2006

The Information Security Standards Marketplace

Richard Baskerville
baskerville@acm.org

The Information Security Standards Marketplace

Richard Baskerville
Email: baskerville@acm.org

Abstract

From the perspective of much of the literature dealing with Information Security Standards, the decision to adopt or follow such standards is mainly a technical decision subject to regulatory requirements. This paper explains why the decision to adopt an information security standard is one taken in a complex marketplace of competing standards, competing service providers, competing security design methods, and competing national and international legislative requirements, all under the oversight of closely watched audit firms and government regulators. While the dependence on standards for guidance in information security is growing, so is the complexity of the decision. The decision affects the economic justification of internal controls in information systems. Without regulatory standards, risk economics are necessary to justify acquisition and implementation of controls. With regulatory standards, risk economics are necessary to justify exceptions to the acquisition and implementation of controls. The impact of this economic shift may drive down organizational competitiveness or increase misleading compliance behaviour among IT professionals.

Keywords

Information systems security, risk management, security standards, risk analysis, compliance, governance

INTRODUCTION

In the wake of a series of unfortunate corporate financial collapses worldwide, government legislative investigations led to a variety of legislation meant to improve the reliability and integrity of information provided by corporations to public shareholders. Most of this legislation has more or less shifted oversight responsibility into the hands of government regulators. While this regulation varied in extreme, the result has been a dramatic effect on the way information security safeguards are specified and evaluated.

Perhaps the most extreme form of this government regulation of corporate governance is the U.S. Sarbanes-Oxley Act of 2002 (SarbOx). It intends to regulate by law the requirements for the independence of public company auditors, ethical reporting to shareholders, and to more severely criminalize misrepresentations of corporate financial situations by senior executives. While the Australian equivalent, the Corporate Law Economic Reform Program (CLERP 9), is less extreme in shifting power from the professions to the government, it has many similar features.

Such legislation has served to increase the emphasis placed by organizations on their internal accounting controls. This increasing emphasis has driven requirements for more severe assurance audits of the information security safeguards designed into information systems. These requirements are increasingly linked by auditors to established, recognized, information security standards and guidelines. As a consequence the importance of information security standards and guidelines in the design and specification of information security safeguards is growing.

However, the adoption of an information security standard is not a straightforward decision for many organizations. It involves selecting a standard that will satisfy auditors, who by regulation are independent and required to be legally disconnected from the decision to adopt the standard. Once adopted, the standard is likely to change the existing approaches most organizations use in establishing security requirements and designing security safeguards. The interaction of information security standards and traditional practices of risk analysis are changed. Further there are a variety of information security standards from which an organization may choose. These include general standards, government standards, and product standards.

In addition, there are a variety of external stakeholders involved in an organization's decision to adopt an information security standard. Aside from the auditors, there may be government regulators, service providers with expertise in particular security standards, and company trading partners carrying baggage involving their own regulatory constraints. This may require an international trading company to conform to regulations in other countries, invoking a sort of required extraterritorial legislative conformity.

This paper explains why the decision to adopt an information security standard is one taken in a complex marketplace of competing standards, competing service providers, competing security design methods, and competing national and international legislative requirements, all under the oversight of closely watched audit

firms and government regulators. While the dependence on standards for guidance in information security is growing, so is the complexity of the decision.

To accomplish this goal, we will discuss the information security standards marketplace in four sections. These include (1) competing national and international legislative requirements, (2) competing standards, competing service providers, (3) reoriented security design methods, and (4) audit firms and government regulators. Figure 1 illustrates these elements and the competition in the security standards marketplace that are discussed in this paper. In this figure, information technology (IT) operations in publicly held firms are scrutinized by external audit firms (themselves scrutinized by government or professional regulatory bodies) in response to competing national and extraterritorial legal frameworks. This scrutiny drives IT security designers to move the basis of security requirements definition toward one of the IT security standard. These standards are competitive in the sense that each is different, and each has a variety of specialized IT Service Providers who advocate each standard. Ultimately, the reoriented security design processes reshape the IT operations. As audits, operations, and standards evolve under the effects of competing legislation and standards, security design processes and security operations continue in the cycle to reshape IT operations.

