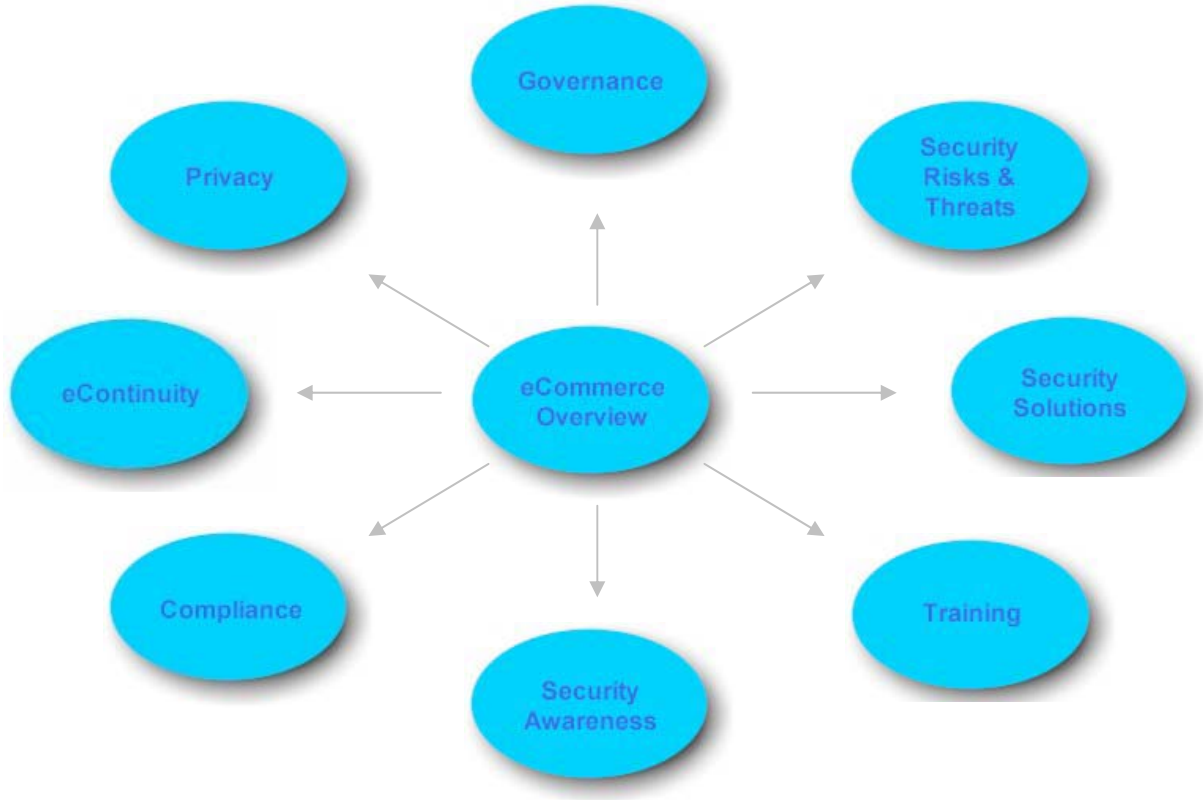
# eCommerce Security

These pages have been designed to provide guidance on eCommerce security and related issues to the members of the UPU and postal administrations.

Eight eCommerce Security themes have been developed and these may be accessed through the links below.




**eCommerce Security Overview**

**Governance**

**Risk and threats**

**Solutions**

**Training**

**Security Awareness**

**Compliance**

**eContinuity**

**Information Privacy**

# eCommerce Security Overview

The delivery of goods purchased over the Internet holds great opportunities for Posts. Some administrations have set up Internet portals that allow access to a number of electronic merchants and provide delivery and payment options. These services may be delivered and managed by in-house resources or through contractual relationships.

These new and faster communications tools have also urged Posts to respond to customer needs for greater security in eCommerce. This offers them opportunities to provide new value-added services based on the trust customers have in the post office. A number of Posts have already established trusted intermediary services and act as certification authorities that guarantee the authenticity of electronic messages for both senders and receivers.



## *Challenges to the Posts*

According to UPU studies conducted in 1997 and 2000, letter volumes worldwide are expected to increase by slightly more than two percent annually through the year 2005.

However, the communications market as a whole, telephone, fax, electronic mail, interactive communication and other forms of eCommerce, continues to progress at a much faster pace than the postal market.

This trend, coupled with growing competition from other service providers, will mean a gradual loss of overall market share for the Posts, even if they are showing real growth in physical mail volumes.

The UPU studies predicted worldwide market share for letter mail to drop to around 15% by 2005.

In some economically developed regions with mature postal markets, such as North America and Europe, mail volumes have begun to show a downturn. But this is offset by still-untapped growth potential, especially for advertising, or direct mail, in other regions of the world.

Posts have demonstrated their ability to adapt quickly to technological developments. Many have already entered the electronic realm, embracing new technologies to improve existing products and services and to create new ones for their customers. The main challenge for Posts is to find ways to effectively counteract substitution of physical mail by electronic communication and, at the same time, to use the opportunities offered by new technology to expand and improve their products and services.

The environment in which postal services operate has changed dramatically in recent years and all indications are that the pace of this evolution will continue to accelerate well into the future. Posts are expected to keep pace not only with developments in the technological field, but also with rapid economic and social changes.

Posts have in recent years faced the realities of the new economic forces of deregulation, globalization, liberalization and, to a lesser extent, privatization. The postal environment is also continuing to change under the impact of increased competition and customer demands. Postal customers are demanding much more than in the past, and if they do not receive the level of service they expect, they will shift their business to other competitors.

While political independence and a free market economy have brought new opportunities for Posts in some regions of the world such as parts of Eastern Europe, economic and political uncertainties in other regions make the provision of basic postal services difficult.

The new technology-driven information society has also changed the postal business environment considerably. It has brought with it a host of new ways to communicate and to do business, such as electronic communication and commerce.

**Top**

## *eCommerce Opportunities*

eCommerce is driving the new economy and the Internet is its primary facilitator. The Internet is a communications network that has revolutionized the way people access, share and use information.

The amount of information and the speed at which it can be exchanged have increased dramatically. Rapid and robust information flow saves time and money. It transforms organizations because it eliminates paper-based functions, lowers transaction costs, flattens organizational layers and integrates global operations.

The benefits of eCommerce are:

- The Internet is ubiquitous, accessible and low-cost.
- eCommerce can be accessed through diverse forms of technology (computers, PDA's, mobile phones, digital TV, kiosks).
- The time to market is shortened.
- Existing card payment schemes can be adapted.
- Significant opportunities for rationalizing operations and downsizing.
- No geographical constraints.

- Middlemen can be eliminated from the supply chain.
- Stockholdings can be minimized or eliminated through just-in-time manufacturing processes.
- Transaction costs can be substantially reduced by eliminating physical points of sale and minimizing the administration overheads of paper-based processes.
- Existing card payment schemes can be adapted.
- Opportunities may exist for rationalizing operations and downsizing.

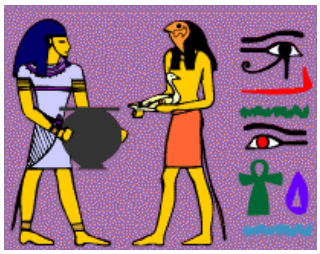
Many organizations are now exploiting the Internet in a commercial way and some of these have had a direct impact on postal business. Amazon (www.amazon.com) is a well-established sales portal and a very good example of an eCommerce company increasing sales for the Posts. There are millions of others companies now trading at local, national and international levels.

Top

## *What is eCommerce?*

In its simplest sense, “commerce” is an act of trade between two parties:

- where the exchange is negotiated under a set of mutually acceptable conditions, so that both parties emerge satisfied with the result
- where the exchange may depend on whether the two parties are prepared to trust one another



More complex transactions such as share dealings need to be supported by rules, procedures and fail-safe mechanisms, which provide trading partners with assurance and recovery methods when trust breaks down.

Adding an “e” to commerce introduces another layer of complexity by transferring all the interactions, rules, procedures and fail-safes into a virtual word. On the internet the provision of trust becomes the keystone of any successful trading model because without trust, no-one will trade.

Most eCommerce vendors are simply offering the customer another access point to the physical commercial model. The same trading activities need to happen:

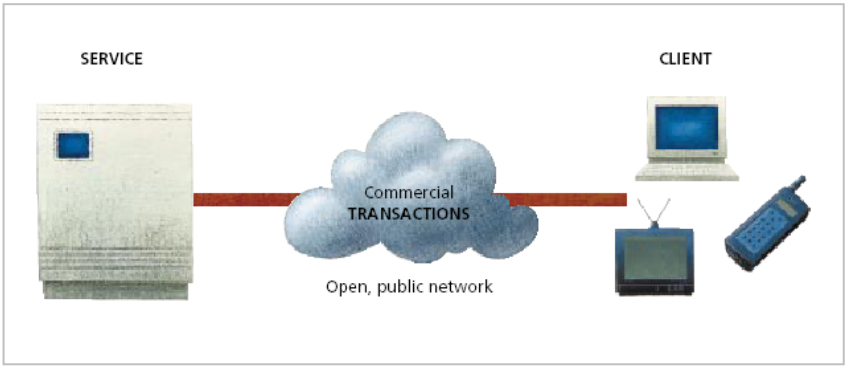
- an offer by the vendor;
- acceptance by the customer;
- an exchange of money and goods or services.

Everything else is padding to attract the customer and facilitate the purchase.

Trading on the Internet requires:

- an organization providing an on-line service accessed via the Internet
- clients (consumers or other organizations) connecting to the service using devices such as computers, mobile telephones or interactive televisions
- the exchange of transactions that relate to the purchase and provision of goods and services.

This is illustrated in the figure below:




**Service**

**Customer**

**Business transactions**

**Open public network**

**Top**

## *Guiding Principles*

Information is:

- A critical asset that must be protected.
- Restricted to authorized personnel for authorized use.

