



DESIGNING IT SOLUTIONS



Data Security Breaches – The Worldwide Epidemic

Ineffective Data Security in organisations worldwide has led to identity theft and fraud becoming the fastest growing and most prevalent crime in society. The statistics surrounding identity theft and fraud are downright frightening. In America today identity theft claims 15 million victims per year with the associated financial losses amounting to \$50billion.

A recent survey by the Ponemon Institute revealed that 73% of businesses surveyed had experienced at least one data breach in the last 12 months. The largest organisations in the world from banks to telco's and government are being attacked and robbed every day, yet it doesn't make the news for a number of reasons.

Firstly the theft occurs without anyone walking into a bank with a gun threatening to shoot people and secondly because currently organisations are not obliged to publicly disclose data breaches to anyone, be it the individuals affected by the breach, the media or the government. There is however new legislation being produced by the USA, the European Union and Australia designed to force organisations who suffer a data breach to report it to the government and to notify all customers who were affected by the breach.

Organised Crime

Organisations need to take action to defend themselves against increasingly sophisticated thieves who are currently stealing tens of billions every year.

The perpetrators of data theft are not just individual "hackers", but increasingly organised crime is getting involved. This is because the stakes are high and ineffective data security is seen as the soft underbelly of the corporate world.

"European banks are likely to face in the near future an unprecedented wave of attempts of identity theft. Hackers are now targeting financial institutions. The global credit crisis has added to the rows of unemployed spies, laid off bankers and computer programmers. Networks of secret agents, knowledgeable financiers and computer savvy criminals have sprung up all over Eastern and Central Europe and the Balkans".

Data Breaches – The Headlines

The Australian Bureau of Statistics

The Australian Bureau of Statistics 2007 Personal Fraud Survey estimates that the total cost of scams and personal fraud for the second half of the year was almost \$1 billion, with credit and bank card fraud accounting for more than 380,000 instances.

The Australian Bureau of Statistics report states that “personal fraud has been recognised as a crime type that is a growing threat to the community, as a result of the rapid expansion and availability of internet technology and the increase in electronic storage, transmission and sharing of data”.

Watch your credit card for Hotel Hacks

DarkReading.com, an online security trade publication, stated that hackers found their way into hotel networks more than any other in 2009. The study also discovered that hotel chains did not discover the security breaches for an average of 156 days.

More electronic records were breached in 2008 than the previous four years combined, fuelled by a targeting of the financial services industry and a strong involvement of organised crime, according to the “2009 Verizon Business Data Breach Investigations Report” (DBIR) released Wednesday (April 15 2009).

This second annual study - based on data analysed from Verizon Business’ actual caseload comprising 285 million compromised records from 90 confirmed breaches - revealed that corporations fell victim to some of the largest cybercrimes ever during 2008.

Federal Reserve Bank of New York - Employee Data Breach

A federal bank information analyst from Elm Park has admitted he stole his fellow employees’ identities so he and his brother could apply for more than \$1 million in student and boat loans. Curtis Wiltshire, 34, committed the fraud from 2006 and 2008, while he was working as an information and technical analyst at the Federal Reserve Bank of New York in lower Manhattan. He had access to computer files with other employees’ names, dates of birth, social security numbers and photographs.

Connecticut sues Health Net over data security breach.

“The missing drive contained information about 446,000 enrollees and their physicians”.

Data Security – The Enterprise Context

At a board level data security is about:

1. Demanding continued vigilance in the protection of information;
2. Setting appropriate policies to mitigate the risk of brand damage and financial losses resulting from a data breach; and
3. Maximising the benefit to the organisation from its investment in appropriate data security controls.

Ultimately, it is about data and information. Who has the data, how much data does each person have access to, and is the data sensitive and financial in nature. Communications is the transport of information and encryption is imperative but so is managing the information in a secure way and this is what has not kept pace with the communications revolution.

The focus in data security over the last decade has been a concept called 'role based' security. This involves managing a person's access via the roles that they have within various applications. These applications in turn read and write the data and are responsible for implementing the security regime. The problem is if you bypass the application you can still get to the data (read and write).

An additional layer of protection is required and it needs to be at the data level. Furthermore, this additional layer of protection needs to be implemented as a piece of infrastructure in precisely the same way that other security measures such as passwords and firewalls are.

Data security needs to be taken out of the hands of the application developers (programmers), it should be provided to them as a piece of infrastructure that is independent of any application.