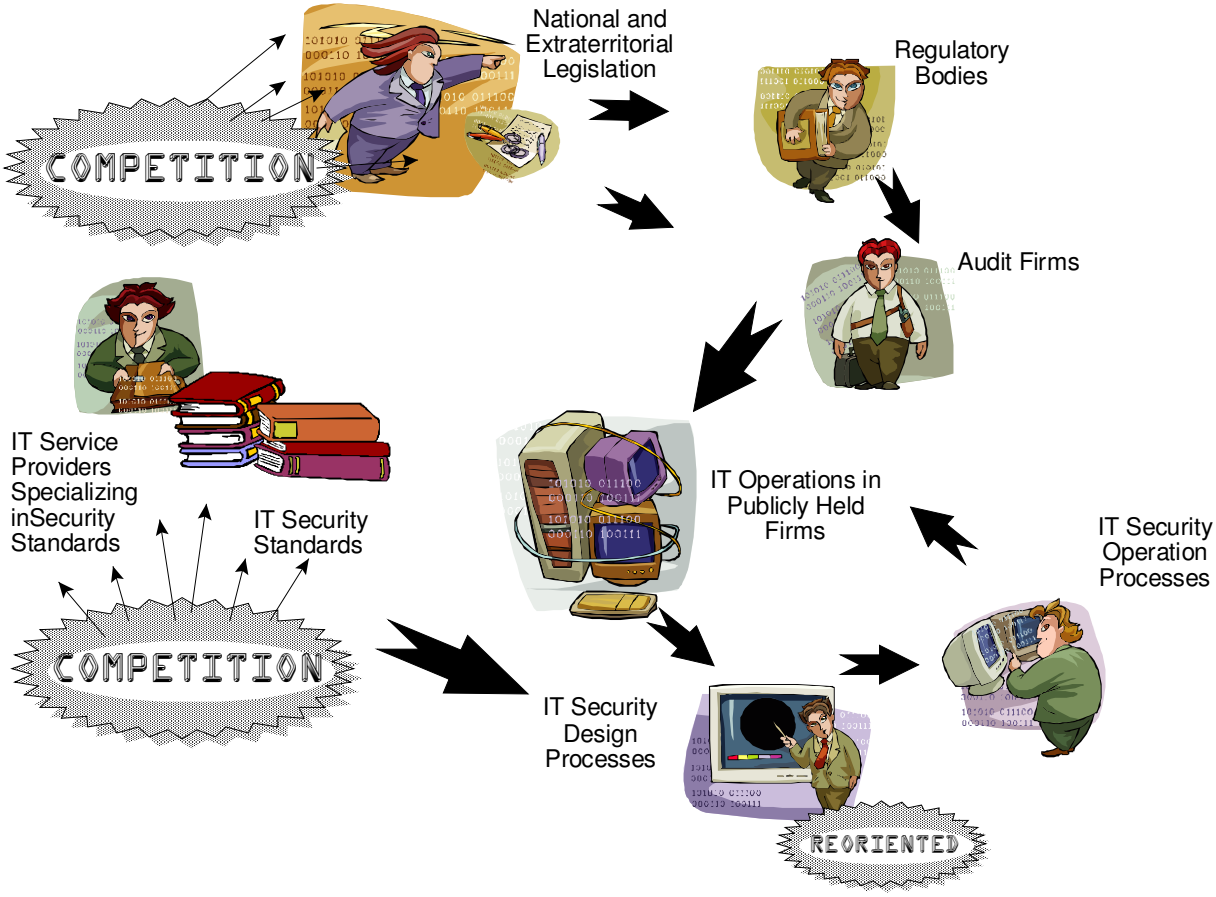

Figure 1. Competition in the security standards marketplace.

COMPETING NATIONAL AND INTERNATIONAL LEGISLATIVE REQUIREMENTS

There were a wide variety of legislative responses to the abuses of ethics and corporate governance that led to a number of spectacular corporate failures in the 1990s. We will select two for a brief comparison, namely the American SarbOx and the Australian CLERP 9.

SarbOx is named after its sponsors Senator Paul Sarbanes and Representative Michael G. Oxley, and was approved by an overwhelming vote in the US legislature. It consists of some 11 titles that provide new regulations for the accountability for corporate and criminal fraud, white-collar crime penalties, corporate tax returns, etc. It has several provisions that have proven to be relevant for information security. Of particular importance is Title IV, which deals with enhanced financial disclosures. This title details company responsibilities for periodic financial reports, assessment of internal controls, codes of ethics, and other aspects of disclosures. Section 404 regards the management assessment of internal controls. It requires an "internal

control report", which means the organization must establish and maintain adequate internal control structures and procedures. More importantly, the organization must assess their effectiveness and disclose this assessment in its normal reporting (AICPA, 2006).

