
Has Your Information Grown Legs?



Has Your Information Grown Legs?

LAPTOP SECURITY

Did you know that your company's confidential information is climbing over your corporate firewall and escaping from your fancy intrusion detection systems? Every day, gigabytes of information walk right out your front door – on your company's laptops. How expensive would it be if one of these laptops was stolen?

Before you start checking the deductible on your insurance premium, take a second to think about the true value of the laptop: the information stored within. Making it even more valuable, or at least potentially costly, is the passage into law of California Senate Bill 1386 (SB1386). The burden of maintaining information confidentiality has been pushed onto the information holder – you.

Per SB1386: Following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information [being a name and social security, drivers license or account, credit or debit card number] was, or is reasonably believed to have been, acquired by an unauthorized person... shall disclose any breach [potentially including] notification to major statewide media.

While there are no direct civil penalties or fines, the disclosure requirements of the law are severe enough to hurt the viability of even the most reputable institution. And, even though it's a California law, it has national implications because of the media notification clause. With this in mind, how much of a liability might that stolen laptop become? With a little up-front due diligence, these liabilities can be reduced by taking some simple steps to help prevent laptop incidents from occurring.

THREATS

The information on a laptop can be compromised in two ways: physical theft of the laptop itself, or a network intrusion while the laptop is attached to an unprotected external network.

From the security checkpoint at airports to the back of rental cars to the presenter table at a conference, information thieves are walking away with laptops every day. While the motivation of most of these thefts is not for the information stored on the laptop but the hardware itself, there have been incidents where specific individuals' laptops have been targeted for the information stored within.

Connecting a laptop to a remote network is the other easy way to compromise the security of confidential information. Remote networks vary from the wireless access point (WAP) at your local coffee shop, to wired connections in a hotel room and the cable modem in your home office.

Thinking about using that wireless network at Starbucks without a personal firewall or VPN? You might as well just run a patch cable around your corporate firewall directly to your laptop. Both ways, your computers are exposed.

POLICIES AND PROCEDURES

As always, the easiest way to prevent something from happening is to implement policies and procedures to ban activities that might compromise data security, and to thoroughly train your employees to follow said procedures.

A very simple policy and cost-effective procedure is to limit the amount of confidential information on a laptop. This could be enforced by periodically wiping clean the laptop of all user information and requiring the user to log and maintain a minimal set of confidential information on the laptop between trips out of the office. By maintaining a log and keeping minimal data on the laptop, liability is limited should an incident occur.

Rather than storing confidential information directly on the laptop, it should be stored on external storage, allowing the laptop to remain void of any confidential information. External storage solutions include network storage (file servers), online data stores (websites) and locally attached storage devices (discs or USB flash drives). USB flash drives are very convenient, holding large amounts of data on a key-sized device for under \$100.

Laptops using a network to download confidential information should not locally cache data. Locally attached storage devices need to be kept separate from the laptop when not in use, and travel separately from the laptop. This eliminates any exposure should the laptop be stolen, the most likely target of a thief, but users definitely need to be vigilant about keeping the external storage device secure.

A firewall and a VPN should be required when a laptop is attached to any remote network, if the policy even allows laptops to be connected to remote networks. Wireless networks should never be considered secure, as the majority are easily tapped. Hotel and coffee shop wireless networks are typically run in an unencrypted manner allowing anyone to watch network traffic to and from laptops. The encryption in modern wireless devices is dreadfully inadequate and defeated by a number of readily available tools. A personal firewall will prevent malicious users from connecting to the laptop and a VPN will encrypt any data sent from the laptop across the air.

Wired remote networks, such as home office DSL, cable modem and dial-up, carry the same threats as wireless networks, in that malicious users can watch unencrypted data across the network and initiate attacks on an unprotected laptop. Once again, a personal firewall and VPN should be in place if the laptop is even allowed to connect to a remote network in the first place.

DATA SECURITY

As mentioned above, the amount of information stored on a laptop should be kept to a bare minimum. Rather than loading up a laptop with all the user information, just download the information that is required for this trip out the office. On the next trip, clean out the old data and load up the new. If an incident occurs, then the liability is much more limited.

Data encryption and digital rights management (DRM) solutions are coming of age and will soon be encrypting all information across networks and laptops. With a DRM solution, all information is encrypted, and requires the user to enter a password to view files. In addition, a detailed history of requested licenses is maintained, which is crucial in case of laptop theft.

Hopefully, you'll never have to worry about a laptop theft, but with a few of these suggestions the risks can be mitigated. Laptops are becoming a pervasive part of today's mobile society, and some will disappear. However, with a few of these suggestions the liability will be minimal, there won't be any information loss, and your only concern will be which shiny new laptop model you'll have to order.

The Redspin team provides objective security evaluations for various industries including banking and financial services, casinos & gaming, oil & gas production, defense contractors, software developers, firewall providers, automated clearing houses (ACH), automated teller machine (ATM) networks and consumer products. Redspin can be reached at info@redspin.com.