Role With It

Michael Barwise

Information assurance is one of those popular terms (like "risk") that is widely used without a clear understanding of its real meaning. To some extent it has been the victim of grade inflation - we started out doing IT security, which gradually became referred to as "information security" and ultimately as "information assurance" - ever grander-sounding titles, despite the actual nature of what most of us were doing hardly changing. As a result, the security remit of most Chief Information Officer (CIO) and Chief Information Security Officer (CISO) roles is today still restricted largely to technologies, often essentially replicating the security remit of the Chief Technology Officer (CTO). Much corporate information assurance therefore exists in name alone.

So what could be done differently? Let's look first at information security (IS). Although this is commonly considered a technological discipline, technological security (ITS) is really only one of its components. Technologies, business processes and people management each contribute roughly a third of both the vulnerability space and protection, but they are not neatly segregated into silos that can be managed independently. Clearly, people management and business processes overlap strongly, but it is less well recognised that both overlap to a considerable extent with technologies as well. Many technological vulnerabilities are exploitable only via human intervention, and protection technologies must not interfere with business operations. Equally, business demands must not conflict with technical security or compliance requirements. Consequently, around 75 per cent of IS does not directly relate to technologies, but to change control, policy and procedure management, business process review, analysis, audit and the security-related components of statutory and regulatory compliances. The remit of ITS is the security of the technological infrastructure over which business information flows and the remit of IS is to ensure business information is managed and used securely over that infrastructure.

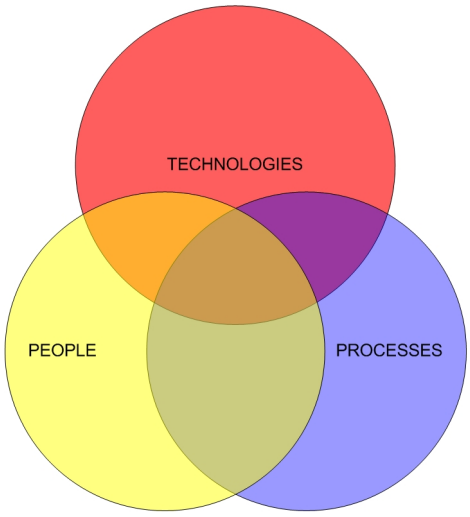

FIG. 1 The components of information security

Our definition of IS seems pretty all-embracing, so how does information assurance (IA) differ from it? IA has a monitoring responsibility for the entirety of IS, but its primary obligations are oversight of the accuracy, authenticity, completeness and accessibility of business information assets, and responsibility for compliance with the business-related components of relevant statutory and regulatory compliances.

Let's examine a simple example to see where the boundaries lie. The UK Data Protection Act invokes eight principles:

1. processing must be fair and lawful
2. processing must be restricted to specific purposes
3. information must be adequate, relevant and not excessive
4. information must be accurate and up to date

5. information must not be kept for longer than necessary
6. processing must be in accordance with subjects' rights
7. technical and procedural security must be adequate
8. data transfers abroad must comply with the above requirements

In this case, ITS would be responsible for the technological components of principle seven, and that's all. The procedural components of principle seven, technical reviews in support of principle eight, and the fulfilment of principle five are the remit of IS. Principles two, three, four and the direction of principle five are the responsibility of IA. Principles one, six and the non-technical aspects of principle eight are matters for the legal department, which comes under corporate governance.

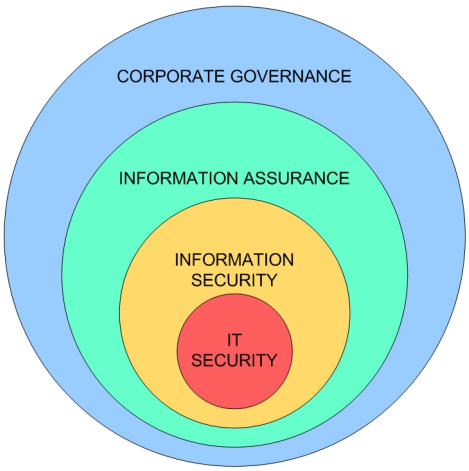

FIG. 2 Corporate information governance

Thus the relationships resolve to a nest of functions with ITS at the centre, surrounded in turn by IS, IA and, finally, the information-related components of corporate governance.

From this is clear that the common practice of positioning IA or IS (or even just Data Protection) within the IT Department is a recipe for failure. Both the range of business and soft skills - commercial acumen, risk expertise, legal understanding and psychology - and the authority and reporting pathways required for proper performance of IS and IA are rarely required of, or used as hiring criteria in, the pure technological security domain.

So, from the security perspective, where should the recognised roles of CTO, CISO and CIO ideally sit, and what are the ideal skill sets for fulfilling them? The CTO is responsible for the technological architecture and infrastructure, including IT security - firewalling, network segregation, intrusion detection and prevention, event monitoring and the provision of adequate backup and disaster recovery (DR) technologies. The role requires a deep understanding of information technologies at the level of first principles, knowledge of and the ability to evaluate current vendor offerings, and awareness of the nature of and changes to the technical threat landscape.

The CISO requires conceptual understanding of technologies with the same scope as the CTO's, but not at such a detailed level. But the CISO must maintain detailed current knowledge of the threat and vulnerability spaces and be able assess current risks to business information with confidence. In addition, the CISO must be able to review business requirements and identify potential vulnerabilities in both processes and technical implementations, for example to ensure that data backup and DR procedures will perform effectively for the business.

The CIO must have a broad understanding of everything within the remit of the CTO and CISO, but should concentrate primarily on those aspects of IA that are outside those remits - ensuring that information-related legal and contractual obligations are fulfilled, that business information can be trusted as a basis for decision-making, and that the required data can be found and assembled into useful information on demand. The CIO role therefore requires detailed knowledge of the business and its expectations, excellent communication skills, and broad understanding of both technologies and regulatory requirements sufficient to enable reliable communication with the CISO and CTO.
Thus we see that the security-related roles of CIO, CISO and CTO are ideally nested in the same way

that we established the disciplines of IA, IS and ITS are. In fact they map pretty much one to one. Each tier has a wider remit than the tier below, relying on the specialist knowledge of that tier to implement specific components of broader security requirements ultimately driven by corporate governance requirements. However, this must not be a command and control hierarchy of silos, but a consortium based on complementary expertise. Nested silos perform no better than parallel silos, and implementing "security" from within silos of any kind cannot deliver real Information Assurance. The free flow of information across the structures outline here is essential to the performance of the whole.

Originally appeared in ITNow, Autumn 2013