IT Crisis Management

The most basic and elementary principals of IT Crisis management for any organization

For use of IT and Non IT manager in order to reduce reputation and collateral damages.

Author: *René Civile*®
NumoQuest®

1996, 2001, 2012, 2013
Version 1.1
March 2013

IT Crisis Management©

In 1998 **René Civile ®** draw the first outlines and blueprint of IT Crisis Management when acting as Special IT Issue and Case & Project Manager for Royal Shell. He discovered that there is a solid and standard way to improve IT chains and disciplines with simple steps and minimum effort and details, creating a very powerful blueprint for IT Crisis Management.

First there is to be acknowledged the fundamental differences between two worlds. It is the fundamental difference that increase the certainty of damages, especially in IT incidents and problems viral out into an IT crisis. By rewriting this document and actualizing it with recent real time occurrences where IT is involved, this document is intended to be the bases for standardizing processes, and procedures, setting role and responsibilities, to prevent and/or limit structural and incidental damages caused by an IT crisis.

Through the years and development of IT, in all it's variety and disciplines, libraries have been filled with books about processes, procedures and of course successes. Strangely enough not a single book of guidelines was written where IT Crisis Management was aligned in the way IT as matter behaves and how IT and Non IT professionals are treating it.

In second, regretfully there aren't to many consultants being able to bridge the ever existing gap between the worlds of IT and Non IT boards and management. Though many professionals are very good in their professional discipline, many professionals allied in IT in other disciplines, only have very limited knowledge and understanding of IT as matter and it's behavior.

Then there is a great world of professionals and non professionals, not having any idea how IT as matter works and behaves and how it should be treated. By not understanding, also caused by a huge differentiation in and with IT, the large scales incident more and more can grow to IT crisis like situation where customers, clients, IT and Non IT professionals and management play crucial roles.

Over 75% of IT crisis situations can be prevented. Easily. Only if IT and Non IT management are willing to start to look at IT the same way. René understands how and why this often doesn't happen. He want to correct this with this document.

René Civile® has a over twenty-five year career from IT operations to IT Portfolio, Change and Project management. He has a straight forward helicopter view on IT chain processes and procedures, pinpointing flaws and being able to offer instant solutions. He has written many comprehensive white papers with IT as Big Thread to bridge the gap between IT and Non IT management. He frequently is consulted to do just that what IT, as vehicle is intended to do. Realizing great savings through automation. The increasing large scale IT crisis incidents in the years 2009 – 2013 has encouraged him to write this document.

Don N. Eastep
IBM

In great memory of Donald N. Eastep. * 19.12.1938 – 27.10.2012

IT Crisis Management©

IT Crisis Management©

1. What is an IT crisis

A crisis is an event or occurrence where many people share a mutual experience with high personal, professional or political impact. In the ordinary every days world we might think as a great flood, earthquake, an airplane crash and so on.

Then there is another world where a major event can cause grave disruption but, not necessary with a personal impact. That is an event in the world of IT. Not necessary in this world is limited. Since IT is almost everywhere, a civil power interrupt indeed may cause harm in secondary circumstances. In a complete power interruption, the chance on an accident is much higher or if some one is relaying medically on a power source, it might have a serious consequence as well.

In IT there often is debate of what one would call 'Crisis'. In the world of IT, a crisis best is described as;

"A major occurrence with a high professional impact where IT or communications peripherals are involved."

Setting this as **your** standard will be your greatest advantage as from here. Regardless how complicated some parties like to present and debate this standard, remember, they have a strong commercial or personal drive. And that drive isn't always IT driven by far.

2. How a crises starts and behaves

Here immediate we come to a number of interesting conclusions. In next, two quite recent IT occurrences with a very high impact are demonstrated. Here one will learn that there is a great number of differences in two worlds.

Diginotar, a Vasco Data Security Company's daughter, an IT certificate authority and exclusive supplier of security certificates to the Dutch Government. In June 2011, someone called himself 'the comodo hacker', tapt into the Diginotar systems leaving exploits, making the systems vulnerable for intrusions. As a result of this action, the systems issued certificates to unnamed persons in Iran. It has been said that these were used to hack Gmail accounts.

At the end of Juli 2011 Diginotar discovered what happened but didn't notified its customers. It was after a blog mentioning the hack and its severe consequence on August 27 2011, that Diginotar was forced to admit what happened, where after the Dutch Government ordered an investigation and for that time closed all on line public services of Governmental servers, to the Dutch public.

Finally, on September 2, 2011, Dutch Government decided to abandon Diginotar as supplier of safety certificates.. Mr Piet Hein Donner declared in an emergency broadcast earlier, what measures he had taken as Minister of Internal Affairs. In an interview several weeks before that broadcast a weekly magazine interviewed him. In that interview Mr. Donner stated, "I'm not to fond about all those modern novelties like PC tablets and such. I'd rather have the old school pencil and paper…..(?!?)" On September 20, 2011 Diginotar was declared bankrupt. For weeks the use of on line governmental services and specific duties were interrupted.

Conclusions:

- **Standard IT Processes and controls Diginotar**

It is evident that the basic IT process in Diginotar weren't professionally up to a minimum standard. If it had been, there wouldn't be a flaw in the Diginotar systems. Hacking the systems much more difficult, detectable and traceble.

