

# The causation issue in computer security breach cases

Courts must recognize that obsolete computer systems are a major cause of security breaches.

by Michael Cherry and Edward Imwinkelried

The growing number of computer security breaches has led to a proliferation of lawsuits, including class actions, against the companies that have experienced breaches—and consequently exposed their customers and clients to the risk of identity theft. One of the key issues in such litigation is causation: What caused the breach, and could the company have prevented it?

The truth is that the system itself—our current approach to cyber security—is badly flawed. The large number of recent, large scale breaches of computer security—including Hannaford Farms, Heartland, and Countrywide—is stunning. Despite all the highly publicized efforts to improve cyber security, the situation seemingly continues to worsen.

Early computers used a limited set of commands that unintentionally minimized the possibility of hacking. The personal computer, which developed decades later, chose a very different approach. The PC used a very responsive interface that allowed suppliers and others to dynamically add new equipment and procedures through the use of simple instructions. Understandably, the vast majority of public and private sector organizations opted for PCs. The obvious upside was that PCs were less expensive to maintain because it was easier for support personnel to master them. However, the combination of the lack of rigorous authentication and the ease of adding new procedures had a significant downside:

It made it virtually impossible to prevent hacking.

As the internet evolved, hacking became more widespread. Organizations attempted to block hackers by resorting to add-ons such as virus scanners, “strong” passwords, and network testing. Ever since suppliers have been on a treadmill, constantly providing users with updates for new add-ons. This reliance on add-ons has failed. It is easier and faster for a hacker to write a new virus than it is for the virus industry to identify an existing one and devise an add-on to counter it.

To prevent hacking, we could: (1) rewrite Windows and UNIX to make them less responsive, or (2) convert to a new operating system that is less responsive and consequently less vulnerable. Both efforts will require significant re-engineering and conversion. But in the meantime, whichever option we choose, we must immediately ensure that systems have the capacity to automatically recognize a breach in progress and the related capability to automatically lock down all sensitive information.

Consider the Countrywide incident. At Countrywide, an employee, a mortgage loan evaluator, brought home more than 5,000 different mortgage applications for “review” every weekend for almost two years. It would have been amazing if he had managed to thoroughly review even 50 files during a single weekend. Yet, he continued bringing home these massive quantities of

sensitive information for an extended period of time until his partner in crime, the buyer of the mortgage applications, was finally caught. By any rational business standard, it should have been obvious that large quantities of sensitive information were being inappropriately retrieved. But Countrywide’s security system did not catch the mortgage loan evaluator because the system did not incorporate any specific retrieval limitations based on business standards.

In the instances of Heartland and Hannaford, large quantities of sensitive information were electronically sent to a third party. The existing computer security systems permitted the transmission of huge amounts of sensitive data to outsiders without sounding any alarm even though it should have been obvious to any objective observer that the massive transmissions deviated from the companies’ normal business process.

Today’s information protection procedures rely almost entirely on external measures such as tests for viruses and malware, passwords, and the use of white-hat hackers to identify network weaknesses. None of these measures factors in an understanding of the normal operations of the business-at-large. That glaring gap is their Achilles heel.

## What’s needed

Since the Year 2000 Problem, large corporations and government entities have evidenced a strong resistance to re-engineer their computer

environments. However, that is exactly what is needed. New procedures are required to (1) automatically recognize when sensitive information is being inappropriately retrieved while it is occurring,<sup>1</sup> and (2) instantly take defensive action, just as when a jet fighter takes evasive action to escape an incoming missile as soon as the jet's radar signals a lockon. The failure to embed these protections is the real cause of security failures.

If we are to prevent large scale breaches, it is imperative that computer systems incorporate the capability to recognize automatically when sensitive information is being inappropriately retrieved. A breach cannot be stopped in time to prevent serious damage unless it can be detected while it is in progress. In case after case—from Hannaford Farms to Heartland to Country-wide—senior executives told the media that despite the massive amounts of data involved, they were unaware of a breach until a third party alerted them to suspicious activity days, weeks, or months after the breach.

In addition to the capacity to automatically recognize a breach in progress, systems need the related capability to automatically lock down all sensitive information. Once the breach is detected, there must be an immediate lockdown. Computer systems have to implement both of

these capabilities to end the long running nightmare of large scale breaches

When an individual plaintiff or a class of plaintiffs sues for a breach of computer security, causation is inevitably one of the issues at trial. The plaintiff must establish that the defendant's action or inaction caused the breach. In past trials, the battle over causation has often focused on the extent to which the defendant employed external add-ons to safeguard the sensitive information of its clients and customers.

However, in fact the causation issue involves much more fundamental questions about the design of the computer system that has been penetrated. At trial, it is highly relevant to inquire about the extent to which the system incorporated logic that would have provided an automated alert and triggered an electronic lockdown. In analyzing the causation issue, the courts and litigants must move beyond the superficial question of add-ons. The problem of causation in computer security breach litigation runs far deeper than that. Systems that lack automated alerts are obsolete and need to be updated.

As the courts probe these causation issues, it will become increasingly clear that that computer systems' failure to embed automated alerts is the root problem and that obsolete computer systems are

largely responsible for the major security breaches. At that point, legislative intervention may be appropriate. A new law, mandating these fundamental changes, may be necessary to guarantee cyber security.<sup>2</sup> In the meantime, though, the courts can lead the way by demanding that litigants address the basic causation question: How could this breach have been prevented? ☞

© Copyright 2009 Michael Cherry and Edward Imwinkelried, all rights reserved.

**MICHAEL CHERRY**

is the Vice Chairman of the National Association of Criminal Defense Lawyers Digital Technology Committee and President of Cherry Biometrics Inc.  
(mcherry@cherrybiometrics.com)

**EDWARD J. IMWINKELRIED**

is the Edward L. Barrett, Jr., Professor at the University of California, Davis, School of Law.  
(ejimwinkelried@ucdavis.edu)

1. This also applies to transmitters placed on ATM and credit/debit card readers.

2. The law might require that an organization automatically detect when its sensitive information is being inappropriately retrieved as it is occurring. Upon detection, it must instantly protect all of its sensitive information from exposure. All ATM's and credit card readers, including those attached to cash registers, must be tamper proof, transmitter free, and must scramble (encrypt) the information they read.