WORKING PAPER

No. 07-07 ACC December 2007

"Passing on Your Passwords"

By

Taylor Klett, JD, CPA
Sam Houston State University

Philip W. Morris, Ph.D., CPA, CFE
Sam Houston State University

Ronald J. Daigle, Ph.D., CPA
Sam Houston State University

The Working Papers series is published periodically by the Center for Business and Economic Development at Sam Houston State University, Huntsville, Texas. The series includes papers by members of the faculty of the College of Business Administration reporting on research progress. Copies are distributed to friends of the College of Business Administration. Additional copies may be obtained by contacting the Center for Business and Economic Development.

Passing on Your Passwords

No business is immune to catastrophic events that can cripple or even terminate its operations. When a catastrophic event is mentioned, many tend to think of such natural or commonly occurring events as losses of power, fires, floods, earthquakes, tornadoes and hurricanes. However, another common event that can most definitely harm a business is the unfortunate passing or incapacitation of a key employee. When a business assesses its own risks and designs its business continuity plan, sound succession planning for the unfortunate loss of an employee should also be accounted for. Specifically, a business should answer the following question: How does a business, especially a small business, survive the loss of an employee when he/she is the only one with *access* to certain data, especially when the data resides *outside* of the defined scope of the organization?

We live in a mobile world where data resides both inside and outside of organizations. At any moment, a business may not know the exact or even the approximate location(s) of its data. Even if known, a password may be required for access to the data, such as in an email account or personal computer. An even bigger concern, however, and one that many businesses may not realize until it is too late, is that personal rights over digital property in an employee's possession may actually trump the rights of a business, thereby impeding a business from having access to its own data. These very real vulnerabilities speak directly to two of the top five technology concerns of 2007 identified by financial professionals, as reported in an annual survey by the AICPA [2007]: Information Security Management (ranked #1 for the 5th consecutive year) and Disaster Recovery Planning and Business Continuity Management.

Businesses need to recognize the thorny issues of digital property and privacy rights and take steps to prevent the loss of data. CPA practices should be aware of the very real risks of losing data and take steps to ensure complete and timely legal access. CPAs should also make their clients aware of these risks. In particular, CPAs should consider passing on their own passwords for accessing their key data to a "data heir", as well as being a "data heir" to their own clients. By doing so, CPAs can not only help maintain their own business, but can grow their own practice by helping their clients maintain their own businesses, as well.

Today's Scope of Digital Data Rights

To understand the complexity of the issue of digital data rights, reflect on the relatively recent creation of cyberspace. This "place" has brought with it the possession of property rights by the owner. Consider a URL – no one else but the owner can legally use it. The URL is available for others to access as long as the owner permits. The owner can control the content of the website, regulate who interacts with it through such means as membership, and can sell the URL to another person or entity like any other property. All of these rights are consistent with those possessed by owners of any traditional piece of tangible property.

Now consider an email account. No one else has the right to use your specific account but you. The account is still "there" in cyberspace even if you are not online. The data in the account typically continues to exist until you choose to delete it. The ability to prevent receipt of email by blocking email addresses, as well as the passage of anti-spam laws such as CAN-SPAM, certainly indicates a property right *must* exist with the email account. Other than perhaps a restraining order preventing contact with a

person, no similar right exists between humans in public spaces. These e-mail rights, as well as rights with computer accounts such as social networking Web pages, and online auction-banking, and stock transacting sites, clearly show that the owner can possess certain definable traditional rights within the domain of cyberspace.

Along with property rights, privacy rights are also present in cyberspace. License agreements between Internet service providers (ISPs) and users guarantee contractually that the user has the right of privacy. The contract typically imposes on the ISP the burden of safeguarding the privacy of information contained within the account in their care. The legal issue typically raised over privacy to an email account is unauthorized access, an issue easily addressed through the use of a password. While most everyone takes for granted the concept of password security, little thought is put into succession issues to the data contained within an email account until it is too late.

People and businesses are painfully discovering the complex problems of legal access and ownership of email accounts upon the passing or incapacitation of an individual. Why the inaccessibility? First, the user had not shared their password with others – as dutifully taught! Second, while many families assume that the accounts will become part of the user's estate, some ISPs have fought this notion. ISPs argue that the user' privacy will be invaded, something the ISP contractually agreed to protect. ISPs believe no assurance has been expressly given that the user wants to share their online materials with others, and thus, even in death, privacy should be preserved. Some ISPs are revising their policy to allow access to data by the executor of the estate. But probate can be a lengthy process, and data may be time sensitive, or even worse, data may

become lost due to account inactivity. These issues need to be recognized and steps taken to ensure timely access to data in the event of the untimely passing of an individual.

Having a Plan for Gaining Legal Access

So, what can a business do to minimize these complex issues? An easy, off-the-cuff response would be to have a policy that prohibits the storing of data outside of the formal scope of the organization. However, this suggestion is simply not practical because of the many benefits provided by offline mediums of storage for conducting day-to-day business.

Instead, the key to minimizing these issues begins with promoting both the efficient and effective use of offline storage. This includes stressing to employees that they should not store data in such places as personal email or a PDA when the business has provided a duplicate or similar medium of storage. Also, the timely movement and backup of offline data to the formal information system is imperative. Employees should not just be taught such policies at the time employed; they should be reminded consistently over time about policies, such as through, ironically enough, email reminders. Employees may be easily tempted to use their personal email or permanently store data on their computer if they are working from home but reminders at regular intervals can help instill the proper policy.

Other steps need to be taken beyond these suggestions, especially for small businesses such as CPA practices and sole practitioners who do not have the resources to implement such a formal succession plan. Individuals should consider having a "data heir" in their estate planning. A data heir is one who is legally directed to inherit data

located in specified locations such as email, cellphones, PDAs, personal and home computers and websites.

A key component of the data heir concept is the creation of a "password stash" of all passwords. A simple and straightforward approach would be for the password "database" to be maintained in a spreadsheet document. This file would be protected by a password and that password be given to the data heir. This approach alleviates the need for the individual to notify the data heir each time a password is modified or created. Some may resist this solution because the fundamental rule that we are all so ingrained with – do not share or write down passwords – is broken. However, the risks can be reduced to a manageable level if carefully done. In choosing this solution, individuals need to be most mindful of updating their password list whenever updating or adding new passwords of importance.

Another form of the password stash might work like this: all passwords are printed out or placed on removable storage devices and are stored in a safe deposit box. By placing this information in a safe deposit box, the user has separation from their normal location, and access is protected by a third party using sign-in and a key (and obviously well protected within a bank vault). The data heir would also have access to the safe deposit box. Another measure that should be considered is specifically writing digital assets into wills and/or giving powers of attorney. While this approach may not be as responsive as desired to time critical situations, the inclusion of digital assets in a will or power of attorney certainly cannot hurt.

A more elegant digital solution could be the use of a software "password vault" similar to AnyPassword, PWSafe, and RoboForm. These encrypted files are virtually

impossible to crack. The software keeps up with all passwords as they are updated or added. Only the "master" password is maintained by the owner and could be shared with the data heir. The pervasiveness of technology requires many businesses to take a step back and consider how to protect their data from being lost. For CPAs, a great practice opportunity exists for advising clients on how to reduce the vulnerabilities of losing data, including becoming their client's data heir.

References

American Institute of Certified Public Accountants. *2007 Top 10 Technology Initiatives*, http://infotech.aicpa.org/Resources/Top+Technology+Initiatives/2007+Top+10+Technology+Initiatives/#toptech (2007).