Voice from the Vault

By Gregory Sanford, State Archivist

Poison Ivy, Cabs, and the Need for Planning

Recently I was watching my daughter's boyfriend Eli contort himself into a series of one legged positions reminiscent of the training scenes from *The Karate Kid*. That he was doing so while staring at his new cell phone encouraged me to risk asking a stupid adult question about what, exactly, he was doing. It turned out he was using his phone to take pictures of his foot, which had become infected from an encounter with poison ivy. The infection had reached the point that it was, apparently, worthy of capture and distribution as a digital image. This made perfect sense to my inner teenager.

To my inner archivist, however, this gave pause. As I noted in my January 2006 column I try to keep pace of technological change by observing my teenage daughters and their friends. It was such observations, for example, that gave me my first inkling that CDs would be superceded by iPods. That Eli could be using a "phone" that easily fit into his shirt pocket to create and transmit digital images provided another archival epiphany.

Actually, it inspired several archival epiphanies, all more or less depressing, but for the purposes of this column let me focus on how transportable our digital technology has become. I recently read in the *New York Times* a prediction that desktop computers will soon be replaced by laptops, PDAs/Pocket PCs, mobile phones, and other more portable devices. After all, why tether employees to a workstation when they can easily wander about with vast, and growing, amounts of computing power and memory?

One study I read estimated that mobile computing devices have a standard memory of capacity of 80 megabytes that can store the equivalent of 6,000 Word documents, 720,000 e-mails, 360,000 contact details, or 7,200 pictures. Of course these devices are not always as mobile as the people who use them.

A recent nine nation survey of leading taxi companies found that tens of thousands of these devices are regularly left in cabs. In Chicago alone, taxi drivers reported discovering, in a six month period, 85,619 mobile phones, 21,460 PDAs/Pocket PCs, and 4,425 laptops left behind by passengers (these figures are from a study sponsored by Pointsec Mobile Technologies).

Combining highly mobile technologies with human frailty can be dangerous. In the first six months of this year 93 cases of significant data loss, affecting more than 32 million individuals, have been reported (http://www.idtheftcenter.org/breaches.pdf.). Thirty-five percent of the incidents involved educational institutions, 23% concerned government, 19% general business; 11% health care facilities or companies; and 12% involved banding, credit or financial services entities. The most spectacular incident was of the theft of a laptop from the home of an employee of the U.S. Department of Veterans Affairs that exposed personal information on 26.5 million veterans (the laptop has since been recovered). In Vermont a laptop stolen from an employee's car contained six years' worth of personal and financial information on an estimated 20,000 employees and students of the state college system.

The Vermont legislature responded to growing concerns about identity theft by passing Act 162, An Act Relating to the Protection of Personal Information. But beyond legal responses the growing threats to personal information embedded in our faster, smaller, more mobile computing and telecommunications devices reinforces the need for sustained planning. In this case, what cost/benefit and risk management assessments should be considered before embracing these mobile devices? What security measures need to be in place before your most sensitive data and documents head out the door?

I recently discovered that my continued cautions about planning are about as welcome as poison ivy. I attended a rather depressing, to me, meeting in which several municipal clerks argued that planning was too time consuming and that implementing information technology should be as simple as identifying a software package and vendor and anointing them as the "standard." The clerks had become impatient with the lack of accessible standards and planning tools and simply wanted to move ahead.

While not entirely unsympathetic to that frustration, comprehensive planning is essential prior to implementing information technologies effectively. We have to understand what we do (our functions), how (business practices and workflow), why (legal and administrative mandates, customer needs, etc.) before we can select appropriate technologies.

Planning tools are becoming accessible. As noted in previous columns, the 2006 report of the Secretary of Administration and State Archives provides a general planning framework that supports an enterprise-wide approach to managing records and information (http://vermont-archives.org/publications/legislative/pdf/LegReport06.pdf).

That plan is based, in part, on the management principles of the International Standards Organization found at: http://www.iso.org/iso/en/iso9000-14000/understand/qmp.html. As we test and identify record and information tools we will share them through our web site and elsewhere.

Other planning aids are coming out of the State's chief information office, including tools for planning, cost benefit analysis, etc. These can be found at: http://cio.vermont.gov/planning_and_analysis.

Admittedly these tools are just a start, but they are currently available and are being expanded. Nor do municipalities have to wait for the State to develop a comprehensive toolkit. Perhaps, as a start, municipalities can review their security and laptop policies before any of their mobile devices get on that death cab for data.