# The faults of defaults

## Don’t let anyone else make your security choices


IFIP WG Meeting, Sorrento, 2014-01-24

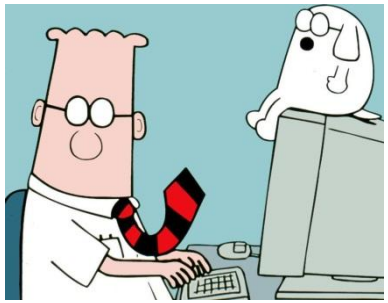
**Andrea Guarino**
**Head of Cyber Security**
**ACEA SpA – Rome**
**(www.acea.it)**

# A few words about myself:

- **More than 25+ years in ACEA,**
- **15+ years focused on ICT Security (since the Y2K bug)**
- **Previously Head of Architecture and Standard, Head of Information Security, Security Advisor**
- **Since 2013, Head of Cyber Security for the whole group**

**Technical interests:**

- **Ethical hacking, Penetration Testing, Reverse-Engineering code…**
- **I'm a Dilbert fan**

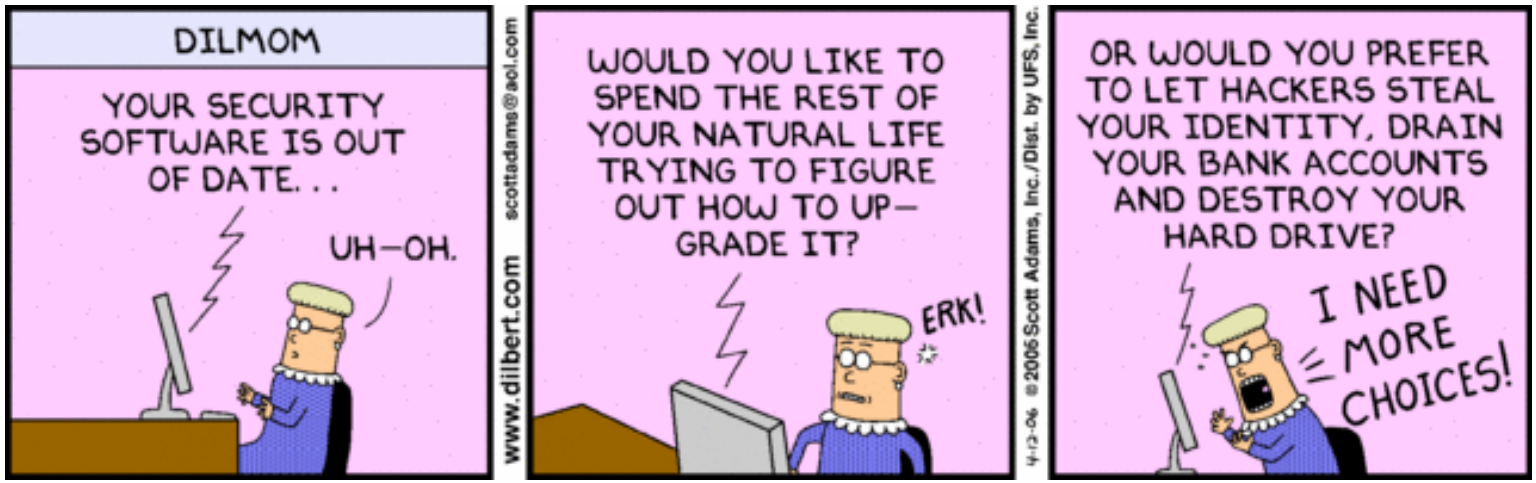


# Cyber Security in a Critical Infrastructure includes:

- All the conventional and widely known ICT issues, problems and incidents, plus…
- Interaction with field-operating appliances and elements with limited hw/sw capabilities (PLCs, RTUs,…)
- Interaction with non-ICT field-based personnel (technicians, local support,…)
- Interaction with providers (telecoms, energy dispatchers, ..)
- More regulations (local, industry sector, national, international)
- Severe penalties / high fines for outages and loss of service to the customer
- Frauds on the metering systems (smart grid is coming in Italy too!)
- Millions of assets and devices to update and/or support (cables, meters, power nodes, valves, pipelines, …)

# Cyber Security isn't just about «technical issues»

- You cannot solve it just usings «products» and «boxes»
- No endpoint protection available on some devices
- Shareholders request a ROI: you cannot spend enough to really protect anything, anywhere perfectly
- Sometimes you just cannot readily «update» a device, so you must cope with its vulnerabilities until you reach / change it: your organization and people must be aware and prepared for that.



