informatica

The Australian data privacy index

The Australian data privacy index

Introduction

Data privacy is a key issue for Australian organisations. The risk to businesses that fail to protect the sensitive information of their customers, employees, suppliers and partners can be high in terms of damage to the organisation's reputation as well as the possibility of legal action.

In Australia, companies like Telstra, Vodafone, Australia Post and AAPT having all fallen victim to data breaches. What this demonstrates is that no organisation, big or small, is excluded from the risk of potential data breaches.

Some organisations may already have had data breaches that have not been widely publicised. However, the mandatory data breach notification laws being considered by the Australian government will mean that more people will know about breaches and the risk to an organisation's reputation will be higher. With the aim of protecting consumers, the requirement to notify will mean organisations will need to more vigilant in protecting sensitive data.

The most commonly thought-of form of data theft occurs when malicious individuals hack into production databases. This has caused many companies to get serious about protecting the data that sits at this level.

However, there is an important tier of data that remains vulnerable. Non-production systems used for development, testing and training purposes use real data, including financial records and identification numbers. Currently most organisations do not adequately protect these environments, making them a soft target for data theft.

It is essential for organisations to consider these environments when developing data protection strategies. Policies and procedures are just as important as technical solutions and both should be used in combination to create a culture of security across the organisation.

What

The Australian Data Privacy Index 2013 provides a snapshot of how Australian organisations view and treat data privacy.

Why

The importance of maintaining controls over the access to sensitive information held by companies is not disputed. The aim of this index is to give Australian organisations a measure to benchmark against other organisations and provide valuable learnings into the challenges other businesses face with data privacy.

The Australian data privacy index 2013 is designed to assess:

- the level of focus placed on data privacy by Australian organisations
- the extent to which data loss has already been experienced
- the potential consequences of data loss
- plans for future implementation of data privacy strategies.

How

Outsource, a third party marketing company, conducted the research for this index on behalf of Informatica. 109 senior IT decision makers from organisations employing up to 25,000 people were surveyed via an outbound telemarketing and email campaign. They represented a variety of industries including manufacturing, utilities, finance, health and pharmaceuticals, retail, technology, entertainment and transport.

When

The survey was conducted in April and May 2013.

What is data privacy?

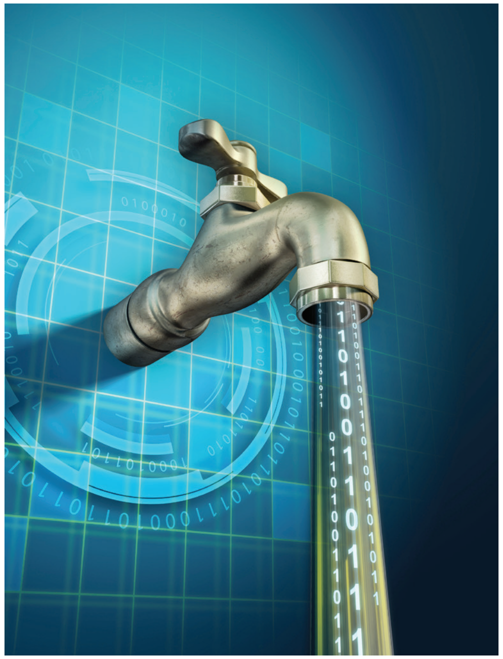
Organisations collect personal information about their customers, staff and partners every day. When this information can be used to identify an individual, it is considered to be sensitive information. Sensitive information may include health or financial records, ethnicity and other demographic information as well as names, addresses and/or birthdates.

Because this type of information can be used for malicious purposes including identity theft or fraud, organisations must be able to store and access the information appropriately while protecting it from unauthorised access.

There are a number of ways to ensure data privacy, from software that encrypts or masks the information to hardware that physically prevents access to the information.

Data privacy is regulated in Australia by the Federal Government's Privacy Act.

Executive summary



31 per cent of organisations have experienced data theft and 30 per cent of those organisations reported damage to their reputation. Only 7.5 per cent of the respondents are very confident that they would be able to even detect the unintentional loss of data. 28.5 per cent say they are confident that they would be able to detect a data loss. 29 per cent of companies say they are not confident they would be able to detect the unintentional loss of information.

While 61 per cent of organisations believe it is critical or very critical to protect data, 21 per cent have no adequate controls in place.

92 per cent of Australian organisations say they believe it is important to some extent to anonymise, mask, suppress or encrypt sensitive information contained in databases. However, they don't pay enough attention to testing and development environments, which is a key area of data vulnerability. In fact, 62 per cent of the respondents agree that their organisation is more concerned with the production environment than the development or testing environments, despite the fact that real data is used in these environments and can be stolen. Many organisations are unaware of the sensitive information that is stored in these non-production environments.

The bottom line is that many Australian organisations do not fully understand the importance of data privacy or the repercussions for failing to protect sensitive information. Currently, many organisations do not fully protect sensitive data, particularly in the development and testing environments, making this a key weakness. In addition, with more companies outsourcing their sensitive information to 3rd parties and the cloud, there is increasing concern to ensure data privacy.

