5/21/2021 | 9 MINUTE READ

Cybersecurity Becomes a CNC Machining Prerequisite

Management software and information technology partner services prove their worth
amid the rollout of defense industry requirements.

Some CNC machine shop leaders have had an education in Bitcoin digital currency, but for the wrong reason: They have been forced to pay ransom online for sensitive data that had essentially been held hostage by hackers.

An anecdote about one of these incidents was shared with me by Olson Custom Designs, a shop specializing in defense-industry contracts. Although the company's own data security has never been compromised (at least not to anyone's knowledge), it has heeded the lessons of incidents experienced first-hand by team members at their past employers. The ransomware story is just one example.

That incident happened nearly a decade ago, and the threat has evolved significantly since then. National security now demands that defense contractors like Olson comply with a new set of requirements: namely, the Cybersecurity Maturity Model Certification (CMMC). CMMC builds largely on the DFARS (Defense Federal Acquisition Regulation Supplement) and incorporates much of the pre-existing NIST (National Institute for Standard and Technology) 800-171 cybersecurity requirements. However, CMMC is different from previous cybersecurity standards in that self-reporting compliance is no longer enough. Rather, certification by third-party auditors will be a pre-condition for quoting work.

> The challenge for a small or mid-sized machine shop is that none of this is free.

At the time of this writing, these supply chain audits have yet to be conducted, and various questions about CMMC remain unanswered. Nonetheless, Chris Jaynes, operations manager, is confident in the team's ability to address the challenges ahead. Securing data is just one aspect of managing data, and this relatively new company has made significant strides in managing data effectively.

These strides have been possible in part because Olson Custom Designs is a business born without preconceived notions about how to start a machine shop. Digitalized data, digitalized workflows and all the necessary software and information technology infrastructure are part of this facility's original infrastructure. Leadership understood from the beginning that capability to effectively manage (and maintain the security of) data is essential not just for meeting new requirements, but also for competing for Department of Defense (DoD) contracts in the first place. As Jaynes puts it, "It's not just about how well you can make the part. It's about how well you can prove how well you made the part."

Eyes on the Prize

The "Olson" in Olson Custom Designs refers to Mitch and Brian Olson, brothers who founded the Indianapolis shop in 2014. Beginning in a rented, 5,000-square-foot space, the Olsons had always intended to move on from their roots in auto racing. They also recognized that their chosen niche of work — carving castings and other defense and aerospace industry parts from high-nickel alloys on five-axis machining centers — requires more than just the right technology and technique. "You've got to have a handle on data," Jaynes says.
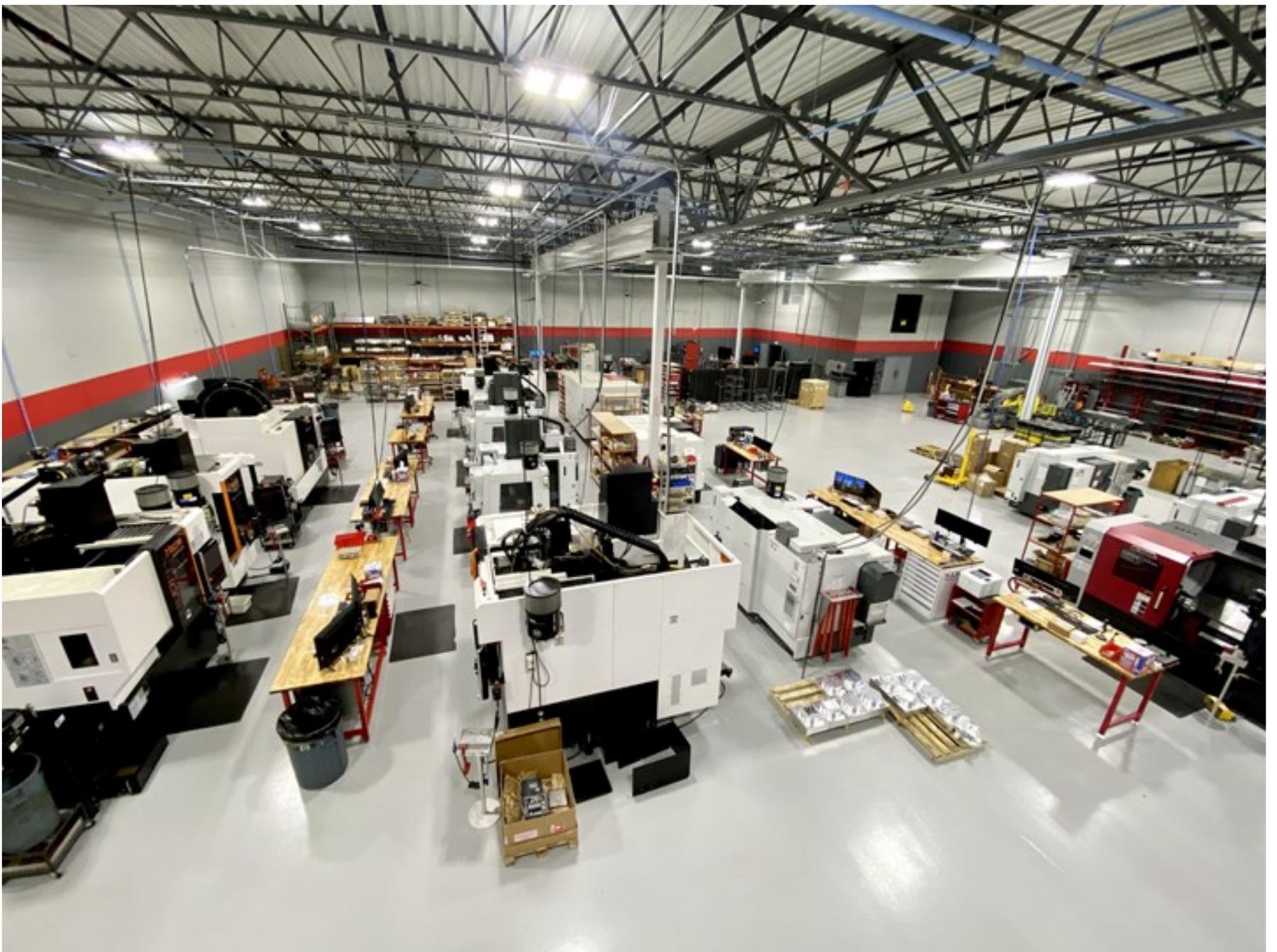
With computers at every workstation and digitalized workflows, shop leadership considers the services of its in-house MSP to be essential. Photo Credit: Olson Custom Designs