# Cyber Security risks cannot be really avoided

- Devices in the field are obviously visible and exposed
- Meters are scattered in houses and customer premises too
- Using private networks isn't always possible
- Viable encryption is sometimes too complex to handle in real-time
- You cannot defend aggressively!

# … so you have to use a risk management strategy

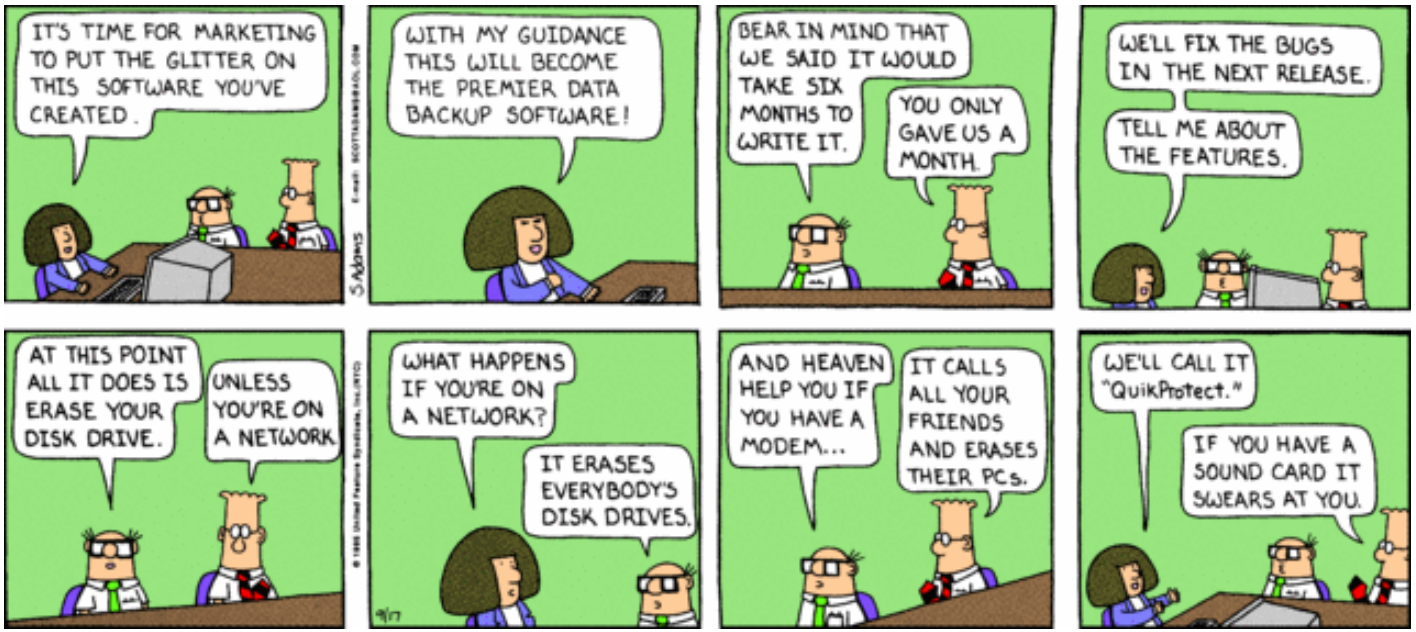
- Business areas must dictate their rules
- Security should write the corresponding policies and enforce them
- ICT and other interested technical areas should obey
- Proper description and evaluation of the risk (and their scores) is critical
- Don’t take anything for granted

# You may get lucky, or you may be not…

- Sometimes you will be asked to evaluate very special risks: like a «black swan» they’re extremely far in terms of chances to be seen
- …but they may be destructive!
- Italy had its «black swan» in 2003 when the power grid went down:

# … and since our «black swan» we learnt the lesson

- Very low probability isn't the same as impossible
- Emergency and crisis systems/assets/procs must be tested routinely
- Did you take into account cross-domain interdependencies?
- Mobile phones/radio batteries are always charged?
- Are you sure about your backups and restore TTR and capabilities?



