Holistic Physical Risk and Crises Prioritization Approaches to Solve Cyber Defense Conundrums.

Dr. Franco Oboni, Oboni Riskope Associates Inc.
Cesar Oboni, Oboni Riskope Associates Inc.
Vancouver, B.C., Canada

ABSTRACT

During the last decade the techniques and tools of cyber attacks have become more sophisticated, the distinctions between actors and threats have become blurred and attack prospects more worrying. The informational threat can hit any type of civilian or military controls, fixed or mobile infrastructures, putting them down or greatly reducing their service capabilities with direct and indirect physical / economic impacts from tactical or local scale to strategic / national and international level. It has been shown that broad spectrum protection investments and particularly poorly prioritized ones are not efficient as oftentimes they are limited in scope by other operational requirements. So it is simply not possible to protect each property from each threat. The cyberdefense must be rooted on intelligence based on prioritized Risk Management and not on standardized audits and practice of indolent regulations, written a priori, or the biased advice of fear monger solutions sellers. RM offers ultimately support for operational decisions and protection (mitigation), provided that we want to define the level of acceptable risk reduction /mitigation and that we formulate measurable performance targets to achieve .

Keywords: Physical Risk, Cyber defense, Prioritization, Risk Analysis

1. INTRODUCTION

During the last decade techniques and tools for cyber attacks have become more sophisticated, the distinctions between actors and threats have become blurred and the consequences of prospect attacks more worrying. The informational threats can hit any civilian or military, fixed or mobile infrastructures targets, putting them down or greatly reducing their service capabilities with direct and indirect/economic impacts ranging from tactical/local to strategic/national and international scale. As an example, during two days operations in 16 countries worldwide, supported by the European Cybercrime Centre (EC3) at Europol, creators, sellers and users of BlackShades malware were targeted by authorities: 359 house searches were carried out worldwide, and more than 80 people were arrested. Over 1100 data storage devices suspected of being used in illegal activities were seized [4]. Today, more than ever, planners and decision makers are oftentimes held accountable for outcomes appearing to be beyond their control, generated by decisions made by others, in different times and socio-economic, industrial and legal environments.

Complex and significantly interdependent systems are difficult to grasp and even perceive and it is often hard to gain clear understanding of their elements and operating conditions, especially since fake apps have proven to be one the most significant methods of distributing mobile malware [2]. However, decision makers can take better decisions, justify them, defend their selections and positions only if they clearly understand their systems and can properly evaluate their 360-degrees risk environment.

The list below shows five major “emerging truths” in the organizational world with corresponding selected cases of successful recent cyber-attacks:

Correct identification of "external" threats and reduction of operational and strategic information (intelligence) gaps are paramount: it is critical to look upstream (suppliers) and downstream (service companies) in the supply chain because vulnerabilities upstream or downstream can significantly affect operations in the considered system.

Example: Attack campaign compromised 300,000 home routers, altered DNS settings. Attackers used a variety of techniques to exploit known vulnerabilities in router models from different manufacturers.

Failure to identify minor deviations and/or near misses which could be signs of an impending attack, or one underway, is a significant flaw.

Example: On July 4 2014 a group of relays that were assumed to be trying to de-anonymize users were identified. They appear to have been targeting people operating or accessing Tor hidden services. The attack involved modifying Tor protocol headers to perpetrate traffic confirmation attacks. The attacking relays joined the network on January 30th 2014, and were removed from the network on July 4th. While the start date is unknown, users who operated or accessed hidden services from early February through July 4th should assume they were affected [11].

Example: Private information about over 80 million clients of American multinational bank JP Morgan were stolen by hackers in a massive cyber-attack during summer 2014. The attack ran undetected for many months.

Treating cyber-security as a IT sector matter (silo-ed information), rather than a global operational / strategic risk is a very significant flaw. A cyber-attack can have the same effect as an earthquake, an explosion, an artillery bombardment, and it is therefore of utmost importance to treat it as any other hazard that may affect a system's service.

