Free ICT Europe
Aftermarket Alliance for Freedom
to Support, Repair and Resell

WannaCry ? Time has come so dry your tears and act!

The unprecedented ransomware attack[1] that started on 12th May was wholly predictable and a wakeup up call of reality to a sleepwalking world.

Everyone seems to have a view on the attack with traditional media and social media being red hot with comments and finger pointing; according to Microsoft it's all the fault of the NSA[2]. In today's world this is to be expected but it is only through serious investigation that the truth will be uncovered and this is the role of the authorities, supported by experts. We can all only hope they succeed in their endeavours.

We must resist the temptation of naivety. Our industry is renowned for its ability in providing innovation and making possible today what was only a dream yesterday but that ability brings with it the paradox that has been with us since the first computer was designed; the products which are launched on the market, either hardware of software, are vulnerable. No manufacturer of IT products can pretend their systems are without a hole or a door that ill-intentioned and very determined individuals or organisations can enter to either steal our identities, to spy on our private lives or to kill our businesses. It is a very reasonable paranoia to declare that WannaCry is just a taste of our future and a clarion call of what is to come.

There are many on-going debates around the world with purpose of setting up rules, providing guidance and introducing policies to deal with the threat so we can be prepared. For example in the US one debate is clearly described in a report under the title "Law Enforcement Using and Disclosing Technology Vulnerabilities"[3]. The questions raised in this report can be condensed as, should we make public a vulnerability to which there is no associated fix and how should we organize and reward the community of "good guys" that detect the vulnerabilities and fix them before hackers exploit them? Those who read the report will be disturbed to discover that security agencies are playing on 2 boards of the same game by exploiting for their own needs the vulnerabilities. This is the real world we are living in and we will not change it by simply trying to wish it away. We have to face the facts and be cognisant of reality.

Contained within the report is a detail which is of most interest for our secondary market industry. On Page 2 is a short but clear definition in a grey box under the title Relevant Terms. Vulnerability is defined as "**a security hole or weakness in hardware, software, or firmware that can leave it open to becoming compromised**." Previous attempts at defining vulnerabilities have never been as clear. Reviewing the "Common and Vulnerabilities Exposures" (CVE) web site[4] we can read : "**A "vulnerability" is a weakness in the computational logic (eg. code) found in software and some hardware components (eg. firmware)…**". We are glad that the definition provided in the report takes us one step further than the CVE definition with the clear distinction between hardware, firmware and software being independently potential sources of vulnerability that require discreet fixes. This definition reflects the point of view of Free ICT Europe despite the many debates and attempts by OEMs and Software Companies to make it confusing.

For our precious secondary market to move forward and be a part of a secure future the lessons to be learned are easy to summarise:

[1] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[2] https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.0000b0jp3ebltdsdrs71bju2qbfb1

[3] https://www.hsdl.org/?abstract&did=800768
[4] https://cve.mitre.org/about/terminology.html

