[49] See subclause 8.5.1 of Procure IT. Note also that subclause 8.5.2 provides further room to reduce the cap for Contracts with SMEs and Contracts for certain telecommunication supplies.

[50] See subclause 8.5.3 of Procure IT

[51] Subclause 8.5.3 of Procure IT; NSW Department of Commerce, *Procure IT User Guide* (2006) at p17; also Procure IT "Frequently Asked Questions" at "How will the process of risk assessment work and will it delay my contract?" available from www.contractservices.nswp.commerce.nsw.gov.au/Procure+IT/FAQ+and+User+Guide.htm

[52] See, for example, World Information Technology & Services Alliance, *Best Practices in Government IT Procurement* (2004) at p17

[53] See the discussion of "Risk in NSW Government contracts" above

[54] Australian Information Industry Association, *Procure IT - Key issues - An Australian Information Industry Association Briefing Paper* (2005) at p11

[55] Australian Information Industry Association, *Procure IT - Key issues - An Australian Information Industry Association Briefing Paper* (2005) at pp11-12

[56] See NSW Department of Commerce, *Contracting Out Guideline* (2002) at p31

Protecting Customer Data in Global Organisations- Regulations and Security Controls

George Arronis

George Arronis is the Information Risk Manager at J.P. Morgan Institutional Services Australia where he oversees and manages the technology control environment.

Organisations operating globally, in particular Financial Services Institutions, face the challenge of complying with multiple regulatory jurisdictions when it comes to the security and privacy of customer data. Managing this regulatory risk is a key driver for such organisations to implement various data protection initiatives to mitigate the threat of exposure. Customer data that is stored and processed by internal systems and/or systems of a third-party business supplier needs to be protected. Balancing regulatory requirements with appropriate technology controls is certainly a difficult and resource-intensive task. The spate of reported cases of customer data issues at various organisations, weighs on their reputation and investor confidence in general. By using the regulatory environment for building a typical security framework and applying suitable technology controls, organisations are increasing their effectiveness in data protection and reducing the risk of being tomorrow's head-lines.

Between June and December 2005, *InformationWeek* cited at least 49 million cases of customer data-loss incidents in corporate America.[1] A number of companies have already settled with the Federal Trade Commission in the United States (US), for failing to provide reasonable security measures to protect customer data.[2] In many of the incidents, the lack of simple information security practices led to the data exposures. It seems a just cause then, that policy makers in the US are proposing a raft of new legislation to deal with data security issues.[3,4]

Notwithstanding any pending legislation, the existing regulatory regimes are no doubt a key driver for data security initiatives; this is a conclusion reflected in responses to global information security surveys by consultants' Deloitte and Ernst & Young[5,6] and other industry news portals.[7, 8] A multi-national organisation would need to comply with numerous laws that encompass the need for consideration of data-security requirements. The complexity (and cost) of complying across a number of geographies then increases. Table 1 provides a *sample* set of rules and regulations (legislation, directive or policy) that drive security initiatives and apply in the US, Europe or the Asia Pacific (APAC) region. For the sample listed, the fundamental objective of each is the protection against: (i) unauthorised access to data (encompassing both internal and external threats) and (ii) unauthorised or accidental modification of data; the former protects confidentiality and the later integrity in information systems. The considerations for security encompass a range of operational, technical and physical controls. For example:

- The Gramm-Leach-Bliley Act (G-L-B Act) *Safeguards Rule* requires financial institutions to document, implement and maintain an information security program;
- The EU Data Protection Directive and Australian Privacy Act include data security considerations;
- The Japan Personal Information Protection Act (PIPA) calls for protection against information leakage and loss; and
- The California SB 1386 entails the

need to protect data through encryption.

The G-L-B Act *Safeguards Rule* provides financial institutions with direction on various functional requirements for developing an information security program. Whilst not exhaustive in its coverage of information security management, the ruling emphasises key control areas that are considered most relevant to the operations of financial organisations. It promotes the use of a life-cycle methodology for managing risk, including an initial risk assessment, prioritisation of risk based on relevance to operations, testing and monitoring of controls and evaluation of the security program based on changes to operations. There is a strong emphasis on assessing controls risk around employee training, attack detection and response, information processing, storage and transmission and third party service providers. On this last point in particular, the growing reliance of financial organisations on third parties is bringing this issue to the top of many risk prioritisation projects. By outsourcing to a third party, the financial services organisation removes the risk of day-to-day managerial responsibility but still remains accountable for the business activity; whilst outsourcing does not eliminate risk, it changes the organisation's risk profile.[9] To mitigate this threat, the G-L-B Act *Safeguards Rule* calls for financial services organisations to implement appropriate legal contracts with third parties for data protection.