Example: Hackers struck a steel mill in Germany. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in reportedly “massive” damage.

Protecting assets in a properly planned and prioritized way is a must. Asset management should be linked to Risk Management (RM). Audits and compliance with regulations do not constitute a sufficient pathway to safety.

Example: In December 2013, Target confirmed that hackers had infected the company's payment-card readers, making off with approximately 40 million credit and debit card

numbers that had been used at Target stores in the United States.

Capabilities of the enemy, whoever it may be should never be underestimated.

Example: Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. Canada Revenue Agency, U.S. hospital chain in the United States and many other where exploited [6].

Thus, it should be concluded that broad spectrum defense investments and in particular poorly prioritized ones are not efficient. "Businesses and government agencies often focus on the next "silver bullet" product, unaware that most cybersecurity problems stem from flawed procedures and human error, said Art Gilliland, senior vice president and general manager for Hewlett-Packard's software enterprise security products", quoted in a recent article [5]. It is simply not possible to protect each property from each threat especially as oftentimes these investments are limited by other competing operational requirements. Cyber-defense must be rooted on intelligence, based on prioritized risk management and not on standardized audits and practice of indolent regulations, written a priori, or fear-monger sellers solutions. RM offers the ultimate support for operational decisions and protection (mitigation), provided clients want to explicitly define the level of acceptable service reduction and risks. It is important that RM efforts are based on methodologies that avoid confusion and help users focusing on scenarios that generate risks that really matter [9]: it has been shown that, typically, a small number of risks scenarios (10%-20% of the total portfolio) represent 80% of the total intolerable risks, in compliance with the well known Pareto principle (a.k.a the 80-20 principle).

The key to success in the risk management approach to Cyber-defense of complex systems like modern corporations or armies lies in:

a) the correct functional analysis of the system, including its inter-dependencies,
b) the abolition of informational "silos" (treating each problem by itself),
c) avoiding paralysis by analysis and
d) looking to the minimal survival criterion of the systems involved and clear social and organizational tolerance criteria. Finally,
e) giving cues on what should be included in the consequences function in order to depict reality as well as we can.

In particular it can be stated that incomplete functional analysis of the system (-a-, above) and information silos (-b-, above) inevitably lead to poorly built hazard identification which in turn can lead to conceptual dead-ends finally clouding the desired results.
In the sections below we discuss these points one by one.

2 NEED FOR CORRECT FUNCTIONAL ANALYSIS OF THE SYSTEM CONSIDERING ITS INTER-DEPENDENCIES

We all know that ISO and other International and National Risk Codes stress the fact that the context of the study, the environment in which systems operate has to be described. However, we have seen so many times project teams and facilitators embarking in FMEAs or other risk related endeavors without taking the time to rigorously describe the system anatomy and physiology. This routinely occurs for "small projects", but we have seen it happening for multi B$ cases. Although it may seem strange to use medical terms in this context, let's follow this train of thoughts in the next two subsections.

2.1 A brief history of medicine

In prehistorical and early historical times human health (the system of interest in medical science) was in the hand of shamans and other medicine-men (and women) who were using empirically selected remedies (herbs and roots, for example) or ceremonies and rituals (including inducing mental alterations of various kind) to heal mind and body. Let's not judge these techniques, especially since, at the time, there were no alternatives to select from and we know by now that some of those remedies actually worked very well. However, humans were neither really happy with the understanding they had of human body nor with the overall rate of survival. They needed to understand more. Hence, for example, Leonardo da Vinci started to perform anatomical studies (dissection was prohibited by the Church and the Law in those times) and recorded his acute observations in the famous sketches we still display in various museums around the world.
Those studies delivered a first understanding of human anatomy. A few more centuries of research brought us to be able to detect genetic mutations, hereditary diseases and much more. The development of this understanding was not always easy, as religion, obscurantism and other agents were not always open to the enhancement of science, and that would be quite an understatement. Only in the early 1900, thanks to S. Freud we started treating psychopathologies with psychoanalysis and then started understanding the link between physical ailments and psychological troubles.

