

## **An Information Security Professional – to be or not to be....**

(speech presented at the GovernmentWare 2009 conference 30 September 2009 by Gerard Tan)

As President of AISP, I am often asked, or challenged, why join AISP? I am already a member of other bodies or associations – so what is different about AISP? What is the benefit of joining AISP?

I am reminded of one of the most famous phrases from Shakespeare's tragedy – Hamlet "**To be or not to be: that is the question**". Who then is Hamlet and what is the meaning behind this famous quote?

**Prince Hamlet** is a fictional character, the protagonist in Shakespeare's tragedy *Hamlet*. He is the Prince of Denmark, nephew to the usurping Claudius and son of the previous King of Denmark, Old Hamlet. Throughout the play he struggles with whether, and how, to avenge the murder of his father, and struggles with his own sanity along the way.

What Hamlet is musing on is the comparison between the pain of life, which he sees as inevitable and the fear of the uncertainty of death and of possible damnation of suicide.

Perhaps, this might also be the dilemma of many of you here in this hall today. Should I remain only as an infocomm security practitioner and face the possibility that one day in the not too distant future, I become a relic in a cyberworld museum. Or should I choose the path of turning myself into a real professional with all its challenges and pain of living, but which will make me relevant for the rest of my natural life.

Unlike Hamlet, fortunately, choosing between the status quo and a professional life is not a life and death decision you have to make; well not yet at least! The play has just started and there is still time before we reach Act 5.

But before we make up our minds on which to choose, perhaps it is only reasonable of me to explain in a little more detail what being a professional really means.

To start, **what is a profession?**

There are many definitions of the word. Sidney and Beatrice Webb, both British socialists, economists and reformers, in an article published in the *New Statements* on 21 April 1917 defined a profession as:

“.....a vocation founded upon specialised educational training, the purpose of which is to supply disinterested counsel and service to others, for a direct and definite compensation, wholly apart from expectation of other business gain”.

## ***An Information Security Professional – to be or not to be...***

From this definition, I believe a professional possesses 5 key characteristics, not necessarily in the order of importance:

1. Academic qualifications or certifications
2. Expert & specialized knowledge and experience in the field of practice
3. Obligation to deliver high quality work & high standards of professional ethics, trust & integrity
4. Membership of a professional body
5. Working under a regulatory framework

Let me briefly discuss each in turn.

### **1. Academic qualifications or certifications**

He would have had formal education or qualifications. It is a universally accepted norm that a professional is a trained person who has received formal education in the field of his expertise. An academic qualification or certification is recognition that he has met the baseline standard of a Body of Knowledge that is expected of that field of expertise.

This pre-requisite is generally similar whether a person wishes to join a professional body or a certification body.

### **2. Expert & specialized knowledge and experience in the field of practice**

Not only must a person be academically qualified, he must convincingly demonstrate expert and specialized knowledge and have sufficient relevant experience in his field of practice.

He is someone widely recognized as a person who not only possesses but is also able to demonstrate his technique and skill. He is looked upon as one whose judgement in his field of work is authoritative and his status is accepted by his peers or the public.

He is also a person who believes in and constantly upgrades himself technically in what is commonly known as Continuing Professional Education. This is especially relevant in infocomm technology and infocomm security where the pace of advances in technology and techniques to breach security moves at lightning speed. Catching up and staying on top of the game is a never ending challenge.

This requirement is quite similar for both a professional body and a certification body. However, I sense that the standard of assessment on the skill sets and experience of the practitioner would be different. A certification body in my experience generally accepts your work experience as declared and verified by your sponsors or bosses without further queries. A professional body,

## ***An Information Security Professional – to be or not to be...***

however, tends to look more carefully at what is declared and validates to ensure that there is substance behind the resumes and statement of experience.

### **3. Obligation to deliver high quality work & high standards of professional ethics, trust and integrity**

A hallmark of a true professional is the obligation to consistently deliver high quality work to his employers or clients, or pay the very high price of being found professionally negligent in his work.

Both certification bodies and professional bodies generally have a **Code of Ethics** which they require their members to comply. Both require their members to only deliver services for which they are fully competent and qualified to deliver. But there is one important difference between a Certification Body and a Professional Body. In the event of a breach, the Certification Body is unlikely to punish its members with punitive penalties.

As a member of a professional body, however, the consequences can be quite different. First, you could be fired from your job or by your client. Then, if there is loss or damage sustained, you could be sued for negligence and end up paying damages. But that is not the end of the story, at least not for you. The professional body may investigate you and censure, fine or even strike you off their registers so that you lose your licence to practice. History is full of such cases of lawyers, accountants and doctors, to name a few, who have suffered this unhappy fate.

