



SMEs Guide to Privacy and Security Obligations - an eB2Bcom White Paper



Date: 14 December 2005

Version: 1.0

Prepared By: eB2Bcom Pty Ltd
Suite 1, 85-87 Charles St
Kew, Vic 3101 Australia
Phone: +61-39851 8600
Fax: +61-39851 8601

DOCUMENT DETAILS

Author: Lisa Vuu BA InfoSys

DOCUMENT SECURITY

This document contains intellectual property of eB2Bcom, and is provided on a COMMERCIAL-IN-CONFIDENCE basis to the party ("Client") named on the front page. It is solely for the use by the staff of Client for the consideration and evaluation of eB2Bcom's proposals. It must not be provided in whole or in part to third parties without the express approval of an authorised officer of eB2Bcom.

REVIEW

Reviewed by: Andrew Ferguson, Troy Braban, and Trevor Hancock
eB2Bcom

DOCUMENT HISTORY

Version	Comment	Date
0.1	First draft – Lisa Vuu	20 October 2005
0.2	Second draft – Andrew Ferguson	10 November 2005
0.3	Third draft – Troy Braban, Trevor Hancock	15 November 2005 08 December 2005
1.0	Approved – Andrew Ferguson	14 December 2005

TABLE OF CONTENTS

DOCUMENT DETAILS	2
DOCUMENT SECURITY	2
REVIEW	2
DOCUMENT HISTORY	2
TABLE OF CONTENTS.....	3
CREDENTIALS.....	4
INTRODUCTION	4
BACKGROUND.....	4
INFORMATION PRIVACY PRINCIPLE	5
<i>Information Privacy Principle 4 – Data Security</i>	5
ISSUES	6
<i>Email</i>	6
<i>PDAs</i>	7
<i>File and Data Security</i>	8
<i>Backup Tapes</i>	8
<i>Removable Media</i>	9
<i>USB Ports</i>	10
SECURITY STRATEGIES AND SOLUTIONS.....	11
<i>PC Desktop Security</i>	11
<i>PDA Security</i>	11
<i>Access Control</i>	11
<i>Removable Media Management</i>	11
<i>Email Security and Labelling</i>	12
<i>File and Data Protection</i>	12
<i>Backup Tape Protection</i>	12
<i>USB Port Protection</i>	12
CONCLUSION.....	13
REFERENCES.....	14

CREDENTIALS

eB2Bcom specialises in security, identity management and associated infrastructure. We are an established provider of software and services to Defence, Intelligence, Police and Government Agencies as well as the private sector. eB2Bcom has offices and works with a range of partners throughout South East Asia, Australia and New Zealand.

INTRODUCTION

Security and privacy issues are common in organisations nowadays especially in Small-to-Medium Enterprises (SMEs). The aim of this whitepaper is to advise SMEs on what can be done to enforce and comply with the privacy legislation. In this paper, several functionalities will be described to assist organisations in protecting their data and manage privacy and security.

BACKGROUND

The Privacy Act – Information Privacy Principle was created to regulate the way in which organisational information is collected, used and handled. Its purpose is to make organisations more responsible for the protection of organisational and customer data.

Recent privacy issues in the media clearly illustrate the electronic threats and increased regulatory demands on organisations today. Privacy and security are important issues for Australian Small-To-Medium Enterprises (SMEs). All organisations must protect themselves and address increasing internal & external concerns and regulations around privacy.

Most companies have not taken an encompassing view of security issues. Organisations are dealing with pieces of data security problems and not really tackling the overall issue by focusing attention on current privacy issues. Only some Australian SMEs have adopted security in accordance to information privacy principles.

SMEs have been really short on action in relation to the privacy amendments, with most business not adequately prepared for the changes and preoccupied with obtaining the latest security technology. Organisations need to be aware of how the legislative changes will affect the way personal information is stored and handled and need to start developing information privacy regulations and adopt the technology which carries out these regulations.

