

trusting the internet



Why should small business be concerned about e-security?



An estimated 500 million people worldwide are connected to the Internet...

A large number of Australian companies are taking important steps to gain competitive advantage through e-business, and in doing so are adopting appropriate e-security tools and strategies.

An estimated 500 million people worldwide are connected to the Internet, and the number continues to rise. The global computer network is now a vital communications system for companies of all sizes. But as it grows in popularity, the security issues associated with conducting business online also increase. These include:

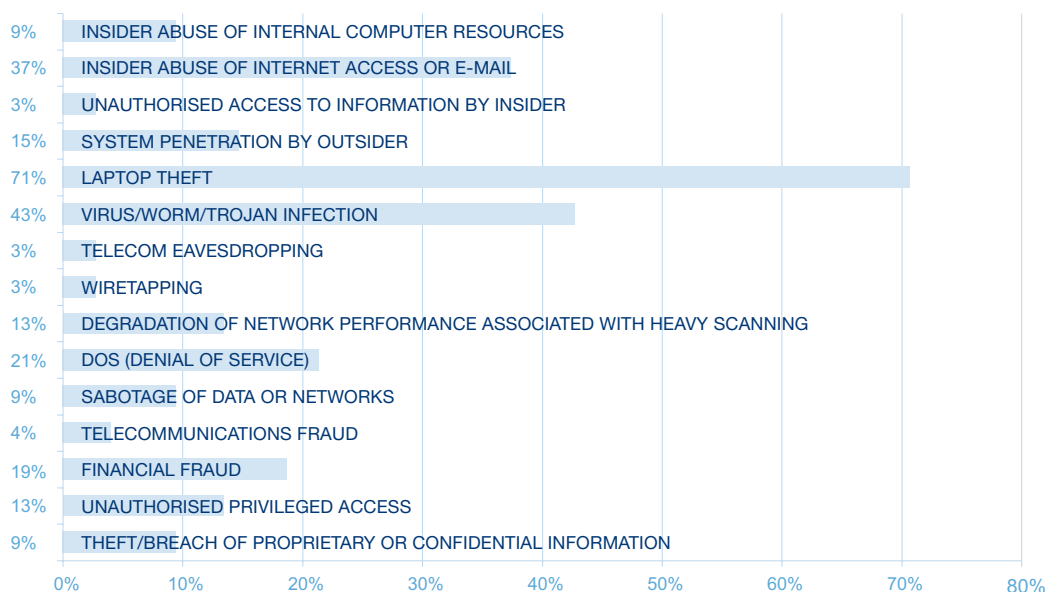
- virus infections or attacks by hackers
- theft of confidential data
- attempts by others to pass themselves off as representatives of your business
- interception of customer transactions

Just how real are the risks? A recent survey of large Australian organisations found that 67% were the subject of electronic attacks in 2001.

While e-security can seem daunting, the rewards for businesses in improved efficiency and expanded market opportunities are well worth the effort. Indeed, when used properly, secure e-business systems can be much more reliable than traditional means of conducting transactions. Taking the time to make sure your online activities are secure will help ensure the long-term security of your entire business.

NOIE has produced a series of small business case studies that demonstrate the benefits to business of ebusiness.

Which of the following types of computer esecurity misuse resulted in financial losses for your organisation in the last 12 months?



Source: *2002 Australian Computer Crime and Security Survey*
Australian Computer Emergency Response Team (AusCERT), NSW Police,
Deloitte Touche Tohmatsu, 2002 Australian Computer Crime and Security Survey,
http://www.auscert.org.au/Information/Auscert_info/crimesurvey.html

e-Security

//



e-Security: Facts and figures

- 87% of Australian companies suffering electronic intrusions were attacked by external parties (Source: 2002 Australian Computer Crime and Security Survey)
- The greatest e-security risk comes from the theft of proprietary business information (Source: 2002 CSI/FBI Computer Crime and Security Survey)
- Virus attacks cost business worldwide US\$13.2 billion in 2001 (Source: Computer Economics)
- One international gang uncovered by the FBI last year had stolen more than 1 million credit card numbers via the Internet (Source: FBI)

How can I protect my business? – *Trusting the Internet*

Electronic security (e-security) needs to be one of the first issues considered when planning to take your business online or connecting your business's computer systems to the Internet.

To help small business owners and operators understand e-security issues the National Office for the Information Economy (NOIE) has produced *Trusting the Internet*, a package of information resources including, e-security fact sheets, checklists and case studies. Basic e-security precautions are as important to your business as having good physical security and a comprehensive insurance policy.

Every business will have different e-security problems to consider. Issues you may need to address include:

- **Protecting against hackers and viruses.** Any computer connected to the Internet is at risk of being attacked by hackers seeking confidential information, or infected with a virus that can damage or disable. A correctly configured firewall and up-to-date anti-virus software can help protect against these threats.
- **Securing email.** Emails are frequently used for business communication, but standard emails can be forged or intercepted in transit. Switching to a secure email service for all or some of your business email will greatly improve security.
- **Buying and selling online.** If you offer sales or accept payments from your website, ensure that your transactions are secure and take measures to prevent fraud. Software to enable secure transactions can be obtained from your Internet Service Provider (ISP), bank or computer supplier.
- **Authenticating staff and customers.** Whenever anyone accesses your business website or computer networks, you need to be sure they are who they claim to be. This can be achieved using a simple system of usernames and passwords. More secure but more expensive approaches involve encrypting and decrypting data, or use an elaborate biometric system checking fingerprints and iris scans. The option you choose will depend on the information and financial sensitivity.
- **Legal obligations.** When conducting any business online, it is important to be aware of legal requirements in the area of customer privacy and information security. In general, online transactions now have the same legal status as paper transactions.