Key findings

Cause for concern

- 40 per cent of those who had experienced data loss said they didn't know what the consequences were. 30 per cent said their reputation was affected.
- 70 per cent of organisations outsource some or all of their IT infrastructure and/or support.
- Only 7.5 per cent of respondents were very confident that their organisation would be able to detect the unintentional loss or theft of sensitive information contained in the company's databases or applications in the production environment.
- 21 per cent of organisations do not have a data privacy strategy in place, nor do they mask data to protect sensitive information.
- 57 per cent said that deploying a data privacy solution was difficult because manual controls were in place, including policies and procedures. 33 per cent said it was because there was no budget allocated to fund a solution.
- The production environment is of highest concern with 62 per cent of respondents agreeing that their organisation is more concerned about information protection in the production versus the development or testing environments.
- This is despite only 53 per cent agreeing that a data breach is more likely to happen in the production versus the development or testing environments.

Good practice

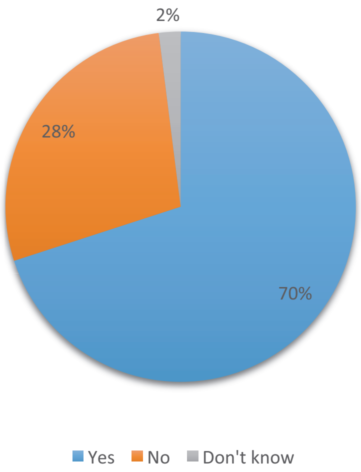
- 61 per cent of respondents said sensitive personal data had never been compromised or stolen by a malicious insider such as a privileged user.
- Two thirds (66 per cent) of respondents are confident to some extent that their organisation would be able to detect the unintentional loss or theft of sensitive personal information contained in databases or applications operated by third parties, including cloud providers.
- Of the organisations that do take steps to protect data, 64 per cent favoured encryption as the key method.
- Of the organisations that do not have a strategy in place, 31.5 per cent plan to put one in place within the next 12-24 months.
- 63 per cent of respondents said they believed their data was adequately masked and/or protected, while 24 per cent said no adequate controls were in place.
- Approximately half (51 per cent) say their organisation does not find it difficult to comply with the amount of privacy and data protection regulations.
- Almost all of the organisations surveyed (92 per cent) said their organisation believes it is important to some extent to anonymise, mask, suppress or encrypt sensitive information contained in databases.

What does this mean for organisations?

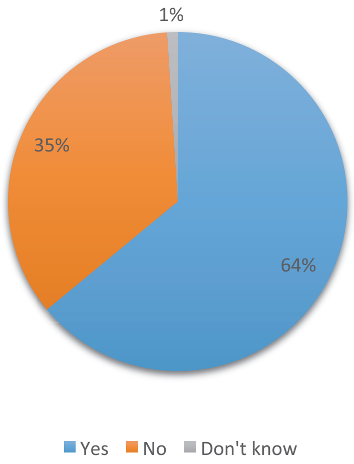
These results show that Australian organisations believe data protection and data privacy are extremely important. However, when it comes to having the right mechanisms in place or knowing how to protect data, there are still gaps. Organisations need to be able to quickly, easily, and cost-effectively manage and protect their private and sensitive data, decrease the risk of data breaches and effectively meet compliance requirements for production and non-production environments.

Results

Do you outsource some or all of your IT infrastructure and/or support?



Do you have a lot of external interfaces to other vendors/environments?

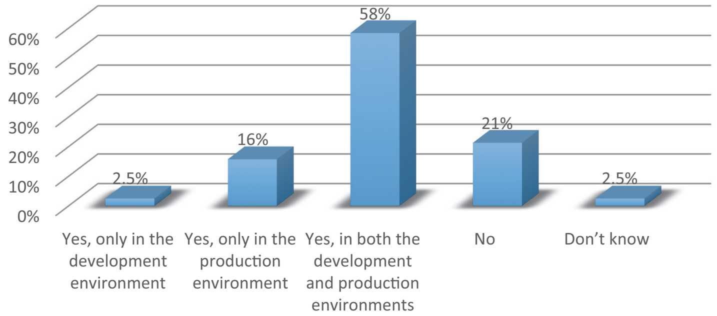


70 per cent of respondents do outsource some or all of their IT infrastructure and/or support, while 28 per cent do not.

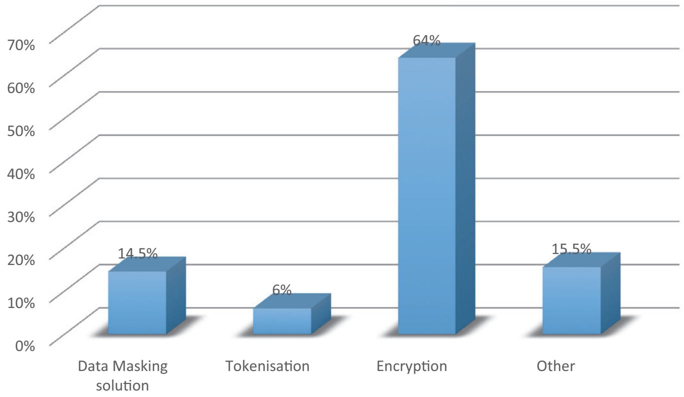
Two per cent of respondents did not know whether they outsource any of their IT infrastructure and/or support.

