KPMG

INFORMATION RISK MANAGEMENT

Information security survey

Six important signals

ADVISORY

AUDIT ▪ TAX ▪ ADVISORY

Introduction

For many years now, information security has been an important topic for organisations. In this respect, they face a number of substantial challenges:

- the risk factors and the nature of the threats are constantly changing as a result of technological and social developments;
- business requires more interaction with other parties through systems and networks (communication and transactions), which involves extra risks;
- new legislation and regulations make it increasingly important to demonstrate explicitly that the risks are under control;
- with regard to information security there is a strong need to control the costs of the measures.

This combination of factors prompted KPMG to carry out a review of the position regarding information security in Dutch organisations. To this end, in collaboration with TNS NIPO, we conducted a survey among 123 organisations with more than 100 employees. On the basis of this research and our own observations we formulate below six important signals.

01

The dynamics of information and communication technology continues unabated. Proper information security is only possible on the basis of sound risk analysis. In many instances this is not the case.

It is obvious that technological innovation and social developments do not stand still. In practice the speed of changes results in tough dilemmas. Any organisation wishing to protect itself structurally against threats will benefit from sound risk analysis: a periodic survey of the threats to which the organisation is exposed, the probability of occurrence of the identified threats and an indication of the potential impact of such threats. After all, only when it is clear what risks are involved, appropriate measures can be taken. It is important for organisations to take a conscious decision on the risks that they will or will not accept. From that perspective, it is remarkable that almost half the organisations do not use risk analysis in formulating information security policy.

Research results:

- **47%** of the organisations questioned do not use risk analysis in determining their information security policy.
- Of the organisations with more than 500 employees that were questioned, **30%** do not use risk analysis in determining their information security policy.

02

Insufficient expertise within the organisation itself is the most important motive for outsourcing security activities.

Outsourcing is gaining in popularity, including when it comes to the topic of information security. One of the major arguments for outsourcing security activities is a lack of expertise within the organisation itself. This is obvious: organisations find it difficult to keep specialist experience and to maintain up-to-date knowledge of security issues. Consequently they increasingly seek such expertise outside the organisation itself. Unfortunately, practical experience quite frequently shows that this results in a lack of responsibility for information security. Wrongly so, because even in the case of outsourcing, the management of the organisation remains ultimately responsible for information security activities outsourced.

Successful outsourcing requires clear agreements with the outsourcing partner on the performance of information security activities (set out among other things in a Service Level Agreement), on accountability in this context (for example by means of a SAS 70 report) and on adapting the organisation itself in line with the outsourced situation (with policy-making of course remaining a task of the organisation itself).

Research results:

- **48%** of the organisations questioned have outsourced one or more activities in the area of information security.
- **41%** of the organisations questioned outsource firewall management. This is the information security activity that is outsourced most.
- **53%** of the organisations questioned name the lack of expertise as the most important reason for outsourcing, followed by problems with 24/7 support **(34%).**

03

Hacking, viruses and worms are still considered significant threats. Organisations still have little insight into the quality of their protection against such threats.

Incidents with hackers, viruses and worms can cause an organisation a great deal of damage. Damage can occur for example as a consequence of fraud resulting from hacking into or leaks in the system and as a result of the disturbance of internal processes. Such incidents damage the organisation's reputation. Consequently, awareness in this area is high. Almost all organisations consider hacking, viruses and worms to be significant threats to the organisation.

At the same time many organisations do not know exactly how substantial the problem is and whether their technical infrastructure meets the necessary security levels. The fact that the use of performance indicators in respect of information security is certainly not yet commonplace, plays a part in this context. Many organisations find it difficult to develop the right indicators and often only gain an understanding of the quality of their information security through the results of external audits. Organisations that have access to more indicators than just the results of audits, obtain a better picture of the quality of their information security.

Research results:

- **25%** of the organisations questioned have been confronted with hacking, viruses and/or worms more than 10 times during the past 12 months.
- **25%** of the organisations questioned are confronted daily with more than 100 spam incidents.
- **72%** of the organisations questioned do not use performance indicators for information security.

04

Within organisations a large number of separate registrations for issued authorisations often exists. As a result, authorisation management usually is structured rather ineffectively and inefficiently.

In practice over the years, organisations have often acquired a multitude of systems and applications – even after the implementation of an ERP system. This multitude also impacts the way in which authorisation management is arranged. Personnel often have to use several passwords in order to perform their day-to-day work and their authorisations have been recorded in different systems. This means that various 'separate' registrations of issued authorisations exist within organisations. This situation is neither effective nor efficient.

