

Information Security Assurance for Executives

**An International Business Commentary on the
2002 OECD Guidelines for the Security of Networks and
Information Systems: Towards a Culture of Security**

October 7, 2003

Contents

PART 1: EXECUTIVE SUMMARY	3
Introduction	3
Meeting the Requirements of Information Assurance	3
Information Assurance Checklist	3
Foundation Principles	3
Social Principles	3
Security Lifecycle Principles	3
PART II: BACKGROUND AND OBJECTIVES	5
Why develop this paper?	5
PART III: TOWARDS A CULTURE OF SECURITY	6
OECD Guidelines for the Security of Information Systems and Networks	6
Foundation Principles	6
Social Principles	6
Security Lifecycle Principles	6
The Role of Business in a Culture of Security	7
How Business can Benefit From the Guidelines	7
Appropriate to Role, Sector and Size	9
Global Interdependencies – Cooperation with Other Stakeholders	9
PART IV: SECURITY ASSURANCE CHECKLIST	11
Structure and Checklist	11
Foundation Principles	11
Social Principles	11
Security Lifecycle Principles	11
Foundation Principles	12
Awareness	12
Responsibility	14
Response	15
Social Principles	17
Security Lifecycle Principles	18
Risk and Risk Assessment	18
Security Design and Implementation	19
Security Management	21
Reassessment	22
CONCLUSION	24

Part 1: Executive Summary

Introduction

All business is a matter of trust. Trust can only develop where the participants in a transaction feel secure. Security from a business perspective must therefore be seen as a business enabler, not as a cost. This paper considers how the OECD Guidelines for the Security of Information Systems and Networks can be used to help businesses develop a culture of security within their own organization, with partners and with customers.

Meeting the Requirements of Information Assurance

This paper presents an information assurance checklist, based around the nine principles of the OECD Information Security Guidelines. With the use of selected examples it seeks to demonstrate to businesses how the requirements of this checklist might be met.

Information Assurance Checklist

The nine OECD principles are arranged into three categories, as follows:

Foundation Principles

1. Awareness
2. Responsibility
3. Response

Social Principles

4. Ethics
5. Democracy

Security Lifecycle Principles

6. Risk assessment
7. Security design and implementation
8. Security management
9. Reassessment

The business checklist is as follows:

1. *Awareness*
 - 1.1 Do you have written information security policies that everyone knows and understands?
 - 1.2 Are your personnel security aware and security educated?
 - 1.3 What do you do to raise security awareness across your partners, suppliers and users¹?

¹ The term "users" includes both on and off-line customers as well as visitors to a website.

2. *Responsibility*

- 2.1 Do you have an information security function (person or group) that reports to senior management, such as the Board or executive committee?
- 2.2 Is your security function empowered and resourced to take appropriate steps to manage security?
- 2.3 Are your employees aware of their responsibilities to help maintain security?

3. *Response*

- 3.1 Are there procedures for responding to and learning from security incidents?
- 3.2 Do you have a clear business continuity plan that is understood and tested regularly?

4&5. *Ethics and Democracy*

- 4.1 Are you aware of the legislation, regulation and customer expectations that may impact your corporate information security practices?
- 4.2 Do you provide guidance to your employees related to appropriate use of corporate resources and information?
- 4.3 Have you developed processes to and specified the employees that will handle requests for information from government agencies or that result from legal process?

6. *Risk Assessment*

- 6.1 Can you identify all the information assets that are critical to your business?
- 6.2 Can you identify the threats to those critical assets and do you know their vulnerabilities?
- 6.3 In light of your business needs and risk assessment have you undertaken a cost benefit analysis of your security plan and determined what may be acceptable risk?

7. *Security Design and Implementation*

- 7.1 Does your security plan address the risks identified in your risk analysis?
- 7.2 Is information security included as part of the requirements in the design of all new systems and upgrades to existing ones?
- 7.3 Are relevant security issues appropriately addressed in all your third party contracts?
- 7.4 Do you have clear change control procedures in place?

8. *Security Management*

- 8.1 Do you have clear procedures for controlling physical, system and application access?
- 8.2 Do you have clear procedures to monitor the operation of your policies, procedures and practices?
- 8.3 Do you have clear procedures for backing up data and maintaining and updating software and infrastructure?
- 8.4 Do you have clear procedures to prevent introduction of malicious code and viruses?

9. *Reassessment*

- 9.1 Do you regularly audit your information security and act on the results of the audits?
- 9.2 After a security incident do you identify and, where needed, correct the issue(s) that led to the incident?

Part II: Background and Objectives

Why develop this paper?

Information Security Assurance for Executives has been produced to raise awareness within the business community of the broad range of information security risks related to the use of the Internet and e-commerce, and of the solutions, measures, practices and policies that can help minimize those risks. Because e-commerce is global in scope and depends on network interconnectivity between large and small businesses as well as end users, it has changed the nature of the boundaries between businesses, partners and customers. The security of networks must now be a holistic endeavor that encompasses all participants in the digital economy.

Through its use of the Internet and e-commerce, business has a leading role in addressing these issues; but must also work cooperatively with other participants to develop a global culture of security. Business must also be aware of the increasing legal and regulatory requirements that are being developed to govern the use of the Internet and e-commerce. These are not dealt with in depth in *Information Security Assurance for Executives*, however, it is important for businesses to make themselves familiar with the specific regulations and laws that may apply to their business sector, the types of transactions in which they engage and the jurisdictions in which they operate.