As first tier consultants in data security we work with organisations from a board level and senior executive compliance level to provide a security model of people, process and platform. We provide a visual representation of how this new security model works in your organisation and an implementation path to introduce technologies, procedures and processes to permanently close back doors to the data.

There are some key issues with respect to why it has been so difficult to implement effective security across an organisation.

- The first issue is that of overall IT infrastructure, systems and databases. Many large organisations have over time merged with other entities or taken over competitors, resulting in numerous databases, links between systems, various hardware and often many old legacy systems. The provision of security in this type of environment is complex and usually provided by application developers building controls into the various programs. The result of this approach is unsatisfactory, as evidenced by the various statistics relating to data fraud.
- Security needs to be effected at an enterprise level across all databases and systems without any back doors or access points created by the various applications that consume the data. The only real way to implement at an enterprise level is to provide it as a piece of infrastructure. This is consistent with the provision of single sign on passwords, firewalls etc.

- Until now it has not been possible to implement an enterprise wide solution providing row level security across multiple systems, databases and hardware platforms. Designing IT Solutions has invented new technology known as Data Chamber. Data Chamber is a technology that is a general way of working with all relational database management systems to provide row level security and close any back door independent of the context of any applications. In other words what we have created is a database wrapper that works as a preventative control. This opens up a whole new way of implementing enterprise wide data security infrastructure.

Data Security as Infrastructure

In recent times there has been an explosion in the field of electronic commerce and the use of information technology across business and government. Vendors have produced faster machines and better applications at an alarmingly fast rate. What hasn't kept up with this amazing innovation is the development of adequate security to protect the massive amounts of private and confidential information stored by large organisations.

The focus in data security in recent times has been twofold. Firstly there has been the development of technology to "protect the perimeter". This of course is implemented as a piece of infrastructure - the DMZ Layer. The DMZ consists of firewalls, routing and protocol standards, it is the first line of defence, a bit like the outside walls of a bank.

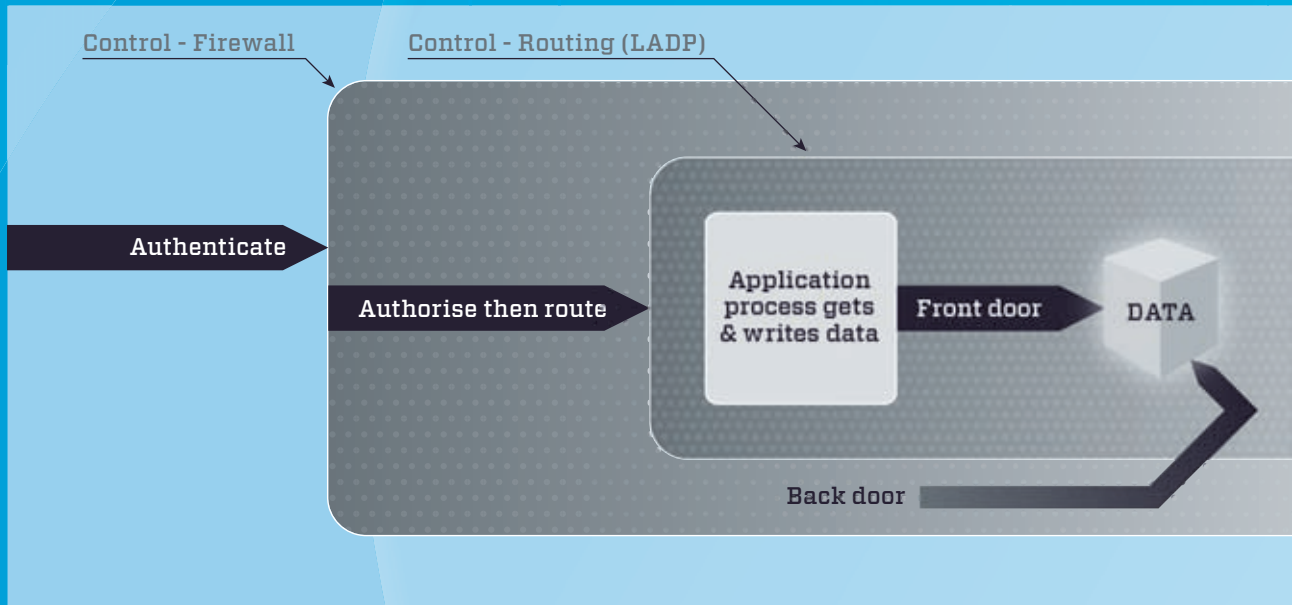
The second layer of defence is the LDAP layer which is also implemented as a piece of infrastructure. LDAP is all about functional constraints, single sign on and service availability. To continue with the bank analogy, LDAP is like the screens between the customer and the teller, it determines where you are allowed to be, once you're inside the building.