INFORMATION PRIVACY PRINCIPLE

The Information Privacy Principles provide a set of policies that regulate the way that an organisation collects, uses and handles confidential information. These sets of standards govern the benchmark procedures of an organisation and which protect the privacy of individuals. For example, many SMEs run autonomous decentralised operations. Records may be stored in a few different places and several of those places may not be physically or electronically secure. This is a legal violation under the Information Privacy Principle. The assessment is stringent and comprehensive and non-compliance can result in substantial fines and even imprisonment.

The Privacy Impact Assessment will:

- identify what areas are at risk and what security arrangements are needed;
- help organisations assess whether the personal information is protected by security procedures commensurate with the sensitivity of the information.

Other objectives of these principles are:

- To demonstrate an organisations commitment to protecting information privacy and to address the privacy concerns that the use of electronic technology may raise
- To describe the way an organisation collects, uses and handles personal information
- To ensure an organisation adopts and complies with the provisions of the Privacy Act that relate to the use and disclosure of information
- To facilitate an organisations compliance with any further developments in privacy protection through legislation or industry standards

Information Privacy Principle 4 – Data Security

Information Privacy Principle 4 states that an organisation should take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure.

There are four points as outlined in the Privacy Act that assist an organisation in determining which technology and what security software would be most suited. eB2Bcom can extensively assist your company with points three and four in the area of security and deterrence/detection of misuse.

1. Right to know

Who has a right or ability to access the information?

Who has authority to access, change, add or delete information?

Who authorises those access rights?

2. Need to know

Is access limited to only those individuals who need to have access to the information to carry out their roles?

Is it necessary to limit the amount of information accessible to certain person, depending on their role?

3. Security

Where information is to be stored or transmitted electronically or otherwise, how secure is the storage and method of transmission?

Using data protection technology solutions ensures that sensitive customer or employee information remains private and their critical business transactions remain

Commercial in Confidence

trusted and secure. eB2Bcom offers data protection technology solutions that easily integrate into existing infrastructure and take advantage of the latest technology and industry standards.

4. Deterrence/Detection of misuse

*How will the information be secured from internal and external misuse?
How is misuse deterred and, if it were to occur, how is it detected?*

Authentication and Credential Management

eB2Bcom can suggest solutions which allow organisations to use authentication and identity management technology solutions to manage trusted identities through strong authentication and password management.

Information Access Management

Although organisations need to ensure that diverse groups of users have access to the resources they need to be productive, companies also need to secure those resources from unauthorised access.

Detection Management

Audit logs and Intrusion detection are means of detecting unauthorised activity to access sensitive or private information. Organisations should document their secure measures. If there is a privacy breach, eB2Bcom can recommend technology which can show they took all reasonable measures to safeguard their data, prevent security risks and analysed the potential for unauthorised disclosure or misuse.

ISSUES

There are a number of ways in which corporate data can be stolen or lost. This can be through:

- Email
- PDAs
- File and Data Security
- BackUp Tapes
- Removable Media
- USB Ports

Email

Today in most companies email is mission critical. Unfortunately today's email comes with spam and viruses. With the continuing evolution of email and Web-based threats, organisations are more exposed than ever before and the need to defend against them has never been greater. These threats, which can include spam, inappropriate content and legal liability for example, must be addressed in both internal and external email as well as email uploads and downloads. To maintain the highest levels of security, organisations email server needs to be maintained and kept up-to-date with current policies.

Organisations are also being forced to conduct business within increasingly tight legislative and regulatory guidelines, set down by governments and industry bodies around the world. Ensuring compliance means that companies need to secure each and every gateway for electronic communications. To avoid this becoming an administrative nightmare, companies need to be able to centrally deploy, manage and report on an encryption system that is cost-effective, transparent to end-users and can be used to send secure messages to anyone.

Having an effective e-Policy is at the heart of safely and effectively exploiting the most valuable of modern business communication channels – email. A corporate

Commercial in Confidence

email system, if inappropriately used, or inadequately managed and protected can lead to high profile security breaches, expensive lawsuits and damaged reputations. Employees may inadvertently and sometimes purposefully leak internal information to the public and competitors through email. In organisations these days with most of the paperwork being converted to electronic means, security has become more vital.

