



# Information Security: A Strategic Issue

by

Jean-Noël Ezingard and Monica Bowen-Schrire

## **Executive Summary**

Research carried out in 25 UK and Swedish organisations has shown that there is a strong relationship between the importance of information systems to business strategy, organisational perception of risk and the way an organisation develops its information security strategy. This research also shows that although organisations budget for information security as a cost, they nevertheless see it as an investment. This suggests that contrary to popular belief many organisations do not see the need to do ROI or ROSI calculations. Organisations recognise that there are trade-offs to be made in information security decisions, and that controls that are too tight may hinder creativity or have a negative impact on trust in the organisation. However, despite trade-offs being recognised, a large number of information security decisions are still driven by the desire to 'keep users under control'. Interestingly, those organisations that are acutely aware of these trade-offs seem to also be those with well-resourced information security functions and those that see people as a cornerstone of their security strategy. Finally, whilst many boards take an interest in information security this interest seems to be reactive (waiting for information) rather than proactive (driving the information security agenda).

# Table of Contents

- 1 INTRODUCTION ..... 4**
  - 1.1 INFORMATION SECURITY STRATEGY: HITTING A MOVING TARGET?..... 4
  - 1.2 STRUCTURE OF THE REPORT ..... 4
  - 1.3 METHODOLOGY ..... 4
- 2 FACTORS INFLUENCING INFORMATION SECURITY STRATEGY DEVELOPMENT..... 5**
  - 2.1 A CONTINUUM OF RISK PERCEPTION ..... 5
  - 2.2 STRATEGIC USE OF IT..... 5
- 3 INFORMATION SECURITY TRADE-OFFS ..... 8**
- 4 TRIGGERS OF CHANGE IN INFORMATION SECURITY STRATEGY AND IMPLEMENTATION ..... 8**
- 5 INFORMATION SECURITY CULTURE ..... 9**
  - 5.1 MANAGING PROCESSES AND STAKEHOLDERS..... 9
  - 5.2 TRUST OR ‘US’ VERSUS ‘THEM’ ..... 10
- 6 CORPORATE GOVERNANCE AND MANAGEMENT SUPPORT..... 10**
  - 6.1 UNIDIRECTIONAL INFORMATION FLOW ..... 10
  - 6.2 INVESTMENT IN INFORMATION SECURITY..... 11
- 7 INFORMATION SECURITY BEST PRACTICE..... 12**
- 8 CONCLUSIONS..... 13**

# 1 Introduction

## 1.1 Information Security Strategy: Hitting a Moving Target?

Will 2003 be the year when the paradoxes of information security are resolved? This year has already seen an explosion of damaging viruses, worms and other forms of indiscriminate attacks on organisations' information resources worldwide. Recent statistics show that the vast majority of managers are concerned. For instance, Ernst & Young's most recent survey<sup>1</sup> shows that 90% of respondents consider information security to be very important or somewhat important to their organisations' overall objectives. Yet, the study also indicated that more than 33% of organisations felt that they were less than adequate in being able to respond to security incidents. These figures are borne up by other recent surveys. For example, the DTI reports that half of the UK businesses surveyed have suffered at least one malicious information security incident in the last year<sup>2</sup>.

Recent virus attacks have had mainly financial consequences, but the damage that a major security breach can have on an organisation can go far beyond direct financial losses and can erode brand and reputation, which can impact significantly on shareholder value<sup>3</sup>.

Yet, despite the threats posed to information security, a company's ability to capitalise effectively on market opportunities is contingent upon having an open, accessible IT environment, balanced with appropriate security controls. At the same time, threats to an organisation's information assets are becoming increasingly sophisticated and the technological environment is constantly changing. Therefore, for some organisations, aligning information security strategy with business strategy can seem to be like trying to hit a moving target.

This study was designed to investigate:

- The influence of various factors, such as stakeholders, risk perception and IT strategy on security decision-making and implementation.
- How information security evolves within organisations.

Our research has also given us some insight into best practice within this area which is presented at the end of this report.

## 1.2 Structure of the Report

After a brief discussion of methodology, we discuss risk perception and the strategic use of information technology as factors influencing information security strategy. These factors are the basis of a perception grid used for positioning organisations in terms of their information security strategy. We then discuss how organisations positioned in the different quadrants of the grid manage information security trade-offs in different ways. We subsequently report our findings on how changes in information security are triggered and the impact of changes on strategy and implementation mechanisms. The report concludes with some insight into information security best practice applied by the organisations participating in this study.