- **Standard IT Processes and controls Dutch Government**

It is evident that the basic IT processes by Dutch Government weren't up to a minimum standard. Before any implementation in IT, a standard investigation is mandatory. Any possible problem for 99% should have been avoided by a standard ITIL process.

- **Communication**

It is quite harsh to see someone like Mr. Piet Hein Donner taking control, clearly without affinity nor professional interest in the matter, but sole flag his personal stature. The matter and weight of the information is by far counterproductive. Here focus and aim of the audience and public has been one of disbelieve and wide spread criticism.

- **Secondary damage**

The online systems by the Dutch Government, are the sole sources for public – governmental services. Disrupted services like Tax admissions, Passport request, Financial and civil tasks, single sided implemented by the government, were disrupted for weeks.

- **Awareness and means to inform the public**

Because of the fact that civil services were disrupted, means of clear communication informing the people, were restricted to news paper, radio and television. The government hasn't any other fallbacks to use since that the problem were the credibility of those on line services.

- **Damaging name and credibility of messenger and government**

Diginotar a few weeks after 'coming out' was declared bankrupt. More damage couldn't be set to them anymore. Mr. Donner, in name and person suffered greater damage as being a person without experience, affinity and knowledge about the matter, demonstrating no expertise in the matter and managing the whole situation. The government suffering more discredit from the public for not being able to implement IT standards.

- **Roles of the media**

Odd enough the press weren't to critical towards Mr. Donner. Reason seemed simple. To be more critical is closing the door to political information. The social media, blogs and forums exploded with angry reactions towards Mr. Donner and the government. All delay and costs finally were to be paid by the taxpayer.

At production of this document the government is increasing effort to digitize services there for increasing chance of impact in future if a major interrupt occurs again.

Beginning of April 2012. At a neighboring company of a strategic Vodafone phone relay center, a fire started. The fire spread rapidly into a blaze, setting fire to the relay center. Vodafone and neighbor lacked sprinklers. The neighbor didn't had a working alarm system. On the moment that the alarm automatically was raised by the Vodafone systems and the time the fire brigade needed to arrive, major calamity became fact.

The fire was that severe that entering the premises became impossible. In the hours during and after the fire, more and more connected antennas went down. It became clear later next morning that over three million Vodafone customers couldn't call or send text messages for days. It became impair that the relay center wasn't constructed with redundancy.

It took Vodafone long days and weeks to restore connectivity. Technical staff was brought in from outside Holland since availability was very dim. Over 700 antennas needed manually activation to restore operation.

The board of Vodafone had taken immediate public action. Webpages informing customer and public were opened. The human resourcing of the helpdesk immediate was upgraded to be able to attend to calls as soon and much as possible. Estimated damages 14 million euro. It has been said that redundancy would've cost 16-20 million.

Experts were utter surprised to learn that a fire at such a crucial, though caused by another factor, could have such an impact. All though management and staff of Vodafone made best efforts, to take positive measures, customer and public satisfaction suffered. In this instance not as much as the Diginotar case.

Conclusions:

- Technical standard precautionary measures

Although Vodafone can't be blamed for this major incident occurred, it is quite odd that a basic safety feature such as a sprinkler, wasn't installed.

- **Heat detection**

With the increasing options and technical possibilities one may wonder why alarm reacted so late.

- **Redundancy and reputation**

Question raised was '*Why wasn't that strategic single point of failure redundant?*' Answer here has been a possible wrong saver. Such becomes evident if a major calamity occurs. Not having redundancy raise the question how much collateral and reputational damage was worth.

Evident here was that customers and public weren't that negative overall with the steps Vodafone had taken. Vodafone offered a voucher to it's customers to be able one day completely sms for free. That gesture was ridiculed since many customers suffered business interrupts also and such a compensation was experienced an outrage.

- **Role of the media**

Journalism wasn't too harsh on Vodafone here. Reason was that though customers suffered interrupt, wide stand personal damage that might have occurred in case of Diginotar here was not a issue.

Because of the ongoing updates of Vodafone there was widespread negative attention in the social media, be it far less than the prior example.
As you here may understand there are different sources that viral into a major calamity, thus IT crisis. Disadvantage today are the roles of media and public social media. Journalists usually are to take the effort investigating 'facts' and comment from there. They also have the tendency to use quite suggestive publications, triggering emotions by readers. The social media is public domain. That by far is faster and often wild spreading.

People in general with crisis like circumstances aren't to distant in their emotions and the psychological crowd like behavior also applies here. This just to mention this fact.

2.1 An angry customer

We sometimes read excessive action of dissatisfied customers in extreme in papers. Like in China a Chinese businessman felt he didn't received the proper care and maintenance for his Maserati and summon press and some volunteers. The volunteers were handed sledge hammers and with clear display of dissatisfaction he'd let the volunteers get at the Maserati.

Some afterwards said it all was a publicity stunt. Be that as it may, take in consideration that not every reader is distant enough to wonder if dissatisfaction here was just or that there could be another argument in the base.

In the world of today the reader, in the least, now understand from which direction a major issue can grow.

Although one may say, 'Hey, it's not my car they're smashing….', on also may understand the publicity it is generating and here the question will be how strong the manager of the Maserati dealership will be. Does he give in or…. Such an action is guaranteed to go viral world wide.