Also from the point of view of compliance it is desirable to structure authorisation management more effectively. Legislation and regulations (such as Sarbanes-Oxley) make it necessary for organisations to explicitly demonstrate that they are in control. Authorisation management is an important part of this. Organisations that wish to comply efficiently with the requirements of legislation and regulations will therefore benefit from the concentration of authorisation management.

It is striking that IT professionals scarcely see this legislation (which has the potential to contribute to a higher level of information security) as an improvement, but above all as extra work. As the most significant effect they noticed more audits.

Research results:

- **42%** of the organisations questioned have recorded employee authorisations in five or more systems and **10%** have concentrated the authorisations in only one system.
- **33%** of the organisations questioned need one to seven days to arrange a new employee's authorisations.
- **40%** of the organisations questioned use configuration (asset) management tools.
- **29%** of the organisations questioned use enterprise security management tools.
- **15%** of the organisations questioned perceive the uncertainty whether the inventory of the IT resources is complete as the major problem with regard to such tools.
- **46%** of the organisations questioned do not (periodically) assess the correctness of the authorisations issued.

05

Continuity management: it is often organised on paper, but it is usually not certain whether it also works well in practice.

In recent decades information systems have evolved from a support factor to the beating heart of many organisations. Modern information systems can make the difference in the competitive battle and often determine an organisation's success. It is therefore of the utmost importance for these systems to be constantly available. This is after all what clients, shareholders, supply chain partners, supervisors and other interested parties expect.

Organisations are well aware of this and seek ways of preparing for calamities and other threats by scrutinising their continuity and recovery capability. It is essential for organisations to approach this systematically. It is clear in practice that improvements are often necessary and this survey confirms this picture.

Research results:

- **36%** of the organisations questioned do not have a continuity plan.
- **28%** of the organisations questioned that do have a continuity plan do not test whether that plan indeed provides effective safeguards and also actually works in practice.

06

The growing use of mobile devices demands attention.

Networks and systems are increasingly developing from closed strongholds into accessible, open structures to which employees, suppliers, customers and other interested parties are connected in various ways. In addition to ongoing chain integration the boom in the use of mobile devices such as mobile phones, PDAs and memory sticks is playing a part in this. Organisations face the challenge of achieving and maintaining an adequate level of security in these open structures, without detracting from the desired flexibility. In recent years the practice of thinking in terms of security architectures has made a cautious start. Examples are the emergence of reduced sign-on, strong authentication solutions and attention to identity management. New techniques can increase the ease of use and at the same time result in a higher level of security.

Research results:

- **72%** of the organisations questioned see the use of mobile devices as a development that will require attention in the area of information security in the years ahead.

- **80%** of the organisations questioned permit the use of memory sticks. In more than half of the cases no additional security measures are defined for this use.

- **79%** of the organisations questioned allow the use of PDAs. In **39%** of the cases no additional security measures are defined for this use.

Our view on information security

Information systems have developed into the nervous systems of our information society. Organisations that have the security and continuity of their systems in place do not need to worry about the risks.

It hardly requires explaining that organisations must take effective measures to control the security and continuity risks that come from using information and communication technology. This demands a well thought-out information security policy and a thorough periodic risk analysis in order to maintain an effective security level.

Managers still too often regard information security as an isolated phenomenon rather than as an integrated part of business management. As a result, information security has been insufficiently incorporated into the work processes. Despite the growing awareness of the importance of the human factor, its complexity is structurally underestimated. Information security also involves motivating individuals concerned and actively and enduringly changing their behavior.

Contact

About KPMG Netherlands

KPMG Netherlands offers services in the fields of audit, tax and advisory. We offer our services to a broad group of clients: major domestic and international companies, medium-sized enterprises, non-profit organisations and government institutions. The complicated problems faced by our clients require a multidisciplinary approach. Our professionals stand out in their own specialist fields while, at the same time, working together to offer added value that enables our clients to excel in their own environment. In doing so, we draw from a rich source of knowledge and experience, gained worldwide in the widest range of different organisations and markets. We provide real answers so that our clients can take better decisions.

