Some Comments on Cyber-Threat Readiness

Greg Baker (The Institute for Open Systems Technologies Pty Ltd)

Summary

This document is IFOST’s submission to the 2015 Defence White Paper and is mainly concerned about the readiness of Defence to handle advanced cyber threats, and what organisational additions could help to protect against them.

The opinions expressed in this document are meant to be unusual and disturbingly different, but also attempt to provide a serious input to the white paper, particularly around the CIOG’s strategic priorities.

- Defence can and should aim to be **nationally autonomous** for operating-system level software.
- Using **industry best practices for IT management** probably won’t fit perfectly with Defence’s mission.

Cyber Threats and the CIOG

It is possible that Defence should take more of a stand on protecting Australia’s critical networking infrastructure outside of Defence, but in this document I’m more interested in discussing how Defence could protect itself better from cyber warfare by looking at organisational structures.

I would presume that Defence have already examined serious cyber threats (e.g. hacking into secure communications channels, and so on). But I think that’s not quite enough. If Australia were in a state of war with a major power, then it will be worthwhile for our enemies to disrupt even very unexciting infrastructure (e.g. payroll, or email access) that is handled currently by the Chief
Information Officer’s Group. An unpaid army out of contact with family and friends is less effective. So we need to consider securing even “ordinary” ICT infrastructure.

The Missing Directorate of Open Source Deployment and Security

Looking at public sources of information (e.g. job advertisements), it seems that Defence make extensive use of Microsoft Windows for both desktop and server roles. This is surprising, and makes Defence exceedingly vulnerable. It is well known (e.g. from the Snowden leaks) that many agencies in the world stockpile vulnerabilities against Microsoft operating systems and applications. While it is possible for an organisation the size of Defence to get access to Microsoft’s source code, it’s unlikely that Defence could hire more than a handful of staff with any experience of working with any large portion of it.

This makes Defence a sitting duck for cyber-disruption. Defence has a major dependency for its day-to-day operations on programs whose security can be violated easily, and for which Defence is heavily dependent upon overseas experts (who would be more than likely heavily occupied by the own country’s needs in this kind of situation).

Using Linux would improve this situation, as there are generally less vulnerabilities on Linux systems and (more importantly) there are many, many Australian citizens who have deep familiarity with the Linux source and could be called upon at short notice in a time of crisis.

Personally, I think that Defence should be running as much as possible using OpenBSD instead of Windows. OpenBSD is an open source Linux-like system which has been developed and audited to be highly secure. While there are fewer individuals in Australia with deep source-level knowledge of OpenBSD, there are still quite a few. I’ll admit that I’m biased -- IFOST was historically the largest OpenBSD consulting company in Australia.

Here’s what I think should be put into the Defence white paper. Defence should aim for 98% national autonomy and self-sufficiency in at least the desktop, server and tablet operating systems in use by 2020. There should be a Directorate (or some higher structure) tasked with compiling the Defence-chosen operating systems from source, not just assembling binaries supplied by vendors. This Directorate should also have responsibility for auditing that source code for to make sure that it cannot be subverted, and for fixing security problems in the source that are found. There will also have to be major projects dedicated to the replacement of the existing insecure infrastructure.
Cyber-Threat Readiness

98% just seems like a reasonable number, and we are unlikely to face a major party threat before 2020. There may be odd cases where it is more sensible to use a commercial operating system, particularly if there is some legacy software involved. Isolating 2% of Defence’s computing fleet in the event of a threat is a large, but plausibly achievable goal.

I should add that a number of vendors will be very, very unhappy with a goal of national autonomy, but I believe IT software self-sufficiency is in the national interest. In general, IT hardware self-sufficiency is less important.

The Missing Directorate of IT Sabotage
Again, looking at job advertisements, it is now public knowledge that Australian Defence in general has been adopting ITIL -- a group of industry best practices for running ICT -- for some time. Many other national defence organisations have done similarly (e.g. the UK, the USA).

One of the best practices suggested by ITIL is the development of careful change management processes to minimise the number of major incidents. In other words, every new computer or program and every modification gets carefully tracked and approved by a change advisory board with a view to making sure that it won’t cause an outage.

It’s a truism that whatever you do a lot of, you will get very good at; and what you don’t practice, you will do badly.

So if we keep the same structures and processes, Defence will be very well placed to implement new systems very reliably and cost-effectively. Defence will be good at implementing structured and planned changes. Unfortunately, it will also mean that Defence will be very inexperienced at dealing with unexpected outages and other incidents.

For commercial organisations, this is quite acceptable. Major outages have a cost; having as few as many of them makes cost-effective sense, and the extreme outlier situations (e.g. hackers breaking in) can be insured against.

But for Defence, I see this as a serious short-coming. Every part of Defence needs to be able to respond to every kind of existential threat. A successful cyber attack will require flexibility and spontaneity to respond to the outage. Quick thinking, communication across teams, access deep into the technical stack of other groups: these are the skills which get developed in chaotic change management. This is precisely what Defence will not have.
I’m not sure what the resolution for this should be, as the obvious answer is very odd. It seems that perhaps there should be a Directorate whose responsibility it is to build up Defence’s capability to respond to major incidents; the only way to be sure that Defence can deal with a threat to “minor” capabilities like payroll and email is to disrupt them and measure the response.

This leads to the very strange conclusion that Defence should be creating an internal group that has the right and responsibility to sabotage all of Defence’s own internal IT systems.

This is obviously silly, but it’s equally true that the current approach of minimising IT’s staff experience of dealing with unexpected change is setting Defence up for failure.

About
Greg Baker (gregb@ifost.org.au) is an Australian author, consultant and programmer who is known for his writings on data protection and ITIL. He is the director of the Institute for Open Systems Technologies (Pty Ltd), a consulting, training and development company based in Sydney.

He consents to have this document published on Defence’s website either named or anonymously.