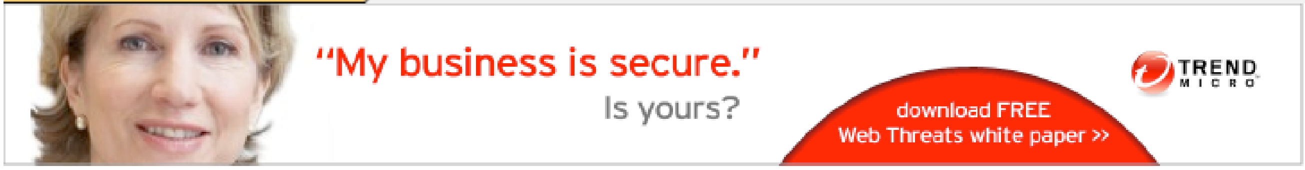
eWEEK ENTERPRISE NEWS & REVIEWS



Securing the Laptop: Mission Impossible?

November 21, 2007

By Stan Gibson

Nearly every week, the report of a stolen laptop hits the news and, with it, a horror story of data loss, identity theft and corporate liability. With a downside that steep, it's no wonder that the laptop is the target of corporate IT security campaigns nationwide. Few corporate executives will sleep soundly until their IT managers have done all they can to lock down laptops and limit the sensitive data on them.

But that's easier said than done.

Lotusphere 2008
IBM
SEE what's new
HEAR the inside scoop
DO things you can't do anywhere else
Come see what all the buzz is about
January 20 - 24, 2008
Walt Disney® World,
Swan and Dolphin Resort
Lake Buena Vista, FL
Register by January 16th to take advantage of the special, discounted rate.

RELATED LINKS

- TSA Demands Encryption Following Dual Laptop Loss
- Romney Campaign Laptops Stolen
- Full-Disk Encryption Is Partial Protection, Analysts Say
- To Encrypt or Not to Encrypt
- Why Encryption Didn't Save TJX

In the age of personal computing, the laptop has emerged as the preferred productivity device for professionals across many industries, thanks to its convenience, usability and ever-increasing power. Because of that popularity, the path to securing laptops is strewn with difficult choices and compromises. Only one thing is certain: The freewheeling laptops-everywhere age is over.

The vulnerabilities that go hand in hand with laptop usage are no secret.

First, the laptop can be stolen. No one likes to lose a spiffy laptop, but most companies can afford to spend a couple of thousand dollars to replace one. However, the data on the laptop could cost a company billions of dollars once all liabilities are added up.

Click here to read more about laptops stolen from the Romney campaign.

Second, CD burners and USB drives sit ready and waiting to drain off critical data and pour it into the hands of thieves.

Third, laptop users are likely to fire up their systems outside corporate firewalls and inside unsecured Wi-Fi networks. They're also likely to swap USB drives with friends and business contacts, as well as participate in consumer file-sharing networks. Those usage patterns exponentially increase the likelihood of data loss and the chances of picking up spyware, Trojans and bots. And that malware may expose sensitive corporate information to thieves via keyloggers and system monitors such as those used in the massive 2006 data theft from clothing retailer TJX.

Faced with such a daunting array of threats, most IT professionals are way beyond the naive stage when it comes to securing laptops and the data on them. Just how far IT pros have gone, or will go, depends on the data's importance, the company's computing needs and just what is politically acceptable in the corporate work force.

Thus, organizations in different industries respond in different ways. A local bank, for example, may limit laptops to a handful of top executives; a global industrial company may be unable to limit the number of laptops but may be able to limit the data that can be stored on them and follow up with an aggressive education campaign.

A logical response for many IT pros is to start with a risk assessment to find out who has what computing devices and who has access to what data. With that information in hand, a defensive strategy can be formed and implemented.

Yet IT managers often find it makes more sense to shoot first and ask questions later—to encrypt all laptop hard drives without taking the time and trouble to analyze precisely who has access to what. Similarly, IT pros are finding it's more efficient to encrypt a hard drive entirely than to pick out, say, only sensitive files for encryption.

