IT Security Management – Time for a Paradigm Shift

Frank W. Holliday, on the 1st of November 2017

The goal to live on the base of a safe information technology is becoming with the growing complexity (diversity/multifaceted/multilayered) and dynamics of our IT landscapes and the increasing importance of information technology for the organization and processes of our life (see buzzword: digital society) for our modern and complex civilization visibly a question of survival. Current approaches of IT security management that are based on the traditional IT risk management show in practice significant shortfalls. The more and more successful zero-day attacks illustrate this evil tremendously. The increasing number of crises ('surprises') despite intensive risk management and intensive modeling e.g., in the financial sector shows we have with our current approaches only limited success.

Why is that?

Risk handling (also called risk management) is dealing with uncertainty. At least we want to be prepared for surprises of the future. According our current physical understanding of the world, the world is built on the foundation of quantum physics, which shows the future of this world is by a natural law not exactly predictable (non-deterministic), or in other words substantially random. Nevertheless, we try to estimate risks by the usage of models and thus to be better prepared for the future. Common procedure for doing so in the information security risk management is to capture as comprehensive as possible in scenarios hazards and threats to security (in the case of threats we have to look further for existing vulnerabilities) and try to determine the need of protection for our vulnerable assets. Usually the potential for damage is calculated as a product of the factors vulnerability, financial impact and likelihood of occurrence for each scenario. The resultant damage potential tableau for all the scenarios is then a reasonable fundament for a smart determination of appropriate countermeasures.

But is that just enough?

Firstly, the success of this procedure is highly dependent on a significant amount of identified scenarios. Due the given efforts for this game we can't play it arbitrarily. But the choice of the sense and termination criteria for this game provokes shattering effects [1] (e.g., see the disaster of the Fukushima nuclear reactors in 2011: tidal waves more than 30 feet height were simply no longer considered in the scenarios catalog because of the assessment that this is a four-centuries-event and can be judged as negligible. The highest measured tidal wave in the coastal area was 69 feet!). Secondly, because of our relatively young field of IT security knowledge we have no reliable frequency ratio of certain security incidents, which is also caused by the concealment of incidents due to the fear of a potential reputation loss. On third, it leads to the phenomenon of being self-perpetuating as this kind of procedure is strongly rewarded for obtaining any certification, which induces the danger of losing its correspondence to reality. Last but not least, security is not a fixed state due to the fact of technological dynamics and the unforeseen. Security must be a continuous improvement process necessarily. As the world changes continuously we need to run this game for sure cyclically. Thus we have the great inherent risk that we rely solely on our 'modeled future' because of the big efforts having been invested.

What is to do?

A similar challenge we have when we look on the topic health. The phenomenon of health can be approached by just looking on possible disease. All possible cases of disease are researched. Therapies are developed and are more and more applied by economic considerations. But the phenomenon health can be seen by the perspective of 'being healthy' (salutogenesis) also. Now the gained knowledge is quite different. Totally other categories are brought into focus. Topics such as robustness, the ability to withstand to stresses, and more specifically, the resilience, the ability to absorb shocks and disturbances preserving the vitality for the future come up to the fore front.

What does this mean being transferred to our challenge of IT security management?

There must be a fundamental change how to view on our systems. Only resilient or in the refined world of concepts named even better as anti-fragile [2] information technology systems with a guaranteed high resilience or high levels of anti-fragility have earned the confidence to deal substantially with the random future.

What do these systems distinguish from others?

Let us have a look on nature first. A large meta-process does exist in the nature, the evolution. All phenomena of nature from category 'living things' on seem to have to go with this process. What does the evolution characterize? Two design principles (key drivers): variation and selection. The one mechanism produces diversity, the other mechanism ensures that only these variations having been created can continue to exist in generations further on, which have proven the future (having been adaptable enough to survive), what 'naturally' means a highly interactive process is happening. Very interesting is that this highly interactive process generates very cooperative subsystems of the system nature, cause not just a simple 'survival of the fittest' in the sense of domination is the key driver, but maximizing symbiotic relationships among the existing species is the real key! Now you can understand why viruses and bacteria are still on the nature's scene, because of their strong diversity capabilities in combination with their strong dependence of an on-going living host.

What are the key drivers of resilient systems?

Surprisingly there are also two main drivers. At first there is the ability of a system to mitigate the adverse consequences of changes and utilize the advantage of the changes (the system ability to learn). Secondly there is a coping capacity, a capacity of existing system resources and skills enabling to mitigate and cope with damaging events (the system reserve for conservation). Just the lack of the latter driver is often responsible that 'efficient systems' do not guarantee long-term success, they are downright trimmed, woe betide, if they are sick or no longer fit to the environmental conditions. Do you see the clue? To learn more about resilience we have to be more multi-disciplinary with the evolution biologists.

IT Security Management – Time for a Paradigm Shift

What does an anti-fragile system distinguish from other systems?

It is a distinctive specialty in the ability of the system to learn, which goes far beyond the unhurried adaptation speed of evolution. Namely by self-organizing accelerated learning (no more variations of generations away) out of carried loads on robustness the design of the system is adopted (a self-learning adaptable system – a prototype for this kind of system is the human being).

If we are able to derive for the security of information technology systems a scale for the system resilience or at top a scale for the system property *anti-fragility*, we have completely new opportunities how to handle risks. Information technology systems are highly modeled artifacts and as such they can at least be simulated. Thanks to our developed computing possibilities, we could allow only such kinds of information technology systems, which have demonstrated either in extensive, fast and large numbered evolutionary test runs a minimum level of system resilience or even better do possess a measured certain level of system anti-fragility as a system property. This would be a completely new approach for a certification of safe information technology systems.

