White Paper

Bloor

EU compliance and regulations for the IT security professional

A White Paper by Bloor Research
Author : Nigel Stanley
Publish date : March 2009

Clearly, and quite rightly, data loss is now a legal issue and IT professionals need to be aware of their responsibilities.

Nigel Stanley

Executive summary

The protection of data as it rests, transacts or journeys through computer systems is seen as a major component of good corporate hygiene. As well as protecting organisations from reputational risk and damaging losses, failure to protect this data can now result in both corporate and personal criminal prosecutions.

The growth of compliance requirements over the past few years has sometimes been seen as a US-based phenomenon as regulations are implemented to address various corporate failures and scandals over the past decade or so. In fact, compliance, rules and regulations to protect data stored by EU-based organisations can be just as onerous as those originating from the US.

This paper highlights key directives and legislation as it affects the member states of the EU.

Data loss prevention technologies are becoming increasingly important as organisations face up to the consequences of unintended data loss. A data loss incident is no longer seen as an unfortunate accident; now it will be accompanied by significant reputational risk and the possibility of legal action against the organisation or, even, executives personally.

Clearly, and quite rightly, data loss is now a legal issue and IT professionals need to be aware of their responsibilities.

Objectives of this paper

This paper highlights key directives and legislation within the European Union that have an impact on IT security practitioners, IT managers and others with responsibility for IT systems.

Legislation is vast and constantly changing. This paper is not designed to be an exhaustive review of every law and directive applicable across the EU and is not to be construed as legal advice. Where appropriate national legislation has been highlighted as it applies to the larger members of the EU.

By reading this paper, IT security practitioners, IT managers and others will gain an awareness of legal factors that affect them today. It is strongly advised that any organisation requiring further explanations or details of appropriate legislation consult qualified legal practitioners.

Introduction to European compliance issues

The EU, or European Union, currently comprises 27 member states. It was established following the Maastricht treaty in 1993, which renewed the union originally called the European Economic Community, or EEC. The EU generates approximately 30% of worldwide GDP and has around 500 million citizens.

The EU has developed a system of laws that apply to the movement of goods and people and the creation of a single trading entity. Each member state is subject to both EU and their own locally created national laws. There are countries that form part of Europe geographically but do not have membership of the EU, for example Switzerland. These countries are therefore not subject to EU-based legislation.

As part of its remit, the EU has created business related compliance and regulatory requirements, including laws that cover the safekeeping and management of data in computer systems. Failure to comply with these laws can result in criminal proceedings and prosecutions, so any organisation operating in the EU needs to take such laws as seriously as those developed nationally. It must be noted that laws are enacted at an individual member state level, which in itself has created problems, as inconsistencies have appeared causing problems for organisations acting across borders.

European Union compliance structure

When considering EU law it is important to understand the structure of the EU and how laws are enacted.

The EU Council represents national governments and is a council of ministers run by a 6-month rotating presidency. National ministers attend meetings as appropriate to their portfolio. The European Parliament is elected every five years by citizens of the member states. Members of the European Parliament have geographically-based constituencies that are generally larger than those for members of a national parliament.

The European Commission acts as a civil service and drafts new laws, which are passed to the European Parliament for discussion and enactment. The EU is based on a rule of law, which is laid down in a series of treaties and directives. These then become a collective legislative act of the EU, which are then enacted in member's state laws. If a member state fails to enact a suitable law then action can be taken against that state in the European Courts of Justice, which is the judicial institution of the Community.

The business benefits of compliance

Running any type of organisation can be complex and time consuming, and pressures exist every day to generate more profits by marketing and selling goods. IT is a business enabler and, as such, needs to be present to help an organisation make money, save time or save money. If an IT system fails to meet one of these objectives then its role, broadly, needs to be reconsidered. In the past IT security was placed a long way down the list of business priorities and it is only in the past few years of internet enablement that the sheer scale of data security violations has been acknowledged.

Compliance and regulatory requirements do place a pressure on IT professionals that is often interpreted as a distraction from their core business. In reality, adhering to a compliance or regulatory framework can enhance a business as policies and procedures can be formalised and security of data and other assets preserved.