Regardless the debate one could have over this topic, bottom line is that this type of publicity spreads viral. For this real time occurrence was in China, this paper is produced in the Netherlands. Within twenty four hours, even faster, news goes global, today. A fact to bare in mind and to consider.

2.2 The Hacker

In the beginning of the internet, the hacker was dramatized, or romanticized by film. One of the very first movies produced was War Games, with Matthew Broderick. He was a playing school student, the prototype of the computer nerd that played in pre-internet times.

He hacked, of course coincidentally into the systems of the Pentagon and played a simple game of chess with the computer. From there the plot went into something distress where in the end, of course, the student became the hero and everything went back to happy normal.

That is the movie. Later, with the spreading of the internet, acts and actions like these also developed in many directions. All kind of young and often 'principal protesters', started to discover that systems and the internet connections had vulnerabilities that could be exploited. It all developed to basically two directions.

The Principal hacker striving for an equal and prosperous world for all. Hacking to make all kinds of information public for they believe the world is to know what was hidden. The criminal hacker who is after information. Information that can be used or abused for personal gain. Read here that industrial espionage is part of that.

Hacking can be done in many sophisticated or very easy ways.

Very sophisticated by using all means of the internet, connectivity and how to hack information, to gain specific targeted information. Using that obtained information for personal or business gain. That could be extortion or blackmail often. Stealing vital and expensive information and sale them back. It xould be very personal information, used for blackmail. 'Pay me or I will put it on the internet….'
The more easy ways? More and more Identity Theft has become an issue. There are handbooks simply telling what steps to take to become someone and take all kinds of actions in name of that someone. Publish, purchase, steal, cheat, fraud, as long as you may get away with it. It has become so easily sophisticated that you even can fade these steps in the digital world, making discovery virtually impossible.

Warning to be aware

Which of the two, basically that doesn't matter. What is important here that you are aware it exists, it is out there, and you could be next. It's just a fact of living in today's world. The best one can do is understand it does exist and take measures. Not sole personal of course but also business wise.

Here also applies. Regardless debate people can have over this issue, bottom line is the possible damage it may cause. Just be aware.

2.3 The Employee

Most of the budget and effort in IT is directed to systems, software and development, not to forget a lot of manhours. Only few are aware the danger of…… The Employee! There are all types of employees. They're like people. Doing people things….. on the work floor. Mayhem and Horror! For we always know and understand what is going on in people and why they behave like they do.

Just two simple observations, again from publicized matter.

The dissatisfied postman

In Milwaukee a dissatisfied postmen was fired after the office discovered he stole social security checks. The postman went home and got three handguns to return to the office. According witnesses said he walked in with terrifying ease and killed his boss point blank. The he turned to three coworkers he had a quarrel with and also killed them.

He locked himself into one of the offices and took his own life.

What is the value, reputation wise, of this kind of information? Does one blame the postman? Does one blame the Postal services of how they treat postmen? Does one blame society that the policy is the right to bare arms? Wasn't the postman paid enough that he turned to steel checks?

Here the issue that wrongs are intended to be regarded as highly personal. Add emotion to it and it becomes a negative spiral. And negative spirals intent to be picked up by others and they add emotion to it and the spiral becomes a tornado. It even can become completely incomprehensive if public dismay can turn criminals into heroes.

How devastating can such an event become for once business and personal reputation?

Not getting a raise

There is quite some literature that talks about not getting a raise and the consequences of an employee that felt wronged. In IT there are examples of IT administrators even changing all Admin passwords on all kinds of crucial system peripherals. The damage became impair months after the IT professional was gone. System administrators couldn't get access to these peripherals with all thinkable consequences and delay.

In later times and IT development, it has become very easy to be very inventive as systems administrator. The tools are there to use, and they are used. Today these tools are called exploits. And these tools may be placed by someone on the inside. Regardless the purpose of placing the exploits, it always will be that someone has access to, or is obtaining information from the outside. Preferably anonymous of course. The chance that anonymity is growing is the latest development of 'Big Data' and the reduction of skilled professionals in IT. Both here mentioned will be the reason that audit also will be reduced. That will be the reason that anonymity is increasing.

2.5 Limiting Audit and control

As prior stated, IT as matter is a very predictable matter. It, as matter, is unchanged since the creation of the Enniac, the very first computer, up to today. The very bases and laws, directions, Do's, Don'ts, processes, procedures, the way to use and scale it, nothing has changed.

In writing this, immediate all kinds of objections, trying to tell that it is different, a whole world of difference with then. IT has evolved to …. Never the less, all here above in essence are entirely the same. IT as matter, behavior, is most predictable and the processes and disciplines are to be too. If they are not in practice, then you know the cause is inconsistency. The process, project, procedure, the particular IT discipline, is not consistent with the linear character of IT as matter.

That is, if people that doesn't understand it's behavior and laws, are setting IT up, demanding IT to do things contra IT. Processes are not aligned with matter, when people reinvent wheels and want to redefine the laws of IT and calling them all kind of appealing names and methods. *Then, dear reader, then it's just waiting for the next fail.* ***And that is guaranteed****.*

Since the entrance of Office Automation (OA), the first local networks (LAN), and later the Wide Area Networks (WAN), the number of disciplines expanded. The bases of the processes? Still the same. The bases of IT? Still the same.

