NUMOQUEST®

Making the Impossible Possible

Visibility of Talent starts here!

™©®1996 – 2016

Predictability of IT/ICT

100%

Why the often so stagering fails and losses?!?

Introduction

NumoQuest® white papers and presentation covers the grey

areas between IT and Non – IT. Vision and presentation are based upon common and best practices in a 'ready to implement' fashion. The term 'Generic' may be read as 'Dynamic' by some. Please bear in mind that the linear principles of Strategic IT are the bases and outlines for IT white papers. Accompanied the IT laws of physics of matter IT are guiding principles.

It is not **NumoQuest®'s** objective or emphases for debate nor

search for opinion. Objective here is to provide the bases from previous experiences of how IT as matter is working and moves, to reach the highest possible in Strategic IT, _**a flawless IT**_. There is no room for debate, politics or act of commerce in IT white papers since matter IT is none of them all.

RenéC 2016

Essence

The founder of today's IT/ITC basically was French man Basile Bouchon who had a series of inventions in 1725 where Joseph Marie Jacquard later continued to build the weaving machine upon. In essence that is to be regarded as the basis for what we now know as IT and ICT or rather, automation and digitizing.

The Universal Principles however, where upon IT ICT is based, is only known by so few. Certainly not the vast majority of IT professionals and surely not to the professionals working in or with IT. Please also bear in mind a very crucial fact, IT professionals and professionals working in IT, for sure aren't informing the mass working and using IT of two major and utter important facts.

1. What IT, automation is
2. How to treat and thus use IT essentially

If one is to look at these two facts perhaps one is as amazed as we are. Stating this is based upon the simple fact that on the moment you, dear reader, and we, would be fully informed how to deal wit IT on a daily and user based, IT professionals lives would be inevitably less complicated towards us and sure we diminish all kinds of frustrations.

IT 100% predictable matter

IT in its essence is 100% predictable. That is that every step in and with IT, ICT, on every echelon, within every discipline, is 100% predictable. It is most simple in principle. A is the current moment, B is the desired moment. In order to get flawless from A to B, in process, project, in step, objectives, criteria and every single element in this instance, is to be specified. If that isn't done, one is simply assured that any set objective, process or step, somewhere, somehow will be hindered or simply come to a halt.

Specified

It also means in simple terms that every item, every step, every instance, calculation, for 100% is to be specified. For IT is a 100% programmed matter that only will act within the programed bandwidth No more, no less.

Disregard every professional that like to state one this otherwise. For it isn't commercially in the interest of IT professionals or commercial oriented professionals working in IT to tell you this. If they would suddenly the world of IT, and the way to treat and look at IT, for Non IT professionals, would all of a sudden make sense.

In other words, refuse to accept that IT professionals and professionals working in IT persist to let IT ICT be a black box towards the rest of the world. So when a IT professional or a professional working in IT states that 'IT' is to complicated to explain, it simply a: is not true or b: the professional don't want you to know or themselves can't explain reasonably.

Assassinators

There are a number of assassinators in the world of IT. We for this document name three;

- *Ignorence*
- *Commerce*
- *Cyber Crime*

Ignorence

There are simple do's and don'ts in and with IT that most professionals and others, using IT, simply aren't aware of. Professionally it still is stunning that organizations still haven't received an actual simple book of reference, a cookbook, a user guide, how to see IT, how to use IT within the organization. The costs for such simplicity may easily be estimated in billions of damages and losses in terms of time and production, hence profit.

Commerce

Commerce, smaller or large, professionally have one single objective. **Sale!** No matter which way, NLP, trick, type of persuasion, anything for closing the deal. Lethal, 100% predictable many bills as a costly result for the organization as costumer. In the race for customers and sales very important aspects, due to diversity and ego in and with IT, anything goes with as 100% predictable consequence Many undesired bills to pay.

Here one as customer simply should ask oneself, if strategic corporate IT is there for the benefit of the organization, to reduce costs, then why still the so many bills to pay?

Cyber Crime

Not really new yet often published. **Cybercrime**. Cyber Crime is a stronger growing virus <u>no longer extinguishable</u>. Let this be put here, plain simple. Commerce and Government are the first to jump up to tell you otherwise, simple fact is that **the battle against cyber crime simply can't be won**.

If the Sh#t hit's the fan, one simply is to late

This is a simple universal rule. This also is working in the two worlds of IT and Non IT. Thus also for **Cyber Crime**. If a burglar breaks into a home, in 99.9% of the instances there will be clear evidence that 'someone' illegally has paid the house a visit. In the digital world it is quite something different. Because of the complexity of the matter, processes, IT peripherals like hard and software, spotting the burglar isn't that easy anymore to state in the least. The burglar has an astonishing array of weapons of choice to hide itself.

Added here; a simple user isn't expected to be that skilled to detect such of course.

In the world of IT one only can act when an intrusion has taken place, which of course is detected or, IT specialists find a loophole or omission in programme or machine and warn the producer, who only then can act. As long as the intrusion or omission remains undetected, the burglar can basically do what it pleases. In both instances one is too late to have counter measure instated since you simply can't take any step against ….. what…?. The only thing one basically can do is to try to think like the criminal in terms of, 'What would she/he do….?' And then take measures. Even so, it never will be enough.

Stating that the war against Cyber Crime is lost is only sound mind and healthy sanity to accept as fact. Rest assure there will be many jumping up to state otherwise. We here gladly refer back to our three assassinators earlier.

