The relevance of legal awareness in e-commerce security

Received (in revised form: 8th December, 2000)

Debbie Williams
Debbie Williams is a qualified barrister, who is employed by Claritas Information Security Limited as a consultant offering advice to clients on information security. She is responsible for conducting risk assessments, policy formulation, audit and reviews of procedures, education and training of users and business continuity planning. As a barrister she practised in a common law chambers, where she advised and represented people on a wide variety of legal issues such as crime, employment, contractual, family, property and personal injury claims.

Abstract The aim of this paper is to provide a simple overview of the legal implications of security in e-commerce. It is targeted at those with little or no knowledge of such issues. The benefits of legal awareness in e-commerce security are considered as they apply to different areas of relevant law. The areas considered are contract, employment, crime, negligence, data protection and privacy. The specific legal issues within each area are identified in terms of relevance to e-commerce security. Practical solutions are offered, where possible, to enable resolution and management of issues.

INTRODUCTION
Knowledge of the law is an important element of e-commerce security. It is beneficial to organisations as they can identify responsibilities and liabilities, ensure compliance and provide for risk reduction. Technical solutions are, however, often seen to dominate other security management solutions. Reliance on technical remedies can be an inadequate approach as illustrated by problems encountered by Powergen and Barclays. These organisations failed to incorporate a balanced set of security measures.

The key issues that ought to be understood and addressed by organisations will follow. These issues are considered in terms of their relevance to the law of contract, employment, negligence, crime, data protection and privacy. Other specific legal issues may need to be dealt with by organisations that are not covered in this paper, thus it must be emphasised that this paper is only intended to provide a general overview of the issues and when in doubt specialist advice should be sought.

CONTRACT
It may be that a firm is contractually bound to include security on its website for e-commerce transactions. It is useful to establish what security issues to be aware of, how they apply and what they necessitate. By undertaking this analysis, a firm will be better prepared when it comes to establishing what is necessary in a contract.

Inclusion of the security measures in a contract make it easier to identify responsibilities. This information could enable a firm to be better prepared in the event of a breach of the security
requirements and it might lead to a reduced likelihood of lengthy legal conflicts.

Besides security features, there are other important terms that need to be included in the contract, such as contract formation, delivery, price, liability, geographical and legal limitations. These terms must be displayed clearly. It is also necessary to obtain acceptance of these terms by getting customers to click and tick a designated box.

Providing details about contract formation is beneficial. A firm and its customers need to know when a contract becomes legally binding. Contracts may be worthless if it is unclear as to when an offer and acceptance arise. Consider the following example:

A customer saw an advert on Careless.Co’s website for custom-made clocks that could be ordered on-line. He wanted a clock so he made an offer to purchase a clock using Careless.Co’s ordering facility. A few days passed and as the customer had not heard from Careless.Co, he assumed that they did not want his custom, so he purchased a clock elsewhere. The next day, however, the custom-made clock from Careless.Co was delivered with an invoice. The customer refused to accept the clock as he claimed no contract was formed.

For a contract to be formed there must be an offer, acceptance, the intention to be legally bound and some form of consideration (payment). Careless.Co’s website was badly made because it did not provide purchasing facilities and details about the terms of the contract.

Care should be taken when advertising using e-commerce facilities. Mistakes can easily be made when products are offered for sale using websites, as Argos found to their detriment when televisions were mistakenly offered for sale at £2,99 each. It ought to be made clear whether adverts represent an ‘invitation to treat’ or an ‘offer’. If it represents an ‘invitation to treat’ then a contract will not necessarily result. If, however, it is an offer, then acceptance may result in formation of the contract.

Firms must also be aware that if an advert constitutes an offer then the firm is obliged to supply the quantity ordered. This could cause problems for companies like Careless.Co if they receive an order for a million clocks and do not have the stock to meet such demand.