IT Disciplines, Design, Support, Service deliveries, Implementation etc. etc.? Very dynamic and often… Often not so complying to these bases of IT as matter. They are often very good professionals, understanding very much the in's and out's of there own disciplines, but surely not always how IT as matter is working, behaving and thus….. sooner or later, confronted with the counter sides and flaw..

2.5.1 The very flexible workforce

In Europe the contingent of the IT workforce constantly was shifting from internal staff to external service delivery. From India, Kuala Lumpur, Thailand back to local resources and from there, because of EU regulations tendering to a mix of local staff and interlocal staff. Many smaller and larger HR supply, cowboys, agencies, independent consultants, all striving for a part of the big customers IT pie and often so incoherent or unorganized, that it causes hamper on the very bases of **Audit and Control**.

Sure, every ISP, Service Delivery group or unit, has the best intentions, interest, service and support for your organization. Never the less, the real controls you need, often is neglected. Due to the passing of so many IT professionals, very important issues such as logs, documentations, de buildup of your organizations IT history, has often shown not to carry any real priority. Of course it was written in the contracts that….. sure it was.

The Flexible workforce has it's own dynamics and therefor at the same time carry risks to be taken in accountant. It bares fare more and reaching consequences than one may think of.

2.5.2 Economical crisis and HR consequences

In times of economic setback, it almost is waiting for the first cuts to make in…… IT. Still IT isn't regarded as Strategic, merely aid and support to the organization. The first cuts often involves IT staff. To many, too expensive. After these are gone ….'Lord behold…. Everything still is working… Those who made the cuts exclaims here's the proof that IT is dearly overrated. See, we could have done with far less.' Objective accomplished.

That the consequences are yet to to come, is what happens every time. When we are talking about automation, independent functioning and operating systems, there will be a moment that something somewhere starts to hamper. First unnoticed, deep within. As long as the issue is minor, it will be dealt with fairly cheap and easy. But what happens if the issue(s) become structural up to thst msjor event?

A fire? A supplier that wasn't checked anymore structural, for we trusted hat supplier didn't we? Or what if we were all of a sudden the interest of that hacker? And we abandoned strategic IT disciplines by making these a simple administrative meaningless task? What if the IT chain starts to disintegrate after most minimum responsible and acceptable bases of decent IT discipline also was deminished?

In HR sense the challenge is to find the best possible professional on that open vacancy. It is common fact, with all respect, that intrinsic understanding of IT and it's behavior and intrinsic knowledge of Human Capital, is not always available in HR. This bare immediate consequence in recruiting staff for that vacancy.

2.5.3 Poor management

Another devastating consequence that an organization walk into is poor management. That poor management may come from any direction and isn't obvious at all. You see it happen of a manager arriving on a certain level through ancient promotion, a position occupied by an internal HR pool, professional who have no intrinsic experience or affinity with the matter or discipline yet follow the rules and procedures without minimum face and challenge..

In political organizations one encounters quite often political engaged occupation of quite strategic IT key positions by politicians or civil servants, not having the slightest knowledge or experience in the matter. Yet, these professionals are, responsible for many very important and strategic decisions. Lacking strategy and IT chain experience, they rely on others, without being able to challenge presented information. Here these professionals seldom feel accountable, never the less being the bases of largest and fastest emerging damage when events occur.

As portrayed in 2.5.2 not understanding the absolute essence of what is viable and safe in an IT organization, one can't even control or challenge the IT Service supplier whether they are performing up to par or not. There often are huge differences in contractual matter and what actual is delivered.

Limiting Audit and Control, what ever the reason, will immediately bare consequences for the entire organization. How large the consequences? That is up to a number of failing contributors in that particular process. But *'the more the merrier'* also applies here.

3. Crisis Catalysts

A catalyst is a natural or non-natural incident, object, time or person, who, independent as a particle, contributes to the process becoming an issue, incident spiraling out to crisis.

To reach the point to 'promote' an event or situation to 'Crisis', one needs Crisis Catalysts who, combined, build up to a level where there is large human or material consequence.
In here before mentioned, a number of 'so called' Catalysts.

Two examples of large scale events.

3.1 The Japanese 2011 Tsunami

On March 11, 2011 a seaquake took place 130 Km's east of Sendai Japan. It was a 9.0 quake on the Richter scale. As a result of that quake a series of monster waves landed on the Japanese coast as first, within two hours. The average height of the incoming waves was measured over 15 meters. The tsunami eventually covered 400 sq. kilometers of Japanese soil alone. Nearly twenty five thousand people died and over eighty seven thousand houses were destroyed.

The catalysts resulting into this crises? An Seaquake, as a result of that quake forming monster waves traveling unstoppable to Japan and elsewhere. Landing as 15 meters high waves destroying anything in its path. Here we have an amount of sole natural catalysts leading to disaster.

3.2 The failing Switches computer

Februari 2012. The railways experiences, on broad daylight in winter, that rail road switches failed. Group by group they went down and what people tried, the couldn't access the systems anymore. They were afraid that the IT systems were compromised. It was the center of the countries railways and many alterations had to take place.

Passengers on stations virtually were not informed and most of the railway employees present on stations, didn't seem to provide satisfactory information at all. Frustration among increasing frustrated travelers reached new peeks. Social media like twitter exploded in reactions. After hours of investigation they found, so it was published in the news media, that somewhere an old crucial pc, containing all the switches information, went down. No one was able to take any action since the computers configuration was hardly known to anyone.

