File 20110426.1016: Notes from 'Fast Forward' lecture on 'What the Security Profession can Learn from the Intelligence Profession' by Ira Winkler. At NSA, he wrote the seminal work on applying intelligence collection techniques to penetration testing, by accident.

Hackers have computer aptitude, but the difference between hackers and intelligence collectors is that the latter have a *process* and support from other resources, e.g., to obtain network diagrams, etc.

The *process* begins with *requirements*. Requirements feed into collection, collection feeds into analysis, analysis feeds into evaluation, and evaluation causes new requirements, in a cycle.

Very interesting story about social engineering a nuclear reactor building company. I missed the first part of the story, so I will go back and hear it again. Getting into the plant, getting badges, distracting the auditors, getting access to `/etc/hosts` and so on. Ira Winkler's speciality is social engineering nuclear power plant designs.

Intelligence agencies start security awareness training on the first day. You can never have enough awareness training. It is critical. It tells people what to look for. Better to have thousands of people running around as little intrusion detection systems than just a few security guards.

Potential loss should drive the security budget.

$$\text{Risk} = (\frac{\text{Threat} \times \text{Vulnerability}}{\text{Countermeasures}}) \times \text{Value}$$

Ira Winkler: 'The only way to get rid of all risk is to get rid of all value. The goal of an infosec professional is to have as much risk as you can possibly tolerate.'

'You can't mitigate threats. They are outside your control. You can only mitigate vulnerabilities.'

References