This required disclosure is generally interpreted to mean that the organization must report inadequate information security safeguards to its shareholders. Both internal and external auditors have become embroiled under this provision in the evaluation of information security and especially of the security controls provided for information technology. Many of these auditors are not trained to encounter either the information technology or the security of this technology. Lacking deep knowledge in systems analysis and design, and also lacking knowledge in information systems security, these auditors are highly dependent on the recommended practices found in highly specified information security standards such as ISO 17799 and COBIT (discussed below).

There are several factors that lead to difficulties between the auditors and the technology. One of these is the sheer scope of being trained in both the audit specialty of accounting and information systems. There are very few programs that currently provide this level of preparation for auditors. Another factor is the requirement for auditor independence under Title II of SarbOx. Title II deals with conflicts of interest in business relationships of audit firms and requires firms to take steps to unveil such conflicts. In section 201 certain activities and service provision outside the scope of practice are prohibited. This section makes it illegal for an external audit firm to provide non-audit services to companies during their audits. For example, it prohibits a firm from providing information systems design and implementation services to its audit clients. To a certain extent this limits the experience of members of audit firms. Another factor is the innate difficulty of communication between two highly defined professions (namely accounting and information systems), each of which has its own jargon.

As a result tension has developed between auditing and information systems. While information systems specialists might see the auditors as poorly prepared for an internal audit of an IT system, the auditors may shift the blame to the IT specialists. There have been concerns that insular and incompetent information technology divisions will sabotage efforts to comply with SarbOx. Accounting specialists have recommended that organizations take steps to improve their information specialists. These specialists are seen to lack domain knowledge and internal control knowledge, and that these combine to create significant weaknesses in the controls in systems developed by information technology specialists. Rather than train auditors on IT, some accounting authorities have recommended training IT specialists on internal control, risk awareness, and functional domain areas (Cannon and Growe, 2004).

From the perspective of some of those faced with this auditing challenge, an alternative to the conversion of weak IT departments would be to outsource the IT altogether. This outsourcing is seen to eliminate a weak company staff and its problems with internal politics. This elimination is also seen to improve management satisfaction with internal IT. Because this management decision is often needed in the context of an internal audit, rather than training auditors in IT, it might be more appropriate to train these auditors about when and where to outsource IT (Lanz and Tie, 2004).

While SarbOx is developing into such a stringent set of IT security requirements that some organizations are advised to get rid of IT altogether, the Australian approach is softer. CLERP 9 is based on disclosure rather than prescriptive rules (The Treasury, 2002). Like SarbOx, CLERP 9 regulates auditor independence, periodic reporting, and corporate certification of financial reports. While the Australian program is less prescriptive, imposes fewer obligations, and draws short of criminalizing reporting deficiencies of executives, the ethical purpose is similar. CLERP 9 establishes new standards for auditor independence that are broadly similar to SarbOx and periodic reporting requirements that provide continuous disclosure. While executives are not required to certify the maintenance of internal controls, they are required to certify to the directors of the company that the financial statements comply with accounting standards and represent the true and fair view of the current financial position of the company (Grey and Dale, 2005).

While CLERP 9 is less of a rule-based approach to regulating the ethics of corporate governance, SarbOx can be more invasive. In certain fairly common situations, such as those involving global companies with publicly held American subsidiaries or publicly held American companies that are closely dependent on foreign trading partners, SarbOx compliance certification may be required for foreign companies. This opens the possibility, for example, in which a firm may be required to be compliant with both SarbOx and CLERP 9. The two systems are similar enough to permit parallel compliance. While the separate governments' provisions differ only in immaterial ways, Australian companies that must additionally comply with SarbOx must invest additional time and resources with the obvious impact on overhead costs and therefore competitiveness. SarbOx, being the more restrictive legislative framework, is consequently becoming a form of legislation known as "extraterritorial law". The act can be seen to override national regulatory authorities in other countries, such as the case where SarbOx takes precedence over CLERP 9 in parallel compliance situations. While there are no obvious conflicts in parallel compliance in terms of internal auditing, some conflicting problems between SarbOx and other national

regulations have arisen, particularly in the area of attorney-client confidentiality (LexisNexis, 2003). The potential for future conflict is present.