The risks of poor IT compliance and security failures

Failing to adhere to an IT security compliance requirement probably means that organisational data is at risk of leakage. Before the proliferation of the PC, data leaks were unheard of outside the scope of targeted espionage as the systems needed to read stolen data were so specialised. Now anyone can read terabytes of corporate data at home on their own PC. Data can leak from an organisation via two routes: the incompetent and non-malicious and the competent and malicious route. The former occurs when data is accidentally emailed, copied, discarded or otherwise incompetently lost. The latter occurs when deliberate data theft is carried out by a suitably trained and motivated individual.

Brand and business reputation

An organisation's reputation is now a vital part of its marketing mix and, as such, needs to be protected as much as any other core company property. In the past, scares such as contaminated products could be dealt with relatively quickly by removing products from shop shelves. Now data leaks are far more personal as millions of confidential customer records can be leaked in seconds. Such a personal affront will create a lot of disharmony in a customer base, and needs to be prevented as a matter of urgency.

Costs

The costs of recovering from a data leak incident have been well publicised in a number of reports. Disclosure rules now exist in some US states, so that if personal data has been leaked then the organisation concerned is legally obliged to inform those potentially affected. There are ongoing discussions across the EU, both nationally and at a European level, to determine if such legislation should be implemented in this region.

Corporate responsibility

Non-compliance can inhibit an organisation trying to achieve funding or a possible sale. During a due diligence process, non-compliance will rapidly be uncovered leading to discussions concerning the overall management of the business and the hunt for additional problem areas. The knock-on effect to corporate valuations and exit multiples can have a direct, profound affect on the principals.

Security policies, reviewed and validated regularly, should now form the backbone of any IT strategy. Compliance requirements have at their heart the protection of organisational data and an insistence that it remains free from corruption. IT professionals must have the same attitude when managing their systems.

Common EU security compliance initiatives

The following is a brief sampling of some of the more common EU security compliance acts.

Data Protection Act 1984, amended 1988 (UK)		
Geographic coverage UK	**Industries/sectors affected** All	**Scope of coverage** Any organisation that collects personal data

Summary

The UK Data Protection Act imposes legal obligations on anyone processing personal data to ensure there is good practice and management of that data. In part 1 of the Act there are 8 enforceable principles of good personal information handling.

Data must be:

- Accurate and up to date
- Fairly and lawfully processed
- Secured
- Not allowed to leave the UK unless the destination countries have similar legislation
- Processed in line with a person's rights
- Only kept for as long as necessary
- Processed for limited purposes
- Adequate, relevant and not excessive

Part 2 of the act gives individuals rights to find out what personal information is held about them on computers and most paper records.

Non-compliance penalties

The UK Information Commissioner's Office has legal powers to ensure that organisations comply with the requirements of the Data Protection Act. A data controller who persistently breaches the Act and has been served with an enforcement notice can be prosecuted for failing to comply with a notice. This offence carries a maximum penalty of a £5,000 fine in the magistrates' court and an unlimited fine in the Crown Court.

Implications for IT security

IT security is not mentioned explicitly in this act, but as IT will be used to store the majority of this data it is vital that these systems remain secure at all times. Data encryption forms a vital part of the secure storage of this data as, once encrypted, it will address the secure requirement as listed above. Data leak prevention technologies could be employed to prevent the data being sent to an inappropriate country either deliberately or accidentally.

Common EU security compliance initiatives

Payment Card Industry Data Security Standards (PCI DSS)		
Geographic coverage International	**Industries/sectors affected** All	**Scope of coverage** Any that process card payments

Summary

The use of payment cards has increased massively with the popularity of online purchasing. PCI DSS was introduced by the PCI Standards Council, which was founded by the major payment card brands in order to enhance the security of payment accounts. At the foundation of the PCI DSS are 12 requirements that specify how payment data should be managed:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

PCI DSS only applies if the payment card primary account number is stored by the organisation. PCI DSS is managed by the payment card industry, which conduct audits and checks dependent on the volume of card transactions. Smaller volume retailers are expected to self audit/self certify that their systems adhere to the PCI DSS requirements. Version 1.2 of PCI DSS was released in October 2008. No changes were made to the PCI DSS requirements, instead it clarified the responsibilities of card processing organisations and brought the legislation up to date with evolving threats.

NOTE: Although not an EU regulation, PCI DSS has been included as it is relatively new and has widespread implications for EU-based merchants.

Non-compliance penalties

Fines and withdrawal of payment card facilities.

Implications for IT security

PCI DSS is very much an IT-focused requirement, with some very specific requirements on the safekeeping of payment card data. The 12 principles highlighted by PCI DSS comprise a valid health check and best practice checklist in their own right.