Information Security is:

- A cornerstone of maintaining public trust.
- A business issue, not a technology issue.
- Risk-based and cost-effective.
- Aligned with organizational priorities, industry prudent practices, and government requirements.
- Directed by policy but implemented by business owners.
- Everyone's business.

**Top**

## *eCommerce Business Models*

eCommerce business models integrate the Internet, digital communications and IT applications that enable the process of buying and selling.

Web-based business to consumer face of eCommerce has succeeded in attracting most of the attention of the business press.

Electronic business is normally defined as:

- B2B (business to business);
- B2C (business to consumer);
- C2C (consumer to consumer).

Electronic Commerce forms the business related information and communication activities that can occur B2B or B2C or C2C which do not directly involve buying or selling. For instance the advertising of products or services, electronic shopping, and direct after sales support.

Web Commerce conducted over the world wide web reflects the fact that there is still a great deal of electronic commerce that is conducted through proprietary EDI channels and value added networks.

Electronic Data Interchange (EDI) precedes modern day electronic commerce by two decades. EDI comprises standard formats for a variety of business commercial transactions such as orders, invoices, shipping documents and the like.

Electronic funds transfer can be conducted over private networks or over the Web. Source Huff, Wade et al "Cases in Electronic Commerce," (London,Ontario: Ivey School of Business 2000) pp 4-5.

**Top**

## *eCommerce Transactions*

eCommerce transactions typically have four phases:

1 Information Provision

Providing pre-sales information on products and services. Typically, this may include on-line catalogues, price lists and product specifications. Information can be tailored to individual needs and previous purchasing history.

2 Agreement

Agreeing the terms of the purchase. These may include price, discount, method of payment and delivery requirements. This phase should result (either explicitly or implicitly) in a clearly understood contract between buyer and seller.

3 Settlement

Fulfilling the terms of the contract. These could include exchange of payment and receipt and arranging delivery logistics. For electronic goods (e.g. documents, music, software), delivery itself may also take place on-line.

4 After-sales

Providing post-sales support. This could include technical support such as electronic conferencing, new product information and product upgrades (e.g. for software). It can be used to maintain continuous contact with customers and feed back into the information phase.

In practice, only some of these phases may take place electronically. For example, many organizations provide web sites that hold product information and also provide on-line after-sales support. However, purchase, payment and delivery of goods may take place through traditional channels.

**Top**

# Governance



## *Introduction*

Governance provides the structure and processes for setting the objectives of an organization and measuring the organization's performance against them.

Responsibility for Corporate Governance lies with the Chief Executive or Executive Board of an organization. In practice there will be some delegation of functional responsibilities. And most likely there will be a number of strands or layers of governance concerned with managing critical functions such as IT, Security and eCommerce.

Governance of eCommerce Security may be addressed through existing IT and Security Governance structures or through a new framework. In either case, it will require new or enhanced policies and processes to be established to address the new security challenges associated with eCommerce.

**Top**

## *Why Governance is an issue for eCommerce*

eCommerce presents a number of risks and issues for an organization that may not be satisfactorily addressed through existing Governance structures:

- The desired speed to market for an eCommerce product may be substantially shorter than for a conventional information system, requiring existing management processes to be shortened or by-passed.
- Security risks are likely to be higher for an eCommerce system than for an in-house information system, requiring stronger countermeasures, involving encryption and authentication technologies.
- Developing an eCommerce system requires a complex, skilful blend of Business, IT and Security knowledge. Close alignment of decision-making across these functions will be necessary to deliver a viable solution.
- Governance may need to extend beyond the boundaries of the organization to include elements of the infrastructure of customers, suppliers and business partners.

- Legislative and regulatory issues may be unknown, uncertain or in the process of being developed. Risks and compliance requirements might be complex and difficult to determine, requiring specialist advice and attention.

At the very least, a review of existing Corporate, IT and Security Governance processes should be undertaken to ensure that they are adequate to direct and control the development of eCommerce solutions.

Top

## *Key elements of an eCommerce Governance Structure*

Key elements of any Governance structure include policies, organizational responsibilities, risk management processes, standards and compliance processes. Each of these items should be reviewed to ensure that adequate guidance and processes are in place to provide the clear management direction necessary to manage the complex risks associated with eCommerce.

The following items represent the key elements of a quality Governance structure for managing the security risks associated with eCommerce. They are consistent with the requirements of the international standard for Information Security Management: ISO/IEC 17799–1:2000.

### Policy

Establishment of clear policy direction and the demonstrated support of management through the issue and maintenance of published eCommerce Security policy across the organisation. The policy should emphasise the importance of eCommerce security and set out or reference the specific policies, principles, standards and compliance requirements for achieving this, including:

- compliance with legislative and contractual requirements;
- security education requirements;
- prevention and detection of viruses and other malicious software;
- business continuity management;
- consequences of security policy violations.

### Organizational responsibilities

Clear and specific accountability for all aspects of eCommerce Security, including:

- A senior management forum to review and approve policy, responsibilities, major risks and incidents, and for approving major initiatives to enhance eCommerce security.

- In a large organization it may be necessary to establish a cross-functional forum of management representatives to coordinate the implementation of eCommerce security controls across the enterprise.
- Allocation of specific responsibilities for the security of individual projects, assets and security processes.
- Authorization processes for the secure introduction of new eCommerce systems and infrastructure.
- A source of specialist eCommerce security advice.
- Responsibilities and contacts for reporting and managing security incidents.
- Responsibility for reviewing organizational practice against policy and standards.

## Risk Management

The need for security controls should take account of the business harm likely to result from security failures. Risk assessment techniques can be applied at an organizational/business unit level, or to an individual information system or asset. In practice, this is likely to be done selectively and at different levels of detail throughout the organization

The following considerations should be addressed:

- Risks should be identified and addressed at the earliest stage in an eCommerce project because controls introduced at the design state are significantly cheaper to implement and maintain.
- Risk assessment should take account of the business consequences of security failures, as well as the likelihood of such failures, bearing in mind the potential level of security threats, the vulnerability of the system or asset, and the controls currently in place to prevent failures.
- Risks should be reviewed periodically to take account of changes to information systems, infrastructure, risk levels or to business requirements and priorities.

## Standards

Policy statements are an essential starting point but in practice they can do little more than convey the intent and support of senior management. More detailed guidance is required to enable the consistent implementation of an effective control structure. In drawing up standards for eCommerce Security, the following points should be considered:

- More than one level of eCommerce security standard will be required to address general control requirements, technical architecture and operational configuration controls.

- For ease of maintenance, it is helpful to separate technical and organizational detail from more general security principles. This will minimize the amount of information that requires frequent updating. General principles and control descriptions should require little change over a five-year cycle. However, technical guidance will need to be refreshed at least every 12–18 months.
- Standards can either be flexible in interpretation (a “code of practice”) or rigid and prescriptive (a “conformance standard”). There is no single best approach that fits all situations. The optimum approach for an organization depends on the culture and overall governance structure.
- The International Standard ISO/IEC 17799–1:2000 “Code of practice for Information Security Management” is a useful reference standard in drawing up eCommerce Security standards.

## Compliance Requirements

The design, operation, use and management of eCommerce systems may be subject to a range of statutory, regulatory and contractual security requirements. The following points should be noted:

- Advice on specific legal requirements should be sought from the organization’s legal advisers or suitably qualified legal practitioners
- Legislative requirements vary from country to country and for information created in one country that is transmitted to another country (trans-border data flow)
- Compliance requirements to consider include intellectual property rights (copyright, design rights, trade marks), software licenses, retention of records, data protection and privacy, prevention of misuse of facilities, regulation of cryptographic controls, collection of evidence, etc.
- Compliance of the organization’s operating practices with the above requirements and with internal policy and standards must be regularly reviewed by a competent, independent body. This will need to be carried out a number of levels: for information systems, infrastructure, service providers, management and users.

Top

# Security Risks and Threats



## *Overview*

Once the decision to engage in eCommerce has been made, organizations are compelled to address a range of diverse factors, including:

- The adoption of radically new business models.
- The need to implement rapidly evolving technology that is not always reliable or predictable.
- How to identify and measure risks and business impacts.
- The potential for widespread and immediate visibility – to the public, trading partners and competitors – of any problems with eCommerce systems, such as system performance problems or corrupted data.
- The impact of service components which are entirely outside an organization's control – namely the Internet and customers' PCs with web browsers.
- Access to the organization's IT systems by customers – essentially unknown third parties – from arbitrary locations.
- The need to address consumers' fears about the privacy of their personal information, in particular credit card details.
- Compliance with legal and regulatory requirements.

While many of these factors are not individually complex, in combination they present a significant challenge. Furthermore, virtually all of the factors have significant security implications that can seem daunting when embarking on the road to providing an eCommerce service.

However, rationalizing the issues and clearly identifying the problems must be the first stage in building a solution. This most important first stage is dealt with in more detail under Risk Assessment.

To further rationalize the process of assessing risks and threats, one method of doing so is to divide the issues into four groups:

- Service-side issues
- Transaction issues
- Client-side issues
- Legal and regulatory issues

**Top**

## *Risk Assessment*

Risk assessment is an essential element of an effective approach to information security. Used appropriately it raises management awareness of security exposures, provides a mechanism for understanding the magnitude and potential impact of these exposures and assists in the evaluation and selection of appropriate safeguards.

However, risk assessment does require certain skills and can be time and resource consuming. It also needs to be carried out consistently within an organization to ensure that security policies are deployed to an appropriate level. It is therefore important that a standard method and approach is adopted.