A very interesting approach in this direction is the EU-funded project 'CyberWiz', which is a part of the European Union Research and Innovation Programme 'Horizon 2020', targeting to enhance the security of critical infrastructures [3]. This is done by enabling to model a given cyber security system in a specification and then measuring its cyber security maturity as a statistical value on the base of the scale 'Time To Compromise' (TTC) by probing the specified model with large numbers of attack samples utilizing a Monte Carlo method. Thus enables to gain lessons learned on cybersecurity just by simulation!

Nowadays on pure software base we are ready to design networks and their structures by the SDN technology or to virtualize them by network virtualization, computers can be virtualized even longer by the VM technology, modern AI technology starting with 'Deep Learning' is enabling us to construct self-learning adapting systems. All these steps together can build up an orchestration to enhance the resilience of information systems just by simulation through probing with large numbers of samples and improving the resilience of these systems evolutionary. So we aren't far away to establish a new area of safe information technology systems.

But is anti-fragility all of it?

IT Security Management – Time for a Paradigm Shift

In addition to the property principle *anti-fragility* of information technology systems we importantly have to watch on the *design principles, manufacturing and appliance* of information technology systems. Now is the time to bring up on the scene 'Secure by Design'. The supreme guideline should be to prevent that security is only a retrofitted 'component' instead it has to be from the beginning on an outbound recognized aspect of the development requirements and the manufacturing process based on safety objectives or needs. What is some kind of interesting is that some of these principles were already identified in 1975 by Jerome H. Saltzer & Michael D. Schroeder in their publication 'The Protection of Information in Computer Systems' [4]. They proposed eight design principles for making safe information technology systems:

- simplicity of protections (Economy of Mechanisms)
- minimum authorization requirements (Failsafe Defaults)
- complete authentication (Complete Mediation)
- open, held not secret design (Open Design)
- usage of a 4-eyes principle (Separation of Privilege)
- alignment of the rights to the minimum (Least Privilege)
- alignment of joint mechanisms at the minimum (Least Common Mechanism)
- being geared to the psychological acceptance (Psychological Acceptability).

Well, that was anyhow in the year 1975. In the meantime additional construction principles among others can be enlisted:

- utilization of an as much as possible automated (quick alert!) detection of anomalies (Intrusion Detection System / IDS)
- utilization of an as much as possible automated (quick response!) defense against discovered attacks (Intrusion Prevention System/ IPS)
- utilization of defense layers using a communicative stack in depth (enabling possible communications between the defense layers about strange behavior resulting through AI driven expert systems in a quick, more holistic interception see e.g., Sophos *infinity loop*)
- identity-based & use-oriented information technology systems (keeping in mind that a doubtless identification is the root of a lot security issues!)
- utilization of a multi-factor authentication (improving the protection against identity theft or abuse distinctly!)
- setting the situational lowest possible authorization (reducing violation level!)
- utilization of a role-based authorization concept (reducing complexity by design!)
- utilization of secure design patterns (reusability of security proven designs!)
- Open Trusted Computing (OTC) (enabling a trustworthy computing base!)
- or even the implementation of a communication security attributed relationships concept, which is better known under the naming 'Jericho Concept' [5] (according the wisdom: 'The Relationships between the objects are more important for the behavior of the system than the objects of the system itselves, stupid!').

To achieve a broad spread of these design principles we might think about enforced legal defined frameworks, which the manufacturers and applicators of information technology systems have to adhere.

IT Security Management – Time for a Paradigm Shift

A recent example of technology being 'Insecure by Design' is the smartphone. Only gradually manufacturers just begin to make this weapon of security mass destruction more secure from the root on (see starting this for instance in 2013 by the mobile operating system BlackBerry 10). The next level of technology still based on unsecure construction and systemic deficits shows up on the horizon: the Internet of Things (IoT) e.g., spreading massively in critical infrastructures by smart metering or in smart homes or in coming autonomous driving vehicles. Improving IoT security by a systemic approach is interestingly shown e.g., by VMware's *micro-segmentation* using the by the virtualization achieved additional abstraction layer as a central security monitor.

Do not misunderstand my comments. I don't say the classic IT risk management needs to be retired. This approach has a lot of benefits to prioritize measures reasonably just in terms of limited opportunities for safeguards and resources. But that approach has, what my statements above have showed off, systemically its limitations in terms of a sustainable success and it urgently needs to be supplemented by the orientation to evolutionary probation and mature design principles named to be a sustainable complementary resilience strategy (SCRS).

As so often in life, the mix makes all the difference;-)

References

1. Taleb Nassim Nicolas (2007) The Black Swan: The Impact of the Highly Improbable, Random House and Penguin, New York
2. Taleb Nassim Nicolas (2012) Antifragile. Things That Gain from Disorder, Random House, New York
3. EU-Horizon 2020-Project 'CyberWiz' https://cordis.europa.eu/news/rcn/131134_en.html
4. Saltzer JH, Schroeder MD (1975) http://www.cs.virginia.edu/~evans/cs551/saltzer/
5. TheOpenGroup Jericho Forum see at https://www2.opengroup.org/ogsys/catalog/W127 or see an application of this concept developed by Google: https://beyondcorp.com/

About the Author

Frank W. Holliday, CISSP & ISO/IEC 27001 Lead Auditor, has over 15 years of information security, IT audit and compliance experience. He is an IT veteran covering over 35 years of experience on a diversity of IT work fields like embedded systems programing, software product development, system administration, software quality management and finally has found his particular interest in information security. He holds a German master degree in communications engineering and is a member of the German Association of Computer Science (Gesellschaft für Informatik e.V./ GI). He is attached to the GI's workgroup SECMGT (Information Security Management) and also is taking part in the task force ISM of the German registered association TeleTrusT.