symantec™

2003 INFORMATION SECURITY AWARENESS Challenge!

symantec™ 2003 INFORMATION SECURITY AWARENESS Challenge!

in

Information Security is not solely an IT issue	2
Introducing the Symantec 2003 Information Security Awareness Challenge	3
Key deliverables	4
What Challenge participants will be required to do	5
Fantastic prizes to get them motivated	6
Detailed reports to reveal strengths and weaknesses	7
National Awards Presentation	8
Technical requirements	8
How to calculate your financial outlay	9
Next steps/Key dates	10
Put an end to your doubt	11
Organising bodies	12

Time for a paradigm

Information Security is not solely an IT issue

Incredible technological progress has been made in the information security field in recent years, it's true, and IT will continue to play a vital role in protecting critical infrastructures.

Disruption to the national infrastructure, even for very short periods, can have an impact on the economy measurable in millions of dollars. Likewise, minor interruptions or security breaches…can cause a loss of confidence in consumers and investors.*

But the fact is that computer crime rates continue to rise, threatening individual companies, government, and indeed national security.

As the National Office for the Information Economy points out, "disruption to the national infrastructure, even for very short periods, can have an impact on the Australian economy measurable in millions of dollars. Likewise, minor interruptions or security breaches, in any form, can cause a serious loss of confidence in consumers and investors."

And it's human error, not just technology, that threatens to allow it to happen. Consider the following US figures, which are broadly relevant to Australian companies:

- US$1.5 trillion globally lost to cyber crime in 2001.[1]
- 99% of attacks are through vulnerabilities for which counter measures are already available.[2]
- 96% of successful attacks could be prevented by adherence to standard security policies.[3]

Without an immediate and significant improvement in information security awareness levels, the potential value of technical solutions will not be realised.

In fact, their presence may actually generate complacency among staff, thus increasing the threats they're designed to prevent.

All staff must take responsibility

If these serious issues are to be adequately addressed, all staff – every single employee accessing or handling company information – must play their part.

Most people don't consider information security to be their problem. Nor do they understand how it affects them. Consequently, they're not interested in memorising 'two-inch-thick' policy documents.

A new approach to learning is required; one that is sufficiently engaging and stimulating to capture and hold staff's attention.

And, ultimately, to permanently and positively influence their behaviour.

*National Office for the Information Economy

1. "InformationWeek" Global Information Security Survey, 2001. 2. Joint study by the CSI and FBI, 2001. 3. US Defence Department, 2001.

Introducing the Symantec 2003 Information Security Awareness Challenge

For the first time, you have access to an information security benchmarking and training tool capable of making an immediate and demonstrable difference throughout your entire organisation.

The Symantec 2003 Information Security Awareness Challenge:

- Requires individual staff to complete an expertly crafted and dynamically presented electronic Q&A challenge.
- Provides powerful incentive for staff to participate and conduct extensive pre-Challenge self-education through a large national prize pool.
- Has employed leading information security professionals to carefully construct each scenario and its related responses so as to clearly identify participants' understanding of their personal responsibilities, and general levels of awareness.
- Focuses on critical but fundamental workplace behaviour requiring absolutely no specialist technical knowledge, making it relevant for your whole workforce.
- Includes a detailed post-Challenge Management Report to clearly and accurately identify areas where your organisation faces its greatest threat and need for improvement.

A complete breakdown of the scenarios, related responses and their corresponding threats will be made available on the Challenge website at www.securitychallenge.com.au from 24th March, 2003.

Establishing consumer confidence in the security of the online environment is a critical element in Australia's transformation into an information economy. As the Australian economy becomes increasingly reliant on networked technologies, it's vital that owners and operators of information systems take adequate measures to ensure their systems are secure.*

Company directors' legal responsibilities

A less obvious, though nonetheless significant outcome of your company's involvement in the Challenge will be its contribution to your directors' personal legal obligations.

Directors are required to exercise due diligence in the protection of corporate assets, which includes the protection of company information by means of effective information security. Failure to do so risks substantial personal penalties, compensation orders, and disqualification.

