7TH EDITION

IT GOVERNANCE

An International Guide to Data Security and ISO27001/ISO27002

ALAN CALDER
STEVE WATKINS

KoganPage

IT Governance

An international guide to data security and ISO27001/ISO27002

SEVENTH EDITION

Alan Calder
Steve Watkins

KoganPage

Publisher's note

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and authors cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or either of the authors.

First published in Great Britain and the United States in 2002 by Kogan Page Limited

Second edition 2003
Third edition 2005
Fourth edition 2008
Fifth edition 2012
Sixth edition 2015
Seventh edition 2020

2nd Floor, 45 Gee Street
London
EC1V 3RS
United Kingdom
www.koganpage.com

122 W 27th St, 10th Floor
New York, NY 10001
USA

4737/23 Ansari Road
Daryaganj
New Delhi 110002
India

ISBNs

Hardback	978 1 7896 6030 2
Paperback	978 0 7494 9695 1
Ebook	978 0 7494 9696 8

British Library Cataloguing-in-Publication Data

A CIP record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication Data

A CIP record for this book is available from the Library of Congress.

Typeset by Hong Kong FIVE Workshop
Print production managed by Jellyfish
Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY

CONTENTS

ABOUT THE AUTHORS

ALAN CALDER

Alan Calder founded IT Governance Limited in 2002 and began working full time for the company in 2007. He is now Group CEO of GRC International Group PLC, the AIM-listed company that owns IT Governance Ltd. Prior to this, Alan had a number of roles including CEO of Business Link London City Partners from 1995 to 1998 (a government agency focused on helping growing businesses to develop), CEO of Focus Central London from 1998 to 2001 (a training and enterprise council), CEO of Wide Learning from 2001 to 2003 (a supplier of e-learning) and the Outsourced Training Company (2005). Alan was also chairman of CEME (a public private sector skills partnership) from 2006 to 2011.

Alan is an acknowledged international cyber security guru and a leading author on information security and IT governance issues. He has been involved in the development of a wide range of information security management training courses that have been accredited by the International Board for IT Governance Qualifications (IBITGQ). Alan has consulted for clients in the UK and abroad, and is a regular media commentator and speaker.

STEVE WATKINS

Steve is an executive director at GRC International Group PLC. He is a contracted technical assessor for UKAS, advising on its assessments of certification bodies offering ISMS/ISO 27001 and ITSMS/ISO 20000-1 accredited certification, and also undertakes information security assessments of forensic science laboratories seeking accreditation to the Forensic Science Regulator's codes of practice and conduct.

He is a member of ISO/IEC JTC 1/SC 27, the international technical committee responsible for information security, cyber security and privacy standards, and chairs the UK National Standards Body's technical committee IST/33 (Information technology – Security techniques) that mirrors it. Steve is also involved with technical committees: RM/1 (risk management) and RM/1/-/3 (responsible for BS 31111, providing guidance for boards and senior management on cyber risk and resilience); IST/060/02 (IT service management) and IDT/001/0-/04 (data protection).

Introduction

This book on IT governance is a key resource for forward-looking executives and managers in 21st-century organizations of all sizes. There are six reasons for this:

1. The development of IT governance, which recognizes the 'information economy'-driven convergence between business management and IT management, makes it essential for executives and managers at all levels in organizations of all sizes to understand how decisions about information technology in the organization should be made and monitored and, in particular, how information security risks are best dealt with.
2. Risk management is a big issue. In the United Kingdom, the FRC's Risk Guidance (formerly the Turnbull Guidance on internal control) gives directors of Stock Exchange-listed companies a clear responsibility to act on IT governance, on the effective management of risk in IT projects and on computer security. The US Sarbanes–Oxley Act places a similar expectation on directors of all US listed companies. Banks and financial sector organizations are subject to the requirements of the Bank of International Settlements (BIS) and the Basel 2/3 frameworks, particularly around operational risk – which absolutely includes information and IT risk. Information security and the challenge of delivering IT projects on time, to specification and to budget also affect private- and public-sector organizations throughout the world.
3. Particularly post-GDPR, information-related legislation and regulation are increasingly important to all organizations. Data protection, privacy and breach regulations, computer misuse and regulations around investigatory powers are part of a complex and often competing range of requirements to which directors must respond. There is, increasingly, the need for an overarching information security framework that can provide context and coherence to compliance activity worldwide.

4 As the intellectual capital value of 'information economy' organizations increases, their commercial viability and profitability – as well as their share price – increasingly depend on the security, confidentiality and integrity of their information and information assets.

5 The dramatic growth and scale of the 'information economy' have created new, global threats and vulnerabilities for all organizations, particularly in cyberspace.

6 The world's first, and only, standard for information security management is now at the heart of a globally recognized framework for information security and assurance. As part of the series of ISO/IEC 27000 standards, the key standard, ISO/IEC 27001, has been updated to contain latest international best practice, with which, increasingly, businesses are asking their suppliers to conform. Compliance with the standard should enable company directors to demonstrate a proper response – to customers as well as to regulatory and judicial authorities – to all the challenges identified above.

The information economy

Faced with the emergence and speed of growth in the information economy, organizations have an urgent need to adopt IT governance best practice. The main drivers of the information economy are:

- the ongoing globalization of markets, products and resourcing (including 'offshoring' and 'nearshoring');
- electronic information and knowledge intensity;
- the geometric increase in the level of electronic networking and connectivity.

The key characteristics of the global information economy, which affect all organizations, are as follows:

- Unlike the industrial economy, information and knowledge are not depleting resources that have to be rationed and protected.
- Protecting knowledge is less obviously beneficial than previously: sharing knowledge actually drives innovation, and innovation drives competitiveness.
- The effect of geographic location is diminished; virtual and cloud-based organizations operate around the clock in virtual marketplaces that have no geographic boundaries.