There are restrictions as to the type of contracts that can be formed using e-commerce. This facility cannot be used if the contract must be by deed or in writing. Sometimes a signature may be required for the contract to be valid, if this is the case, then the Electronic Communications Act 2000 may enable the firm to contract using electronic signatures.

It is advisable to consider the UK’s obligation to comply with the requirements of EC Directives such as the E-commerce Directive on certain legal aspects of information society services. The aim of this Directive is to clarify the regulatory framework and safeguard the rights of users of e-commerce. It is due to be incorporated into UK legislation within a year.

It may be that a firm wishes to trade globally. If so, it is necessary to identify whether there are jurisdictional legal differences. It might be that certain acts are legal in one country and not in another. Therefore it is advisable to identify a target market and specify which countries it is possible to trade with. It is equally important to act with vigilance when purchasing from another country, in order to check that sufficient safeguards exist in the event of problems occurring.

In the UK legal protection is offered to contracting parties. Firms therefore
need to be aware of their rights and responsibilities. Liability for everything can not be excluded, no matter how strong the firm's bargaining position. Death and personal injury resulting from the sale of defective goods can never be excluded or restricted. The ability to limit liability in consumer transactions is restricted by legislation such as the Sale of Goods Act 1994, which provides for implied terms requiring goods be of satisfactory quality and fit for their purpose.

Additionally, in the UK liability can only be limited by using reasonable exclusion clauses. The Unfair Contracts Terms Act 1977 states that a term in a contract is reasonable if it is fair and it was in the contemplation of the parties when the contract was made. Other matters to consider in relation to exclusion of liability are:

- the relative bargaining power of the parties, which may exist if one party is in a stronger position than the other
- whether it is reasonably practicable to obtain advice from an alternative source
- the difficulty and dangerousness of the task to be undertaken, i.e. the risk
- the practical consequences of the court's decision, the ability of the parties to bear the losses involved and the availability of insurance.

Rights and responsibilities are more easily communicated if contract contents are comprehensive, clear and easily identifiable to the consumer. It is not advisable to neglect putting contract terms on a website just because space is limited or the terms look dull.

**EMPLOYMENT**

Employees may pose risks to an organisation when they act without the appropriate authority when contracts are negotiated or when they gain access to information without authority. It may be that an employee's unauthorised actions occur accidentally and are non-malicious — various levels of damage can, however, result. For example, contracts may be formed which are costly to an organisation and confidential information may be carelessly revealed to a competitor by an employee accidentally gaining access to details on a restricted access database.

Guidance and training should be given to employees on their rights and responsibilities. This should contribute to an organisation's ability to provide secure e-commerce transactions. Clear guidelines should be provided to employees on the extent of their ability to conduct transactions and their access rights. Such guidelines should reduce accidental or intentional alterations to contracts, websites or other company property.

Organisations should act cautiously in relation to material that employees can view via internal and external communication systems. It may be necessary to create a communications or e-mail policy. It may be decided that monitoring of communications is essential to ensure that business processes are being carried out properly and to prevent and detect crime. Such a policy must not contravene the Human Rights Act 1998 and should be in accordance with the requirements of the Regulation of Investigatory Powers Act 2000. For example, a financial institution had been susceptible to employee crime. As a matter of practice the directors ensured that every potential employee was aware of the company's intolerance of such behaviour, which would result in dismissal for gross misconduct. Employees and customers knew that periodic checks were made of communications to ensure that illegal activities were stamped out.
During a check it was discovered that a male employee had been harassing fellow employees and customers by sending threatening and offensive messages. The managing director was worried about such behaviour as she was 'vicariously' liable for employee actions. Company policy stated that such behaviour would result in dismissal, so, after following the appropriate employment law procedures, the employee was dismissed. The employee attempted to claim that his right to privacy (a right that exists by virtue of Article 8 of the Human Rights Act 1998) was contravened. It was argued successfully, however, that this right was waived as he had impliedly consented to have his communications monitored by commencing employment, where he was forewarned of the procedures. In addition, the institution were exercising their right to intercept communications for the purpose of monitoring or keeping a record of communications as allowed by virtue of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations implemented under s.4(2) of the Regulation of Investigatory Powers Act 2000.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations should make it easier for an organisation to maintain essential records of transactions and other communications conducted by electronic means such as telephone or e-mail. For the Regulations to apply certain conditions need to be satisfied, eg:

- the consent of the system controller has been given
- the communication is made in connection with the carrying on of any business
- monitoring or keeping a record of transactions is required to ensure: the existence of facts; compliance with business regulatory or self-regulatory practices; national security; the prevention or detection of crime; or effective operation of the system.

Consent must, however, be obtained from the sender or receiver of e-mails, if interception is conducted for reasons other than those provided for in the Regulations. Acting contrary to the Regulations may result in an offence being committed under the Regulation of Investigatory Powers Act.

The Department of Trade and Industry have, however, stressed that these regulations do not necessarily comply with the Data Protection Act 1998 and the Human Rights Act 1998. Therefore there may be an element of legal conflict in relation to the processes that an organisation decides to use. It is not clear which rules will prevail. By communicating an agreed coherent e-mail policy to an organisation, the likelihood of related legal problems arising should be reduced.

The draft code of practice released by the Data Protection Commissioner in October 2000 may provide some guidance in relation to monitoring communications, such as e-mails and Internet access. It is worth remembering that this is only a draft code and it may change. The code reflects the Commissioner’s views of good practice requirements and recommendations. In relation to monitoring e-mails and Internet access the code provides for the communication of such standards as:

- ensuring that employees are clearly aware which e-mails will be read at work
- informing employees whether e-mails will be read in their absence
- providing employees with the reasons
for monitoring, eg to ensure the business responds properly to its customers.

CRIME
Failure to conduct secure e-commerce transactions can result in an organisation being criminally liable or a victim of crime. Criminal liability can arise by failure to comply with legislation such as the Data Protection Act 1998, the Computer Misuse Act 1990 or pornography-related legislation. Alternatively, an organisation might become a victim of crime by virtue of the same legislation.

It is important that an organisation or its employees do not contravene criminal law. The criminal actions of employees may lead to the prosecution and possible imprisonment of the employer. An organisation needs to appreciate that an employer is vicariously liable, that is responsible, for the actions of its employees. Informing employees that criminal behaviour is not tolerated and that periodic checks will be made is one way of ensuring that a firm’s business practices are lawful.

There are many different criminal activities that could be encountered in e-commerce transactions:

- fraud
- theft
- damage from the introduction of malicious software
- hacker-manipulated and changed data.

Protective measures must therefore be adequate to deal with the different types of criminal behaviour.

It is unlikely that all criminal acts can be prevented. Criminal activity can, however, be managed more effectively by generating awareness of the relevant legislation. This knowledge should reduce a firm’s potential exposure to criminal liability and activity.

NEGLIGENCE
There is a potential for failure to conduct secure e-commerce transactions to result in liability for negligence. Negligence arises when a duty of care is owed by one party to another, who may not be party to a contract. A breach occurs from failure to maintain this duty of care and if damage results from this breach, the firm will be liable.

In general, for a duty of care to arise certain elements need to exist, such as foreseeability, proximity, and that it is fair, just and reasonable to expect a duty of care. It is possible that individuals other than parties to an e-commerce contract will suffer damage. For example, the manager of a hospital information security system, carried out a risk assessment of the system. He identified that there was a need to consider the threats from negligence, such as the disclosure of information relating to the treatment of patients, which if leaked could cause harm to families and/or friends of patients. As a result of the risk assessment, the manager conducted a risk management exercise and implemented controls that would reduce the chances of such information being accessible, by using techniques such as access authorisation. In this way he reduced the risk of legal action for negligence.