The importance and awareness of security have greatly increased since the terrorist attacks of September 11, 2001. There is a heightened level of security at airports, borders and elsewhere. However, the increased level of security awareness and concern at the broad societal level is only beginning to manifest itself in relation to the Internet. The main public concerns on the Internet remain centred around privacy and the security of personal information. There is less awareness about the broad range of risks that systems and networks may be subject to, or about potential cyber attacks that can be generated from failure to properly secure computers. There is even less awareness of protective steps, both proactive and reactive, that can be taken to minimize these risks.

Many large businesses have been aware of and dealing directly with security issues for some time. Viruses, distributed denial of service attacks and the potential, both external and internal, for system and network compromise have been topics of concern for businesses with IT departments for several years.

Information Security Assurance for Executives is not a blueprint for IT security. Rather, it informs business executives and small to medium enterprises (SMEs) so that they are better able to ask the right questions of IT professionals. The level and type of security deployed will ultimately be a decision that affects businesses in terms of cost, architecture, resources and business optimization. This document provides some of the security context that can help inform these decisions.

Part III: Towards a Culture of Security

OECD Guidelines for the Security of Information Systems and Networks

On 25 July 2002, the OECD Council adopted the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (“the Guidelines”)². The Guidelines consist of nine principles that comprise a framework for considering security issues. The principles are both brief and basic in their phrasing to increase their accessibility to all participants. *Information Security Assurance for Executives* elaborates on those principles to increase their relevance and tailor their applicability to the business community.

The Guidelines address the evolving risks and greater interconnectivity of a networked economy. These new circumstances have also broadened the scope of applicability of the Guidelines. Until relatively recently, IT security was a specialist discipline that seldom came to the attention of anyone in business or government aside from IT professionals. World events in the intervening period; from virus attacks that can disrupt business to issues related to physical security, have placed security among the top concerns of business, government and civil society. This changing attitude to security is reflected in the new subtitle of the Guidelines, “***towards a culture of security***”, and the fact that they are directed to ALL participants, as appropriate to their roles.

The nine principles in the Guidelines can be considered in three main categories as follows:

Foundation Principles

- Awareness
- Responsibility
- Response

Social Principles

- Ethics
- Democracy

Security Lifecycle Principles

- Risk assessment
- Security design and implementation
- Security management
- Reassessment.

The foundation principles focus on the need to be aware of risks, the need to take responsible action related to those risks and the need to coordinate that action in timely response. The social principles address issues related to behavior, fairness, openness,

² <http://www.oecd.org/pdf/M00034000/M00034292.pdf>

The 2002 Guidelines are an update of the OECD Security Guidelines first issued in 1992.

transparency and values. The last four are more operational in nature and address the 'security lifecycle'. They focus on the need to:

- Identify and evaluate risks.
- Design and implement systems and solutions appropriate to the required mitigation of the risks.
- Develop the policies, processes and procedures needed to manage these systems and solutions.
- Review risks, systems, solutions, policies, procedures and processes in light of new risks, new technologies, incidents and the normal lifecycle of systems.

The Role of Business in a Culture of Security

All parties have a role to play in a culture of security, but business, as the principal innovator, developer, user and provider of Information and Communication Technologies (ICT), has a broader role than most. Business can be a developer, implementer and user of security technology, practices and policies, as is stated in Principle 7 of the Guidelines:

“Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.”

Business can help to ensure that security is designed into products, can help promote the use of secure technology, can provide information and assistance in the secure configuration and implementation of technology, and can help raise awareness of its customers about the importance of security and steps they can take to develop a culture of security.

How Business can Benefit From the Guidelines

While these are voluntary Guidelines, promulgated by an intergovernmental institution, they were developed in partnership with, and are addressed to, all segments of business and society. Their core message – security is now an integral part of everyone's civic responsibility – has far-reaching implications for business, which is uniquely positioned regarding security. Business is the predominant owner and operator of the information systems and networks that comprise the networked economy. Business has the greatest operational control over the current and future security of those systems and networks, and is the prime developer and originator of security solutions, measures, practices and policies. The international business community should view this responsibility as a confirmation of the importance of security as both an existing and evolving business imperative and enabler.

The concept of a culture of security encompasses the notion of what is appropriate to the role of individual participants and situations. While children at school are taught about crossing streets, we also employ crossing guards and have designated places where crossing is more secure. Similarly, security in the school, home and workplace needs to be appropriate to the task. While many security concepts and policy issues appear to be relevant only at the enterprise level, they apply at the home office and to Small and Medium-sized Enterprises (SMEs) as well. The culture of security needs to result in an intuitive behavior and reaction. Tools such as virus checkers are only useful if used and updated. Passwords and other authenticating procedures will only be effective if kept secret. These concepts should become as reflexive and common-sense as looking both ways before crossing the road.

From a business perspective, the most important role of the Guidelines is that they complement, and in a sense complete, an existing hierarchy of business policies, practices and processes in the field of ICT security. By providing an overarching set of general principles, the Guidelines link the existing business framework into a larger societal context. They also link to the increasingly strict regulatory and legal frameworks in which businesses are operating globally. Such frameworks, such as the work by the Bank of International Settlements (Basel II) on the control of operational risk in the finance sector, require businesses more and more to conduct their operations in a securely managed way. The following table shows how the Basel II requirements can map to the Guidelines:

OECD Information Security Guidelines and Basel II Operational Risk Controls.

