Donna Ruginski

Executive Director Cybersecurity Initiatives

University of Maryland Baltimore County

Standing in the way between cybercriminals and a rapidly digitizing manufacturing industry is Donna Ruginski, the Executive Director for Cybersecurity Initiatives at the University of Maryland, Baltimore County (UMBC). She's involved with both to help the manufacturing industry find the right cybersecurity talent, and to sound the alarm about dangers that lurk over the horizon, or even within company walls.

She and UMBC colleagues Dr. Nilanjan Banergee, Professor of computer science and electrical engineering, and Dr. Keith Bowman, Dean of the College of Engineering and Information Technology, partnered with MxD because they see a labor shortage nationally and internationally in the cybersecurity workforce, especially in manufacturing. "I believe that this program for improving cybersecurity in operational manufacturing technology (CyMOT) will create a learning platform that can be done synchronously or asynchronously for professionals in manufacturing," Ruginski said. "Existing employees may need to take on new responsibilities, or they may want to move into a new role within their company that has a cybersecurity focus."

She believes that in the near future, federal compliance requirements will make every manufacturer in the U.S. take cyber attacks seriously, regardless of size. According to Ruginski, small- to medium-sized manufacturers are easy targets for cybercriminals.

"Small- and medium-sized manufacturers don't have departments focused on cybersecurity like large manufacturers do," she explained. "But these smaller entities still are dealing with the same challenges and have to be able to address them in order to stay competitive."

She hopes that manufacturers are concerned enough by the frequent stories about hacking in the news to take action. If the U.S. government can be hacked, then a little-known manufacturer in the Midwest can also be hacked. Companies cannot afford to think that it cannot happen to them. "This brings to bear research that's required to enable manufacturers to operate even under attack, so that they don't have to shut down operations completely, but can continue to operate in some form."

CyMOT's unique cybersecurity for manufacturing training is a pilot program at MxD, and is funded by the Department of Defense. The plan is to use the feedback from manufacturers in this first phase to refine the course. "Our goal is to create a full, comprehensive curriculum that mirrors the MxD hiring guide," she said. "What's unique about this partnership is we have engaged an academic institution, the University of Maryland, Baltimore County, a leader in cybersecurity education; we also have UMBC Training Centers, who are experts in workforce development programs in cybersecurity; and we have MxD, who are experts in manufacturing and cybersecurity."

Of all the cyber threats that worry Ruginski, none is more troubling than ransomware. She fears that it is only a matter of time before a large manufacturer gets hacked through no fault of their own. Threats happen quickly, using stealth tactics, and are evolving. Without the new technology, the countermeasures, and the application of best practices, manufacturers are vulnerable.

“The ransomware threat that we face, because we’re inundated with emails daily, can so easily lead to a bad event happening,” warned Ruginski. “You have to be really on your toes about what you’re looking at, what you’re opening, and not becoming a victim, if you haven’t become one already.”