Behind the WikiLeaks furore, there's a much bigger issue at stake: America's slack approach to information security. The UK national interest lies in demanding that the USA act to stop its government computer systems being breached time and again, and in reviewing British data security as well.

Dec 16 2010

American elites have fiercely denounced Julian Assange and WikiLeaks for the latest, and largest, release of secret documents, covering over 250,000 diplomatic cables. And with the notable exception of an unfazed Ken Clarke, British elites (both Conservative and Labour) have rushed to follow suit. Yet ***Jerry Fishenden*** *argues that it is not WikiLeaks that the UK and world publics should be worried about, but instead very poor information security in American government.*

What a week it's been for WikiLeaks, which finds itself and its founder Julian Assange at the centre of a concerted, sometimes histrionic, barrage of criticism for publishing leaked US government information. But we should not allow ourselves to be distracted by all this diversionary heat and noise: there's a much more important issue at stake here. For the US government to lose one set of secure information in this way might be regarded as a misfortune. But for its computer systems to be breached time and time again begins to look like carelessness.

The "WikiLeaks affair" exposes an apparent malaise in the US government's approach to information security. It suggests that the US government has few if any of the defence in depth measures in place that would normally be used to protect secure computer systems. The US government has often been quick to criticise private companies who fail to protect customers' privacy and data – on the back of high profile examples over recent years such as the theft of around 100 million records from the TJX group of companies, CitiGroups' "loss" of some 3.9 million customers' details, and the breach of 40 million Visa, Mastercard and American Express records.

Image Credit: Wikimedia Commons

Yet WikiLeaks allegedly obtained its information from a US army private who could freely access and download information from a "secure" government computer system. And if a US Army private could access and download such sensitive information, he's unlikely to be alone in having done so. It would be surprising if overseas regimes and organisations have not been busy exploiting such lax security for years. To focus on WikiLeaks is to miss the point.

The current leaks from US government computer systems imply a catalogue of failures across multiple levels – risk management, access control, confidentiality and cryptography, to name a few. Collating information into a single place was always going to create a significant security threat. It's a fundamental tenet of computer security not to aggregate and store all of your sensitive information in one place. Best security engineering design operates on the assumption that at some stage computer systems will be breached, whether that breach results from insider or outsider attack, and whether because of negligence or malevolence. Yet there appears to have been no layered defence within the US systems: once inside, users appear to have been offered unfettered access. And far too many users seem to have had access in the first place. These are all such elementary failures of security that they would deeply embarrass even an undergraduate computer science student.

This poor level of security engineering in the intelligence and defence sectors is worrying. It suggests some potential cross-contamination from the civil sector, where governments have been progressively promoting bad computer engineering practice, pushing for massive centralised databases that contain more and more information. Here in the UK we've seen examples that include the UK identity card register and the national

children's database, based on the naïve and dangerous premise that compiling large quantities of sensitive personal information into computer systems would somehow better protect us rather than exposing us all to an increased level of risk.

Now it seems as if the US government has taken ideas that were ill-suited to the civil domain and applied them in the military, diplomatic and intelligence domains. No-one should claim to be surprised by the outcome. There's also a deeper and more troubling issue here: poor US government computer security is not a new problem. For example, amongst a catalogue of other breaches, in 2006 some 26.5 million records were stolen from the US Department of Veteran Affairs. WikiLeaks may in fact have done the US a big favour, highlighting on a worldwide stage the inadequacy of US government computer security. Provided, of course, that someone now knuckles down to fix the problems instead of merely berating WikiLeaks.

Then there's the ongoing case of Gary McKinnon, currently being requested for extradition to the US to face potential prosecution for allegedly hacking into secure US computer systems. McKinnon, you may recall, is alleged during 2001 and 2002 to have breached the security of nearly 100 US computer systems. McKinnon however claims that he found the systems (including those of the US Army and Department of Defense) open, inadequately secured with either no passwords or with default passwords, and with none of the expected defence in depth that is usually mandatory for sensitive systems.

All of which raises the question of what has been done by the US government since those earlier high profile incidents to address their security failings? Has there been any investigation and prosecution of those responsible for failing to properly engineer, operate and safeguard sensitive systems? Some 8 or 9 years since the alleged acts of McKinnon, here we are witnessing yet another high profile example of information accessed in "secure" US government information systems. On the face of it, no lessons have been learned and no improvements made during the last decade. So why shout noisily at the publishers of such information if you're not prepared to fix the root cause of the problem?

Closer to home, the UK government's national security adviser, Sir Peter Ricketts, has requested Whitehall departments to review their current computer security. Something that should be a routine, regular process in any case. But that alone will not go far enough; it's the quality of US government computer security that should also concern us at the moment. The UK and US governments share a great deal of sensitive information about common interests, from the interception of terrorist communications to intelligence insight. Weaknesses in US government systems are a threat to the UK too.

The UK government should demand, in public not just through covert channels, that the US government takes immediate, effective action against those responsible for these systemic failures of security. We need credible assurances that UK interests will not be damaged by further inadequate computer security. Those responsible for the US government's approach to information risk, and who should have implemented rigorous defence in depth, must be subjected to a thorough independent investigation. And, if found negligent, prosecuted in a criminal court. The US government must hold itself accountable to the same high standards as it expects of others.

If meaningful action is not taken now it is only a question of if, not when, UK interests at home and abroad will be placed in serious peril by yet more damaging disclosures from the other side of the Atlantic. Unless US government information security is rapidly improved, the next breach of its systems could make the current media storm about WikiLeaks look like a minor ripple in a teacup. So let's move on from WikiLeaks. There is, after all, a much bigger and more important issue at stake.

Click here to respond to this article.

Please read our comments policy before posting.

You may also be interested in the following posts (automatically generated):

1. In Post Office privatization, fair regulatory rules can protect service levels and stop the excesses of previous privatizations
2. National security concerns continue to dictate Britain's government aid and development agendas
3. Wikileaks: an example of 'new' and 'old' media collaboration. But does freedom of expression trump diplomatic confidentiality?
4. Government productivity in UK social security has not grown across two decades to 2008 – largely because DWP senior civil servants blocked any move to 'digital era' services