There are several approaches to risk management:

Each option has advantages and disadvantages and the choice will depend on security requirements and the resources available.

| | **Advantages** | **Disadvantages** |
|---|---|---|
| **Baseline approach** | Pre-assessed safeguards are suggested in manuals.<br>Time and resource requirements are relatively low.<br>Provides a minimum level of security across the whole organization. | The security level might be too high or too low. |
| **Informal approach** | No additional skills are needed for carrying out the analysis.<br>Performed quicker than a detailed risk analysis. | Likelihood of missing risks is high.<br>Analysis might be influenced by subjective views.<br>Very little justification of selected safeguards. |
| **Detailed risk analysis** | The appropriate security level is identified for each system.<br>Safeguards are justified. | Takes a lot of time, effort and experience to carry out a detailed risk analysis. |

| | | |
|---|---|---|
| **Combined approach of baseline plus detailed risk analysis** | The results of a high level analysis help to save resources.<br>Good planning aid.<br>Resources are applied where they are most effective. | If the baseline level analysis is inaccurate, some of the safeguards might not be sufficient. |

## Definitions

| | |
|---|---|
| Threat | Any potential event or act, deliberate or accidental, that could cause injury to employees or assets |
| Risk | The chance of a vulnerability being exploited |
| Vulnerability | An inadequacy related to security that could permit a threat to cause injury |

## Methodologies

There are many risk assessment methodologies available, ranging from simple judgment-based assessments to detailed software-driven assessments. Most methodologies analyze systems criticality as well as categorizing threats in terms of Confidentiality, Integrity and Availability.

Some organizations have taken these methodologies and adapted them for internal use. Other organizations prefer to obtain risk assessment products and services from the many companies that specialize in this area.

A risk assessment will examine:

- what threats exist or might exist;
- what impact the threats might have;
- what likelihood there is of the threats occurring;
- what responses are required.

A very simple approach to risk assessment is demonstrated in the following example:

**Simple Web Portal**

This Simple Web Portal has been designed with baseline security measures. The risk assessment considers some of the risks that might not be addressed by such measures. **Impact** assesses how much harm might be inflicted if the threat occurred. **Likelihood** assesses how adequate the baseline security measures are. The **score**, a multiple of impact and likelihood, identifies the criticality of the threat in relation to

the Simple Web Portal. The response defines additional security measures to be deployed, or the reasoning for accepting residual risk.

| Threat | Impact | Likelihood | Score | Response |
|---|---|---|---|---|
| **CONFIDENTIALITY** Theft of customer credit card details | 3 | 2 | 6 | Customer detail database and file transmission to be encrypted |
| **INTEGRITY** Sales data manipulation | 2 | 1 | 2 | Adequate access control mechanisms in place |
| **AVAILABILITY** Denial of Service | 2 | 2 | 4 | Introduce contingency through mirrored sites |

The scoring mechanism employed in the table is:

Impact: High = 3; Medium = 2; Low = 1

Likelihood: Highly Likely = 3; Moderately Likely = 2; Unlikely = 1

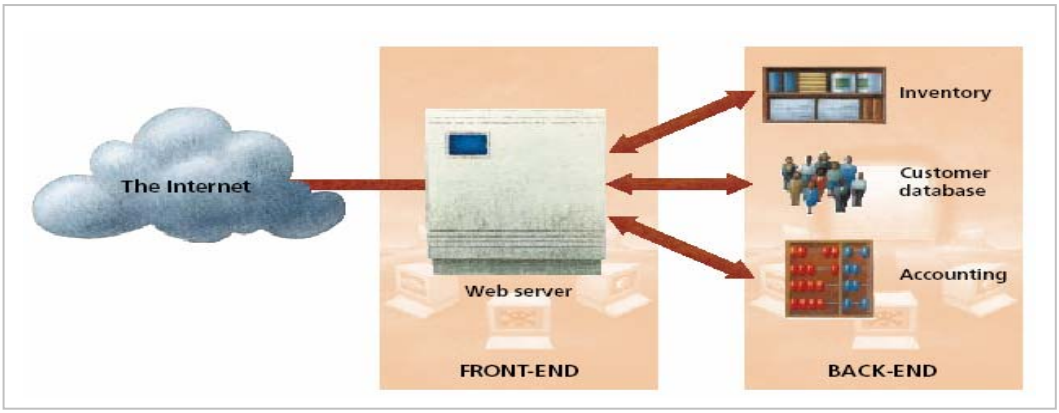
Further information about risk assessment is available from many sources on the internet. A primary source can usually be found through government websites, or through the major international consulting companies.

Top

## *Service-side Issues*

An organization's infrastructure for supporting an eCommerce service will typically have two main elements:

- an eCommerce front-end (generally one or more web servers connected to the Internet)
- back-end systems needed both to supply information to the front-end systems (such as product information and stock holding) and to extract information from them (such as orders for transferring to logistics systems and payments to be cleared through third parties).



**Front-end systems**

The main threats to front-end systems and the resulting business impacts are illustrated in the following table.

| Threats | Business Impact |
|---|---|
| Web server or Internet connection overload due to unforeseen demand for access, causing degradation of performance or loss of service. | Loss of revenue as customers move to alternative services. |
| Web server failure due to unreliable software or hardware, or operational mistakes. | Loss of reputation due to high visibility of problems. |
| Web pages contain inaccurate product or price data. | Erosion of profits if products are sold at the wrong price. |
| Web pages modified to include obscene or defamatory material. | Loss of customers offended by content. |
| Potential customers attracted to the wrong web site, e.g. www.microsfot.com which advertises Linux, a rival to Microsoft's NT product. | Loss of potential revenue to competitors. |
| Inappropriate disclosure of confidential information held on web sites (e.g. customer personal details and financial information) through misconfiguration of security controls. | Loss of customer confidence in system. |

Setting up and running a web server has many pitfalls and needs to be managed with care.

**Back-end Systems**

Connections made to internal systems to enable eCommerce can expose critical business systems to new threats that were perhaps not envisaged when they were originally designed. The table below shows the main threats and their possible business impacts.

| Threats | Business Impact |
|---|---|
| Unforeseen volume of transactions from eCommerce web servers, degrading the performance of key internal systems. | Critical business functions disrupted by the unavailability of systems on which they depend. |
| Failure of links between front- and back-end systems, causing out-of-date or inaccurate information to be displayed on web front-ends. | Commitments made to customers, which are unachievable. |
| Internal systems opened to unauthorized access from the Internet. | Serious disruption of business through hackers corrupting critical information. |
| Front-end eCommerce applications subverted to pass incorrect or unexpected data to back-end systems, causing them to behave in undesirable ways. | Failure of critical business systems through inability to cope with unexpected input. |

Top

## *Transaction Issues*

Transactions between buyers and sellers in eCommerce can include requests for information, quotation of prices, placement of orders and payment, and after sales services. The high degree of confidence needed in the authenticity, confidentiality and timely delivery of such transactions can be difficult to maintain where they are exchanged over an untrusted, public network such as the Internet.

The interception of transactions, and in particular credit card details, during transmission over the Internet has often been cited as a major obstacle to public confidence in eCommerce. In fact this risk is generally exaggerated and sensitive information is more likely to be at risk of disclosure while stored on web servers. However, public perception of insecurity can be a true barrier to eCommerce and organizations must take care to address this.

The main threats to eCommerce transactions are listed below.

| Threats | Business Impact |
|---|---|
| Sensitive payment details (e.g. credit card numbers) intercepted. | Loss of customer confidence, especially if details are used to make unauthorized purchases. |

| | |
|---|---|
| Passwords and other system access information intercepted. | Release of sensitive information due to unauthorized access to systems. |
| An agreement to purchase at a specified price subsequently denied by a customer. | Unrecoverable costs incurred in fulfilling the order. |
| A transaction modified or forged before delivery. | Goods dispatched to a fraudster. |
| Transactions failing to arrive or substantially delayed through network congestion. | Loss of customers through frustration. |

Top

## *Client Side Issues*

A key component of most eCommerce applications is the computer (or other intelligent device) operated by the customer or trading partner – the 'client-side'. In most cases, the client environment is outside the direct control of those offering eCommerce services. This distinguishes eCommerce from traditional business applications where organizations can often specify the software, hardware and configuration details of the client environment.

Some of the main threats resulting from this lack of control of the client-side are shown in the following table.

| Threats | Business Impact |
|---|---|
| Passwords or other system access information held on an insecure client PC and disclosed inappropriately. | Release of sensitive information due to unauthorized access to systems. |
| Different web browser types have varying features and could interact in different ways with an eCommerce web server. | Loss of customers who cannot make effective use of the service with their browsers. |
| Users, or their organization's networks blocking 'cookies' or 'active content' technologies such as Java, JavaScript and ActiveX, because of concerns that they could include malicious capabilities. [These technologies are widely used to improve the functionality, performance and appearance of eCommerce applications.] | Loss of revenue if users are unable to access the service. |

Top

## *Legal and Regulatory Issues*

The legal and regulatory framework for international eCommerce is an area of wide debate and covers areas outside the scope of this report, such as taxation, consumer protection and jurisdiction. However, many legal and regulatory issues are directly related to the security aspects of eCommerce and are illustrated in the following table.

| Issues | Business Impact |
|---|---|
| **Internationalize (Privacy Section)**<br><br>The European Union Directive on Data Protection of 1995 requires Member States to enact new measures to ensure that personal information held on information systems is adequately protected. One of the key measures introduced is a restriction on the export of personal data to countries that do not have comparable legislation in place (see Information Privacy). This has a bearing on eCommerce applications that involve cross-border transfer of personal information. | Additional costs involved in complying with data protection legislation.<br><br>Possible restrictions in scope of eCommerce applications.<br><br>Legal action following breaches of the EU Directive. |
| The legal recognition of electronic documents as substitutes for paper equivalents varies from country to country. In some cases certain types of document have to exist in paper form to have legal validity. Similarly, electronic (or digital) signatures used to prove the authenticity of electronic transactions have varying legal acceptability in different jurisdictions. | Lack of legal recourse in the event of a dispute. |
| Some security solutions for eCommerce rest heavily on cryptographic products. These products are subject to restrictions on export, import or use in some countries because of their potential military or criminal application. However, the situation with cryptography is changing and moves are being made in some countries to relax controls. | Restrictions on an organization's freedom to employ the desired level of protection leading to unacceptable business exposures. |

The legislative and regulatory regime is undergoing rapid change in response to the development of eCommerce. However, some countries react more quickly and thus incompatibilities arise, particularly affecting cross-border eCommerce. Organizations should monitor this area carefully to enable them to adapt their eCommerce strategies appropriately.