Many fingers pointed to IT service delivery units. They responded that they were advised not to touch the computer when inventoried because of the crucial vulnerable information on it. A pensioned IT technician heard the news and found he had quite some trouble getting in touch with the department where the computer was situated.

After three hours finally he spoke to a lady of the sales department who had 'mind' to take charge and contacted the IT department. Initially even the lady didn't got any access to a manager where

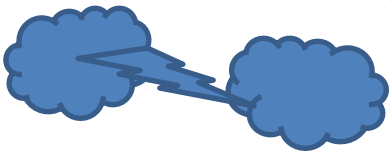
after quite frustrated she walked to the department and had to shout to get any attention. Finally the IT professionals contacted the pensioner and the problem swiftly could be resolved.

Catalysts here were several IT professionals in transit over time, an old computer with very viable information and software on it, incomplete procedures, lack of competence and control, and lack of documentation and clear process. Last but not least ***no E2E IT procedure***.

The consequences are quite obvious. Many thousand train passengers waiting for hours, virtually no decent communication, no means of communications with the railways information services, increasing frustration.

In the aftermath the railways apologized to all its passengers but offered no compensation what so ever. Here the damage is multiple. Where IT is involved, process and procedures simply are predictable. Due to classic faults, a serious situations occurred before and will occur again. Until….

3.3 Contradictive Communication



A negative force to take in account often is '*contradictive communication'* coming from the same organization. Press often show to be quite resourceful in obtaining information in case of such a thing as a 'wide spread' occurrence. Another instance is that contradictive information may come from different source outside the organization, all contributing to undesired opinion forming by the public.

3.4 Public Information Sources (radio/television/Internet)

In this rapid and speedy world, there is the dangerous tendency by press, politicians and 'experts' to philosophize aloud in terms as '… If that is the case then….', 'It very well could be the case that….', 'If that is fact then…..' presenting that as being a solid opinion or fact. The public intent to use the internet as first source of validation and one can understand what happens next.

Presently it is seen that news sources often simply copy information or facts and publish them. This often incorporates inconsistency for not all 'journalists' intent to check facts. Hypelike information provisioning is contributing to a certain undesired flow of reactions that finally is by far exceeding any ground or 'the simple facts' of the event or occurrence.

3.5 Social Media

Up following last mentioned, the social media often contributes as greatest source to bring an occurrence to 'hype state'. In more then 90% of the cases of an hype the case here is that people intent to simply copy and paste what others prior stated, taking these simple for fact. Especially twitter, Facebook and other types of fast media are contributing often to a series of action and event leading to…..

Even after facts were contradicting the hype(s), people still believe some sort of cover up is the case tot validade the wrong.

IT Crisis Management©

Here is a simple overview of a series of catalysts that spark and fuel an event or occurrence into a uncontrollable seeming disaster.

Natural Catalysts

- **Extreme natural behavior**
- **Economical circumstances**
- **Business circumstances**

Mechanical Catalysts

- **Faulty IT peripherals**
- **Faulty software**
- **Bad/wrong implementation**
- **Fire caused by short circuit**
- **Non redundant IT systems**
- **Data carriers**
- **Hubs/Routers/Switches**
- **Strategic LANs**
- **Strategic WANs**

Human Catalysts

- **Ego**
- **Non intrinsic knowledge/experience**
- **Miscalculation**
- **Miscommunication**
- **Assuming without verification**
- **Misrepresentation**
- **Poor judgment**
- **Poor management**

As last it needs to be mentioned that it also can be desired by certain source that an occurrence is to be wide spread. Please remember, incident, event and occurrences also can bare deliberate steps.

IT Crisis Management©

4. Simple outlines and routines.

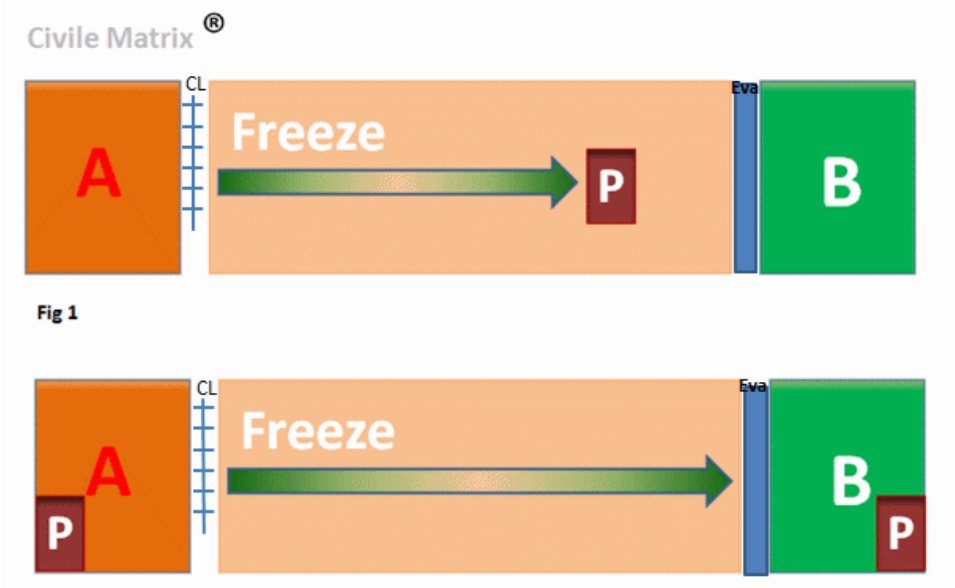
When an IT incident, event or occurrence is spiraling out of control, one is in need of a strong way to get grips and control again. In the woods of 'IT methodology', strangely enough there is no Comprehensive Simple Method that enables one to regain charge….. again. Many 'dynamic' processes all of a sudden seems to become a part of the overall picture. Be that as it may, there is a very simple and most effective way to regain control.

