



SAFECOMMS

CPA AUSTRALIA: ACHIEVING AN APPROPRIATE LEVEL OF INFORMATION SECURITY

CPA Australia is a high profile organization that represents - and provides a range of services to - over 100,000 professional accountants in Australia. It also provides advice and information to the general public.

From an IT perspective, CPA Australia is heavily dependent upon the reliability and security of its IT infrastructure - both in terms of its internal operations (it has around 400 staff using its network) and also in terms of its web based applications which enable interactions with its widespread membership and also with the public.

In short, it is a fairly typical medium sized contemporary Australian organization that makes extensive use of the business opportunities afforded by a strong online presence.

"We certainly view Safecomms as a strategic partner to the organization. They have shown the kind of flexibility and commitment you look for in an ongoing business relationship, and they certainly know their stuff. Above all, they're practical: they've got a lot of real experience under their belts, and whatever I get them involved with, you can pretty much guarantee they will have been there before - usually many times over."

David Camilleri – Infrastructure Manager, CPA Australia

The Challenge

David Camilleri joined CPA Australia as Infrastructure Manager in early 2005. A major part of his brief was information security. What he found was a situation that is common to many medium sized organizations. There had been a sizeable investment in security technology in recent years, but very little focus on the "people and process" aspects of information security.

As a result, Camilleri believed that his new organisation was almost certainly less secure than it believed. As he puts it, "I'm not a security guru, but I know enough to understand that all the security devices in the world are not much use if the underlying security processes are weak, or if users are naïve about security issues - for example, careless about keeping their passwords confidential."

He wanted to shift CPA's approach to information security from being "technology led" to being "process driven" (with a fair amount of user education thrown in for good measure). He also wanted to ensure that he did not go overboard and introduce a level of security that would be excessive (in terms either of cost or rigour) for an organization of CPA's size and profile. He had to find the right balance of security, usability and cost.

A Long Term Security Partner

Camilleri knew he was embarking on a journey that would cover a lot of ground and would need to be undertaken at a pace that ensured no hasty wrong turnings were made, and that the entire organization came with him - including those who initially did not fully recognize there was a problem that needed fixing.

He also knew he would need help from an external organization. His own IT team were already working at full stretch, and in any event did not possess the requisite level of highly specialist knowledge of information security. By bringing in an outfit that did this kind of project day in day out for numerous similar profile organizations, Camilleri knew that he would effectively be getting the benefit of learning curves that had already been gone through, and authentic practical knowledge of what works and what does not based on real world experience.

Organizations need to shift from a "technology led" approach to security, to a "process driven" approach.

Millions of dollars are being wasted by investing in more security devices rather than addressing processes and user behaviour.

It is essential to achieve a level of security that is appropriate for your individual organization. There is no "one size fits all" answer to the question of what is "appropriate".

The organization's risk profile needs to be understood, and then the right balance of security, usability and cost needs to be arrived at to create a security regime that addresses that risk profile in the smartest way.



CASE STUDY: CPA AUSTRALIA

Organizations today are exposed to numerous risks that traditional security devices - firewalls, anti virus etc. - do nothing to counter.

Even with regard to the types of risks that security devices are designed to address, they are often of limited effect. Many firewalls are misconfigured, and the fact that many organizations are still being hit by malware demonstrates that anti virus solutions are by no means a failsafe.

In today's risk environment, a "Defence In Depth" strategy is required. This means a greater focus on implementing procedures that ensure the infrastructure is managed in a more secure way, and that the underlying security architecture is properly designed and configured.

Educating the user community is also essential. Your security can be blown apart by one piece of naïve or unthinking behaviour by a user.

For David Camilleri, Safecom was an obvious choice. He'd seen them at work in the organization he'd been with before he moved to CPA, and had liked what he'd seen. "They clearly had real subject matter expertise, but above all they seemed very pragmatic and were clearly committed to working out what was the right level of security for this particular organization - they actively thought about that and discussed it with you, rather than saying 'best practice requires you to have x, y and z so that's what we'll do for you'."

The Starting Point

But before setting out, Camilleri first had to ensure that his views regarding the (then) current state of security were accurate, and convince the board that this was a path that really needed to be gone down. An external objective assessment was needed.

He therefore asked Safecom to carry out a rapid assessment of the state of security of the CPA data centre and existing security procedures, and also a penetration test identifying ways in which a hacker could bypass the existing perimeter defences and gain access to the internal network.

Within a week, Safecom presented their findings. The results of the assessment and penetration tests came as no surprise to Camilleri - but certainly surprised the board and also the IT team that had been in place before his arrival. The bottom line was that CPA Australia had a number of significant exposures and vulnerabilities, despite a substantial historic investment in security technologies. It was clearly time to shift to a process driven approach.

Setting The Agenda

Armed with the findings of the risk assessment, David and his team sat down with Jason Harris, one of Safecom's Principal Consultants, and quickly thrashed out a road map for the structured implementation of a new information security regime that was right for CPA Australia.

Harris takes up the story. "What we found at CPA Australia was fairly typical of what Safecom generally finds at most of our new clients. Historically they had focused on addressing security by implementing traditional security technologies - firewalls, anti virus, etc. However, they were exposed to numerous other security risks that these technologies do nothing to counter - risks that can only be addressed by putting in place procedures that ensure the infrastructure is managed in a more secure way, and by reconfiguring the underlying security architecture. We needed to work with the CPA Australia team and help them to address the risks that so many organizations still seem to overlook - patch management, hardening of servers, network segmentation, making remote access more secure, back up procedures etc. etc. - all the usual suspects".

