THE Open GROUP
Making standards work®

Information Security Strategy

A Framework for Information-Centric Security Governance

A White Paper by:

The Open Group Security Forum and
Cyberspace Law Committee, Business Law Section,
American Bar Association

October 2007

Information Security Strategy:
A Framework for Information-Centric Security Governance

Document No.: W075

Published by The Open Group and American Bar Association, October 2007

Any comments relating to the material contained in this document may be submitted to:

The Open Group (ogpubs@opengroup.org)

or to:

American Bar Association (copyright@abanet.org)

Contents

Abstract

This White Paper proposes a new framework for ensuring enterprise-level information security that reflects current realities of enterprise, network, and information sharing and access. In the "old" paradigm – one based on concepts of securing ownership of proprietary information – information security was accomplished mainly through securing a physical "perimeter" focusing on network hardware and software technologies. The new realities of information access and use – based now on distributed networks, distributed relationships within and between enterprises that use a mix of proprietary and non proprietary information – require securing information and infrastructure access and flows beyond the perimeter. This new paradigm requires dynamic interaction of technologists, legal advisors, and business policy makers.

The production of this White Paper is in itself an example of the process proposed in the paper. The Security Forum (bringing the perspective of standards, technology, and business), together with the Cyberspace Law Committee (bringing the perspective of business legal advisors), have cooperated in analyzing and recommending improvement to current, perimeter-based, and proprietary-based enterprise-level information security practices to propose a new framework for effective information-centric security.

Boundaryless Information Flow™
achieved through global interoperability
in a secure, reliable, and timely manner

Executive Summary

In the globally connected business environment, enterprises require IT systems and services that are (in no particular order) available, easy-to-use, reliable/robust, globally networked, agile/adaptable to changes in business operations, manageable – and all this safely, securely, compliant to applicable regulations and audit practices, and achieved at lowest cost. In this environment, information security solutions (securing the value in information and information flows) are not simply technical in nature.

Today's globally networked systems need a governance team that includes the viewpoints of all the business stakeholders, to reconcile the often competing and conflicting objectives from each community of interest, so as to arrive at appropriate solutions. The stakeholders that security architects and IT technologists need to work with as a team include public policy makers, corporate legal counsel, corporate policy makers, risk management decision-makers, auditors, and business managers, to information technologists, auditors, and business managers.

While these functional responsibilities will likely always remain in any enterprise, this White Paper proposes a dynamic, process-oriented, information-centric security governance framework that cuts across functional boundaries that will aid in resolving conflicting viewpoints – a methodology for security compliance both within and beyond the perimeter of the enterprise – and recommends further development to support information-centric security in a boundaryless environment. Information governance determines many things central to achieving effective information security, including:

- Prioritizing and managing risks to information security
- Funding or sponsoring new security initiatives and sustaining the operations of old ones
- Ensuring corporate compliance to applicable law and regulation
- Building a business that successfully competes within its chosen market

All these considerations are included in this White Paper, which also presents a dynamic framework for how an enterprise-level governance team can approach information-centric security. It describes:

- A framework for information-centric security governance by identifying key stakeholders, their roles, and areas of responsibility
- A methodology for security compliance both within and beyond the perimeter of the enterprise

- Key new standard proposals on areas to support information-centric security in a de-perimeterized environment

This White Paper proposes a strategic approach to a program of work over the next year and beyond. It is intended to be a "living" document, to be re-evaluated and revised as practices evolve in this area. It is not intended to be prescriptive, except in the sense of recommending a more dynamic process-oriented approach to information security. The end of this White Paper considers what further work needs to be done to realize this framework, and what can be done to advance the practice of the security team in support of delivering better information security governance.

The problem in perspective

Among the reasons to analyze the effectiveness of current information security practices are fundamental changes in the underlying assumptions upon which those practices are based – that property (in this case proprietary information) needs to be secured, and that security can be achieved through erecting physical barriers.

Borne out of industrialization in Western Europe, "The idea of the importance of property only originates in scarcity" is the operating premise of much of current information security.[1] There is a history of securing the hardware, software, network, and storage of the infrastructure, dating back to the Orange Book of 1983.[2] For over twenty years enterprises have invested in securing operating systems, networks, storage, communication channels – investments that protect the computing equipment … property that is no longer scarce, and in fact that is so abundant that the very idea of considering it property is no longer important.

