

Information Security

Protecting **and** sharing information

Making sure the next breach is not you



Foreword

Ciarán Kelly (Partner — Performance Improvement)

We live in an increasingly data rich society where information is more accessible and shared than ever before. However, at the same time, the need for this information to be protected from misappropriation is vital.

Advances in technology mean that organisations are increasingly dependent on information to meet the needs of customers and citizens. This information — in some cases millions of records — can be stored on highly portable devices or transferred at the press of a button.

While the transfer of data is state of the art, the tools we use often belong to a bygone era. The approach to Information Security can be likened to waging war on a modern army equipped only with swords.

Security incidents of increasing gravity continue to occur with alarming frequency. Sustained media attention results in such incidents being placed under the public spotlight, with associated impacts on reputation and customer trust.

Regulators within the EU and UK ranging from the Data Protection Commissioner to the Financial Regulator are clamping down and gaining more power to penalise businesses and organisations for both individual and systematic failures.

Coupled with this, the increasing prevalence of the 'extended enterprise', both geographically and organisationally, has added to the pressure of being able to access and share information quickly and seamlessly.

The ways of securing and protecting this information, however, have not kept pace, nor recognised the critical importance of non-IT related aspects of effective Information Security.

Are you fighting the battle with the wrong tools?

Read on and see what you need to do to effectively manage your organisation's information in the Information Age.

Information security issues

We find the following common key issues in many organisations we work with.

A lack of management priority and clear commitment

A lack of focus at the top of the organisation will manifest itself in employees either being unaware of their personal responsibilities regarding information security, or simply not being bothered about it.

We believe 'what gets measured gets done' — and objectives set at the top of the organisation need to be reflected in both business unit and personal objectives.

Information Security is often regarded as solely an IT issue

When issues of Information Security are raised, there is a tendency to focus on purely technical security safeguards, such as encrypting data on laptops or disabling USB memory sticks. This creates a false sense of security.

Thinking Information Security is solely about IT results in a failure to identify critical supporting aspects in people, process and organisation.

These four dimensions need to work together to create an Information Security framework that leverages and balances particular strengths and weaknesses in the organisation.

An inconsistent approach to information risk management

Organisations often do not identify and assess information risk in a consistent manner.

The lack of a clear understanding of which risks are acceptable, and which are not (risk appetite) results in a 'one-size fits all' approach.

Such an approach can result in high value information not being sufficiently protected and an overbearing approach to less sensitive information.

A lack of control over information in the 'extended enterprise'

Organisations often don't understand the 'end-to-end' nature of information flows, particularly where third-party service providers are involved. The ownership of an organisation's information does not stop at the organisation's physical boundary.

Accountabilities and responsibilities for storage, processing and transfer of information should be clearly identified from start to finish, irrespective of which entities are involved.

Information Security is uncoordinated with the rest of the organisation

Organisations often have a number of change programmes running at the same time, ranging from workforce planning and IT implementations to lean programmes.

Information Security considerations can often either be overlooked when planning and implementing such programmes, or added as an 'after-thought' which can be more of a hindrance than a help.

A myriad of IT applications, databases and spreadsheets

Fragmentation of information processing is prevalent in many organisations. Information passes from IT application to database to spreadsheet and back again — creating risks for how this information is managed and secured.

Short-term planning horizons can result in 'sticking plaster' solutions to information processing and management issues. To compete effectively in the Information Age, organisations must challenge themselves to lengthen these horizons.

How do they resonate with your organisation?

How does your organisation stack up?

Answering the following five questions will give you a quick understanding of how your organisation stacks up:

1. Do you know the top five Information Security risks for your organisation?
 Yes
 No
2. Do you assess and manage Information Security risks by applying the same (best practice) techniques you apply for other risks?
 Yes
 No
3. Does your organisation manage information in an 'end-to-end' approach that crosses organisational boundaries?
 Yes
 No
4. Are you confident you know what Information Security standards your suppliers are actually working to?
 Yes
 No
5. Do you think it is easy for individuals within your organisation to find simple, clear Information Security guidance?
 Yes
 No

If you have ticked 'No' more often than 'Yes', you may want to consider taking our 10 minute online, interactive Information Security diagnostic that provides you with some pointers on areas you should be addressing.

The diagnostic can be found at: <https://surveycenter.pwc.com/se.ashx?s=1A7312045960C2F2>.



Support available from PricewaterhouseCoopers



PricewaterhouseCoopers is a global leader in Information Security and privacy solutions, with more highly trained professionals in the field than any other organisation. Our multi-disciplinary teams help clients effectively identify, assess, implement and manage security and privacy solutions.

We focus on delivering pragmatic solutions, leveraging the broadest range of skills in the market. Our core strength is our global ability to deploy consistent capabilities in 120 different countries and provide truly independent trusted advice.

Within the information and data security arena PwC can provide a wide spectrum of services:

- conducting audits
- assessing the scale of the vulnerabilities and risks
- planning and executing change programmes to mitigate those risks
- mounting post-breach investigations to pinpoint what went wrong and how to prevent it happening again

Contacts

If you would like to have a conversation on any of the topics mentioned, please contact:

Ciarán Kelly
Partner

+353 1 792 6408
+353 87 810 6408
ciaran.kelly@ie.pwc.com

Kieran Mongan
Senior Manager

+353 1 792 8632
+353 87 937 3425
kieran.mongan@ie.pwc.com

Liam McKenna
Senior Manager

+353 1 792 8897
+353 86 380 5472
liam.mckenna@ie.pwc.com

www.pwc.com/ie

© 2009 PricewaterhouseCoopers. All rights reserved. "PricewaterhouseCoopers" refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin 1 is authorised by the

Institute of Chartered Accountants in Ireland to carry on investment business.