Baldrige and Cybersecurity

by Tony Scott

> “Baldrige helped transform many industries, and the practices and processes that were developed and institutionalized are now the norm across many industries.”

In my role as the Federal Chief Information Officer for the U.S. Government during the last two years of the Obama Administration, I became acutely aware of the risks associated with poor cybersecurity practices in many federal government agencies. For example, after only a few weeks on the job, I learned of the massive data breach at the Office of Personnel Management (OPM), which at the time was one of the largest incidents in history. The investigation of, and the subsequent response to, this breach became a major focus for me and my team in the ensuing months.

Among the many things that we learned from our work on the OPM incident and our examination of broader government-wide practices was that in many cases, agencies lacked the proper funding to do the required work, didn’t have the right people with the right skills to do the work, and often didn’t have the right information at their fingertips to help guide them along a path to success.

In reflecting on the broader issues we were seeing, I was reminded of an earlier era—the 1970s and the 1980s—when manufacturing quality in the United States was inferior to other global competitors (Japan in particular). It was in response to that quality crisis that Congress created the Malcom Baldrige National Quality Award, and over the ensuing years it has become a widely respected global symbol of excellence. Baldrige helped transform many industries, and the practices and processes that were developed and institutionalized are now the norm across many industries.

It struck me that many of the issues I was seeing in cybersecurity were, in fact, very similar to many of the manufacturing quality issues of earlier years. These included process defects, poor measurement and detection tooling, lack of understanding of the root cause of cybersecurity defects, etc. And, while the National Institute of Standards and Technology (NIST) had produced an excellent Cybersecurity Framework (CSF), I felt more was needed, and I came to believe that Baldrige-based approaches were a potential solution to some of the problems I was seeing.

I was delighted to learn that others felt the same way, and, in particular, that the Baldrige Performance Excellence Program had begun work on a tool called the Baldrige Cybersecurity Excellence Builder (BCEB). Its introduction has been well received, and BCEB and the CSF are the now the go-to tools in many institutions.

There is good reason for that. The BCEB brings together the systems perspective, measurement, and results focus of the Baldrige Excellence Framework and the cybersecurity outcomes identified by the Cybersecurity Framework, to provide a unique tool for organizations across the economy to prioritize and execute cybersecurity enhancements. By involving boards and C-Suites, it breaks down the stovepipes that can lead to technological solutions that fail to protect critical cyber infrastructure. It makes

Tony Scott (from right) with Al Faber, President and CEO of the Baldrige Foundation, and Russell Branzell, CEO and President of the College of Healthcare Information Management Executives.

organizations safer by enabling them to better understand the effectiveness of cybersecurity risk management efforts in the context of their overall organizational needs, objectives, and outcomes.

After leaving government, I was asked to join the Baldrige Foundation Board, and I accepted enthusiastically. Through the Foundation's work, I know we will see a heightened focus on cybersecurity as part of an overall effort to grow and promote Baldrige thinking and institutional performance excellence in participating organizations.