Common EU security compliance initiatives

Capital Requirements Directive/Basel II Accord

Geographic coverage	Industries/sectors affected	Scope of coverage
International	Banking and Finance	Internationally-active banks with assets greater than $250 billion or foreign exposures greater than $10 billion.

Summary

Basel II is designed to create an international standard that can be used by banking organisations when creating regulations concerning the amount of capital banks need to set aside to guard against operational risks. The accord is designed to prevent international financial problems being created by collapsed banks, and sets rules on the amount banks need to keep in reserve based on their exposure. Advocates of Basel II see that it will introduce better safeguards into the worldwide financial community. Basel II is based on the concept of three pillars that encompass how banks can prepare for credit risks, interact with regulators and provide responsible disclosure.

Non-compliance penalties

Non-compliance can result in institutions having to reserve greater amounts of capital to cover their risk exposure resulting in less favourable pricing in capital markets.

Implications for IT security

Operational risk forms the heart of Basel II. An institution therefore needs to protect its data with the utmost integrity—be it data at rest, in motion or during transactions.

Common EU security compliance initiatives

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995		
Geographic coverage EU	**Industries/sectors affected** All	**Scope of coverage** Personal data

Summary

As part of the development of the EU this legislation has been put in place to harmonise data protection laws across the EU. The law focuses on seven key principles concerning the use of and access to personal data. Member states of the EU have generally implemented their own local data protection laws that enshrine the principles of Directive 95/46/EC; for example the UK has implemented the Data Protection Act, Germany has The Federal Data Protection Act (Bundesdatenschutzgesetz) and the Netherlands has the Personal Data Protection Act (Wet bescherming persoonsgegevens).

Non-compliance penalties

Each nation member can impose their own penalties. These generally comprise of fines imposed by courts.

Implications for IT security

Any organisation holding personal data subject to this directive must ensure that the information is protected according to seven principles:

- The Principle of Openness
- The Principle of Individual Participation
- The Principle of Collection Limitation
- The Principle of Data Quality
- The Principle of Finality
- The Principle of Security
- The Principle of Accountability

These principles rely on good, overall system security including ensuring that data is protected both at rest and in motion.

Common EU security compliance initiatives

MiFID - The Markets in Financial Instruments Directive		
Geographic coverage EU	**Industries/sectors affected** Banking and Finance	**Scope of coverage** Companies and banks trading in financial instruments and businesses that deal in advisory services

Summary

The directive affects the way in which some share trades are undertaken. Instead of using exchanges, banks are able to deal "off-book"; buying and selling shares through customers directly. This is seen to be easier than using a share exchange. It is an update to the Investment Services Directive and is referred to in some places as ISD 2. The original Investment Services Directive was not successful.

Non-compliance penalties

MiFID is monitored by local authorities responsible for the regulation of financial transactions (for example the Financial Services Authority in the UK). Non-compliance will be investigated and, if appropriate, fines will be imposed by these regulators.

Implications for IT security

Businesses will need to prove that they are able to provide 'best execution' on any deals they are conducting. This will need to take into account cost, speed, pricing and venue and any records created will need to be stored for a minimum of 5 years. There will be an increase in algorithmic trading using automatic systems to determine the best trade venues, which will need to provide a clear audit trail.

From a security perspective it will be vital that these trades are protected during the transaction phase and that records created are stored securely for the minimum 5-year period.

Common EU security compliance initiatives

Freedom of Information Act (UK)		
Geographic coverage UK (Scottish public authorities are subject to the Freedom of Information (Scotland) Act 2002)	**Industries/sectors affected** Government bodies, local authorities and companies owned by the government	**Scope of coverage** Information held by authorities, excluding personal data

Summary

The Freedom of Information Act allows access to recorded information such as notes from meetings, research reports and emails held by public authorities. Under the Act any individual can make a request for information and have the necessary data sent to them. Any refusal to supply the information needs to be justified in writing to the applicant, making the reasons for the refusal clear.

Non-compliance penalties

The Information Commissioner can serve an enforcement notice on a body that fails to provide information. Failure to comply with an enforcement notice may result in the Commissioner referring the matter to the High Court. The High Court can deal with the public authority as if it had committed contempt of court. A public authority may appeal against an enforcement notice to the Information Tribunal.

