

Tinker, tailor, soldier... cyber-defender?

We've come a long way since the 1970s.

When Le Carré wrote *Tinker, Tailor, Soldier, Spy*, the East and West were locked in an expensive and dangerous game. Spies like Smiley's roamed the world, gathering state secrets for their masters.

Today, we're locked in a very different conflict – one between cyber-criminals, cyber-terrorists and state-sponsored attackers on one side, and IT security specialists and cyber-defence teams on the other. Costs are escalating – a report produced for the Cabinet Office estimated the hit on the British economy at £27 billion a year – and spies are back in vogue. The costs of intellectual property theft and industrial espionage alone were projected at more than £16 billion a year.

The tabloids may focus on teenagers hacking into highly-secure IT systems from their bedrooms, but this is clearly just a small part of the problem.

Look deeper and you get an entirely different picture – one in which criminal 'firms' are emerging and operating on an industrial scale. While teenage hackers do the equivalent of spraying graffiti and breaking windows, these professionals are getting away with organisations' crown jewels. There is even talk of them having developed specialised operating systems for their computers – things analogous to Windows, but tailored to their illicit tasks.

So what can be done to counter this growing and increasingly serious threat? One thing that's certain is that traditional ways of defending organisations against attack are unlikely to be enough.

Organisations have tended to take blanket approaches to information security. Some have tried to protect everything against every imaginable threat – sometimes at tremendous expense. Others have spread whatever they can afford evenly, hoping it would be enough to keep attackers at bay.

Compounding this, the emphasis has been on countering individual attacks. People and technologies have been deployed based on their type and severity, rather than on their impact on the organisation concerned.

To meet today's threats, a much more sophisticated and much more strategic approach is needed – one that matches investments in security to factors like the value of assets and levels of risk.

The first step is to define what we call a 'risk appetite' – the level of risk you're prepared to take in each area of your operations, from your interfaces with the outside world to the inner sanctums that hold your most valuable assets. That done, you can start to think not just about the defences you need to put in place, but the processes you need in order to deliver the levels of security policy you need.

To help organisations put such strategic approaches to security in place, we've developed a Cyber-Defence Managed Service (CDMS). A flexible solution, it includes everything you might need – people to help you investigate and understand the risks you face, processes from threat correlation and analysis to incident reporting, and best-in-class technologies that will keep watch over access to your networks and IT systems and flag any abnormal behaviour. The aim is to come up with measures that are effective, tailored to your situation and financially appropriate. CDMS delivers real-time insight into the threats facing organisations and also allows them to continually monitor and model potential attacks to their key systems. This enables organisations not just to react to ongoing attacks, but to be prepared in advance and proactively manage down the risks that they face.

CDMS has its roots in a cyber-security solution called eCND (enhanced Computer Network Defence) that went into service earlier this year. Developed by experts from BT and the Ministry of Defence, it protects the ICT systems on which Britain's Armed Forces depend.

Attempts to access the MoD's networks and IT systems had been becoming more frequent, more complex, better coordinated and ever more difficult to detect. To give an indication of the scale of the problem it faced, in June 2011, then Defence Secretary Liam Fox said that the MoD had detected and blocked more than 1,000 "potentially serious" attempts to infiltrate or disrupt its computer systems in 2010.

The organisation was finding it increasingly difficult to respond. Equipped with an array of different ICT systems from different suppliers, the MoD is responsible for thousands of devices worldwide. It had become difficult, time-consuming and expensive to manage and maintain the armoury of security mechanisms used to protect them.

To move forward, the MoD needed a centralised, business-driven security capacity that would adapt quickly as the threat landscape changed. To truly protect its infrastructure, it needed an intelligence-led approach – one that could use information from a wide range of sources to help it outwit and outflank attackers.

“This capability makes a real difference. It means we can successfully complete work that previously took around two weeks in less than 30 seconds”

Member of the MoD Information Systems and Service (ISS) organisation

A wide range of stakeholders – from CIOs, their peers to information security specialists – was involved in eCND's design and configuration. Based on Commercial Off-The-Shelf (COTS) components, it meets not just exacting national criteria but the MoD's more-stringent requirements.

Centralised processes monitor and correlate feeds from many different systems to identify anomalous behaviour that could indicate an attack. The results give cyber-defenders a real-time view of the MoD's ICT estate and make it both easier and quicker for them to decide where and how to adjust defences as new threats emerge and others evolve. And when we say quicker, we really mean it. Tasks that used to take two weeks can now be completed in just a few seconds.

To find out more about BT's Cyber Defence Managed Service, contact your account manager or visit www.bt.com/defence