From here IT in it's most Essence is illustrated and demonstrated. To gain and hold control, is simply a matter of following IT in it's most elementary form. Regardless all the dynamics or turmoil often surrounding the world of IT.

In any occurrence or event in IT, large or small, it is mandatory to keep the focus on the way IT as matter works and behaves. Doing that on crucial moments will bring you more clarity, focus on the important points of issues, tasks and gathering required information and surely focus on the fact and answers. In length to that it also brings you the root cause and how to deal with the surroundings of an event or occurrence. Basically it is straight forward.

Before we start, very brief here illustrated and demonstrated how the principal of IT as matter works. Please be aware, with all due Respect, over 75% of IT professionals, though experts in their field(s), are not aware of the basic IT behavior as matter. Understanding and adopting this all, will let you as management be fast, and remain in control on fastest most secure terms.

4.1 The Civile Matrix.



IT in behavior, reaction, discipline or process, is bound to these very simple principals. A to B. To get from A to B, one need a series of requirements (Values in Check List gathered). Here it becomes evident that IT in its essence is most predictable. Since one need value to let IT do 'Something', one also can decide to have IT do nothing. Simply by doing nothing.

Then there is the most essential process, demonstrated as the rose field stating 'Freeze'. Freeze means that during any process, anything is abandoned in order to prevent any incident, event or occurrence from happening, baring impact on that process. Safeguarding that the process progress as aimed. Then, if everything is completed as planned, one comes to the blue field to evaluate, then one arrives in B.

If a process encounters **P**, for **P**roblem, one has a simple moment to decide. The **P**roblem is minor and can't or will not disrupt the process. In that respect one may put **P** in **B** and deal with it later. When **P** becomes larger than the process? An IT process will come to a halt. There will be no human action required. It is IT law. In real life human intent jump up when incident, event or occurrence emerges. Still the answer is simply: **Halt!**

Pick up **the Civile Matrix®**, punt that moment in **A**, and restart the that process. The sooner one understands and incorporates this? The faster results and profit. In every desired respect. Multiple processes or projects? Line them up next to each other, or in front, side by side, never stack processes or projects on top of each other.

This simple essential principle step, can be repeated infinitive. This is what IT as process is to be seen and used, since matter IT behaves this way. The matter is linear as well as the disciplines, processes, projects and programs are to be, on every level. Not complying to this essential routine? Then be sure that some moment, near or later in the process, project, program, plan, scheme you'll guaranteed to be confronted with **P**. The more one ignores this principal? The larger the **P**.

4.2 Freeze

Freeze is a mandatory instance on the moment an IT process is live. Whatever that process is. Often this mandatory instance of that process, is neglected. The consequences, depending of the size of the process, is the root cause of things that goes wrong. Many managers react, when things start to go different then desired, to take some sort of action. Depending the moment and circumstances, often the steps are most time counterproductive. They haven't knowledge and understanding of the essential IT principal in the bases and will take any action to have that process continuing.

Remember the **P** in the Matrix? **P** will become larger than that process. From there it is physical law of IT that there will be a moment that the process will collapse. It will **Halt!** The consequences? It is like fueling a blaze in stead of try to distinguish one. Regardless the size of that particular process, remember **the Civile Matrix® ?** If the problem is larger then the process, simply the process will **Halt!**. Look at **P** and decide. Resolve **P** later or put **P** in **A**. Simply restart the process.

The advantages?

- **Control**
- **Speed**
- **Clarity**
- **The cause becomes evident**
- **One has learned**
- **Process becomes faster and faster**

To Simple? Who said it must be complicated?

4.3 Ownership

The most important moment is the moment when a situation is spinning out of control as earlier portrayed and illustrated. Depending the bases of origin of an event, incident, occurrence emerges, suddenly one sees 'egos' want to take control. Often with very counterproductive outcomes.

No we have established the very essential bases of an IT process in process, the next step is **Ownership!** Very Crucial. Ownership in IT is a mandatory rule. It often isn't described as such in all the methods, but here it is, in essence.

E2E procedure

Any member of the organization carries equal responsibility for the production and outcome of that organization. Therefor any member is equally responsible for processes and best possible outcome. To reach that every member carries the responsibility to take ownership of an instance, incident, occurrence or event, and convey or delegate that instance to the rightful echelon to be resolved. At any given moment the member is owner of that instance, incident, occurrence or event until that member is released by the resolving echelon.

By acting according this basic principal, an organization is slowly becoming aware that all members, regardless role and responsibility, are equally responsible for another member in the organization. This principal is part of the awareness that transcends individual role and responsibility.