Basel II Operational Risk Principles	OECD Guidelines
1. Directors must define an operational risk management framework.	Principle 1.
2. There must be an internal audit of the operational risk management framework.	Principle 8.
3. Responsibility for the operational risk framework must rest with senior management.	Principle 2. Principle 7.
4. There must be an operational risk assessment for all new systems.	Principle 6.
5. There must be regular monitoring of operational risk and mechanism for reporting to Board.	Principle 9.
6. There must be periodic review of, and adjustment to, the operational risk management strategy	Principle 9.
7. Contingency and business continuity plans must be in place.	Principle 3.
8. There must be a framework to identify, assess, monitor and control/mitigate material operational risks.	Principle 8.
9. There must be independent, external evaluation of operational risk-related policies, procedures and practices.	Principle 5.
10. Sufficient public disclosure to allow assessment of operational risk control mechanisms.	Principle 4. Principle 5.

Businesses large and small have a variety of security needs, resources and abilities. There is no one-size-fits-all solution, often even within a single enterprise. The security requirements for mission-critical applications differ from those for more routine applications, yet all are related and must be treated as such.

Business should be able to use the Guidelines and this commentary to:

- Provide a context for executives to understand the business implications of security both across the enterprise and in society more broadly
- Provide high-level resources that they can use to ensure that their companies continue to live up to the expectations of their shareholders, customers, employees, regulatory authorities and the general public
- Raise awareness concerning security among those businesses that have no ICT professionals on staff or retainer or are only recent entrants in e-commerce
- Help business understand what roles they can play in helping to define and develop a culture of security.

In preparing this commentary, the ICC and BIAC, on behalf of the global business community, hope to make a contribution to the dissemination and implementation of the Guidelines. This is intended to be a living document and will be updated as needed to reflect changing circumstances and evolving security imperatives.

Appropriate to Role, Sector and Size

A business's efforts to reinforce a culture of security both within its own organization and with its partners and customers must be appropriate to its role, sector and size. Influencing factors include the:

- Nature of the business
- Nature of the information being secured
- Size and type of its infrastructure
- Extent to which external parties can access the organization's information assets and infrastructure
- Number of users
- Level of control over the design, development, configuration and operation of ICT-related components
- Knowledge of legal/regulatory security obligations and methods of compliance
- Numbers of security incidents recorded.

The level of security necessary is directly related to the risks identified within the business and the cost of security breaches to the business. Within typical commercial environments, the effort required to manage such risks should be proportionate to the value of the information and size of the organization. Some business environments may require specialist controls, and greater levels of investment by businesses in that sector. Cost benefit decisions may of course also be influenced by regulatory requirements or applicable laws.

Those who develop and implement systems and networks, the software that runs them and the hardware they run on, have a vital role to play. Security needs to be built into the development of product or process, not bolted on as a feature. Part of this role includes providing information on the security functionality of products so that users can understand it.

The concepts and guidance embodied in this paper are meant to address all businesses from large global enterprises to SMEs, but those companies with little experience in electronic commerce, technology and security may still have trouble identifying with the paper. In the resources that will accompany the online version of this paper we will provide references that are more specifically tailored for SMEs and hope that these resources help to put the guidance provided by this paper into a clearer context.

Global Interdependencies – Cooperation with Other Stakeholders

One defining feature of today's environment is that all parties depend on each other's security assurances. The rapid integration of national economies into a global marketplace and the intrinsically borderless nature of the Internet mean that every security flaw has the potential to expose many, if not every, participant in the global marketplace to risk. It is therefore in business' interest to raise security awareness, both because of global

connectedness and because security is the essential building block in the development of trust and confidence in on-line transactions.

Business must also engage in appropriate coordination with outreach conducted by governments, intergovernmental organizations (such as the OECD) and consumer and civil-society organizations. Business recognizes the interdependency of these groups, and is keen to play its proper part in a cooperative global move towards a culture of security. BIAC, the ICC and other business organizations stand ready to organize, participate or otherwise facilitate such cooperation as necessary.

Business should also work in conjunction with governments on the creation of a culture of security. Cooperation may range from voluntary sharing of appropriate information about security incidents, to working cooperatively to address issues of cybercrime and to raising public and industry awareness about the importance of security. It is obviously difficult for those companies who create technology that addresses security from being considered unbiased in promoting the benefits of security. Government can help promote the benefits of security as both an unbiased commentator on the general importance of security and by setting an example by highlighting its strong commitment to the importance of security in its deployment of government to citizen, government to business, and back-end services and technology.

Business should also work with individual end users to better understand whether they are providing appropriate and understandable information on the utility and functionality of the security features in their products. Business should continue to try to make the security functionality of consumer and end user products as easy to configure and maintain as possible.

Part IV: Security Assurance Checklist

Structure and Checklist

The nine OECD principles are as follows:

Foundation Principles

1. Awareness
2. Responsibility
3. Response

Social Principles

4. Ethics
5. Democracy

Security Lifecycle Principles

6. Risk assessment
7. Security design and implementation
8. Security management
9. Reassessment

The business checklist is as follows:

1. *Awareness*
 - 1.1 Do you have written information security policies that everyone knows and understands?
 - 1.2 Are your personnel security aware and security educated?
 - 1.3 What do you do to raise security awareness across your partners, suppliers and users³?
2. *Responsibility*
 - 2.1 Do you have an information security function (person or group) that reports to senior management, such as the Board or executive committee?
 - 2.2 Is your security function empowered and resourced to take appropriate steps to manage security?
 - 2.3 Are your employees aware of their responsibilities to help maintain security?
3. *Response*
 - 3.1 Are there procedures for responding to and learning from security incidents?
 - 3.2 Do you have a clear business continuity plan that is understood and tested regularly?
- 4&5. *Ethics and Democracy*
 - 4.1 Are you aware of the legislation, regulation and customer expectations that may impact your corporate information security practices?

