

Business must join rivals to fight cyber terror

Like it or not, business has been drafted into the frontline of the nation's defence and now has the difficult task of securing Australia's critical infrastructure.

In effect, companies are being asked to put aside commercial rivalries and share information freely in order to defeat threats ranging from cyber-sabotage to e-crime.

"These are extreme and testing times," Attorney-General Daryl Williams told business representatives at the launch of the Trusted Information Sharing Network (TISN) in Melbourne this month.

"It is imperative that we put the national interest before business, political or state rivalries."

Problem is, many companies haven't realised that when the Attorney-General is talking about the nation's critical infrastructure, he's talking about their corporate systems -- particularly those belonging to essential services such as banking and finance, telecommunications, utilities, health and food providers.

Businesses often view infrastructure protection as a government problem, according to Tom Patterson, head of Deloitte & Touche Security Services in Europe, the Middle East, Asia-Pacific and Africa.

"People think it's a matter of securing government computers, and that it's the government's job to secure them," Patterson says.

"If you look at what runs the economy, it's not your government, it's your companies. Every company has an obligation to protect its business not only for its stakeholders and its shareholders but also for the economy as a whole."

The government hopes TISN will become a forum for open exchange of information about system attacks and vulnerabilities, as well as protection of key sites from cyber-sabotage or chemical, biological and radiological threats to water and food supplies.

A Critical Infrastructure Advisory Council will be set up to oversee efforts in various industry sectors as well as developing strategies for business continuity and consequence management.

Williams says protection of the nation's infrastructure is "not an entirely altruistic act".

"Our economy and international competitiveness are based on a series of complex inter-connections," he says.

"If just one part of the economy is attacked, the repercussions are likely to be felt by all sectors and all businesses."

But IT security experts fear that this focus on cyber-terrorism may distract people from the real threats.

Instead of preparing for Star Wars-style strikes, Tom Patterson says governments and business should be steeling their systems against waves of hackers.

Many people who may not "have the guts or wherewithal to go to Baghdad and pick up a gun" may instead aim a web attack on companies that make up a nation's critical infrastructure, he says.

"Waging a cyber-war is very inexpensive, you just need a computer and an internet connection," he says.

"You don't have to fly anywhere, you don't need to buy a gun and you don't even have to be that smart.

"We're not talking about Defence complexes, we're talking about the people who ship eggs. If food supplies stop flowing, that's a serious problem."

Patterson warns that every company executive has to get involved in the task of securing computer systems right now, because the threats "are only going to get worse".

"It's not enough to delegate this to some IT guy," he says.

"Most companies are evolving their information networks at a very rapid pace because they're enjoying the efficiencies the internet can bring.

"But as they look at their supply chains, they see how many different companies play a part in delivering their product, and when they look at their customer relationship systems they see how many computer systems that they don't control are involved.

"You have to take all that into account, because it only takes one link in the chain to go down and the company's out of business."

John Donovan, managing director of security specialist Symantec, shares a concern that the government may be pushing the concept of cyber-terrorism as a "call to arms".

"We know cyber-terrorism is not really a huge threat in terms of the world stage," he says.

"We are not seeing what (the government) is positioning as the big threat from terrorism.

"The greater threats come from more general, blended, threats that don't have a specific attack point.

"It's much more likely that Australia's infrastructure will be damaged through things like the evolution of Nimda or Code Red than by anyone launching an attack on the telecommunications backbone or a financial institution."

Blended threats combine the characteristics of viruses, worms, Trojan horses and malicious code to exploit computer system vulnerabilities.

On average, Symantec found seven new vulnerabilities a day over the past year.

Symantec's latest Internet Security Threat report, for the last half of 2002, says a number of high-risk future threats emerged that attackers and malicious code writers are just beginning to leverage.

"Three blended threats -- Klez, Bugbear and Opaserv -- were the source of nearly 80 per cent of malicious code submissions to Symantec Security Response over the previous six months," the report says.

"A large percentage of cyber-attacks detected were caused by only a handful of both old and new blended threats such as Bugbear, Nimda and Code Red."

Donovan says these types of threats require a different approach to what's being proposed through TISN.

"We're not seeing attacks coming from politically or religiously motivated groups," he says.

"Instead, we are seeing an increase in the complexity and number of threats where people are just going after general weaknesses.

"What's needed is a concerted approach to information sharing and management of security assets -- keeping in mind those are the sorts of attacks we're likely to see, not cyber-terror attacks on individual organisations or infrastructure.

"The problem is, the government's involvement in this space has not been strong.

"This is really their first stab at bringing business groups together with the public sector, and they have to go down the path of proving validity in the concept."

Dr Jan Hruska, founder and chief executive of anti-virus software vendor Sophos, says it's unlikely Iraqi sympathisers are spending much time creating viruses.

"Of course we are always watching like a hawk, and any hint of a new threat will be dealt with just the same way we deal with other threats that are large-scale and immediate."

AustralianIT, April 22, 2003.