- As knowledge shifts to low-tax, low-regulation environments, laws and taxes are increasingly difficult to apply on a solely national basis.
- Knowledge-enhanced products command price premiums.
- Captured, indexed and accessible knowledge has greater intrinsic value than knowledge that goes home at the end of every day.
- Intellectual capital is an increasingly significant part of shareholder value in every organization.

The challenges, demands and risks faced by organizations operating in this information-rich and technologically intensive environment require a proper response. In the corporate governance climate of the early 21st century, with its growing demand for shareholder rights, corporate transparency and board accountability, this response must be a governance one.

What is IT governance?

The Organization for Economic Co-operation and Development (OECD), in its *Principles of Corporate Governance* (1999), first formally defined 'corporate governance' as 'the system by which business corporations are directed and controlled'. Every country in the OECD is evolving – at a different speed – its own corporate governance regime, reflecting its own culture and requirements. Within its overall approach to corporate governance, every organization has to determine how it will govern the information, information assets and information technology on which its business model and business strategy rely. This need has led to the emergence of IT governance as a specific – and pervasively important – component of an organization's total governance posture.

We define IT governance as 'the framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensures that the organization's information systems support and enable the achievement of its strategies and objectives'.

There are five specific drivers for organizations to adopt IT governance strategies:

- the requirements (in the United Kingdom) of the Corporate Governance Code and the Risk Guidance; for US-listed companies, Sarbanes–Oxley; for banks and financial institutions, BIS and Basel 2/3; and for businesses everywhere, the requirements of their national corporate governance regimes;

- the increasing intellectual capital value that the organization has at risk;
- the need to align technology projects with strategic organizational goals and to ensure that they deliver planned value;
- the proliferation of (increasingly complex) threats to information and information security, particularly in cyber space, with consequent potential impacts on corporate reputation, revenue and profitability;
- the increase in the compliance requirements of (increasingly conflicting and punitive) information- and privacy-related regulation, particularly the EU GDPR and regulations inspired by it.

There are two fundamental components of effective management of risk in information and information technology. The first relates to an organization's strategic deployment of information technology in order to achieve its business goals. IT projects often represent significant investments of financial and managerial resources. Shareholders' interest in the effectiveness of such deployment should be reflected in the transparency with which they are planned, managed and measured, and the way in which risks are assessed and controlled. The second component is the way in which the risks associated with information assets themselves are managed.

Clearly, well-managed information technology is a business enabler. All directors, executives and managers, at every level in any organization of any size, need to understand how to ensure that their investments in information and information technology enable the business. Every deployment of information technology brings with it immediate risks to the organization, and therefore every director or executive who deploys, or manager who makes any use of, information technology needs to understand these risks and the steps that should be taken to counter them. This book deals with IT governance from the perspective of the director or business manager, rather than from that of the IT specialist. It also deals primarily with the strategic and operational aspects of information security.

Information security

The proliferation of increasingly complex, sophisticated and global threats to information security, in combination with the compliance requirements of a flood of computer- and privacy-related regulation around the world, is driving organizations to take a more strategic view of information security.

It has become clear that hardware-, software- and/or vendor-driven solutions to individual information security challenges are, on their own, dangerously inadequate.

While most organizations believe that their information systems are secure, the brutal reality is that they are not. Not only is it extremely difficult for an organization to operate in today's world without effective information security, but poorly secured organizations have become risks to their more responsible associates. The extent and value of electronic data are continuing to grow exponentially. The exposure of businesses and individuals to data misappropriation (particularly in electronic format) or destruction is also growing very quickly. Ultimately, consumer confidence in dealing across the web depends on how secure consumers believe their personal data are. Cyber security, for this reason, matters to any business with any form of web strategy (and any business without a web strategy is unlikely to be around in the long term), from simple business-to-consumer (b2c) or business-to-business (b2b) e-commerce propositions through enterprise resource planning (ERP) systems to the use of e-mail, social media, mobile devices, Cloud applications and web services. It matters, too, to any organization that depends on computers for its day-to-day existence or that may be subject (as are all organizations) to the provisions of data protection legislation.

Newspapers and business or sector magazines are full of stories about criminal hackers, viruses, online fraud, cyber crime and loss of personal data. These are just the public tip of the data insecurity iceberg. There is growing evidence of substantial financial losses amongst inadequately secured businesses and a number of instances where businesses have failed to survive a major disruption of their data and operating systems. All businesses now suffer low-level, daily disruption of normal operations as a result of inadequate security.

Many people also experience the frustration of trying to buy something online, only for the screen to give some variant of the message 'server not available'. Many more, working with computers in their daily lives, have experienced (once too) many times a local network failure or outage that interrupts their work. With the increasing pervasiveness of computers, and as hardware/software computing packages become ever more powerful and complex, so the opportunity for data and data systems to be compromised or corrupted (knowingly or otherwise) will increase.

Information security management systems (ISMSs) in the vast majority of organizations are, in real terms, non-existent, and even where systems have been designed and implemented, they are usually inadequate. In simple terms, larger organizations tend to operate their security functions in vertically segregated silos with little or no coordination. This structural weakness means that most organizations have significant vulnerabilities that can be exploited deliberately or that simply open them up to disaster.