³ The term “users” includes both on and off-line customers as well as visitors to a website.

- 4.2 Do you provide guidance to your employees related to appropriate use of corporate resources and information?
- 4.3 Have you developed processes to and specified the employees that will handle requests for information from government agencies or that result from legal process?

6. *Risk Assessment*

- 6.1 Can you identify all the information assets that are critical to your business?
- 6.2 Can you identify the threats to those critical assets and do you know their vulnerabilities?
- 6.3 In light of your business needs and risk assessment have you undertaken a cost benefit analysis of your security plan and determined what may be acceptable risk?

7. *Security Design and Implementation*

- 7.1 Does your security plan address the risks identified in your risk analysis?
- 7.2 Is information security included as part of the requirements in the design of all new systems and upgrades to existing ones?
- 7.3 Are relevant security issues appropriately addressed in all your third party contracts?
- 7.4 Do you have clear change control procedures in place?

8. *Security Management*

- 8.1 Do you have clear procedures for controlling physical, system and application access?
- 8.2 Do you have clear procedures to monitor the operation of your policies, procedures and practices?
- 8.3 Do you have clear procedures for backing up data and maintaining and updating software and infrastructure?
- 8.4 Do you have clear procedures to prevent introduction of malicious code and viruses?

9. *Reassessment*

- 9.1 Do you regularly audit your information security and act on the results of the audits?
- 9.2 After a security incident do you identify and, where needed, correct the issue(s) that led to the incident?

The remainder of this section contains suggestions for implementing the requirements of the checklist, together with examples drawn from actual businesses. The section is structured to reflect the checklist above.

Foundation Principles

Below the three foundation principles are examined in more detail.

Awareness

This consideration of security awareness looks at the principle in terms of general personnel issues and of security awareness and education.

General Personnel Issues

While specific security configurations and network architecture may need to be kept secret, a culture of security will only be created within a company and in the larger society if awareness raising and education campaigns are put in place. Security as a company priority

needs to be highlighted at the highest levels of the company and needs to become ingrained in the corporate ethos across all levels of the company. This requires top-down leadership and bottom-up participation.

The need for security should be identified clearly at the recruitment stage, and reinforced by training for as long as the employment continues. Potential recruits, not only for sensitive positions of trust but all those who have access to networked systems, should be adequately screened. Companies might find that local data protection regulations limit ready access to security information. With appropriate notice, purpose and use limitations, much of the information that is beneficial to security evaluation and investigation may be obtained within the context of applicable legislation. As a minimum, checks should be made to verify the identity of prospective employees and to ensure that they have not lied about their qualifications or previous employment history. It is also important to ensure that similar checks are carried out on contract staff.

Businesses must work with their employees to develop a co-operative approach to security. Employment agreements and contracts with relevant third parties should include appropriate confidentiality (non-disclosure) obligations and requirements for the application of security standards that match those within the organization that is placing the contract.

‘Social engineering’ or ‘people hacking’ techniques are used more commonly than technology-based methods to circumvent an organization’s security. The ability to breach security in this manner is often the most insidious and hard to discover, as the source is often an overly helpful employee who unknowingly passes system-critical information to a hacker posing as a systems engineer. Businesses should therefore develop and provide appropriate training on potential ways that employees may be tricked into compromising security. Awareness-raising through periodic training and appropriate standards for what information staff should or should not provide to a caller can help address these issues. Managers should likewise be trained to notice unusual employee behavior or system use that may be telltale signs of security breaches or other suspicious actions. Box 1 outlines some typical social engineering incidents.

Box 1: Social Engineering Tactics

Outsiders using remote connections to pose as system support employees can be one of the greatest threats especially among administrative staff. These efforts can seem more credible when the calls or e-mails seem to originate from within a company. It is easier to get employees to rely on calls or e-mails that appear to be internal or from a trusted source. Emails can easily be spoofed in terms of originating address and calls that are transferred internally or made from an extension in a reception area may all appear to be internal. Compromises can occur more easily in such situations if employees are not trained or if established security processes don’t exist. Callers intent on breaking in may ask to verify passwords or settings that will assist in the compromise of the system. The less familiar employees are with technology and system operation the less they are able to discern the veracity or appropriateness of such requests.

Internal solutions can include better training as well as standard templates and originating address for corporate security e-mails and the need to call back selected security numbers to verify requests for login or setting information. Neither of these is foolproof, however, and proves the need for continued training and vigilance. A recent virus was transmitted by a hacker that imitated the look and a feel of a real software company’s Security Alert and another fraudster e-mailed a major banks’ customers and asked them to provide information on a spoofed site. In both cases visits to the actual “company”.com website would have clarified the issue.