Electronic
security (e-security)
needs to be one
of the first issues
considered when
planning to take
your business
online...

Case Study



Entech Pty Ltd



Adelaide business Entech Electro Graphics demonstrates both the benefits of using e-business and the importance of ensuring that security is part of all e-business planning.

The company, which employs 35 people, specialises in the development of product decals, graphic overlays and product marking for the industrial electronics market. It began using electronic data interchange (EDI) technology in 1990 to exchange designs and data with its clients. More recently, Entech has built a website to allow customers to access up-to-date order status information from its enterprise resource planning (ERP) system.

The company received a stark reminder of the importance of e-security when it was infected with a virus attached to an incoming email. All of its computer systems were down for a day while the virus was removed, making it difficult to communicate with customers. Entech has since enhanced their firewall, e-security systems and management practices and have remained problem-free since.

Entech is far from alone in suffering such problems. According to research group Computer Economics, virus attacks cost businesses worldwide US\$13.2 billion in 2001.

But despite such hurdles, e-business has proved a definite boon for Entech. In its first year using the enhanced website system, it attracted more than \$240,000 in extra business because customers preferred the new electronic system. This contributed more than \$72,000 in extra profits for Entech.

More recently, Entech has built a website to allow customers to access up-to-date order status information from its enterprise resource planning (ERP) system.

Key E-Security Issues

Is your business e-secure? You should be able to answer 'yes' to all of the following questions.

- Are all our computers protected against viruses and other malicious attacks?
- Have we taken measures to secure our computers and related information resources?
- Can staff send emails securely and privately?
- If we offer sales via our website, are customers guaranteed that their information will remain confidential during transmission and are these details stored securely on our network?
- Can our computer systems keep track of who has accessed important information?
- Do we have an e-security and a privacy policy, and are all staff aware of it?
- Do we have documented IT security procedures for managing and maintaining our network securely?
- Do we have physical security measures in place for all our IT equipment?

If you are not sure about any of these issues visit www.noie.gov.au/trustingtheinternet



How do I?



As part of its mission to ensure Australia develops a world-class online economy, the National Office for the Information Economy (NOIE) is committed to helping organisations of all sizes deal with e-security issues.

The following e-security Fact Sheets are included in the *Trusting the Internet* Guide and are available separately online at www.noie.gov.au/trustingtheinternet

The following e-security Fact Sheets are included in the Trusting the Internet Guide and are available separately online

Top Ten eSecurity Tips

How Do I Set Up a Secure Web Site?

How do I tell if I'm completing a secure transaction?

How do I protect my company from viruses?

How do I manage real world security risks?

How do I manage my e-security when the service is outsourced?

How do I make sure my passwords are appropriate and secure?

How do I make sure my PC is secure?

How do I make sure my digital certificates and keys are secure?

How do I ensure my emails can't be intercepted?

How do I choose the best authentication system?

In addition to these Fact Sheets, you can also use the services of specialist consultants on computer security issues.

If you are searching the Web on this topic, try the following search terms:

- **e-security; information security; security settings; security updates.**

A directory of Australian businesses providing electronic authentication expertise and services can be found at <http://www.aeema.asn.au/neac>

The Defence Signals Directorate plays a key role in the protection of Australian official communications and information systems and has established the Australasian Information Security Evaluation Program. E-security products are listed on the Evaluated Products List – <http://www.dsd.gov.au/infosec/>

AusCert also provides a single, trusted point of contact in Australia for the Internet community to deal with computer security incidents and their prevention. Their checklists and information papers are available at http://www.auscert.org.au/Information/Auscert_info/papers.html

Australia has taken a prominent role in the development of consumer protection in electronic commerce internationally. For more information on key national consumer regulatory policy issues see <http://www.ecommerce.treasury.gov.au/> and for practical self-help information on consumer protection in Australia see <http://www.consumersonline.gov.au/>

The Business Entry Point (www.business.gov.au) provides online government services and information for Australian business. This includes information on start-up, assistance, taxation, licences, legislation, as well as significant transactions such as taxation compliance and licence applications.

About NOIE



NOIE is the National Office for the Information Economy – Australia's lead Commonwealth agency for information economy issues.

NOIE is helping Australians create a world-class online economy and society through its work coordinating Commonwealth Government responses to the information revolution. NOIE develops and coordinates advice to the Government on information economy issues.

NOIE's key priorities in 2002 are to:

- Promote E-Security, facilitating implementation of a coordinated National e-Security Agenda;
- Accelerate the uptake of e-business and e-procurement by small to medium business enterprises;
- Develop strategic advice on the demand drivers for Broadband, and provide the secretariat for the Australian Broadband Advisory Group;
- Encourage economic transformation through better information and communications technology (ICT) use across the Australian economy;
- Transform Australian government information, services and administration through application of information and communications technologies;
- Map the long term strategic environment for the ICT industry, as a contribution to the ICT Industry 'Framework For the Future' study.

www.noie.gov.au/trustingtheinternet

