Social Networking: Insider Threat or Threat to the Individual?

There's no statement as true as "Better the devil you know, than the devil you don't". In today's society it would be remiss of any Subject Matter Expert (SME) or data owner to not accept that, arguably, the biggest single risk to our information assets is the user - also referred to as the insider threat. But what can you and/or your organisations do about it?

Let us forget the Hostile Intelligence Service, Aggressive Journalists, Industrial Espionage, Organised Crime types and other Threat Sources for now (they will come into play later). Predominantly they all have something in common in that they require someone or something to facilitate access to the information in the first instance. This often requires a long game strategy including finding motivation, capabilities, target acquisition, social engineering, financing, support, logistics etc, etc.

However, in an era of global austerity measures, redundancy, personal financial instability and the unsure future of our countries' economic status' we are faced with higher risks from disgruntled employees or opportunists, driven by their own moral values who would exploit our information giving it freely to the likes of Julian Assange's WikiLeaks.

The recent scenario with Edward Snowden is probably a timely reminder that this threat is very real. Time will tell whether his reasons were truly those of moral virtue or in fact there were underlying motives. It has been reported[1] that he took the job as a contractor Systems Administrator to specifically gain access to this information. However, routes to the public audience with such information are far easier than Snowden's globetrotting efforts. Albeit the price to pay in his case is probably amongst the most severe on the planet, and it is therefore slightly understandable why he has gone to such lengths to secure himself a safe harbour from extradition.

For most, though, in modern society it is easier to blog, Tweet, Facebook or post it on one of the many other social network forums and paste bins out (As per Anonymous and associates) in the WWW, let alone provide it to any of the fore-mentioned Threat Sources for a myriad of other reasons.

So what do we know about our current or future employees? Within Her Majesty's Government (HMG) they have the use of the National Security Vetting (NSV) services who conduct background checks relevant to the level of access the individual requires to information assets. This will include checking referees, finances, Criminal Records, identity fraud, personal interview and, in extreme circumstances, cross referencing to other Government Departments. Yes, Snowden was a US NSA security cleared contractor and the risk was still realised. But, I'm sure at this very moment the NSA are analysing the lessons learned.

It must be noted that vetting alone should not be the only control against a risk of information breach from an insider threat, but the purpose of this paper is to look at what we know about these individuals to whom we give, sometimes very uncontrolled, access to our information.

[1] South China Morning Post

In the private sector, where there is no access to HMG vetting agencies, how should we tackle the problem? There may be legal obligations to conduct Criminal Records checks in some circumstances (working with children and vulnerable persons), but every employer should follow up referees and previous employers, some organisations even do rudimentary checks on the social networks. But investigation of the internet, data mining, analysis and subject profiling is not the pre-requisite of most, if any HR departments. For most Police Forces and Intelligence Organisations this requires specialist training, it is therefore understandable that as a routine practice commercial organisations may not see the requirement.

But what about exceptions to the rule; what about when you're employing individuals who you will effectively be giving the keys to the kingdom? In these circumstances would it not be sensible to ensure that checks go further than just the routine? HMG have Developed Vetting (DV) status for this very reason. It would therefore be equally prudent for commercial organisations that experience a major security breach from a trusted individual to review their vetting processes and revisit those key individuals who have access to or hold the organisations most sensitive information and conduct a more in depth check.

When reviewing an individual's background there are other areas of risk to be aware of, the risks to brand and reputation. These risks are presented to your organisation from the day to day social network activity and web presence of the individual and not through information breaches. The how, why and what have long been discussed in security white papers and forums over the years and on the whole have been addressed by the fairly common introduction of Corporate Social Media and Acceptable Use Policies.

From a vetting perspective the key to understanding the risk from the individual goes beyond the questions of;

- What do your employees really think about their employer?
- How and to whom are they expressing their feelings?
- Or, is the clean cut individual who was sat at the interview really as clean cut as the image they portray?

You also need to understand the risk the individual presents to themselves; are they making themselves an easy target to be approached. What are their true allegiances, can this be exploited?

If you were a multi-national organisation would your business interest best be served by an individual who spends their weekends going to rallies opposing major global political issues? Do their activities potentially put them at cross purposes with the authorities? Are they members of Social Network Groups that could provide Threat Sources with an indicator of their worth from an intelligence point of view i.e. a member of a Security Advisory Council or Security Cleared Job forums? These are just a few of the areas of concern and only begin to scratch the surface of the problem.

When a Threat Source is looking for an angle of attack, be it motivation, weakness or opportunity all of this information is out there for the gathering. Google is constantly expanding its foot hold on the WWW and with it, pooling information together to form one holistic database of information that can be mined and used to gain advantage; they are not alone in this.

Do you look for this information and more importantly do you know where to find it? What do you do if or when you find it? If it is a new employee with an excellent reputation, say in Business Development, but has a high risk Social Media and web presence, do you avoid them or not? An existing employee with a proven record managing your IT assets and system administration but on review they also have a high risk web presence, how do you handle the risk? Having the information is to your advantage, and using this in

mitigation for managing the risk should be a Board level decision, but at the very least it must be a well informed decision. Within HMG, information known about an individual is used as a tool to mitigate risks associated with their personal, financial circumstance etc. If an organisation knows everything about an employee and the employee concerned is informed of the fact[i], then Threat Sources have a difficult time using this to gain an influence with that individual.

Outsourcing this level of vetting to an organisation with the capabilities to do the in depth investigative and analysis work may not be a cost effective solution when it comes to all employees, but for those key individuals who hold or may hold higher privileges or access to more sensitive information within an organisation this could be money well spent and save money and angst in the long run. The current maximum fine that can be imposed by the Information Commissioners' Office for an Information Breach is £500,000. The cost to an organisation's brand and reputation is often immeasurable.

When you next compile a personal appraisal on one of your key employees, ask yourself, what do you know about them? Then ask how much you don't know. Are they a risk to your organisation and/or a risk to themselves as an easy target for compromise by an external Threat Source?

[i] The individual as part of any vetting process should be aware of the information you require and why you require it, along with the fact that you will corroborate that information via other means and that all this information will be protected accordingly.