

Tech Talk: Securing your data goes beyond the obvious

By **MJ Shoer**

May 07, 2010 2:00 AM

I have written several columns over the past year focusing on data privacy and security. Over this time, there have been several new regulations that have come into effect that require businesses to take specific steps to secure their customers' data.

With all that has been written, by myself and others, there are still an alarming amount of data breaches. Individual computer users and companies at large continue to do reckless things online that put data and business security at risk. You would think this would not be the case, but it is. A recent report by Consumer Reports notes more than 1.7 million cases of online identify theft over the last year. The report further stated more than 2.4 million individuals submitted information to phishing e-mail messages. Phishing e-mail messages are e-mails that often appear to be coming from legitimate organizations, like your bank, and ask you to reply with specific sensitive information, like your account number or other similar information. The report estimates the cost of cyber crime last year at \$4.5 billion. That is a staggering cost and one that needs to be mitigated.

With the dramatic increase in use of social networking sites like Facebook, Twitter and others, this report and others find that people post far too many details about themselves, facilitating identity theft. Many surveys show people will post complete address information and even things like names of their children, which may potentially expose your children to online advances. The threats are numerous and getting very subtle, so vigilance and common sense needs to be stressed at every opportunity.

A threat often overlooked in the office environment is the office copier, more commonly referred to as the office multi-function device. These are your large copiers that are now much more; the network scanner, copier and fax machine. These devices have changed dramatically over the years. Remember when you got your first office copier how you had to place the document in the feeder and wait for the copier to warm up, then it would pull in the original and kick out the copies one by one. Today, everything is based on the scanning engine in these units. When you place your original document into the device, it will rapidly scan in the document and then print the copies. This has led to dramatic increases in efficiency with these devices, but it also has introduced a security threat very few people recognize. In fact, you may have seen a recent CBS news expose on this topic.

Simply stated, when you use these devices, the documents you are copying and scanning are being stored, albeit theoretically temporarily, on an internal hard drive within the device. After you have received your scanned document or taken your copies back to your desk, data on those documents remains on the internal hard drive. When the time comes to dispose of this device, either by direct disposal or a trade-in back to your vendor, the data goes with it. There are documented cases of multi-function devices being removed from medical offices and returned to the vendor and replaced with a new unit. When the returned unit was inspected and hard drive removed, sensitive medical data was retrieved from the drive and that medical office had just violated Health Insurance Portability and Accountability Act privacy laws. This is a serious matter and one very few business people understand.

These devices are often leased and every few years, the vendor will replace the leased device with a new one. It's very important that part of the process be a secure wipe of the internal hard drive to ensure your business does not expose sensitive data or worse, unknowingly facilitate a data breach by not managing these devices properly.

As you can see, there continue to be many threats to your data security and privacy, some of which are obvious and some are not. It's important to maintain a dynamic information security policy in your organization that adapts with the changing landscape and helps you do everything possible to keep your systems and data safe.

Thanks for reading.

MJ Shoer is president and virtual chief technology officer of Jenaly Technology Group, a Portsmouth-based outsourced IT services firm. He may be reached at mshoer@jenaly.com.

