

ONLINE SECURITY WAR CONTINUES

HOW TO PROTECT YOUR INFORMATION

1. Identify and classify risk to confidential information.
2. Develop information protection policies and procedures that address privacy and regulatory compliance.
3. Deploy technologies that enable policy compliance and enforcement.
4. Communicate, educate and create awareness with employees, partners and suppliers.
5. Integrate information protection practices into businesses processes.
6. Report to the board and executive team.
7. Support due diligence and regularly audit practices, processes and technologies.

Source: Symantec

UNPRECEDENTED ACCESS TO GOVERNMENT PROCESSES VIA THE INTERNET IS BRINGING WITH IT INCREASED TRANSPARENCY. BUT IT IS NOT WITHOUT SIGNIFICANT SECURITY CHALLENGES, REPORTS **KATRINA GANIN**.

As the Australian public sector embraces Government 2.0 the potential online security risks are coming into sharp focus.

Challenges abound, and the planned National Broadband Network (NBN) will mean Australians will soon be living and working digitally like never before. With greater digital ubiquity comes risk.

Add to this the increasingly complex cybercrime landscape and the need to control expenditure, and you have enough to keep government IT security professionals very busy.

GOVERNING ONLINE

Finance Minister Lindsay Tanner, writing in a recent blog called *The Razor's Edge* illustrates the enthusiasm with which the Government is embracing all things digital. Tanner points to a taskforce report – *Engage: Getting on with Government 2.0* – which recommends public servants blog in online communities relevant to their work and proposes much greater accessibility to public sector data.

The benefits of Government 2.0 do not come risk-free. The report also calls for the Defense Signals Directorate (DSD) to provide guidance to agencies on the appropriate mitigation treatments to address concerns or exposures relating to the use of social networking and related tools.

"The lead agency, in conjunction with DSD," the report says, "should develop a Better Practice Guide to assist agencies in the effective, efficient and secure use of Web 2.0 tools and how to undertake associated risk assessment."

It is clear that as the Government puts more of its operations online it opens itself to the risk of cybercrime.

According to Craig Scroggie, vice president and managing director,

Symantec Australia and New Zealand, the underground cyber-economy is growing at an explosive rate.

"If it was a legitimate business, people would be investing in it," he says.

"The Government needs to find a balance between finding a good security posture and doing it in a cost effective way."

Michael Sentonas, director of sales engineering and services for McAfee Asia Pacific, says 90 per cent of Australians have been targeted by internet scams in the last year with a billion dollars lost due to cybercrime.

"We need to be constantly vigilant. The Government's key challenges are no different to private enterprise – adequate resourcing being directed towards fighting cybercrime."

THREAT LANDSCAPE

According to Graham Titterington, principal analyst, Ovum, in the UK, the security threats to government include managing the relationship with the citizen (e-government and online identity management), protecting the national infrastructure and defending the state in the cyber wars.

Andrew Walls, research director – security, risk and privacy at Gartner, says there are two major factors that governments of all levels must contend with in regard to security: the sheer quantity of government data and the need to change from an IT-focused to a managerial-focused approach to security.

"Almost everything government does today involves IT infrastructure," he says. "Now the purview of security has expanded massively to cover just about every process in government."

"The amount and type of data the government must manage is changing as it becomes more aligned with business and the exposure it has with the outside world."

"THE GOVERNMENT'S KEY CHALLENGES ARE NO DIFFERENT TO PRIVATE ENTERPRISE – ADEQUATE RESOURCING BEING DIRECTED TOWARDS FIGHTING CYBERCRIME."

Michael Sentonas, director of sales engineering and services, McAfee Asia Pacific.

After all, governments are now tier-one merchants as they process payments for all types of government services online.

Walls says the risks associated with these online transactions are well known in the commercial world, and governments need to take advantage of the security knowledge of the private sector.

"The cost to government to keep up with security issues will be a major consideration," he says.

"We have to keep beefing up our security due to the evolution of the threats. Governments are therefore looking for cost efficiencies and for ways they can work securely without increases in security costs."

It is not feasible to keeping increasing the number of security staff to fix security problems, Walls says, so new approaches must be found.

"This means security can no longer sit in a corner. It is now a standard function of government and this requires a shift in perception and approaches to security management within government agencies," he says.

"Security people have to become very knowledgeable about how government works and what it is trying to accomplish, then reflect that in how they manage security."