Security Awareness and Education

All people involved in the organization should understand their roles and responsibilities in relation to security assurance, as well as those of the people they deal with. All employees should receive mandatory security training and education at a level, and with a frequency, that is appropriate in terms of their role, business need and type of information accessed. Awareness-raising and education should be pursued throughout an organization's zone of influence; including suppliers, contractors and customers. Issues to be addressed in education, training and awareness include the following:

- Security requirements
- The origin and nature of threats and vulnerabilities
- Common attacks and breaches
- Correct usage and interpretation of credentials (including digital credentials), authorizations and permissions
- Incident response
- Consequences of breach
- Legal responsibilities (including respect for personal data and intellectual property)

This training should not only cover the appropriate policies and procedures, but highlight the importance that the company places on security, the employee's role in helping keep the company secure and, where appropriate, what the employee can do help customers, partners and suppliers better understand their roles in security. The consequences of security violations must also be clearly dealt with; this is particularly important in the context of employment legislation.

Responsibility

Responsibility is considered in terms of the need for senior management involvement and the establishment of a security policy, backed from the top of the organisation.

Management Involvement

Security assurance requires clear instructions from the top. However, management should effectively incorporate input from all levels of the organization. Over time security has become a concern at all company levels from the Board of Directors to the temporary worker. The roles and responsibilities they assume in the business vary considerably and there is no magic formula for allocation of responsibility. For some organizations, a security committee may be appropriate; for others, a chief security officer or perhaps a distributed responsibility across a number of key executives. It is important that the business develops a method in keeping with its organizational structure, resources and risk analysis. Companies need to develop processes and mechanisms that allow them to evaluate security performance, appropriately delegate decision-making related to security, and periodically reassess the company's security analysis and performance in light of changing risks, new technology and critical business functions.

Security Policy

As a basis for an organizational culture of security, management should set a clear direction and demonstrate commitment to security. Part of this commitment includes working with appropriate personnel to develop and maintain a security policy that covers the whole

organization. The policy should address all aspects of security in the organization, and should have an 'owner' (whether a group or individual), properly empowered and resourced, who will be responsible for its maintenance and appropriate review according to a defined process. It is important that the basic security policy statement is short, clear and endorsed from the top of the organization. It must be seen, read and understood by all employees and agents of the Organization. The consequences of non-compliance must also be made clear.

Security and security policies go beyond the traditional concepts of physical defenses, firewalls, anti-virus software and passwords. Security policies may include other policies or an aspect of policies, including personnel polices, access-control policies, media control and disposal policies, disaster recovery and business continuity policies and others. The size and scope of a business enterprise will increase the complexity of some of these policies, but all businesses, regardless of size, must think of security holistically and across disciplines and job functions.

The security rules, founded on the basis of a policy that is clearly endorsed by the top management, are supplemented by more detailed procedural documents at various organizational levels. All those specific procedures are needed to ensure effective policies. The interoperation of these rules and the procedural documents is necessary to ensure a coherent approach across the organization. All of these essential steps related to these polices must be communicated to be effective, Box 2 gives an example of this.

Box 2: Security and Training – Communicating Responsibility

Security and related polices are often drafted by security, policy or legal experts. While great efforts are taken to simplify the form and content of these polices, the mere dissemination of the policy may not be sufficient to appropriately modify existing practices. Training tailored to the content and the audience must also be developed to assure that the skills, habits and practices become ingrained in your employees. The training also helps communicate the corporate value placed on education and the expectation that all employees have a role in the company's successful implementation of the polices.

Education can be developed internally, or provided by outside experts. Training can be off line, online or a combination of both depending on the needs and resources of the company. Training should be provided upon employment and periodically thereafter. Training should also be supplemented by corporate messages that reinforce the importance and relevance of the training as well as serve to update issues and policy guidance as needed. The training courses themselves should be updated to provide both the most up-to-date policy guidance as well as timely examples.

Training is often considered most effective when it provides both theory and examples of practical application. The more closely tied to your company/sector the examples, the more relevant it becomes to employees. Training may also contain evaluative sections, this provides an ability to gauge how well the employee has understood the training and may highlight places where the training should be strengthened or clarified.

Response

The response principle is discussed in relation to issues involving incident handling and response, cooperation and sharing data, and business continuity and disaster recovery.

Incident Handling and Response

Incidents affecting security should be reported quickly through appropriate management channels. All employees and contractors should be made aware of the procedures for reporting the different types of incident (security breach, threat, weakness, malfunction or issue related to a policy) that might have a security impact. Incident management responsibilities and procedures should be established to ensure a quick, effective and orderly response to security incidents.

Procedures must be taught to all appropriate employees and regularly rehearsed to ensure that all concerned are familiar with what they have to do in an incident. Regular rehearsal will also expose weaknesses in the system, and allow lessons to be learned and improvements to be made. An important aspect of incident handling is to have in place a system for capturing details of any incidents that take place. A mechanism should also be in place to ensure that these details are fully analyzed, and that appropriate remedial action is taken.

Incident handling often requires a cross-functional approach that may involve representatives from technology, legal, policy, human resources and public relations departments. Incident handling should be coordinated by those responsible for security compliance, reporting to the highest level of the organization.

The number of people involved in dealing with an incident will depend on the nature of the business and the type of incident. Where technical proficiency exists within the organization, different approaches to security incidents may be developed. In all cases, security breaches, attempted hacks, etc., must be contained. However, in some cases, the incident may be allowed to proceed under control, to allow security personnel to gather information for forensic or investigative purposes.