Connectivity, storage, and computing resources are abundant. Whether measured by price or general availability, users today do not perceive this infrastructure as having intrinsic economic value. What once were scarce resources only twenty five years ago – storage, memory, computing engines, and network connections – are today available virtually on demand. Advances in computing power and storage capacity, coupled with the evolution of a globally connected economy, have eliminated any real scarcity of the IT connectivity, storage, and computing infrastructure. Yet the way technologists, business managers, policy makers, and others have been taught to treat the security of their information is still through the protection of their computing resources.

On the other hand, information access, integrity, and use, all still represent high business value. Information services providers can still charge high premiums for their services to provide and maintain "asymmetric" differences in information availability. For some enterprises competing in the information age, keeping information scarce is their only business advantage – the only thing worth preserving.

Today's global critical information infrastructure increasingly requires that the private sector, public sector, and consumers have all assumed a spectrum of new risks. At the same time that many who are charged with managing these risks seem not to understand them adequately, the power of individual users of IT systems (through negligent or malicious misuses of systems by employees, contractors, etc.) to do great harm with commodity technology is rapidly growing. Reacting to this concern, industry groups, public interest groups, policy makers, regulators, and others are developing new standards and regulations that place controls on the security management of information systems and their information.

[1] The Theory of Value: A Reply to Professor Macvane by Friedrich Wieser, Annals of the American Academy of Political and Social Science II, (1891-1892), pp. 600-28

[2] Otherwise known as the DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, US Department of Defense, December 1985, supersedes April 1983.

A proposed response

Managing this growing enterprise risk requires a multi-disciplinary effort involving improved collaboration from all those stakeholders who share responsibility for delivering effective enterprise information technology governance: information technologists, legal professionals, business process managers, business policy makers, regulators, and auditors. Unfortunately, the functions, framework, traditions, and standards for this collaboration are not necessarily supportive of a holistic approach in most enterprises. While all these professionals need to work together as a governance team, they simply do not have the guidance that helps them better specify and implement solutions to control sensitive information, consistent with the interests of the business and public.

This White Paper suggests that effective information security will be based on a dynamic, multi-disciplinary consultative governance process. Technologists alone cannot secure the value of the enterprise's information, but a governance team that includes policy makers, legal advisors, corporate policy and risk management, information technologists, auditors, and business management are more likely to identify, assess, and propose holistic solutions for the enterprise than any one group can do individually. Working in concert, rather than in isolation, each of the functional disciplines can contribute to holistic solutions.

What is information security, and how is it achieved?

ISO/IEC 17799[3] gives the following definitions:

> Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.
>
> Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed, and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

Architecturally, the term "security" is used in two contexts. In the first, security can be thought of as a set of features and functions to protect the confidentiality, integrity, and availability of information systems. This context has been well developed by vendors and users alike, resulting in a vast selection of tools, technologies, and standards widely available to customers. From a standards perspective, The Open Group Security Forum currently does not see a particular new contribution that it needs to make that differs from what other standards consortia are already doing.

In the second, security is considered a property of the IT system similar to quality, manageability, and usability. In this context, security is a non-functional property of the IT system and becomes more difficult to conceptualize, measure, and discuss unambiguously. This White Paper is devoted to this non-functional context of "security", in an attempt to give it some definition and to explore value-added standards and initiatives that The Open Group Security Forum, in partnership with complementary stakeholder interest groups, can take as its strategic agenda.

Non-functional system qualities – such as quality of information, quality of service, manageability, security, and usability – tend to be processes that resemble negotiations which resolve conflict amongst competing interests. In this manner, the journey – the continuing dialog, debate, conflict resolution, lessons learned, and continual improvement – is often more important than an arrival at a final destination. [Conducting this journey

[3] BS ISO/IEC 17799:2005, Information Technology — Security Techniques — Code of Practice for Information Security Management

lends itself well to the role security architects take within the enterprise, and as such aligns very well with the interests and expertise of The Open Group and its Security Forum.]