Implications for IT security

Data that is subject to the Freedom of Information Act can be resident in a variety of forms throughout an organisation. This could be in the form of emails, Word documents, spreadsheets or written notes. Secured data will need to be accessible when requests are processed.

Common EU security compliance initiatives

Regulation of Investigatory Powers Act 2000 (RIP or RIPA) (UK)		
Geographic coverage UK	**Industries/sectors affected** All	**Scope of coverage** All electronic data

Summary

RIPA allows government organisations to access an individual's electronic communications. This can range from access to Internet Service Provider records through to telephone and email data. ISP records can be demanded from service providers who are under a legal obligation to provide them. Part III of the act allows certain government agencies to demand the cryptographic key to be supplied if the actual decrypted data was not available.

Non-compliance penalties

Failure to provide a cryptographic key can result in a 2 year jail term.

Implications for IT security

A demand to access data under RIPA must be adhered to by those receiving the request. If data encryption has been poorly implemented and the decryption key lost then there would be significant implications for the manager of that encryption system.

Efficient and effective key management is a vital part of any encryption deployment.

Common EU security compliance initiatives

The Rules Governing Medicinal Products in the European Union and Commission Directives 91/356/EEC, 2003/94/EC and 91/412/EEC		
Geographic coverage EU	**Industries/sectors affected** Pharmaceuticals Manufacturing	**Scope of coverage** Computers used in the manufacturing process

Summary

The EU has high standards of pharmaceutical manufacturing. In an effort to maintain these standards, rules have been introduced to ensure that approved manufacturers maintain appropriate standards. This good manufacturing practice, known as GMP, as been codified in two directives which have been adopted by the European Commission. Annexe 11 of this regulation determines best practice use of computing in good manufacturing practice.

Non-compliance penalties

Fines imposed by the EU.

Implications for IT security

This regulation insists that good computing practice be implemented for proper control of the manufacturing process. This ranges from the best principles of systems development through to the implementation of system security and safeguards. Data can only be entered or updated by approved people and any changes are to be recorded. Systems are to be fully backed up to prevent data loss. Data must be protected against inappropriate changes and adequately secured.

Common EU security compliance initiatives

Statutory Audit and the Company Reporting Directives (EuroSox)		
Geographic coverage EU: must be implemented into local laws by EU member states by 2010. The provisions of the Statutory Audit Directive are implemented into UK law through the Companies Act 2006	**Industries/sectors affected** All	**Scope of coverage** Public companies

Summary

Two European directives were issued by the European Union Council of Ministers aiming to create more transparency and public confidence in the operations of companies operating within the EU. The Statutory Audit Directive is designed to strengthen the standards and public accountability of the audit profession and the Company Reporting Directive aims to enhance confidence in financial statements and annual reports from European companies.

Non-compliance penalties

EuroSox will be incorporated into local national company laws; therefore penalties will vary from member state to member state.

Implications for IT security

EuroSox will demand that IT maintains accurate, dependable records with full audit trails of any data changes. Management will expect accurate and dependable reports created from within IT systems. IT systems will need to be secured to meet auditor approval and data must be protected from unauthorised access.

Common EU security compliance initiatives

Federal Data Protection Act (November 2006) (Germany)		
Geographic coverage Germany	**Industries/sectors affected** Public bodies of the Federation and the Länder. Private organisations and businesses.	**Scope of coverage** Private data held by these organisations

Summary

This is the implementation of EU Directive 95/46/EC in Germany and covers the protection of data held by organisations, in a similar way to the UK Data Protection Act. The act adheres to the seven basic principles of EU Directive 95/46/EC in the protection of data relating to individuals or data that allows an individual to be identified.

The 16 Länder have their own data protection regulations that cover local public bodies. These local regulations are similar in spirit to the Federal Data Protection Act.

Non-compliance penalties

Fines imposed by the Federal Commissioner for Data Protection and Freedom of Information. Possible imprisonment.

Implications for IT security

Good data security is a key aspect of this legislation and the onus is on the data keeping body to ensure that data is held in a secure and reliable way.

Common EU security compliance initiatives

Freedom of Information Act (2005) (Germany)		
Geographic coverage Germany	**Industries/sectors affected** Government and public bodies	**Scope of coverage** Information held by authorities (excluding personal data)

Summary

Citizens in Germany can request information from Government bodies irrespective of whether the individual requesting has a legal interest in gaining access to these documents. There must be minimal delay in providing the information and a maximum time limit of 2 months is given to service the most complex enquiries.