**Top**

# eCommerce Security Solutions

This section describes how security solutions can be used to address the issues described in the section on Security Risks and Threats, many of which may be holding organizations back from participating in eCommerce. Careful implementation of these solutions will enable businesses to exploit the benefits of trading electronically while minimizing the security risks.



## *Service-Side Solutions*

The front and back-end systems supporting an eCommerce application can be protected by:

- developing applications and supporting systems that are robust;
- establishing a network environment that protects these systems;
- introducing essential management practices that ensure security is maintained over time.

### Applications and Supporting Systems

The eCommerce application and the web servers and internal systems that support it should be resilient to deliberate security attacks and to the common problems of overload and systems failure. The following measures should be implemented:

- Web servers should be based around robust platforms that can be readily scaled in terms of disk space, memory and processing capacity to accommodate increases in demand.
- Web servers should be built from software components (e.g. operating systems, web server applications) that are well understood and can be supported by the organization.
- Operating systems, applications and platforms should not be installed “out of the box”, with security switched off.
- Internal systems should be protected against unexpected volumes of transactions that could cause critical business functions to become unacceptably slow or even completely unavailable.
- Software components should incorporate the most recent fixes to known security weaknesses.
- eCommerce applications should validate all user inputs to avoid deliberate subversion or accidental corruption.

- Systems and applications should be designed to avoid disclosing information about their internal working as this can be exploited by attackers.
- Use, where appropriate, of tamper-proof hardware devices for storing cryptographic keys and performing cryptographic functions.

## Network Environment

The network environment of an eCommerce application supports the interconnection of the various service components and their connection to the Internet. The two main security requirements are to:

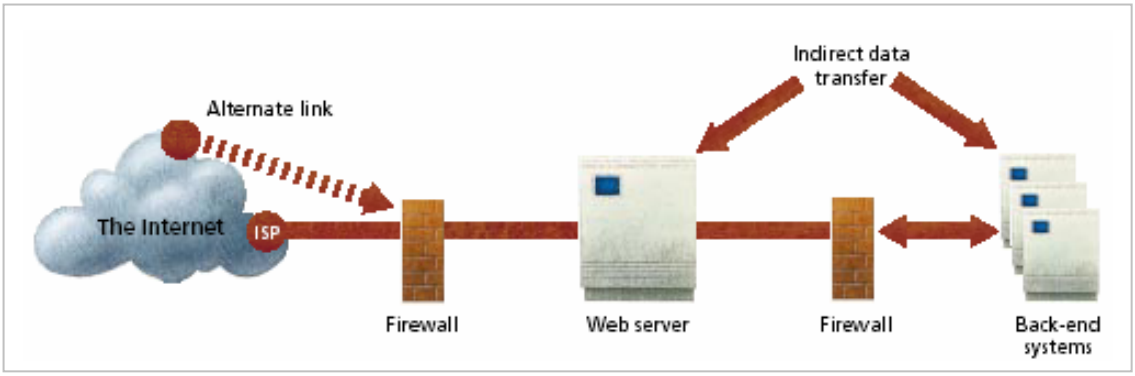
- avoid service availability problems caused by accidental overload and failure of communications links;
- protect both web servers and internal systems from deliberate attacks by implementing appropriate network configuration measures.

In order to avoid availability problems, organizations should estimate likely traffic volumes as accurately as possible so that web server communications links to the Internet and supporting internal systems can be increased quickly to match requirements.

For applications with particularly high availability requirements, single points of failure can be minimized by establishing hot-standby communications links with alternative telecommunications organizations and Internet Service Providers (ISPs).

The network architecture can be used to protect eCommerce systems against deliberate attacks by limiting the way network connections can be made to the web server and to internal systems. This can be achieved through employing firewalls – a widely used means of protecting Internet-connected systems from external attacks. Firewalls can also be employed to restrict access to back-end supporting systems, providing a degree of logical separation.

The figure below illustrates the way these solutions apply to the eCommerce model.



## Management Practices

A robust technical environment must be reinforced by strong management practices to ensure that a secure infrastructure for eCommerce is maintained. These practices should include:

- a capacity planning process to ensure that systems and communications links are upgraded before any increase in traffic becomes a serious problem;
- a mechanism for quickly addressing newly-discovered security problems (the Internet itself is widely used to disseminate this information);
- a rigorous change management process to avoid ad hoc technical changes;
- a process for continuously testing the security of the eCommerce infrastructure, including external 'penetration testing' of firewalls, web sites and connections to internal systems;
- efficient arrangements for the detection of security incidents and a plan for a rapid and effective response.

An organization's commitment to good security practices can help to build the necessary confidence of customers – particularly those concerned about the privacy of their personal information. A number of initiatives exist to allow organizations to gain accreditation against standards of good practice for protecting customer data, for example:

- WebTrust (American Institute of Certified Public Accountants, Canadian Institute of Chartered Accountants, and a consortium of chartered accountancy bodies in the United Kingdom).
- TRUSTe (CommerceNet and Electronic Frontier Foundation).
- Online Privacy Alliance (Netscape, Microsoft, AOL).
- ISO 17799.

**Links required**

## *Transaction Side Solutions*

eCommerce transactions take place over an open, untrusted network that is largely outside the control of the trading parties. The principle means of countering the threats to transactions in this environment is through the use of cryptography.

Cryptography essentially provides three distinct capabilities:

- the content of electronic transactions can be hidden;
- any changes to electronic transactions can be detected;
- the source of electronic transactions can be confirmed.

These capabilities are achieved through a combination of encryption and cryptographic digital signatures.

## Encryption

Encryption allows the content of messages to be hidden and so plays a crucial role in maintaining the confidentiality of electronic transactions.

Current Internet technology has an in-built mechanism, known as Secure Sockets Layer (SSL) that can be used to encrypt messages sent between web browsers and web servers. This mechanism is widely used by on-line merchants to ensure that credit card numbers and other sensitive information sent by customers are protected during transmission across the Internet.

Encryption can also be used to create a virtual private network (VPN). This is effectively an encrypted channel across the Internet between two organizations or two parts of the same organization. VPNs are becoming increasingly used for business-to-business eCommerce.

## Digital Signatures

Cryptographic digital signatures provide two basic capabilities: they allow the source of an electronic message to be confirmed and also permit any changes to the message to be detected. These capabilities give digital signatures a major role in securing eCommerce because they can help to:

- prove the authenticity of an electronic transaction to prevent forgery;
- confirm the identity of an individual to prevent impersonation on-line;
- provide proof of transmission and receipt of transactions to prevent repudiation.

As with encryption, basic digital signature capability is built into standard web servers and browsers through SSL, which then allows users to:

- prove their identity in a way that is much more reliable than user-name/password mechanisms;
- confirm the identity of the web server with which they are communicating (e.g. to ensure they do not provide sensitive information to the wrong web site).

To enable digital signatures to work in practice, a complex range of technologies, standards and practices known as a public-key infrastructure (PKI) needs to be in place.

In practice a PKI is based on digital IDs – known as digital certificates – which are issued by Certification Authorities (CAs) to individuals after reliable confirmation of their identity. Such an infrastructure allows:

- standards to be established so that digital certificates can be created which are valid across different business units, organizations and countries;
- digital certificates and associated cryptographic keys to be created, stored and managed securely;
- expired digital certificates to be renewed;
- digital certificates to be revoked, e.g. if they have been used fraudulently.

The role of PKI in underpinning trust in eCommerce will make it an increasingly important technology. It is also important in the delivery of eGoverment services, which will provide the catalyst for other more commercial products and services. The products and services needed to build or use a PKI are still immature but are developing rapidly. Organizations considering implementing PKI should be aware that it is a highly challenging technology to implement and maintain. Identifying best practice among successful organizations is highly recommended.

Organizations with eCommerce plans that rely on the strong authentication of trading partners and transactions should define their strategies in this area. This should involve:

- developing or acquiring the necessary technical and management skills;
- considering whether to develop an internal PKI or employ outsourced services;
- piloting PKI technologies and services.

**Links required**

Entrust

RSA

## Secure Electronic Payment

One of the key practical applications of cryptography in securing eCommerce transactions is in the settlement phase. Here payment for goods and services often needs to take place on-line in a way that is trusted by business, consumers, banks and regulators. The main options for implementing secure payment schemes are:

**Credit and debit card payments**

The use of SSL for encrypting payment card details is currently the dominant approach adopted by Internet merchants as it is cheap to implement and appears to be gaining consumer acceptance. However, alternative approaches to securing payment card details have been developed, including:

- SET (Secure Electronic Transactions): developed by MasterCard, Visa, Microsoft, Netscape and others to provide confidence in on-line credit card payments by using encryption to preserve the confidentiality of transactions and also by enabling the mutual authentication of card-holders and merchants via digital signatures.
- S/MIME: a standard for providing secure e-mail which can be used to protect payment details sent via this method.
- proprietary systems: such as that of CyberCash Inc which provide purchasers with an electronic wallet which stores payment card details securely on a PC and encrypts transactions between the purchaser and Internet merchants.

**Electronic cash**

For low value transactions (say, less than $10), credit and debit card payments are inappropriate because of their relatively high cost overhead. Visa estimates that the total world-wide annual spend on transactions less than $10 is $1.8 trillion and therefore there is a potentially large market for eCommerce involving low value transactions, for example to pay for weather reports, news, stock prices and on-line gambling. Low value/high volume transactions are still vulnerable to fraud and the emerging mechanisms for enabling such payments over the Web use cryptographic techniques to prevent forgery of what is effectively electronic currency.

The main initiatives in the electronic cash field are currently:

- Systems employing an electronic wallet through which low value purchases from web sites may be made. One leading implementation from CyberCash used digitally signed CyberCoins created when funds are transferred to the wallet from an existing bank or credit card account. CyberCash has now been taken over by Verisign and the service transferred to Verisign's Payflow product.
- Micropayment projects, such as Millicent, developed by Digital (now part of Compaq), which uses a software electronic wallet for payments of $5 to less than $0.01. Many of these projects are on hold or not being delivered due to the complexity of the solutions.
- Smartcard-based solutions such as Mondex and VisaCash which have been piloted in high-street retail for several years but which are now being used in Internet applications.
- Schemes designed to allow truly anonymous and untraceable electronic payments (features of real cash transactions) by use of digitally signed electronic vouchers.