Because a member of a professional body cannot afford to breach any of its ethical rules no matter how minor the infringement, his conduct and behavior in his professional, and I might add, his personal life as well, is one of aversion to unnecessary risk taking where he could be held accountable for negligence and/or have questions raised about his personal or professional integrity.

These are therefore very strong deterrents. On the brighter side, if you are a professional, you will enjoy the recognition of not only **competence** but also **trustworthiness** – two **highly valued attributes** that distinguish you from the ordinary practitioner or technical specialist.

### **4. Membership with a professional body**

A hallmark of a professional is belonging to an association or body whose members are like-minded professionals and who are committed to setting standards, codes of ethics, enforcement, continued professional development and promoting its standing in society as the voice of the profession. Even the fictional James Bond belongs to MI6, a professional organization in the British Secret Intelligence Service that trains and equips him and gives him the license to kill.

**What then is a professional body?** *Lee Harvey and Selena Mason, in a 1995 research report entitled “The Role of Professional Bodies in Higher Education Quality Monitoring”, defined a professional body as a group of people in a learned occupation who are entrusted with maintaining control or oversight of the legitimate practice of the occupation. A true professional body safeguards public interests, represents the interest of its professional practitioners and represents its own self interest to maintain its own powerful position as a controlling body.*

Our infocomm security practitioners need to join forces for reasons of mutual interest, self-interest and to gain legitimacy in our field of work. The phrase “**No man is an island**” by John Donne, a 16<sup>th</sup> century British poet, priest and lawyer, is most apt here. We need to come together and work together for the survival of our species.

## **5. Working under a regulatory framework**

To have teeth, professional bodies are typically regulated by statute. With it comes the responsibility to set entry requirements and very likely examinations for qualification or certification, issuing of practicing licences to members, powers of enforcement and censure, amongst others.

The infocomm technology profession is one that is particularly challenging to define and regulate. This “profession” if one may call it, is better known for defining and certifying specific technical competencies. This is because the field is so wide and use of technology is so widespread that drawing a fine line between an “infocomm technology professional” and one who is not, is extremely difficult. Maybe that is why you do not really have a licensing body for infocomm technology practitioners.

However, if you narrow down the disciplines to specialized fields like infocomm security, the potential is there. You can define the boundaries of a body of knowledge for an infocomm security practitioner, which the AISP has done. You can test the practitioner’s knowledge to assess if he has met the baseline standards, which AISP will soon do through a qualifying examination. You can follow up to assess his minimum work experience and hold him to high ethical standards as defined by a Code of Ethics. And if he meets all these criteria, you can admit him to an exclusive club of professional infocomm security specialists.

What is now missing is **licensing** of such practitioners in Singapore. I am unaware of any other country that has done that either. But that would be a logical next step once the key processes and a reasonably large pool of qualified members are established. With that, infocomm security practitioners who retain their professional membership and practicing license are likely to be highly sought after and command a premium in wages. In addition, in certain highly sensitive jobs or assignments, there is a high chance that only they will be eligible to offer their services.

So is this the direction Singapore is headed? Is it just an aspiration or will it be a reality?

## ***An Information Security Professional – to be or not to be...***

I would personally like to believe we have begun the journey in 2008 when AISP was formed. It was formed because the market believes that there is a strong driver for professionalizing the infocomm security profession. It is not enough just to be certified by your examination body and be bound loosely by its rules and code of ethics that do not necessarily promote the interest, values and trust that are needed of a true profession. Clearly, more is needed to be done to raise the bar and status of the profession.

### **Conclusion**

Wind the clock forward a few years from today. What do we see out there? Advances in technology, and most noticeably, changes in the way people and businesses use technology in their daily lives, will be dramatic. The bright spot for hackers and cyber criminals is that computer systems and networks are becoming increasingly vulnerable to attacks and security breaches. **What is maybe more scary is where are we going to find infocomm security specialists whom we can trust!**

If I may quote Warren Buffett:

**“Somebody once said that in looking for people to hire. You look for three qualities: integrity, intelligence, and energy. But if they don’t have the first, the other two will kill you”.**

Seeing this danger heading our way, the infocomm technology industry in Singapore with the strong support of the IDA, rose to the occasion to face this challenge head on.

Lawyers have their Law Society, Accountants their Institute of Certified Public Accountants, and Doctors their Singapore Medical Association. Infocomm Security practitioners have the Association of Information Security Professionals or AISP. AISP is your professional body that aims to raise the standard of the infocomm security profession in Singapore and elevate your status in society.

We certainly do not want to end up like Hamlet, who eventually poisoned himself as he chose death. We need to choose “Life” by transforming ourselves into true infocomm security professionals. AISP is here to help you walk that road to achieve that status and recognition. Join us and be part of this important journey!

Thank you.

Gerard Tan

President, AISP, 30 September 2009