It is advisable that care is taken to ensure that people other than those subject to a contract are suitably considered. Liability for negligence can be reduced or prevented by establishing the potential duties of care to others and implementing measures to prevent breaches.
DATA PROTECTION AND PRIVACY

Failure to provide security measures ensuring data protection and privacy may lead to action being brought against an organisation by the Data Protection Commissioner, resulting in large financial penalties being imposed. It is important to comply with legislation such as the Data Protection Act 1998 and the Human Rights Act 1998, as failure to do so can result in criminal or civil liability.

The Data Protection Act gives effect to eight principles of good practice, requiring that personal data in the UK be:

— processed fairly and lawfully
— obtained for specific and lawful purposes and not further processed in ways incompatible with those purposes
— relevant and not excessive
— accurate and kept up to date
— kept for no longer than necessary
— processed in accordance with the rights of data subjects
— protected by adequate security
— transferred to countries outside the European Economic Area only if adequate protection is available.

The Human Rights Act, among other things, requires that an individual's privacy is respected (Art. 8) and that an individual has the right to protection of property (Art. 1 of the First Protocol). These particular requirements of the Human Rights Act should be of concern, as security infringements could lead to breaches of these rights. This could result in an award of damages being made to the aggrieved party.

Security is paramount to ensure compliance with legislation. According to the Data Protection Act an organisation could be prosecuted for failure to maintain the appropriate security measures, which require consideration of:

— technological developments, such as encryption and firewalls, and implementation costs relative to the harm that might result from a breach of security
— organisational measures, such as contracts with Internet Service Providers
— the nature of the data to be protected
— the reliability of staff with access to the personal data.

In November 1997, the Data Protection Registrar recommended in a consultation article on information security that a risk-based approach to determining the standard of security be undertaken. Reference was further made to British Standard (BS) 7799, which is the Code of Practice for Information Security Management.

Adoption of BS 7799 should provide a guideline by which to develop, implement and measure effective information security management. It makes reference to the need for a risk assessment, security controls and legal and technical compliance. It acknowledges the legal significance of security in relation to data protection and privacy. It further stresses the need for regular IT health checks to ensure technical compliance.

Other legislation that may be relevant in terms of privacy is the Regulation of Investigatory Powers Act. This Act requires care to be exercised in relation to monitoring communications and using encryption. It attempts to ensure that the relevant investigatory powers are used in accordance with human rights. Surveillance techniques used by the authorities are regulated to ensure that the public is safeguarded from unnecessary invasion of their privacy. Refusal to comply could result in imprisonment.

A problem may exist, however, for those subject to the requirements of the
Data Protection Act, as there is a conflict between the Regulation of Investigatory Powers Act and the Data Protection Act. A requirement of the Data Protection Act is that information should not be retained for longer than is strictly necessary, whereas the Regulation of Investigatory Powers Act requires the delivery of information upon request. There are no guidelines of the procedures to adopt should this situation occur, although it is likely that a commonsense approach would consider the:

— individual circumstances of the case
— nature of the information held
— reasonable expectation that such information should be retained.

It is unlikely that a prosecution would instantly follow from a breach, as the Data Protection Commissioner is likely to forgive such actions if the organisation:

— accepts there has been a breach
— identifies the problem
— provides formal assurances of procedures to ensure it does not happen again.

An organisation is, however, more likely to benefit from taking steps to ensure initial compliance, as complaints or action as a result of data protection infringements may also damage the reputation of the organisation.

SUMMARY
It is important and beneficial to be aware of the law in relation to e-commerce security. Responsibilities and obligations can be more easily identified and set out, and customers can be made aware of their rights. These factors should enhance the reputation and credibility of an organisation. It provides the opportunity to implement risk reduction measures by:

— generating clear and comprehensive contracts
— assessing and managing exposure to crime, by awareness of criminal liabilities and activities
— providing guidelines as to employee rights and responsibilities.

Such risk reduction techniques should ensure compliance with legislation and assist in the discharge of duties and responsibilities. Failure to reduce or eliminate the likelihood of liability could result in imprisonment and large financial penalties.

©Claris Information Security Limited 2000