COMPETING STANDARDS AND COMPETING SERVICE PROVIDERS

A recently published study of worldwide information security risk management practices has shown that the use of information security standards in developing the security requirements for information systems has become a global best practice (Baskerville, 2005). For example, 41% of surveyed companies are following ISO 17799, 21% are following CobIT and 17% are following BS 7799 (these categories are not exclusive).

The rise of the use of security standards is connected with difficulties in using traditional risk analysis calculations for developing economic justification for the acquisition of security controls. The study shows that only about 25% of the surveyed organizations are using serious risk analysis approaches. This risk analysis approach involves complex calculations on questionable data and consequently fails to economically justify some of the most basic and essential security safeguards. Instead, it seems, most organizations are following a security standard. Justification for the acquisition of proper safeguards according to an internationally recognized standard may carry more weight with management that using economic risk analysis.

Because the internal auditors are reaching for the standards in the audit of systems for SarbOx compliance, it becomes more rational to use widely recognized standards as the basis for selecting and implementing controls in the first place. As long as the auditors use the same standard as the system designers, and the safeguards are operated properly, SarbOx compliance certification is more likely.

There are competing standards. Table 1 lists examples of these standards in comparison to their scope. Some standards are international in scope while others are promulgated by national governments. Still others are developed by professional organizations as standards of professional practice. Finally there are security standards promoted by industry groups.

Scope of Standards	**Examples**
International Standards	ISO/IEC 15408 ISO/IEC 17799:2005 ISO/IEC 27001:2005 OECD Guidelines RFC 2196
Government Standards	ACS133 BS 7799 German IT Baseline Protection Manual US NIST 800 Series
Professional Standards	CobIT ITIL
Industry Standards	PCI

Table 1. Examples of standards of differing scope.

A notable front runner is the ISO/IEC 17799:2005. This standard provides a security management framework, and detailed recommendations for security policies along with a wide variety of specific safeguards and controls such as access control, communications controls, physical security, personnel security, etc. (ISO/IEC, 2005). This standard was developed from the original British Standard, BS 7799, and with the endorsement of the International Standards Organization, has substantial adherents.

But another front runner is CobIT, Control Objectives for IT (2005a). This standard is growing in importance because of its tight connection with compliance under SarbOx. The standard evolved from the more general internal audit compliance framework from the "Committee of Sponsoring Organizations" (COSO). The development of CobIT within the COSO framework means that the controls recommended from this standard are highly consistent with standard auditing frameworks (Edelstein, 2004). Not surprisingly, CobIT has more appeal when the controls standards are invoked because of SarbOx compliance. Auditors find the framework within which this set of controls is developed to be more familiar and consistent with audit reports.

Standards such as ISO 17799 and CobIT are available for selection to guide organizations in specifying requirements for their information security. The standards are not entirely conflicting. At the basic level, the safeguards and controls recommended by both standards are rather similar and entirely compatible. However, definitions for the processes by which safeguards and controls are specified and acquired are more complete and independent in the ISO standard than in the CobIT standard (von Solms, 2005). The similarities and differences between these two front running standards suggest that the adoption decision for the appropriate standard will be based on a number of factors aside from the exact controls requirements of an internal audit. These decisions

will also be based on the organizational environment and the type of information security management operating in the firm.

But these are not the only two information security standards. In fact, the original BS 7799 has continued to evolve independently of ISO 17799, and now exists as a separate international standard (ISO/IEC 27001:2005). This standard has evolved toward the development of management systems for information security and provides a stronger basis for third party audit and certification. It offers a managerially-oriented complement to the technologically-oriented ISO 17799.

A variety of other general international standards exist, ranging from the more technical (e.g., the *RFC2196 Site Security Handbook* of the Internet Engineering Task Force) to the more abstract. As an example of the later, the OECD Guidelines provide a direction for national legislation that seeks to create a proper security culture in organizations (2002)

There are also a wide variety of national IT security standards. These standards are generally developed for the purpose of mandating security requirements for the relevant government agencies. In other words, government organizations are required to adhere to the nationally defined IT security standards. Examples of these include the Australian Communications Security Instructions Number 33 (ACSI33) *Security Guidelines for Australian Government IT Systems*, the encyclopaedic US NIST 800 series standards, and the German Federal Agency for Security in Information Technology's *IT Baseline Protection Manual*.