2.2 A brief history of Risk Assessment Methods

Most common practice tools date from WWII and the '50s. At the beginning only weapons and blatantly hazardous systems were studied using those methodologies. Industry was still generally using the so called "insurance gals" to transfer risk, without any serious evaluations, to insurance companies willing to take a bet on them. Later, a series of mishaps, public outcry and political pressure events, lead "risk" to become a buzz-word. Risk assessment and risk management were nice words to say, and common practice percolated down to the minimum common denominator, using FMEA and other inappropriate methods and models to give a "placebo" to everyone. Accidents were still occurring, foreseeable failures were still called unforeseeable, potential consequences were still looked at cursorily and in a compartmentalized way. No one was carefully describing the system's anatomy and physiology. It was the time of open risk workshops gaining the status of "instant risk assessment". Actually most of the time participants were able to voice concerns and fears, without having dissected the system under consideration, pretty much like we used to do in medicine before understanding anatomy and physiology. Then large scale terror acts (9-11-2001) occurred on US soil and in 2008 there was a global recession. All of a sudden new words were coined to hide what we Humans knew very well already: poorly made risk assessments do not bring any value.
The discussion drifted toward systemic risk, dysfunctional models, black-swans (legitimate ones and silly ones), fragility, complexity, etc. It was a feast of magic revival, obscurantism,

denial of bad habits. All of those efforts just to conceal one simple fact: unless we take the time and effort to properly define our systems, we cannot perform any serious analysis on them! The parallel is striking: if we do not know the human body anatomy and physiology, any surgery or drug will have a very poor rate of success, or may even become detrimental.

So, getting back to risk assessments:

- Is it true that our systems are complex? Yes.
- Do they have fragility because of their complexity and other reasons? Yes.
- Do rare, extreme, but often foreseeable events occur? Yes.
- Do we have systemic risks in our systems? Yes.
- Is it true we can dig our head in the sand, say there is nothing we Human can do to evaluate the above and merrily keep doing the same mistakes? YES.
- Is it reasonable, socially acceptable, good for Humanity to do so? Heck, absolutely NOT!

Just for fun one can set-up the same list of question replacing "system" by "human body"; "events" by "diseases". Enjoy!

By fostering a systematic analysis of system's anatomy and physiology, we can avoid most, if not all, of those pitfalls. That preliminary effort:

- brings rationality, clarity and transparency to our endeavors,
- makes risk studies scalable, flexible, adaptable to new conditions,
- yields a holistic understanding of the risk landscape surrounding your operations/projects.

3 NEED TO ABOLISH INFORMATIONAL "SILOS" (TREATING EACH PROBLEM BY ITSELF)

3.1 Understand your system and its process

Risk management has to encompass asset management, a concept lately embraced by ISO 31000 and ISO 55000 in an effort to reduce "silos culture". It seems that ISO is also finally recognizing that QMS (Quality Management Systems) cannot be dealt as information silos, independently from Risk Management and therefore puts clear emphasis on Risk-based management:

- consider issues,
- determine the risks and opportunities,
- define actions to address the risks,
- etc.