No Limits

Cyber Criminals have no limits. They become increasingly smarter, have more and more free resources, connections and time and there are many more of these than on the 'good side' If you, dear reader, only now want to contemplate about the fact what commerce is building for Walhalla for Cyber Criminals, one is to be truly warned and hopefully eyes opened. For the chance that your computer, laptop, tablet or android will be hacked, violated, broken in to simply is a matter of 'WHEN!', not IF!   It is a guarantee.

Divide and Conquer

This universal principle also simply applies here in the world of IT and Non IT alike. For sake of the Big Bucks, the last five years alone commerce is hyping and shouting all kind of new ways, new schemes, new products and using such techniques that they make you believe that all that is what you WANT, what you NEED, what you're about to CRAVE for.

What they don't tell you is that your life, your privacy, your independence and your security is at stake here. By the massive invasion of commerce and government at and in IT to your daily lives' even a greater danger than they want you to believe.

If one have an open eye for it.
Commerce nonstop is bombarding you with all kind of products, services, apps an what not, trying you simply to persuade to Buy Buy Buy! Governments increasingly abusing IT for sake of the danger of crime and terrorism to invade your privacy and bit by bit are more and more abusing IT to control.

They turn the table telling you that your private cams, connected to the internet should play a key role in counterattacking crime or terror so you may join the scheme with the government that they, REAL TIME, may use your cam. They didn't explain to you that they already have the means and technique to operate every cam you have in your laptop, mobile phone or anyone connected to the internet.

Something to think about…

If you, dear reader, think that is all, then we like to give you some additional food for thought that are financial drains of commerce, if you will. Just that because you as professional, or organization, aren't to aware of how automation in basis is to work, not how commerce or government is exclaiming.

Cloud

Cloud is something upcoming in all kinds of publications hyped by commerce. Fact here is that the illustration of a cloud, internationally simply means 'Internet'. 50% of the cloud story is simply commercial while the benefits hyped, by far questionable.

All your (corporate) data is to be put in the cloud so it can be accessible globally, 24/7. What not is revealed is the fact that you will be depending on millions of IT peripherals, between you and your data, that there is absolutely no guarantee that your data is a: Safe B: 24/7 globally accessible. Simple fact here is that just one minor yet strategic IT part in the chain has to break down and your data simply can't be accessed.

Technically: having your data back home or in the office is equally as accessible as in cloud. Yet you are in control and can take measures on your own terms, to stay in control. And that of course isn't that commercial yet, you make use of equipment you already have. Did we mention globally there are also legal issues as well in terms of who is proprietor of that data and intellectual ownership in countries where your data is stored?

Apps

All are by now familiar with all kinds of hyped apps and how convenient apps can be. Generation after generation grows up with developing IT. These generations also are growing up with lesser awareness of security and the fact that your personal data, personality, staying security wise updated, makes you ever so more vulnerable for intrusion and breaking in.

More and more intrusions take place with all kinds of perils like identity theft, fraud and rest assure, by far the security of apps and mobile phones are not baring highest concern of commerce. Increasingly, however, the interest of criminals is obvious.

Internet of Things (IOT)

IoT has all to do with consumer goods connected to the internet. Cars connected to the internet for safety reasoning where the car send data, without your consent or interference nor owners control to parties where the data owner has no say nor insight of. The refrigerator, almost empty, now can talk through the internet to warn that it is running low on food and beverage. One step further here, it already IT wise is possible for your refrigerator to talk to groceries delivery and order for you. Isn't that convenience?

The smart multi metre placed by the energy supplier to enable not sole wireless and distant control over certain' convenient' aspects of the house like preheating before arriving home or switching on/off lights and other equipment.

Commercially pretty advanced and for sake of consumer convenience. The Downside is that security of equipment often is so poor and appalling crime has found already many loopholes in these to assess whether the house is occupied or not for criminal visit.

Big Data
More and more 'Big Data' is promoted to be some sort of commercial God who will bring you the world of consumer's data all for the benefit of the profit of your organization. The down sites? Approximate 45%-50% of the Big Data is flawed, contaminated, questionable and there are no means in place to ascertain which facts or parts of the +45% of all data is flawed.

Corporate Big Data
Although corporate Big Data is more reliable and controllable, it is commercially viable to prepare and present such data in such positive and profitable manner that even these sometimes is more than questionable usable by third parties.

The more the merrier…..
The exploding diversity and increase of use of the internet draws a landscape of opportunities, also crime wise, and it already is clear that the numbers of technical incidents and crime wise doubling since 2008 annually. The lack of registration of IT incidents or intrusions, real time reliable statistics often are hard to come by.

Diminish of IT staff and professionals
Commercially driven, the hunt for saving spending has reached levels that contribute to the increase of bigger IT incidents with higher impact. Commercially damage always directly inflict sales price where in the end the consumer is paying for lack, impotent and incompetence of commerce and government. By replacing experienced IT staff by the non or low cost student, intern, 'Young Upcoming Talent' has as result that security processes and IT chain experience rapid has declined since 2008.

And just that has had a staggering billions € consequence at the expense of consumers at the one hand, the taxpayer on the other. A consequence that with the same 100% predictability could have been avoided. There are many ways to reduce peril, incidents, cost of loss, and damage name and reputation before it emerge. Here also the **100% certainty** is a **_Guarantee_**. It all starts with the simple awareness how damaging commerce and ignorance show to be in favour of Cyber Crime.

Good luck in any endeavour you're pursuing…

Rene C 2016