# Risk management is tied to security assessments

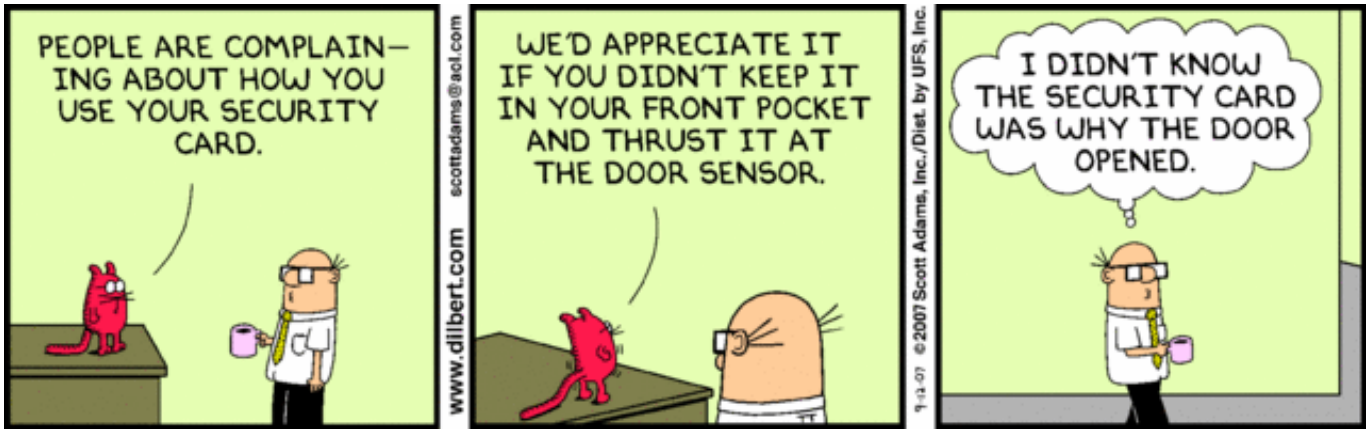
- How do you handle a security assessment of a smart meter?
- Which KPI will you choose?
- How many of them?
- Too much info is equal to having none or worse if you're not able to filter out what you really need
- We experienced that the «quick wins» aren't the best choices for us
- You need to think long-term (5-10 years, depending on assets)

# Things get so complex you cannot experiment?

- When new pieces get introduced in your architecture, vendors just say «leave them at the default configuration»
- Doing this particularly with security products is not efficient!
- Try to ask what that «heuristic» parameter stands for
- Be careful when evaluating things like «maximum bandwidth» performances: they may depend on the ruleset (actual configuration) you're using and may even change during testing
- Don't overdo in production environments without testing!