It appears that the new ISO 9001 2015 draft (to be published in September 2015) includes in the "Understanding the organization and its context" section a requirement for the company to be certified to determine external and internal issues relevant to its purpose and that affect its ability to achieve the intended outcomes of its QMS (i.e. risks). In other words it is asked to a company requiring ISO 9001 certification to be clear on its organizational structure and its context (see section 2 above), then perform a risk management approach to determine what could go wrong that could prevent quality to be maintained as intended by the QMS. In fact, today, declaring Antivirus Software Dead, many firm turn their attention to minimizing damage from breaches [14].
ISO stresses a "process approach", i.e. understanding the anatomy and the physiology of the considered system, including upstream (suppliers, logistic) and downstream (clients, logistic) entities and related processes. The Draft also stresses that top management must demonstrate leadership and commitment with respect to customer focus showing how interpenetrated this goal is with risk management. Customer trust *is considered to be the connective tissue that holds customers, brands, and enterprises together; and, without trust, these connections would quickly dissolve*. All of the above is clearly the result of silos erasing efforts. Over the last few years we have spent a lot of R&D funds and efforts to study the relationship between public perception of risks, risk assessments and crises developments, coming to the same conclusions.
If trust is not built through at least:

- transparent and rational risk assessments,
- proper internal and external communication and
- true dialogue between projects' proponents, operational entities, governmental agencies and the public,

then projects, operations, initiatives are inevitably rejected, boycotted; protests can even degenerate into violence (see section 4 below). It has been stated that "50% of the problems with communication are due to individuals using the same words with different meanings. The remaining 50% are due to individuals using different words with the same meanings" [1].

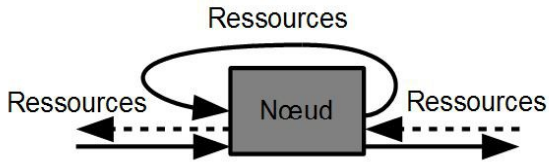

Fig. 1 Schematic representation of a generic node. The dotted arrows are there to back the rigor of the exercise, showing that system's interdependencies are generally bidirectional. One flow direction is usually dominant in the generation of risk. The resources marked by the "internal loop" are those sometimes generated by processes within a node, but not going out as node's outbound resource (products). Their inclusion can be practical, at the macro level in many industrial/construction processes where, for example, energy is generated within a process and recovered to assist in the production of the outgoing resource.

We recognize that what drives customer trust works as well for good risk management and the resulting social license to operate! Examples abound in Italy and the rest of Europe, and, of course world-wide, where poor communication has lead to significant difficulties. An integrated customer-centric communication/experience plan can be fully integrated with risk/crisis assessment/management plans, yielding impressive ROI on smoother and more efficient operations, higher (internal/external) satisfaction and awareness and fostering/preserving social license to operate. Changing the silo culture is paramount to achieve these goals and the steps below will help:

- Implementing a repeatable and inexpensive operation risk awareness and preparedness approach revealing

global strengths and weaknesses of the management and leadership of the evaluated entity. The approach should also deliver a metric of the Operation/ Corporation/ Project Survivability Readiness and Awareness in case of hardship, extreme events, crises and mishaps. This will help guiding efforts in an efficient and concrete way;

- Implementing an explicit, up-datable and transparent Risk Assessments method:
  - to describe the physical world and portraying the results of interactions among its components, with linguistic clarity and suggesting clear direction of actions essential to resolve emergencies [13].
  - to determine optimum risk estimates fostering intelligent developments, abiding to the "science of complexity" as it enlarges the domain of demonstrable results in the service of humanity and is actionable [12].

