The University of Kentucky is building a joint cybersecurity task force focused on defending the University from cyber-attacks, responding to incidents, ensuring appropriate management of threat intelligence, forensics, and emerging cybersecurity issues.

Recent cyber-attacks on healthcare organizations in the state of Kentucky underscore the need to have greater capacity in gathering threat intelligence. In a cybersecurity event, quick, proactive action must be taken in terms of countermeasures that will mitigate harm.

To that end, the task force will collaborate with law enforcement, federal agencies, Information Sharing and Analysis Centers (ISACs), and peer institutions to gather and share threat intelligence, coordinate the implementation of best practices, and increase cybersecurity awareness in our community.

The University of Kentucky conducts much of this work already, collaborating with the FBI, CISA, and REN-ISAC on threat intelligence, vulnerability scanning, and tabletop exercises.

This task force, though, will enhance and focus these efforts, fund dedicated positions, and allocate physical space for the task force to collaborate.

The creation of the task force also aligns with UK's educational mission. Students have been incorporated into our security operations, actively participating in cybersecurity activities such as incident management and vulnerability management. These initiatives are providing valuable experience to the students and supporting the development of the future cybersecurity workforce – a critical and growing sector of the economy.

While our initial efforts focus solely on protecting the University and its health care organization, in the future we will explore partnerships with other universities, public/private partnerships, and increasing our scope to provide services to other state and local agencies. We will also consider pursuing grant funding to support and expand the task force.