Information Security Architecture

The information security architecture journey consists of governing the resolution of tensions between competing public sector, business sector, and consumer interests:

- Public sector interests are those that governments hold and are manifested in law, regulation, and enforcement. Example interests include public safety, national security, critical infrastructure protection, macro-economic financial risk management, and consumer protection.
- Business sector interests generally balance risk and reward with the objective to achieve optimal shareholder financial results. Wherever possible, risk is minimized for optimal return. To the business sector, information security is an economic risk management problem to be managed in favor of business objectives.
- Consumer interests center around the unintended consequences and assumed risks of the use and misuse of consumer information. Consumers have expressed interests in their controlling the use of information about them by both the business and public sectors. Government can assist the consumer through legislation and regulation.

Resolving the inherent tensions between these three sectors becomes the information security architect's primary objective in developing the non-functional security component of the IT architecture. The architect must consider a new community of stakeholder, their range of interests that need to be represented in the security architecture, and to the extent that is practical, why those people and interests need to be included in the compromise that the security architecture necessarily arrives at as a quality of the information system.

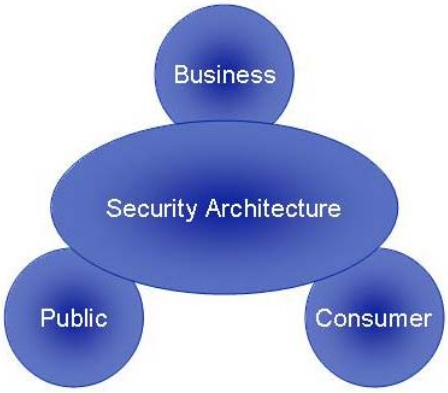

Figure 1: Information Security Architecture

The shapeless security perimeter – information-centric security

Information security used to be about defining infrastructure (connectivity, storage, and computing resource) policy to, in turn, define a closed perimeter by controlling:

- Who went across it (in and out)
- What they could do with the resources (information access)

- When they could cross (time)
- How they could cross (entry port, service)

In this outdated model, infrastructure-based security controlled access to what were then scarce resources:

- Connectivity (bandwidth and network access)
- Storage
- Computational resources/speed

Nowadays, with the decline in scarcity of these resources – evidenced by the requirement to support outsourced information services, supply chains, customer services, and other business needs – security perimeters have become so porous that for many intents and purposes they do not exercise control over a significant proportion of the traffic that passes through them, including email, web, voice over IP, encrypted traffic (SSL, SMTP-TLS, VPN). The Jericho Forum in its brochure "Jericho Forum™ – An Overview and How to Get Involved" puts it this way:

> "While traditional security solutions like network boundary technology will continue to have their roles, we must respond to their limitations. In a fully de-perimeterized network, every component will be independently secure, requiring systems and data protection on multiple levels, using a mixture of encryption, inherently-secure computer protocols, inherently-secure computer systems, and data-level authentication. The design principles that guide the development of such technology solutions are what we call the Jericho Forum "Commandments", which capture the essential requirements for IT security in a de-perimeterized world."[4]

While perimeters, borders, or boundaries may be shrinking – and in some cases disappearing – they are more often than not changing to perimeters without any specific shape. Perimeters still exist, but they traverse across traditional borders of enterprises and systems and assume shapes that many security architects are inexperienced with. This new "shapeless perimeter" reflects the loss of the traditional shape of enclosing an entity with traditional forms, such as the enterprise perimeter, or host platform system. Instead, this shapeless perimeter surrounds the information, from wherever it is to wherever it is going. This raises the question: "How are non-functional security qualities established around something as intangible as information?" We've entered a new paradigm – information-centric security.