3.2 Transparency starts with proper system definition and includes interdependencies

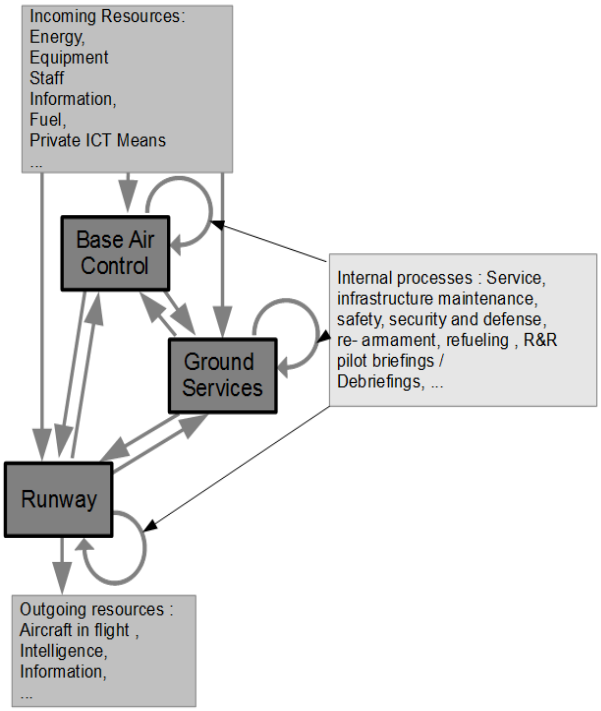

Fig. 2 An example of secondary nodes drawn from a Air Force Base analysis. Just three secondary nodes are displayed. All interdependencies among the three secondary nodes are displayed. "Internal loops" generate the same set of internal processes and resources.

Any civil or military system, consists of nodes (Fig. 1) which receive, process or transform, and produce resources. The nodes are generally interdependent, as we shall see later in detail.

The system's architecture must be carefully studied by people who intimately know the system. The risk assessment expert can only support as he does not know the structure's intricacies. However, he/she may, in specific cases help the customer solve and simplify the model to reflect reality while remaining as simple as possible. The study begins by defining all the types of primary nodes. Then, the secondary ones are defined (Fig. 2) and so on, depending on the required level of detail. This procedure can be repeated to the local, micro levels, knowing that it could go even further: nano, pico, etc. In a preliminary phase the definition will probably stop at secondary level. The scalability of the model will thereafter allow to zoom in one or other of the nodes (or all) to set details depending on the needs.

The system description is completed when the incoming resources, produced, processed, transported and the outgoing ones are listed in each node. In this phase it will be necessary to use engineering good sense and modeling tact in order to prepare lists compatible with the level of detail required by the customer and not to paralyze the work. The scalability of the system will eventually allow refining the descriptions.
The definition of the source of the resources and client-nodes allows processing in a reasonable manner the system's interdependencies (internal-external). Interdependencies between nodes (of given levels) have to be processed in a simple, but effective way, in order to avoid a "paralysis by analysis".

4 AVOIDING PARALYSIS BY ANALYSIS

In the last fifteen years there have been significant, but sometimes difficult to spot changes in the RM arena. Here is a "partial" list:

Tolerance/acceptability/appetite have mostly turned into buzzwords, rarely towards scientific approaches: ISO 31000 and many corporations/governments/authors "talk" about tolerance, but do not discuss how to develop it in "real" life. We have developed rational models, proven and calibrated

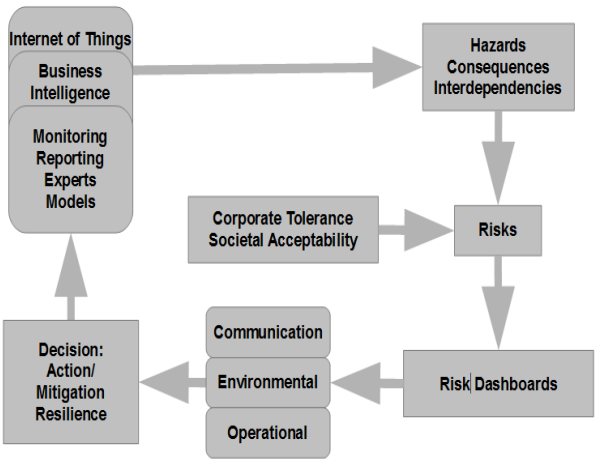

Fig. 3 Communicating risks, addressing the laws of complexity and satisfying the five roles of system science with ORE [12] [13].

them over hundreds of real life case studies. In our courses we teach the principles and we have an application that allows us to build a tolerance threshold for any company, any project, no matter the size. Instead of "crossing arms" in front of an apparently arduous problem, practical solutions are available, avoiding paralysis or the need to adopt misleading, oversimplified solutions. The importance of focusing on the architecture of the hazard/risk register, to avoid double counting, to provide detailed understanding of the risk landscape of any corporate/project has emerged. The architecture of the risk register is part of the know-how

that has enabled us to develop Optimum Risk Estimates (ORE), our flagship product (Fig. 3). We deploy ORE for all our clients who require a 360-view, deep understanding of their risk environment. With ORE deployment they get a focused mitigation road-map and acquire a distinct competitive edge over their competitors. In our courses we teach the principles of this architecture which, again avoids paralysis or the need to adopt misleading, oversimplified solutions.