Jaynes had managed larger machine shops before the Olson brothers hired him in 2017 as the company's fourth employee. Based on that experience, his first order of business was investigating enterprise resource planning (ERP) software. "We knew we'd have to start right then because we'd need it down the road," he says. "If you wait until you grow to 10 to 15 people, then you have this ingrained culture of 'but that's the way we've always done it.' That makes things more difficult."

By February 2018, the newly wired-up shop was managing its operations with Proshop ERP. The Olson brothers also had decided that they finally had the right people, the right infrastructure, and enough work to compete for defense-industry contracts. During the course of the next year, they purchased a new 24,000-square-foot facility, expanded the staff to 35 employees and obtained the necessary quality certifications. "We added a large amount of overhead in a short amount of time," Mitch Olson recalls.

Maintaining sufficient cash flow to fuel growth has been essential. Proshop helps make the machining business scalable by facilitating a largely paperless workflow, which customers and prospective customers tend to notice, Jaynes says. From the moment a request for quote (RFQ) is entered into the ERP system, all digital documentation associated with a job remains associated with that job, from purchase orders and material certifications to quality documents and data associated with providers of heat-treat, plating and other outside services. Quality management procedures are "embedded in the system," and any information an ISO or AS9100 auditor might request is generally within a few clicks away, he says. "From a chain of evidence standpoint, there's never any question about what we've done."

ERP Shepherds CMMC

Establishing a clear chain of evidence will be similarly important for meeting new DoD cybersecurity requirements, Jaynes says. Reports indicate that CMMC audit teams could begin visiting defense contractors as early as this fall. In addition to specific practices, they will evaluate the processes used to implement and

enforce those practices across 17 different "capability domains" (categories such as "asset management" and "incident response"). "It's all about demonstrating how practices are tied to processes to ensure they are sustained going forward," he explains.

CMMC evaluates both processes and specific practices. Which level must be met as a pre-condition of doing business depends on the nature of the information requiring protection, which includes federal contract information (FCI) and controlled unclassified information (CUI). Image Credit: Department of Defense

Jaynes is confident that the shop will be able to meet CMMC Level 2 (which denotes "intermediate" cyber hygiene) by the end of the year. Level 2 practices cover all relevant Federal Acquisition Regulation (FAR) requirements (which must be implemented for Level 1, or "basic cyber hygiene," certification), as well as a large portion of the controls from the previous, self-assessed NIST standard. Examples include multi-factor authentication (that is, requiring more than just a password or other single key to access sensitive systems); implementing a "least privilege" access model that restricts personnel to only the data required for their jobs (for instance, shopfloor machinists have no need for purchase orders or other contractual information); and protection against on-site risks (such as the malicious use of USB sticks or even the accidental installation of malware).