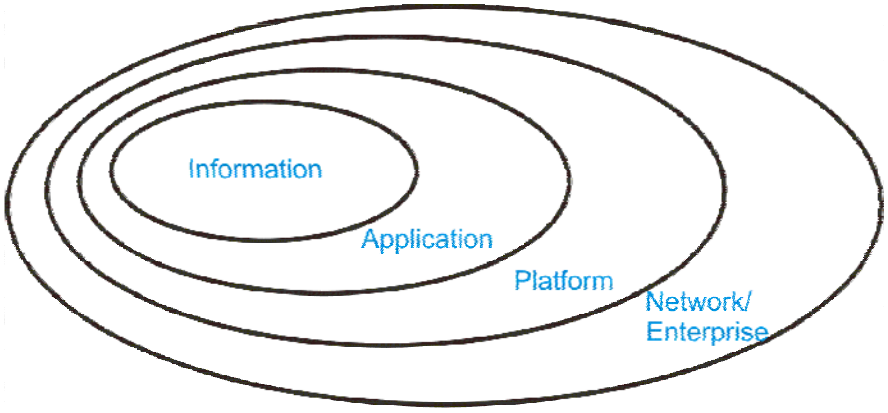

Figure 2: Traditional Layered Enterprise Perimeter Security Model

[4] From Jericho Forum home page – www.jerichoforum.org, August 2007.

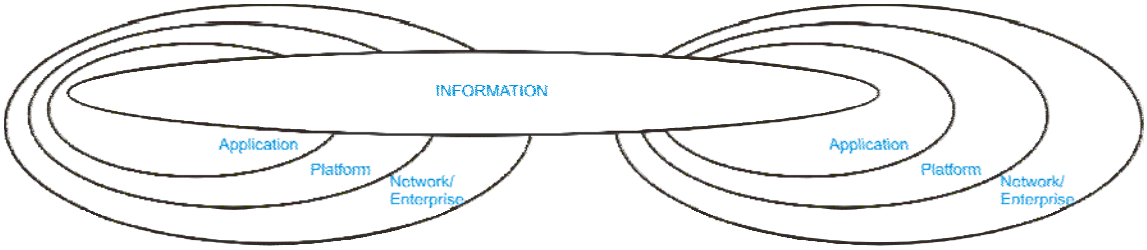

Figure 3: Information-Centric Security

Information-centric security is all about control

Previous work of The Open Group Security Forum and the Cyberspace Law Committee[5] has already recognized[6] that the "control" of intangible electronic assets – i.e. information – is a functional equivalent for "possession" of physical assets in the physical world. By extending the example of this path-breaking work here, information-centric security becomes a question of maintaining the equivalency of ownership through control over information assets wherever they are. To this end, four key principles of control emerge:

- Information now is a "controlled substance". Just like other controlled substances in the real world – such as drugs, liquor, and weapons – information can be used both usefully and destructively, making information and its stores both assets and liabilities. The state expresses its interest in control of information through regulation in its use and public disclosure in cases of loss of control.
- Control is a people, process, and technology problem. Technology alone cannot control information. People must take responsibility for the information entrusted to them by adequately safeguarding it through appropriate administrative and technical control purposes.
- Information can only be controlled within a perimeter – what The Open Group calls the Control Environment. Unless the information carries with it protection mechanisms that can enforce or extend control over its access and usage, once information leaves the controlled environment, its owner has lost control of it.
- Control at a distance is hard. Controlling information within a managed application or firewall perimeter is hard enough. Extending that control beyond the enterprise is very hard, but that is what is necessary to enable the global extended enterprise to share at an acceptable level of risk its sensitive information assets with its customers, suppliers, business partners, and outsourced service providers. Control beyond the enterprise is accomplished through the establishment of and compliance with:
  - Legal agreements between information sharing parties
  - Verifiable administrative, technical, and physical control practices
  - Standards that set expectations for control

[5] See The Open Group publication G061 (www.opengroup.org/bookstore/catalog/g061.htm) dealing with electronic chattel paper.

[6] Uniform Commercial Code section 9-105.