While certain government agencies may be required to follow the appropriate national information security standards, the government standards setting agencies publish the standards to permit their adoption by non-government organizations in the interest of promoting better information security nationwide or worldwide. The standards will almost always be followed by organizations with close commercial contracting ties to the government, and in some cases may be required where these commercial contractors are developing or using sensitive government information.

In at least one case, government efforts to develop better government security have evolved into broader professional standards. The IT Infrastructure Library (ITIL) is a series of monographs to promote best practices for managing information technology services. This IT services orientation has led to a set of best practices that are integrated and process based. These have clear objectives in the quality, efficiency, and cost-effectiveness for the delivery of IT services. ITIL volumes include software asset management, planning for service management, etc. There is a volume dedicated to security management that has all the elements required for an information security standard including process areas at strategic, tactical, and operational levels. The volume encompasses security products, such as policies, processes, procedures, and work instructions (Weil, 2004).

There are also industry standards that are mandated for compliance by organizations operating in those industries. One good example of an industry standard is the Payment Card Industry (PCI) Data Security Standard developed by Mastercard and Visa to impose minimum security standards on any organization processing credit card data (2005b).

Although less relevant as a framework for information security management in information systems, there are standards that provide evaluation criteria for computer products. Foremost among these standards is the Common Criteria (ISO/IEC 15408), developed by standard setting bodies from a variety of countries including Canada, France, Germany, The Netherlands, the UK, and the US. This standard provides assurance based on evaluation and active investigation of IT products or systems that are to be trusted. It is distinctive in the value it assigns to expert evaluators and its emphasis on scope, depth, and rigor. However, it has not been formally applied as an overall information security management standard, but rather focuses on the certification of products that might be acquired as components of a secure information system.

In terms of specifying requirements for information systems security, many organizations could select any of the above information security standards. Contingency theory would suggest that it might be possible to develop a set of universal criteria by which the ideally appropriate standard could be deduced from a set of organizational and environmental characteristics (Davis, 1982). However, side-by-side comparisons of these standards are relatively rare and anecdotal (cf. von Solms, 2005, Roberts, 2006). The lacuna in the literature may be caused by the dramatic difference between the standards. Each is based on differing frameworks, philosophies, and assumptions about information systems and their security. Comparison criteria are likely to favour one or two of the standards over the rest in most situations. Consequently the selection of the appropriate standard becomes a situational, ideographic problem. The problem is exacerbated by the wide variety of available standards for adoption.

This problem provides an unusual market setting for competition between the standards for adoption by "customers" in need of an externally validated security requirements definition. However, few of these standards are developed by organizations with commercial goals that profit from discrete adoptions of their standards. Neither the standards nor their or originating organizations are intent on competition with other standards. The

commercial competition arises from commercial organizations and IT service providers that develop specialized expertise in the area of one or more of the standards. In this way the marketplace for the standards is shaped by the specialties and preferences of the service providers available to help organizations in adopting and applying a particular standard, and competing with other service providers with similar expertise or specialized expertise in competing standards.

The presence of the service providers in a setting where potential adopters of security standards face a confusing array of highly situated alternatives makes this marketplace very real and very competitive. In the presence of this marketplace, information security standards adoption is rarely a rational and obvious decision for each organization. To a degree, the competitive nature of the standards marketplace is not well recognized by many organizations. In fact, the selection of a security standard is akin to the selection of ideal product to match the adopting organization, its culture, its situation, its scope, and its economic profile.

AUDIT FIRMS AND GOVERNMENT REGULATORS

Because of the presence of government or industry regulations and guidelines, this marketplace is also inhabited by organizations and individuals connected with developing and enforcing these regulations. For example, audit firms under SarbOx are charged with reviewing processes for assessing internal controls. Note carefully that the external audits may not extend to actually reviewing the internal controls, but rather reviewing the processes for assessing internal controls. This is an important distinction because the audit firm may directly evaluate the security standards adoption decision as a component for developing and assessing internal controls in IT systems. In other words, an auditor may well be required to evaluate whether an organization that adopted ISO/IEC 17799 for assessing internal controls should have instead adopted CobIT.