*Joint press release by the Attorney General, the Minister for Defence, and the Minister for Communications, Information Technology and the Arts.

more reasons why

Peace of mind that you've made an important contribution towards protection of your own and Australia's critical infrastructure, thereby reducing the threat to the national economy.

Key deliverables

In addition to the benefits mentioned on the previous page, participation in the Symantec 2003 Information Security Awareness Challenge also promises:

- Improved efficiencies and increased value for money from strategic investment in IT information security solutions.
- Realistic benchmarking of associated threats and exposures across your organisation.
- A measured educational framework with which to reduce uncertainty and better understand and control future training expenditure.
- Increased consumer confidence – information security is currently considered an area of industrial weakness.
- Completion of an integrated post-Challenge survey to provide a collective view of how seriously your company considers information security.
- Peace of mind that you've made an important contribution towards protection of your own and Australia's critical infrastructure, thereby reducing the threat to the national economy.

easy-to-follow instructions

What Challenge participants will be required to do

All staff that you register to participate in the Symantec 2003 Information Security Awareness Challenge will be required to answer 37 multiple-choice questions to complete the on-line challenge.

They will be required to do this on their own PCs within a five-day period from 3rd–7th March, 2003.

Presented in a dynamic electronic 'quiz show' format, each scenario describes a different situation for which four possible responses are provided.

These scenarios, non-technical and highly relevant to all staff, will include issues such as:

- Document Storage and Classification.
- Correct use of Passwords.
- Computer Viruses – protection from, and containment of.
- Disaster Recovery and ensuring Business Continuity.
- Compliance with Privacy Legislation; etc.

Each of the four possible responses to the 37 scenarios will represent varying degrees of threat and danger. When selected, each response will highlight a different level of awareness ranging from full compliance and understanding of the related threats to a lack of appreciation of the dangers that lie therein.

Importantly, however, all answers will appear to be reasonable options to an uneducated participant.

Participants will find the Challenge software extremely easy to use. Above question text for illustrative purposes only.

Stimulates discussion and self-education

The Challenge's entertaining game-play format should not be mistaken for a lack of serious intent. It has been included solely to generate interest in the topic and desire to participate.

The emphasis is squarely on stimulating internal discussion, debate and self-education, with participants strongly encouraged to investigate their own organisation's security policies in preparation.

And as you'll see on the following page, we're providing some very attractive personal incentives for them to do so.

staff incentives

Fantastic prizes to get them motivated

If the integrity of an organisation's network is to be protected it's critical that employees stop writing off information security as someone else's problem.

IT departments and senior management obviously have important roles to play, but all staff must take the time to understand their personal responsibilities.

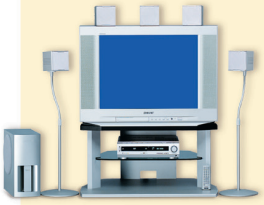
With this in mind, the Symantec 2003 Information Security Awareness Challenge offers substantial individual rewards for the nation's best performed entrants, providing a powerful incentive for self-education.

Prize winners[1] will be selected from those who answer all 37 questions correctly in the fastest times.

Plus, the creators of the Challenge, Edusec Pty Ltd, will set aside 10% of your organisation's total registration fee for you to use as an internal prize, recognising the best performed participant within your company.

1st Prize
A New Ford Focus

2nd Prize
$10,000 Cash



3rd Prize
Complete Sony Home Entertainment System

4th Prize
3-Day Luxury Holiday for 2

5th Prize
Sony Laptop Computer

1. The Symantec 2003 Information Security Awareness Challenge national prize pool is only available to companies and their employees who reside within Australia, and excludes Symantec employees and their families and Commonwealth Government employees.

Enable strategic

You, your industry bodies and participating Commonwealth agencies will have an informed, reliable benchmark upon which to base strategic decisions regarding specific information security training.

Detailed reports to reveal strengths and weaknesses

Perhaps the most valuable outcome of your organisation's participation in the Challenge will be the detailed intelligence it delivers.

Upon completion, you will be provided with a full results analysis of your company's performance, clearly identifying:

- Areas in which you face the greatest threats to security.
- Improvements in employee awareness during the five-day Challenge period, measured from first to last attempts.
- How information security was viewed in your company both before and after completion of the Challenge.

