Information Assurance

In days gone by, Information Assurance was referred to as “Computer Security” because risks surrounding the computer were all we were concerned with. Today, that has all been rolled up into Information Assurance. This term covers all aspects of protecting information whether it be in transit (being communicated) or at rest (stored somewhere). Information Assurance covers a plethora of security topics. Some (but not all to provide a flavor) are:

- *digital encryption* - privacy protection
- *anti-virus* - detection and protection
- *anti-malware* - detection and protection
- *network intrusion* - detection and protection
- *database intrusion* - detection and protection
- *mobile device* – susceptible to all of the risks associated with any network connected device plus the surveillance and tracking that is imposed by various venders, operating systems, and applications in use
- *data access control* – to ensure that only authorized persons have access to appropriate data/information and nothing else
- *communications protection* – to protect the channels of communication as well as the data/information passing over them
- *penetration testing* – a process for improving security measures currently in place
- *digital forensics* – for investigating crimes with a digital component
- *system documentation* – to protect the resiliency of managing system/program change
- *standards* – to assure best practice and form is being followed
- *archiving* – to securely manage data/information that must be retained
- *records retention* – to securely manage the disposition of and disposal of data/information
- *physical security* of IT resources – to protect against physical intrusion and access to sensitive areas and IT resources by those without the authority to be there

The list goes on. In fact each of these topics encompass whole bodies of knowledge and processes wherein you can earn certificates of competence. There continues to be shortages of qualified professionals in the field of information assurance.

Why Information Assurance? Everything is controlled by or operates using information. That means business, health, military, education, retail, manufacturing, etc, etc. Almost 6 billions people carry their own private computer around with them 24 hours a day, 7 days a week. Their lives are measured and monitored, and their relationships are impacted by these devices. In fact many of these billions are addicted to their mobile device. This is evidenced by their use patterns: first thing looked at upon awakening each day, last thing they look at prior to going to bed, as well as many hours of use and activity throughout the day. When the device is not available for any reason, anxiety is escalated. This paper is not about mobile devices. There are plenty of other writings about that in the Information Communications Technology (ICT) sphere. However, the mobile device is just one more platform where Information Assurance is important. It may be the most important because people keep a great deal of personal information on these devices in addition to information about their minute to minute movements and communications activities being collected and used to meet the objectives of others.

There are many universities around the world that have dedicated Information Assurance degrees. There is a well established US program that provides a set of guidelines for universities who wish to pursue the formation of such a degree and thereafter the new degree can be certified, according to a well defined measure as well. There are also universities who take the position that this topic is not an accepted academic pursuit. They do not see the opportunities for research, which are many, and for publication in relevant academic journals.

The notion that academic journals are useful is a topic for further discussion in another venue. However, there is only one question that I would pose about them: when was the last time that you saw a refereed academic journal for sale at your local newsstand, bookstore, or wherever you buy magazines and the like? The obvious answer is the 12th of never. These publications are incestuous (purchased almost exclusively by academics and university libraries – and extremely expensive as well) and are dedicated for the sole use of academics. Therefore, whatever is written there almost never gets to the audience (outside academia) that might make use of it. Moreover, the nature of academic publication is such that whatever is published is at least six months out of date.

How does that relate to Information Assurance as an academic topic? Well, protecting the ICT function is done in real-time. The attacks come in real-time and new (zero-day) attacks are created on an almost daily basis. Therefore, research in this domain by its nature must also be in real-time. Any new techniques developed academically are automatically out of date and irrelevant whenever they are published. In addition, ICT professionals in the main do not have the luxury to read academic journals – because, for the most part, they are not relevant to protecting the ICT functions they are responsible for. Search, hard as you might, and you will find few refereed academic journals dedicated to Information Assurance and the topics that comprise this domain.

The field of Information Assurance is rich with challenges and interesting technologies and theories. This field provides a long term profession for young people beginning their careers. The bad guys are not going to go away anytime soon. The prizes on offer, if one can compromise any targeted system, are sizable. So for the bad guys, this field offers a lucrative low risk opportunity to make a profitable career. On both sides of the divide the future prospects are very attractive.