Controlling information within a virtual perimeter

The Open Group Security Control Framework presents the fundamentals underlying securing information. Essentially, information security in this context consists of:

- Defining actions to take
- Monitoring that they have occurred
- Taking action when they haven't

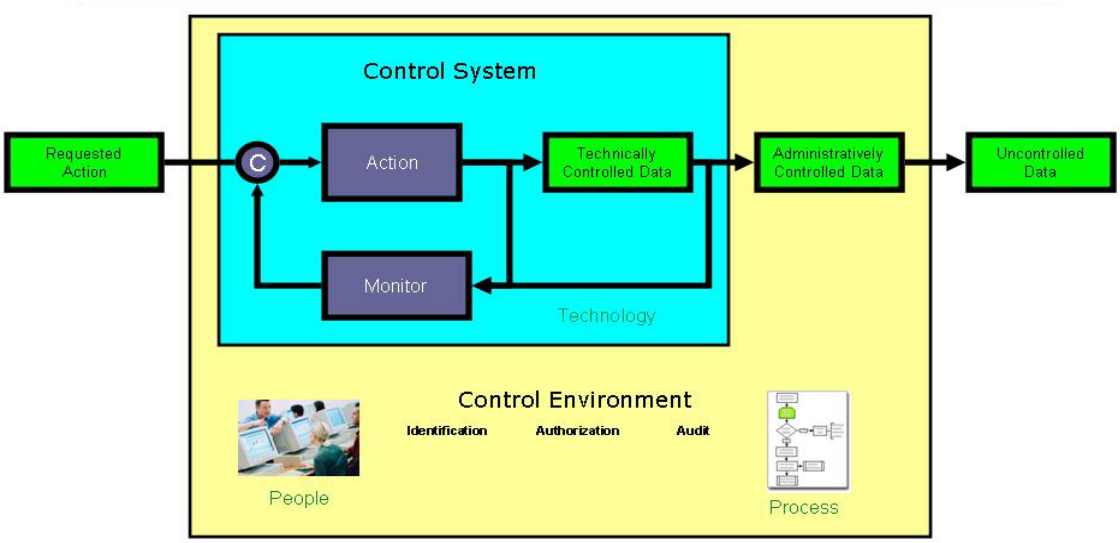

Figure 4: Framework for Control

Extending control beyond the perimeter or control environment

As mentioned earlier, control beyond the enterprise's environment is hard. It's hard primarily because of two considerations:

- A larger group of professions and people beyond the information systems and technology people are involved. This increases the dialog, complexity, and opportunities for misunderstandings to occur.
- Once information has left the controlled enterprise environment, all that's left is for the information owner to place their trust in the control exercised (or not) by external people, processes, and technologies.

Compliance

Managing people, processes, and technologies outside of one's own direct control has strong parallels with the general problem of compliance to external standards, regulations, or policy. It's appropriate, therefore, to begin a discussion of extended control with a discussion on the general process of compliance with policy or standards.

A generalized compliance model works such that if the corporate policy complies with the external requirements, legal and otherwise, and if the IT operation complies with policy, then the IT operation complies with the external requirements.

