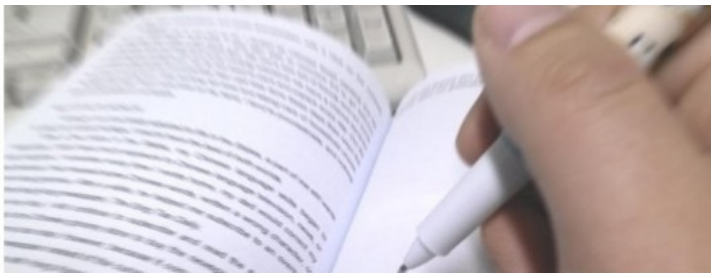

These updates (Copyright 2013, 14) apply to CISA and CISM…

Special reading – espionage and spying

Espionage is spying. An insider refers to an individual who tries to make legitimate access to an organization for malicious purposes. An insider may be a fulltime staff, a contractor or anyone who provides support services to the target organization. Manipulation refers to attempt to access an organization through using techniques to manipulate innocent staff. Military secrets may include items such as weapon information, troop locations and so on. Industrial secrets may include information on proprietary technologies, products, processes and plans. Political secrets may include confidential information on affairs with a political or security nature as well as sensitive economic information and policies.

In the US, 18 USC Chapter 37 deals with espionage broadly. 18 USC § 793 defines the gathering, transmitting or losing of defense information. On the other hand, 18 USC § 798 deals with the disclosure of classified information. In the UK, the 1911 Act defines the offence of spying.

Special reading - threats from social networks

The key understanding you and your users should have is that once information is posted to a social networking site, do not expect it to stay private. The more you post, the more vulnerable you will become. In particular, the personal information you share will likely be used to conduct attacks against yourself or your coworkers and friends.

Common scams on social networks (such as Facebook) may include cross-site

scripting, clickjacking, survey scams and identity theft. With cross-site scripting AKA Self-XSS, malicious messages with Like or Dislike button may take you to a web page somewhere that tricks you into pasting a malicious piece of code into your browser. Sometimes the attack may even run in a hidden manner as many computers allow Javascript execution without your knowledge.

Clickjacking AKA likejacking AKA UI redressing attempts to trick you into revealing confidential information when you click on a seemingly innocuous webpage. Clickjacking often uses embedded code or script, typically in the form of a button (for example, in order to view a video you must first click on a Like button ...etc). Survey scams, on the other hand, try to trick you into installing an application from a spammed link.

Tumblr (a site full of blogs) encourages users to post and repost content. When there are fake Tumblr staff blog entries that provide free-like offers after completing a survey, the threat can get wide spread pretty quickly. On Twitter, rogue links in Tweets that take users to malicious sites that are hosted somewhere else.