In the last decade or so it has become obvious that common practice risk assessment systematically underestimate the consequences of potential mishaps. In our courses we explain how holistic consequences can be evaluated and included in a risk assessment avoiding the "paralysis by analysis" syndrome or the need to adopt misleading, oversimplified solutions.

We have become more and more involved into clearly and rationally defining all the terms we use, for lack of clarity and confusion have shown to be the source of horrendous corporate overspending. Terms like "strategic", "manageable/ unmanageable", "credible" etc. are now clearly defined and correspond to concrete and reproducible situations.

Due to the stronger influence of emerging risks, climate changes we have introduced a strong focus on Force Majeure, as these clauses, present in all commercial contracts actually do represent a significant risk to all involved parties.

4.1 Looking to the minimal survival criterion of the systems involved and clear social and organizational tolerance criteria.

In our papers [7] [8] we tackled the problem posed by poorly structured and poorly communicated risk assessments. Although the papers appeared in mining conferences, the discussions apply to any industry, worldwide, and, of course, cyber-risks. We focused the attention on misleading and fuzzy commonly used risk assessments methods, lack of communication and conflict of interest and attempted to explain why we, humans, keep merrily using ill-conceived methods. One key point of confusion is the expected minimal survival criterion, or what can be corporately and socially tolerated in term of holistic losses. Corporate tolerance and societal tolerance are very different and should not be confused. We have tested and proven the concept and published papers on the subject [9] [10]. A 2013 landmark decision by the Mackenzie Valley Review Board in Canada on the Giant Mine Environmental Remediation defined, in its Appendix D, what a Risk Assessment that would be societally acceptable should include. That "checklist" encompasses the evaluation of holistic risks in a clear and rational, transparent way, their comparison to a societally agreed tolerance threshold and many other points that common practice approaches are disregarding. It is heart warming to see that corporations around the world are developing strong social awareness and are following the path of CSR. We foster the concept of ORE (Optimum Risk Estimates) where the adjective "optimum" is there to show that whatever we do, we have to strive towards reasonable and sustainable systems, where the desire to protect and be protected is properly balanced with the desire to expand, make a good living, in full respect of all the stakeholders' interests. ORE is presently being deployed for alternative selection (Risk Based Decision Making) related to complex logistic of hazardous substances by railroad and trucking. We do not see why the same concepts would not apply to cyber risks, and actually have successfully proposed ORE for a country wide military cyber-defense approach (Fig. 4).

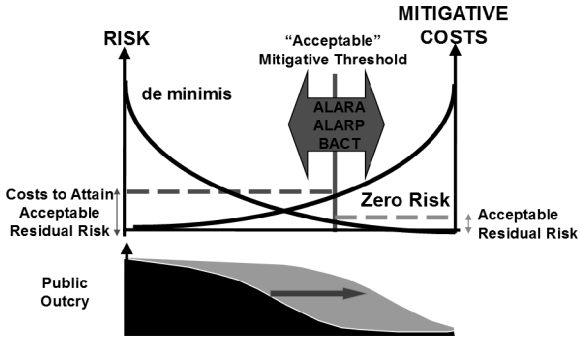

Fig. 4 A risk-reduction vs. mitigative investment plot. Generally agreed mitigation level (ALARA, etc.) are more stringent than the "theoretical technical optimum". Public pressure/outcry keeps pushing further out the gap between rational and perceived levels of desirable mitigation.