The results will allow you to make additional assessments such as:

- Whether employees realised you had an information security policy already in place, and had read it.
- Whether staff consider information security to be important.
- Whether staff felt the Challenge improved their level of awareness.

You will also receive a summary of vulnerabilities across your industry and the nation's entire critical infrastruture.

In short, you, your industry bodies and participating Commonwealth agencies will have an informed, reliable benchmark upon which to base strategic decisions regarding specific information security training.

Focused objectives will be able to be established with confidence. And real progress will be able to be made.

large training outlays

Economies of scale in creation of future programs

Following the completion of the Symantec 2003 Information Security Awareness Challenge, Edusec Pty Ltd will undertake strategic, focused development of appropriately targeted educational products and services with which to help mitigate the threats identified across the program as a whole.

Through economies of scale, high quality tailored products will be made available for the first time for a fraction of the price that such product development would cost a single organisation.

The products will build on the measurable foundation provided by the Challenge.

to celebrate

National Awards Presentation

After individual participants' details are recorded on their organisations' servers, their actual Challenge entries will be submitted in complete privacy.

Each time they complete the Challenge, their entry will be automatically given a unique encrypted identifier code by the software.

The top individual performers in the Challenge across the nation, and the top performer in each participating organisation, will be identified only after the relevant unique identifiers are returned to the organisations from which they came to unlock the names of the winners.

The winners' names will then be delivered to Edusec, as the organiser of the Challenge, and Edusec will advise the winners of their success and invite them to the National Awards Presentation.

This event will be held at a location and date to be advised after the correct identification of winners and final delivery of Management Reports to all participating organisations.

The nation's top five individual performers – those who answered all questions correctly in the fastest times – will be named as the overall winners of the Symantec 2003 Information Security Awareness Challenge.[1]

1. Independent and authoritative adjudicators will be assigned in order to verify the winning entries.

Your ability to

Technical requirements

In order to participate in the Challenge and operate the software effectively, your organisation must have the following minimum level of technical capacity:

Network Server

- Windows NT 4 Server SP6a (or later); or Windows 2000 Server (Service Pack 3)
- TCP/IP
- Pentium 120 MHz 32 MB RAM minimum hardware

Participants' PCs

- Windows 98, NT, 2000, XP (with latest Microsoft recommended Service Packs)
- TCP/IP
- Pentium 120MHz 32 MB RAM minimum hardware

Full details can be found on the Challenge website at: www.securitychallenge.com.au

your costs

How to calculate your financial outlay

Registration fees for the Symantec 2003 Information Security Awareness Challenge are variable, depending on the number of individuals registered across your organisation. These costs are calculated on a per-participant basis, much like commercial software licences.

Precise costings can be found on the restricted registration section of the Challenge website at: www.securitychallenge.com.au. To access this you will need:

- User ID: Awareness2003
- Password: AddedValue4us

The calculator can be used to estimate your maximum cost for participating in the Challenge.

Upon registration, the first-part invoice you receive will reflect the software licence fee for those staff registered to participate.

You will then receive the Challenge software for installation on your network, and this will track the number of individual participants from your organisation who actually complete the Challenge during the five-day Challenge period, as well as the number of times they complete it.

Each completed Challenge entry will attract a minimal charge, as detailed on the pricing model located on the restricted registration section of the Challenge website. This will be reflected in your final invoice, to be supplied with delivery of final Management Reports.

You can gain all the significant strategic benefits of this program – including supply of all Management Reports – from around $5 per head.

Can you control the number of attempts your staff are allowed?

Yes. To enable you to set a defined budget for this exercise you will have the option of restricting your registered staff to a set number of attempts between one and the default play rate of five.

Keep in mind, however, that the more attempts staff are allowed, the more chance they will have to win, and the more effort they're likely to put into the learning process.

Next steps  Key dates

1. Meet Registration deadline 21st February, 2003

To register your organisation, first calculate how many staff you wish to participate, remembering that information security is everyone's responsibility. Then complete and return the enclosed Registration Form.

You can also register on-line at the restricted registration section of the Challenge website by using the User ID and Password (p.9).