## 1.3 Methodology

In order to obtain a rich picture of how organisations deal with information security, we interviewed 25 organisations each with a minimum of 250 employees and from a wide cross-section of sectors in the UK and Sweden. The interviews were structured, and comprised both open-ended and closed questions. They were carried out in the spring and summer of 2003. A profile of interviewees is provided in Appendix 1.

---

<sup>1</sup> Ernst & Young, 2003. Global Information Security Survey 2003.

<sup>2</sup> DTI, 2002. *Information Security Breaches Survey*. DTI.

<sup>3</sup> Lohmeyer, D. F., McCrory, J., & Pogreb, S. 2002. Managing Information Security. *McKinsey Quarterly*, Special Edition: 12-15.

## 2 Factors Influencing Information Security Strategy Development

### 2.1 A Continuum of Risk Perception

As in previous research<sup>4</sup>, we have found that risk perception is one of the main factors affecting how information security strategies are developed. Organisations differ in the way that they perceive and handle risk. Organisations at one end of the risk continuum will see a breach in security as a low risk whereas others, at the opposite end, will constantly explore their own security procedures looking for potential gaps in their defences. Some organisations undertake a minimal amount of information security, such as using anti-virus software and installing an appropriate firewall. Other organisations constantly explore ways of breaching their own security so that they can continuously improve their defences and their confidence in their own safety.

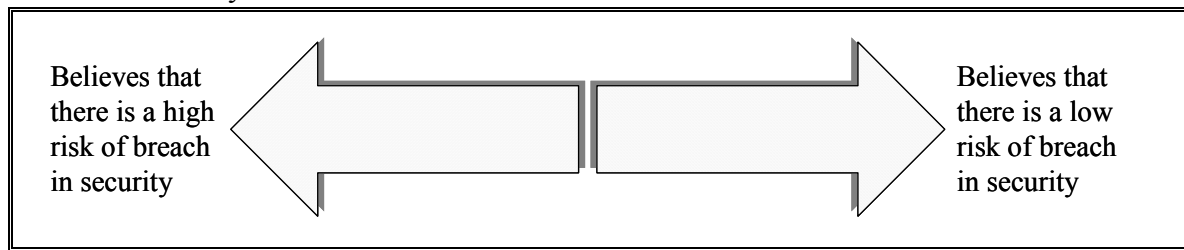


Figure 1. Risk continuum

*"Due to the level of system integration alone, anyone – such as a hacker or due to an internal failure – could access the system and display any information he or she wants. Goodwill is lost when this type of thing happens."*

*"We don't have many secrets. The kind of information we have is not very attractive to a hacker."*

The risk continuum does not represent a static situation. Organisations' perception of risk can change very rapidly, causing them to reposition themselves along the risk continuum. We have noticed that these changes often occur in response to internal and external triggers and have an impact on information security implementation mechanisms. This is explored in greater detail in Section 4 below.

#### Key findings:

- Just over half (52 %) of the organisations that we interviewed had a high perception of risk
- 60 % specifically mentioned unauthorized access to information as a result of intentional or unintentional human action as a source of risk and
- 33 % of these mentioned human error as a key area that was difficult to control (see Section 5.2 below).

*"We've been proactive in implementing solutions that would prevent information security from being compromised from internal and external attacks. However, human error is something we can't cover completely."*

*"The key area of risk is trying to stop human error. That's the biggest problem."*

### 2.2 Strategic Use of IT

Our interviews also confirmed that information security strategy is influenced by how organisations apply information technology. For some organisations, information technology will be a tool for achieving competitive advantage while for others it will only play a

<sup>4</sup> Birchall, D., Ezingeard, J. -N., & McFadzean, E. 2003. *Information Security. Setting the Boardroom Agenda*. London: Grist Ltd.

supporting role. Strategic information technology applications are those that are critical for business success, allowing organisations to gain an advantage over competitors and to create innovative new products, procedures and systems. However, although these applications give organisations a competitive advantage, they also expose them to information security risk. Alternatively some organisations see information security as an operational necessity and as playing no part in overall business strategy. Out of the 25 organisations we interviewed, we estimate that 9 used information systems for strategic purposes.

*"IT is an important part of our business processes. We are not manufacturers, we produce knowledge which is transported via IT."*

*"We have a limited awareness of the opportunities that technology can bring ... and the potential that it has as an enabler and differentiator ... we're moving too slowly."*

Is there something different about these 9 organisations in the way that they handle their information security strategy? Our proposition is that there is a relationship between the strategic importance of information systems in an organisation, organisational perception of risk and the way the organisation develops its information security strategy. This led us to position the organisations we interviewed on a 'perception grid' that models an organisation's perception of risk and the strategic importance of IT. We found that grid position has a significant impact on the way that an organisation goes about developing its information security policies and practice.