As a consequence, adoption decisions made in the information security standards marketplace may be subject to review by audit firms. Because audit firms are required to be independent of the organizations they audit, these firms cannot consult in the adoption decision. By regulation, at least under SarbOx, the audit firm cannot predetermine the safeguards standard adoption decision. Organizations that adopt a security standard should be able to demonstrate in an external audit that the standard is the most ideal for the organization. But inevitably, the organization must independently make this decision in the security standards marketplace.

Government regulators may also be a distant factor in the security standards adoption decision. For example, SarbOx Title I creates the Public Company Accounting Oversight Board (PCAOB). This board is charged to register and review public accounting firms that provide external audit services to publicly held companies. The PCAOB has responsibilities for investigations and disciplinary actions for breaches of accounting standards. Ultimately, any lapse in audit independence could be subject to investigation and punishment by this board. The PCAOB is an indirect factor in the standards marketplace by ensuring that organizational decisions about standards adoption are made independently from an external auditor.

REORIENTED SECURITY DESIGN METHODS

In the presence of stringent IT controls assessment by internal and external auditors, security standards become benchmarks for measuring internal control. This benchmarking drives the use of information security standards as a mechanism for specifying security controls requirements. This drive has forced security design methods to evolve. However, the evolution is a somewhat subtle one. In general, the overall process for security safeguards specification is largely unchanged. This generic process is shown in Table 2.

Stage 1: Identify and evaluate system assets
Stage 2: Identify and evaluate threats
Stage 3: Identify possible controls
Stage 4: Risk analysis
Stage 5: Prioritize controls for implementation
Stage 6: Implement and maintain controls

Table 2. Generic security project stages (from Baskerville, 1993).

Implementation of the generic stages varies with overall methodology and variations offer features that provide situated improvements. An example of an instance of this generic model is shown in Table 3.

Phase 1: Build Asset-Based Threat Profiles
Process 1: Identify Senior Management Knowledge
Process 2: Identify Operational Area Knowledge
Process 3: Identify Staff Knowledge
Process 4: Create Threat Profiles
Phase 2: Identify Infrastructure Vulnerabilities
Process 5: Identify Key Components
Process 6: Evaluate Selected Components
Phase 3: Develop Security Strategy and Plans
Process 7: Conduct Risk Analysis
Process 8: Develop Protection Strategy

Table 3. Octave Method, Operationally Critical Threat, Asset, and Vulnerability Evaluation (Alberts and Dorofee, 2001)

Traditionally, risk analysis offered a form of economic cost-benefit analysis that could be used to justify the acquisition of a safeguard identified in earlier steps. Risk analysis provided information about whether the cost of the safeguard would be greater than the probable losses without the safeguard in place. If the cost of the safeguard was lower than its potential benefits, the safeguard was acquired. What is philosophically important in this process is that risk analysis provided the means by which a decision was made to adopt a safeguard. Theoretically, without the risk analysis, safeguards were unjustified, and none were adopted.

What changes in both the generic model and its instances is the usefulness of the risk analysis in the presence of indirect regulatory mandates for IT security controls. Regulatory mandates define a requirement for the assessment of information assurance. This required assessment results in the selection and adoption of an information security standard from the standards marketplace. The adopted security standard defines a set of IT security requirements in the form of various information systems security safeguards and controls. In cases where security safeguards, as defined in standards, are not implemented then at some point assurance auditors will compare internal IT controls with those in established standards. This comparison will generate exceptions where the absence of controls indicates a failure to comply with standards. Such exceptions become urgent requirements in the next round of security safeguards specification.

Importantly, the presence of regulations and standards shapes a default decision to adopt all safeguards defined as appropriate in the standards. The role of risk analysis now changes. Risk analysis can provide information about safeguards that have been recommended in the standards but are economically unjustifiable when compared to the probable benefit. This risk analysis evidence can be presented to assurance auditors to explain why the exception is justifiable. In other words, risk analysis is used as a mechanism by which an organization might choose *not* to adopt certain safeguards and controls as defined by the standards. Theoretically, without the risk analysis, all safeguards are justified, and all are adopted.