There may also be instances when law enforcement authorities are alerted to assist in the investigation or develop a case for prosecution. All employees should be made aware of the names and contact details of those to be informed in the case of a security incident.

Cooperation and Data Sharing

Businesses should also consider whether and what types of information they may wish to share with other businesses, emergency response centers and government bodies, and under what circumstances such sharing should take place. Providing too much information, or information before some remedial steps are in place, may potentially expose the company, and possibly its partners and customers, to the risk of more significant breaches. Information sharing and media communications, where appropriate, should be through designated employees according to defined procedures.

Issues surrounding the anonymization and aggregation of security incident data also need to be addressed. The ability to spot trends in attacks is greatly facilitated by quick and broad dissemination of such data. There are numerous mechanisms whereby this can be collected, assessed and disseminated as information. Business must evaluate the various types of sharing and reporting mechanisms, as well as the level of specificity and identification required to determine what level of participation might be appropriate.

Business Continuity and Disaster Recovery

One aspect of incident handling and response should be business continuity and disaster recovery planning. Business continuity generally operates at a lower level than disaster recovery, and implies the existence of 'work around' mechanisms that allow a company to continue to operate in the event of a non-catastrophic failure. Disaster recovery implies the

existence of procedures and infrastructure necessary to maintain the business in case of catastrophic events. As such, it will entail issues of logistics, power supply, communications, redundancy (e.g., back-up data centres), location of assets, distribution of workforce and knowledge of the status and location of assets and workers in time of crisis. A decision to employ business continuity or full disaster recovery will depend on the nature of the business and the individual business risk assessment. An example of how incidents can be assessed to trigger the activation of a business continuity plan is shown in Box 3. This is taken from an actual Business Continuity Plan (BCP).

Box 3: Triggering a BCP

In the event of a security incident, the duty operations supervisor should ‘triage’ the severity of the incident. The triage criteria are as follows:

An incident that will be handled by the high-availability systems, causing transient (less than 2 minutes) disruption to customer service.

An incident that will cause disruption that can be solved either by the high-availability systems, or by immediate action within the building, within 20 minutes.

An incident that is likely to cause disruption that is unlikely to be resolved within 20 minutes.

A security incident is defined as: “any detected action or inaction which results in loss of information or damage to its confidentiality, integrity or availability. Or which tends to increase risk either permanently or temporarily.”

Social Principles

Ethics

As organizations’ ICT systems become more integrated, each organization’s information security policies and practices impact and can result in damage to others. Providing an appropriate level of information security is part of every business’ civic responsibility. Compliance with relevant information security best practices will help organizations to meet their national and international legal and regulatory obligations. When developing and implementing security policies, practices and procedures businesses should be aware of the legislation and regulation and reasonable customer expectations that may impact such policy, practices and procedures and adjust them accordingly.

Businesses must also make employees aware of what activities may be undertaken using corporate resources through appropriate acceptable use policies and training. Businesses should seek to make sure that these policies are not only in keeping with the letter of the law, but also the spirit of the company’s corporate values and code of ethical behavior. In a number of cases, companies have been able to use such responsible behavior as a way to further establish customer trust and beneficial brand reputation.

Democracy

Security is a key requirement for ensuring and conveying an appropriate level of trust in an organization. The Guidelines recognize though that security is part of a larger pool of societal values, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection

of personal information, openness and transparency. Accordingly, businesses must work to ensure that their security policies, practices and procedures are compatible with the larger pool of values and other internal policies relating to customers and employees. This includes accommodating the legitimate interests of others, such as protecting sensitive business information, personally identifiable information about customers and employees, and intellectual property. Good security is predicated on businesses identifying and appropriately protecting business-critical and sensitive information assets. Businesses may need to deploy certain internal monitoring systems to assure such security. To ensure corporate-wide compliance with the security policy, practices and procedures that are compatible with the larger pool of values, businesses should provide guidance to employees on the appropriate use of corporate resources and information and clearly detail the potential sanctions for misuse. All of this should limit as much as possible restrictions on information flows.

As noted, security is one of the elements required in developing customer trust, as are openness and transparency. Companies must strive to determine what aspects of their security practices and processes they may disclose in order to maximize trust without compromising security. In these matters, general explanations in accessible language may be more preferable than detailed statements.

Security Lifecycle Principles

Risk and Risk Assessment

Decisions related to risk and its mitigation should involve senior management. It is important that risks specific to the business are identified, prioritized and an action plan agreed. The essence of this action plan will contribute to the security policy. ICT-related risks must be integrated into the overall corporate risk assessment in order to ensure that the appropriate priority is given to them. Mitigation of such risks may be through legal (contractual), insurance, procedural or technical means. Or the risk may simply be accepted. Whatever the decision, it should be recorded and agreed by senior management and periodically reviewed together with the action plan.

Among the questions that need to be considered by a risk assessment are:

- What are the risks to the company?
- What can be done to minimize risk?
- What risks may be acceptable?
- What risks may be unavoidable?
- Is the potential for certain risks sufficiently small, or is the harm that could result so attenuated, that the risks don't justify the costs of countermeasures?

It is important to remember that only those who understand the business and its circumstances can determine the proper responses to questions such as those posed above.