Strategic importance of IT	High	a, b, c, <i>d</i> , <i>e</i> <b>Patrons</b>	<i>f</i> , g, <i>h</i> , <i>i</i> <b>Centurions</b>
	Low	<i>j</i> , k, l, <i>m</i> , <i>n</i> , <i>o</i> , <i>p</i> <b>Custodians</b>	<i>q</i> , r, <i>s</i> , <i>t</i> , u, <i>v</i> , w, <i>x</i> , <i>y</i> <b>Sentinels</b>
		Low	High
Risk perception			

Figure 2. Perception Grid<sup>5</sup>

**Custodians** (non-strategic use of IT/low risk). A Custodian is a keeper or guardian. Custodians do not need to use information technology strategically, nor is there a tremendous amount of risk involved in guardianship. Our interviews suggest that custodians fall roughly into two equal groups – those who feel that *controls have to be tight* and those who adopt a more relaxed attitude, believing that people should be given considerable freedom.

**Sentinels** (non-strategic use of IT/high risk). A Sentinel is a person posted to guard an establishment or one or more individuals. Sentinels do not need to use information technology strategically, but the occupation does include a considerable degree of risk. Our interviews suggested that Sentinels are mainly *control-driven (rather than trusting)*. 77 % of these organisations feel that opening up their systems involved a measured risk. In the case of 33 % of these organisations, systems had been opened up for ease of business, but these were mainly tried and tested solutions. In general, these organisations tend to shy away from unnecessary risk if possible.

**Patrons** (strategic use of IT/low risk). In ancient Rome, a Patron was a former master of a freed slave or a patrician who gave legal aid to a client. A Patron uses information technology strategically but operates in a low-risk environment. Our interviews suggest that Patrons are generally *not restrictive with respect to opening up their systems* to take advantage of business opportunities. For example, the information security strategy of one Patron is *driven by business innovation*. However, while not as restrictive as the Sentinels, they do not take undue risk. In these organisations, information security is generally in place to support the business.

**Centurions** (strategic use of IT/high risk). A Centurion was an officer who commanded 100 soldiers in the time of ancient Rome. Often these soldiers were sent into battle against the ‘barbarian hoards’. Consequently, a Centurion was a leader who commanded during very hazardous times. In this quadrant, organisations use information technology strategically and operate in a high-risk environment. Our interviews suggest that Centurions are, in general, business-driven in their approach to information security. Therefore, if the business needs a

<sup>5</sup> (Organisations in italics are those that have experienced a significant change in their information security policy or procedures over the past two years)

certain information technology solution in order to develop, they will try to reduce the associated risk as much as possible and implement the solution. They are constantly grappling to maintain an optimum balance between information security and other business objectives, and ***recognise that compromises need to be made***. They also generally have a ***well-resourced information security function*** (most of the Centurions had a high ratio of information security staff to the total number of employees).

### *3 Information Security Trade-offs*

Underlying this finding – that Centurions recognise that compromises have to be made for an information security strategy to be successful, both in terms of business and risk management – is the notion of information security trade-offs which we have identified in previous research<sup>6</sup>. This research shows that information security decisions within organisations are driven by five (sometimes conflicting) imperatives that need to be reconciled by decision-makers. These trade-offs are: procedural controls versus creativity; top-down control versus trust; exposure versus ease of doing business; insourcing versus outsourcing and reputation versus the bottom line. A definition of these trade-offs is given in Appendix 2. These trade-offs also underlie information security decisions in the 25 organisations we interviewed and are balanced differently depending on where organisations are positioned on the perception grid.

*“We try to allow people access so that they can do their jobs. If we have no other option but to open up our systems we do so.”*

*“We put information systems that have to be accessed by external parties (e.g. suppliers) outside our firewalls. We have very strict procedures for connecting to the outside world, so we don't let just anyone in. We're worried about hackers who could sabotage our systems.”*

*“Before such systems are put in place, we discuss the pros and cons carefully. We find out exactly what the system does, how secure it is. We try to solve any problems by improving the technology and by constant monitoring.”*

### *4 Triggers of Change in Information Security Strategy and Implementation*

As discussed in Section 2.1 above, risk perception is a dynamic variable and a change in risk perception can be triggered at any time, causing an organisation to reposition itself on the risk continuum. More than half of the organisations that we interviewed (64 %) reported that they had changed their information security strategy in the past two years in response to an internal or external trigger. Only 25 % of these conducted information security reviews less frequently than once a year. 50 % of these were currently improving their review processes. The types of triggers reported by the organisations that participated in the study are:

- System changes (e.g. new software, changes in outsourcing arrangements)
- IT strategy review
- Virus attack
- General awareness of the need for increased security (based on incidents in other companies, media reports etc.)
- Preparation for an initial public offering or merger
- Misuse of information by employees (e.g. unintentional leaks)
- Audit recommendations/findings, that suggested there were weaknesses.