The age of encryption

It's safe to say that the age of laptop hard drive encryption has arrived, for two main reasons: technology advances and legal requirements.

Just a few years ago, encrypting a hard drive unacceptably degraded system performance. Faster processors have changed that. "Three or four years ago, it wasn't nearly as realistic an option as it is today, because of the performance hit," said Jon Allen, information security officer at Baylor University, in Waco, Texas. "Now, it's a 3 percent to 5 percent impact on the CPU, which is not noticeable for most users."

Click here to see an eVideo on notebook drive encryption.

In addition, legislation in many states requires that an organization disclose the thefts of laptops containing personal information if the data on them is unencrypted. Such disclosures require the time and trouble of mailings and press releases to affected parties. And such mea culpas can give organizations a public black eye that damages credibility and prestige.

Baylor finds itself in the middle of a mushrooming laptop population among its 2,500 faculty and administrative staff members, combined with a greater impetus than ever to protect laptop data. The result has been a campaign to encrypt the hard drives of all laptops belonging to faculty and administrators.

"Higher education has seen a great move to mobility," Allen said. "We have gone from a few laptops to a good majority. That really changes the way you look at data security."

Page 2: Securing the Laptop: Mission Impossible?

Allen began the process of hard disk encryption two years ago using PGP's Whole Disk Encryption and Universal Server. It was not practical to do a full-blown inventory project, Allen said, so he started with laptops known to contain confidential data. Earlier this year, encryption of all faculty and staff laptops, along with some desktops, was completed.

Centrally managed PGP encryption does not, however, extend to Baylor's approximately 14,000 students, 93 percent of whom have laptops. In safeguarding data on those systems, the university seeks to control access to sensitive information and prevent it from getting on student systems to begin with, according to Allen.

Kevin Wilson, an architect planner for the desktop at an energy company in North Carolina, took a similar approach. "It's easier to encrypt them all rather than to find the ones that are most at risk—and then risk the theft of the one you haven't encrypted," Wilson said. "If I put a machine name in an Active Directory group, then it's going to get encrypted. I can do 20,000 as easily as I can do 20."

Even so, Wilson does move laptops that are likely to contain personal information to the top of the encryption queue. He said he uses Utimaco's SafeGuard Easy for encryption.

In his next wave of laptop purchases, Wilson is ordering systems that come with hard drives pre-encrypted by the manufacturer. This will save time and trouble, Wilson said, but will also introduce an additional type of encryption to his organization, creating the burden of carefully tracking and managing each system.

Gartner analyst John Girard said the presence of multiple encryption methods in an enterprise means IT pros need broader management tools. "An encrypted drive is a great idea, but you need an overarching system that lets you manage the drives," Girard said. "Your primary encryption method needs to offer management of other encryptions."

Businesses that upgrade to Microsoft's Windows Vista Ultimate or subscribe to the company's Software Assurance program may deploy Microsoft's BitLocker encryption algorithm, but since most companies won't move all their systems to Vista at once, they are also likely to face the problem of managing a laptop population using different types of encryption. Furthermore, BitLocker encrypts only single drive volumes and not USB drives.

A laptop with an encrypted hard drive could still be a leaky data faucet if it is used to write critical information to a USB drive or to burn a CD or DVD. The approaches taken to eliminating these sources of data leakage range from the reported use of glue to plug USB drives by some federal agencies to the disablement via software of CD- and DVD-burning capabilities.

Full-disk encryption is only partial protection, experts say. Click here to read more.

These measures, while effective, tend to rile users because they impede the utility of their laptop machines. IT managers are likely to find that purchasing encrypted USB drives or software for encrypting the data stored on USB drives and CD and DVD storage makes more sense.

To ensure that sensitive data never is written to removable storage devices in the first place, organizations can choose from a variety of software from vendors such as Reconnex and Vontu that recognizes patterns in data—such as telltale signs of intellectual property or the numerical pattern of Social Security numbers—and prevents writes from taking place when those patterns are detected.