A framework for compliance

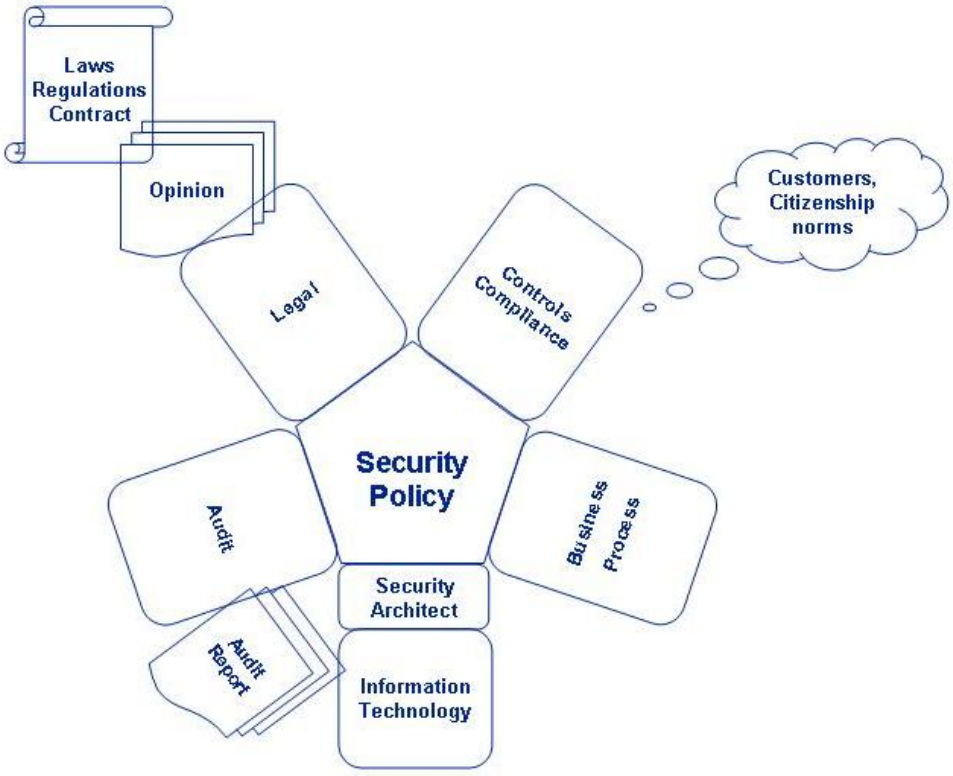

Figure 5: Framework for Compliance

There are six important major activities:

- **Determine the Compliance Objective.** Compliance must be discussed as "compliance to what standard or objective?" Compliance to legal and regulatory requirements alone may not be good enough to meet business requirements. Contractual obligations, service level agreements, customer expectations, and norms of good corporate citizenship all are external requirements that must be complied with.
- **Assess external compliance requirements.** For those compliance objectives that are legal in nature, corporate legal must assess the external requirements to determine what applies to the enterprise and its business. Assessment of applicable law and contractual obligations is a legal function.
- **Establish corporate policy.** For compliance objectives that are not legal in nature, business process people and corporate management must establish policy consistent with corporate business objectives.
- **Evaluate compliance to external requirements.** Working with a policy group (called "controls compliance"), the legal function must determine and document through a legal opinion whether the enterprise, through correct implementation of its policy, complies with the applicable legal requirements. Only the legal team can write this opinion, and the attorneys then assume that policy is followed.

- **Implement information systems compliant to corporate policy.** The information technology people must implement systems that are compliant to policy.
- **Evaluate compliance of internal systems implementation to corporate policy.** The audit function assesses whether that the information systems processes and technologies comply with corporate policy, providing management assurance that the intentions of the policy have been carried out.

Using the compliance model to extend control beyond the enterprise

Largely established through formal agreements such as a contract or service level agreement (SLA), control beyond the traditional enterprise perimeter consists of:

- Establishing an agreement to control the information through the perimeters of the enterprises involved
- Verifying compliance to an SLA

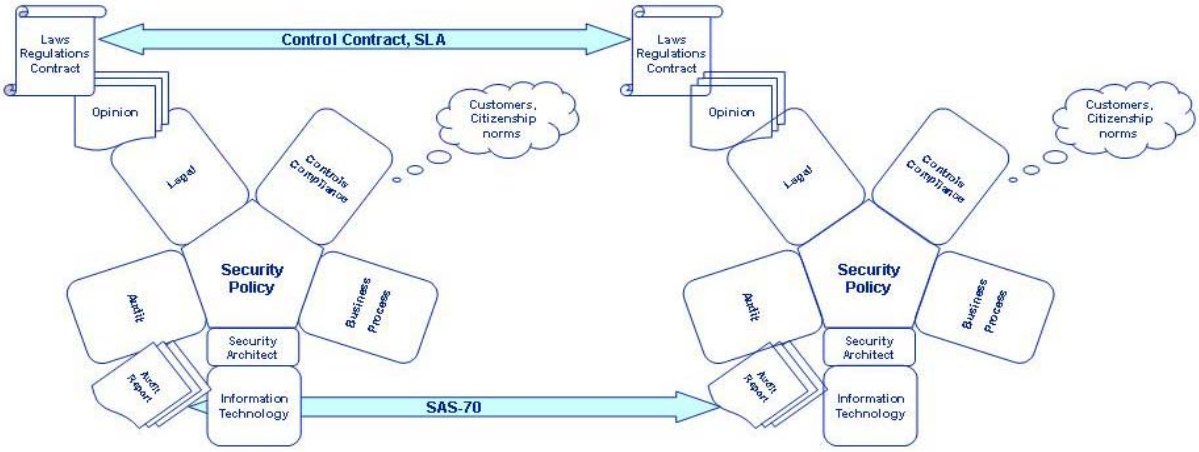

Figure 6: Control beyond the Enterprise

Establishing service level agreements is a business management and legal process. Verifying compliance to an agreement may be achieved though an interoperable, standard audit methodology known as the Statement on Auditing Standards (SAS) 70 report.