Carrying out a risk assessment involves consideration of three sets of factors. The first is how critical the information is to the business, and the impact should it be lost, damaged or exposed. This will depend on the nature and type of the business. The second includes the vulnerability of the business and its systems to exposure. This will largely depend on issues such as remote connectivity and use of the Internet. The third involves an assessment of the threat to the business; again this will depend on the type of business. For example a high profile retail company might be the object of a much higher threat of website defacing or denial of service attack than a B2B company might be. The threat assessment should

consider issues such as the number of contractors used and any partners with which the organization is networked. When assessing security risks, companies must also factor in the negative publicity that can result from security issues.

Risk analysis must occur on multiple levels that are then compared to understand the potential effects on the company. Thus it is not sufficient to identify possible threats such as a virus, hack attempt of defacing of a website without also analyzing the impact on business operations. Defacing of a website, for instance, has a greater business impact on an ISP than it may on businesses less related to technology. It is that combination of potential threats, possible outcomes and likely effects that allows companies to determine the true risk environment. An example of some of the general threats to business operation that may need to be considered are given in Box 4, the examples are taken from an actual risk assessment.

Box 4: Examples of Threats

The events likely to threaten normal operation of the system are identified in the Risk Assessment as follows:

1. Evacuation of Building
2. Non-Availability of Staff
3. Destruction of SOC
4. Connectivity Failures
5. Software Failures
6. Power Outages
7. Hardware Failures.

Security Design and Implementation

Information security assurance should be an integral component of ICT solutions and should be pursued in a holistic manner. Organizations involved in the design, development, configuration or operation of ICT-related components should always build in security that is appropriate to needs and circumstances. Consideration of needs will always include balancing issues of costs and benefits. Such an assessment should be included as part of the overall risk assessment and management plan. This section looks at the design and implementation of security in terms of the importance of designing-in security, at implementing appropriate technological solutions, and at the use of best practices and standards.

Designed-in Security

Security is best achieved when built-in as part of the product or system development process, not bolted on as an afterthought. The level of security that will be designed into a product is often related to its anticipated uses. Users should take this into consideration when selecting and implementing products. Users should also be aware of information provided by developers and manufactures about appropriate use of products. They should also consider any third-party reviews of the security of products, as well as the type and level of any security certifications the products may have achieved.

Security should be an important consideration in the procurement of all ICT-related products and services. Selection of products and services should be based on pre-established requirements, consistent with an organization's security requirements and policy. An open

Request for Proposal (RFP) process is an effective mechanism for ensuring a sufficient understanding of the strengths and weakness of products and services.

Implementing Appropriate Solutions

There is no such thing as off-the-shelf security. Very high-level security that is very slow in operation will not be appropriate for a business that deals in heavy volumes of real-time transactions. The needs of the business model, importance of the information, and likely vulnerability to threats will all be factors in determining which features provide the greatest value to the company and what constitutes appropriate security.

Each organization has unique vulnerabilities, imperatives and options requiring an individual security approach. There are many off-the-shelf solutions that may be applicable to a number of security needs, especially for SMEs, but the technology has to be part of the development of a corporate approach to security. There must be appropriate operational and organizational policies, standards and procedures that work with the deployed technology to constitute the information security policy. Technology that is relevant to security can range from tested and hardened mission-critical applications, high-level cryptography, intrusion-detection systems and firewalls, to desktop virus software, secure socket layer (SSL) connections and physical locks for laptops.

While costs will be a factor, a culture of security must result in a heightened priority for security planning and management as well as an understanding of the need for security among all participants. Security is too often traded off against notions of increased cost and decreased convenience. Security should be one of the motivating decision criteria in purchases, and a priority in the deployment and use of systems and networks. Not all uses and functions need the same security. However, security that is appropriate to the role and function may come at some increased cost in terms of price, time or convenience. Therefore, the cost of increased security, provided it is reasonable and appropriate, should become an accepted part of all information systems.

Use of Best Practices and Standards

While it may be hard to gauge, reference is often made to what is the standard of the particular industry or sector. In some cases, trade or specialist associations may develop best practices. In others it will require some level of consultation and comparative benchmarking with peers.

Third-party evaluations and certifications may also provide external validation of the security aspects of a product and its development process. Similar reviews can be undertaken to assess the operational security of an environment. It should be noted that these certification and evaluation processes may be costly and may not be appropriate for all types of applications or sizes of enterprise. SMEs may also rely on more generic evaluations and comparisons that may appear in the trade press and published reports about types of products and services. All of these factors will need to be considered to determine how they fit with the business requirements of the company.

One selection criterion for security assurance products and services is compliance with commonly accepted industry best practices and standards. However, such compliance is never a guarantee of the product or service fulfilling an organization's individual need and can never replace a proper requirement definition and vendor selection process. However, commonly accepted industry best practices and standards do provide a benchmark for comparison. The international standard for information security management systems (ISO/IEC 17799:2000) provides a general code of practice. Its ten control areas are shown in Box 5.

Box 5: Information Security Management System Control Areas :

1. Security Policy
2. Security Organisation
3. Asset Classification and Control
4. Personnel Security
5. Physical and environmental security
6. Communications and operations policy
7. Access control
8. System development and maintenance
9. Business continuity management
10. Compliance.

Security Management

Security management is considered in this section in terms of the importance of roles and responsibilities and the use of a classification system.

Roles and Responsibilities

A major benefit of the Internet is its ability to make information available in a fluid, less restricted, more user-friendly fashion. However, the greater availability and accessibility of information does not obviate the need for appropriate control of access to information through authentication of users and management of privileges. Security is as much about making sure that only the right people can get access to the information as it is keeping the hackers out.

