



Professionalism key to information security



John Colley

CYBER crime knows no borders. We have moved on from the days when security was like a village – everyone knew everyone and knowing who to trust was easy.

Globally, information security staff in corporations and governments are expected to be risk managers, business continuity planners and business enablers. The field is changing and the risks are increasing.

Today, the scope, volume and diversity of work tackled by security professionals means you need international measures of competence and currency, instead of knowledge of individuals. A key component of securing business and public systems in a networked world is that people charged with developing, implementing and maintaining security policies are highly-qualified professionals with validated knowledge and experience.

Information security practitioners need a common benchmark – they must be able to understand each other and have confidence in each other's base level of knowledge and those of their international suppliers. Recognising information security

as a profession will really make a difference.

About 15 per cent of a nation's critical national infrastructure is owned by its government; the rest is privately owned.

The responsibility on corporations to protect these assets is a weighty one, as breaches of any magnitude can quickly affect consumer confidence, stock price and economic stability.

Yet the irony is that information security professionals do not receive much in the way of corporate attention. Our success is silence, and our managers measure our success by our invisibility.

But according to the 2004 *Global Information Security Workforce Study* by (ISC)² and IDC, the number of information security professionals is expected to increase from 1.3 million to 2.1 million by 2008. The study also indicates that for 93 per cent of security recruiters, accreditations are important when making hiring decisions. They afford the employer some degree of comfort or a guarantee as to an individual's competency/knowledge level, and can be critical in terms of legal liability or corporate due diligence.

Accreditation offers the professional a public recognition of ability, and their employer the peace of mind that the holder has made a commitment to maintaining competency and adhering to a strict code of ethics.

Security practice is at the heart of a well-governed organisation, but how do we define it? How do we govern it? How do we ensure its validity?

Mastery of access control, cryptography, telecoms security, internet and operations security are just the beginning. The diversity of knowledge and skill required makes it tough to establish common ground without a good degree of professionalisation.

Although a professional information security body does not exist in the same

Our success is silence, and our managers measure our success by our invisibility

sense as for doctors and lawyers, there are many publicly-recognised forms of competence available.

The opportunities are diverse – from undergraduate programmes, to Masters, to job-based professional qualifications. For example, the Certified Information Systems Security Professional accreditation from (ISC)² is ideally suited for experienced information security professionals seeking a long-term management career spanning a broad area of security disciplines. Others are more suited to highly technical roles.

The ultimate sign of a sector that is professionalised is that its people are interchangeable. A company can hire an accountant and expect him to take over the work of another accountant.

Imagine if accountants were not governed by a professional body (and hence subject to professional standards). The businesses they represent would have difficulty attracting investors, and investors would not know how to compare one corporation with another. Similarly, in a few years, businesses without a security policy that is quantifiable and recognisable to outside investors may not form a viable basis for investment.

I recommend that security professionals do the following three things:

- Take responsibility for your own professional behaviour and development
- Stay current – undergo continuous development and training
- Embrace risk – business risk management is increasingly the skill of currency.

Information security professionalisation is a key foundation block in society, and it is only through mentoring, community outreach and understanding what 'professionalisation' entails that we will find a meaningful way forward.

John Colley is chairman of security accreditation body (ISC)². See: www.isc2.org