For instance, while the corporate lawyers will tackle all the legal issues (nondisclosure agreements, patents, contracts, etc), they will have little involvement with the data security issues faced on the organizational perimeter. On the organizational perimeter, those dealing with physical security concentrate almost exclusively on physical assets, such as gates or doors, security guards and burglar alarms. They have little appreciation of, or impact upon, the 'cyber' perimeter. The IT managers, responsible for the cyber perimeter, may be good at ensuring that everyone has a strong password and that there is internet connectivity, that the organization is able to respond to malware threats, and that key partners, customers and suppliers are able to deal electronically with the organization, but they almost universally lack the training, experience or exposure adequately to address the strategic threat to the information assets of the organization as a whole. There are many organizations in which the IT managers subjectively set and implement security policy for the organization on the basis of their own risk assessment, past experiences and interests, but with little regard for the real business needs or strategic objectives of the organization.

Information security is a complex issue and deals with the confidentiality, integrity and availability of data. IT governance is even more complex, and in information security terms one has to think in terms of the whole enterprise, the entire organization, which includes all the possible combinations of physical and cyber assets, all the possible combinations of intranets, extranets and internets, and which might include an extended network of business partners, vendors, customers and others. This handbook guides the interested manager through this maze of issues, through the process of implementing internationally recognized best practice in information security, as captured in ISO/IEC 27002:2013 and, finally, achieving certification to ISO/IEC 27001:2013, the world's formal, public, international standard for effective information security management.

The ISMS standard is not geographically limited (eg to the United Kingdom, or Japan or the United States), nor is it restricted to a specific sector (eg the Department of Defence or the software industry), nor is it restricted to a specific product (such as an ERP system, or Software as a Service). This book covers many aspects of data security, providing sufficient information for the reader to understand the major data security issues and what to do about them – and, above all, what steps and systems are necessary for the achievement of independent certification of the organization's ISMS to ISO27001.

This book is of particular benefit to board members, directors, executives, owners and managers of any business or organization that depends on information, that uses computers on a regular basis, that is responsible for personal data or that has an internet aspect to its strategy. It can equally apply to any organization that relies on the confidentiality, integrity and availability of its data. It is directed at readers who either have no prior understanding of data security or whose understanding is limited in interest, scope or depth. It is not written for technology or security specialists, whose knowledge of specific issues should always be sought by the concerned owner, director or manager. While it deals with technology issues, it is not a technological handbook.

Information security is a key component of IT governance. As information technology and information itself become more and more the strategic enablers of organizational activity, so the effective management of both and information assets becomes a critical strategic concern for boards of directors. This book will enable directors and business managers in organizations and enterprises of all sizes to ensure that their IT security strategies are coordinated, coherent, comprehensive and cost-effective, and meet their specific organizational or business needs. While the book is written initially for UK organizations, its lessons are relevant internationally, as computers and data threats are internationally similar. Again, while the book is written primarily with a Microsoft environment in mind (reflecting the penetration of the Microsoft suite of products into corporate environments), its principles apply to all hardware and software environments. ISO/IEC 27001 is, itself, system agnostic.

The hard copy of this book provides detailed advice and guidance on the development and implementation of an ISMS that will meet the ISO27001 specification. The IT Governance website (www.itgovernancepublishing.co.uk/category/toolkits-information-security-iso27001 (archived at https://perma.cc/7FED-RY3Y)) carries a series of ISO27001 Documentation Toolkits. Use of the templates within these toolkits, which are not industry or jurisdiction specific but which do integrate absolutely with the advice in this book, can speed knowledge acquisition and ensure that your process development is comprehensive and systematic.

Organizations should always ensure that any processes they implement are appropriate and tailored for their own environment. There are four reasons for this:

- Policies, processes and procedures should always reflect the style, and the culture, of the organization that is going to use them. This will help their acceptance within the organization.
- The processes and procedures that are adopted should reflect the risk assessment carried out by the organization's specialist security adviser. While some risks are common to many organizations, the approach to controlling them should be appropriate to, and cost-effective for, the individual organization and its individual objectives and operating environment.
- It is important that the organization understands, in detail, its policies, processes and procedures. It will have to review them after any significant security incident and at least once a year. The best way to understand them thoroughly is through the detailed drafting process.
- Most importantly, the threats to an organization's information security are evolving as fast as the information technology that supports it. It is essential that security processes and procedures are completely up to date, that they reflect current risks and that, in particular, current technological advice is taken, to build on the substantial groundwork laid in this book.

This book will certainly provide enough information to make the drafting of detailed procedures quite straightforward. Where it is useful (particularly in generic areas like e-mail controls, data protection, etc), there are pointers as to how procedures should be drafted. Information is the very lifeblood of most organizations today and its security ought to be approached professionally and thoroughly.

Finally, it should be noted that ISO27001 is a service assurance scheme, not a product badge or cast-iron guarantee. Achieving ISO27001 certification does not of itself prove that the organization has a completely secure information system; it is merely an indicator, particularly to third parties, that the objective of achieving appropriate security is being effectively pursued. Information security is, in the terms of the cliché, a journey, not a destination.

1

Why is information security necessary?

An information security management system (ISMS) is necessary because the threats to the availability, integrity and confidentiality of the organization's information are great, and always increasing. Any prudent householder whose house was built on the shores of a tidal river would, when facing the risk of floods, take urgent steps to improve the defences of the house against the water. It would clearly be insufficient just to block up the front gate, because the water would get in everywhere and anywhere it could. In fact, the only prudent action would be to block every single possible channel through which floodwaters might enter and then to try to build the walls even higher, in case the floods were even worse than expected.