Everyone in a company has a defined set of responsibilities. Most companies find it efficient to allocate responsibilities in accordance with a designated role or job-title. Most roles require that the employee has access to certain information on a 'need to know' basis. There may be times when access to other information is appropriate, and standards and procedures need to be in place to deal with this. However, it is important that access controls are appropriately managed and kept up to date. By sticking to the 'need to know' principle, any additional access rights will be removed when the requirement for them is no longer present. Only by using such controls will it be possible to effectively track who has access to what information, and create an audit trail that may be used in an investigation following a security breach. Access controls can be automatically established on an information system, based on rules relating to a user's role, circumstances and individual identity.

In many companies employees change jobs and responsibilities on more frequent basis than before. These more dynamic organizational structures create greater possibility for the misalignment of jobs, responsibilities and access privileges. It is important to assure that all of these factors are kept up-to-date to assure that the need to know is appropriately applied to the employee. While it is essential to employ appropriate methods of authentication to validate the employees' credentials when accessing the system, it is equally important to assure that that employee's access rights and privileges are up to date and accurate.

Security management involves a broad management of security issues that span a number of personnel and other polices that are related to security, but would not be considered a security policy. This requires cooperation between a number of departments and a team approach to security. There is no magic formula to developing this kind of cooperation as the company must develop processes and procedures of cooperation that are suitable to its requirements and resources.

Information Classification

A comprehensive approach to the use of 'need to know' must include a system of information classification. The purpose of information classification is to ensure that all the information held by a business is protected in accordance with its sensitivity. An example of a real information security classification system is given in Box 6 below.

Box 6: An Information Classification System

At its simplest, a classification system might consist of four types:

1. Time-sensitive company information (for instance relating to unpublished annual results);
2. Customer details (this will probably be the type of information protected under data protection legislation, where this is in force);
3. General company commercial information (for example relating to a company's competitive position);
4. Public information (such a might be published on a website).

Implementing an information classification system will involve the company in making sure that appropriate restrictions are placed on each type of information. An example would be placing all time-sensitive information on a server behind a firewall that ensures it can be accessed only by employees in the finance department and by senior management. While technology can assist in providing the appropriate controls related to these functions, business needs will drive the classification of information and determination of who has access to it. Where possible, roles and responsibilities should also be clearly segregated to reduce opportunities for abuse of power or authorization.

Reassessment

The management of information security needs the cooperation and participation of all business and IT units, and the legal/compliance functions of the company. This participation is vital, as the operation of the information security system must subject to third-party scrutiny, enabling a more objective reassessment and audit process. This will ensure appropriate separation between those who operate the technology infrastructure and those who enforce the policies.

The continued effectiveness and relevance of security products and services, as well as the security level of all other ICT-related products and services, should be regularly reviewed. Components that do not meet the required level of security should be updated or, if appropriate, replaced. Regular reviews and assessments may be required throughout the lifecycle of security products and services. In many cases, organizations cannot maintain an appropriate level of security without the involvement of a third-party audit, dynamic testing or

monitoring service. All third parties must be appropriately selected, controlled and contractually bound to avoid incorrect use or sharing of confidential, sensitive or proprietary data.

For the larger business there are policy automation and product-based dynamic testing tools available. These can contribute significantly to security assurance and audit process.

Depending on the size and resources of the enterprise, external testing for security vulnerabilities of the operational environment may also be critical, as some security issues may arise in the configuration of a product or the inter-operation of a number of products. Third-party audit and certification of the whole, or part of an organisation's information security management system may also be undertaken. Box 7 gives an example of the advantages of a third-party audited information security management system to business.

Box 7: The Advantages of Third-Party Audits

Many businesses find that third-party audits of their information security management system delivers significant advantages. Amongst these are:

Internal:

- To allow audits to take place, clear processes must be documented.
- An audit trail must be put in place. This ensures that problems and faults are corrected as soon as possible, and that checks are made on actions taken.
- Having an independently audited process allows an organisation to respond more easily to questions about security, when responding to requests for tenders or proposals.

External:

- The process is open to inspection by prospective customers and partners.
- Customers can more easily assure themselves that secure processes are in use.
- There is a third-party assurance of the effectiveness of the security management system used.

Conclusion

Security is neither a one-time process, nor a one-size-fits-all solution. It is a continuous process of change management. Security mechanisms, policies, practices procedures must be responsive to changes as to risks, business imperatives, legal requirements, technology solutions and innovation, and business rules and processes. Security should be both reactive to incidents and proactive in preventing incidents. The greatest benefit that security can provide is that you never need to respond to an incident. It is the hard to measure benefits of avoiding financial loss, negative press and customer dissatisfaction. More recently security is becoming part of a positive trust enhancement perception and brand differentiation that helps to underscore the benefits inherent in security.

Security should no longer be considered to be just the purview of security professionals as it has become a company-wide concern that reaches from the boardroom to the boiler room. This document is meant to be living document that will be revised as needed. While grounded in the principles of the OECD Security Guidelines it is meant to provide context and guidance for business executives who are faced with greater responsibility and accountability for security.

ICC and BIAC welcome further input into this document; including both examples of how companies have implemented some of the principles as well as topics that you feel have not been addressed, or have been addressed in insufficient depth.

After the Oslo conference, this document will be posted on the BIAC and ICC websites supplemented with further practical examples and links to resources and practices related to security in the business environment.