Virtually every sector of American society has decided to rely increasingly on computer data. The very future of our society is tied to the accuracy and security of that data. For example, a steadily increasing number of statutes and regulations prescribe requirements for the accuracy and confidentiality of such data:

• The **Sarbanes-Oxley Act** mandates such requirements for certain financial data [15 U.S.C. §§ 7201-66].

• Under the **Gramm-Leach-Bliley** legislation, financial institutions must take steps to secure customer data from

Copyright © 2008 by the author.
For reprint permission, contact the publisher: **www.plaintiffmagazine.com**



unauthorized access. [15 U.S.C. §§ 6801-27].

• For its part, **Health Insurance Portability and Accountability Act (HIPAA**) [Pub.L. No. 104-191, 110 Stat. 1936 (1996)] imposes security measures for the information that doctors, nurses, and other health care providers insert in patients' medical files.

• Under the **FBI/INS/Homeland Security** program, fingerprint repositories used to identify criminals and terrorists must be secured from tampering.

• In **medical trials**, the accuracy of test results throughout product development has to be protected.

Like the average citizen, the typical participant in the legal system tends to have naive faith in the effectiveness of the popular safeguards against Internet alteration. During both pretrial discovery and at trial, the focus is on the question of whether the evidence proffered at trial correctly reflects the data on the computer. The texts and articles on e-discovery address such problems as acquiring diskettes printed out from the computer, learning the passwords to the electronic files and gaining access to the hard drive. Today the "hot button" discovery issue is obtaining the metadata, the embedded information which reflects the deliberate changes to the electronic file. At trial, when the proponent lays a foundation to *authenticate* computer data under Federal Rule of Evidence 901, the understanding is that the proponent's obligation is to show that the exhibit tendered at trial accurately reflects the data in the computer. In the typical trial, there is little, if any, attention to the risk that Internet alteration may have rendered the data substantively inaccurate.

As we shall see in the initial section of this article, today that is a huge risk. Every year computer thieves create 10 million false identifications[1] in the United States. Those thefts are only the tip of the iceberg of alteration. The second section of the article explains that the problem is mounting precisely because of the inadequacy of current strategies relying on Internet surfware. The final part of the article argues that a radical solution is necessary: isolation. And when we use the expression, *isolation*, we mean it in a truly radical sense. We do not mean a mere firewall – Internet hackers often defeat firewalls. Rather, we mean that computer systems maintaining sensitive data should be isolated from the Internet, from any resource that has been in contact with the Internet, or even any resource that has interfaced with a resource that has contacted the Internet.

Simply stated, despite funds previously spent, business and government computers used to maintain the crucial records necessary to comply with statutes such as Gramm-Leach-Bliley, Sarbanes-Oxley, Homeland and HIPAA, must be reengineered to operate in an isolated production environment free from Internet alteration. The accuracy and security of the data we rely on can be guaranteed only if we adopt a fundamentally different strategy to counter computer theft and alteration. The shift in strategy to radical isolation may be expensive and inconvenient, but it is nonetheless imperative.

The magnitude of the problems of theft and alteration

The accuracy and security are concerns for both the individual citizen and society as a whole. A recent USA Today story discussed an all-too-typical identity theft victim:

David Joe Hernandez returned to his home in Oak Forest, Ill after a four-year Air Force enlistment to find collection agents coming after him, looking to make good on some 20 accounts opened in his name and drained to the point of delinquency. Unfortunately, the ramifications of Mr. Hernandez's identity theft did not end with cleaning up his bad credit report. As an employee of Best Buy, he was informed his salary would be garnished to pay child support to a woman he never met. It took weeks and meetings with state family officials to prove his whereabouts in the military. Ironically, he later lost his entire salary after being terminated as the result of an erroneous criminal check linking him to a string of felonies, including drug charges.

To date, Mr. Hernandez has spent a year and half of his time and resources to recover his identify. Unfortunately, Mr. Hernandez's case is hardly an isolated incident. Internet hijacking and the manipulation of information are pervasive. As previously stated, approximately 10 million untrue identifications are created each year in the United States.

