THALES

Keeping secret data secret

Thales UK is trusted by organisations across the private and public sectors to deliver secure network communications. Even with the most senstive data it is essential to be realistic about how to protect it, says Account Director for Government & Commercial, Ross Parsell.

> *"The future will be putting your security guard on data up or down according to conditions, just as the physical security guard has different stages of readiness depending on circumstances..."*

It's a long way from the deserts of Iraq to Julian Assnage's self-imposed siege in central London, but the chain of events involved perhaps shows the ramifications of what can go wrong when secret data turns out to be insecure.

The deluge of information released by Wikileaks as a result of the actions of one disaffected American soldier is an extreme example of this phenomenon, but the dangers are obvious: if something can be copied and pasted it can, in principle, go anywhere.

Ross Parsell, key account director for government and commercial at Thales, and an expert in cyber security, says data held by the Ministry of Defence or other national secrets, needs to be protected in the same way that physical secret documents were in the past.

Barracks and bases have high walls round them, and guards on varied states of alert at their entrances. This is the model to follow in the electronic age.

"There is always a residual risk because the bad guys move very fast and you are never going to have 100% protection," he explains.

"So the residual element of risk that is acceptable is going to depend on the risk appetite of the organisation.

"Clearly with the MoD or anything to do with national security that appetite will be very low."

To make the residual risk as low as possible data will be encrypted, something Mr Parsell says the MoD "is very good at and its people are used to doing".

Many of them work on a base or barracks that that they seldom leave and so are security-minded and, "it is not like civilians taking work home with them.

"There are high walls and nobody is going to physically get in, and it has a similar attitude to encryption to build walls round its data."

The MoD estate is changing with more civilian contractors being used, who do not necessarily have the same attitude to security "so there is a need for a culture change piece there and for education in handling information," he says.

Prevention – stopping data from going where it should not – is obviously vital, but Mr Parsell says this is not enough on its own: "The main dimension to be speeded up is detection and response and to be pro-active rather than just protective, because if you lose information it is gone," he says.

It is however, important to know what information to protect tightly and which it would be regrettable, but not disastrous, to lose.

Mr Parsell says: "The Wikileaks leak showed what can happen when the systems work but there is one disgruntled individual who sends information outside them.

"To one extent there was a positive in this, in that the leaks caused some embarrassment but governments kept talking to each other and the world carried on.

"It showed us whether we were protecting the right information and whether it was actually that important."

Wikileaks could have led to worse consequences and Mr Parsell says human resources teams will need to learn to look for disaffection and intervene to prevent those concerned from doing damage.

"There is a culture and education piece to do with those people," he says.

To detect problems, commercially available detection protocols will look for unusual things going on.

"The skill is looking for changes and anomalies," Mr Parsell says.

"For example, if I were monitoring I might say 'I have seen a change in the type of traffic, should this kind of information being going out through a firewall at midnight."

He adds: "The future will be putting your security guard on data up or down according to conditions, just as the physical security guard has different stages of readiness depending on circumstances and can be raised or lowered according to threats, you would move to higher or lower levels of encryption, depending on circumstances."

Then comes the part that few see. Once an attack has been detected, a response will be prepared.

"Once you know that something is criminal you can go back to find the source. That may involve the police or national security and they will decide what action to take."

Just as anyone in an office will be familiar with the idea that the IT department can 'take over' their computer to fix a problem, so IT security can remotely take over computers on which improperly removed confidential government data is found and recover it.

"These are the dark parts of IT! Little is heard of it in public," he says.

Mr Parsell says there is no need to assume IT is insecure and so not fully exploit, nor to assume that it is secure and disregard the dangers.

"We still have some way to go to use IT to be more efficient and effective," he says.

"At the moment we are still burning things onto CDs and printing them off. The way of the future is use electronic data more."

To find out more about Thales UK's security solutions, visit:

www.thalesgroup.com/security