Whilst the DMZ and LDAP layers are working to a degree, there is a final layer of infrastructure required, and that is around the data itself. This layer needs to be independent of any applications that consume the data and able to lock down every row of information in the database. This final layer of security is as close to the data as you can get and effectively closes any back doors to the data. Think of it as the vault in the Bank. If someone left the door of the vault open at night and somebody walked in, they could help themselves to all the cash they liked. Without this final layer of infrastructure in place, organisations are effectively leaving the door of the vault open. Our patented solution to providing this layer of infrastructure is known as "Data Chamber".

“Every bank in the world has a vault to secure its monetary assets. Every business needs to protect its information assets in the same way. Firewalls and LDAP are the perimeter defences. Data Chamber is the vault!”

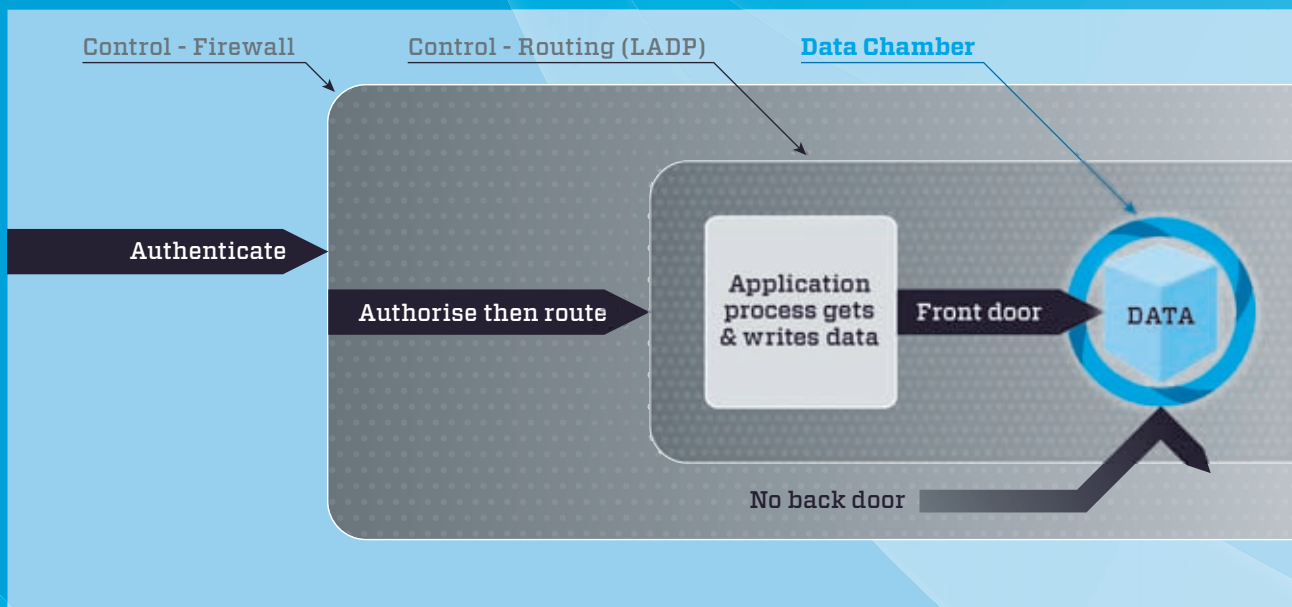
Typical Enterprise Security

In a typical enterprise, security infrastructure is focused solely on the perimeter. Authentication and authorisation are provided as infrastructure. The application itself does not have to deal with these issues. Data security however is left to the application.



