

# Information Security in the Manufacturing World

THL Gordon, FIOM

Typically, when thinking about the subject of information security, if we think about it at all, we assume that it is only a problem for banks, hospitals, despotic governments and intelligence agencies. It has nothing to do with manufacturing! This could not be further from reality; a cavalier attitude to information security, and the consequences of not protecting information assets, could close the plant. Ask yourself the question, “How long could this organisation function without issuing and receiving parts, invoicing, shipping, meeting payroll, raising shop orders, designing products etc?” Generally not very long, assuming that the information systems are designed to be a tool to assist in meeting customer requirements.

Information security is a balance between ‘confidentiality’, ‘availability’ and ‘integrity’ of information; all organisations have different needs in this respect and all organisations must decide for themselves the appropriate balance. Information, to be usable in any meaningful sense, must be shared; it must be available to those, and only those, who need it and it must possess a high degree of integrity - the only thing worse than losing information is not knowing whether the information available is corrupt or not.

An Information Security Management System [ISMS] is designed to assist an organisation in making a realistic balance. All organisations, including manufacturing organisations, are vulnerable to threats [internal and external]; an ISMS is about the handling the threats to the organisation and the procedures and controls necessary to mitigate the risk or, in the final analysis, provide management with the necessary information to accept those risks. It is probably worthwhile putting the words “threat”, “vulnerable” and “risk” in

context; this is best done by using an analogy.

If a normal person decides to walk around a high crime area late at night they run a risk, they are vulnerable to the threat of being mugged. What can you do about it? You can avoid it by not walking around that area alone at night, you can manage your vulnerability by carrying a Browning 9mm automatic or you can simply ignore it – the ‘it will never happen to me’ syndrome. The threat will change of course; after a few muggers have been shot, the remainder will invest in bullet proof vests – it is a Darwinian process – the clever ones adapt. So the midnight stroller must adapt, too. It is the same in any business.

The Information Security Management System, ISO 27001, was released in the autumn of 2005. ISO 27001:2005 is designed to coordinate the information security activities necessary in an organisation. It is deliberately designed as a fit with your existing QMS and EMS – why have more than one management system in the organisation?

ISO 27001 requires that the organisation undertakes a risk analysis and assessment process, which covers all known threats to the organisation and then decides how to handle them. Leadership in the organisation might decide to accept those risks, for various reasons; might decide to transfer those risks, for example by purchasing insurance; or by implementing controls to handle them. ISO 27001 requires the organisation to consider a wide range of controls; people, infrastructure, technology, business disruption and legal compliance amongst others. Manufacturing presents a number of interesting problems for information security. The integrity of information is vital, without that no manufacturing system will work. Availability is vital because a wide range of functions both inside

and outside the organisation must have access to the information in order to function. However, is confidentiality that vital? What is really so confidential that a well informed outsider cannot make an educated guess about the organisation’s systems, procedures, pricing, costing, forecasting or strategic planning?

To take a specific example, which is probably fairly unique to the manufacturing environment? Let us suppose that we are considering sole sourcing a vital component to a vendor. What are the things we need to know? We need to know that the vendor has the ability to consistently supply a product that meets our needs. However, we also need to know that the vendor has thought about possible disruption to their business: loss of key employees, strikes, sabotage, bankruptcy, fire, flood, business continuity etc. ISO 27001 requires the organisation to put in place controls to mitigate these problems. 100% security is an impossibility, but if your potential supplier takes the attitude “It will never happen here” then a wise organisation avoids that vendor like the plague!

ISO 27001 is in its infancy. Just as ISO 9000 was a customer ‘exciter’ twenty years ago and is now a required ‘commodity’, 27001 will probably go through the same developmental phases. A wise organisation will think about ISMS now before it becomes a general requirement.

## About the author

**Tom Gordon** FIOM, CFPIM, CQE, CQA, CQMgr is a senior member of the American Society for Quality. He is a British expatriate working in the USA and teaches the IRCA 27001 Lead Auditor courses.