An Original

Article

Information Security Management Systems
The ISO Alternative

By Tom Gordon
Missouri Enterprise Project Manager

Abstract.

According to an article in the June edition of "National Defense", Cyber-attacks are becoming the 'new normal of enterprises'. [1] An article in a recent "Economist" [2] reports a study that showed an increase of 42% in successful cyber-attacks, weekly, over 2012. The "Economist" article goes on to suggest that over 75% of attacks were successful because of weak user names or passwords. It suggests that these 'holes' could be plugged for very little expense compared with the costs of 'hacking back'. ISO 27001 is one of the relatively straightforward ways to plug a great many holes.

Breaching an organization's [or individual's] information security boundaries can be both fun and profitable! At the recent "BLACK HAT" and "DEFCON" events in Las Vegas, presentations with titles like, "Stalking a City for Fun and Frivolity", "Home Invasion 2.0" and "Dude, WRF in my car" created a great deal of interest amongst hackers and wanna be hackers. [3]

While it is true that "white hat" hackers can perform a valuable service by finding security flaws before nefarious folk discover them, it is also true that many organizations have been unwittingly hacked without their awareness. [4]

It is rather frightening that hackers have to be right just once; to protect against them an organization must be right many hundreds of times.

---

[1] Jacob Pankowski et all, "Corporate Cybersecurity Plans must evolve", National Defense, June, 2013, p9.
[2] The ECONOMIST, August 10th, 2013, p11.
[3] The ECONOMIST, August 3rd, 2013, p. 52.
[4] Mr Barrnaby Jack has been credited with "Jackpotting" – hacking ATMs so that they just spewed out banknotes but, on a positive side, also discovered flaws in heart pacemakers and defibrillators.

Today, the information economy demands the development, exploitation and protection of information assets to allow the long-term competitiveness and survival of corporations [and, perhaps, entire economies].

The protection of information assets, termed information security management, is, consequently, overtaking physical asset protection as a fundamental corporate governance responsibility.

Information Security Management can be defined as "the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investment and business opportunities" [5]

Manufacturing organizations are particularly vulnerable. The tendency today is to maximize the effectiveness of the supply chain from raw material to Customer. This involves the sharing of a high level of data throughout the chain; however, as the common saying goes, "Three people can keep a secret but only if two of them are dead". [ISO 9001:2008 mentions "intellectual property" but only as a footnote to §7.5.4, Customer Property.]

Information Security is based upon three "pillars": Confidentiality, Integrity and Availability.

The information that an organization relies upon must meet all these three requirements to function; they are also the 'doors' through which the organization's intellectual property can be stolen.

ISO 27001 concerns itself with all three pillars.

Certification to and implementation of ISO 27001 will not stop the Chinese military from hacking into your computer systems.

Constant vigilance and education is the only way to prevent those attempts: for example the only protection against spearphishing is paranoia, especially as the hackers are getting better at disguising phishing e-mails!

What certification to 27001 will show your Customers and other stakeholders is that you have approached securing your systems in a structured and comprehensive manner. ISO 27001 is about risk analysis and, once identified, the steps that an organization is able to take to mitigate the perceived risks.

There are 4 components of Risk:

- The magnitude of loss

[5] ISO 27002:2005, clause 0.1

- The chance of loss
- The exposure to loss
- The effort it takes to recover from loss

A definition of Risk Management could be:- “Dealimg with risk and the decisions taken that works to the best interest of the Organization”.

Risks to your organization and data come in three flavors, ISO implementation can help, to varying degrees, with all three:

- Risk that can be mitigated by Company systems, plans and procedures. This is the principle arena of the ISO standard. Appendix A of ISO 27001 identifies the controls, which are necessary, and are derived from the Top Management “Statement of Applicability” [much as the Quality Objectives are derived from the Quality Policy in ISO 9001]. The subsequent Risk Treatment Plan identifies the Organization’s approach to risk and the criteria for handling risk.

- Risk that can be mitigated by the use of outside bodies; for example insurance, righteous hacking, back hacking and other services. Certification to an ISMS, like ISO 27001, will help to defray some of the costy of these services.

- Risk that has been identified but, because of cost, technology or other factors, must be accepted as a function of doing business. This is termed “Risk Appetite” and the degree to which an organization accepts this risk must be carefully considered. Certification to ISO 27001 will ensure that Top Management understands what is involved in risk appetitite and is prepared to accept the degree of risk **from a position of knowledge**, as opposed to the common practice of ignoring the problem in the hope that it will go away.

The Missouri Enterprise implementation methodology focuses upon the following areas:

- Risk assessment
- Risk management objectives
- Roles and responsibilities within the Organization
- Threats and vulnerabilities
- Impact on assets
- Likelihood and Risk Level
- Selection of appropriate controls
- Maintenance and Continual Improvement

The cost of implementating 27001 will vary depending upon the sophistication and size of the organization. As with all the ISO family, most organizations that set out to achieve certification will already have a number of the necessary controls in place.

ISO 27001 necessitates ensuring that that existing controls are adequate and appropriate to the business and that any additional controls are implemented as a matter of urgency. [6]

The first step in the implementation process is, therefore, a Gap Analysis, determining what is in place and what should be in place.

The Missouri Enterprise approach to a Gap Analysis is 'Top Down", as this will most quickly identify the critical loopholes in the existing security system as well as controls, which are unnecessary and are NVA.

A typical Gap Analysis, depending upon the Organization in question, can take from 3 to 5 days on site.

[6] A personal experience in auditing a large, Government Organization for certification. Each System Designer was required to have a complex password and to change it on a regular basis – Good. However, a list of usernames and current passwords were posted on the department notice-board – not so good!