Proshop ERP offers CMMC-specific functionality to help guide machine shops through compliance.
Photo Credit: Proshop USA

All of these practices were already in place by the time the shop began to focus specifically on CMMC. So, most of the work so far has focused on documenting what the shop was already doing as part of Level 2's process requirements. The ERP system offers CMMC-specific tools, including "work orders" that guide staff through checking off requirements in the same way that shop-floor work orders guide them through machining parts. Working with the various templates, checklists, explanations of requirements and other resources embedded in the software reminds Jaynes of the shop's earlier efforts to attain ISO and AS9100 certification. "There was a lot of 'Oh, we do that, we just don't document it,'" he says. "So far, I'm seeing a lot of the same with the CMMC."

This annotated Proshop ERP screenshot (a work order) depicts the use of hyperlinks to connect all data associated with a job. Photo Credit: Proshop USA

Although ERP is a critical tool, Proshop emphasizes that its system's CMMC functionality is not meant to handhold, but rather to provide a template for shops to develop individualized cybersecurity policies. Recognizing this, and still facing unanswered questions, the Olson brothers have no intention of pushing the company toward compliance by its own efforts alone. Two partners help shoulder the burden.

Experts Required

By the time CMMC language starts appearing in requests for quotes, Olson Custom Designs must reach level 3, Jaynes says. Level 3 ("good" cyber hygiene) covers 130 different cybersecurity practices (including all of NIST 800-171, plus 20 more), compared to 72 for level 2 and 17 for level 1. On the process side, level 3 requires not only performing (level 1) and documenting (level 2) all required practices, but also managing them. Essentially, this means outlining the specifics of who does what; the nature of any required training, tools and other resources; progress toward important milestones; and other evidence to show auditors precisely how internal processes contribute to meeting CMMC requirements.

To help, the shop has hired Reveal Risk, a consulting group that is helping write policies and procedures in preparation for an eventual CMMC audit. Teams of Reveal Risk personnel have regularly visited the shop to consult about potential threats and response strategies. Much of this work is hands-on, involving not only consulting but also drills to test various cybersecurity measures. "Their team is particularly sharp at conducting tabletops — or as they refer to it, 'wargaming' — to think through security problems and the optimal solutions," Jaynes says.

The challenge for a small or mid-sized machine shop is that none of this is free. That includes time spent offline preparing for meetings, lining up training, purchasing software and protections, and otherwise making good on the partner's recommendations. Not unlike quality certification requirements, preparing for CMMC is simply a

cost of doing business in an increasingly exclusive sector of manufacturing. "Every minute I spend on CMMC costs money," Jaynes says.

CAM programmers use high-end computers with better graphics cards and other high-end features. Photo Credit: Olson Custom Designs

One advantage for Olson Custom Designs is a special relationship with the second partner: Teknabyte, the managed service provider (MSP) that set up the company's IT infrastructure. When the company moved into its current facility, the MSP came along, too, renting a portion of unused office space. Close proximity fosters the kind of close relationships, speedy response and professional service that would otherwise be possible only with dedicated, in-house IT personnel. In addition to troubleshooting more than 40 computers when something goes wrong (including more powerful models for CAM programmers), MSP services include upgrading and installing workstations, software and networking infrastructure; onboarding new employees (and removing departing ones); and myriad other irregular but essential tasks. "Most companies our size can't afford to have the proper IT people on staff," Jaynes says.

Boldly Forward

At the time of this writing, Jaynes and the rest of the team at Olson Custom Designs have many unanswered questions about CMMC. The most pressing examples include precise timetables for audits and the appearance of CMMC language in RFQs; the extent to which new regulations will apply to contracts retroactively; the extent of compliance required for providers of outside finishing services and other subcontractors; and, perhaps most importantly of all, how everyone is going to pay for all of this as the costs associated with CMMC compliance filter through the supply chain.

> "It's not just about how well you can make the part. It's about how well you can prove how well you made the part." – Chris Jaynes

Whatever the answers to these questions, shops like Olson Custom Designs are pressing boldly forward. By starting off right — that is, with a clear plan of action and without preconceived notions about how to run a machine shop — this company laid an ideal foundation for ramping up quickly into a sector with increasingly burdensome barriers to entry. Moving forward, this team is likely to apply the same vision in pursuing increasingly exclusive machining opportunities.