LOCKING DOWN SOLUTIONS

Government in Australia has, in the past, embraced outsourcing as a means of containing costs. Today the shared services model is being increasingly applied to contain costs through improved efficiencies.

Walls says shared services is a sound approach given 80 per cent of every government department's processes are common with that of another department.

"A lot of what security does is common to many agencies such as firewalls, anti-virus and intrusion detection, so it makes no sense for each agency to run their own," he says.

In addition, cloud computing is being seriously considered

by many government agencies for its ability to contain costs.

Titterton says there are some key advantages to be gained by government, as cloud computing provides a consistent security classification framework.

"In fact government has a unique option open to it that the private sector doesn't," he says.

"Most organisations can

only choose from a public cloud or an in-house model. Governments have a third way – a private government cloud that can be domiciled in-country."

Cloud computing allows agencies to control security from end to end, says Sentonas.

"It means you have multiple virtual systems sitting on a single layer that allows you to communicate across all of them. Anytime somebody accesses the cloud they do it through a secured portal or a secured process.

"It is also good for mobile devices because you are using a dumb device to connect to the cloud to access information from any location."

He says, however, there is a flip side.

"If the 'hypervisor' or underlying layer is compromised you lose everything," Sentonas says. "Despite a lot of theory-based attacks there has not been an attack that has caused problems. We work with a lot of organisations within government to roll out this type of technology without any issue."

He says there are pluses and minuses for any technology.

"You need to aware of the risks, then manage those risks." **GN**

"THE AMOUNT AND TYPE OF DATA THE GOVERNMENT MUST MANAGE IS CHANGING AS IT BECOMES MORE ALIGNED WITH BUSINESS AND THE EXPOSURE IT HAS WITH THE OUTSIDE WORLD."

Andrew Walls, research director – security, risk and privacy, Gartner

TRENDS TO WATCH IN 2010

- **Antivirus is not enough** – traditional approaches to antivirus are not sufficient, as new malicious programs are being created at a higher rate than good programs. New approaches that will include all software files, such as reputation-based security, will become key in 2010.
- **Social engineering as the primary attack vector** – direct attacks on end users will increase via tricks to cause downloading malware or divulging sensitive information.
- **Rogue security software vendors escalate their efforts** – rogue security software scams to increase, including hijacking of users' computers, rendering them useless and holding them for ransom.
- **Social networking third-party applications will be the target of fraud** – fraud against site users to grow. Vulnerabilities of third-party applications used to defend attacks will be attacked.
- **Windows 7 will come into the cross-hairs of attackers**
- **Fast flux botnets increase** – a technique used by some botnets to hide phishing and malicious websites behind an ever-changing network of compromised hosts acting as proxies. The original geo-location of the botnets are difficult to trace.
- **URL shortening services become the phisher's best friend** – short URLs are harder to distinguish as suspect and are therefore more readily clicked on.
- **Mac and mobile malware will increase** – as Mac and smartphones continue to increase in popularity more attackers will devote time to creating malware to exploit these devices.
- **Spammers breaking the rules** – more organisations selling unauthorised email address lists and more less-than-legitimate marketers spamming those lists.
- **Spam volumes will continue to fluctuate** – as spammers continue to adapt to the sophistication of security software.
- **Specialised malware** – use of insider knowledge to create malware targeting electronic voting systems, as used in political elections and public telephone voting.
- **CAPTCHA technology will improve** – as spammers have a more difficult time breaking CAPTCHA codes (which determines if a response is not generated by a computer) through automated processes, spammers in emerging economies will devise a means to use real people to manually generate new accounts for spamming.
- **Instant messaging spam** – instant messenger (IM) attacks will grow in popularity. IM threats will largely be comprised of unsolicited spam messages containing malicious links.
- **Non-English spam will increase** – as broadband connection penetration continues to grow across the globe, particularly in developing economies.
- **Drive-by-downloads lead the way** – attackers increasingly compromise legitimate websites.
- **Rise of polymorphic threats** – malware that is slightly different than the one before it. The automated changes in code made to each instance do not alter the malware's functionality, but virtually render traditional antivirus detection technologies all but useless against them.
- **An increase in reputation hijacking** – where names and reputations of smaller free web services, such as URL shortening sites, are being abused by spammers.
- **Data breaches continue** – with 59 per cent of ex-employees admitting they took company data when they left their jobs.

Source: Symantec