About KPMG Information Risk Management

KPMG Information Risk Management (IRM) specialises in supporting its clients with regard to controlling the risks associated with the use of information and communication technology (ICT). KPMG Information Risk Management supports its clients at strategic, tactical and operational levels in order to optimise the use of information and ICT and further increase their reliability. Information security is one of the services provided by KPMG Information Risk Management

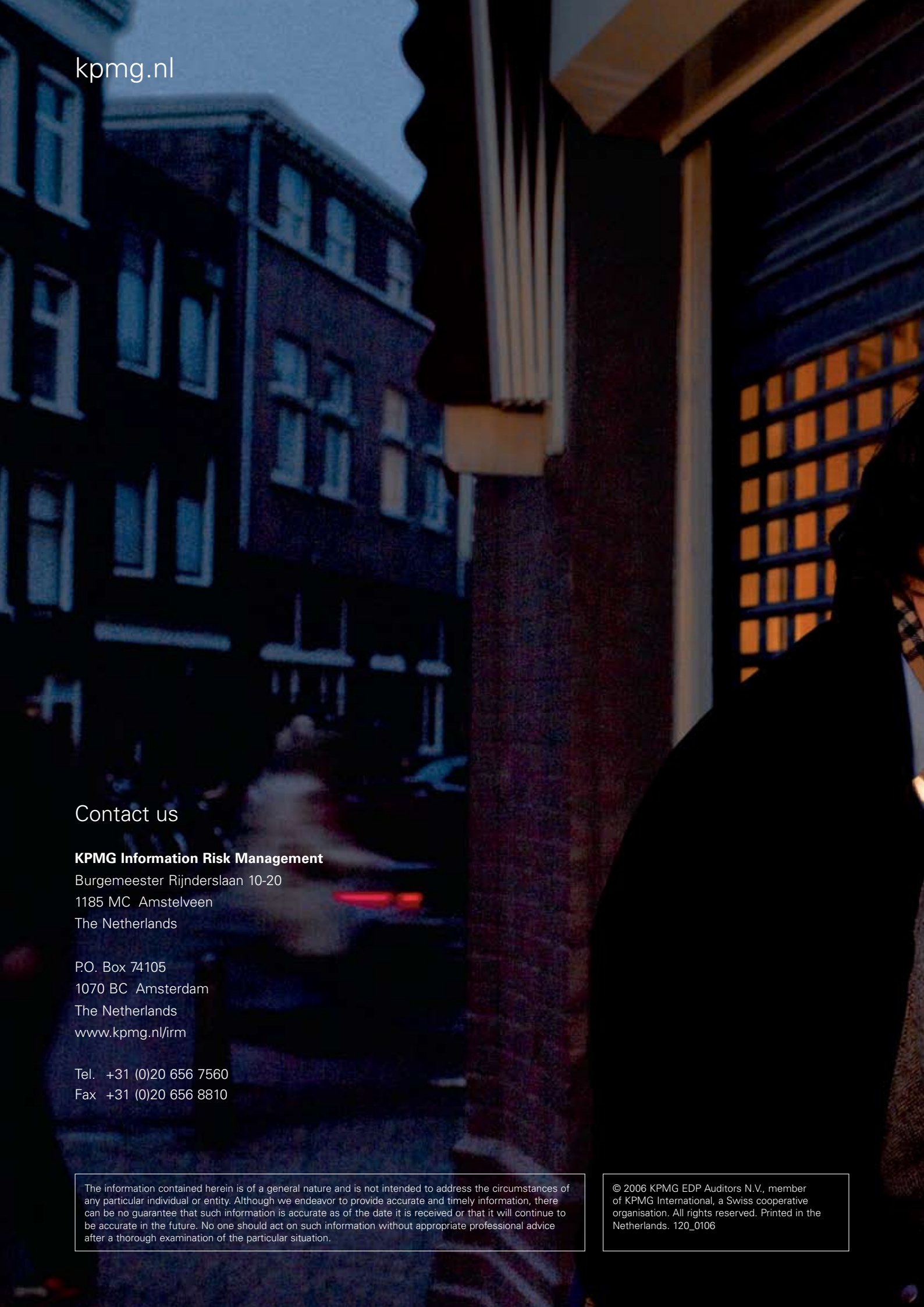
Further information

You will find further information about our services at www.kpmg.nl/irm. For a personal explanation, please call your contact at KPMG or get in touch with:

KPMG Information Risk Management
Tel. 0031 (020) 656 8383
Fax 0031 (020) 656 8388

Arjen van Zanten
vanzanten.arjen@kpmg.nl

Edo Roos Lindgreen
roos.edo@kpmg.nl



kpmg.nl

Contact us

KPMG Information Risk Management
Burgemeester Rijnderslaan 10-20
1185 MC Amstelveen
The Netherlands

P.O. Box 74105
1070 BC Amsterdam
The Netherlands
www.kpmg.nl/irm

Tel. +31 (0)20 656 7560
Fax +31 (0)20 656 8810