## *Client-Side Solutions*

The lack of direct control over the client's computer can make it difficult for organizations to implement security measures. Thus, compensating mechanisms may be needed in the eCommerce architecture.

However, there are some measures that can be adopted, particularly in situations where a degree of control exists over the client environment or where there is user cooperation.

### End-user Agreements and Education

Even if technical mechanisms are implemented successfully on the client-side, security will always be dependent on the correct behavior of users, for example in protecting passwords, PINs and smartcards from misuse.

Organizations should aim to establish binding agreements with users through on-screen terms and conditions. Comprehensive and practical advice should also be provided to raise user awareness of security issues and education

### Hardware Tokens

Although standard web browsers provide support for handling the cryptographic keys and certificates needed to employ digital signatures, weak PC security can reduce the reliance that can be placed on these mechanisms.

A potential answer to this problem is the smartcard – providing both storage and computer processing on a relatively tamper-resistant hardware platform. Smartcards provide an ideal method of storing cryptographic keys and are already being used successfully in eCommerce applications.

An explosion in the use of smartcards has been predicted for some time but has been held back by a profusion of competing standards and the need for a smartcard reader device wherever the card is used. However, progress is being made in both these areas – for example through initiatives by Microsoft and leading PC manufacturers – which indicates that the smartcard may become one of the key technologies in secure eCommerce.

Hand-held tokens that generate passwords provide another option for enhancing client-side security. They provide a stronger alternative to user selected passwords by generating a password that changes for each login. These tokens need no reader device at the client-side but do not provide the wide functionality offered by smartcards.

### Customized Client Software

It is possible (but it may be impractical) to implement additional security measures at the PC by:

- replacing the standard web browser with a version customized for a specific application;
- introducing additional security software that works in conjunction with a conventional browser;
- Implementing security functionality in Java applets or other active content technologies that are automatically downloaded to the user's PC. However, users can elect not to receive such active content, which may reduce the market that the application can reach.

## *Legal and Regulatory Solutions*

Organizations can address the legal and regulatory issues in two ways:

- Passive monitoring of developments
- Active participation in influencing legislation.

### Monitoring

All organizations should monitor closely the evolution of legislation and regulations affecting eCommerce. Any new laws or regulations in this rapidly changing environment will certainly influence the mechanisms and practices that need to be adopted to conduct secure eCommerce. Organizations that can predict developments and react quickly to exploit them will gain an advantage. For example, the disparity in legislation between different countries could have an influence on the best location for eCommerce operations.

### Lobbying

Organizations should seriously consider participating in the development of eCommerce legislation. Inappropriate legislation could significantly increase the costs or risks of carrying out eCommerce. Good understanding of the issues at stake is not widespread and most legislators are currently receptive to the opinions of business. Lobbying for workable and beneficial legislation can be conducted directly or through external bodies.

Top

# Training



## *Introduction*

Training is of critical importance for a successful eCommerce security framework.

Training referred to in this context encompasses awareness of the need to protect information, training for skill areas needed to operate electronic commerce systems securely and education in specific security measures or best practice methodologies.

Top

## *Recruitment Considerations*

The use of technology to sell products and services electronically is a steeply rising trend. So too is the trend in security related issues and the need for skilled IT security personnel.

### External Sources

Traditional sources of trained security personnel include the military, defense departments and ministries, programmers, networking professionals and external consultants.

Obtaining the right balance of skills and competencies through external recruitment of personnel with an information or technical security background, with those able to understand the unique business drivers of a postal system, remains a challenge.

### In-house talent

Based on industry trends, enterprises will need to become more creative in their staffing efforts, finding most of their employees inside the organization and then training them in the most effective way.

Recent research indicates that it is more productive to identify internal staff with core competencies and overlay the requisite security training and education to develop this desired skill-set.

Top

## *Training Evaluation*

Training today augments traditional instructor-led training with on-line and web-based technologies. These alternate forms of delivery can be very helpful in reaching remote users and allowing users to pursue specific security training at their own pace.

Components to consider when evaluating a security-training program:

- Coursework;
- Drills with specific threat scenario focus;
- Conferences;
- Product-specific training;
- Research and self-study;
- Measurement.

### Coursework

Coursework will encompass a wide range of topics and should be based on a skill inventory and needs assessment. Many companies retain an internal training department to review and develop proprietary training or often work with subject matter experts to deliver to the security team. A common approach used to target specific training requirements involves hosting seminars delivered by SMEs or visiting industry guests. Seminar examples include threat and risk assessment methodology or extensive penetration testing exercises.

### Drills with specific threat scenario focus

Drills familiarize staff with established procedures and they are invaluable for demonstrating potential threat scenarios. These activities can range from the highly realistic to conceptual scenario that draw from fundamental concepts, such as common exploit types, and then move to more complex applications that build on business continuity requirements of the eCommerce business unit.

### Conferences

Information security conferences and forums provide opportunity to expose security staff to new trends in the field as well as network with peers. Conferencing serves both as a learning opportunity and provides a motivational factor for employees. Conference attendees should be prepared to deliver subsequent training sessions to share observations for the benefit of the enterprise.

### Product-specific training

Vendor-hosted classes and certification tracks provide the opportunity to sample newer products and understand the security concepts behind them. Caution should be exercised to ensure instructors are qualified and accredited.

### Research and self-study

Keeping abreast of current exploits and continuous learning of new security threats and countermeasures is essential. Conducting research and studying security resources such as newsgroups, websites and periodicals provide value added insight to the security practitioner. Additionally, subscriptions to security alert/news services provide timely updates and analyses of security events in timely fashion. Companies who support a hands-on test lab to encourage security analysts to pursue self-study projects and investigations are traditionally well positioned when these security incidents do occur.

### Measurement

Once an investment in developing and maintaining a training program has been made, the final step includes tracking the program's effectiveness. It is important to gauge learners' opinions of training and design mechanisms that track trainees' retention and application of the instruction provided.

**Top**

## *Training Programs*

Information Security is a very broad discipline with opportunities for specialists in diverse technologies, consultancy, program management, policy and strategy.

There are several internationally recognized centers of information security education. These programs intend to reduce vulnerabilities in the information infrastructure by promoting higher education in information assurance and producing a growing number of professionals with expertise in various security disciplines. However, before deciding to take advanced training in the security discipline, it is wise to verify accreditation and the local recognition of any foreign academic credentials to be obtained.

There are many training programs available, some backed by professional certification, others more modular providing specific skills in specialized subjects. It is important to understand the capabilities and career needs of employees before embarking upon a particular training program.

Uniformity of training delivery throughout an organization is important to ensure that security is deployed consistently and that standards are maintained to a baseline level. Sourcing training from a recognized professional body or academic institution will demonstrate commitment and professionalism on the part of the organization.

## Conclusion

Management of IT security issues can be complex ranging from discovering impacts resulting from a compromised system, log examination, evidence preservation, incident response, hardening against the exploits through to complex forensic investigations. In addition to expending resources to build and maintain these functions, companies will also have to devote time for research and how best to keep current in their field of endeavor.

The recruiting and training procedures a company implements in the security area will set the foundation of trust supporting a long term on-line business strategy.

Training human resources to defend your significant eCommerce investment is a challenge that can prove to be extremely rewarding when approached correctly.

**Top**

# *Training Resources*

There are many companies, industry associations and academic institutions offering training courses across a broad spectrum of skills in the eCommerce security field.

Professional Bodies Certifications and Associations

INFOSEC Training sources, learning aids, tutorials and programs

INFOSEC Academic Programs - Outside the USA.

INFOSEC / Information Assurance Academic Programs - USA based.

## Professional Bodies Certifications and Associations

**Association for Computing Machinery** (ACM) Special Interest Group – Security, Audit and Control (SIGSAC) http://www.acm.org/sigsac/ has a newsletter and an annual conference.

**American Society for Industrial Security** (ASIS) http://www.asisonline.org/ has an active information security program including Cybercrime conferences.

**European Institute for Computer Antivirus Research** (EICAR) has an active Web site http://www.eicar.org/ , annual meetings and is open for use in Europe and around the world.

**High Technology Crime Investigation Association** (HTCIA) http://htcia.org/ is an international organization with many regional chapters. HTCIA "is designed to encourage, promote, aid and effect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership."

**Information Systems Audit and Control Association** (ISACA) http://www.isaca.org/ "sponsors international conferences, administers the globally respected CISA® (Certified Information Systems Auditor™) designation earned by more than 24,000 professionals worldwide, and develops globally applicable Information Systems (IS) Auditing and Control Standards." Membership is limited to law-enforcement officials and security professionals.

**Information Systems Security Association** (ISSA) http://www.issa.org/ has chapters all over the world and "provides education forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members

**Institute of Internal Auditors** (IIA) http://www.theiia.org/ is active in all aspects of internal auditing including information security audit practices. The IIA sponsors conferences, works with academia to encourage and support the development and implementation of internal auditing courses and curricula, and manages the CIA (Certified Internal Auditor) professional designation.

**International Systems Security Engineering Association** (ISSEA) http://www.issea.org/ is a specialized group "focused on the adoption of systems security engineering as a defined and measurable discipline. The ISSEA's initial focus is the achievement of an ISO standard to guide and improve the practice of systems security engineering. The ISSEA will accomplish this through its oversight of the Systems Security Engineering Capability Maturity Model (SSE-CMM) Support Organization (SSO)."

**International Information Systems Security Certifications Consortium Inc.** (www.isc2.org) is a global, not-for-profit organization that: maintains a Common Body of Knowledge for Information Security [IS]; Certifies industry professionals and practitioners in an international IS standard, Certified Information Systems Security Professional (CISSP); Administers training and certification examinations; Ensures credentials are maintained, primarily through continuing education.