The SAS 70 report is a tool of IT audit/attestation used to provide a measure of comfort that IT is operating as anticipated to address process or organizational goals. For example, examining controls around system access builds confidence that only the right people (as defined by management) have access to data held within critical systems. To avoid having to conduct an audit on a vendor of critical systems, the information owner can request the vendor to produce a SAS 70 report. By choosing controls that measure the vendor's compliance to predetermined standards or objectives, legal and regulatory requirements, contractual obligations, service level agreements, or best practices, the information owner can determine the degree of the vendor's compliance, and so evaluate whether the vendor meets or exceeds the information owner's goals for managing its information.

Conclusion

Whether described as "de-perimeterization", "information centric security", or "a framework for the control of electronic assets", the information security governance team must consider economic, policy, and technical

factors impacting the security architecture, and represent all the different "views" needed to sustain all of the stakeholders in the process. Security as a combination of "people, processes, and technology" is nowhere more evident than in the control of information across enterprise perimeters. Corporate legal, corporate policy, and internal audit are now among the key stakeholders in a corporation's security architecture. The needs of these stakeholders have in the past not been well articulated within the architecture community, but they need to be.

Helping these new stakeholders to better understand the processes and technologies used to implement policy is essential to making the compliance framework work. As a quality of the system, security contributes significantly towards resolving the needs and tensions between these stakeholders. Security architects can take a lead role in facilitating this dialog between the different stakeholder viewpoints.

The Open Group Security Forum, as a leading consortium representing the value that sound enterprise security architecture practice contributes towards delivery of effective information security solutions, wants to facilitate and encourage development of tools, methods, and open standards needed to improve security architecture methodology and essential practices. These will enable the security architect to contribute most effectively to the community of excellence that the governance team (described in A proposed response) represents, to take information-centric security from an as-is-now to a where-we-want-to-be state.

Additional strategy components

The items below are highly relevant components in consideration of security strategies, so are listed as placeholders which can be expanded as progress is made on implementing the strategy outlined in this White Paper.

- Monitoring is a key piece of control, but there are few standards in this area. It also is a politically charged issue – what can and should you monitor? What records are appropriate to include here, bearing in mind privacy and related constraints? This would be a good multi-disciplinary project to take up – including as it should a joint discussion with the legal community leading to clarification on what can and what should not be monitored. This area of work should include developing a standard for log interoperability and analysis.

  A proposal now underway in The Open Group Security Forum to extend the existing Open Group Distributed Audit Services (XDAS) Preliminary Specification (1998) to meet today's requirements for logging and other features. This work is expected to go some way towards meeting this requirement.

- Develop guidance on additional architectural viewpoints needed to serve the legal and audit communities. Include these in The Open Group Architecture Framework (TOGAF) including its Architecture Development Method (ADM).

- Develop additional viewpoints on control. For example, develop a monitoring and corrective action viewpoint and integrate it into TOGAF.

- Develop additional architectural views for compliance.

  If this is risk-based compliance, then an acceptable risk framework to demonstrate compliance is necessary. A project is now underway in The Open Group Security Forum to develop a standard for Risk Analysis and Risk Management, based on the Factor Analysis for Information Risk (FAIR) methodology. This project is expected to provide a suitable framework to meet this requirement.

- Collaborative awareness and joint project work with the legal, technical, business process, and audit professional associations – from a security architecture perspective.

About the Authors

Mike Jerbic CISSP, PMP

Mike Jerbic is an independent consultant who specializes in high technology engineering and project management. With over 20 years' experience in hardware and software product development, engineering management, and IT project management, Mike's interest area is in solving complex, multi-faceted problems that require a varied background and experience to solve, such as the control of electronic chattel paper.