In this way, compliance with standards reorients typical security design methods. The presence of regulatory mandates and standards for information security changes the default decision and changes the role of risk analysis in information security management. Before regulatory mandates and standards, risk analysis was used to justify the adoption of the safeguard. After regulatory mandates and standards, risk analysis is used to justify a decision not to adopt a safeguard. The inversion of the default decision and the changing role of risk analysis and information security is an important one. Previous research is shown that only about 25% of organizations are likely to practice risk analysis and in a methodical way. Prior to regulatory mandates and standards, this meant that organizations were in danger of having inadequate security and safeguards in place because of a lack of risk analysis to justify the adoption of these controls. After regulatory mandates and standards, organizations are in danger of adopting too much security, and far too many safeguards and controls than economically justifiable and thereby unnecessary for due care in their business.

DISCUSSION

Legislation intended to improve public disclosure of organizational operating profiles has developed substantial changes in the manner in which IT security controls requirements are specified. The economy of IT controls has been reversed, meaning that organizations working to justify controls must now work to justify avoiding controls. While this reversal certainly improves the security of IT systems, it opens up more possibilities for IT systems that are overly expensive. Such expensive IT systems may thereby diminish the competitiveness of the overall organization. If there is a reduction in competitiveness for compliant firms, there are serious implications for the ethics and culture of the professions involved in developing compliance.

If the burden of the mandated IT systems security leads to diminished competitiveness, the situation is not likely to prevail in the long term. Uncompetitive organizations must reorganize or fail. One possible avenue for

reorganization regards "creative" or misleading compliance (Cooper and Deo, 2005, p. 162). Creative compliance is an endemic problem that creates cycles of regulatory failure. Existing management systems endure regulatory reforms, and continue to promote professionals who control and thwart new regulations. Such management systems can exploit, for example, the IT security standards marketplace. Inappropriate, ineffective, but cheaper, security standards might be adopted in order to reduce the overt requirements for security safeguards. For example, an organization might choose to adopt the narrower CobIT standard where their situation calls for the broader, more process-oriented ISO 17799. This adoption could reduce the overall security costs without recourse to extensive risk analysis. Auditors and regulators could be satisfied and security costs reduced, but undue information risks may result because the wrong standards are adopted.

Another possible way that creative compliance can exploit existing management systems would be to adapt security design methods to streamline processes that justify internal controls exceptions. For example, "improved" tools for the automation of risk analysis that more frequently undervalue risks would create a larger number of economically justified controls exceptions. Such undervaluation of risk could effectively rebalance the IT safeguards economy closer to its original (and more competitive) state.

Creative compliance arises because standards and regulatory environments represent technical and political dimensions of corporate governance. The more important dimensions are the ethical and cultural aspects (Robins, 2006). The current cycle of regulatory reform will progress steadily toward a new cycle of regulatory failure unless the professions correct the ethical and cultural flaws that will inevitably abuse management systems to defeat costly regulation.

In terms of correcting the professions' ethical and cultural flaws in the case of IT security safeguards, IT professionals would seem to have a large degree of progress available. Observations by the audit profession that IT professionals lack knowledge in information security controls (Cannon and Growe, 2004, Lanz and Tie, 2004) are confirmed by studies in security awareness (possibly the most prevalent information security organizational policy). A recent survey by the Computer Research Institute reports that most security respondents believe that security awareness training is important, yet on average, they don't believe their organizations invest enough in it (Anonymous, 2005). This result is not surprising, since the security awareness has a very high ROI, and yet is underrepresented in the literature:

> "Additionally, I fear that too many security training and awareness efforts are sub par. Some organizations' security training and awareness programs are, bluntly put, pathetic -- they simply present platitudes about security to their captive audiences instead of teaching things that could and should make a practical difference in each attendee's daily job. Many programs are (like so many security practices) out of alignment with the organization's business goals and/or out of date with current technology." (Schultz, 2004, p. 2)

As measured by the status of security awareness training, there is room for improvement in the ethical and cultural frames of IT security professionals. If the ethics and culture are poorly developed, the effective implementation of standards adoption will be limited. The implications suggest it is quite possible that the current overzealous attention focussed on information security controls by regulatory reforms will dissipate into creative compliance with little lasting impact on the effective internal controls in an organization's information systems.