**Sicherheit in Rechner Netzen** (SIRENE) http://www.semper.org/sirene/ is a collaborating group of researchers from different organizations" in Finland, Germany and Switzerland who "share an interest in security and privacy." They publish technical papers in electronic commerce, medicine, mobile communication, theoretical cryptology and distributed systems.

**The System Administration, Networking and Security Institute** (SANS) (www.sans.org) was established in 1989 as a cooperative research and education organization. The SANS Institute offers rigorous training and certification programs, including intrusion-detection, firewall and incident-analysis certifications.

## INFOSEC Training sources, learning aids, tutorials and programs

**Avi Rubin** has compiled an extensive list of international security courses at http://avirubin.com/courses.html.

**Computer Emergency Response Team Coordination Center** (CERT-CC) offers courses; see the home page http://www.cert.org for links to upcoming sessions.

**Computer Security Institute** (CSI) http://www.gocsi.com/infosec/wkshop.html supplies has a catalog of its excellent live courses

**CISSP Open Study Guide** (OSG) http://www.cccure.org/ is a new collaborative project offering online documentation to help people study for certification as CISSPs (Certified Information Systems Security Professionals).

**Commonwealth Films** http://www.commonwealthfilms.com/home.htm makes training videos about information and computer security, communication, records, software, workplace laws, sexual harassment, antitrust compliance, depositions, discovery, defense, and compliance with regulatory laws;

**Computer Security Awareness Training** Web page sponsored by the US National Institutes of Health (NIH) at http://wwwoirm.nih.gov/sectrain/

**Center for Education and Research in Information Assurance and Security** (CERIAS) for instructions and links to the schedule of upcoming presentations. http://www.cerias.purdue.edu/secsem/streaming.php

**Dataware™** http://www.datacircle.com/dataware.htm is an online mini-course that contains the most current and essential elements necessary in order to practice prudent data security, to help avoid security errors and proactively protect a company's information"

**DCI** http://www.dci.com/ offer a wide range of IT courses and symposia including a dozen dealing with security topics.

**George Mason University's Hyperlearning Center** http://cne.gmu.edu/ includes many valuable free Web-based courses; the course called "The Core of Information Technology" http://cne.gmu.edu/modules/itcore/ has modules on security at http://cne.gmu.edu/itcore/security/ that cover fundamentals, authentication, encryption, exchange transactions in ecommerce, and digital signatures.

**Global Information Assurance Certification** (GIAC) http://www.giac.org/ includes courses that are available for Web-based training. See also the home page, http://www.sans.org/newlook/home.htm for more pointers to SANS online training courses.

**Information Security University** - online security training services are described at http://www.infosecu.com

**MIS Training Institute** http://www.misti.com offers its courses not only at its conferences but also on-site for groups of employees.

**SECEDU** http://groups.yahoo.com/group/secedu is an informal moderated list run by Fred Cohen that caters to information security educators.

**Web-based Internet Security Education** (WISE) http://www.infosec.spectria.com/products/wise.htm from Rainbow Technologies includes courses on information security basics, PC & LAN security, Internet security, system server security, database security and preparation for the CISSP exam. The same organization offers a systematic approach to security awareness employees called SAFE (Security Awareness for All Employees) http://www.spectria.com/services/security.htm#wise

## INFOSEC Academic Programs – Outside the USA.

Many academic Institutions are now offering graduate and post-graduate degrees or diplomas in Information Security and Secure eCommerce:

**Algonquin College** in Ottawa, Canada http://www.algonquinc.on.ca/ has a one year full-time program for certification in information security http://www.algonquinc.on.ca/acad_menus/current/0445X1FWO.html#Program Description

**Cambridge University** in England offers the Computer Laboratory as the Computer Science departments research facility http://www.cl.cam.ac.uk/UoCCL/intro

**Georgian College of Applied Arts and Technology** in Barrie, Ontario Canada http://georgianc.on.ca/ has a residency and on-line program leading to a postgraduate diploma in cyberspace security. http://www.georgianc.on.ca/calendar/programs/B265.htm

**Royal Holloway (University of London)** (www.isg.rhbnc.ac.uk) The Information Security Group (ISG) offers an active research environment with ten established academic posts and a large number of research students, making it one of the largest academic security groups in the world. MSc. courses are offered in Information Security and in Secure Electronic Commerce.

**Queensland University Of Technology** (QUT) in Brisbane, Australia has an Information Security Research Centre http://www.isrc.qut.edu.au/ with strong ties to the AUSCERT (Australian Computer Emergency Response Team).

**Université d'Avignon** http://www.dess-e-com.univ-avignon.fr/ has an eCommerce course with three modules: information technology, commerce, and communication.

**Université de Bordeaux** http://www.math.u-bordeaux.fr/CCSI/ offers an engineer level diploma specialising in "Codes, Cryptology, and IT Security". Former studentsoften work in smartcard development, eCommerce, IT Security, electronic weaponry.

**University of Hamburg** http://www.informatik.uni-hamburg.de/ (in German) or http://www.informatik.uni-hamburg.de/welcome_eng.html (in English) is home to the Virus Test Center http://agn-www.informatik.uni-hamburg.de/vtc/naveng.htm under the direction of Prof. Klaus Brunnstein.

**Université Paris II** http://dup2.free.fr/ offers a diploma in eCommerce. Of the four modules one is Information Security related.

## INFOSEC/Information Assurance Academic Programs – USA based.

Centers Of Academic Excellence In Information Assurance Education as designated by the US National Security Agency (NSA); http://www.nsa.gov/isso/programs/coeiae/index.htm through the National INFOSEC Education and Training Program (NIETP).

As of March 2002, there are 36 universities designated as Centers of Academic Excellence in Information Assurance Education:

**Air Force Institute of Technology** – http://www.afit.edu/

**Carnegie Mellon University** http://www.heinz.cmu.edu/infosecurity/ Carnegie Mellon University in Pittsburgh, PA is home to the Software Engineering Institute (SEI) http://www.sei.cmu.edu/ and the Computer Emergency Response Team Coordination Center (CERT-CC) http://www.cert.org

**Drexel University** http://www.ece.drexel.edu/ECE/home.html

**Florida State University** http://www.cs.fsu.edu/infosec/in Tallahasee, FL has an Information Technology Assurance and Security initiative focusing on software reliability, information assurance, and computer and communications security.

**George Mason University** http://www.isse.gmu.edu/~csis/intro.html in Fairfax, VA offers an academic / commercial certification program related to the CISSP (Certified Information Systems Security Professional) certification managed by the International Information Systems Security Certification Consortium (ISC)2 .

**George Washington University** http://www.seas.gwu.edu/%7Einfosec/ in Washington, DC has graduate INFOSEC programs in its School of Engineering and Applied Sciences (SEAS)

**Georgia Institute of Technology** http://www.cc.gatech.edu/

**Idaho State University** http://www.isu.edu in Pocatello, ID has a Center of Excellence http://security.isu.edu/ in operation

**Indiana University of Pennsylvania** http://penguin.nsm.iup.edu/security/ia_center.htm

**Information Resources Management College of the National Defense University** http://www.ndu.edu/irmc/

**Iowa State University** http://www.issl.org/

**James Madison University** http://www.infosec.jmu.edu/ in Harrisonburg VA has a Master's program in INFOSEC that uses on-line distance learning

**Mississippi State University** http://www.cs.msstate.edu/~security/

**Naval Postgraduate School** http://cisr.nps.navy.mil/

**New Mexico Tech** http://www.cs.nmt.edu/page_home.html

**North Carolina State University** http://ecommerce.ncsu.edu/infosec/

**Northeastern University** http://www.northeastern.edu/

**Norwich University** http://www.norwich.edu/biz/cs/

**Polytechnic** http://isis.poly.edu/links/

**Purdue University** http://www.cs.purdue.edu/ West Lafayette, It has excellent undergraduate and graduate programs and research opportunities

**CERIAS/Perdue University** center for multidisciplinary research and education in areas of information security (computer security, network security, and communications security), and information assurance (www.cerias.purdue.edu)

**Stanford University** http://crypto.stanford.edu/seclab/ in Palo Alto, CA has a detailed calendar listing about its B.Sc., MSc. and Ph.D. programs in computer sciences, with courses in security and security-related topics. Also, see http://www.stanford.edu/group/tdr-security/master.html for a list of institutions offering higher educational courses and other resources in information security.

**State University of New York, Buffalo** http://www.cse.buffalo.edu/caeiae/

**State University of New York, Stony Brook** http://www.sunysb.edu/

**Syracuse University** http://www.csa.syr.edu/ Assurance---the correctness, reliability, availability, safety, and security of information and information infrastructures is crucial for the economic well being of commercial enterprise and national security

**Towson University** http://www.towson.edu/CAIT/award.html

**University of California at Davis** http://seclab.cs.ucdavis.edu/ has programs emphasizing identification and authentication research, and research and development in cryptology, cryptanalysis and public-key infrastructure

**University of Idaho** http://www.csds.uidaho.edu/ in Moscow, ID has a Certificate of Completion in Secure & Dependable Computing Systems

**University of Illinois at Urbana-Champaign** http://ciae.cs.uiuc.edu/

**University of Maryland, Baltimore County** http://www.cisa.umbc.edu/

**University of Maryland, University College** http://www.umuc.edu/

**University of Nebraska at Omaha** http://nucia.ist.unomaha.edu/

**University of North Carolina, Charlotte** http://www.sis.uncc.edu/LIISP/

**University of Texas, San Antonio** http://www.utsa.edu/

**University of Tulsa** http://www.cis.utulsa.edu/ has graduate programs in computer science with concentration in security.

**U.S. Military Academy, West Point** http://www.itoc.usma.edu/

**West Virginia University** http://www.lcsee.cemr.wvu.edu/

Top

# Security Awareness



## *Introduction*

Most international security standards treat security awareness as a fundamental requirement for supporting business operations. Although the coverage and scope may vary considerably, security awareness is a cornerstone of a successful eCommerce security framework.