Two thirds of respondents (64 per cent) reported what they believed to be 'a lot' of external interfaces to other vendors/environments.

Results



Does your organisation have a data privacy strategy (i.e. policy, in place) and/or mask sensitive data to protect sensitive information such as company financial information, company revenues, customer account details, employee records, and/or payment tra



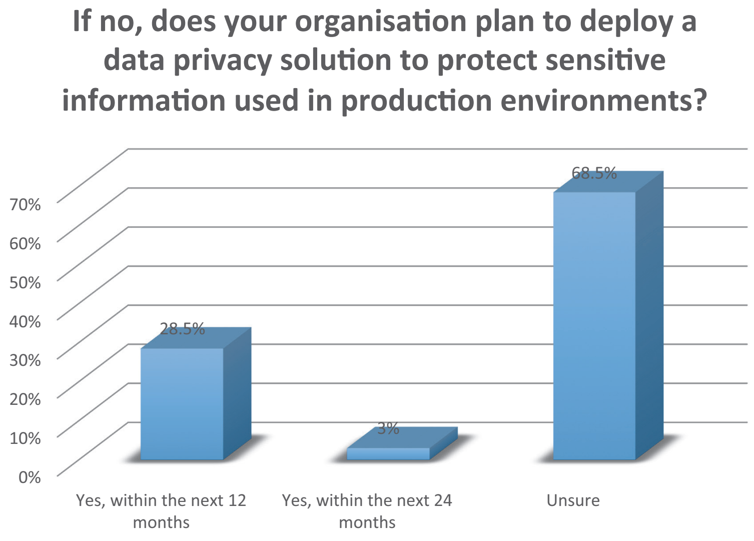
If yes, does your data privacy strategy include any of the following?

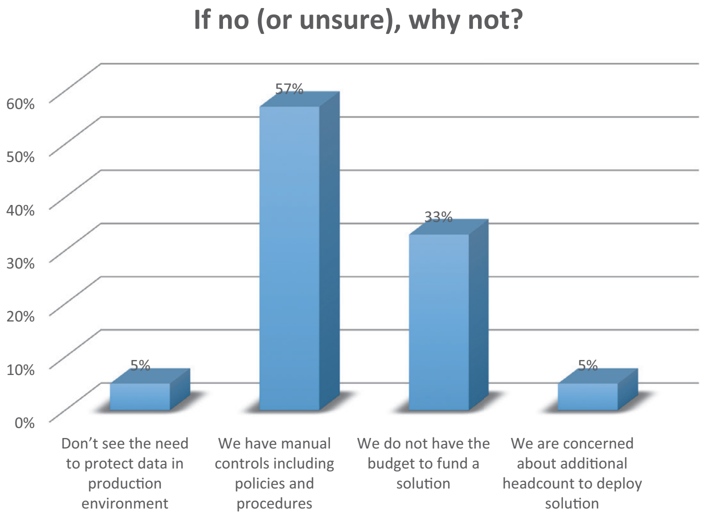
Three quarters (76 per cent) of respondents reported that their organisation does have a data privacy strategy in place and/or masks sensitive data either in the development environment (two per cent), in the production environment (16 per cent) or in both environments (58 per cent).

21 per cent did not have a data privacy strategy in place, nor did they mask data to protect sensitive information.

Of those respondents who did have a data privacy strategy in place, 64 per cent included encryption, 14.5 per cent included data masking solutions and just 6 per cent included tokenisation. 15 per cent used some other approach to data privacy.

Results





Of the respondents who reported not having a data privacy strategy in place, more than 30 per cent said their organisations planned to deploy a data privacy solution in the next 24 months, with 28.5 per cent planning to do so within the next 12 months.

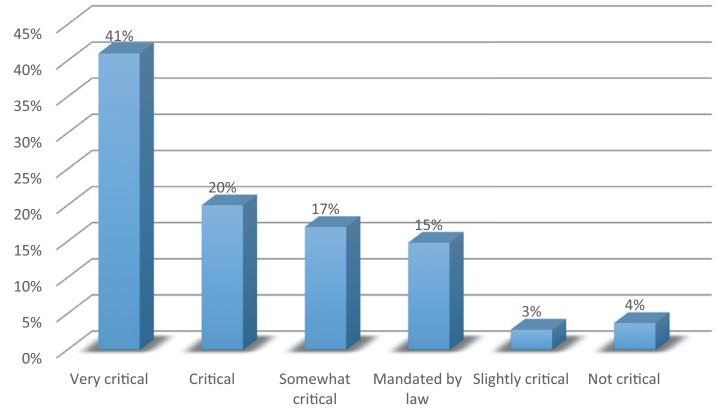
Of the respondents who said they were unsure about deploying a data privacy solution 57 per cent said this was because manual controls were in place, including policies and procedures.

33 per cent said it was because there was no available budget to fund a solution while 5 per cent said they were concerned about the additional headcount needed to deploy a solution.