So it is with the threats to organizational information, which are now reaching tidal proportions. All organizations possess information, or data, that is either critical or sensitive. Information is widely regarded as the lifeblood of modern business. Advanced Persistent Threat (APT) is the description applied to the cyber activities of sophisticated criminals and state-level entities, targeted on large corporations and foreign governments, with the objective of stealing information or compromising information systems. Cyber attacks are, initially, automated and indiscriminate – any organization with an internet presence will be scanned and potentially targeted.

Not surprisingly, the PricewaterhouseCoopers (PwC) Global State of Information Security Survey 2018 said that 'most organizations realize that cybersecurity has become a persistent, all-encompassing business risk'. This is because the business use of technology is continuing to evolve rapidly, as organizations move into cloud computing and exploit social networks. Wireless networking, Voice over IP (VoIP) and Software as a Service (SaaS) have become mainstream. The increasingly digital and inter-connected supply chain increases the pressure on organizations to manage information and its security and confirms the growing dependence of UK business on information and information technology.

While it is clearly banal to state that today's organization depends for its very existence on its use of information and communications technology, it is apparently not yet self-evident to the vast majority of boards and business owners that their information is valuable to both competitors and criminals and that how well they protect their systems and information is existentially important.

There is no doubt that organizations are facing a flood of threats to their intellectual assets and to their critical and sensitive information. High-profile cyber attacks and data protection compliance failures have led to significant embarrassment and brand damage for organizations – in both the public and private sectors – all over the world.

In parallel with the evolution of information security threats, there has – across the world – been a thickening web of legislation and regulation that makes firms criminally liable, and in some instances makes directors personally accountable, for failing to implement and maintain appropriate risk control and information security measures. It is now blindingly obvious that organizations have to act to secure and protect their information assets.

'Information security', however, means different things to different people. To vendors of security products, it tends to be limited to the product(s) they sell. To many directors and managers, it tends to mean something they don't understand and that the CIO, CISO or IT manager has to put in place. To many users of IT equipment, it tends to mean unwanted restrictions on what they can do on their corporate PCs. These are all dangerously narrow views.

The nature of information security threats

Data or information is right at the heart of the modern organization. Its availability, integrity and confidentiality are fundamental to the long-term survival of any 21st-century organization; in survey after survey, 9 out of 10 organizations make this claim. Unless the organization takes a comprehensive and systematic approach to protecting the availability, integrity and confidentiality of its information, it will be vulnerable to a wide range of possible threats. These threats are not restricted to internet companies, to e-commerce businesses, to organizations that use technology, to financial organizations or to organizations that have secret or confidential information. As we saw earlier, they affect all organizations, in all sectors of the economy, both public and private. They are a 'clear and present danger', and strategic responsibility for ensuring that the organization has appropriately defended its information assets cannot be abdicated or palmed off on the CIO, CIOS or head of IT.

In spite of surveys and reports which claim that boards and managers are paying more attention to security, the truth is that the risk to information is growing more quickly than boards are recognizing. The annual Verizon Data Breaches Report gathered data from 80,000 data breaches (which occurred in a 12-month period) across the world to conclude that 700 million compromised records were the cause of financial losses of some $400 million. Matters are worse in every subsequent year.

Information security threats come from both within and without an organization. The situation worsens every year, and cyber threats are likely to become more serious in future. Cyber activism is at least as serious a threat as is cyber crime, cyber war and cyber terrorism. Unprovoked external attacks and internal threats are equally serious. It is impossible to predict what attack might be made on any given information asset, or when, or how. The speed with which methods of attack evolve, and knowledge about them proliferates, makes it completely pointless to take action only against specific, identified threats. Only a comprehensive, systematic approach will deliver the level of information security that any organization really needs.

It is worth understanding the risks to which an organization with an inadequate ISMS exposes itself. These risks fall into three categories:

- damage to operations;
- damage to reputation;
- legal damage.

Damage in any one of these three categories can be measured by its impact on the organization's bottom line, both short and long term. While there is no single, comprehensive, global study of information risks or threats on which all countries and authorities rely, there are a number of surveys, reports and studies, in and across different countries and often with slightly differing objectives, that, between them, demonstrate the nature, scale, complexity and significance of these information security risks and the extent to which organizations, through their own complacency or through the vulnerabilities in their hardware, software, and management systems, are vulnerable to these threats.

Information insecurity

Annual surveys point to a steadily worsening situation. The annual Verizon Data Breach Investigations Report, conducted with the US Secret Service, and which draws data from both the United States and internationally, regularly reports that:

- data breaches occur within all sorts of organizations;
- hundreds of millions of records are compromised every year;
- most breaches originate externally, a significant per cent internally, and more than a quarter were carried out by multiple agents.

The United Kingdom's annual Information Security Breaches Survey (ISBS), managed by PwC, looks at the state of information security across a representative sample of UK organizations. Key findings include:

- Almost all large organizations suffer data breaches, and often multiple breaches; large organizations tend to be specifically targeted by attackers.
- More than 50% of small organizations are breached; because they are not specifically targeted, they suffer fewer breaches every year.
- The average cost to a large organization of its worst breach is between £600k and £1.15 million.
- For a small organization, the range is between £65k and £115k.
- More than three-quarters of large respondents suffer from a malware or virus infection, often delivered via a phishing e-mail.
- More than half of large respondents suffer an external attack; quite often this is some form of denial of service attack, and less than a quarter are able to identify that their defences have actually been penetrated.
- The majority of organizations also suffer staff-related security breaches; one-third of the worst breaches are caused by inadvertent human error.

Surveys and data from other OECD economies suggest that a similar situation can be found across the world. Hackers, crackers, virus writers, spammers, phishers, pharmers, fraudsters and the whole menagerie of cyber-criminals are increasingly adept at exploiting the vulnerabilities in organizations' software, hardware, networks and processes. As fraudsters, spam and virus writers, hackers and cyber criminals band together to mount integrated attacks on businesses and public sector organizations everywhere, the need for appropriate cyber security defences increases.