It is easy to make a mistake and send an email to the wrong person. For example in August 2005, up to 20,000 pages of confidential police files were leaked by Victoria Police in one of the biggest breaches of privacy in the state's history. (T.Giles, 2005) The files sent to the prison officer contained information including the full name and private addresses of victims of crimes, including victims of rape and sexual assault, and the records of alleged offenders.

Employees might also accidentally send along confidential information to a third party without even knowing it. While a phone call or outside discussion cannot be stopped, a content rich email with supporting company documents can often be more dangerous in the wrong hands. Therefore a flexible security solution will allow organisations to create policies based on security measures.

Establishing, enforcing and maintaining corporate email policy can be achieved through the implementation of eB2Bcom's email monitoring and security software. That can ensure all messages containing executable attachments are now being blocked before they reach your internal system. This will also have the effect of blocking messages containing flash animations, games, etc. which are mainly of a non-business nature.

Another key area for many organisations today is the application of security labeling to each message. That is the application of either a formal classification label (Top Secret, Commercial in Confidence, Directors Eyes only etc) contained either in a formal label or carried in the First Line of Text in the Message (FLOT). As well as adding the label at the client (There are solutions available for Outlook and Notes), one also needs the ability to have that control afforded to sensitive information, achieved by applying consistent labeling of messages (e.g. Commercial in Confidence) and regulating the movement of this sensitive information at the Email Gateway to the Internet.

The task of monitoring e-mail should be simple by using a powerful keyword and phrase search engine that can spot words and phrases even if they are miss spelt, have endings such as "ed" and "ing" or use "sound-alike" spelling and providing boundary protection wherever an organisation has a "trust gap", such as between the corporate intranet and the Internet, for example. Such solutions act as a "proxy" server intercepting and examining messaging traffic, under the direction of the policy configuration and management tool.

PDA's

PDA's are everywhere these days. The strengths of the PDA are also what make them so easily susceptible to being lost or misplaced and also make them easy targets for thieves and hackers. PDA's have very few security features built-in. Pre-programmed security usually consists of little more than password based authentication.

The implication of a breach of PDA security on PDA users, their clients, patients and employers can be extremely detrimental. For example, thieves net about \$85 per holdup and are caught 80% of the time. Information thefts average \$800,000 in

Commercial in Confidence

value and are caught 2% of the time. (Lyon, 2002) That is why it is crucial to be proactive and install high levels of security at all of the PDA's vulnerable points.

For instance, in the health sector, a potential situation for GP's and specialists would be a patient whose personal and/or confidential information may be stored on their doctors hand held device. By storing this information on the PDA, the patient does not have any control or influence on the security measures adopted by the owner. This breach of patient confidential information may subject the doctor to legal liability for breach of their physician-patient privilege.

In the end confidentiality starts with putting policies in place and educating employees. It won't prevent breaches altogether, but it will help to raise awareness about the potential severity of even an accidental breach.

To keep the mobile workforce secure, strong encryption keeps data confidential – even in transit over the Internet. Also having a transparent background operation means that users do not need training or elaborate new work routines. And easy central implementation and enforcement of the company security policy keep the environment consistently protected.

File and Data Security

IT officers want steady network operations. Additional security software must be integrated smoothly and its use must not be an obstacle for administration or for end-users. As far as solutions for the protection against unauthorised file access are concerned, there are specific organisational and technical requirements that need to be addressed. Multiple users should have simultaneously but exclusive access to confidential files: locally or in networks on hard drives and mobile storage media and devices. Most data protection measures are designed to counter danger from outside a company, while most in-house risks are usually ignored. However, the potential for damage caused by the misuse of confidential company data is exactly the same.

The current practice of saving data centrally on servers, multi-site workplace networking and the use of mobile data media means that security risks are become greater and greater. As more and more organisations outsource their IT departments, in an effort to reduce costs, they are finding that their worries about data confidentiality increase accordingly. What is needed is an eB2Bcom security solution that only lets authorised user groups access sensitive data across an organisation, since even in-house system administrators or personnel from the outsourcing company should not be permitted to see confidential data.

