

The Nature of Data – Volume 1

abstract

Oh boy! We're messing up our thinking on the subject of Data! No, not the character on StarTrek but the real world of 'big data', the world where your bank account lives, the title to your property is, your credit rating is evaluated, your health records are stored, your spending habits are evaluated - and the world in which most Governments, Financial Institutions, Medical, Commerce and Business see the real "you". And yet, over the last year, we have been deluged by reports of hiccups, lost data, serious downtime... it's seemingly epidemic. Not to mention, identity theft is now the highest profile white-collar crime that we all live in fear of. It's time to take the subject of "data" very seriously.

The nature of data, data storage and data processing has changed dramatically - unfortunately our attitudes at a personal level have not.

This discussion paper is the beginning of a series intended to explore the meaning of 'data' and our ability to keep it safe – in the hope of creating dialog and some saner approaches to the safekeeping of 'real data'. This, the first in the series, looks at what we are doing with data and hypothesizes where we are going with it.

background

The worldview of you... is now almost completely digital. Don't you think it only right that we "systems people" put a little more thought into its protection, its integrity, and its privacy – heck, what on earth is going on?

Below are a few, by no means all, Internet links in regards to the lost processing or horrific loss of data that has been widely reported in the last year or so. It is the cascade of these "hiccups" that has sparked this paper. My apologies in advance to the London Stock Exchange, the Royal Bank of Canada and Her Majesty's British Government, all very fine establishments, all visibly embarrassed by these happenings. By no means should these institutions be considered to be the only ones – just a selection of the ones I picked as the example, the ones with very visible processing and with the integrity to have the incidents reported and subsequently openly investigated. I am 100% positive that there are others that are not generally known or not as widely reported. Links as follows: -

The world of lost processing ability...

<http://www.linke.de/2008/09/10/london-stock-exchange-crippled-by-system-outage/>

<http://www.thestar.com/article/521158>

<http://hardware.slashdot.org/article.pl?sid=07/04/20/1446220>

<http://thebankwatch.com/2004/06/04/royal-bank-of-canada-computer-glitch-causes-payments-chaos/>

<http://www.computerworld.com.au/index.php/id;911308040;fp;16;fpid;0>

The horrifying world of lost data...

http://news.bbc.co.uk/2/hi/uk_news/7663941.stm

There was one more incident that I couldn't find – the fact that a local high-technology worker in Ottawa, Canada, a software developer working for a telecommunications company had, for a number of days, been emailing 'wedges' of

computer code out to his relatives in China. Fortunately some internal email protection systems had picked this up at the time and the employee was severely disciplined for an act that he clearly saw no problem in doing.

Why are we in this mess? How come we've lost control? Companies routinely spend a fortune protecting data and, despite that, we continue to lose it, to dispense it, to publish it and to abuse it. What is it about the way we build and maintain automated systems and digital data that has gone so awry? This series of papers begins to explore some of the issues and, although may not be able to make suggestions, will hopefully kick-start some additional thinking and dialog.... We have to get better from here!...

it all starts here... digitizing data, the bottom line

IF YOU DIGITIZE DATA – EVEN A CHILD IS CAPABLE OF STEALING IT!

We now live in a world where, at the touch of a button, real data can morph into digital information and be stored on your desktop or a mainframe or, in fact, on your MP3 player or cell phone. That's fine for the frivolous world of music, movies and so on (copyright issues aside) – a little more disturbing when it becomes your banking information – but totally catastrophic if it's biometric information such as your fingerprints!!!

In everyday life, we live under what our old-fashioned systems people refer to as 'the Chinese seal' model. He who has the seal; has absolute authority... over everything! Think about that for a second. You want money, you sign for it. You want to put something on your credit card, you sign for it. Should you really be quite so willing to digitally sign for something?

Next time you are signing for a FedEx receipt or a parcel from your Post Office and the person behind the counter asks you for a signature – remember that, once you've signed, they now have a perpetual digital copy of your signature. This signature is going to live on into perpetuity – you just assume the collecting organization is honest enough not to use it multiple times. In fact, I suspect you assume that it will never be kept on file... but it has to be! The person checking for where their tracked parcel is located can usually see who signed for it and what their signature looks like.

IF YOU DIGITIZE DATA PERTAINING TO A SINGLE PERSON WHO CAN BE UNIQUELY IDENTIFIED – THEN YOU HAD BETTER BE PREPARED TO PROTECT IT!

Next time you swipe your thumb over the fingerprint reader on your laptop – remember the same thing. Not only are you willingly committing your definitive source biometric identity to your disk – it can now readily be accessed and taken to re-use anywhere. You have potentially empowered another person with intensely private and definitive information. You are now fully able to be a replicate; you just don't know who, at the other end, is going to use it.

Don't give your data away. Be skeptical, ask for the policy and ask why and where they plan to use it – because, in the wrong hands, it can be used as a definitive source for you. And heck, you can't even repudiate it! IT IS YOU...

The only source of my fingerprints – should be on the ends of my fingers. Storing this level of highly intrusive definitive information is not only making it replicative, it can be used against you (the precept being that you gave it willingly) – and even a child can steal it.

IF YOU HAVE YOUR PERSONAL DATA DIGITIZED – THEN YOU HAD BETTER TRULY TRUST THE PEOPLE LOOKING AFTER IT!

Digital data is invariably a copy. Regardless of it being music, a movie, a file record, your Facebook profile, your healthcare records, your bank account statement – its merely a copy. At least, it used to be – now, I'm less sure and that's the rub. How come no one seems to know that? And even if they do know that – how do I authenticate myself? Is it important... more important for some things and not others?

Next time you give away your data... ask about the trust issues and weigh if this is really a trustworthy body? Oh, and trustworthiness is NOT proportional to the amount of money that organization spends to protect your data – we're way beyond that now.

In conclusion:

1. In our clamber to collect everything meaningful in digital form, we may have forgotten just how sensitive the vast majority of that digitized data can be. And once digitized – how fragile and meaningless we have made it.
2. It costs a fortune – to secure data! Few can afford it - and, despite the money they spend, it is extremely difficult to stay ahead of the “leakage” and “loss” threat.
3. It is vital that we absolutely trust those that store and protect our data... who is trustworthy to this degree?

For more information on data breaches and losses, and to see how widespread this problem really is, I strongly suggest you sign up at www.datalossdb.org.

As I write this – the following happened in London!



UK police chief quits over blunder

Britain's counter-terrorism chief officer quits after accidentally revealing details of a secret operation aimed at thwarting a possible al-Qaeda plot.

news.bbc.co.uk, april 2009



insight

Produced by: Sue Hardman, Principal, Blue Rabbit Consulting Inc.

Blue Rabbit is a consulting company in Ottawa, Canada dedicated to creating winning strategies for technology-based companies.
Telephone: (613) 692-3868 or shardman@bluerabbit.ca