2. Challenge Software Module mailed early in new year 2003 and/or prior to 24th February, 2003

Install this software on your network and perform any necessary tests. A demo Challenge will be available at this time for review as the live Challenge will NOT be accessible until the Challenge release codes are made available.

3. Challenge Release Codes made available 24th February, 2003

These codes will allow you to unlock the live Challenge on your network. They will be made available on the Challenge website through use of your company's name and registration number, provided with the software. Note, however, that the software is programmed to not actually allow access to the live Challenge until the first day of the 5-day Challenge period.

4. 5-Day Challenge Period 3rd – 7th March, 2003

From 9am on the first morning until 5pm on the last, all registered participants will be able to complete the Challenge. They will be able to submit up to 5 completed attempts if the default setting is left in place. If you've pre-set a different limit (from one to five), however, that number will apply.

5. Return of Challenge Entries by 21st March, 2003

All Challenge entries must be returned for processing prior to 5pm (EST) 21st March, 2003 in order to qualify for the national prize pool. Entries received after this date, however, will still be eligible for the internal award of 10% of your organisation's registration fee as your organisation's top performer.

6. Management Reports distributed 4th April, 2003

This report will assist in pinpointing your organisation's information security weaknesses. The final invoice accounting for the total number of entries processed will also be provided at this stage.

7. National Awards Presentation April, 2003

The nation's top five individual Challenge performers – those answering all questions correctly in the fastest times – will receive their respective prizes as the overall winners of the Symantec 2003 Information Security Awareness Challenge.

The occasion will be an integrated corporate event. Informative presentations from global information security heavyweights will be
a highlight, revealing the seriousness of the threat on a world scale, and discussing vital strategic responses.

Put an 

to your doubt

And prove you're up to the Challenge

Are you absolutely sure that your entire workforce is adequately schooled in best-practice information security procedures?

As countless organisations around the world have learned at their own expense, even the strongest technical solutions can be negated by the uninformed behaviour of a single employee.

The Symantec 2003 Information Security Awareness Challenge represents the ideal counter measure.

For as little as around just $5 per head, it provides an unprecedented opportunity to:

- Motivate and educate your staff.
- Identify exactly where your current weaknesses lie.
- Enable well informed, strategic decision making.

Can you seriously afford to let it pass you by?

Register now.

www.securitychallenge.com.au
1300 302 199
PO Box 285
Kent Town SA 5071

"Changing user attitudes is recognised as one of the most significant barriers to improved security."*

*AusCERT's 2002 Australian Computer Crime and Security Survey.

Keeping 

Who's behind the Symantec 2003 Information Security Awareness Challenge?

Symantec
www.symantec.com.au

Symantec Australia is the program's major sponsor, and has also performed an advisory role to Edusec in the program's development.

The world leader in Internet security technology, Symantec provides a broad range of content and network security software and appliance solutions to individuals, enterprises and service providers.

Edusec Pty Ltd
www.edusec.com.au

Edusec is the primary creator and marketer of the Challenge.

The company's charter is to have an immediate and demonstrable effect in raising information security awareness levels across the nation, through meaningful and effective training initiatives.

Edusec believes the combination of rising global computer crime rates and falling security policy awareness presents a clear and present danger that must be addressed.

National Office for the Information Economy (NOIE)
www.noie.gov.au

NOIE plays a key role in the Commonwealth's E-Security National Agenda.

The Electronic Security Coordination Group, chaired by NOIE, is the Commonwealth's core policy development and coordinating body on e-security matters, and has the strategic goal of creating a secure and trusted electronic operating environment for the public and private sectors.

The Attorney General's Department (AGD)
www.ag.gov.au

Australia's economy and national security are dependent on a reliable and secure national information infrastructure (NII), most of which is owned by the private sector.

The AGD will coordinate measures to identify and protect the critical elements of the NII, including creation of a national early warning system and information sharing arrangements with the private sector.

The AGD will also lead efforts to further e-security and critical infrastructure protection issues internationally through bilateral and multi-lateral arrangements, and development of crisis management arrangements for the NII.

symantec™

chimo
TECHNOLOGY.CREATIVITY. INTELLIGENCE.

NOIE
The National Office for the
INFORMATION ECONOMY

Attorney-General's Department

EDUSEC