

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.nsw.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