IT Crisis Management©

If there is a hole in the pavement near the entrance of the building, on doesn't like to step into it as much that he/she wants someone else it to happen. This mutual responsibility isn't difficult to understand or to implement. It is easy. It prevents and saves immediately while enhancing and bonding the organization.

4.4 The Basic Chain of command when 'it' occurs.

When an event occurs, that is beyond one discipline, where IT is involved, a simple chain of command is to be established. Many organizations have many plans, but not always a plan for an IT crisis situation. The chain of command is the same in essence as the essence of the most basic IT process.

The top of the chain is to be occupied by a experienced professional. Whether she/he is a board member or not, is not really an issue. Issue here is that that professionals understands what an IT process is, understands in essence how control in IT disciplines flows and how to obtain valuable information. In addition that professional is best to gather experience in communicating within the organization, but more important, ready to communicate to the outside world, in different directions.

Directly below, the highest IT authority of the organization will be situated. There after simply the professionals who carry reaching responsibilities out in different disciplines in the organization.
In bases an illustration may look like following.

Board Executive	Member of the board communicating with other members. Delegating tasks - Internal External comm - Process owner	⇨
CI(T)O	- IT Analysis & report - Delegates tasks - Source of information - Internal/External Comm?	⇨
IT Management	- Delegates tasks - Source of information - Internal/External Comm?	***No Comment***

Networks	Office Automation	1st/2nd line support	Service Desk	Internet
IT Security-Administration	Etc			

IT Crisis Management©

A board member, or someone on Executive level takes ownership and control.
She/He establishes chain of command according procedures created for instances like these.
Together with the CI(T)O an assessment will be done to classify an event or incident, and assess possible implications. Here she/he may decide what to do. To delegate or not to delegate.

The CI(T)O on her/his turn, becomes the source of information. In length she/he starts communication with next coming IT echelons to gather and verify information. IT Management relays on IT disciplines like every day in the operations.

As one can see, there are no 'interesting/complicated processes or procedures to be designed. All elements are there in any organization. Key simply is to be aware they are and shift awareness to use roles and responsibilities best in certain situations.

Procedure:

1. **Freeze!**
2. **Connect required people, describe issue/event**
3. **Never assume, always verify -> Check fact and source of origin**
4. **Assess (possible) immediate danger or damage**
5. **Declare 'yes/no' emergency internal**
6. **Obtain the shortest route to solution**
7. **Execute solution**
8. **Communicate external yes/no.**
9. **Document all for future reference**

Always Freeze. No matter the dynamic of the surrounding world, just Freeze. Don't fuel any energy coming from the surrounding world. Get in touch with the pre-set key figures, simply ask how, what, where, and take it from that point. If the matter is quite easily to be resolved, just delegate it to the rightful discipline, and continue.

If the situation becomes really critical, then assess what situation is. See that your source is internal, not what is been hyped out there. If an crisis is declared, state this clear internal. As of that moment a number of things are changing in every days chain of command within an organization. The urgency of the matter needs priority to be resolved a.s.a.p.

When the solution is there, execute it. At the same moment communicate the most essential internal. Always stay aware that providing very detailed information of any solution internal, also increases the chance that information can be leaked to the outside world.
Finally look back together and document events for future referral.

If communicating with the outside world can't be avoided, or is highly desired

Do!

- **Take and keep control**
- **Admit there seems to be an issue(never problem) that is addressed, if applicable**
- **Never become intrinsic, use third name illustration or demonstration**
- **Consider the use of social media and/or news media**

- **Avoid revealing details**
- **Limit chance of over flooding phone lines by issuing ongoing statements**
- **Limit and focus to facts, never engage in hypotheses**
- **Ignore pressure of news and social media**
- **Be discrete, don't point fingers**
- **If a fault or mistake becomes public, simply understand that there are people at work, mistakes happens, be loyal**
- **State what is done for the future and end debate**

Having contact with news media needs a certain mind set and attitude. This is not for every one. Realize that everything one says or displays, will immediately enlarge in the media. There are professional ways to become familiar with the subject and the hazards surrounding using of becoming a part of news media.

Take every opportunity to get familiar with them.

A real time event

In 2011 a hacker declared through a social media that he hacked an organization that provides IT and telephone services. He claimed to have obtained customers names, addresses, phone numbers and even log on credentials and passwords.

The distress grew as the news media picked up this 'news' and even before any decent investigation the online newspapers and other media, exclaimed, ***"Organization hacked, names and passwords stolen!!!"*** *Over the internet that went viral and before anyone knew what was going on, sources were stating that over one hundred thousand name, addresses and private details where stolen by a hacker.*

That evening a spokeswoman for that organization, attended a television show where she gave very poor information. She couldn't answer most of the simple questions set. She stated that it was important to emphasize that customers should be aware of the vulnerability of their accounts and email and never to give any one passwords. One of the host stepped in by saying,' quite nicely put but the IT systems of your organizations were compromised by a hacker, any customer doesn't have anything to do with it….'

The organization took action. What action? That remained invisible. After two days they decided to close more the two million mailboxes of their clients to safeguard personal data. Shortly after that action, it was announced that the published list the hacker did publish, contained names and details of a on line web shop, not even connected to the organization.

