Data Destruction

TAKING LAPTOP SECURITY BEYOND PASSWORDS, ENCRYPTION

BY CAM ROBERSON, MBA, AND DOUGLAS J. RUSCH, CPA

For some time, you've been reading about the risks of data exposure. And while we believe that businesses have gained the upper hand in dealing with hackers, a new threat is emerging—lost or stolen PCs, specifically laptop computers.

According to research firm IDC, as much as 60 percent of corporate data resides unprotected on desktop and laptop computers. Client information, intellectual property, customer identity files, financial plans and other sensitive information are just one misstep away from compromise.

And according to a CSI/FBI survey, one in 10 laptops will be stolen. Of these, less than 3 percent will be recovered.

The potential cost of even a single lost PC, including negative publicity, regulatory non-compliance and legal liability can be staggering.

State and federal lawmakers have stepped in with legislation to better protect personal identity information, including the California Security Breach Act (SB 1386), which mandates a business that owns or licenses electronic personal information must disclose any security breach of the system to any resident of California whose personal information was, or reasonably believed to have been, acquired by an unauthorized person.

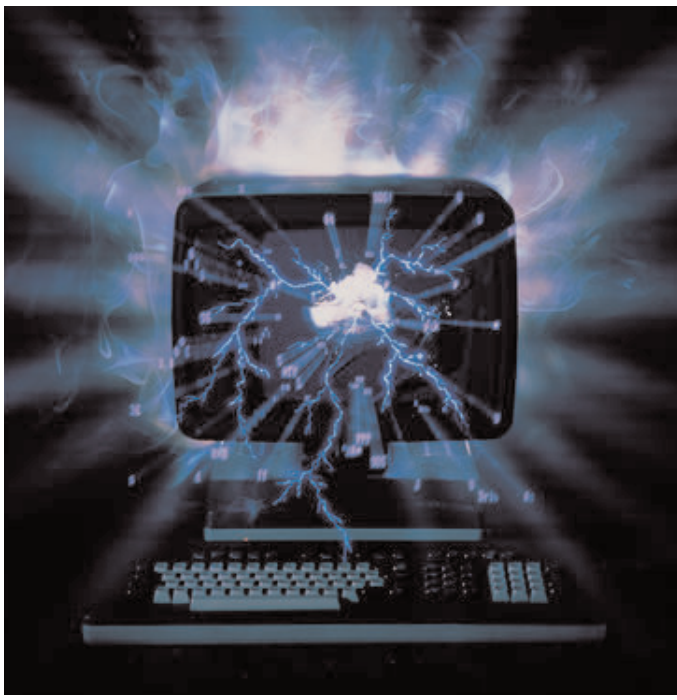
Other federal legislation includes the Health Insurance Portability & Accountability Act; the Financial Modernization Act of 1999, popularly know as the Gramm-Leachy-Bliley Act; the Fair and Accurate Credit Transactions Act of 2003; and the Sarbanes-Oxley Act.

Clearly, companies must take absolute care to ensure data security. But where to begin?

IT professionals have stressed the use of strong passwords, data encryption, tokens (a portable user authentication device that is usually read or plugged into the computer), biometrics and data back-up plans.

However, security measures such as strong passwords too often rely upon the end-user for efficacy. Users routinely select passwords that are easy to remember—birthdates, children's names or other personal information—so they can access their computer quickly. While easy to remember, these passwords also are easily cracked via multiple means.

But laptop security is moving to the next level, from a system that relies on the user for security to one that puts controls in the hands of the business.



DATA DESTRUCTION

An emerging data protection plan is data destruction—software that can reach out and eliminate data from a computer after the business has lost the device.

Data destruction provides an absolute, final step in ensuring that behind authentication, no matter how robust, sensitive data is not exposed to unauthorized eyes.

Data can be destroyed by a variety of trigger mechanisms. If a client/host communication can be established, destruction commands can be pushed down from a host server and executed on the lost or stolen laptop.

This is a fairly straightforward process, but requires a network connection.

Since a business can't be assured that a laptop will again connect to the internet, other triggers should be established to eliminate sensitive data.

Such triggers can be based on pre-set rules and conditions, including maximum time between communication events or number of unsuccessful login attempts.

If either of these behaviors violate or exceed parameters that the company has established, the data should be eliminated.

In this instance, the user has access to the data for that finite amount of time the company establishes. That period, however, can be extended when the user checks in with the server and provides proper authentication.

Data destruction provides further assurances that the company can exercise control over the data for which it's responsible, even if the hardware is outside its control. Destroyed data is the only data that a company can be sure will never be compromised.

Computer users should be focused on productive mobile computing tasks that generate returns for the company, and not security compliance. To do so, the company must have the tools that provide control over the data that resides on laptops—no matter how far they stray from the confines of the traditional network. CPA

Cam Roberson, MBA, *is director of marketing communications and* **Douglas J. Rusch, CPA**, *is controller for Santa Clara-based Beachhead Solutions. You can reach them at croberson@beachheadsolutions.com and drusch@beachheadsolutions.com, respectively.*