Information is Money

Part I: Value-izing your information

This is part one of a four-part series that identifies business information assets, helps business owners understand the value of their information and then explains how best to protect information as a valuable business asset.

It's an unusually sunny, winter Monday morning. You have successfully covered the coffee stain on your shirt by buttoning your jacket, so you know it is going to be an alright day. Upon stepping into the office, the front desk staff lets you know he's having some trouble getting into his email and shared files. Nothing the IT administrator can't fix, you reassure him. Five minutes later, you meet up with the IT administrator, who is frantically looking for you. The server has crashed; it's been down since late Friday night; and the back up system hasn't backed up a single document since April! The only thing left of your "good Monday morning" is a slight wisp of smoke that smells faintly of burning wire.

Are your business assets secured? Many business owners believe their assets are safely protected, but they fail to protect one of their most valuable assets: information. Physical assets are protected by insurance policies. How are your information assets protected?

Security needs to be addressed with a comprehensive approach, including organizational, physical and technical aspects. This tactic is true of information security. The trick, though, is to ensure you are spending the proper amount of time and dollars to protect your business from outside intrusions and inside losses. This has become known as Return on Security Investment (ROSI). Much like the age-old ROI methodology, ROSI specifically looks at the validation of security investments.

Just like an insurance policy, several things need to be considered to avoid spending too much on information protection. Most businesses don't understand how to properly value their information. This is a critical step to knowing the true cost and potential return on security investment.

First, how much did it cost to originally capture, generate or develop the information? This may be software, hardware and operating systems acquired to manage, store and modify the information. It may even include a custom-developed solution. In either case, the initial value of information is the tool used to collect, manage and report it. When disaster hits, hardware and software can be replaced but time cannot.

Second, what would be the cost to recreate the information if it were lost or destroyed? Each administrative employee within your company creates documents. Each of these documents requires hours of labor. Each hour of that labor costs your company money. Using a bare minimum example, if an individual is paid $10 per hour to enter and manage the information from each transaction of services or goods – maybe only 20 hours per week – for 52 weeks, this business is looking at a minimal expense of $10,400. Narrowing documentation recreation efforts to the accounting department alone is enough to make a business owner cringe.

Finally, what is the impact of the information in regards to your business? Can your business really function without technology? Sure, pen and paper are still handy resources, but can you run your business solely on those resources? An average, small business in Whatcom

County may generate revenues close to $2-3 million per year. Based on that average, this leads to more than $10,000 per day. If your business experiences interruptions due to information loss for three or four days, your business is looking at more than $40,000 lost in revenue.

Measuring the impact on your business, loss of production and/or sales, and costs of recovery and recreation are all factors that lead to the true value of your information. This sort of appraisal should be performed on each of your information systems because these are all your information assets. Businesses perform this type of evaluation for their physical assets. Why not information assets too? One final point with information appraisals, what would the impact be on your customers if you were not able to support them? Would they vote with their feet?

Chances are most business owners don't want to wait to find out. Good security is based on the development and implementation of best practices. Best practices are defined as proven business processes that help ensure the best return on your investment. After your first step of appraising your information, you will be able to determine how much you may be willing to invest to preserve that asset.

In the next three issues, we will discuss some of those best practices and how businesses should be preserving information assets from an organizational, physical and technical standpoint. As you assess ROSI, remember information value is a combination of several factors: 1) Acquisition cost of collection and management tools, (software, hardware, operating environment and installation expense); 2) Implementation and startup costs including configuration and staff training, as well as the reduced productivity due to initial training curve; 3) Ongoing data collection expense; 4) Cost of recovery or recreation; and 4) Overall customer loss of goodwill.

A business is created with an idea. A business is successful with proper processes and utilization of data. This is proprietary information and the lifeblood of any business. Its protection should require diligence and a well thought out plan like any other business asset because of its value. What is the value of your information? Or, rather, what is the value of your business?