Digital innovation & Technological explosion
The new challenges of the Security Management

Franco Guidi,   Giancarlo Caroti

Neumus Srl

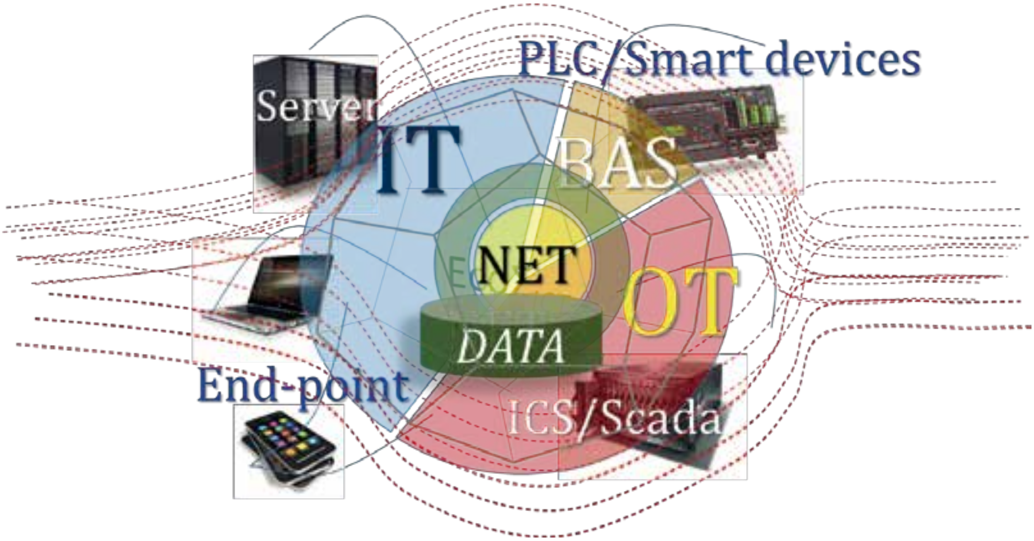
Florence, Italy

fguidi@inwind.it   giancarlocarots@gmail.com

Cyber Ecosystem always more complex

Digitization become deeply embedded in each strategy, as nearly all businesses and activities have been slated for digital transformations.

The technological revolution has the intensity of a tsunami: the traditional ICT systems move to complex digital ecosystems. Operational Technology (OT) such as industrial control systems and elements of smart grids such as smart meters, vehicles, and smart buildings are all examples of innovative enterprise.



Several new assumptions have to be made about the cyber environments, because of their evolution over the years:

- Modern networks are very large, very interconnected, and run both ubiquitous protocols and proprietary protocols. Therefore, they are often open to access, and a potential attacker can attach with relative ease, or remotely access, to such networks. Widespread IP internetworking increases the probability that more attacks will be carried out over large, heavily interconnected networks.

- Computing systems and applications attached to these networks are becoming increasingly complex. In terms of security, it becomes more difficult to analyze, secure, and properly test the security of the computer systems and applications; it is even more so when virtualization is involved. When these systems and their applications are integrated in large networks, the risk to computing dramatically increases.

Warning: «Cyber space» interacts with «Reality»

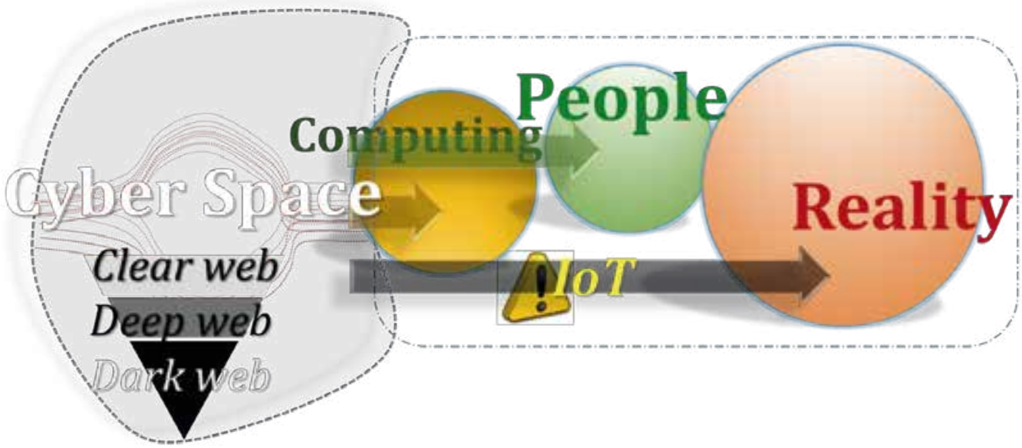
Smart devices, machine-to-machine (M2M) communications and cloud-based services, among many other technologies, are advancing the next-generation of networked societies.