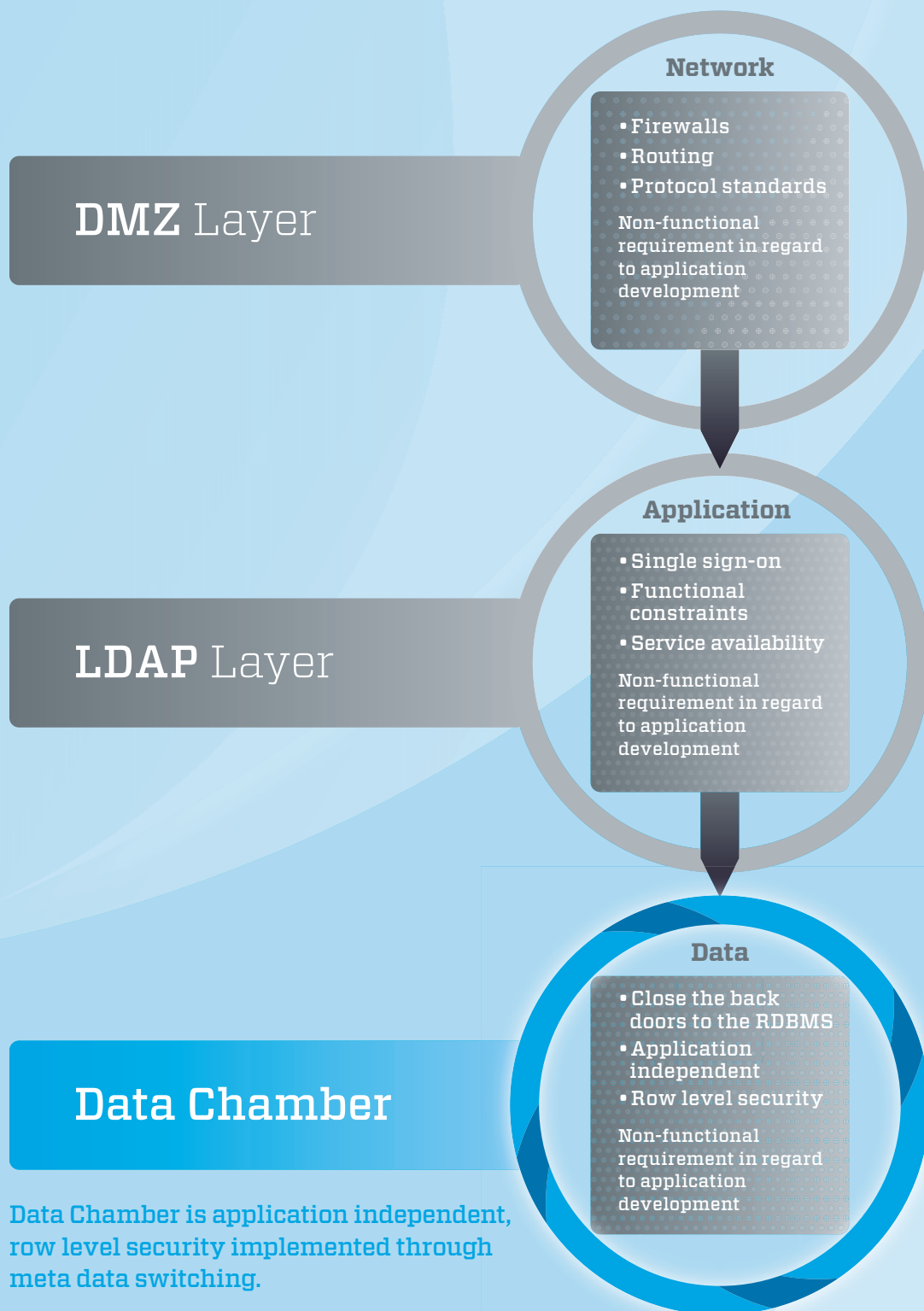
Adding Data Security

Data Chamber provides an additional layer of infrastructure, around the data itself, taking this out of the application. This reduces security holes and greatly simplifies applications.



DATA CHAMBER

With Data Chamber, data security, like network and application security becomes a non-functional requirement for application development and deployment.



Data Chamber is application independent, row level security implemented through meta data switching.

General Consulting Approach

Data security has to be taken seriously at every level of the organisation, from the board room to the back room. Defensive layers need to be implemented so that they compliment and overlap each other, but this can only happen after a careful consideration of exactly what needs to be defended, and who the potential enemies are. For example, for most companies it would be far less damaging if details of their suppliers were leaked than if they unintentionally disclosed customer details.

For many organisations, none of this is treated seriously until a breach actually occurs, and then there are reviews, finger pointing and damage control, but the cost to reputation, not to mention direct cost, loss of competitive advantage and impact on brand can never be recouped.

Often, some of the more important aspects of security are overlooked. The focus is on intrusion prevention, but equally important are: detection, reaction and recovery from breaches. Another important issue is the handling of data to minimise exposure to threats. Customer privacy must be enforced not only against external threats, but also against internal dangers.