Often – but not always – information security is *in reality* seen only as an issue for the IT department, which it clearly isn't. Good information security management is about organizations understanding the risks and threats they face and the vulnerabilities in their current computer processing facilities. It is about putting in place common-sense procedures to minimize the risks and about educating all the employees about their responsibilities. Most importantly, it is about ensuring that the policy on information security management has the commitment of senior managers. It is only when these procedural and management issues are addressed that organizations can decide on what security technologies they need.

Roughly one-seventh of businesses are still spending less than 1 per cent of their IT budget on information security; although the average company is spending just under 4 per cent, the benchmark against which their expenditure should be compared is closer to the 13 per cent average of organizations where managers genuinely care about information security. That less than half of all businesses ever estimate the return on their information security investment may be part of the problem; certainly, until business takes its IT governance responsibilities seriously, the information security situation will continue to worsen.

Impacts of information security threats

As indicated above, information security breaches affect business operations, reputation and legal standing. Business disruption is the most serious impact, with roughly two-thirds of UK breaches leading to disruption of operations, with consequent impacts on customer service and business efficiency. As well as business disruption, organizations face incident response costs that include response and remediation costs (responding to, fixing and cleaning up after a security breach), direct financial loss (loss of assets, regulatory fines, compensation payments), indirect financial loss (through leakage of confidential information or intellectual property, revenue leakage), and reputation damage, with successful hack attacks and data losses both attracting increasing media attention.

There is a wide range of information available about the nature and average cost of a breach. The annual Verizon DBIR gathers information from 61 countries and multiple industry sectors in order to conclude that no industry is immune from data breaches. In 60 per cent of cases, attackers are able to compromise targets 'within minutes'; it still takes longer to detect the compromise than it does to complete the attack. Verison's forecast average financial loss per breach of 1,000 records is between $52,000 and $87,000. Most importantly, they conclude that the consistently most significant factor in quantifying the cost of loss for an organization is not the nature of the breach, but the number of records compromised.

The various components of that financial loss include discovery, investigation, response, remediation, customer notification costs, legal fees, regulatory breach notification costs, and increased operational, marketing and PR costs.

As the Target (a large US retailer) breach, in the USA just before Thanksgiving back in 2013, proved, damage to corporate reputation, shareholder class actions and straightforward loss of customers and the fall in net revenue arising from a successful breach can have a far more significant impact on the future performance of the organization – and, increasingly, on the continued employment and future careers of the directors at the helm of the organization when the breach occurred.

Cybercrime

The US State of Cybercrime Survey (conducted by CSO Magazine, the US Secret Service, the CERT Division of the Software Engineering Institute, and Price Waterhouse Cooper) spoke to 557 organizations about their experience in the previous 12 months. Thirty-two per cent of respondents said that damage from insider attacks was more severe than that from outsiders; 76 per cent of incidents involved theft or compromise of confidential records. Thirty-seven per cent of cybercrimes were not prosecuted because the culprits could not be identified and, for 36 per cent, the evidence was inadequate to support a prosecution.

In reality, many information security incidents are actually crimes. The UK Computer Misuse Act, for instance, makes it an offence for anyone to access a computer without authorization, to modify the contents of a computer without authorization or to facilitate (allow) such activity to take place. It identified sanctions for such activity, including fines and imprisonment. Other countries have taken similar action to identify and create offences that should enable law enforcement bodies to act to deal with computer misuse. Increasingly, this type of illegal activity is known as 'cybercrime'.

The Council of Europe Cybercrime Convention, the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks, was signed in November 2001. The United States finally ratified the Cybercrime Convention in 2006 and joined with effect from 1 January 2007. The Cybercrime Convention was designed to protect citizens against computer hacking and internet fraud, and to deal with crimes involving electronic evidence, including child sexual exploitation, organized crime and terrorism. Parties to the convention commit to effective and compatible laws and tools to fight cybercrime, and to cooperating to investigate and prosecute these crimes. They are not succeeding in this aim.

Europol, the European police agency, publishes the Internet Organized Crime Threat Assessment (iOCTA). iOCTA 2014 said that current trends suggest considerable increases in the scope, sophistication, number and types of attacks, number of victims and economic damage from organized crime on the Internet. The Crime-as-a-Service (CaaS) business model drives the digital underground economy by providing a wide range of commercial services that facilitate almost any type of cybercrime. Criminals are freely able to procure such services, such as the rental of botnets, denial-of-service attacks, malware development, data theft and password cracking, to commit crimes themselves. This has facilitated a move by traditional organized crime groups (OCGs) into cybercrime areas. The financial gain that cybercrime experts have from offering these services stimulates the commercialization of cybercrime as well as its innovation and further sophistication. Legitimate privacy networks are also of primary interest to criminals that abuse such anonymity on a massive scale for illicit online trade in drugs, weapons, stolen goods, forged IDs and child sexual exploitation.

The internet is, in other words, digitally dangerous. Organizations must take appropriate steps to protect themselves against criminal activity – both internal and external – in just the same way as they take steps to protect themselves in the physical world.

Cyberwar

Cybercrime is a serious issue but, in the longer run, may be a lesser danger to organizations than the effects of what is called 'cyberwar'. It is believed that every significant terrorist or criminal organization has cyber-capabilities and has become very sophisticated in its ability to plan and execute digital attacks. More significantly, many nation states now see cyberwar as an alternative – or an essential precursor to – traditional warfare.