Digital technology and internet connectivity, are being systematically integrated into all verticals of the private and public sectors, offering significant advantages like productivity, speed, cost-reduction and flexibility.

In the cyber environment it's increasing the role of the Cyber-Physical Systems (CPS), whic refer to the seamless integration of computation and networking with physical processes, possibly with humans in the loop.

In these systems, embedded computers and networks monitor (through sensors) and control (through actuators) the physical processes, usually with feedback loops where physical processes affect computations and vice versa.

A key point in these systems is the control of physical processes from the monitoring of variables and the use of computational intelligence to obtain a deep knowledge of the monitored environment, thus providing timely and more accurate decisions and actions.



The growing interconnection of physical and virtual worlds, and the development of increasingly sophisticated intelligence techniques, has opened the door to the next generation of CPS, referred to as "smart cyber-physical systems" (sCPS).

A new family of risk factor arises, however, from the possible short-circuit between the cyber space (and its cyber-threats) and the controlled real world, cutting off altogether people's intervention.

Trust challenges for the success of digital projects

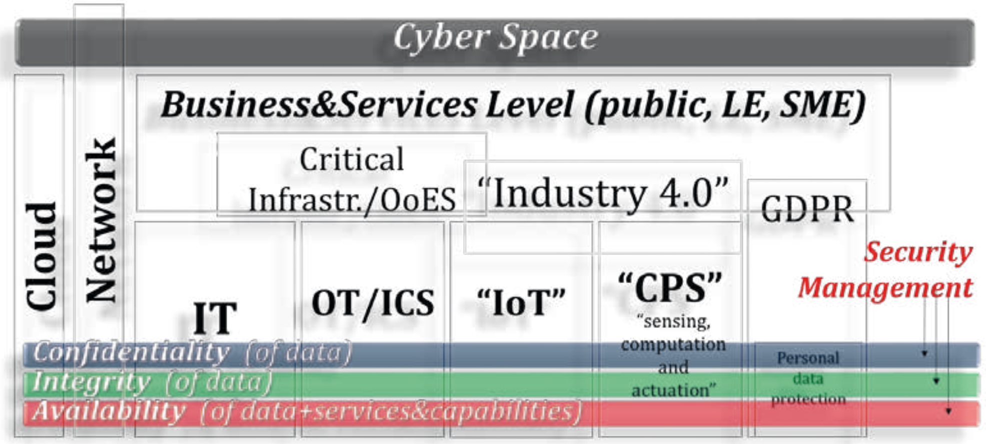
Establishing and maintaining a secure computing environment is obviously mandatory, but it's increasingly more difficult as networks become increasingly interconnected and data flows ever more freely.

In such scenario, one methodological approach calibrated and not generalist became unavoidable.

Security … Common issue!

Cybersecurity became an essential requirement when living in a digital world.

The number of data breaches and the level of cyber-attacks suffered by organizations around the world increases almost daily, making it imperative that every organization have an effective cybersecurity program in place.


Cyber Space
Business&Services Level (public, LE, SME)
Critical Infrastr./OoES
"Industry 4.0"
GDPR
Cloud
Network
IT
OT/ICS
"IoT"
"CPS"
"sensing, computation and actuation"
Security Management
Personal data protection
Confidentiality (of data)
Integrity (of data)
Availability (of data+services&capabilities)

The develop of one cyber&information security management strategy and the relative governance actions are now key topics for to ensure data protection, asset defence, system resilience and overall continuity and capabilities of business processes and services.