Mike chairs The Open Group Security Forum and is a member of the American Bar Association's Business Law Section and many other technical professional associations. He holds bachelors and masters degrees in Electrical Engineering, with emphasis on controls and systems, from the University of California at Berkeley.

Richard Keck

Richard Keck practices in the area of corporate and business law. He has experience in mergers and acquisitions, commercial transactions, regulated industries, tax, securities, and antitrust. Richard also has extensive experience in telecommunications law and policy, information technology, outsourcing, electronic commerce, intellectual property, privacy, and information security. He has counselled clients in various industries, including telecommunications, cable television, broadband, technology, software, energy, financial services, insurance, airline, manufacturing, distribution, and retail.

A member of the American and Federal Communications bar associations, the State Bar of Georgia and the Law Society of England and Wales (not practicing), Richard is a 1985 cum laude graduate of Harvard Law School and a 1982 graduate of Emory University.

David Satola

David Satola is Senior Counsel in the Finance, Private Sector Development & Infrastructure Unit of the World Bank Legal Department. His work focuses on legal aspects of the enabling environment for ICT infrastructure and services, Internet governance, new technologies (e.g., VoIP), competition regulation involving ICTs, Critical Infrastructure/Network Security, and Alternative Dispute Resolution. His project work at the Bank spans more than 70 countries. He was seconded from the Bank to the UN's Working Group on Internet Governance and acts as the Bank's representative on the Internet Governance Advisory Group to the UN's Internet Governance Forum secretariat as well as to UNCITRAL's Working Group on e-Commerce. He is co-Chair of the Subcommittee on Computing Infrastructure, Storage, and Connectivity and the Internet Governance Task Force of the Cyberspace Law Committee of the Business Law Section of the American Bar Association. David has published articles, chapters, and books on legal aspects of ICT reforms.

David received his BA and MA from the Johns Hopkins University, his JD from the University of Wisconsin, and also studied at the London School of Economics and the Hague Academy of International Law.

About The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow™ will enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group works with customers, suppliers, consortia, and other standards bodies. Its role is to capture, understand, and address current and emerging requirements, establish policies, and share best practices; to facilitate interoperability, develop consensus, and evolve and integrate specifications and Open Source technologies; to offer a comprehensive set of services to enhance the operational efficiency of consortia; and to operate the industry's premier certification service, including UNIX® system certification. Further information on The Open Group can be found at www.opengroup.org.

About the American Bar Association, ABA Section of Business Law & the Committee on Cyberspace Law

The American Bar Association (ABA) is the largest voluntary professional association in the world. With more than 400,000 members, the ABA provides law school accreditation, continuing legal education, information about the law, programs to assist lawyers and judges in their work, and initiatives to improve the legal system for the public. The mission of the American Bar Association is to be the national representative of the legal profession, serving the public and the profession by promoting justice, professional excellence, and respect for the law. Further information is available at www.abanet.org.

The ABA Section of Business Law serves the public, the profession, and its nearly 60,000 members by furthering the development and improvement of business law, educating Section members in business law and related professional responsibilities, and helping Section members serve their clients competently, efficiently, and professionally. The Section, through its committees, often provides comment on policy to Congress and government agencies. It supports a robust offering of CLE in all aspects of business law and publishes a library offering over 100 titles in addition to The Business Lawyer, the nation's premier journal of business law. The Section is devoted to promoting full and equal participation in Section activities and in the practice of business law by minorities, women, and persons with disabilities. Further information is available at www.ababusinesslaw.org.

One of the fastest growing Committees in the Business Law Section – the Committee on Cyberspace Law – provides a forum for analysis of corporate, transactional, and regulatory issues related to the Internet and digital technologies. The Committee works in a wide range of legal disciplines including electronic commerce, communications, contracts, consumer protection, intellectual property, cybersecurity and privacy, jurisdiction, Internet governance, electronic assets, and online financial activities. The Committee seeks to identify and address legal, business, and consumer issues affected by the implementation of emerging technologies and to facilitate the creation of legal infrastructures that protect and support electronic commerce. The Committee provides practical tools and guidance both for practitioners who regularly deal with cyberlaw issues and for those who encounter them only occasionally. Further information is available at www.abanet.org/dch/committee.cfm.