

## The Tweety Bird Got Ate

The U.S. Department of Defense is banning Twitter. All social networking. Or trying to. Or maybe not. The debate is on.

The same pro and con arguments that affect the defence establishment are currently the source of many debates within countless private and public organizations that have concern for their own security.

You know that Twitter, Facebook, LinkedIn and an endless gamut of social networking sites are relentlessly popping up... and too many companies are merely treating them as the latest exercise in Whack-a-Mole security.

There are two fundamental issues to be considered by Enterprise policy makers when attempting to decide whether 'To Tweet or Not to Tweet'.

1. Technical
2. Human Behavior

Technical issues abound. Like any 'new' (communications) technology, security is the last item to be addressed – often years after deployment. *"We can deal with it later."* *"It's not going to be a problem."* Apathy and arrogance. In 1987 I was working with groups to have security embedded into cell phones, at a cost of less than \$1, yet that never happened. *"Too expensive."*

Secure O/S for PDAs and cellphones? Barely. We've seen desktop security problems extended to every increasingly intelligent function-based end-point device we can come up with and there is no hint that the vendors are doing anything other than push the problem forward in time so the next administrator can deal with it: ignorance is bliss, security be damned.

Of course, it is fairly simple for any decent administrator to block the 'offending' sites, traffic patterns and other work-arounds from the enterprise desktop. But this action might cause user reaction encouraging them to learn how to bypass the controls. However, such breaking of policy should be detectable, triggering Hammerabi-like retribution. Right?

The Brits are taking the typically British approach in the Ministry of Defence policy document, DMC-PR-05-07-02 dated 5 August 2009. Be smart. Think security. Follow opsec... and so on. They are empowering the defence establishment to do the right thing... and if they notice something wrong, report it.

But that flies in the face of the recent revelations that the wife of Sir John Sawers, the soon to be head of MI6 (their version of the CIA), published personal details and photographs on her Facebook page. Lady Shelley Sawers disclosed extensive compromising information about her own family, including their children and parents, as well as friendships with famous public figures, entertainers and controversial diplomats. Mrs. MI6 placed no privacy protection on her account, allowing any of Facebook's 200 million users in the open-access "London" network to see the entries.

The question becomes one of human behavior: how do you control it? One of my colleagues says education is the answer. After 25 years of awareness, training, and attempting to educate the non-technical masses and inculcate the most basic principles of cybersecurity into their behavior, I have to disagree.

A recent study into corporate security cultures showed that from 22-45% of a given enterprises's staff will in fact respond to social engineering attacks such as phishing, despite extensive awareness training. Another study showed that 16% of those surveyed admitted to responding to spam e-mails, largely due to curiosity – which apparently outweighs any security concerns.

The answer is ... you need a good, strong, well thought out combination of technology and education as the foundation of any security effort. The problem is two sided and the solution must be similarly comprehensive.

So, when you think about allowing access to social networking sites from enterprise equipment, the first thing that should come to mind is the risk it presents to your company, your image, your customers, your compliance and governance requirements and personal privacy. Do any of the increased risk factors raise the possibility of data breaches, or any other untoward security event?

Only you can determine that.

- Do you have enough internal technical controls to detect what is being said on social networks, how it may influence your company and react in a timely manner? Think deep packet inspection.
- On a scale of 1 to 10, how much faith do you place in your trusted employees to follow security policy and make smart choices 100% of the time? 90% of the time... which means 10% of your employees will screw up some of the time.
- Do your employees ever make errors? Cut and paste or comment on the wrong chat window?
- Is there a compelling business need that your company needs social networking to succeed?
- How much good will you build with your staff by allowing social networking? Internal only or external exposure?
- If you allow one social network, do you allow them all?
- Should you instead provide public kiosks, not connected to the company networks, and allow staff to use them on their own time... not on your time?
- What are your personal company-resource use policies and do you want them to extend to social networking?
- Does your public relations or marketing department regularly use social networking tools? Can anyone else?

Me? Public is public. The DoD should keep its affairs private and enforce them with overwhelming security controls to prevent unintended disclosure. I agree. The MoD made a different choice... so far.

Now, you need to make your choice before the choice is made for you.