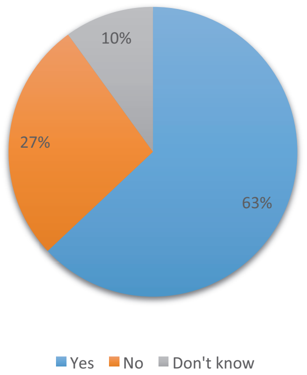
5 per cent of respondents said they didn't see the need to protect data in a production environment at all.

Results

How critical is protecting data in your organisation?



Do you currently believe that your data is adequately masked and/or protected?

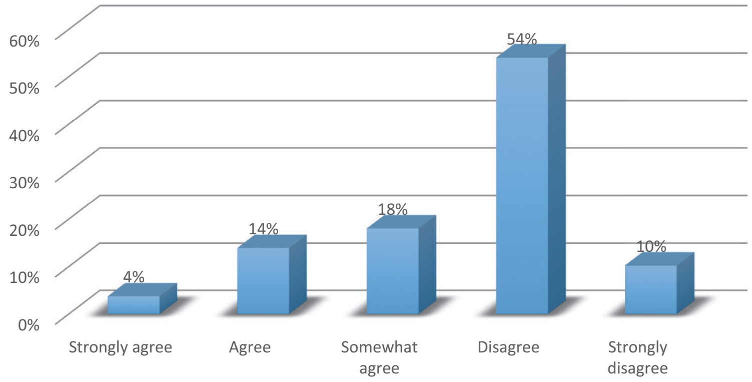


More than half (61 per cent) of respondents believe it is very critical to critical to protect data in their organisation

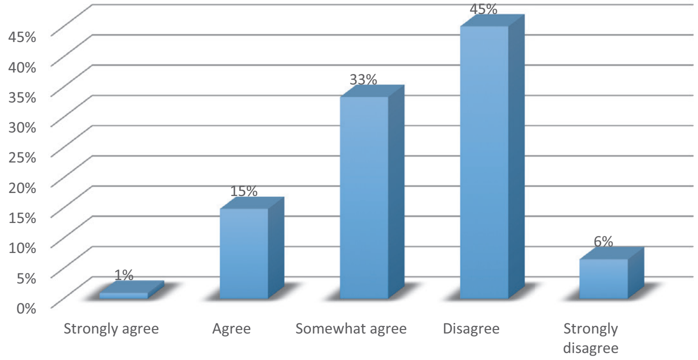
63 per cent of respondents said they believed their data was adequately masked and/or protected. 27 per cent said they did not believe their data was adequately masked and/or protected.

Results

My organisation finds it difficult to restrict user access to sensitive information in the IT and business environments.



My organisation finds it difficult to comply with the amount of privacy and data protection regulations.

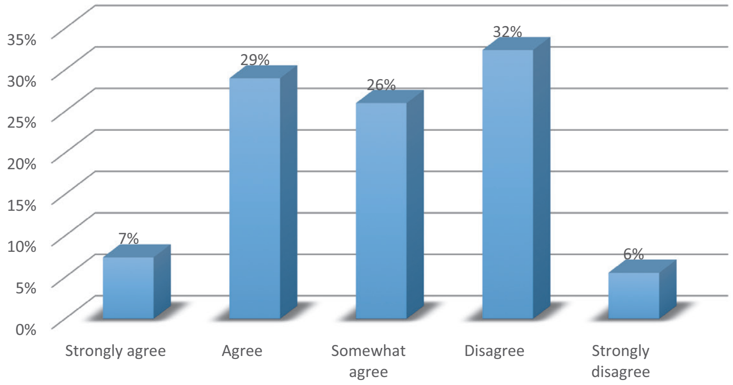


More than half (54 per cent) of respondents disagree with the statement that their organisation finds it difficult to restrict user access to sensitive information in the IT and business environments. A further 10 per cent strongly disagree with that statement.

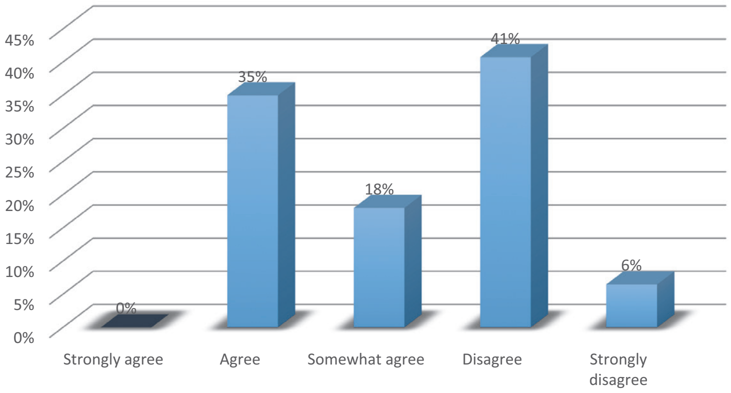
Almost half (49 per cent) of respondents agree that their organisation finds it difficult to comply with the amount of privacy and data protection regulations.

Results

My organisation is more concerned about information protection in the production versus the development or testing environments.



In my organisation, data breaches are more likely to occur in production versus development or testing environments.