How to cope the digital risk in the digital era

As the global digital revolution takes hold and proliferates into our economies, societies and governments, the potential for information to be electronically tampered with and controlled is real.

Digital and technology risk is a term encompassing all digital enablements that improve risk effectiveness and efficiency—especially process automation, decision automation, and digitized monitoring and early warning.

In particular, small companies quickly moving to digitalization, often unwittingly open the door to attackers through a variety of unsecure practices. Small enterprise security policies that don't quell missteps such as employee downloads of unauthorized software, rogue Wi-Fi installations, and password sharing will actually promote such behaviors.

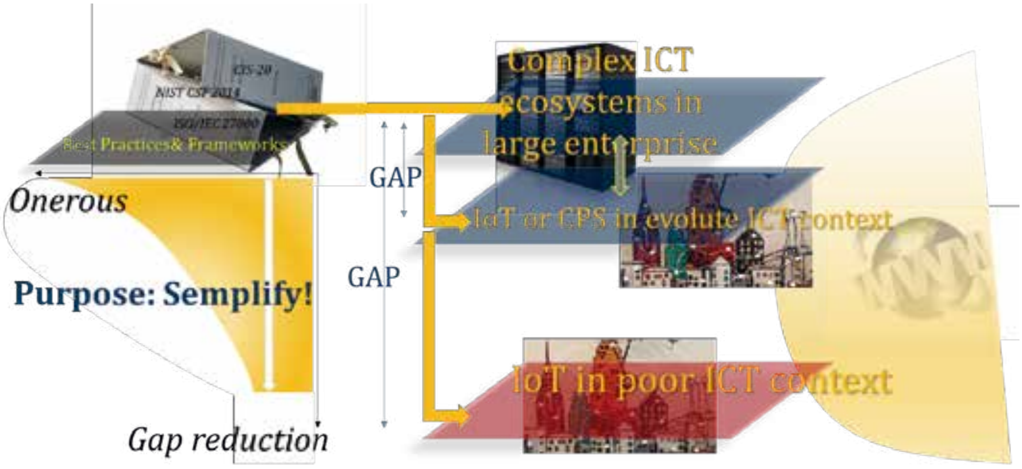
Therefore, already tested models of reference are necessary, but unfortunately these have very difficult management characteristics and heavy effort for the SME target.

To overcome the Adoption/Execution Gaps

The needs of protection for the large or small networks are essentially the same, but the framework for action must to be adjusted, to response to very different operational conditions.

For to determine the risk factors, the step is to perform a risk assessment on the organization's "cyber presence" in the ecosystem, by looking at information assets, interdependencies with other organizations, threats (including insider threats), vulnerabilities, cybersecurity controls, and security testing activities, including business continuity/disaster recovery and reconstruction capabilities.

This means examining those factors that affect the extent of the organization's control over its ecosystem and the means by which that control can be exercised.