A good Information Security Awareness program highlights the importance of information security and introduces Information Security Policies and Procedures in a simple yet effective way. The main objectives of the program are to:

- Communicate policies and instill understanding of the purpose behind them
- Communicate operational procedures and provide opportunities for testing
- Communicate the security aspects of eCommerce to customers

## *Awareness Program Success Factors*

To be effective, a Security Awareness Program should have the following characteristics:

- Alignment – it should be integrated with sound management and business practices.
- Commitment – all levels of management should support it. Commitment from the Executive Board should cascade down through all levels of management.
- Coordinated – it should be delivered consistently across the organization and will be most effective if managed by a single unit or group.
- Current – it should be kept up-to-date and relevant. Advisory documents (such as Do's & Don'ts Checklists) should be regularly re-evaluated in the light of the evolution of threats, company strategies, etc.
- Measurable – it should be possible to monitor and quantify the effectiveness of the awareness program through feedback, surveys or testing methods. It should be possible to use feedback to target awareness campaigns and improve poor results.
- Pervasive – it should reach everyone with access to the organization's information or information systems, such as customers, vendors, suppliers and third parties. Communication should be regular, using diverse media, such as email, intranet, newsletters, brochures and leaflets.

- Structured – subject material should be organized around key policies and procedures and presented in a logical way to build an information security culture within the organization. Opportunities for formal education or training programs with specialized awareness material should be available for those individuals with specialist roles. See Training.
- Supported – the program should be supported by security policies, standards, baseline security procedures, codes of conduct and reporting processes. Users should understand what the organization expects of them and any consequences of misuse of organizational assets. The organization should clearly state its approach to the monitoring of user activity and the collection, analysis and use of activity/filtering logs.
- Targeted – the program should be able to support the awareness or training requirements of specific roles with information security responsibilities. Security awareness and training should be able to overcome the perception that security policies are restrictive and interfere with the employee's ability to work effectively. It should also inform management about potential internal security threats.

## *Security Awareness Resources*

There are many resources available on the Internet offering a wide variety of materials that can be used to provide information security user awareness. Resources range from free downloads, screensavers and advisory notices to tailored newsletters, professional videos and courses.

### Free Resources

There are numerous resources available on the Internet but it is always advisable to check out the trustworthiness of such resources. Some of the better-known examples providing a general background on cyberculture and use of information technology resources are:

Microsoft offers two free security awareness screen savers: the Ten Immutable Laws of Security and the Ten Immutable Laws of Security Administration. http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26684

Cybercitizen Awareness Program is directed mainly at children and young adults but provides some useful background material.

http://www.cybercitizenship.org

SANS provides a reading room facility with articles and papers on security awareness. Access is free following registration.

http://rr.sans.org/index.php

## Vendors

Links to vendor sites are provided without any endorsement of the products on offer.

**Commonwealth Films** http://www.commonwealthfilms.com/infosec.htm have a wide variety of security awareness videos and CD-Rom presentations.

**Computer Security Institute** https://wow.mfi.com/csi/order/publications.html offers security awareness newsletters, security alerts and security assessment kits.

**Green Idea** http://www.greenidea.com offers a visual PC presentation/security awareness reminder tool.

**Interpact Inc.** http://www.interpactinc.com/home.html offers a variety of services including awareness programs, seminars, brochures, artwork, and others.

**Native Intelligence Inc.** http://www.nativeintelligence.com offer a variety of awareness services including tutorials, posters, screen savers, animations, and haikus to help educate users.

**Security Awareness Inc**. http://www.securityawareness.com has several offerings including tutorials, posters, screen savers, an awareness workshop, banners, and other educational tools

**Security Web Sites** http://www.securitywebsites.com offers a customizable website service, and awareness presentations.

**Spectria –** http://www.spectria.com/safe/index.html offers a web-based product that publishes, educates and tracks employee security awareness by combining the organizations' specific policies with general security practices.

**Top**

# Compliance



The design, operation, use and management of ecommerce systems is likely to be subject to a range of statutory, regulatory and contractual security requirements. Advice on specific legal requirements should therefore be sought from the organization's legal advisers or suitably qualified legal practitioners at the earliest possible stage in the development of an eCommerce system.

## *Why Compliance is an Issue for ecommerce*

To summarize, the purpose of compliance is to:

- avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements;
- ensure compliance of systems with organizational security policies and standards; and
- maximize the effectiveness of and to minimize interference to/from the system audit process.

eCommerce systems are designed to operate across organization boundaries and across national borders. Legislative requirements vary from country to country and for information created in one country that is transmitted to another country (trans-border data flow). Legislation governing eCommerce is still in its infancy and is likely to be subject to continuous change for many years to come. These factors present a new set of risks that are difficult to identify and assess, and dynamic in nature. It is also unlikely that business managers and development staff will be aware of the existence and consequences of the full range of risks. An effective compliance structure should ensure that management and staff are aware of the nature and range of legal, regulatory and contractual requirements associated with the deployment of eCommerce systems, and that adequate controls are in place to assess and manage the resultant risks.

## *Compliance Considerations*

Compliance requirements to consider include the following:

- Intellectual Property Rights.
- Safeguarding of records.
- Data Protection and Privacy.
- Prevention of misuse of IT facilities.

- Regulation of cryptographic controls.
- Collection of evidence.
- Organization Compliance.

This is a list of the most general types of compliance requirement that are likely to affect the design and deployment of eCommerce systems. Other legal requirements, e.g. governing distance selling or consumer rights, are likely to exist in many countries. Appropriate legal advice should therefore be taken to identify the full range of considerations that may apply.

## Intellectual property rights

Appropriate procedures should be in place to prevent infringements of copyright, design rights and trademarks, and to ensure compliance with software licenses. It is prudent to publish a software copyright compliance policy, to establish strict controls over the acquisition of new software products, to restrict unauthorized copying of software, and to maintain registers of such assets, as well as proof of ownership of licenses. Regular audits should be carried out to ensure continuing compliance with the policy.

## Safeguarding of records

Consideration should be given to legal or regulatory requirements to retain documents for specific periods.

Records of transactions and audit logs should be maintained in a secure fashion using an appropriate media to safeguard the records from loss, destruction and falsification.

## Data protection and privacy

Many countries have now introduced legislation placing controls on the processing and transmission of data on living individuals who can be identified from that information. These controls may impose duties on those collecting, processing and disseminating personal information, and may restrict the ability to transfer that data to other countries. Compliance with data protection legislation requires an appropriate management structure with senior-level oversight, the adoption of a set of principles governing the handling of personal data, and an education program to ensure management and staff are fully aware of their obligations. Policy statements should be published on Websites to inform customers of the practices used by the organization in processing customer information.

## Prevention of misuse of IT facilities

Organizations should establish appropriate controls to prevent unauthorized use of facilities by internal staff or customers for non-business purposes. Many countries have or are in the process of introducing legislation to protect against computer misuse. Appropriate warning messages to individuals logging on to private systems should be considered. Care should be taken to ensure that any monitoring activity, designed to detect unauthorized use of facilities, meets local legal requirements.

## Regulation of cryptographic controls

Cryptography is used extensively in eCommerce to authenticate individuals and to safeguard the confidentiality of transactions passing across public infrastructure. Some countries have implemented agreements, laws or other instruments to control the access to or use of cryptographic controls. These controls may restrict the import, export or use of computer hardware and software for performing cryptographic functions. Legal advice should be sought before deploying such technology, especially if it is planned to transmit or move encrypted information or cryptographic systems to another country.

## Collection of evidence

In the event of an incident resulting in a prosecution or disciplinary action against an individual, it will be necessary to produce adequate, perhaps admissible evidence. In eCommerce, there is a danger that the necessary evidence might be erased or destroyed before the seriousness of the incident is realized. Information systems should therefore comply with published standards or codes of practice for the production of admissible evidence. Amongst other things, it will require that a strong evidence trail is established, with original paper documents kept securely with details of who found it, where it was found and who witnessed the discovery. And with secure logs of all actions taken during the copying of any electronic documents.

It is always advisable to check with local law enforcement agencies and legal counsel for the proper handling of evidence because this can vary from country to country.

## Organization compliance

Appropriate processes should be established to ensure that the organization's operating practices continue to comply with the above requirements and with internal policy and standards. A competent, independent body should carry out regular reviews. In practice, this will need to be done at a number of levels to address the different levels of scope, detail and technical content associated with reviews of information systems, infrastructure, service providers, management and users. Special care should be taken to control the use of powerful audit or testing tools that may be used to enable unauthorized access to critical systems or sensitive data.

**Top**

# eContinuity



## *Introduction*

eCommerce grew out of:

- the use of email to place orders and raise queries;
- electronic publishing to advertise products and services;
- EDI (electronic data interchange) enabling customers to place orders electronically and access databases containing account information and history.

Over the last ten to fifteen years many organizations have migrated those business applications from mainframe legacy systems across to distributed LAN and WAN environments and then into eBusiness environments.

This migration has introduced a much higher level of operational risk, in which significant financial loss can occur within hours of a service interruption. The diminishing tolerance for service outages and drastically reduced recovery time is driving organizations towards high availability solutions and eContinuity planning.

## *What is eContinuity?*

The risks inherent in this environment are driving a new approach in Business Continuity Planning, where the distinction normally drawn between traditional IT Disaster Recovery processes and day-day operational recovery processes is becoming less distinct. The management disciplines that support day-to-day operational recovery need to be considered when eContinuity planning. These are:

- Enterprise High Availability.
- Service Level Management.
- Business Continuity Planning.

### Enterprise High Availability

An organization dependant on its Internet presence has a lot to lose. The cost of failure is linked to loss of customer loyalty, loss of market share and an undermining of stakeholder confidence. The challenge therefore is to underpin the availability of the Internet presence.

The goal is to achieve and maintain 99.999% (the five nines) availability of the organization's eCommerce infrastructure. This difficult target can only be attained by addressing the following aspects of information technology:

- data storage management;
- network management;
- platform and hardware;
- applications and software management;
- facilities management.

