# Fixing the Cyber Security Problem

September 1 2009

(PhysOrg.com) -- Our flawed approach to cyber security needs a dramatic overhaul -- and courts should lead the way to reform, argues Edward Imwinkelried, a professor of law at the University of California, Davis, and one of the nation's leading experts on scientific evidence.

In an article in the September-October issue of *Judicature*, a refereed journal published by the American Judicature Society, Imwinkelried and co-author Michael Cherry call on courts to recognize that obsolete computer systems are a major cause of security breaches.

"As the courts probe (the) causative issues, it will become increasingly clear that computer systems' failure to embed automated alerts is the root problem," they write.

The authors contend that firms must be required to institute the following safeguards to prevent potentially devastating cyber security breaches:

• The ability to automatically detect when sensitive information is being inappropriately retrieved -- as the breach is occurring.

• The ability to instantly protect sensitive information from exposure on detection of a breach.

• ATMs and credit card readers should be tamper proof as well as transmitter free, and they ought to scramble (encrypt) the information that they read.

Recent large-scale breaches of computer security at major companies such as Hannaford Farms, Heartland and Countrywide were not discovered until days, weeks or months after they occurred, the authors note.

In past trials over cyber security breaches, Imwinkelried says that most arguments have focused on the extent to which companies employed external add-ons to safeguard the sensitive information of their clients and customers.

Instead, Imwinkelried urges courts and litigants to "move beyond the superficial question of add-ons."

"The problem of causation in computer security breach litigation runs far deeper than that," he says. "Systems that lack automated alerts are obsolete and need to be updated."

Imwinkelried stressed that the issue has broad significance beyond the courts. "Legislatures contemplating new statutory computer security mandates and companies hoping to upgrade their security should address this as well," he said.

Imwinkelried is the Edward Barrett Jr. Professor of Law at UC Davis and co-author of "Scientific Evidence," a leading treatise in the field that has been cited several times by the U.S. Supreme Court. Cherry is vice chair of the Digital Technology Committee of the National Association of Criminal Defense Lawyers and president of Cherry Biometrics, a Virginia-based consulting firm that advises corporate clients on cyber security of computer systems.

About UC Davis

Citation: Fixing the Cyber Security Problem (2009, September 1) retrieved 27 April 2024 from https://phys.org/news/2009-09-cyber-problem.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.