Another approach is to make the USB drive itself the trusted device. RedCannon's KeyPoint Alchemy, for example, encrypts USB devices and implements policy management rules for their use. Similarly, VMware's ACE 2 implements a virtual PC, with security policies, on a USB drive. "The USB drive is a manageable asset," Gartner's Girard said. "It will cost you some money, but you can do it."

The epidemic of laptop thefts has spurred other, more novel approaches. Absolute Software's Computrace LoJack for Laptops works much the same as the LoJack automobile anti-theft device. When a stolen system is connected to the Internet, it sends out a signal that enables it to be traced. The signaling works even if the hard drive is removed and installed in another system.

Page 3: Securing the Laptop: Mission Impossible?

Human beings: a clear and present danger

As long as there are laptops, human factors will remain both a weak spot and a key to defense. After all, most laptop losses can be chalked up to user negligence: An executive left his or her laptop on the podium after a speech; a salesperson inserted a USB drive that contained a keylogger; an accountant's teenage son borrowed the laptop and allowed someone to burn a CD; a help desk worker left a laptop on the exposed seat, rather than in the enclosed trunk, of a car.

So it stands to reason that user education and training is a not-to-be-neglected component of any laptop security program.

A recent study by the Computing Technology Industry Association found that only 42 percent of companies had either completed or planned a mobile computing user security education program. Perhaps that reticence has something to do with the difficulty of implementing an effective program.

"How do you communicate to businesspeople in a manner they can understand and relate to?" said Eric Litt, chief information security officer at General Motors. "That's the skill. It may be more art than science. You have to build credibility."

Litt holds Security Awareness Week sessions at GM, an intensive push to educate the automaker's legions of employees, including tens of thousands of laptop users, on the latest security practices. And retelling the tales of laptop woes is part of the program.

These tales include the one about the millions of U.S. veterans whose personal data was exposed when the laptop of a Veterans Administration employee was stolen. "You talk about the VA and make sure people understand the risk of identity theft when you go to a kiosk that has a keylogger and check a bank account," Litt said.

"It's hard to clamp down," said an IT executive at a global manufacturing company based in the Midwest. "It becomes a political minefield and a nightmare. It's Big Brother, and people don't like that."

The IT executive said that he has managed to persuade his organization to encrypt all laptop hard drives but that USB and CD/DVD encryption is, as yet, too unpopular. Still, users must be educated, he said, noting that with hard drive encryption in place, users' data may be unrecoverable if they fail to perform backups.

Other organizations are cutting back on laptops themselves. Glen Chrzas, vice president of technology at Altura Credit Union, has cut the number of laptops at the financial institution from 50 two years ago to 35 today. Only 20 of those users have their laptops' USB ports enabled, Chrzas said.

Wilson, meanwhile, depends on his company's employees to lock up laptops left in the office overnight, preferably in a file cabinet or desk drawer. On the road, his users are expected to use a Kensington cable to affix their laptops to an immobile object. But will users listen? Will they remember? Will they follow instructions? Many IT pros admit that, inevitably, some will not.

"While everybody recognizes the need for security, how willing are they to walk the walk?" said Paul Tinnirello, a CIO in the financial publishing industry. "How much do they want to be inconvenienced to protect themselves? Most people have no idea how vulnerable they are."

The conclusion is inevitable: Some laptops and the data on them will continue to disappear. With this in mind, many IT pros are looking beyond the era of the laptop to the era of centralized computing based on virtualization technology, when server-based data is parceled out judiciously only to those who need it.

Wilson, for one, said he is looking into what he called "loosely coupled centralized computing," a model in which users access servers to run applications. "The trick is to keep data within the firewall," Wilson said.

Still, he added, "Laptops won't go away. Someone who is on the road will always need a laptop. But the data needs to be stored behind the firewall, with local subsets of just what they need. Make the data easy to get when they do need it, but don't let them download it."

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at eWEEK's Security Watch blog.