OPINION PAPER

Cyber Security

Is your house in order?

Delivering Transformation. Together.

sopra steria

What does Cyber security mean, and what should you be doing to ensure your enterprise is in good shape to deal with a journey down the information super-highway? Sopra Steria's Business Development Director Secure Systems, Alan King, shares his views on what organisations must do to combat the Cyber threat.

It seems that 'cyber' is the latest buzzword to catch the imagination and many organisations are jumping on the bandwagon. Hardly a week rolls by without a conference or a new product hitting the streets.

Both professionally and privately, we are increasingly more aware of the value of information, and why others might want to get their hands on it, using fair means or foul. No longer do memory sticks seem such a good idea. They are nice convenient data storage and transfer mechanism, but what happens if a memory stick is lost? Another question we continually ask is 'could a virus find a way around my firewall?'.

'Cyber' can mean many things to many people. In the wider context, anything from robots to genetic engineering, but in the IT world, not much more than good old Information Assurance (IA), plain and simple. Well, why all the interest and why should I be worried? The world is changing all around us. Data is an increasingly valuable commodity, bought and sold in just the same way as raw materials have been for decades. Data is the fuel for business intelligence which drives competitive advantage. Clearly then, data needs to be managed effectively, and in cyber security terms this means keeping the bad guys out and keeping the data where it is supposed to be.

A best practise recommendation is to look at things from a risk management perspective. This means taking a holistic assessment of the likelihood of your data being stolen on the one hand, and lost on the other. The process is known as Information Risk Management (IRM). Loss of data, for whatever reason, can be bad news; it translates into either loss of intellectual capital, reputational damage, or both.

What do I do before I begin my journey down the information super highway? Probably the best place to start is with an IT Health Check. This is a semi-formal process designed to assess the vulnerability of an IT system and its components. However, for information to be assured, this is not just about the tin and string; it is about the people, the process and the technology. Remember that the system is only as good as the weakest link, and the hacker's job is to find that weak link and then to exploit it.

The Weakest Link?

An interesting recent development is the use of social engineering to gain (un)fair advantage. People are waking up to the fact that if you publish something on the internet, it is there for ever. Something said today in the exuberance of youth may not be your finest hour in the future. Indeed the whole issue of privacy settings on social networking sites has come under the spotlight recently as it has not been very clear who has access to what, and sensitive information may have inadvertently been released to the wider world.

In the same way that the anti-theft system on a modern car has become so sophisticated that criminals sometimes resort to other methods to obtain the keys, a determined hacker can socially engineer his way into the network. It is not always the case that a strong, regularly changed password provides the only way into the network; single sign-on, as it is known, is the 'Holy Grail'. However, in the fast moving world of growth by acquisition, IT systems are constantly being merged, updated and renewed. Additionally, pressure on IT budgets means that IT systems may be joined, but not integrated, leading to more passwords and more potential entry points. Great steps in the right direction can be made to promote awareness through proper education and staff training to encourage best practise.

Promoting best practise against a rising tide of cybercrime

Another common lesson learned from IT Health-checks is the importance of installing software updates in a timely fashion. Far too often, system patches are not applied when they should be; leaving any inherent vulnerabilities in the system to be found by anyone who may wish to exploit them. Deployment of system updates can be an onerous, time consuming activity for the system administration team, who, without suitable automation, resources or foresight, simply fall behind the curve. Sometimes, systems simply grow like Topsy, with new components added, unbeknown to the original designer or system administrator. This leads to an inconsistent build profile, which is very hard to manage.

The problem is actually much wider. The use of domestic wireless enabled networks is growing; and conceivably the hi-tech burglar doesn't even need to get inside the house anymore as the network can be accessed some distance away. Then there are 'Trojans' that hide inside seemingly innocuous files, e.g. Adobe PDF, but instead contain malicious code that can perform very undesirable operations. Web browser malware also continues to rise and even if the website appears genuine it may well not be.

The Sopra Steria way

Sopra Steria has been providing IT enabled business solutions for four decades. Assuring the integrity of client information is the cornerstone for the range of services that we provide, be it Business Process Outsourcing (BPO), IT outsourcing (ITO), or Applications Portfolio Management (APM).

As a vendor neutral systems integrator, we are very well placed to offer impartial advice on building, supporting and maintaining information systems. Services offered include early lifecycle ngagement, such as advice from our CLAS (CESG Listed Advisor Scheme), policy advice on implementing standards such as ISO 27001 or the new Information Assurance Maturity Model, and down-stream services such as governance review, compliance and audit.

We also recognise that people, education, attitude and culture play a vital role in information assurance and our in-house team, Sopra Steria Learning Services, can provide classroom training aimed at improving IA maturity.

We recognise that one size does not fit all. Information risk management is at the heart of our approach. We take a pragmatic approach, following best practise CESG guidelines, aimed at protecting information at each stage of the system lifecycle.

We recognise that one size does not fit all. Information risk management is at the heart of our approach.

About Sopra Steria

Sopra Steria, European leader in digital transformation, provides one of the most comprehensive portfolios of end to end service offerings in the market: Consulting, Systems Integration, Software Development and Business Process Services. Sopra Steria is trusted by leading private and public organisations to deliver successful transformation programmes that address their most complex and critical business challenges. Combining high quality and performance services, added-value and innovation, Sopra Steria enables its clients to make the best use of information technology.

SOPRA STERIA
Three Cherry Trees Lane, Hemel Hempstead, HP2 7AH
+44 (0)370 600 4466 - info.uk@soprasteria.com

www.soprasteria.co.uk