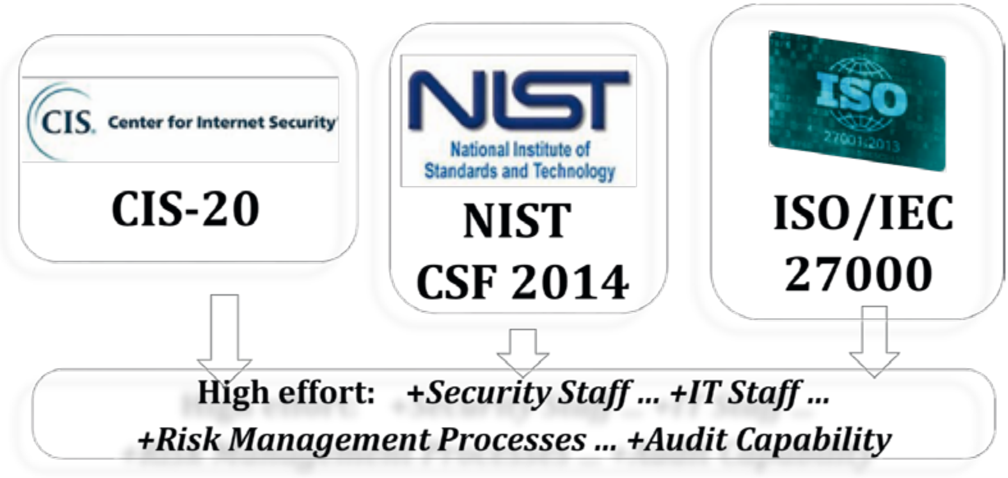


- The solution of using more famous structured models requires an unsustainable effort for small but very digitized organizations (for example, robotised SME), creating a very big "gap" for a practical application.

- Moreover, some good practices that can give an added-value to new digital projects, require intervention by the market players who operate upstream of the deployment and are therefore not governable by the customer. Many of the vulnerabilities in IoT/CPS devices could be mitigated through recognized security best practices, but too many products today do not incorporate even basic security measures; other contributing factors include a lack of incentives for developers to adequately secure products, since they do not necessarily bear the costs of failing to do so, and uneven awareness of how to evaluate the security features of competing options.

Best practices too much «expensive»

The most famous best practices and the most common standards (including certifiable schemes) need staff and resources almost always absent in small organizations.


CIS Center for Internet Security
CIS-20
NIST National Institute of Standards and Technology
NIST CSF 2014
ISO 27001:2013
ISO/IEC 27000
High effort: +Security Staff ... +IT Staff ...
+Risk Management Processes ... +Audit Capability

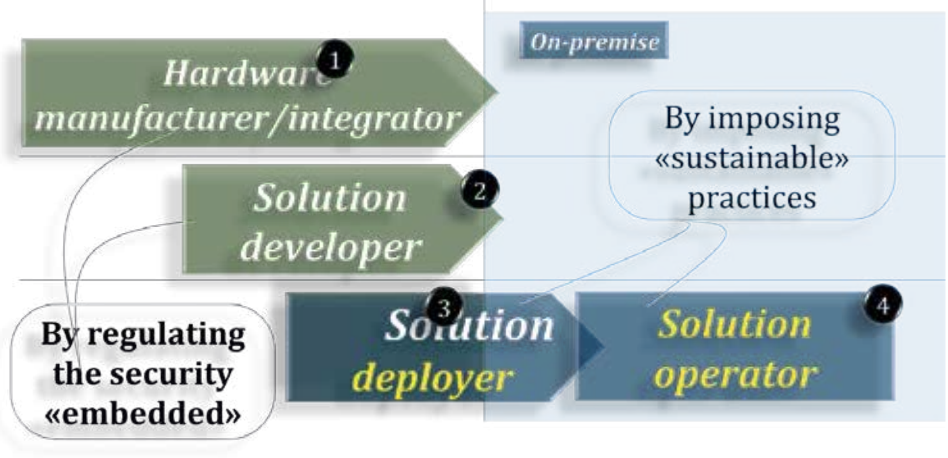
The perspectives …

- **Quick-win and simple and low-cost practices and techniques**
- **Act on overall "life cycle" of the innovative technologies**

In the light of all this, it is unavoidable it and almost mandatory to direct efforts, at the same time, towards two areas of action:

i) By working on the frameworks, for to implement "sustainable" practices and simplify the controls for implementation to technologies, people and business processes (and/or obtain them, effective and cheap, like managed services from specialized third parties, where advantageous and practicable) in less staffed companies.

ii) By introducing a regulatory schema, imposing a minimum common framework for all market players, to incorporate the baseline security controls from the beginning of the life of technological components and devices (security is to be evaluated as an integral component of any network-connected device). An active role is here hoped and expected from the national Authorities, for to create a contribution with security certification, at least for to be considered trustworthy those standalone certified devices (before integration in a real computing environment).


On-premise
Hardware manufacturer/integrator
1
By imposing «sustainable» practices
Solution developer
2
By regulating the security «embedded»
Solution deployer
3
Solution operator
4