NIST CSF v2.0
A contribution from a cyber-security researcher, entrepreneur in Mexico

Which corrective cyber-security control do you know about that is more effective when applied regularly as a preventive control? Hints: It is considered in the NIST CSF v1.1. It applies to IoT, OT, IT, and networking devices. It enables a zero-trust architecture to achieve system integrity.

Perhaps you guessed it right: **system restoration**. It is currently considered as a corrective cyber-security control by the **NIST CSF v1.1**, **Recover** function, **Recovery Planning** category, **RC.RP-1** sub-category.

The following paragraphs, however, briefly elaborate on our learning. It is more effective to convert system restoration into a preventive cyber-security control within the **Protect** function, **Protective Technology** category, **PR.PT-5** sub-category. This is possible thanks to techniques that allow a technician or cyber-security practitioner to complete preventive system restoration much faster than its corrective counterpart.

Why system restoration?

Cyber-security and IT operations communities trust system restoration as the best way to recover system integrity. It eradicates undetected malware and fixes altered configurations. We base our learning on almost 24 years of developing software hygiene techniques and more than 150,000 hours of tests on real-life computers. Thus, we conclude that system restoration is more effective when regularly applied *in-vitam* before a cyber-attack concludes.

The traditional way is to conduct a *post-mortem* system restoration. After responsive procedures have taken place and the organization is already under the painful effects of an unstoppable cyber-attack. System restoration includes hard disk reformatting and software reinstallation, which comprises firmware, drivers, and updates. When necessary, configuration and data backup take place to prevent loss and later restore those elements.

Why change an obsolete paradigm?

A knowledgeable technician completed a system restoration in 12-16 hours in the year 2000. Today, using disk cloning tools and cloud storage, the time to finish such a process has been reduced to 1-2 hours. However, as a time-consuming and cumbersome process, system restoration has always been considered *post-mortem*.

We propose to change that paradigm by (i) drastically reducing the time it takes to complete the process and (ii) limiting losses on configurations and data. Our best time is less than 9 seconds with no data loss and controlled impact on system configurations.

For the upcoming CSF v2.0, we invite the NIST team to consider pointing cyber-security practitioners towards the implementation of regular preventive system restoration enhanced by software hygiene techniques due to the following reasons:

1. **It is time to evolve the digital immune system architecture (DISA) design in all computing devices.** Evidence shows that today's one-layered approach does not detect that which is unknown. An evolved DISA design provides a two-layered digital immune system, like the one in vertebrate organisms that evolved after millions of years. Preventive system restorations enhanced with software hygiene techniques provide a digital immune system with the missing additional layer to regularly destroy the unknown by using brute force, not detection. Nature knows better, but humans must evolve themselves the digital immune system in computing devices.
2. **Preventive system restoration enhanced by software hygiene techniques enables zero-trust system integrity.** It does not depend on detection. It is quick. Repeatable. Non-destructive for data and configurations. Affordable to digital device owners. Achievable by technicians, not only experienced, certified cyber-security practitioners.
3. **Computing devices that quickly recover system integrity send a compelling message to cyber-adversaries.** Suppose that an enemy infects a digital device. But if a preventive system restoration occurs one, two, or three times a day, the window of opportunity for invaders is less than practical. Thus, intruders will move away to choose other targets.

We can foresee financial benefits for the organization that implements preventive system restoration enhanced by software hygiene techniques. Reducing the impact of materialized risks and lowering cyber-insurance fees, for instance. However, we are unable to state such benefits with precision at this point.

Vendor-neutral and technology-agnostic

We understand that the NIST CSF v2.0 aims to be vendor-neutral and technology-agnostic. In our experiments, we achieved the above by employing interchangeable tools. We aim NOT TO base our software hygiene technologies on one specific configuration or tool set. We also aim to become vendor-neutral and technology-agnostic in our implementations.

Contact me should you wish to see a demonstration. I have a clear mission to prevent billions of people from becoming victims of cyber-attacks, whether as individuals owning digital devices, as digital users serviced by companies, or as digital citizens served by governments.

Yours truly,

Manuel Fernando Mejías Butrón

Kreissontech 21, Founder
GSB Solutions, Innovation Manager

LinkedIn. https://mx.linkedin.com/pub/manuel-mejías/a/77b/995/en
E-mail. m.mejias@infinitummail.com and manuel.mejias@gsb.lat