Safecom also identified a pressing need for raising levels of awareness about information security across the user community. "Whatever security technology you implement, whatever procedural protections you put in place, the whole security set up can potentially be blown apart by one unthinking or naïve bit of behaviour by a user," said Harris. "In our experience, a minor investment in user awareness training can bring a much greater 'security dividend' to the organization than a major investment in the latest and greatest security devices."

A step by step transition program was agreed with Safecom. Central to the whole project was the concept of Safecom transferring know how to the CPA Australia team along the way, something that was particularly important to David Camilleri. "I wanted to make sure that as Safecom helped us to implement new ways of managing security across our infrastructure, we learned as we went so that the specialist security focus that Safecom were bringing to the table would become ingrained into the way we work in the future."

CASE STUDY: CPA AUSTRALIA

Establishing The Foundations

The first and most critical activity in making the transition to a process driven approach to information security was to develop a set of policies, procedures and standards. These would form a constant point of reference to enable new working practices to be developed over time, and would be the glue that held the CPA Australia approach to information security together.

“Creating a first draft set of material was a much quicker exercise than I had envisaged,” said Camilleri. “Safecoms had obviously done this kind of project for a number of organizations that were quite similar to us in terms of size and IT infrastructure, and they knew exactly which areas to home in on as being the most problematic. They spent time discussing with us the various different ways in which the hard issues could be tackled, and helping us to make the right choices. They then went away and produced a first draft that reflected the way we wanted to address all the key issues, and which also took into account tried and tested ways of implementing information security such as the recommendations in AS7799.”

Areas covered by the comprehensive new policy set included:

- Roles and responsibilities in managing security
- Third party access to the network
- Remote access
- Information management (encryption, confidentiality, standards)
- Security incident management
- “Acceptable Use” Agreement for all staff
- Physical access controls
- Protection against malware
- Secure configuration of different types of computing equipment
- Back up procedures
- Wireless computing
- User access management
- Authentication controls
- Change management
- Disaster recovery
- IT asset management
- Maintenance and protection of IT assets

“Of course, in order to comply with our new policy set, we had to lift our game in several areas, so the next phase of the project was about Safecoms helping us to address the most high risk and difficult issues”, said Camilleri.

Two Factor Authentication

Given the business need for remote access to systems and the need to protect particularly carefully against unauthorized access to member information and other types of confidential data, Safecoms recommended the implementation of two factor authentication. “By this stage they understood our infrastructure very well, and they were able to point us straightaway at the best solution for CPA Australia. One of the things I like about Safecoms is they are not aligned with any technology vendors, so if they steer you towards a particular product you know it’s for all the right reasons” said Camilleri. Safecoms actually implemented the two factor authentication solution for CPA Australia, saving them time and money.

Server Hardening

Many of the exposures identified by Safecoms during their original security assessment were capable of being fixed by effective hardening of the Windows servers at CPA Australia. David Camilleri knew this was a particular strength of Safecoms, and he was particularly keen to make use of this skill set.

“I know from previous experience that hardening servers can be a nightmare, and that the guides published by Microsoft and NSA really do not go anywhere near far enough at the practical level.

A process driven approach to security is built on a platform of a comprehensive set of policies, procedures and standards.

There is no “one size fits all” approach - policy sets have to be tailored to meet the unique operational needs of each individual organisation.

Once the policy set is in place, you have an agenda (and a “how to” manual) that drives the process of ensuring that the infrastructure is securely managed.

Transitioning to a process driven approach to security rarely involves investment in more technology. It’s about managing what you already have more effectively.



SAFECOMS

CASE STUDY: CPA AUSTRALIA

Contact Safecoms

Tel: +61(0)2 8234 4000

Fax: +61(0)2 8234 4099

info@safecoms.com.au

**PO Box A2161
Sydney South
NSW 1235**

So when Safecoms said they had developed a set of 'gold standard' hardening templates that were in use at some of Australia's biggest companies and that they would customize and guarantee these for CPA Australia, I was impressed" says Camilleri. "In the course of five days they fully hardened - and documented - five different server roles, and they have been rock solid ever since. Better still, they made sure one of our system administrators was sitting alongside them throughout the process so he can roll out the templates to additional servers as we implement them."

Patch Management

At the practical day to day level, achieving effective patch management within necessary timescales is one of the toughest challenges facing most IT departments today. CPA Australia was no exception.

"There's no 'silver bullet' available when it comes to patch management", says Jason Harris of Safecoms. "However, by using tools such as Microsoft WSUS and building practical and well defined procedures with clear responsibilities at the personal level you can certainly make life a lot easier for people and take a lot of the pain out of the process. When you get an organization like CPA Australia that is really committed to effective management of the security of its infrastructure, we can inject our practical experience of what works and what does not work, and make the whole patch management process a lot more manageable".

Active Directory Design

CPA Australia saw that a new design of its AD schema would enable much more granular management of user access rights and systems, and would make practical implementation of such fundamentals of security as the "principle of least privilege" much easier at a day to day level.

Many organizations fight shy of taking this step. However, Camilleri was keen to press ahead, seeing the longer term advantages. Whilst much of the detailed data gathering and analysis was performed by members of the CPA team, Safecoms provided the overall design structure and management level guidance for the project.

User Awareness Training

"The Safecoms information security awareness DVD is the best training aid I have seen in this space", says David Camilleri. "We had Safecoms make a few customizations to it to fit our house style, but we are now going to make it the centerpiece of our information security user awareness program."

Aimed at non technical users, the DVD (which can also be streamed in chapters for viewing over the internet using standard WMP technology) ensures a consistent message is delivered to all users in an entertaining and in formative way.

CPA Australia are now looking at the new InfoAware add on's recently brought out by Safecoms to supplement the DVD, which include an online questionnaire and an administration interface enabling organizations to keep a track of who has viewed which chapters of the training video, and what scores they achieved in the online questionnaire.