It became clear that the hacker indeed compromised systems of the organization but wasn't able to gain access to sensitive customer data. Further investigation did reveal some tempering of systems which were corrected. Customers who couldn't access their email, were send letters with new passwords as an additional service. The service desk over flooded by customer requests and contacts and it had taken weeks to restore all to normal

***

This incident isn't an isolated one since it is occurring more frequent then often admitted. On the outside it became very clear that that organization didn't had any IT crisis procedure to fall back on. They didn't follow any essential basic procedures to assess the situation. Eventually they were led by the dynamics of the surrounding world. Of course the organization denied that this has been fact.

If you now look to the simple straight forward list and illustration, it becomes quite clear why an organization should instate such a process and procedure. We are living and using a increasing digital society and with that, the chances of becoming the target, also increases. It is just fact.

Last piece of advise in here? Simulate!

Create that IT Crisis procedure for your organization. All it take is some time but when '**it**' happens….. You will be prepared. Set up that procedure and simulate it once a month or quarter. Reason to advise you that is that people in general intent to get awareness and motion in there physics by repetition. That also applies for getting ready for that moment you hope that will never come.

5. Finally

IT is a great and predictable matter, that is, can be of great benefit to any organization.
Professionals also are to be aware that there are laws and mandatory ways to look at, work with and explain how IT works and works best, to get the highest benefit and advantage out of it.
To help those interested Executive, board member, manager and professional, IT and non IT, to gain even more, here a number of considerations…… next to **The Civile Matrix®**

Before any step where IT is involved, set two questions. If either one of the two questions aren't answered to satisfaction or comprehension, then one is to think again to take that step.

1. Why do we automate?

One automates to increase speed and ease in manual actions, gaining time, be more productive and be able to increase productivity with less manual input and resources.

If there is no benefit in here? Why automate?

2. Why should we automate?

This question raises the clear awareness to think why one should take a step. Does in increase productivity and output or is someone trying to sale us something. This is not limited to hardware but more to all kinds of methods in and for IT.

3. The Civile Matrix®

Up to today the Civile Matrix still seems to be the most comprehensive illustration of the essence of essence of the IT process principally. Any larger process or procedure in IT, consists out of multiplication of that essence. Before you think some one is trying to sell you something, it is free of charge for the benefit of your organization.

4. Never assume, always verify

Because of the nature and linearity of It a matter, IT is a very predictable matter. It also means that disciplines, processes and procedures are to be implemented with the same linearity. Something often forgotten. If one is assuming that …. Then the risk of running into **P** will increase.

5. Simple, Simpler, Simplest

Where has it been written that interested should be complicated? People in It that make things often complicated? They have something to cover, they have something to sell you or they want to make things look more interesting. Remember this; The more parts or people you need, the less you are about to safe. Law of physics will tell you the more components, ways, people, the higer the risk that somewhere, somehow, something can go wrong.

6. Fix the problem, not the cause

Many think it's very profitable to gather in an emergency meeting and come down to 'important' understanding about 'how a problem should be labeled or named'. Next step in such a sequence is to try to find out what caused it and how it happened and who was responsible for what.

IT as matter doesn't care about that. IT is a dead matter and it remains that way until, until someone decides to take a step. Debate and philosophizing is not taking ownership nor decision. IT as matter is predictable and therefor the cause of a problem, will emerge in the process of fix! Don't waste your time and energy on debate.

7. Use proven concepts

If you want to be guinea pig, then let them pay you. It happened so many times before that 'Offers' did show overall not to be 'That Great Offer' with all consequences there of. New ways of Projects or Program Management. Professionals coming from agencies that you won't have to pay for the first two weeks, or the free app or software package.

IT as matter is aimed conceptual and objective orientated to increase productivity, save time and with that increase profitable margin. The chance that valuable time is wasted for debate, adjustments or production decrease, is not the objective of using IT in the organization.

8. Test, testing test, test….

When cuts are made, budgets cut in half, something else 'down the line' has to give. Quality is lesser issue. Later in the process the number of errors will increase as a consequence. This is a clear reminder how important seeming lesser important steps in the processes are.

9. Pilot

Pilot is a phrase that came from another territory. Basically it was another word for trial. In IT a pilot is the very first trial to see whether what was designed, formed or planned, is behaving as documented. Out of wrong type of saving, more and more the pilot as a mandatory step of a large scale implementation is neglected. The direct results are an exploding number of fails in implementation.

After that the consequence of not piloting can easily be summed up. People are infected with the negative outcome that may bring frustration up to loss of time and production. Precisely what was the aim of prevention that Pilot stands for.

10. Roll Back!

One of the most costly mistakes one may run into is forgetting to check one simple thing. Roll Back. There are great planning's, projects, programs, presentations of implementations ….. The biggest pitfall one may think of? Roll Back. There are many contributing factors to take into consideration and account, that has an influence or the chance of impact on every step one is about to make in IT.

IT Crisis Management©

It is a **mandatory** part of the overall IT process and procedure that is a most neglected factor so often. If a thorough thought and tested rollback isn't part of a planned implementation? Consider how large the bill in the end will be if it happens to you.

IT, a great matter, to bring you benefit. But in the hands of not so great professionals, it easily brings you large bills. Simple facts to consider, absolutely free of charge.

Good luck with your IT endeavors.

René Civile®
IT Crisis Mgt.
Rotterdam NL
info@numoquest.nl
+31 (0)6 2936 1218