

Discussion with Amanda Smith, the Vice President of Corporate Marketing for Layton Technology

SCJ: *What is the biggest security challenge posed by removable media devices today?*

Smith: In today's every growing technology world, we are faced with an emerging security threat in the form of Removable Media Devices (RMDs). It seem as if it is only recently, that IT administrators are becoming aware how prolific the use of these devices has become. The biggest challenge any IT administrator faces is enforcing domain policies to restrict and govern the usage of these devices.

An IT administrator can easily implement a verbal and/or written policy to restrict users from connecting these devices, as the most typical use of RMDs tends not to be business related. The challenge with this is much like telling a user he or she cannot surf the web on company time. In many cases, though, these policies are rarely enforced and the users are back to surfing the web again shortly thereafter. The same can and will occur for RMDs. It has become a necessity to help the IT administrator lock down, govern and manage the use of these devices.

SCJ: *What seems to be the greatest risks that organizations face in protecting their data and company profiles?*

Smith: Typically, we hear from our customers that IT administrators stress over the fact that their users can connect USB drives or other sorts of RMDs and potentially steal sensitive/confidential company data, or possibly even upload a virus that could take down an entire network. The overall lack of control of what can easily come in and out of the

network is a risk to the organization that is far too critical to simply ignore.

SCJ: *Who would be considered at risk or a target for the threat from within?*

Smith: Any company that values its data to a point they feel it should be treated as confidential is a target from either someone within or even some external breach. Now, would you want someone to share sensitive company data with outside sources? If the answer is no, then any company is at risk of not only being a target, but also subjected to employees who may unknowingly or knowingly compromise the company or network data.

SCJ: *How do you prevent your organization/network from becoming a victim?*

Smith: The first key is assessing the threat. Determine who legitimately needs to use RMDs that connect to your networked PCs and the ones that do not. There are ways to block, restrict and govern the use of RMDs through software packages that allow you to create network policies to be deployed to all of the networked PCs. Policies that will effectively prevent users from using various types of devices such as USB storage devices, iPods, WiFi devices, Blue Tooth, infrared, CD/DVD drives, floppy drives and cameras. Exceptions can be created for specific users to write *.DOC files to a USB storage drive or another group of users to have CD/DVD access, while still enforcing the blockage of other devices.

SCJ: *Why aren't protocol and policies enough to protect your company data?*



Smith: Let's be realistic here – we are dealing with people. People, in some cases, do not or cannot control their actions, or simply ignore company policies that are set fourth to help prevent security breaches.

SCJ: *Do you have any recommendations regarding the protection of networks and viable company information?*

Smith: In order to effectively perform a job, you must have the necessary tools that enable you to complete the task at hand and to efficiently utilize your time. For example, even the simplest task like changing a tire on the car will prove to be quite difficult and time consuming without the proper tools. The correct tools can give you the power to control the outcome. Find a tool that empowers you to control who gets access to what within the network that you are ultimately responsible for. Monitor the usage of this access to be aware of the frequency of how often these RMDs are used, and in what fashion they are being utilized. **SC**