Backup Tapes

In many cases in organisations, low paid workers are handling sensitive back up tapes, but only a small fraction of organisations are securing the data with encryption. (Lemos, 2005) These days many organisations are reconsidering their security and backup policies after a number of organisations have admitted that tapes holding unencrypted customer data have gone missing. For instance, one trading firm recently acknowledged that the company that handles its backup data had lost a tape containing information on about 200,000 customers. The financial firm had to dramatically revise its backup policies and, in the interim, halted all movement of backup tapes. (Lemos, 2005)

One of the important things SMEs need to understand is that unencrypted information stored on backup tapes is difficult to read, but it is not impossible. Companies need to reassess their backup strategies and seriously consider

Commercial in Confidence

encrypting sensitive data to prevent a potential breach of privacy. The reconsideration of backup policies comes as the whole financial industry sector is recovering from several high-profile data leaks due to lost or stolen tapes. A large Bank recently told government officials in February that the company had lost a tape containing account information on a large number of government credit-card holders. (Lemos, 2005) Even without evidence of theft, the lack of encryption is disturbing, if entirely expected.

Recently an analyst from a research firm polled almost 400 companies and found that, despite renewed focus on securing customer data, more than 60 percent of the companies do not encrypt any of their backup data, and only 7 percent actually encrypt all their backup data. (Lemos, 2005) Two-thirds of the financial firms polled never encrypted the data that they were backing up. The majority of larger firms also failed to encrypt their backup data, with about 56 percent of companies with revenues greater than \$1 billion never having encrypted their data before putting it on tape. Online backup services that fail to encrypt information could represent similar security risks as does any information stored on a hard drive that can easily be stolen, pointing to a recent rash of stolen laptops that contained medical information.

Because backups tend to be done by the least important members of the information technology staff, sometimes disparaged as "tape monkeys," and therefore the tapes are at greater risk of insider attacks as well. Moreover, insiders have the access to know what data is on each tape, information that could help identity thieves target the right tapes. "The process is totally insecure," one recent article said. "You put you most junior people on this job, and those are the people that are most likely to be bribed and look for another way to make money." Jon Oltsik, senior research analyst for the Enterprise Strategy Group. (Lemos, 2005)

Removable Media

Controlling data import/export functions is an important issue when maintaining IT environments where users handle sensitive data. Denying the ability to use removable media like floppy drives or CD-ROM's is usually not a feasible solution. Administrators might want to allow a user to use a CD with the latest customer or catalogue database, phonebook or navigation data. On the other hand, the administrator might want the user to be prevented from importing personal CD-ROMs containing games or potential virus infected code.

What is needed is some sort of centrally managed advanced security removable media management capability that allows a Network or security administrator to define which CDs or DVDs shall be accessible by certain users. The administrator simply scans allowed media with a management console and creates a set of checksums. Only media then corresponding to an approved checksum may be accessible by users when this function is activated. Depending on security/performance demands, checksums can be created over the disk ID, the directory or the complete content of a disk.

Using solutions like this company will realise the following benefits:

- Users can make use of removable media for business purposes. Drives need not be completely blocked.
- Administrators can be sure that users do not introduce malicious or virus infected code to their computer via these media.
- Administrators can be sure that the users do not introduce unauthorised or unlicensed software (e.g. games or company software the users have no right for).

USB Ports

Nearly all current computers (PCs, Notebooks, PDAs) have interfaces (USB, Firewire or Bluetooth) which support Plug and Play. In Windows 2000 and XP operating systems, Plug and Play (PnP) devices can be connected by users and be used exported, so downloads via the company's immediately, also in a wireless mode. USB ports cannot be controlled or deactivated by operating system resources. Users are able to export and import files without being controlled by means of cost-effective PnP memory media. By implementing some sort of PnP Management tool it protects from:

Export:

PnP memory media are big enough to take up server backups, complete customer databases and other files. Data theft has never been easier.

