

Central Ohio Cybersecurity Initiative



Franklin County Emergency Management and Homeland Security (FCEM&HS) is serving as the lead agency for the development of a regional public/private sector Cybersecurity Work Group. The work group will consist of decision makers from the public and private sectors throughout Central Ohio and provide an additional benefit for Franklin County as it will strengthen coordination and cooperation.

According to the largest online daily news publication Homeland Security Newswire (August 2014) “Cyberattacks loom as an increasingly dire threat to privacy, national security, and the global economy, and the **best way to blunt their impact may be a public-private partnership between government and business.** The time to act is now, however, rather than in the wake of a crisis, says an expert in law and technology.” According to Jay Kesan Law Professor at University of Illinois “Information-sharing framework is necessary to combat cybersecurity threats.”

What is Cyberterrorism?

Cyberterrorism uses various means to exploit system vulnerabilities in compromising a particular computer, a software application, an IT network, or military and critical infrastructure command and control systems. Individuals or groups may intentionally target a specific cyber asset or indiscriminately attack a broad range of assets using a virus, worm, or malware distributed over the Internet

What is Cybersecurity?

Cybersecurity is measures taken to protect information systems and data against unauthorized access or an attack against information systems which sustain modern society. Financial institutions, manufacturing, utilities, healthcare, research & development, transportation, critical infrastructure and emergency response and homeland security agencies are some public and private organizations vulnerable to cyber threats.

Why is Cybersecurity Collaboration Important for Central Ohio?

Cybersecurity involves the Homeland Security Enterprise (HSE), the “whole community”. It is a shared responsibility amongst the public and private sectors involving partnerships encompassing emergency management, law enforcement, public health, local/state/federal government, private sector, nongovernmental organizations, faith-based & community-based organizations, and the public. “Improving cybersecurity and ensuring the resilience of systems will require cooperation between members of the private sector and the government.”

Although Cybersecurity has been the purview of the Federal Government and large corporations, we must build efforts at the local level which embrace the cybersecurity challenges, tap local resources for education and awareness, protect critical infrastructure, key resources and businesses as well as help communities safeguard their citizens from cyber-attacks.