Thresher Networks SM

www.ThresherNetworks.com Thresher Networks LLC
manager@ThresherNetworks.com Duane Thresher PhD
Mail: 250 4th Ln NE, Fairfield MT 59436 (406) 467-2790

IT Hall of Shame

DPHHS Coverup

Re: The coverup of the DPHHS Breach, where the sensitive information, including medical records, of tens of thousands of children was lost through negligence to hackers, possibly predators and thus endangering the children, by the Montana Department of Public Health and Human Services; responsible officials included Ron Baldwin, Montana Chief Information Officer, and Richard Opper, Director of DPHHS.

BS By Any Other Name Would Stink As Much!

Keep in mind that Richard Opper, Director of DPHHS, seems to consider himself primarily a writer (warning: his works are for adults only).

As repeated, variously carefully reworded, in the DPHHS-hacked letter to the parents of the child victims, whom DPHHS obviously believes are stupid, and in press releases, gullibly reprinted by the media:

"at this time, we have no knowledge that any information on the server was used inappropriately, or was even accessed"

"we have no reason to believe that any information contained on the server has been used improperly or even accessed"

My wife and I used to be scientists and one of the first rules scientists learn is "absence of evidence is not evidence of absence", especially when one is motivated NOT to find evidence or is incompetent to do so, both as in this case.

An example: If Richard Opper, Director of Montana DPHHS, Ron Baldwin, Montana Chief Information Officer, and Steve Bullock, Montana Governor, have children or grandchildren under 18, they could get their kids' "demographic information" (name, address, date of birth, Social Security number, phone number, school, etc.) and medical records (particularly the embarassing blackmailable stuff) and release it somehow, unknown to them or me, into the Internet. I could give them 100% assurance that I have no knowledge any of this information was used inappropriately, or even accessed.

How would DPHHS even know if the information was "used inappropriately"?

And what is "inappropriately"? More honestly (i.e., not so carefully worded) it should have been phrased "used criminally" and judging from the trivial protection DPHHS offered the child victims -- a single year of credit checking (which they could do for free themselves) -- they were just talking about identity theft. What about protection of the children from abduction, made much easier by their hacked information? DPHHS does not even hint at this far greater danger.

Don't have kids and think abduction unlikely? In my IT work in Montana I discovered a registered sex offender, a pedophile, providing computers to libraries and possibly schools (library and school computer systems, which are usually insecure, have become prime targets for pedophiles). Further, over the years there have been numerous campaigns to teach children to be safe online to prevent just this danger from predators.

Just around here, since the DPHHS breach there has been a police call where the female caller said "her daughter was outside of their residence playing and a red car pulled up, [the car occupant] took out her cell

phone and took a picture of her [daughter]. She [the caller] described the occupant of the car as a lady with short black hair and black glasses." Is the FBI comparing such reports -- or at the very least children who were actually or almost abducted -- against the list of DPHHS's child victims?

According to Montana's Department of Administration's Risk Management and Tort Defense's cyber information security FAQs:

"The term 'breach' may be easily misconstrued and implies that the state was negligent; therefore, a cyber/information security situation should be referred to as an 'incident' and reported to the Risk Management and Tort Defense Division (RMTD) [...] RMTD will work with the state's insurance carriers [Lloyd's of London syndicate 'Beazley'] to determine whether or not a 'breach' has occurred."

In more honest words, "don't call it a breach, DPHHS needs the insurance money". Just try renaming your negligence in order to get the insurance money and you will be charged with insurance fraud.

This "don't call it a breach" also explains why in the annual reports that Montana Chief Information Officer Ron Baldwin has to file the number of "breaches" is ALWAYS given as an impressive "0" while the number in the other, less-serious category, "incidents", is always in the hundreds.

In the end, all DPHHS has to say about its breach that endangered children, down on its home page, right above its HealthCare.gov Marketplace options, is "DPHHS Server inappropriately accessed". This sounds more like a scolding of an elementary school computer lab; certainly not something you'd pay attention to. That's as watered down as you can get without not mentioning the DPHHS breach at all.

DPHHS never caught the hacker and probably never even tried (and yes, it's possible to catch them) but it doesn't matter now because in their attempt to water down and cover up what really happened, DPHHS made what the hacker did not a crime. If caught the hacker would just say, "if DPHHS doesn't consider it a crime then why should the judge".

(By the way, around here if you "inappropriately access" someone's home you will be "appropriately axed".)

Hide The Hack Date! (It Was 10 Months Before Discovery!)

The only dates concerning DPHHS being hacked mentioned in the DPHHS-hacked letter to the parents of the child victims are:

"On May 22, 2014, an independent forensics investigation determined that an agency computer had been hacked. The forensics investigation was ordered on May 15, 2014 when suspicious activity was first detected by DPHHS officials. As soon as the suspicious activitiy was discovered, agency officials shut down the server and contacted law enforcement."

This gives the completely false impression that DPHHS was hacked in May 2014, when actually that was only when DPHHS finally discovered it. This was the same never-corrected false impression given by DPHHS to the media, including Reuters:

"Hackers of unknown origin gained access in May [2014] to a computer server tied to the Montana Department of Public Health and Human Services, exposing sensitive or confidential information of current and former medical patients, health agency employees and contractors."

Much media has become merely lazy gullible press release reprinters but you might expect that if Reuters said this they were very actively misled by DPHHS.

According to just one of DPHHS's only two news releases (in May and June 2014) about being hacked, and not in the notification letter, "the server was likely first accessed in July 2013", 10 months before being discovered! Even that long period may be an underestimate since the competence of the suspiciously-unnamed people doing the "independent forensics investigation" is not known. If it took that long to discover, it was almost certainly just accidentally discovered and means DPHHS was not doing at-least daily computer security checks (e.g., checking logs), which is incredibly incompetent (if they did not know to do this or how to) or negligent (if they knew but didn't).

Among other significant IT qualifications, I (Duane Thresher) have a BS in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (MIT), a PhD in a supercomputing field from Columbia University and NASA, and I have worked at a Department of Defense supercomputing facility.

MT Chief Information Officer Ron Baldwin's Exaggerated Resume

According to Ron Baldwin's Background on his official MT CIO page, "Baldwin has degrees in Computer Science and Biology/Chemistry".

You would expect that the relevant degree for a CIO, Computer Science, was at least a Bachelor's. Even elementary schools in Montana, and most of the US, require their teachers to have at least Bachelor's degrees. However, according to a Missoulian newspaper article this degree is only an associate's from a community college in 1982, more than 10 years before the 'Internet' and around the time of the first PCs. Further, community colleges, as well as for-profit educational institutions, are the leading culprits in producing unqualified IT workers.

The newspaper article also says that Ron Baldwin got a Bachelor's degree in 1979, in Biology/Chemistry. But also from Ron Baldwin's Background, "Baldwin is an adjunct professor at Carroll College in Helena where he teaches project management". At reputable colleges, professors are required to have at least Master's degrees, if not Doctorates, and usually relevant to what they are teaching. At the very least credits taught by those with less are non-transferable (do Baldwin's students know this?).

I (Duane Thresher) have a Doctorate (PhD) in a supercomputing field from Columbia University and NASA, as well as a Master's (MS) in that field from the University of Arizona, and a Bachelor's (BS) in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (MIT).

Updated 30 Mar 2015.

To Be Continued ...