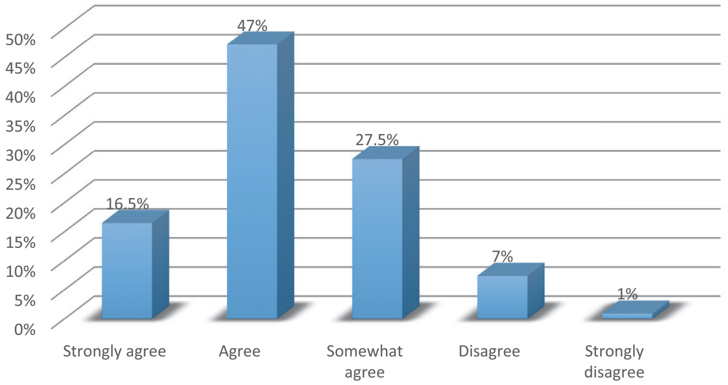
When asked whether their organisation was more concerned about information protection in the production versus the development or testing environments, most respondents agreed to some extent, with 7 per cent strongly agreeing, 29 per cent agreeing and 26 per cent somewhat agreeing.

None of the respondents strongly agreed that, in their organisation, data breaches were more likely to occur in production versus development or testing environments. 41 per cent disagreed with the statement and 6 per cent strongly disagreed.

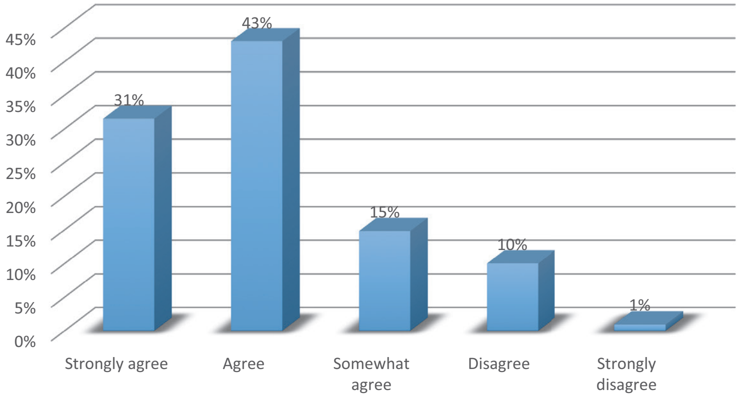
35 per cent said that data breaches were more likely to occur in the production environment and 18 per cent somewhat agreed.

Results

My organisation believes it is important to anonymise, mask, suppress, or encrypt sensitive information contained in databases, storage devices and servers.



My organisation believes it is important to anonymise, mask, suppress, or encrypt sensitive information before transferring this data to third parties including cloud providers.

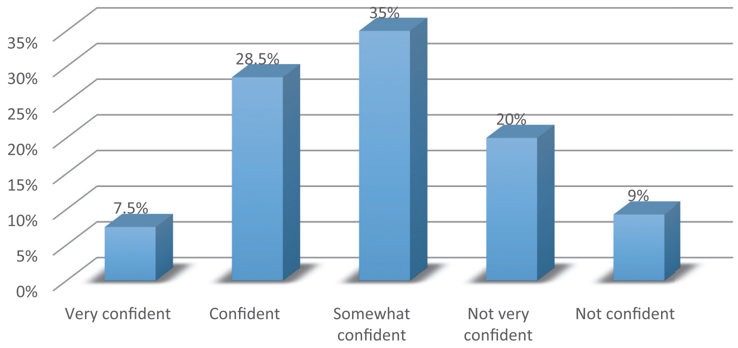


Almost all of the organisations surveyed (92 per cent) either strongly agreed (16.5 per cent), agreed (47 per cent) or somewhat agreed (27.5 per cent) that their organisation believes it is important to anonymise, mask, suppress or encrypt sensitive information contained in databases.

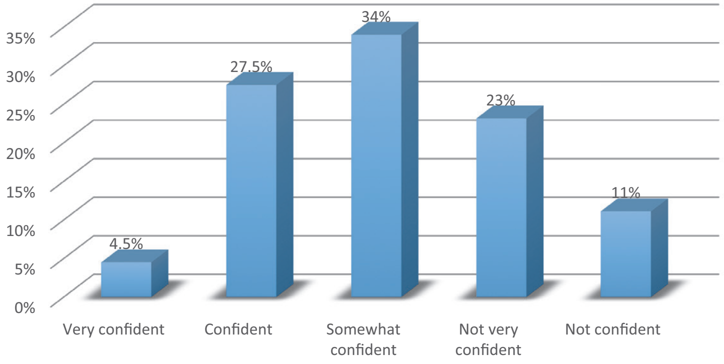
Similarly, most respondents (89 per cent) said their organisations believe it is important to anonymise, mask, suppress or encrypt sensitive information before transferring this data to third parties including cloud providers. 31 per cent strongly agreed, 43 per cent agreed and 15 per cent somewhat agreed.

Results

How confident are you that your organisation will be able to detect the unintentional loss or theft of sensitive personal information contained in your company's databases or applications in the production environment?



How confident are you that your organisation will be able to detect the unintentional loss or theft of sensitive personal information contained in databases or applications operated by third parties including cloud providers?