# So, you'll need a full-featured testing plant?

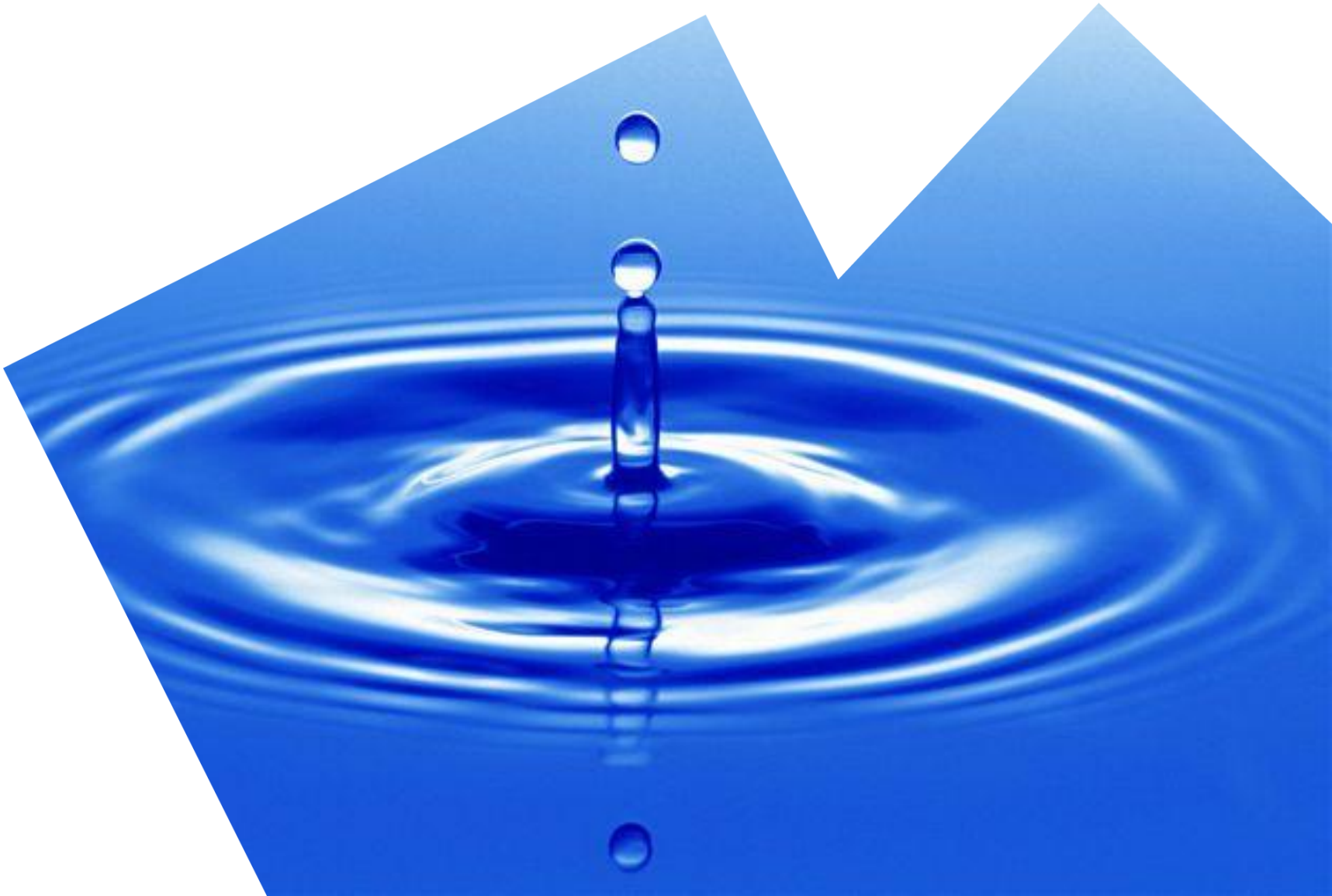
- Staged updates are enough. Just don't forget to extend them to all machines in a timely manner (decided with Operations in mind)
- Updating through Internet (like Android OTA) may seems a good idea, but you will have to expose your network somehow to do it
- Better prepare some off-line container for updating and patching most critical systems (example: www.wsusoffline.net )
- Always use write-protected removable storage when doing software or firmware updates (remember Stuxnet, DuQU, Flame, etc.)



# … but you will discover this isn't enough

- Once-a-time monthly assessments don't give you the real picture
- Time required to scan all devices is too long
- Better using passive techniques to understand the security posture of devices using configuration and network traffic data
- Sometimes human reaction times are too slow to defend
- Humans take minutes/hours to study an anomaly and decide what to do (or what to undo)

# We had to find a new way…



# PANOPTESEC

SEVENTH FRAMEWORK PROGRAMME

## A state-of-the-art prototype offering "Dynamic Risk Approaches for Automated Cyber Defence"

Prevent, detect, manage and react to cyber incidents

Support breach notifications and improve cyber situation awareness

Support cyber operator decision-making processes

Operate in enterprise and critical infrastructure environments

## Proactive methods to

Analyze vulnerabilities and attack paths

Conduct mission impact analysis

Recommend priority mitigations that minimize mission impact

## Reactive methods to

Detect incidents that may target mission critical resources

Recommend priority mitigations in real-time

Support automated response