This Week’s CISO STORIES podcast guest discusses actionable insights from the ‘grey box’ authored in the following extract.

TODD FITZGERALD
FOREWORD BY DR. LARRY PONEMON
Much energy was expended by organizations during this period to determine compliance through initiating gap analysis, remediating the gaps, and reporting compliance to company committees. This evolution of the CISO was also marked with limited enforcement of the security controls by some regulators such as HIPAA, and increased scrutiny by others, such as the Sarbanes–Oxley section 404 audits by the company external auditors. External enforcement may have been a mixed bag, as organizations tried to get to “100% compliant with X regulation.” The valuable Information Security Officer at this time was one that comprehended the regulations and could offer administrative, technical, or operational safeguards to protect the organization. Organizational skills and working across the organization became more important than the deep technical skills. This era represented a shift in the expectations of a CISO as we know it today, as now the CISO needed to be able to interpret legal regulations, and work with the General Counsel and other executives to formulate the strategies required. This period is also responsible for the beginning of senior management to become engaged with the information security controls and privacy processes protecting the organization.

LEE PARRISH: THE COLONOSCOPY OF CYBERSECURITY

VP, CISO, Blucora

The companies I have worked for as CISO offer a generous life insurance policy that provides a standard amount, with an option to increase coverage at my own expense. I chose a higher level of coverage which required that I go through several administrative processes. I first completed a questionnaire asking me basic questions about age, current medical conditions, smoker/nonsmoker, and other standard questions. The results came back and said that I passed the first milestone, the next one being a medical examination. I scheduled the screening, and a representative from the medical firm came to my office and performed the examination. He efficiently and professionally took my blood pressure, resting pulse rate, height, weight, and a urinalysis screening. He asked a few more questions and then put the results into a report that was submitted to his firm. The results came back in 2 weeks and said that for the level of insurance I was requesting, I was in good health and insurable to the level. Separate but related to this, I visit my primary care physician each year. She takes my blood pressure and resting pulse rate, asks me multiple questions, performs several tests of my blood, conducts Electrocardiogram tests, and gives me a prostate examination, a urinalysis screening, and several other tests. Additionally, she puts me through other testing protocols such as stress tests for heart health and a colonoscopy procedure. At the end of all these tests, the physician makes the determination that I am in good health. Both scenarios seek to accomplish
The compliance era was beneficial in ushering in new regulations and focusing organizations on information security. One could also evaluate this phase as being necessary, but not sufficient. The problem was that information security became a check-in-the-box-done approach. After the implementations of the regulations were considered complete, organizations disbanded the working committees for the project and went back to their normal activities. Security spending may have become elevated; however, the institutional focus was no longer on information protection. After all, the security project was done and just needed an annual review, right?

In addition to complying with the regulation, it became clear that implementing the same controls across the entire organization was inefficient and maybe not the best investment. For example, does the internal employee newsletter need to have the same protections as an externally facing health information inquiry system? In recognition that different risks may require different levels of investment and protection, the focus shifted from compliance with all the regulations to taking a risk-based approach to the information being protected. For example, as more and more information was stored on laptops, the sensitivity of the information needed to be evaluated. A watershed moment for laptop encryption came in 2006 when the Veterans Administration lost a laptop containing personal information of 26.5 million veterans. Many organizations at that time were not encrypting laptops. I recall asking at conferences during those years how many had encrypted their laptops and only half of the hands would go up—today, it would be rare to see anyone (admit) in a publicly traded or government entity not encrypting their laptops as a fundamental control. A compliance approach, at the time, would have mandated all computers be encrypted. A risk-based approach would have evaluated the desktops or servers as being internal to the locked building, and a much less probability of being lost or stolen (today, most organizations move to encrypt all devices as the threat has increased and the cost of the software has decreased).