Tool Talk Blog#11 – Security

Years ago I had the pleasure of being the guest editor for the Telecommunications Journal of Australia, where the theme was internet security. Amongst the many articles written was one by an author friend "Dez" based on a hypothetical "little Johnny" and the ease of which he could get around the supposed security. The message was clear (if not a little scary), security is less about technology and more about human nature.

Security in relation to EPM/PPM tools comes in many forms:

- The hosting and network environment
- The encryption within the browser and PC security (e.g. no malware)
- The authentication of the user
- The role based security settings of the user (which determines what functions the user can use)
- The structural based security settings of the user and/or the projects (which determines what the user can see, add and/or change)
- The management of physical and electronic reports

One experience from a previous project I had worked on for an un-named organisation, where thousands had been spent on firewalls and security experts to create a completely secure environment. But then all PCs provided to people within that environment had active USB slots plus allowed browser based Email anyway.

Another experience from a previous project I had worked on, was where extensive designs were done for user and structural based security settings but everyone just logged in as the same super user so they could see/do everything. From memory the user had not worked on the project for months.

And yet another was where there were excellent security settings within the EPM/PPM tool but then all the commercially sensitive portfolio summary reports were made available via an open access SharePoint site and emailed around internally and externally. Add to that the executives giving their admin assistants their passwords and full access to systems anyway. Or others keeping usernames and passwords on sticky notes on their screens or providing to their colleagues. It's no wonder their IT security is at risk.

We have been seeing the emergence of simple to configure Software as a Service (SAAS) based EPM/PPM tools for some years. These offer great, cost effective solutions but do have a perceived security risk due to the reliance on a third party for security. We have seen the emerging fear, which comes quite sensibly, from hosting sensitive company data on a third party's infrastructure on the internet. Some organisations, e.g. Defence, Banks etc. will not consider them. There are too many stories of systems and data on the internet getting hacked to take security lightly. Despite the cost impact, many companies prefer to keep their data behind their firewall.

We are also seeing the emergence of social networking and collaboration technology such as LinkedIn, Facebook etc. Keeping data, analysis and ultimately knowledge secure requires people to adopt a security focus. Not to discuss certain things, not to share certain things, be wary of innocent questions from strangers. Keep passwords for social sites quite different to work related sites. These are all basics which align with adopting a security focused culture.

Back to my author friend Dez, he would argue that through one or more phone calls and a bit of research, using credible names and stories, he could convince people to give him access to just about anything. With the analogy to the security on your house, his argument was that you make the systems as secure as you reasonably can, but do not think they are ever 100% secure. He argues that you should put your energy into educating the users on security and make it as easy as possible to be secure.

So if you are working in the PMO space, and are considering Enterprise Project Management systems, keep them simple. Try your hardest for single sign on (e.g. using pre-existing user authentication). Do not go overboard with structural coding systems. Be careful where you publish aggregated reports. Have a diligent security custodian, a super user who can assess access requests and provide necessary access to data and functions. Be careful who provides the IT support and has access to the backend data and backups.

In the back of our mind we all probably think that if someone wants to break in they probably will. Still, it does not mean we do not lock the door and do our best to make things secure.

martin.vaughan@coreconsulting.com.au