Information Security Now – 44

Information Systems Assurance

(from the back room to the front office – a 50 year journey)

John Mitchell

Fifty years ago, in the very early days of commercial computing and just ten years after the formation of the BCS, some extremely far-sighted people realised that the need to control the new devices was at least as important as the need to exploit them. In those early days, assurance was deemed as being non-core to computing and indeed was relegated to the back-room of IT advances. Yet these far-sighted people persevered and in 1965 the BCS's Auditing By Computer (ABC) specialist group was formed, becoming in turn the Computer Audit Specialist Group (CASG) and eventually in its current manifestation as the Information Risk Management and Assurance (IRMA) specialist group. Through their steady efforts, IT assurance moved from the back-room to the front-office of IT governance. IT governance being the term used to describe the totality of how computerised systems are managed, whether they be for scientific, educational, health, military, business, or for social purposes.

IT security is a sub-set of IT governance and was initially viewed as the triage of confidentiality, integrity and availability (CIA). Although this was useful in identifying the areas of concern, little coherent research was conducted in the early days as to how these concerns should be resolved. As is so often the case the exploitation of the technology exceeded our ability to manage it. However, the application of the CIA triage gradually led to the concept of compliance, which became an extension to the original triage. However, compliance implies that there is a framework with which to comply and this was sadly lacking in the explosion of technological innovation which began in the early nineteen-seventies. Although the concept of control has been around for at least five thousand years (the Egyptian Pharos used auditors to verify the grain harvest) the things being controlled tended to be physical and therefore visible, but the challenge with IT is that the really important things tend to be invisible. You cannot see or touch the data, the software, or the network traffic, so the challenge was to create a control framework which recognised these limitations. Although CIA identified the main problems (can we keep things secret; can we assure their integrity; can we control their availability?), it did little to provide the solutions. However, it did provide a starting point by identifying the challenges. In the early 1970s assurance providers commenced the not inconsiderable task of providing a control framework for invisible things.

Three organisations played a considerable part in the development of what are now complimentary governance frameworks: the BCS, the British Standards Institute (BSI) and the Information Systems Audit and Control Association (ISACA). The initial British Standard for Information Security (BS 17799) was primarily developed by the BCS in conjunction with the BSI. This was eventually subsumed into ISO 27000. Meanwhile, ISACA developed its own

open standard, Control Objectives for IT (COBIT). These standards eventually became risk based and underpin our current governance frameworks.

The major challenge faced in developing any IT security framework is the dynamism of the technologies we are trying to control. Since the 1960s we have seen the following developments, each of which has had a significant impact on the risk model and the associated control paradigm.

- Single batch program (making the data & process invisible)
- Batch multi-tasking (shared environments)
- On-line retrieval (remote access)
- Real-time update (remote immediate update)
- Databases (shared data)
- Stand-alone PCs (end-user computing)
- Networking (linking of devices)
- File servers & distributed processing (shared processing & data storage)
- Internet, Intranet & Extranet (extension of wide area networks)
- Phone devices (remote access to data via personal phones)
- Bring your own device (personal devices used in the office)
- Cloud computing (data, software & security as a remote service)
- 3D printing (bypasses controls at national borders)
- Smart devices (everything from the kettle to the fridge)
- The Internet of Things (joining the smart devices together)
- Specific Artificial Intelligence (expertise in a limited area)
- General Artificial Intelligence (the shape of things to come?)

The initial challenge was to simply manage the conversion of physical records into electronic records and dealing with their subsequent invisibility and processing (garbage in, garbage out). This was nothing however, when compared with the challenge of real-time update conducted from a multitude of geographically dispersed devices and users. The internet and cloud computing muddied the pitch even further, because we now did not even know who was at the other end of the wire and where our data and software was stored. The Internet of Things (IoT) now means that a fridge can be subverted to send spam and driverless cars can be hacked. The white-hats are always running behind the black-hats. You can't defend against malware that hasn't yet been invented, but when that zero-day attack does happen, we are on the back foot of trying to find a defence. However, our security frameworks have prepared us for this and the catch-up is now very fast.

Sixty years of IT exploitation has led to some good theoretical security frameworks such as multi-factor authentication, but until recently organisations viewed security as a cost, rather than a benefit. It is only in recent memory that the regulators have started to punish organisations which breach statutory and regulatory requirements. Even now the sanctions do not tend to hit individuals, but rather the stakeholders. The new European Data Protection directive permits the imposition of massive fines and the potential for individual accountability and this will, hopefully, tend to focus the corporate mind on the need for better security. It becomes more than a simple cost benefit analysis if an individual can have their freedom revoked for an act of negligence. Which brings me to a very important consideration. We can control the technology

absolutely. It will always do what we tell it to do. However, we can only manage people. They have free-will and can do what they like. It is people, good and bad, who exploit the technology and that free-will means that no matter how good your assurance frameworks there will always be some people looking for ways of circumnavigating them. So far, I have been discussing negligence rather than criminal activity. The former arises from stupidity, the latter from intent. I have never known a criminal who thought that he would get caught and therefore the threat of a sanction as a deterrent is a hope rather than an effective control. Indeed, with IT. what we really need is immediate detection of a circumnavigation of our security paradigm. What in 2004 Brewer and List[1] would have defined as a 'type 1' control. We now have a better understanding of control anatomy and even ways of measuring control effectiveness. We have come a long way in in fifty years in providing an assurance framework, but the greater part of the journey is still before us.

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a previous member of BCS Council, and is a current member its Risk Audit & Finance Committee. He is an active member of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)7774 145638.

[1] Measuring the effectiveness of an internal control system. Dr. David Brewer and William List - 2004