Insuring Cybersecurity as an Organizational and Quality Challenge:

U.S. and Japan Compared

A common belief among those assigned to protecting organizations is that the key to cybersecurity can be found in technology solutions, led by cybersecurity experts. A closer analysis of the everyday challenges facing those working to protect organizations, however, reveals that cybersecurity is, above all, an organizational challenge. Moreover, it is a challenge which like the quality challenges, must be met by all employees and departments, participating in identifying risks and developing solutions.

We can view successful cyberattacks as cases of quality failure on the part of host organizations. By contrast, quality success, applied to this domain, involves keeping an organization's digital system free from malign influences and maintaining safe processes..

In addition, if an organization's digital system has been penetrated, is that organization then able to detect that intrusion? If so, can that organization isolate and then eliminate the attack? Moreover, are these capabilities purely technological or are organizational/quality capabilities required. Detecting and responding to process abnormalities is key. That of course, has been a central capability of the quality discipline. One can also observe dangerous tradeoffs being made between exploitation (managers focusing on short-term efficiency gains) and quality (insuring for the long term, safe processes).

Both Japan and the U.S. have strong but different potential assets for insuring cybersecurity. We will explore these possibilities while suggesting new career paths for quality professionals in an era of disruptive technology.

Robert E Cole, UC Berkeley.