

Re: Special considerations with SBS2003 for CPA's, lawyers, medical, e

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-02/msg04107.html>

- *From:* "Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]" <sbradcpa@xxxxxxxxxxx>
 - *Date:* Wed, 22 Feb 2006 07:18:42 -0800
-

(falling over laughing)

Just yesterday a fellow CPA sent me, another CPA a pdf of a tax form with SSN numbers unencrypted. You first need to educate us on secure practices of handling data.

My profession hasn't a clue as far as what is a "best practice".

CPAs are covered by GLB and State law in my State (SB1386/AB1950)

There isn't a web site because no one knows the exact legal definition of "take reasonable precautions to secure the personal identity information"

Extreme best practices for any industry that has on their server PII (personal identity info) would be to

1. Encrypt backup tapes (SBS won't do this natively, Ultrabac does and has a SBS module)
2. Secure sending of email. In a small firm, usually cheaper to buy individual certs than try to deploy a PKI infrastructure. This is soooooo much an end user education thing it's not funny. I personally do not use Outlook over the Internet on traveling laptops to also better protect the data by leaving it on the server.
3. Password requirements. There are no legal requirements of length, type, two factor, etc..... Have a good strong pass phrase.

For Doctors, you need to get into Hipaa and ensure that again you have logging that identifies the ePHI and the logging of entry and exit of that.

You'd have to consult with an attorney, but in my mind, unless your client informs you of their legal requirements, or you hold yourself out to be a consultant that makes someone Hipaa compliant, the legal liability is on the back of that client. Dana Epp will be doing a presentation on Compliance issues for the MS Small Business Summit

<http://www.sbsummit.com/FAQ.aspx> (for some reason the main page isn't working right now)

Given that SBS is international, and Microsoft would be taking liability to try to list out all the professions and their requirements, I doubt you'll ever see a page like this.

Good practice is how do you want YOUR personal information handled. Ever single tax program out there does not encrypt SSNs inside the database.

dsatchell wrote:

I'm wondering if there are any special settings or set-up procedures for specific client types such as CPA's, lawyers, doctors, etc., and what is involved with regard to SBS2003.

Three things that come to mind are: 1. secure/encrypted backups
2. secure sending of email (not OWA)
3. password requirements.

What I would really like to see is either a web site or a document with each profession listed and a list of what is considered good practice in that industry and what is required by that industry.

Out of curiosity, is there any point as a consultant or employee that we can be held legally liable for not following through on due dilligence(sp?) on meeting legal requirements?

Thanx, David.