## Service Level Management

Building an appropriate technology infrastructure is a good foundation but there must also be robust management practices in place. Downtime is more often related to people or processes than to IT.
Deploying robust management practices will:

- extend the useful life of the infrastructure;
- facilitate the introduction of new technology when required;
- facilitate modifications to technology;
- improve quality assurance;
- reduce the time to market;
- avoid software failure and avoid downtime;
- facilitate the 24 x 7 operation.

Service Levels will also address performance related issues such as:

- reasonable and constant service response times;
- consistent quality and richness of content;
- consistent quality of customer service;
- capacity planning - particularly during periods of growth.

## Business Continuity Planning

Business Continuity Planning (BCP) is the traditional approach to minimizing the downtime of key business processes in the event of major disruption. BCP is sometimes referred to as "Disaster Recovery" but this is only a small aspect of BCP and there is much more involved in the overall planning process.

To ensure that normal service can be resumed in the shortest possible timescales it is essential that plans address:

- the further reduction of overall risk following the implementation of Enterprise Availability and Service Level Management;
- implementation and testing of the emergency response procedures;
- the updating of the business continuity plan following testing of procedures or changes to business process, structure, technology and personnel;
- personnel training requirements;
- administration and review of the plans.

## *Links*

There are many suppliers and service providers who will be pleased to support the continuity of your eCommerce business. Most of these advertise services and solutions on the internet.

There also many organizations providing information sources relating to business continuity. The following links are provided without any recommendation from the Universal Postal Union:

**The Business Continuity Institute** http://www.thebci.org promotes the art and science of business continuity management. The website has a wealth of information, most of which requires membership for access.

**Survive, The Business Continuity Group** http://www.survive.com is an international, industry-wide user group for business continuity planning and disaster recovery professionals. The website provides a comprehensive, international listing of vendors.

**Global Continuity** http://www.globalcontinuity.com/ provides a wealth of online resources plus a personalized newsletter delivered by email to your desktop.

**Advisor, Technology Know-How** http://e-commerceadvisor.com/ is a source of publications and articles, as well as providing information about conferences, training etc. The site also hosts the *e-Business & Security Advisor Forum*

**Top**

# Information Privacy

Security concerns are often cited as a major barrier for consumers who are cautious about participating in eCommerce. Repeated polls have shown that many consumers are concerned primarily about the confidentiality of personal information.

To earn their customers' trust and repeat business, eCommerce businesses may place greater emphasis on protecting privacy. It may also be likely that governments will enact laws to regulate privacy on the Internet.



## *What are the Privacy Issues?*

According to survey data 92% of consumers are concerned (67% are "very concerned") about the misuse of their personal information online (http://www.ftc.gov/reports/privacy2000/privacy2000.pdf). Consumer apprehension about the misuse of personal information precludes their use of the Internet to make purchases. One study estimates loss of online sales revenue to be as much as $2.8 billion in1999 because of privacy concerns.

Consumers are primarily concerned about four privacy issues:

- When one's information will be used, by whom and for what purposes.
- Choice about whether or not to volunteer one's personal information.
- Ability to access one's information to perform corrections and /or updates.
- Protection of their information from third parties who may steal it for unauthorized purposes.

A report released by the Pew Internet & American Life Project 2 studied the public's views on online privacy. The report found that the public shares two common views:

- Internet users want a guarantee of online privacy.
- Many consumers are not versed on how privacy invasions occur and what technological solutions are available to prevent them.

## *Regulation or Self-Regulation*

The international debate on whether regulation or self-regulation should be applied to protect individual rights of privacy is ongoing.

In the United States, the approach to protecting the privacy of personal information is through a mix of legislation, regulation and self-regulation without government intrusion, whilst in Europe a legislative approach resulted in the "Directive on Data Protection", which became effective on October 25, 1998.

The European Directive has two basic objectives:

- To protect individuals with respect to the "processing" of personal information (defined as information relating to an identified or identifiable natural person)
- To ensure the free flow of personal information within the European Union through the coordination of national laws.

The United States has not enacted similar, comprehensive privacy legislation, which could have significantly hampered the ability of U.S. companies to engage in many trans-Atlantic transactions. To bridge the gap between the two approaches the U.S. Department of Commerce, in consultation with the European Commission, developed The Safe Harbor Accord. This arrangement is designed to allow U.S. organizations to comply with the requirements of the European Directive on Data Protection for transfers of data to third countries and to ensure that data flows are not interrupted.
For more information on The Safe Accord follow these links:

- US Department of Commerce http://www.exports.gov/safeharbor
- European Union: http://europa.eu.int/comm/external_relations/us/summit_05_00/statement_data_privacy.htm

## *Privacy Initiatives*

### Platform for Privacy Preferences Project (P3P)

P3P is a standard developed by the World Wide Web Consortium to provide an automated way for users to express their privacy preferences through their browsers.

P3P is a standardised set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P enhances user control by putting privacy policies where users can find them, in a form that they can understand and, most importantly in a way that enables users to act on what they see.

P3P on the World Wide Web Consortium website: http://www.w3.org/P3P

## OECD Online Privacy Generator

The Organization for Economic Cooperation and Development (OECD) is an international organization helping governments tackle the economic, social and governance challenges of a globalized economy.

The OECD has developed Privacy Guidelines and an Online Privacy Generator (endorsed by the OECD's 29 member countries) to help organizations develop online privacy policies and statements for display on the Web sites.

The OECD Privacy Policy Statement Generator was developed in cooperation with industry, privacy experts and consumer organizations. The Generator offers guidance on compliance with the OECD Privacy Guidelines and helps organizations develop privacy policies and statements for display on their web sites. The Generator has been made freely available online, in order to:

- Foster awareness of privacy issues amongst web site owners.
- Increase awareness among visitors about privacy practices on the websites that they browse.
- Encourage user and consumer trust in global networks and eCommerce.

OECD Privacy Generator website http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm

## Privacy Seal Programs

Privacy seal programs allow organizations to signify to consumers that the owner or operator of a Web site has adopted a privacy policy that meets the standards of good practice for protecting customer data.

Examples of third-party certification services that examine the privacy policies of Websites are: WebTrust, CA WebTrust, TRUSTe www.truste.org/, BBBOnline http://www.bbbonline.org/

# *Legislation*

## United States Legislation

The Federal Trade Commission (FTC) has enforcement authority over deceptive practices both online and offline in the United States. Failure to follow publicly stated privacy policies can be a deceptive practice. Companies that do not tell the truth about how they are using personal information may be charged by the FTC.

In May 2000, the FTC recommended congressional action to protect consumer online privacy. The FTC's 2000 Survey targeted a random sample of all Web sites with at least 39,000 unique monthly visitors. The results showed that only 20 percent of the sites had implemented all four widely accepted fair information practices; notice, choice, access, and security.

Legislative solutions have been implemented for sensitive areas including financial and medical records, genetic information, Social Security numbers, and information involving children. The following laws have been enacted to regulate privacy for highly sensitive information:

- Children's Online Privacy Protection Act requires sites aimed at children to get verifiable parental consent before they gather and use personal information received from children under 13.
- Health Insurance Portability and Accountability Act of 1996 provides a baseline of legal protection for sensitive medical records.
- The Gramm-Leach-Bliley Act (GLB) requires financial institutions to give notice of their privacy policies and a way for consumers to "opt-out" of some their information-sharing practices.

## European Legislation

Since the 1970's, several Member states of the European Union have passed legislation protecting the fundamental rights of individuals and in particular, their right to privacy from abuses resulting from the processing. International institutions such as the United Nations, the Organization for Economic Cooperation and Development (OECD) and the Council of Europe have all produced legal texts addressing these issues. In 1981, a Council of Europe convention (Treaty 108) established the basic principles regarding the protection of individuals with regard to the processing of personal data, which can be found in all data protection laws in Europe.

In 1995, The European Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data was issued, requiring all Member states to pass legislation on Data Protection effective from 25th October 1998.

Subsequently the fifteen member states have passed or are in the process of implementing national legislation to meet the Directive. Examples of the legislation may be found on the EU website:
http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm

## *Privacy Links*

### International Privacy Legislation Links

| Country | Function |
|---|---|
| Australia | Privacy Commissioner - Data protection, privacy laws and business, department for Australia. |
| Austria | Datenschutzkommission - Austrian Data Protection Commission. |
| Belgium | President - Consultative Commission for Protection of Privacy. |
| Canada | Privacy Commissioner for federal institutions. |
| Czech Republic | The Office for Personal Data Protection |
| Denmark | Datatilsynet - Danish Data Protection Agency. |
| Estonia | Estonia Data Protection Authority. |
| Finland | Data Protection Ombudsman - Data protection commission for Finland. |
| France | President - National Commission for Freedom of Information. |
| Germany | German Federal Privacy Commissioner. |
| Greece | The Greek Data Protection Authority. |
| Guernsey | The Data Protection Commissioner - site includes up-to-date news and guidance notes |
| Hong Kong | Privacy Commissioner - Office of the Privacy Commissioner for Personal Data (PCO). |
| Ireland | The Irish Data Protection Commissioner |
| Isle of Man | Data Protection Registrar - Information and guidance about Data Protection for those operating within the Isle of Man's jurisdiction. |
| Italy | The Italian Data Protection Authority. |
| Lithuania | Lithuania's Data Protection Inspectorate. |
| Netherlands | Registratiekamer - Data protection/privacy commission for the Netherlands. |
| New Zealand | Privacy Commissioner - Data protection/privacy commission for New Zealand. |
| Norway | Datatilsynet - Norwegian office for data protection. |
| Portugal | Comissao Nacional de Proteccao de Dados - Data protection commission for Portugal |
| Spain | Agencia de Protection de Datos - Data protection commission for Spain. |
| Sweden | Datainspektionen - Data protection commission for Sweden. |
| Switzerland | Data Protection Commission - Data protection/privacy commission for Switzerland. |
| United Kingdom | Office of the United Kingdom's Information Commissioner. |

**Top**