Import:

Viruses and Trojans can be introduced very easily and endanger the stability of the IT environment. Virus scanners are updated regularly, but what if the user had been on the road for a week? Users are able to import games and other unwanted programs or data (e.g. MP3 files). This way, the productivity may suffer, let alone provide license violations.

By using PnP protection, the private use of the company IT systems can be stopped. This reduces expenses and spares resources. PnP Management closes the gaps on PnP interfaces and preserves the complete integrity of the IT infrastructure and productivity of the staff.

PCs have many weak spots such as USB, DVD and CD drives. Sensitive information stored on these devices demand constant protection. Technology is required to prevent unauthorised users from access this information and copying the data.

The IT infrastructure has many potential weak spots. Sensitive information stored on servers and personal devices demand around the clock protection. Security issues include prohibiting unauthorised access to devices, application and the company networks preventing users from installing unauthorised software and hardware and blocking unauthorised web access. By protecting these areas, SME can guard against unauthorised access and misuse as well as import and export of data.

Controlling data import/export function is an important issue maintaining IT environments where users handle sensitive data. Denying the ability to use removable media like floppy drives or CD-ROMs is usually not a feasible solution. Administrators might want to allow a user to use a CD with the latest customer or catalogue database, phonebook or navigation data. On the other hand, the administrator might want the user to be prevented from importing personal CD-ROMs containing games or potential virus infected code.

SECURITY STRATEGIES AND SOLUTIONS

Levels of security adoption are strongly related to the complexity of the IT environment that SMEs operate in. Companies buying security technologies are addressing resources in specific areas particularly investing in anti-virus tools, firewall appliances and security solutions. However, many Australian SMEs are still convinced that simply having some security solution is enough. These companies are lacking policies to implement and enforce security. This approach needs to change because the privacy of SMEs may be compromised in a number of ways when the Internet is widely used for businesses.

eB2Bcom is an innovative Australian company specialising in the privacy and security advice solutions. eB2Bcom can assist in the following areas of data security for PDA's, PC security and encryption as well as solutions for email security such as:

PC Desktop Security

Organisations need an eB2Bcom solution that provides organisational data protection where no authorised user may access the device, read data or use the device as a tool to enter the company network. If a device gets into unauthorised hands the data is securely protected even if the hard disk is removed. Complete encryption of the entire hard disk and a user authentication procedure should run before the operating systems boots to provide secure protection.

PDA Security

To keep the mobile workforce secure, organisations need a solution that provides strong encryption to keep data confidential as well as in transit over the Internet. There are many types of authentication mechanisms available such as biometric signature recognition or symbol pin. In addition to enhancing security, the software adopted must also be easy to use. The products recommended should have a transparent background operation where users do not need training on elaborate new work routines. eB2Bcom can provide solutions such as this.

Access Control

Today's networked business environment, the unstoppable and rapid emergence of mobile computing make a business's IT infrastructure a key ingredient for business success. Likewise, the IT infrastructure has many potential weak spots. Sensitive information stored on servers and personal devices demand around the clock protection and system availability is a prerequisite for business continuity. Therefore, unauthorised access to the IT infrastructure is a major concern. Security issues include prohibiting unauthorised access to devices, applications, and the company network, preventing users from installing unauthorised software and hardware, and blocking unauthorised web access. eB2Bcom can assist organisations to make serious efforts to establish company wide security policies and enforce them.

Removable Media Management

Often users have access to data on certain removable media such as CDs or DVDs. However, in managed IT environments, not all media types should be available to all users. Programs installed by an unauthorised user from a CD can endanger system integrity or can cause license violations or perhaps infections from new viruses. eB2Bcom has a solution that allows a user to make use of only specific types of media that have been approved by administrators.

