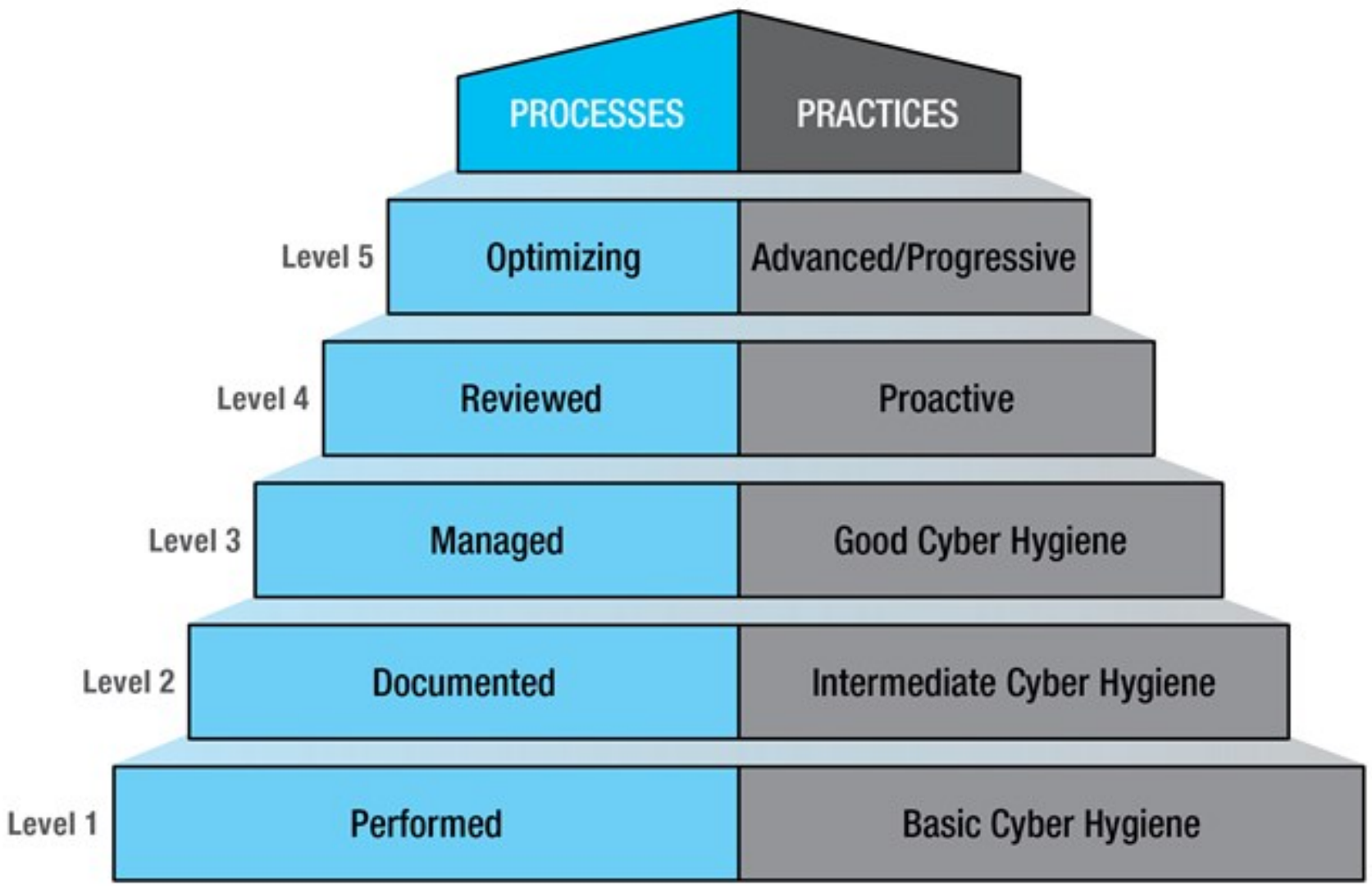
5/31/2021 | 4 MINUTE READ

Cybersecurity Process Maturity Demands a Plan

Plans may fail, but planning has intrinsic value for building sustainable, adaptable data defenses.
#datamatters

Good generals are good planners. On a strategic level, they see each unit as a cog in a greater machine that must be continually primed to respond to any move an adversary might make. Now, this thinking is spreading throughout the defense industry supply chain with new contract language that, for a manufacturer, sends a clear message: You are a cog in this machine, too, and national security demands that you think similarly about cybersecurity. If planning for every contingency demands as much of your resources as producing defect-free parts, then that is a necessary cost of preventing sabotage, theft or other malicious manipulation of data that puts lives and livelihoods at risk.

