Starbulletin.com

thINC.

A forum for Hawaii's
business community to discuss
current events and issues

Sunday, May 25, 2003

BACK TO TOP

DAVID SWANN / DSWANN@STARBULLETIN.COM

Safeguarding documents is critical

The absence of an original document can dramatically change your estate plan, even if a copy is available

By Judith Sterling and Michelle Tucker

In this electronic age of copy machines, fax machines and scanners we often lose sight of the distinction between an original document and one that has been copied, faxed or scanned. However, at times, especially in estate planning, there is no substitute for an original.

J. Douglas King's family found out just how important an original can be. In 1994, Douglas executed a will leaving everything to his second wife, Laurel, with whom he had two minor children. He also had three adult children from his first marriage, Rebecca, Rachel and Jason. He made provisions for these adult children, but only if Laurel predeceased him.

Between 1994 and 1997, Douglas and Laurel's wealth grew rapidly to $8 million. Douglas decided to rethink his will and consulted an attorney. He brought her a copy of his will. Pursuant to his instructions she prepared an amendment or "codicil" to the will, changing some minor provisions.

The attorney retained the copy of the 1994 will and the original 1997 codicil. In 2000, Douglas died in a motorcycle accident and the original will could not be found. The copy of the will and the original codicil were offered to the probate court.

However, Douglas' children from the prior marriage contested the admission of the copy, alleging that he must have destroyed it, intending to revoke it. If Douglas had intentionally destroyed the original will, the destruction would have revoked it and his assets would have passed under the laws of intestacy, letting the children from the prior marriage share in his wealth.

A bitter fight ensued. The adult children brought up that their father and Laurel had repeated marital problems, including a divorce filing that was later withdrawn. They also testified that the accountant had told them that their father had told him he had provided for all of his children.

To further complicate matters, the accountant was unavailable to testify because he was wanted for embezzling more than $1 million from Douglas' estate.

The New Hampshire Supreme Court, citing a New Hampshire presumption that a

missing will indicates revocation, found it was unclear whether the will was missing because of loss or intentional revocation by destruction. The court considered the will revoked and ordered the estate distributed pursuant to the laws of intestacy. Under those laws, Laurel and each of his children, minor and adult, would share in his estate.

This case illustrates how the absence of an original document can dramatically change your estate plan, even if a copy is available.

A qualified estate planning attorney can help you avoid hidden pitfalls like this that can sabotage your estate plan. Further, such an attorney can help you stay organized by providing you an estate planning portfolio including copies of all your estate planning documents in a simple, organized binder for your reference. Then, you can put the originals away for safekeeping.

Attorneys Judith Sterling and Michelle Tucker are partners in the Honolulu law firm of Sterling & Tucker. Reach them through www.sterlingandtucker.com or www.hawaiielderlaw.com, or by calling 531-5391.

BACK TO TOP

There are many reasons hackers might target you

By John Agsalud

I'm often asked by friends and associates why they should bother to protect their networks from intruders. The usual comment is, "Why would a hacker be interested in my network? No one is going to confuse my company with the Pentagon, General Motors or even Burger King."

Granted, there are plenty of big fish out there, but there are some good reasons why a hacker will come after you:

>> You're an easy mark. Chances are your

Avoiding the hack

There is not much you can do to prevent a skilled, resolute individual from breaching your network, but you can deter the casual hacker.

Installing a firewall, whether it be a hardware-based firewall appliance or a software-based

company doesn't have a multimillion-dollar IS budget. If you're just a small- to medium-size company with one network administrator (who has 24 other responsibilities), you may be vulnerable to a smart, determined hacker.

>> Hackers may want to steal more than the obvious. Stories abound of bad guys breaking into networks and stealing credit card numbers or trade secrets. However, there may be other, more sinister motives for hacking a network, and this entails identity theft. He (and they are nearly always men) may want to use your systems as a relay to probe for weaknesses in other networks. In other words, a hacker could use your machine to scan other people's networks for weaknesses. By hijacking someone else's computer, authorities would be hard-pressed to trace the intrusion to the real culprit.

system, is a first step for any company (and only the first, but that is the subject of another article).

Whether you're a one-man office in Kakaako or a Bishop Street corporation, you'll need good systems to keep the bad guys out. The main thing is to approach security in a proactive manner. Even if no one is out to get you, don't assume you're safe.

Identity theft has other ramifications. As master hacker Kevin Mitnick said in his recent book, "The Art of Deception," if a hacker can learn your name and e-mail address -- which is not particularly hard to do -- he's in a position to impersonate your e-mail, raid your contacts list, impersonate you at chat groups and even send nasty letters or death threats to your boss under your name. The possible litany of mischief is endless.

>> Hackers may just want to get at your computing power. Once free to roam your network, don't assume a hacker is just interested in looking at your private correspondence.

Rather, they may want to leverage your CPU cycles, the raw processing power in your computers, for their own purposes. One company I heard of used a dozen or so PCs and a high-speed connection to win, of all things, an encryption-cracking contest. Although in the scheme of things this is relatively innocuous, criminals may have more malevolent uses for your CPU power (such as the next example).

>> Hackers want your bandwidth. Your CPUs combined with your Internet bandwidth can be leveraged to create havoc with other servers. "Denial of service" or other similar types of attacks require large numbers of computers aiming a fusillade of data at servers and in effect, overloading them.

With a fire hose of data aimed at a system that can only handle a trickle of information, a server may be crippled and eventually crash. Hackers use other computers (unbeknownst to their users) to do the dirty work, turning them into

zombies so that they can't be traced.

>> Hacking isn't personal. Chances are the hacker doesn't know you and stumbles on your network in a random fashion. He probes for a vulnerable network with a "scanner," an application that can be downloaded free off the Internet. This seeks any network with open ports through which someone can enter. If you get hacked, it's not personal. It's as if you left your front door open and a burglar walked right in. Hackers can use computers of innocents (such as you) to create remote-controlled zombies for purposes such as perpetrating denial-of-service attacks. Such an attack occurred in February 2000 when a teenage e-punk used zombies belonging to dozens of small and home-based businesses to cripple Yahoo, eBay and CNN.

>> Hackers will hack just for the hack of it. A hacker-in-training may be interested getting inside your network just because you're there or because he needs the practice.

John Agsalud is president of ISDI, a Honolulu-based IT outsourcing, systems integration and consulting firm. He can be reached at jagsalud@isdi-hi.com or by calling 944-8742.

To participate in the Think Inc. discussion, e-mail your comments to **business@starbulletin.com**; fax them to 529-4750; or mail them to Think Inc., Honolulu Star-Bulletin, 7 Waterfront Plaza, Suite 210, 500 Ala Moana, Honolulu, Hawaii 96813. Anonymous submissions will be discarded.

E-MAIL THIS ARTICLE | PRINTER-FRIENDLY VERSION
E-mail to Business Editor

BACK TO TOP

Text Site Directory:
[News] [Business] [Features] [Sports] [Editorial] [Do It Electric!]
[Classified Ads] [Search] [Subscribe] [Info] [Letter to Editor]
[Feedback]