The G-L-B Act *Safeguards Rule* provides the foundations for the creation of a framework approach to information security. Looking at Table 1 further (see below), additional security-related provisions (*or implications for security*) to address threats to information assets can also be compiled and added to this framework. For example:

- California's SB 1386 legislates against the unauthorised access to unencrypted data. Lost or stolen mobile devices (e.g. laptops or hand-held devices) can contain confidential information; encrypting data on laptops using commercially available software to prevent unauthorised access to data, would seem to satisfy SB 1386. Of course, this is merely a tactical approach and is only one additional component in the security program.
- Japan's PIPA specifically calls for protecting against information leakage and the EU Directive asks member states to legislate against the processing of data identifying, for example, race, ethnic origin or religious beliefs. The former implies that organisations need to install virtual check-points throughout the organisation to minimise the risk of exodus of confidential information (e.g. loss through email, USB devices, CD or other removable media) and the later, a validity check of information about to be processed (that is, what's to say information to be processed has not been cleansed appropriately?). The ability to provide content filtering (including lexical analysis) across various exit/entry channels, then becomes a key component in the management of information flow into and out of the organisation.
- Australia's Privacy Act and the EU Directive, make consideration for Transborder data flows. The focus is on ensuring that privacy protection is maintained when personal information is sent cross-border and that the recipient also has adequate provisions for information security. Assuming both sender and recipient have appropriate controls in place, then the intrinsic residual risk is the trust placed in the method used to send the data to the recipient (that is, to ensure that the confidentiality and integrity of the data is maintained during transfer). Whether this method is the Internet or a private network (or even courier), then the level of controls used must be adequate to retain the level of confidentiality assigned to the data by the sender. Cryptographic mechanisms are used to secure data during transfer. If sender validity is also required, then non-repudiation mechanisms are also required (e.g. digital certificates).

By using the presenting regulatory regime as a driver for building a security framework, organisations can identify some of the key requirements for managing and protecting customer information assets and determine the appropriateness of each to their operations. Combining the various legislative and policy components described above, a simple functional model for a security framework is possible to define, the elements of which are:

- The risk assessment life-cycle (shown in Diagram 1). It is imperative that an organisation first identify the information assets it needs to protect. A threat-risk assessment then looks at the likelihood and impact of a threat and provides a starting point for prioritising the risk to information assets. The agreed solution to mitigate risk will always be a trade-off between the cost outlay and the residual risk an organisation is willing to tolerate. To determine the on-going effectiveness of the solution, regular testing (possibly by an independent party) and monitoring is required. Only through testing and monitoring can an organisation determine if it is maintaining its risk tolerance to appropriate levels.
- The key information security objectives - confidentiality and integrity. The trust placed in an organisation to maintain the confidentiality and integrity of customer information is fundamental to the relationship. The risk to reputation in the event of a data breach, is also key to driving security initiatives.
- Various operational, technical and physical controls (which support the security objectives). The extent of controls used to reduce risk should be commensurate with the level of risk tolerance identified in the risk assessment.

The security model is shown in Diagram 2 below. The diagram lists typical functional (and tactical) considerations within an information security program. Whilst this framework is built upon a sample regime heavily focused on financial institutions, the fundamental objectives for protecting information are the same regardless of industry. The model identifies the need for a mix of policy, processing rules, detection & response mechanisms,

encryption, employee training and legal contracts to make security work. The control parameters in Diagram 2 amount to a layered approach to security. One cannot rely on data encryption or access control systems alone to achieve security. Each component, whether technical or physical also requires the appropriate operational policy and procedure to support it. Taken further, integrating the components into a cohesive framework that supports the business objectives, requires additional oversight and management. Effective security is possible when all the operational, technical and physical controls are able to consistently maintain the required risk profile across the organisation.

Notwithstanding, the scope of such a model does not cover all aspects of security. Developing a comprehensive approach to information security is enhanced through standards such as ISO/IEC 17799, a code of practice for information security management. It defines a menu of controls for information systems across areas including security policy, asset classification, system planning and business continuity and can be used to augment the gaps in an existing information security program. Furthermore, whilst various security implications of privacy legislation are highlighted, the privacy program itself and other regulations, provide additional components to building a framework for managing and protecting customer data. These laws include notions of providing adequate notice at time of collection, principles of appropriate disclosure and data retention.