The company's overall security and privacy policy needs to be a focus of the board and executive layers of the company. How this policy is implemented in the everyday procedures and processes of the company falls on the shoulders of line management. Ensuring that the appropriate controls and defences are in place to enforce policy and protect company data assets generally falls to the IT department.

Designing IT Solutions is able to help right across the spread of data security, from policy to procedure to protection. Our consultants have experience across all levels of the business spectrum, from having been CIO of an ASX 100 listed company, to working as an auditor down at the lowest level of detail. We have experience across a broad range of industries, including government, banking and finance, manufacturing, distribution, R&D, mining, consulting services, telecommunications, education and publishing.

We are constantly refining and developing our methodologies. We keep up with the latest research and evaluate when to incorporate new thinking into what we do. It's important to stay ahead of the game, but we have no interest in being on the bleeding edge either. We continue to refine what information we present to our clients, and how that information is presented. Too often, information is presented in a format that is so technical that the audience cannot really understand it. If you can't understand it, then you can't really sign off on it, and you certainly can't implement it. We aim to ensure that all information is pitched at the correct audience, without skimping on the needed detail.

4 Fundamental Questions

Overall there are 4 fundamental questions that need to be asked about security, they naturally flow from the top of the organisation down.

Does the Company security policy comply with legislation and support overall organisational objectives and values?

Do the company's business procedures and business processes uphold the company security policy?

Do the controls enforce the company security policy?

Does the data security model support enforcement of the company security policy?

Designing IT Solutions centre our approach around 5 pillars: -

- Assessment of potential security risks
- Prevention of these risks
- Detection of breach events
- Reaction to breach events
- Recovery from breach events

We understand that security is about more than the software that your company uses. Security is a complex layering of controls, some of these are about hardware and software, but just as important are the people and processes within the organisation.

Final Report - Data Security Control Review

The final report structure is as follows:

The final report will provide:

- An enterprise list of the major data information assets that need protection.
- An enterprise list of vulnerabilities that each data asset would be in danger from.
- A calculation of likelihood and organizational impact for each identified asset.
- A list of the existing controls for each asset that mitigate risk.
- An assessment of the effectiveness of the list of controls in terms of adequacy.
- A road map in terms of fixing the gaps and the way forward.

Designing IT Solutions – Management Team

David Finlayson - Consulting Partner

David Finlayson gained a degree in accounting and economics. For the past twenty years, he has been working in IT across a variety of industries including, Banking and Finance, Manufacturing, Government and Telecommunications. After consulting on one of the earliest business intelligence projects in Australia, he has been designing databases to solve business problems ever since.

He has spent much of his career on business processing systems, integrating with and extending accounting and ERP systems. This has included EDI integration, third party warehousing solutions, revenue analysis and reporting solutions.

M: +61 419 482 419

T: +61 2 8001 6324

E: davidf@designingits.com

Mark Stocks - Consulting Partner

Mark Stocks believes computing science is the key to economic innovation.

Mark's resume includes CIO of one of Australia's largest contract mining corporations, management consulting and application architecture consulting. He holds a masters degree in computing science and has consulted internationally. He considers people the most important component of a business system and this is reflected in the architecture of his IT designs where he articulates a design to create shared meaning between the stakeholders.

Mark has designed solutions across many industries, particularly banking, finance, mining and telecommunications. He has designed 'client server' applications in finance, 'data warehouse' applications in wealth management and 'web based online' transaction systems in banking.

M: +61 414 397 214

T: +61 2 8001 6324

E: marks@designingits.com

Morris Levitzke - Manager, Institutional Sales

Morris has a Business Degree majoring in Information Systems. After beginning his career as an IT consultant Morris moved into the Financial Services Sector. Over the last 20 years he has worked within Corporate and Institutional Banking, Wholesale Investments, Corporate Superannuation, Insurance Product Management and Business Development.

M: +61 450 324 024

T: +61 2 8001 6324

E: morrisl@designingits.com

Grahame Stocks - Business Development Manager (Media and Film)

Grahame Stocks has a Communications and Media Degree. After beginning his career in law, Grahame moved into Film and TV and has over fifteen years production experience in media and film as a Senior Agent in film production and development.

M: +61 410 306 061

T: +61 2 8001 6324

E: grahames@designingits.com

**“Data Security needs
to be dealt with in
the boardroom and
then implemented as
infrastructure in the
back room”**



**DESIGNING IT
SOLUTIONS**

Designing IT Solutions Pty Ltd

16 Lindsay Gordon Place, Heathcote NSW Australia 2233

T: +61 2 8001 6324 | info@designingits.com | designingits.com