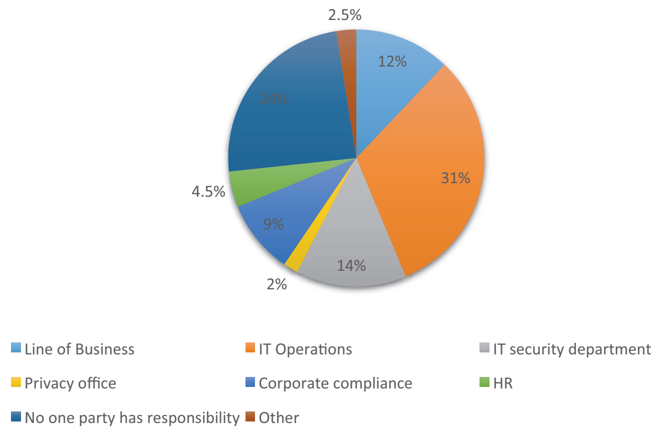
Only 7.5 per cent of respondents were very confident that their organisation would be able to detect the unintentional loss or theft of sensitive personal information contained in their company's databases or applications in the production environment.

29 per cent were not confident that their organisation would be able to detect the unintentional loss or theft of sensitive personal information.

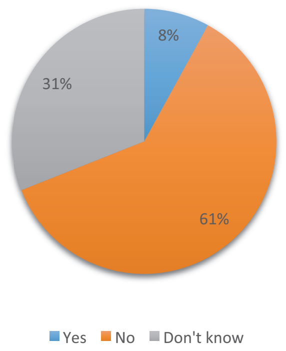
Two thirds of respondents were very confident (4.5 per cent), confident (27.5 per cent) or somewhat confident (34 per cent) that their organisation would be able to detect the unintentional loss or theft of sensitive personal information contained in databases or applications operated by third parties including cloud providers.

Results

Who within your organisation is most responsible for protecting sensitive personal information contained in your company's databases and applications?



Has sensitive personal data contained in your company's databases and applications ever been compromised or stolen by a malicious insider such as a privileged user?



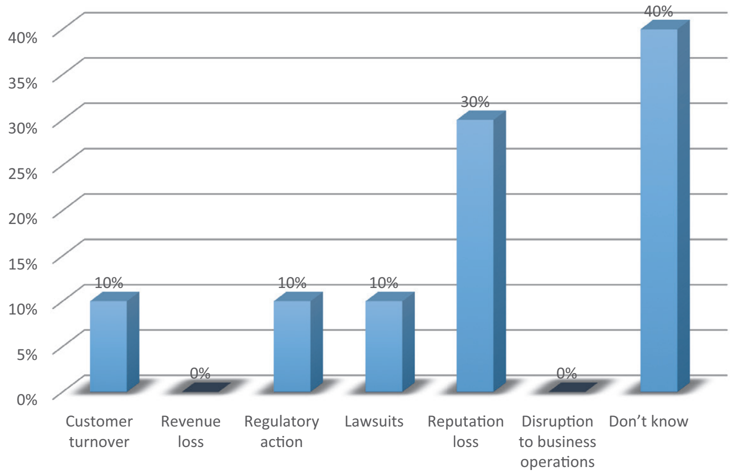
In 31 per cent of the organisations surveyed, IT Operations is most responsible for protecting sensitive personal information contained in the company's databases and applications.

A mere two per cent of respondents said a privacy office was most responsible.

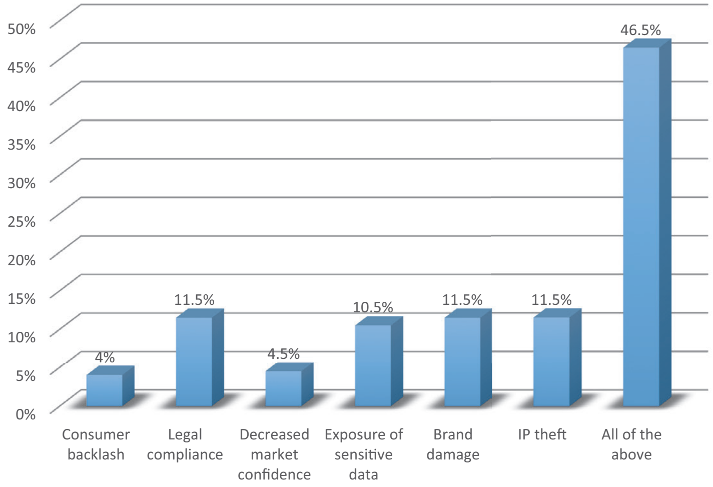
61 per cent of respondents said sensitive personal data contained in their company's databases and applications had never been compromised or stolen by a malicious insider such as a privileged user.

Results

If yes, what were the main consequences of the data loss experienced by your organisation?



If no, what is your organisation's biggest concern in the event of a data breach?



Of those 30 per cent said their reputation was affected, while 10 per cent each said they experienced customer turnover, regulatory action or lawsuits as a result of the loss.

None of the respondents reported a revenue loss or any disruption to business operations as a result of the loss.