Although identity theft is a problem, alteration poses an even broader challenge to the security of computer data. Achraf Bahloul,[2] a Moroccan resident, was recently convicted of writing computer attacks that in August 2005 infected more than 100 American organizations including banks, news networks, the Immigration and Naturalization Service, US Homeland Security, and perhaps even a number of Automated Fingerprint Information System sites. Related Freedom of Information Act documents indicate the extent of the danger; those documents suggest that at least 1,313 of the infected Homeland Security computers were of the very type used to determine whether the same person who was approved to travel to the United States was in fact the person who entered the United States.

Atilla Ekici[3], a resident of Turkey, is charged with paying Achraf Bahloul to write the attacks for him. FBI Cyber Division Assistant Director Louis M. Reigel III[4] remarked, "In today's world of sophisticated technology, cyber criminals need very few tools to carry out their crimes. With a few strokes on a keyboard and a click of a mouse, malicious computer code can instantly spread across computer networks all over the world causing significant damage and dollar loss."

Commenting on the Bahloul incident, Mark A. McManus, vice president of technology and research at Computer

Copyright © 2008 by the author.
For reprint permission, contact the publisher: **www.plaintiffmagazine.com**



Economics, a California consulting firm, stated that "[a]s enterprise hacks go this was considered a small one." He prepared a chart illustrating the impact of the major hacks. His chart listed several hacks costing in excess of $10 billion, worldwide. According to his chart, the Bahloul incident may have cost $500 million.

The current inadequate security strategies

These problems have arisen despite the highly publicized push to use up-to-date virus scanners, firewalls, spyware detectors, intrusion detection and filters. These products are not foolproof. A naive belief in and reliance upon their overall security capabilities are a large part of the problem.

An "all clear" from the combination of a virus scanner, spyware detector, penetration detector and filters is not strong enough to guarantee that no alteration exists. An active virus may be present for years before the Computer Emergency Readiness Team (CERT) or virus scanner finally identifies it. Penetration detection and correction are fallible. Undiscovered alterations from the Internet may be well nigh inevitable. However, given the stakes, we must do everything within reason to prevent the alteration of the computers involved in the administration of HIPPA, Sarbanes Oxley, Gramm-Leach-Bliley, medical testing and FBI/INS/ Homeland.

The harsh reality is that most of the computer systems currently in place have hacking vulnerabilities, only some of which have been discovered. Those vulnerabilities exist in the private as well as the public sector. For example, many Internet shopping sites claim they are "Hacker Safe." Yet, based on their testing for vulnerabilities, Sla.ckers.org found that many sites easily open to hacking.[5] "Add Ace Hardware, American Red Cross, GNC, HP, Johnson & Johnson, Nike, Northrop Grumman, Petco, Ritz Camera, the Red Cross, Sony, Sports Authority, World Bank, Yahoo, and Yankee Candle to the list of Hacker Safe-labeled Web sites identified by sla.ckers.org as containing ...vulnerabilities."[6] Internet shopping sites should do more to vigilantly protect the sensitive information in their possession. New information such as credit card numbers, Social Security numbers, and resumes ought to be quickly encrypted, and previously collected information should be isolated from the Internet and its constant stream of hackers.

Isolation strategies

One technical solution is to isolate and segregate all mission critical computer- based information including Homeland, Gramm-Leach-Bliley, Sarbanes-Oxley and HIPAA from the Internet and from any computer or IT resource connected to the Internet. To be frank, though, Internet use is such a common practice that its discontinuation will be both time-consuming and complicated.

A second technical solution is to revert to the past: building computer processes that are unreceptive to alteration. Modern computer technology allows additions and changes to be made while a process is running. Unfortunately, many of the additions are viruses. In contrast, the large banking applications that process billions of dollars every night were developed before this built-in capability for change became widespread.[7] The fact that these older computers lack the change capability explains why large money banking breaches do not occur and why those systems do not need virus scanners.