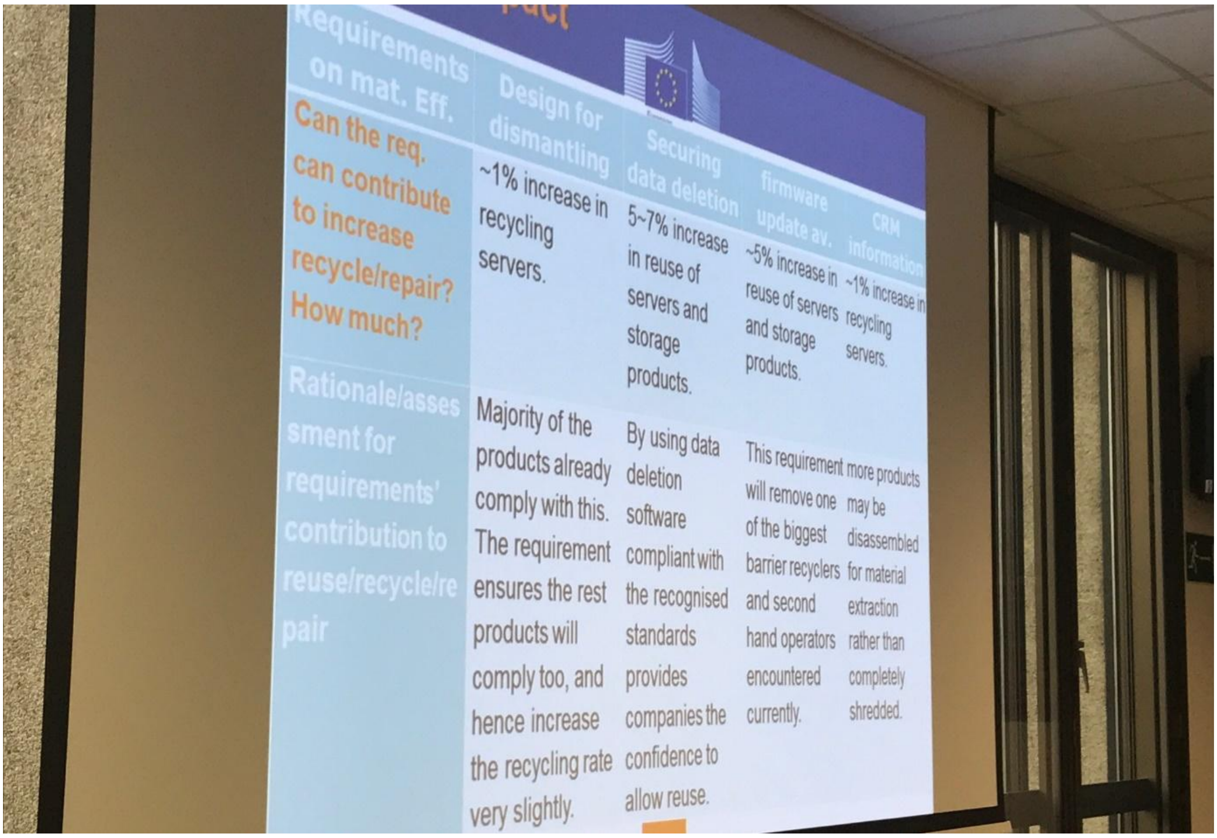
- Firmware & Software updates that fix vulnerabilities should be applied on a regular routine basis and in emergency when an attack in imminent or in progress
- If it is a customer responsibility to keep their infrastructure up to date and protect them with all technological means, independent services providers should advise customers of serious threats which are in the scope of the commitments of their services agreements
- **OEMs and Software Companies should make available without charge, unfettered and in an expeditious way all vulnerability fixes, without the precondition of a service agreement and allow independent providers to act on the behalf of their customers**

The last point in the list is one of the main positions we defend at Free ICT Europe. We have tirelessly campaigned to raise the awareness of the stakeholders and are heavily involved in the legislative agenda of the European Commission.

In discussions with the new initiative of Directive for Ecodesign[5], we have successfully introduced the obligation on an OEM to provide firmware updates in to their project. This is just a first step but we will not giving anything away.

To enable us to reach the goals that will benefit us all your support is more than precious and we are thankful for your contributions. The very future of our industry is in our collective hands.

Don't give up, be part of the solution and join us. We need you, you need us, we all need each other.



Requirements on mat. Eff.	Design for dismantling	Securing data deletion	firmware update av.	CRM information
Can the req. can contribute to increase recycle/repair? How much?	~1% increase in recycling servers.	5~7% increase in reuse of servers and storage products.	~5% increase in reuse of servers and storage products.	~1% increase in recycling servers.
Rationale/assessment for requirements' contribution to reuse/recycle/repair	Majority of the products already comply with this. The requirement ensures the rest products will comply too, and hence increase the recycling rate very slightly.	By using data deletion software compliant with the recognised standards provides companies the confidence to allow reuse.	This requirement will remove one of the biggest barrier recyclers and second hand operators encountered currently.	more products may be disassembled for material extraction rather than completely shredded.

[5] https://bookshop.europa.eu/en/ecodesign-technical-assistance-study-on-standards-for-lot-9-enterprise-servers-and-enterprise-data-storage-pbET0216987/?CatalogCategoryID=2QcKABstE4IAAAEjwJAY4e5L