In fact, insufficient cybersecurity can be just as disqualifying as insufficient quality control under the new standard: The Cybersecurity Maturity Model Certification (CMMC). Although the specific definition of "maturity" differs from contract to contract under this five-level system, retired Army officer and cybersecurity specialist Aaron West says the basic idea is to institutionalize best practices — that is, to ensure that data defenses are sustainable and adaptable as threats evolve.



A shop demonstrating Level 3 practice maturity — "good" cyber hygiene — has implemented all of the practices required by previous Federal Acquisition Regulation (FAR) and National Institute for Standards and Technology (NIST) standards, as well as various other protections required for the first time under CMMC. However, Level 3 process maturity requires that practices be "managed," and that requires a proven, actionable plan. Image: Department of Defense (DoD).

With government audits looming and CMMC language already appearing in some contract proposals, defense-oriented manufacturers are already at work. One example is Olson Custom Designs (OCD), a CNC machine shop that has been working closely on CMMC compliance with Reveal Risk, the cybersecurity consulting firm where West is CMMC practice lead. By the time I reached out to OCD for an article, the shop already had implemented two thirds of the specific practices required to meet CMMC Level 3 (for example, tools and systems for backing up and delineating access to data). However, "checking boxes" is not enough for CMMC, West says. The new

certification also measures the maturity of the processes behind the practices. As a result, most of the work so far has been as much about documenting existing policies and procedures as implementing the rest of the list of Level 3 protections. “A lot of the results achieved in CMMC at OCD thus far have been because of the time and effort put into the System Security Plan,” he says (the SSP is essentially an overview of a shop’s security controls and procedures).

In fact, implementing and documenting all practices required for Level 3 will still leave the shop at only Level 2 in terms of its process maturity (and thus, Level 2 overall). Level 3 process maturity requires a cybersecurity system to be not only “documented,” but also “managed.” In essence, this means not just making plans, but also proving that plans can be executed. As an example, West cites response strategies for when a threat becomes real. “So, for Incident Response, maybe you have a plan, but have you tested it?” he asks. “Did you conduct a ‘wargame,’ and can you show us what was learned? When was the plan last updated? For Security Awareness, how often are you training, and what means and methods are you using to stay up-to-date? These are all indicators of a full program.”

Incident Response and Security Awareness are just two of 17 different capability domains evaluated for CMMC certification. To achieve Level 3, shops must prove that every domain is backed by a documented, managed process. Planning these processes requires setting specific goals; dedicating the necessary resources and materials; probing for weak points; and otherwise preparing for every possible contingency, not unlike a battlefield general would.

A good general understands that no plan is perfect. History is replete with examples of dynamic, quick-thinking battle commanders stepping in when plans go awry. The case is the same for a good shop leader, who must seize opportunities to invest, diversify and improve while avoiding missteps. However, good generals and good shop leaders tend to be good planners anyway, because they understand that the value of planning is intrinsic.

A plan provides a framework for action even in the face of the unknown, not unlike how machining automation can be configured to accommodate a range of novel part geometries. Just as a general might anticipate the need to protect the flank of an advancing troop column, a shop leader designs quality control processes around preventing what is mostly likely to go wrong. The strongest framework holds firm even amid unexpected change — maybe the other flank is the one that needs protecting, or a shop’s most experienced machinist unexpectedly quits. Analogies aside, the point is the act of planning helps institutionalize patterns of activity that can help ensure any process is sustainable and adaptable enough to be called “mature.”

Former U.S. president and general Dwight D. Eisenhower explained it best, West says. “(Eisenhower) had a pretty good quote where he said, ‘Plans are nothing, but planning is everything.’ He saw that in the many the plans he wrote during World War II, things always changed after the plan was written. So, the value wasn’t so much in the piece of paper as all the integration and synchronization that went into its development.”