Eliza Manningham-Buller, the then director-general of the UK security service MI5, said this at the 2004 CBI annual conference:

> A narrow definition of corporate security including the threats of crime and fraud should be widened to include terrorism and the threat of electronic attack. In the same way that health and safety and compliance have become part of the business agenda, so should a broad understanding of security, and considering it should be an integral and permanent part of your planning and statements of internal control; do not allow it to be left to specialists. Ask them to report to you what they are doing to identify and protect your key assets, including your people.

A decade later, Sir Ian Lobban said much the same thing in an open letter to CEOs and Chairs of FTSE 350 companies, encouraging them to undertake a 'cyber health check' after a KPMG security survey found that all of them were leaking data, such as employee usernames, e-mail addresses and sensitive internal file location information online.

Certainly, businesses appear to have got this message, with 97 per cent of them claiming to be concerned at board level about cyberwar. They should be. More than 400 million computers are linked to the internet; many of them are vulnerable to indiscriminate cyber-attack. The critical infrastructure of the First World is subject to the threat of cyber-assaults ranging from defacing websites to undermining critical national infrastructure.

A growing number of countries are at last putting cyber security strategies in place. The UK government's 2015 national security strategy recognized cyber risk as a Tier 4 national security risk and its national cyber security strategy has the objective of making the UK one of the most secure places in the world to live and work online. The EU's 2013 cyber security strategy ('An Open, Safe and Secure Cyberspace') has similar objectives.

While organizations that are part of the Critical National Infrastructure (CNI) clearly have a significant role to play in preparing to defend their national cyberspace against cyberattack, all organizations should take appropriate steps to defend themselves from being caught in the digital crossfire.

Advanced persistent threat

The term advanced persistent threat (APT) usually refers to a national government – or state-level entity that has the capacity and the intent to persistently and effectively target – in cyberspace – another entity that it wishes to disrupt or otherwise compromise. While cyberspace is the most common theatre of attack, other vectors include social engineering, infected media and malware and supply chain compromise. Attackers usually have the resources, competence and available time to focus on attacking one or more specific entities. The Stuxnet worm is an example of one such attack, but there are many others. For most large organizations, the critical consideration is not whether or not they have been targeted (they will have been), but whether or not they have been able to identify and neutralize the intrusion.

Future risks

There are a number of trends that lie behind these increases in threats to computer-based information security, which when taken together suggest that things will continue to get worse, not better:

1. The use of distributed computing is increasing. Computing power has migrated from centralized mainframe computers and data processing centres to a distributed network of desktop computers, laptop computers, microcomputers, and mobile devices, and this makes information security much more difficult to ensure.
2. There is an unstoppable trend towards mobile computing. The use of laptop computers, personal digital assistants (PDAs), mobile and smartphones, digital cameras, portable projectors, MP3 players and iPads has made working from home and while travelling relatively straightforward, with the result that network perimeters have become increasingly porous. This means that the number of remote access points to networks, and the number of easily accessible endpoint devices, have increased dramatically, and this has increased the opportunities for those who wish to break into networks and steal or corrupt information.

damage to the victim organization. Computer fraud, conducted by staff with or without third-party involvement, has an immediate direct financial impact.

- Regulation and compliance requirements will increase. Regulators will increasingly legislate to force corporations to take appropriate information security action and that will drive up the cost and complexity of information security. Breaches will increasingly also trigger mandatory reporting requirements and lead to significant fines.
- Reputations will be damaged. Organizations that are unable to protect the privacy of information about staff and customers, and which consequently attract penalties and fines, will find their corporate credibility and business relationships severely damaged and their expensively developed brand and brand image dented.

The statistics are compelling. The threats are evident. No organization can afford to ignore the need for information security. The fact that the risks are so widespread and the sources of danger so diverse means that it is insufficient simply to implement an antivirus policy, or a business continuity policy, or any other standalone solution. A conclusion of the CBI Cybercrime Survey 2001 was that 'deployment of technologies such as firewalls may provide false levels of comfort unless organizations have performed a formal risk analysis and configured firewalls and security mechanisms to reflect their overall risk strategy'. Nothing has changed. It was clear from the UK's ISBS that there is a correlation between security expenditure and risk assessments. On average, those respondents that carried out a risk assessment spent 8 per cent of their IT budget on security. The average expenditure for those that did not was 5 per cent or less. It seems likely, therefore, that those that have not actually assessed their information security risks are also under-investing in their security.

The only sensible option is to carry out a thorough assessment of the risks facing the organization and then to adopt a comprehensive and systematic approach to information security that cost-effectively tackles those risks.

Legislation

Certainly, organizations can legally no longer ignore the issue. There is a growing number of laws that are relevant to information security. In the

United Kingdom, for instance, relevant laws include the Companies Act 2006; the Copyright, Designs and Patents Act 1988; the Computer Misuse Act 1990 (as updated by the Police and Justice Act 2006); and the Data Protection Act 2018.

The Data Protection Act 2018 (DPA) is perhaps the most high-profile of these recently passed laws; it implements the EU GDPR into UK legislation and requires organizations in both the public and the private sectors to implement data security measures to prevent unauthorized or unlawful processing (which includes storing) and accidental loss or damage to data pertaining to living individuals. Fines of up to 4 per cent of global turnover may be imposed by the Information Commissioner's Office for breaches of the DPA.

While these Acts apply to all UK-based organizations, Stock Exchange-listed companies are also expected to comply with the recommendations of the UK Corporate Governance Code and the Risk Guidance on effective controls. Crucially, these require directors to take a risk assessment-based approach to their management of the business and to consider all aspects of the business in doing so.

