To whom it may concern:

I think that there is still a perception that a general cybersecurity specialist exists that can adequately take care of an organization's total data security concerns. This usually falls in the lap of an organization's network administrator.

We might be better served in bridging the workforce gap, especially in larger organizations, if we started to think of the cybersecurity workforce in the same way that we have come to see the healthcare workforce. Rather than having one staffer with a master's degree in computer science, or a network administrator with an umbrella cybersecurity certification, perhaps the cyber workforce should be broken down into specialties (penetration testing, ethical hacking, intrusion detection, etc.) where people are trained in time periods of 12-24 months to perform specific complementary cybersecurity functions.

Most of all, the training of all computer users in the recognition of phishing, and general malware avoidance needs to be addressed outside of the domain of IT education. Social engineering and bad decision making by unaware users is key to the success of any cybersecurity strategy. Training needs to begin in k-12 schools, and continue on through college and be integrated into *ongoing* practice in enterprises of all types.

John Hamerlinck
Rural Information Technology Alliance, Grant Manager
Central Lakes College
501 W College Drive
Brainerd, MN 56401
jhamerlinck@clcmn.edu