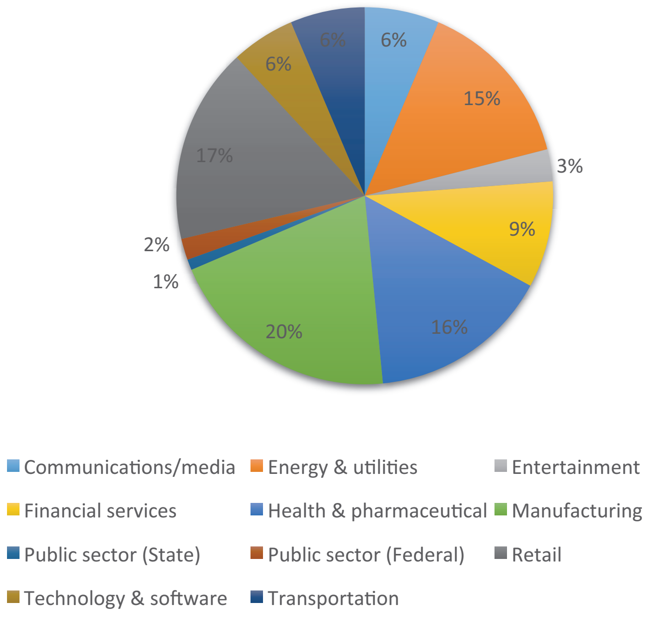
Of the organisations who had not experienced a data breach, the top three concerns were legal compliance (11.5 per cent), IP theft (11.5 per cent) and brand damage (11.5 per cent).

10.5 per cent were concerned about exposure of sensitive data, while 5 per cent were worried about decreased market confidence. Just 4 per cent cited consumer backlash as their biggest concern.

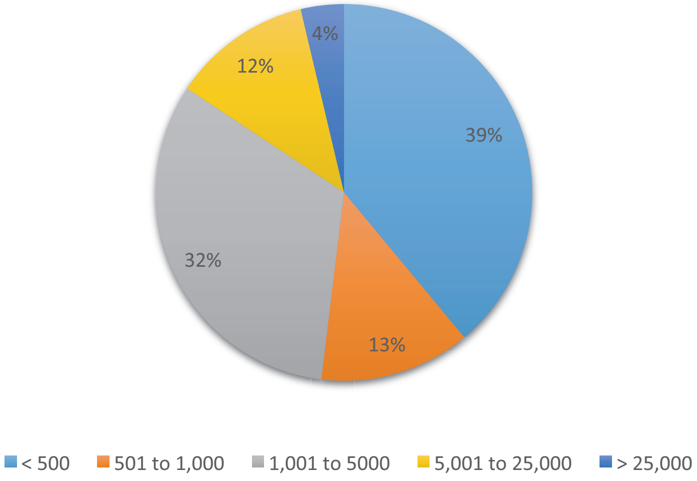
46.5 per cent of respondents said they were worried about all of those factors equally.

Research

What industry best describes your organisation's focus?



What is the size of your company?



informatica

How to get started: A few suggested next steps

Research current regulations

❑ Review the current Australian Privacy Act: www.oaic.gov.au/privacy/privacy-act/ to determine sensitive data requirements

❑ Check your internal business policies and ensure they meet the current privacy act requirements

Take inventory

❑ Define a list of data domains (such as credit card holder) and their characteristics

❑ Interview developers & DBA's to gather complete list of databases

❑ Interview data analysts and data stewards to identify all inbound and outbound data feeds

❑ Discover location of sensitive data

Asses rick level & implement plan

❑ Determine high risk systems based on locale and types of users

❑ Introduce dynamic and persistent data masking and test data management practices and tools

Informatica Data Privacy Solution

Informatica solutions for data privacy are based on proven, next-generation technology that enables organisations to quickly, easily, and cost-effectively manage and protect their private and sensitive data, decrease the risk of data breaches, and effectively meet compliance requirements for production and non-production environments on a timely basis.

Based on an innovative, open architecture, these comprehensive solutions are highly flexible and scalable, and provide for real-time or batch processing – dynamic or persistent. With easy, fast, and transparent deployment, plus a centralised management platform, Informatica solutions for data privacy will help your organisation or agency to maintain control and access to your transactional and analytic data, minimise compliance costs, and ensure data privacy.

To learn more or have an Informatica Specialist deliver an in person demonstration, you can contact us at:

Informatica Australia
Phone: 02 8907 4400
Email: info-au@informatica.com
Website: www.informatica.com/au
Level 5, 255 George Street, Sydney, NSW 2000

About Informatica

Informatica Corporation (Nasdaq:INFA) is the world's number one independent provider of data integration software. Organisations around the world rely on Informatica to realise their information potential and drive top business imperatives. Informatica Vibe, the industry's first and only embeddable virtual data machine (VDM), powers the unique "Map Once. Deploy Anywhere." capabilities of the Informatica Platform. Worldwide, over 5,000 enterprises depend on Informatica to fully leverage their information assets from devices to mobile to social to big data residing on-premise, in the Cloud and across social networks.

Appendix – methodology

Outsource, a third party marketing company, conducted the research for this index on behalf of Informatica, via an outbound telemarketing and email campaign.