Information can be withheld on the basis of security, defence, tax-related issues or for the protection of trade secrets.

A number of Länder have their own similar laws.

Non-compliance penalties

Fines imposed by the Federal Commissioner for Data Protection and Freedom of Information.

Implications for IT security

As for similar legislation across the EU, requests for information can touch on a large amount of data sources, both electronic and paper based. Good corporate data hygiene is therefore paramount to ensure data is held safely and securely.

Common EU security compliance initiatives

Data Protection Act (2004) (France)		
Geographic coverage France	**Industries/sectors affected** All	**Scope of coverage** Any organisation that collects personal data

Summary

This is the implementation of EU Directive 95/46/EU in France and follows the same broad protection requirements of similar legislation in the EU. Enforcement is undertaken by CNiL, the National Commission for Data Protection. The law enables an individual to find out what data is being held about them on payment of a small fee.

Non-compliance penalties

5 years' imprisonment and/or €300,000 fine

Implications for IT security

As with the other data protection acts in the EU, data needs to be stored safely and securely, as well as kept to a minimum.

EU Compliance—Summary Comparison Table

Act	Geographic coverage	Industries and sectors affected	Scope of coverage
Data Protection Act 1984, amended 1988	UK	All	Personal data
Payment Card Industry Data Security Standards (PCI DSS)	International	All	Any that process card payments
Capital Requirements Directive/ Basel II Accord	International	Banking and Finance	Internationally-active banks with assets greater than $250 billion or foreign exposures greater than $10 billion.
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995	EU	All	Personal data
MiFID - The Markets in Financial Instruments Directive	EU	Banking and Finance	Companies and banks trading in financial instruments and businesses that deal in advisory services
Freedom of Information Act	UK (Scottish public authorities are subject to the Freedom of Information (Scotland) Act 2002)	Government bodies, local authorities and companies owned by the government	Information held by authorities excluding personal data
Regulation of Investigatory Powers Act 2000 (RIP or RIPA)	UK	All	All electronic data
The Rules Governing Medicinal Products in the European Union and Commission Directives 91/356/EEC, 2003/94/EC, and 91/412/EEC	EU	Manufacturing Pharmaceutical	Computers used in the manufacturing process
Statutory Audit and the Company Reporting Directives (EuroSox)	EU: must be implemented into local laws by EU member states by 2010. The provisions of the Statutory Audit Directive are implemented into UK law through the Companies Act 2006	All	Public companies
Federal Data Protection Act (November 2006)	Germany	Public bodies of the Federation and the Länder. Private organisations and businesses	Private data held by these organisations
Freedom of Information Act (2005)	Germany	Government and public bodies	Information held by authorities excluding personal data
Data Protection Act (2004)	France	All	Any organisation that collects personal data

Other significant legislation and regulations

The following legislation and regulations may be of interest to those investigating IT compliance requirements in the EU but detailed coverage is not included in this paper as they primarily have a US focus or have limited relevance to IT security;

- Sarbanes-Oxley Act of 2002 (SOX). US legislation that only covers EU companies that have a presence in the United States
- Health Insurance Portability and Accountability Act of 1996 (HIPAA). US legislation that applies to healthcare providers based in the United States
- The Gramm-Leach-Bliley Act (Financial Modernization Act of 1999). US legislation that covers the protection of financial institutions' private customer data
- USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001). US legislation that covers the use of surveillance by government agencies and the requirement of business to report computer-based crime.
- The Turnbull Guidance. The Turnbull Guidance sets out best practices on internal control for UK listed companies. The US Securities and Exchange Commission has permitted use of the Turnbull Guidance as a suitable framework for complying with US requirements to report on internal controls over financial reporting, as set out in Section 404 of the Sarbanes-Oxley Act 2002 and related SEC rules. Limited direct relevance to EU-based IT professionals
- California Data Security Breach Notification Law Cal. Civ. Code 1798.82 and 1798.29. This law, enacted in 2002, requires that if personal data security has been breached then those individuals possibly affected must be notified of this breach. This law is seen by many to be the model breach notification legislation. EU legislators are considering a similar law in the EU.
- The Companies Act 1985 (Investment Companies and Accounting and Audit Amendments) Regulations 2005. This UK Act changes the financial reporting requirements for some companies, notably smaller businesses. Limited direct relevance to EU-based IT professionals
- International Financial Reporting Standards (IFRS). A set of standards and a framework for the preparation of accounts. Limited direct relevance to EU-based IT professionals
- Companies Act 2006 – Electronic Communications. This UK legislation sets out the framework for communicating with shareholders using email. There are no additional or specific data security requirements in this legislation but it may be of interest to EU-based IT professionals
- Electronic Communications Act 2000 gave the UK Home Office power to create a registration regime for encryption services. It contained a 5-year sunset clause which expired in 2005 and the legislation was removed from the statute book. Included as a matter of interest only.
- Data Retention Directive 2006/24/EC. The Directive requires member states to ensure that communications providers must retain, for a period of between 6 months and 2 years, data created concerning the type, nature and time and date of data carried by telephone and internet service providers. Included as a matter of interest only.
- Money Laundering Regulations 2007. UK legislation that requires certain businesses to register with HMRC and monitor financial transactions for possible money laundering activities. Included as a matter of interest only.
- Human Rights Act 1998 (UK)/ European Convention on Human Rights. Legislation that sets out an individual's rights such as a right to privacy. Included as a matter of interest only.