Organisations will need to tackle the challenge of implementing such frameworks for protecting data with limited resources and budget in the face of increasing regulations pertaining to data security.[10] Organisations thus need to prioritise risk by determining relevance to operations and strike a balance between the cost, risk and the data being protected. Overall, a robust and well governed security program entails a mix of the right people, processes and technology to achieve the organisation's objectives for protecting information assets they own. By taking a proactive approach to managing information security and protecting customer data, organisations can demonstrate their maturity in this complex area and reduce the risk of being tomorrow's headlines.

Table 1 Sample Regulatory Environment (Legislation, Directive, and Policy)

Country	Legislation or Policy	Example Security Requirement
United States	Gramm-Leach-Bliley Act *Safeguards Rule*	Requires "financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information."[11]
	California Senate Bill 1386	Requires disclosure when "any breach of the security of the data...to any resident of California whose ***unencrypted*** personal information was...acquired by an unauthorized person."[12]
Europe (European Commission)	EU Data Protection Directive (DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL)	"Member States shall provide...appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access..."[13]
Australia	Privacy Act 1988 (Cth) and Privacy Amendment (Private Sector) Act 2000 (Cth)	**Principle #4 (Private Sector)- Data security** "An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure."[14]
	Australian Securities & Investments Commission: *Policy Statement 164 Licensing: Organisation capacities*	**[PS 164.126]- (For holders of Australian financial services licence):** "To ensure licensees continue to meet their licensee obligations, we expect licensees using IT systems to regularly review: (a) their IT system security..."[15]
Japan	Personal Information Protection Act	**Article 20 (Security Control Measures)** "An entity handling personal information must take necessary and proper measures for the prevention of leakage, loss, or damage, and for other control of security of the personal data."[16]
Singapore	Singapore Banking Act	**Section 47 (Banking Secrecy)** "Customer information shall not, in any way, be disclosed by a bank in Singapore or any of its officers to any other person except as expressly provided in this Act."[17]

References

[1] See: http://www.informationweek.com/story/showArticle.jhtml?articleID=183700367 [cited 25 March 2006]

[2] See: http://www.ftc.goc/privacy/index.html [cited 02 February 2006]

[3] The Economist 2005, 'Privacy laws gain support in America, after a year of huge violations' 1 Dec

[4] See: http://www.ftc.gov/opa/2005/06/datasecctest.htm [cited 23 January 2006]

[5] See: Deloitte 2005, *2005 Global Security Survey*

[6] See: Ernst & Young 2005, *Global Information Security Survey 2005- Report on the Widening Gap*

[7] See: http://www.informationweek.com/story/showArticle.jhtml?articleID=170100825 [cited 7 April 2006]

[8] See: http://www.computerworld.com/securitytopics/security/story/0,10801,105936,00.html [cited 7 April 2006]

[9] Australian Prudential Regulatory Authority, *Regulatory Impact Statement: Outsourcing* [online] Available from WWW: http://www.apra.gov.au/ADI/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=4601 [cited 19 September 2005]

[10] Olstik, Jon. 2006, *Research Report: Protecting Confidential Data* [online] Available from WWW: http://www.enterprisestrategygroup.com/_documents/CentralZone/CentralZoneAtt11.pdf [cited 17 April 2006].

[11] See: http://www.ftc.gov/privacy/privacyinitiatives/safeguards_lr.html [cited 1 December 2005]

[12] See: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html [cited 20 January 2006]

[13] See: http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [cited 1 February 2006]

[14] See: http://www.privacy.gov.au/publications/npps01.html#d [cited 30 January 2006]

[15] See: http://www.asic.gov.au/asic/asic.nsf/lkuppdf/ASIC+PDFW?opendocument&key=ps164_pdf [cited 5 December 2005 2006]

[16] See: http://www.privacyexchange.org/japan/japanindex.html [cited 15 February 2006]

[17] See: http://www.mas.gov.sg/masmcm/bin/pt1Banks.htm [cited 7 April 2006]

Diagram 1 Risk Assessment Lifecycle

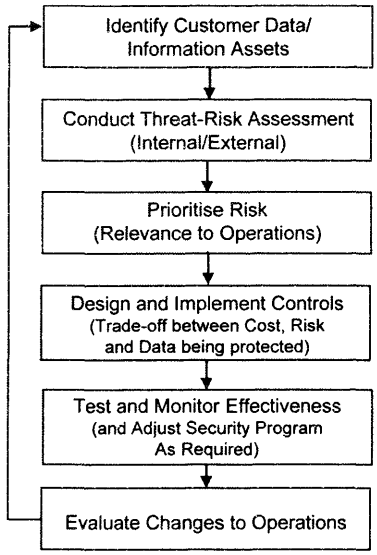

Diagram 2 Regulatory-Driven Security Controls Model