Email Security and Labelling

The spread of email is continuing at a rapid rate in regards to personal communication and more significantly as a valuable business tool. Most organisations place great emphasis on their email environments for communication to staff, customers, partners and amongst senior management. As this grows, the type and value of information that is often exchanged means that it should be protected against unauthorised access or accidental misuse. Legal and privacy implications also need to be considered. eB2Bcom can aid organisations to classify their email (For instance to separate personal from customer from management communication) and provide far greater security than is provided by standard email programs.

File and Data Protection

Today, at almost every PC workstation in most organisations, access is available to proprietary or confidential data in file form. In modern IT environments complete control over the use and distribution of confidential data seems impossible. It is a difficult enough task to restrict access to confidential data to authorised users. Additional challenges to data security are created by file storage in multiple locations, system use by business partners or consultants, and by the increasing use of outsourced service providers. Some information has to be protected to fulfill legal regulations, such as staff and customer data. However, the access to critical data such as management reports or the results from the R&D department or product development must be controlled. Announcing or publishing confidential corporate data by unauthorised persons can have serious legal, financial and productivity consequences. It is also important to introduce into system administration a "division of powers" between system administrators and IT security staff. Due to inherent risks involved, end users cannot be counted on to guard corporate secrets. Manual systems for secure data storage and encryption cannot be relied upon. Therefore, eB2bcom automated solutions that protect data from unauthorised access without end-user interaction is required.

Backup Tape Protection

There are many choices for back up protection. The tape is the most universally accepted backup medium as it provides many advantages in terms of its transportability and cost effectiveness.

eB2Bcom can assist in recommending which backup software solution to use. Backup software is designed to manage the replication of primary data files to a secondary storage medium and catalogue their location on the new medium in a database. Depending on the organisation need, there are different types of backup including full back up, differential back and incremental backup.

Data and storage requirements are growing at extreme rates for SME's. While every organisation will have individual needs to support the protection of their data, the most common issue faced is development of the business process to support data protection.

USB Port Protection

Company wide security USB policies should be implemented regardless of whether users work with different platforms or access different devices – PCs, notebooks, terminal servers. It is recommended that organisations adopt software which allows the administrator to define certain CDs or DVDs that can be accessed by certain users. The administrator can simply scan the allowed media with the console and

Commercial in Confidence

create a set of checksums. Only media corresponding to an approved checksum may be accessible by users when this function is activated.

CONCLUSION

Today's regulatory environment demands that organisations address internal and external concerns around privacy, confidentiality and security. A comprehensive security plan must include the aspects described above.

It is critical that privacy is placed on the business agenda at the board level and not the IT level. Privacy law changes can affect everything from using information to storing personal information. It is up to an organisation to take 'reasonable steps' to ensure information privacy.

eB2Bcom provides cost-effective advice and solutions to SMEs, governments, and larger enterprises – we can help you.

eB2Bcom can offer unique protection for confidential data against access by any unauthorised insider or outsider. Even in-house system administrators or personnel from the outsourcing company would not be able to gain access to confidential data. They can still manage the system as usual but have no means to decrypt any files. Organisations need a fully-automated file encryption to provide valuable protection for confidential files. The bottom line is that organisations need to treat their data with greater care.

REFERENCES

Giles, T (2005) **Police Files Debacle**,
http://www.heraldsun.news.com.au/common/story_page/0,5478,16273836%255E2862,00.html, August 2005

John, Sunny (2005) **Protecting Data to Deliver Business Value**, IT Observer, August 2005

Lemos. R (2005) **Backups Tapes are Backdoor for Identity Thieves**, Security Focus, April 28th 2005

Lyon. D.M (2002) **The Dilemma of PDA Security: An overview**, SANS Institute

Sophos (2005) **Effective Compliance Practices: Information security, email security, proof of control**, May 2005

Cisco (2002) **Privacy, Security, Personal Health Records and the Enterprise**, CIO

Ziff Davis Media, **Best Practices in Messaging Security**, November 2004



Sydney: +61-2-9779-1597
Melbourne: +61-3 -9896-7800
Brisbane: +61-7-3871-1440
Singapore: +65-6841-7374
email: sales@eb2bcom.com
Web: www.eb2bcom.com