In the United States, most states now have data breach reporting laws, and sectoral regulation such as HIPAA, GLBA, FISMA and others impose strict requirements on organizations. While the United States still has no federal data protection legislation, California (CCPA) does. So do Canada (PIPEDA), Australia and other members of the Commonwealth. In the EU all countries are subject to the EU GDPR, the core of which is exactly the same in all member states. Emerging economies are also passing data protection and cyber security laws, recognizing that improved security is a prerequisite for competing in the data-rich developed world.

In parallel, PCI DSS, a private sector security standard, has emerged as a contractual requirement for organizations that accept payment cards and, interestingly, compliance with PCI DSS has been enshrined in law in some US states; the ICO, in the UK, has recognized its importance.

Directors of listed businesses, of public-sector organizations and of companies throughout their supply chains must be able to identify the steps that they have taken to protect the confidentiality, integrity and availability of the organization's information assets. In all these instances, the existence of a risk-based information security policy, implemented through an ISMS, is clear evidence that the organization has taken the necessary and appropriate steps.

Benefits of an information security management system

The benefits of adopting an externally certifiable ISMS are, therefore, clear:

- The directors of the organization will be able to demonstrate that they are complying with the relevant requirements of Sarbanes–Oxley, Basel 2/3, the FRC's Risk Guidance or with current international best practice in risk management with regard to information assets and security.
- The organization will be able to demonstrate, in the context of the array of relevant legislation, that it has taken appropriate compliance action, particularly with data protection legislation such as the GDPR.
- The organization will be able systematically to protect itself from the dangers and potential costs of computer misuse, cybercrime and the impacts of cyberwar.
- The organization will be able to improve its credibility with staff, customers and partner organizations, and this improved credibility can have direct financial benefits through, for instance, improved sales. This competitive requirement is increasingly becoming a critical factor for organizations in winning new business from clients that are aware of the need for their suppliers to demonstrate they have implemented effective information security management measures.
- The organization will be able to make informed, practical decisions about what security technologies and solutions to deploy and thus to increase the value for money it gets from information security, to manage and control the costs of information security and to measure and improve its return on its information security investments.

2

The Corporate Governance Code, the FRC Risk Guidance and Sarbanes–Oxley

The Combined Code

The first version of the UK Combined Code, issued in 1998, replaced, combined and refined the earlier requirements of the Cadbury and Greenbury reports on corporate governance and directors' remuneration. It came into force for all listed companies for year-ends after December 1998. Since then, UK corporate governance has been on a 'comply or explain' basis; in other words, listed companies are expected to comply but are not statutorily required to do so. Simplistically, if they have good reason, they can choose not to comply with a particular provision of the Combined Code as long as they then explain, in their annual report, why that decision was taken. However, as the market nowadays punishes companies that choose not to comply, any decision about non-compliance is not expected to be taken lightly. (In actual fact, the requirements are a bit more complex than this.)

The Combined Code requirements were broadly similar to those of the earlier reports, but in one important respect – reporting on controls – there was a major and significant development in 1999, prior to the May 2010 revision of what is now formally the UK Corporate Governance Code. While the Cadbury Report had envisaged companies reporting on controls generally, the original guidance that was issued at that time to clarify those requirements permitted, and indeed encouraged, companies to restrict their review of controls, and the disclosures relating to that review, to financial controls.

This meant that potentially more important issues relating to *operational* control were left outside the reporting framework. The current version of the Corporate Governance Code was published in September 2014 and applies to companies listed on the main UK stock exchange (but not to AIM-listed companies). Principle C.2 of the Code says: 'The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.'

The Turnbull Report

The Turnbull Report – 'Internal Control: Guidance for directors on the Combined Code', published by the Internal Control Working Party of the Institute of Chartered Accountants in England and Wales – provided further guidance in 1999 as to how directors of listed companies should tackle this issue. After multiple revisions, it is now an FRC (published September 2014) publication formally titled 'Guidance on Risk Management, Internal Control, and Related Financial and Business Reporting'. It provides specific guidance on how to apply section C.2 of the Code, which deals with risk management and internal control and establishes the principle that: 'risk management and internal control should be incorporated within the company's normal management and governance processes, not treated as a separate compliance exercise.'

Paragraph 28 of the Risk Guidance states that a company's 'internal control system encompasses the policies, culture, organization, behaviours, processes, systems and other aspects of a company' that, taken together:

- Facilitate its effective and efficient operation by enabling it to assess current and emerging risks, respond appropriately to risks and and significant control failures and to safeguard its assets.
- Help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organization.
- Help ensure compliance with applicable laws and regulations.

Paragraph 29 recognizes that 'a company's system of risk management and internal control will include risk assessment, management or mitigation of directors' report that auditors are required to comment on. This provision has been carried forward to the Companies Act 2006. This leaves no 'wiggle room' for directors; all important risk issues have to be identified and disclosed.

While the UK Corporate Governance Code is not, at first sight, relevant to any businesses other than those listed on the UK Stock Exchange, its impact is widely felt throughout the United Kingdom and through the national and international supply chains of UK-listed companies. This means that the FRC Risk Guidance will have an impact on all businesses in those supply chains, and all directors of them will need therefore to be aware of its requirements and implications. It has particular relevance to the management and security of data assets.

The UK government (through HM Treasury) adopted the principles of internal control set out by Turnbull and in 2004 published its 'Orange Book' (*Management of Risk – Principles and concepts*), in which it adapted Turnbull's recommendations to the public sector. All non-governmental organizations (NGOs) and non-departmental public bodies (NDPBs) are expected to conform to these requirements, and all government and government-controlled bodies were expected to ensure implementation and integration of the processes.