In the referenced papers we also discussed social acceptability of risk, risk estimates and risk communication in view of new projects world-wide and difficult choices humanity will have to make under demographic and climatic pressure. For the sake of simplification we have often considered consequences only in terms of casualties; risks linked to various industries were compared to well known, previously published acceptability criteria and codes. A comparison of the acceptability of these risks was then carried out from a quantitative risk evaluation point of view. In order to develop the discussion, the concepts of social perception quantification, which could be applied to any accident, in any industry, while developing a holistic risk assessment was illustrated. The perception gap between societally perceived consequences and factual consequences was explored, as it is a significant source of the pervasive mistrust in technical and scientific opinions. We then showed that the selection of the type of consequences and their combination can severely bias the perception of the results of a classic risk assessment application. A communication strategy was suggested to convey to clients the correct message when dealing with "societal" consequences of private industry risks.

Of course we also discussed monetary losses and showed the shape of common tolerance thresholds. The concepts developed for human losses appear to be applicable to physical losses. The functional link between tolerance and manageable vs. unmanageable risks was exposed and then analyzed to describe how governance and leadership can be damaged without proper risk evaluations, prioritization and a deep understanding of tolerance. In a recent paper [10], we showed that the selection of the type of consequences and their combination can severely bias the perception of the results of a classic risk assessment application. The functional link between tolerance and manageable vs. unmanageable risks is exposed and then analyzed to describe how governance and effective leadership are enhanced by proper risk evaluations, prioritization and a deep understanding of tolerance.

For years we have been fostering "good and rational" approaches which include, but are not limited to:

- reasonable and auditable estimates of probabilities,
- proper definition of social and economic tolerance/ acceptability,
- the development of rational prioritization allowing defensible decision making.

4.2 Giving cues on what should be included in the consequences function in order to depict reality as well as we can.

Performing risk assessments that exclude some particular type of consequences (we heard that environmental consequences were excluded from the analyses in some proposed methodologies!) and then saying this assessment can be used to make decisions is another blatant case of biasing and censoring.

However, common practice FMEA starts with an event, a failure, due to an hazard, but it does not require a detailed identification of all the possible hazards (like HAZOP) . Subsequently it evaluates failures' effects, often following simplified methodologies as described below. FMEA does not explicitly require a detailed understanding/modeling of the systems' functional relationships. No wonder that then we tend to easily invoke complexity and poorly understood interdependencies. In FMEA a failure probability can only be estimated or reduced by understanding its mechanism. Therefore if the system is not well understood or an inexperienced reviewer starts the exercise, it is very likely that some failure mode will be left-out. FMEA is generally blind to inter-dependencies unless a specific effort is made to include cascading events (domino effects). FMEA generally give a false sense of precision and simplicity of risk matters to their users.

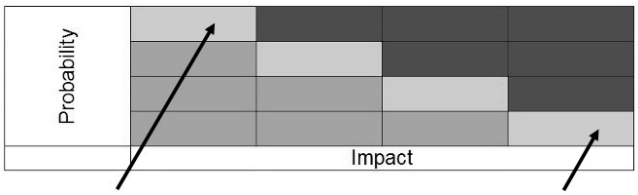

Fig. 5 Within this framework Fukushima disaster would be lowest class of probabilities, highest consequences, certainly not a significant risk!...(left arrow). ...same class of risk as the CEO getting a seasonal flu: Highly probable, very low consequences!

As detailed consequences' analysis is generally not part of common practice FMEA, the risk is not properly evaluated (oftentimes underestimated). It is common for example, when applying FMEA, to see teams selecting the worst among financial, human, or environmental category of consequences and forgetting their possible combinations. Results are often displayed as Probability Impact Graphs (PIGs) where matrix cells coloring gives a sense for risk criticality. PIGs are fraught by many problems and similar failures events, in term of probabilities, can oftentimes be prioritized similarly even thus their risk could vary significantly (Fig. 5).