The survey was conducted in April and May 2013.

109 senior IT decision makers participated in this inaugural Informatica survey on the attitudes and approach taken to data privacy by Australian organisations.

The questions asked for this report were:

Demographic questions including:

1. Job Title
2. What industry best describes your organisation's focus?
   a. Communications/Media
   b. Energy & Utilities
   c. Entertainment
   d. Financial Services
   e. Health & Pharmaceutical
   f. Manufacturing
   g. Public Sector (State)
   h. Public Sector (Federal)
   i. Retail
   j. Technology & Software
   k. Transportation
3. Size of company
   a. < 500
   b. 501 to 1,000
   c. 1,001 to 5000
   d. 5,001 to 25,000
   e. > 25,000
4. How large is your IT organisation?
   a. Small: < 50
   b. Medium: 50 – 200
   c. Large: > 200
5. Do you outsource some or all of your IT infrastructure and/or support?
   a. Yes
   b. No
   c. Don't know
6. Do you have a lot of external interfaces to other vendors/environments?
   a. Yes
   b. No
   c. Don't know

Index questions

1. Does your organisation have a data privacy strategy (i.e. policy, in place) and/or mask sensitive data to protect sensitive information such as company financial information, company revenues, customer account details, employee records, and/or payment transactions?
   a. Yes, only in the development environment
   b. Yes, only in the production environment
   c. Yes, in both the development and production environments
   d. No
   e. Don't know
2. If yes, does your data privacy strategy include any of the following:
   a. Data Masking solution
   b. Tokenisation
   c. Encryption
   d. Other
3. If no, does your organisation plan to deploy a data privacy solution to protect sensitive information used in production environments?
   a. Yes, within the next 12 months
   b. Yes, within the next 24 months
   c. No
   d. Unsure
4. If no (or unsure), why not?
   a. Don't see the need to protect data in production environment
   b. We have manual controls including policies and procedures
   c. We do not have the budget to fund a solution
   d. We are concerned about system performance
   e. We are concerned about additional headcount to deploy solution
5. How critical is **protecting data** in your organisation?
   a. Very critical
   b. Critical
   c. Somewhat critical
   d. Mandated by law
   e. Slightly critical
   f. Not critical
6. Do you currently believe that your data is adequately masked and/or protected?
   a. Yes
   b. No
   c. Don't know
7. My organisation finds it difficult to restrict user access to sensitive information in the IT and business environments
   a. Strongly agree
   b. Agree
   c. Somewhat agree
   d. Disagree
   e. Strongly disagree

8. My organisation finds it difficult to comply with the amount of privacy and data protection regulations
   a. Strongly agree
   b. Agree
   c. Somewhat agree
   d. Disagree
   e. Strongly disagree
9. My organisation is more concerned about information protection in the production versus the development or testing environments.
   a. Strongly agree
   b. Agree
   c. Somewhat agree
   d. Disagree
   e. Strongly disagree
10. In my organisation, data breaches are more likely to occur in production versus development or testing environments
    a. Strongly agree
    b. Agree
    c. Somewhat agree
    d. Disagree
    e. Strongly disagree
11. My organisation believes it is important to anonymise, mask, suppress, or encrypt sensitive information contained in databases, storage devices and servers
    a. Strongly agree
    b. Agree
    c. Somewhat agree
    d. Disagree
    e. Strongly disagree
12. My organisation believes it is important to anonymise, mask, suppress, or encrypt sensitive information before transferring this data to third parties including cloud providers
    a. Strongly agree
    b. Agree
    c. Somewhat agree
    d. Disagree
    e. Strongly disagree
13. How confident are you that your organisation will be able to detect the unintentional loss or theft of sensitive personal information contained in your company's databases or application in the production environment?
    a. Very confident
    b. Confident
    c. Somewhat confident
    d. Not very confident
    e. Not confident

14. How confident are you that your organisation will be able to detect the unintentional loss or theft of sensitive personal information contained in databases or applications operated by third parties including cloud providers?
    a. Very confident
    b. Confident
    c. Somewhat confident
    d. Not very confident
    e. Not confident

15. Who within your organisation is most responsible for protecting sensitive personal information contained in your company's databases and applications?
    a. Line of Business
    b. IT Operations
    c. IT security department
    d. Privacy office
    e. Corporate compliance
    f. HR
    g. No one party has responsibility
    h. Other
    i. Do not know

16. Has sensitive personal data contained in your company's databases and applications ever been compromised or stolen by a malicious insider such as a privileged user?
    a. Yes
    b. No
    c. Don't know

17. If yes, what were the main consequences of the data loss experienced by your organisation:
    a. Customer turnover
    b. Revenue loss
    c. Regulatory action
    d. Lawsuits
    e. Reputation loss
    f. Disruption to business operations
    g. Don't know

18. If yes, what was the estimated cost of that breach?

19. If no, what is your organisation's biggest concern in the event of a data breach?
    a. Consumer backlash
    b. Legal compliance
    c. Decreased market confidence
    d. Exposure of sensitive data
    e. Brand damage
    f. IP theft
    g. All of the above
    h. None of the above