The key questions that directors of listed companies and 'Orange Book' public-sector organizations seek to answer in respect of their supply chains are the same questions that directors of companies in those supply chains therefore need to be able to answer for themselves. These questions (which are not meant to be exhaustive) now set out in Appendix C to the Risk Guidance and are quoted below. Key questions the board could ask include the following:

- Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis? (Significant risks may, for example, include those related to market, credit, liquidity, technological, legal, health, safety and environmental, reputation and business probity issues.)
- Does the board have clear strategies for dealing with the significant risks that have been identified? Is there a policy on how to manage these risks?
- Are information needs and related information systems reassessed as objectives and related risks change, or as reporting deficiencies are identified?

- Are there specific arrangements for management monitoring and reporting to the board on risk and control matters of particular importance? These could include, for example, actual or suspected fraud and other illegal or irregular acts, or matters that could adversely affect the company's reputation or financial position.

The Risk Guidance does not specify which risks should be included in the scope of the board report and what can be left out. The Guidance simply says, in paragraph 24, that 'the board has responsibility for an organization's overall approach to risk management and internal control.' It goes on to stress that the board should set appropriate policies on internal control and seek regular assurance that will enable it to satisfy itself that the system is functioning effectively. Finally, it makes the point that the board is responsible for determining its risk appetite and for putting in place adequate processes for assuring itself that its risk management objectives are being achieved.

Given the absence of definitive guidance on what risks to include or exclude, the board of directors should seek to be as comprehensive as possible. This means that (among others, including health and safety, environment, employment legislation as well as more obvious strategic risks) information risk (covered in Chapter 1 of this book) must be considered, and therefore information security management will be critical to all organizations. Equally, in assessing risks to the organization, directors will have to assess the risks associated with their supply chains. Data interdependence is a characteristic of supply chains, and therefore risks to data security anywhere in the supply chain are a risk to the whole supply chain. Boards will have to assess these risks, the scale of which were indicated in Chapter 1, and implement appropriate control mechanisms to limit their potential impact.

It is clear that systems designed to meet the requirements of the FRC Risk Guidance should be integrated into the organization. This means that the necessary internal control systems should form part of the organizational culture and be part of the day-to-day management of the organization. They certainly should not be a separate structure designed solely for the purpose of complying with the Code, nor should they be introduced from outside the organization without there being real ownership within – and from the top of – the organization. Implementation does require the entire organization to embrace the principles of the Code; this can only happen if the process is taken sufficiently seriously for it to be embraced at board level and to be owned by the chairperson, CEO and the whole board.

TABLE 2.1

	Section		
	302	404	409
Requirement	Quarterly certification of financial reports	Management's annual certification of internal controls	Monitor operational risks
	Disclosure of all known control deficiences	Independent accountant must attest report	Material event reporting
	Disclosure of acts of fraud	Quarterly reviews of updates/changes	'Real-time' implications – four business days allowed for report to be filed
Responsibility	CEO	Management	Management
	CFO	Independent accountant/auditor	Independent accountant/auditor

https://perma.cc/BD5A-K68N)). The sponsoring organizations included the AICPA, the Institute of Internal Auditors, the Institute of Management Accountants and the American Accounting Association. The PCAOB (Public Company Accounting Oversight Board, at www.pcaobus.org (archived at https://perma.cc/T6VV-SAM7), created under SOX to oversee the activity of the auditors of public companies in the United States) expects the majority of public companies to adopt the COSO framework, and its Auditing Standard No. 5 (AS No. 5), dealing with audit of internal control over financial reporting, assumes that the COSO framework (or one substantially like it) will have been adopted.

COSO identifies two broad groups of IT systems control activities: general controls and application controls. General controls are those controls that ensure that the financial information from a company's application systems can be relied upon. General controls exist most commonly as part of an information security management system (such as that identified in ISO/IEC 27001). Application controls are embedded in the software to detect or prevent unauthorized transactions. Such controls can be used to ensure the completeness, accuracy, validity and authorization of transactions.

AS No. 5 goes on, at paragraph 36, to require that 'the auditor also should understand how IT affects the company's flow of transactions. The auditor should apply paragraph 29 and Appendix B of Auditing Standard No. 12, *Identifying and assessing risks of material misstatement,* which discuss the effect of information technology on internal control over financial reporting and the risks to assess.'

IT controls are fundamental to financial control, and ISO/IEC 27001 sets out a structured approach to identify risk and select appropriate mitigation for that risk.

Enterprise risk management

Enterprise risk management (ERM) has emerged over the last few years as a fundamentally new way for organizations to approach risk. This is driven partly by the extensive overlap between the risk management requirements of SOX, Basel 2/3, and corporate governance regimes elsewhere in the world, as well as ongoing changes in the global information economy. Organizations face new and complex risks in a rapidly changing business, technological and regulatory environment. They cannot afford not to identify and control against all areas of risk – including those that might remain unidentified or unforeseen, such as currency fluctuations, human resource issues in foreign countries, changing or disappearing distribution channels, corporate governance and regulatory pressures, and the range of risks associated with technology, information and intellectual assets.

An ERM process should ensure that a uniform approach to risk identification, measurement and treatment is taken across the organization. ISO31000 is emerging as a widely recognized standard for enterprise risk management.

COSO ERM framework

COSO's internal control framework has become the *de facto* standard for companies complying with SOX. COSO started work on developing a separate risk management framework in 2001. This framework, the 'Enterprise risk management – integrated framework', was designed to provide a common framework, 'key principles and concepts, a common language, and clear direction and guidance' (as stated in its executive summary, COSO, 2004). This framework expands on the internal control

INDEX