5 CONCLUSIONS

Preparing a solid cyber-defense approach is a new necessity for many commercial or administrative entities. Many of those don't know how to tackle the problem and some invest significant amounts of resources to gain a perceived comfort, without first attempting to understand their holistic risk landscape. This comfort vs. reality gap becomes particularly blatant once it is recognized that antivirus softwares only catch 45% of cyber-attacks—a truly abysmal rate [3].

Other use misleading Risk Assessments methods which are not suited for this type of application and are known to present many flaws. Taking the risk of sounding "boring", we can quote Albert Einstein saying "We cannot solve our problems with the same thinking we used when we created them." However, as demonstrated in the paper, as past thinking was generally clouded by significant misconceptions, their correction will help to find solutions.

If the great body of experience and science developed over the last couple decades is skillfully and correctly integrated, by generalizing ideas and processes that have been working and proven, we can effectively solve the conundrum posed by cyber-defense risk management. The problem posed in not a "new" problem, but and old one that has already been solved in other arenas: what does change is that the technology and the speed of development is different and it is time to correct chronic risk misconceptions, bad habits and normalization of deviance, as there is no "old-normal" state, but a "new-normal" one. Thomas D'Agostino, head of the U.S. National Nuclear Security Administration, has stated that "nuclear labs are under constant attack receiving up to 10 million security significant cyber security events each day."

REFERENCES

[1] Appleby, M., Forlin, G., et al. **The Law Relating to Emergencies and Disasters. Tolley's Handbook of Disaster and Emergency Management: Principles and Practice**. R. Lakha and T. Moore, Butterworth-Heinemann, ISBN 0-406-97270-2, 2003

[2] Bobrov, O., Fake Applications: Why mobile users can't judge a book by its cover. **Social Engineering Ep. 2** Lacoon, April 22, 2014 http://tinyurl.com/ofs4g5z

[3] Eddy, M., Symantec Says Antivirus Is Dead, World Rolls Eyes, **Pcmag**, May 07, 2014 http://tinyurl.com/p2zfy6b

[4] Europol, May 19th, 2014, http://tinyurl.com/lagdzkw

[5] Gross, G., **Computerworld**, April 7th, 2015 http://tinyurl.com/njullhb

[6] HP Security Research, **Cyber Risk Report 2015**, 2015

[7] Oboni, F., Oboni, C., Zabolotniuk, S., Can We Stop Misrepresenting Reality to the Public?, **CIM** 2013, Toronto

[8] Oboni, F., Oboni, C., Is it true that PIGs fly when evaluating risks of tailings management systems? Short Course and paper, **Tailings and Mine Waste '12**, 2012, Keystone Colorado

[9] Oboni, C., Oboni F., Factual and Foreseeable Reliability of Tailings Dams and Nuclear Reactors -a Societal Acceptability Perspective, **Tailings and Mine Waste 2013**, Banff, AB , November 6 to 9, 2013

[10] Oboni,C., Oboni. F, Aspects of Risk Tolerability, Manageable vs. Unmanageable Risks in Relation to Governance and Effective Leadership, **International Symposium on Business and Management**, Nagoya, Aichi-ken, Japan, April 2014

[11] Tor Security Advisory: "Relay early" traffic confirmation attack, **torproject.org**, July 30th, 2014 http://tinyurl.com/kyymdqn

[12] Warfield, J. N. Understanding Complexity: Thought and Behavior. **AJAR Publishing Company**, Palm Harbor, Florida, isbn 0-971-6962-0-9, 2002

[13] Warfield, J. N. A Proposal for Systems Science. **Systems Research and Behavioral Science**, 2003, 20(6): 507-520.

[14] Yadron, D., Symantec Develops New Attack on Cyberhacking, **The Wall Street Journal**, May 4, 2014 http://tinyurl.com/puksfdb