Conclusion

What does all this mean to American society in the long term? Simply stated, we have to confront the reality that half measures such as Internet surfware are inadequate to protect the accuracy and security of our most sensitive computer data, including information introduced in court. Even though it will entail considerable cost and time, the most viable strategy is isolating computer systems maintaining critical data from the Internet.

What does this mean for the legal system in the short term? When a defendant company or agency offers computer data in court, the plaintiff's attorney should demand to know whether the data has been maintained in a computer system isolated from the Internet. If not, the judge should accord the plaintiff especially liberal discovery of the proponent's computer system. It is not enough for the defense to produce accurate printouts of the data in the system; if the system has been exposed to the Internet, the data itself may already have been compromised. The court ought to permit the plaintiff's experts to examine the proponent's computer hardware and software – and allow testing for alteration, including the presence of viruses and spyware. Some alterations of digital information are not detectable, but others are. Further, the plaintiff may be able to identify evidence of alteration by comparing source data with the version of the data on the computer in question. If the defendant's system has not been isolated from the Internet, the plaintiff should have the right to test for indicia of alteration.

In addition to permitting thorough pretrial discovery relating to Internet alteration, judges should allow the airing of the issue at trial. When the defense's IT experts take the stand, the judge ought to permit probing cross-examination about the extent to which the computer system has been exposed directly or indirectly to the Internet. The cross-examination can explore the safeguards incorporated in the system as well as the safeguards that have been neglected.

Further, the judge should allow the plaintiff to present expert testimony about the magnitude of the problem of Internet alteration and the vulnerability of the popular safeguards to hacking. In the words of Federal Rule of Evidence 702, such testimony "will assist the trier of fact to understand the evidence"; that is, to appreciate precisely how vulnerable computer data is to alteration. Unless we immediately confront the problems aris-

Copyright © 2008 by the author.
For reprint permission, contact the publisher: **www.plaintiffmagazine.com**



ing from computer systems' exposure to the risk of Internet alteration, alteration could become so widespread that it will seriously hamper the courts' search for truth. The plaintiff's bar can help to educate the courts about the inadequacy of the existing Surfware technologies to protect this nation's most sensitive data.

Endnotes:

[1] http://www.ftc.gov/opa/2005/02/ncpw05.shtm
[2] http://www.fbi.gov/pressrel/pressrel06/zotob091306.htm
[3] http://www.fbi.gov/pressrel/pressrel06/zotob091306.htm
[4] http://www.fbi.gov/pressrel/pressrel05/zotob_release082605.htm
[5] "Dark Reading," November 13, 2006, http://www.darkreading.com/document.asp?doc_id=110363
[6] http://www.darkreading.com/document.asp?doc_id=110495&WT.svl=news1_3
[7] Kernel and shell based applications integrity assurance http://doi.ieeecomputersociety.org/10.1109/CSAC.1997.646171

Michael Cherry is the president and chief technology officer at Cherry Biometrics Inc., a technology firm that focuses on Internet security and identification/authentication solutions. He is vice chair of the Digital Technology Committee for the National Association Criminal Defense Lawyers. He votes on the international biometric standards used by law enforcement including the FBI and Interpol.


Cherry

Ed Imwinkelried is the Edward L. Barrett, Jr. Professor of Law and Director of Trial Advocacy at the University of California, Davis, School of Law. He is a former chair of the Evidence Section of the American Association of Law Schools. He is the coauthor of Scientific Evidence *(4th ed. 2007) and* McCormick, Evidence *(6th ed. 2006). He is the author of* Evidentiary Foundations *(6th ed. 2005) and* The New Wigmore: Evidentiary Privileges *(2002). He has lectured on evidence and trial advocacy in 46 states.*

The authors would like to thank Frank Pergolizzi, information technology specialist, for his contributions to this article.

Copyright © 2008 by the author.
For reprint permission, contact the publisher: **www.plaintiffmagazine.com**