CONCLUSION

An organizational decision to adopt an information security standard is one taken in a complex marketplace of competing standards, competing service providers, competing security design methods, and competing national and international legislative requirements. The decision, and the security safeguards adoptions that are implied by this decision, are reviewed by closely-watched internal and external auditors whose actions are subject to further review by government regulators. Far from being a straightforward, rational, technical decision, the decision to adopt a security standard is problematic for contingency criteria, and highly situational.

Once standards are adopted, firms subject to close oversight of internal IT controls will find that the nature of their security design methods is changed by the adoption. Where previously risk analysis was necessary to justify controls acquisition, risk analysis is now necessary to avoid unnecessary controls acquisition. The default setting is the broad acquisition/implementation of all recommended safeguards in the adopted security standard. As a result, the overhead for IT controls compliance is likely to rise for organizations falling under tight regulation controls without more careful attention to the risk analysis component in security design methods.

The reaction to the rising overhead may also include less ethical behavior than improved risk analysis. IT professionals and system auditors may succumb to the alternative of creative compliance with standards. This kind of compliance means that organizations would ultimately make misleading public statements about their IT security. Such intentional misstatements were most certainly not the intended effect of the more extensive

requirements for disclosure. Yet this outcome can easily occur if the responsible IT professionals fail to fully understand the security standards adoption decision, and the complex marketplace within which this decision is taken.

REFERENCES

(2002) OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security *Directorate for Science, Technology and Industry* Paris, Organisation for Economic Co-operation and Development

(2005a) COBIT--Overview. Rolling Meadows, Illinois, Information Systems Audit and Control Association.

(2005b) Payment Card Industry Data Security Standard O'Fallon, Missouri, MasterCard International.

AICPA (2006) Summary of Sarbanes-Oxley Act of 2002 New York, American Institute of Certified Public Accountants.

Alberts, C. J. & Dorofee, A. J. (2001) OCTAVE Criteria Version 2.0. Pittsburgh, Software Engineering Institute.

Anonymous (2005) Businesses Respond to Cybercrime and Security Trends. *The CPA Journal,* 75**,** 9.

Baskerville, R. (1993) Information systems security design methods: Implications for information systems development. *ACM Computing Surveys,* 25**,** 375-414.

Baskerville, R. (2005) Best Practices in IT Risk Management: Buying safeguards, designing security architecture, or managing information risk? *Cutter Benchmark Review,* 5**,** 5-12.

Cannon, D. M. & Growe, G. A. (2004) SOA compliance: Will IT sabotage your efforts? *The Journal of Corporate Accounting & Finance,* 15**,** 31.

Cooper, K. & Deo, H. (2005) Recurring Cycle of Australian Corporate Reforms: "A Never Ending Story". *Journal of American Academy of Business, Cambridge,* 7**,** 156.

Davis, G. (1982) Strategies for information requirements determination. *IBM Systems Journal,* 21**,** 4-30.

Edelstein, S. M. (2004) Sarbanes-Oxley Compliance for Nonaccelerated Filers. *The CPA Journal,* 74**,** 52-59.

Grey, K. & Dale, L. (2005) Australian companies and Sarbanes-Oxley: Governance regulation in a parallel universe. *Keeping Good Companies*.

ISO/IEC (2005) ISO/IEC 17799: Information technology -- Security techniques -- Code of practice for information security management. Geneva, International Standards Organization.

Lanz, J. & Tie, R. (2004) Advise Businesses on External IT Resources. *Journal of Accountancy,* 197**,** 55.

LexisNexis (2003) Sarbanes-Oxley Disclosure and Confidentiality: The 2003 LexisNexis-IBA Legal Survey. LexisNexis and International Bar Association.

Roberts, P. (2006) Calculating Risk, Navigating Compliance. *Infoworld,* 25**,** 21-28.

Robins, F. (2006) Corporate Governance after Sarbanes-Oxley: an Australian perspective. *Corporate Governance,* 6**,** 34.

Schultz, E. (2004) Security training and awareness - fitting a square peg in a round hole. *Computers & Security,* 23**,** 1-2.

The Treasury (2002) Corporate Disclosure - Strengthening the financial reporting framework. Canberra, Commonwealth of Australia.

Von Solms, B. (2005) Information Security governance: COBIT or ISO 17799 or both? *Computers & Security,* 24**,** 99-104.

Weil, S. (2004) How ITIL Can Improve Information Security. *Security Focus.*

COPYRIGHT