

To many, IA refers to information assurance. I really like this term much better than information security since it speaks to the broader concepts of informational integrity and places emphasis on a far-more committed and positive notion - assurance.

However, to others there is an equally important I and A. This is integrity and availability, two of the three traditional goals of security represented by the famous triad c-i-a. For far too long, information security has focused almost exclusively on the "c", confidentiality. In far too many aspects of our modern digital age, integrity and availability are as important or often more important.

I'll never forget a meeting with a retired hospital CEO who scolded me on the destructive influence and operational damages brought by information security professionals who thought HIPAA was about privacy and confidentiality rather than portability and efficiency.

One of the most important lessons I can share about the triad is that these goals are usually competing and at times mutually exclusive. All too often, it's a zero sum game. That is, to get more confidentiality, we forsake integrity. This is a lesson I often share in our CISSP boot camps. When one looks at the early abstract security models, the Bell-La Padula model suggests that for multi-layered security one cannot write data down from a higher level of security to a lower level, nor can one read from a lower level to a higher level (insert graphic). While Bell-La Padula played a vital role in framing our understanding of multi-level security and how a system might be architected to implement these capabilities, it was limited in focus to only confidentiality. BIBA produced a model several years later that addressed the more likely commercial concerns about data integrity. To maintain multi-level data integrity, the BIBA model states that one cannot write from a lower security level to a higher level nor can one read **from a higher level from a lower level** ??????

What we see is these rules are mirror opposites. What provides confidentiality of information prevents integrity controls, and what provides the greatest integrity controls compromises confidentiality.

This makes sense in the real world too. When we think about trying to make strategic decisions based on confidential information, we have the challenge of adequately vetting the information. If I can tell the whole world we're invading Iraq based on a variety of intelligent sources, we then

must disclose those sources. Intelligence personnel are concerned that disclosing their sources will compromise their sources. They fail to appreciate that they compromise the integrity of the source by protecting its confidentiality. How do we review and judge accuracy and quality of information without disclosing the sources for rigorous review?

So, is it information assurance or integrity and availability that we need to add to our agenda? Actually, I think both go hand-in-hand which, when one thinks about it, might be just what we needed.