Strategies for managing information technology compliance

Information technology can be notoriously complex and often sees business managers chased away from getting involved with decisions related to technology. Whilst this may be appropriate in very narrow technical decisions it is important that business understands IT and how it is benefiting the business.

From a compliance perspective it is very easy for the business to be frightened by talk of liabilities, whilst technicians appear to spend budgets with limited care for the overall business benefit. When considering IT compliance, it is imperative that a strategic approach is taken based on clear, rational thinking. Many businesses have rushed into a technical solution that was sold as solving compliance issues only for them to quickly realise the limitations of the product. Most IT security compliance initiatives require a continuous process to collect data and demonstrate compliance. Organisations are best off leveraging tools and solutions that can automate such compliance processes and can use it across multiple compliance initiatives or mandates.

Further Information

Further information about this subject is available from http://www.BloorResearch.com/update/1015

Bloor Research overview

Bloor Research has spent the last decade developing what is recognised as Europe's leading independent IT research organisation. With its core research activities underpinning a range of services, from research and consulting to events and publishing, Bloor Research is committed to turning knowledge into client value across all of its products and engagements. Our objectives are:

- Save clients' time by providing comparison and analysis that is clear and succinct.
- Update clients' expertise, enabling them to have a clear understanding of IT issues and facts and validate existing technology strategies.
- Bring an independent perspective, minimising the inherent risks of product selection and decision-making.
- Communicate our visionary perspective of the future of IT.

Founded in 1989, Bloor Research is one of the world's leading IT research, analysis and consultancy organisations—distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services and consultancy projects.

About the author

Nigel Stanley
Practice Leader—Security

Nigel Stanley is a specialist in business technology and IT security and now heads up Bloor's IT Security practice.

IT security comprehensively covers the whole remit of protecting and defending business or organisational systems and data from unwelcome attacks or intrusions. This large area includes protection from the outer edges of the security domain such as handheld devices through to network perimeter, inside threats and local defences. It looks at the ever growing threats, many of them new and innovative. It includes use of firewalls, data loss prevention, data encryption, anti-malware, database protection, identity management, intrusion detection/prevention, content management/filtering and security policies and standards.

For a number of years Nigel was technical director of a leading UK Microsoft partner where he lead a team of consultants and engineers providing secure business IT solutions. This included data warehouses, client server applications and intelligent web based solutions. Many of these solutions required additional security due to their sensitive nature. From 1995 until 2003 Nigel was a Microsoft regional director, an advisory role to Microsoft Corporation in Redmond, which was in recognition of his expertise in Microsoft technologies and software development tools.

Nigel had previously worked for Microsoft as a systems engineer and product manager specialising in databases and developer technologies. He was active throughout Europe as a leading expert on database design and implementation.

He has written three books on database and development technologies including Microsoft .NET. He is working on a number of business-led IT assignments and is an executive board member of several privately held companies including Incoming Thought Limited a partner company to Bloor Research that specialises in security consultancy and education.

Nigel continues to write many papers and articles on IT.

Copyright & disclaimer

2nd Floor
145—157 St John Street
London, EC1V 4PY
United Kingdom

Tel: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Web: www.BloorResearch.com
email: info@BloorResearch.com