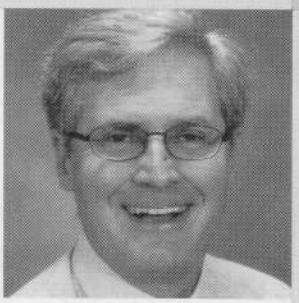

A Higher Standard of Due Care

DURING THE LAST SEVERAL YEARS, I HAVE NOTICED CERTIFIED public accounting (CPA) firms harvesting specialized technology credentials. It is not uncommon for CPAs and other professionals at these firms to possess Certified Information Systems Security Professional or Certified Information Systems Auditor credentials for performing assessment, assurance, and attestation services in cyber-security and other technology-related areas. Addressing today's technology risks, however, requires expertise and extensive training, beyond just certification. Professionals who provide technology or other specialized attestation need to possess appropriate, expert-level qualifications — especially where the risks can be truly catastrophic.

In the United States, the standard of "due care" has risen dramatically since events such as the Sept. 11 attacks, the collapse of Enron, and the Iraq war. Greater consequences from risk events have led to increased control requirements and, subsequently, a higher standard of what truly constitutes due care. Cyber-security, bio-terrorism, and other threats have raised "proficiency" and "assurance" thresholds as well.

Regulatory authorities — such as the U.S. Department of Homeland Security and the Securities and Exchange Commission — are also raising the standard. The Sarbanes-Oxley Act of 2002 and Federal Information Security Management Act, for example, demand much higher levels of organizational vigilance and professional attestation. In light of the elevated regulatory climate, as well as increased nonregulatory threats, professionals who conduct work outside their areas of expertise can expose the organization to significant harm and even subject themselves to litigation risk.

To meet today's due care standards, organizations need to ensure that those who perform attestation work possess the right level of expertise. To address heightened cyber-security and other technology-related threats, for example, those performing IT and security assessments should ideally possess a software engineering degree or comparable background. Similarly, a bio-terrorism assessment should be conducted by a biologist with a doctorate-level foundation of expertise. Generally, technical or other highly specialized assessments should be handled by an expert with appropriate academic training and a professional license in the area under review.

CIO magazine forewarns, "In 2010, information security will be much better than it is today. But between then and now, everything will get inconceivably worse." Despite this and other signs of increasing security challenges, one training firm currently offers to provide a cyber-security certificate in just seven days. Can individuals who obtain this type of certification truly provide the requisite "due diligence" and "due care" in areas where they are not degreed or licensed?

Superficial training and token credentials hardly seem adequate for the threats facing today's organizations. It is not sufficient to merely comply with established laws and requirements or give cursory treatment to risk areas. The security and overall health of the organization demand a much higher standard.

To comment on this article, e-mail the author at ghutchins@theiia.org
The opinions expressed are solely those of the author.