It can therefore be argued that it is, again, increased risk awareness that causes information security to change. These triggers resulted in changes being made to the organisations' information security procedures, policies and sometimes strategies. Most of the changes

---

<sup>6</sup> Birchall et al., op. cit.

involved ***low level/technical changes***, such as modifications in access privileges, transaction logs, changes in the security level for viruses and implementation of virus software (52 %). However, ***high-level process changes*** were also reported (20 %) such as an improved information security policy, an improved information security organisation with a clearer allocation of roles and responsibilities and reporting as well as decisions to implement or accelerate the implementation of ISO 17799. In the case of the Centurions and Sentinels, management was largely involved in driving the changes forward (66 %). The changes organisations made altered the balance between trade-offs. 50 % changed the trade-off between top-down control and trust, moving more towards control.

*“People are restricted by the present system and can’t do the things that they could do before.”*

*“We implemented much stricter authorization controls on the transactional level. This was not the case before. Now we have defined exactly which transactions can be performed and by whom.”*

19 % felt that these changes had helped them to achieve the right balance in that people now knew the rules of the game.

*“Things are clearer – the responsibilities are clearer”*

*“We’ve removed the ‘negative’ creativity from the standpoint of information security and have let the ‘positive’ creativity remain.”*

In three cases, however, the changes were restricting creativity, and in one case this had also impacted on the ease of doing business.

*“We’ve gone to an extreme where it is very difficult to get a password for a new member of staff. When we use temporary employees [they refuse] to give them passwords because they’re not ‘real’ employees ... I think we’ve gone too far.”*

5 Information Security Culture

## ***5.1 Managing Processes and Stakeholders***

A generally accepted practice, which is also included in industry standards and recommendations (such as ISO 17799), is that to deal with information security effectively, organisations must link processes and stakeholders to its information security strategy. Periodic reviews of risks and controls and clear roles, responsibilities and reporting for information security are also acknowledged best practice. Moreover, a multi-disciplinary approach should be taken to information security implementation, involving users, specialists, line and functional managers and auditors. One individual should be appointed to be responsible for the overall development and co-ordination of information security efforts, although the operational implementation may be distributed throughout the organisation. Allocating responsibility to a single individual in the organisation is not only a way of effectively co-ordinating information security across an organisation but a practical means of managing the sometimes conflicting attitudes and expectations of different stakeholders who influence information security in the organisation.

### ***Key findings:***

Most of the organisations we interviewed had processes for frequent reviews, with clear responsibilities and roles as well as multidisciplinary involvement.

- 44 % of the organisations that we interviewed reported that they reviewed information security more frequently than once a year
- 28 % did so once a year
- All of the organisations have designated at least one individual as responsible for information security

- In only three of the organisations that we interviewed, was this responsibility split between IT and a separate security function.

This suggests that most organisations are taking an integrated and centralised approach to information security, but that there are still many cases where information security is not reviewed as often as best practice recommends.

When reviews occur, they tend to involve multiple stakeholders. All but 12 % of the organisations reported that they had multidisciplinary teams involved in reviews and audits. When it came to implementation mechanisms, specifically communicating changes resulting from reviews to the organisation and following up these changes, all of the organisations had processes in place for communicating changes to the organisation and all but 16 % had some process in place to follow up changes. ***Centurions stand out*** in that all but one have training as part of their information security process and clearly see people as a cornerstone of their security strategy.

## 5.2 *Trust or ‘Us’ versus ‘Them’*

Our interviews also suggest that ***attitudes to users by executives and decision-makers*** could be a barrier to effective information security implementation.

Information security has its origins in the military domain. This culture is still in evidence in some organisations where information concerning information security is strictly provided on a need-to know basis and the approach taken is primarily one of control. A number of organisations prioritise control over trust (56 %), however, as most of these same organisations also acknowledge, control is not enough (78 %).

*“Trust and control go hand in hand. Without trust, regardless of how good your controls are, it won’t work.”*

Research also shows that unless users are educated about security issues, they are likely to construct their own model of threats and the level of security needed and these can be radically inaccurate, increasing the threat to the organisation<sup>7</sup>.

Given the level of perceived risk from intentional or unintentional human action as discussed in Section 2.1, organisations should be trying to tackle the problem from both sides – focusing efforts on implementing an appropriate level of control as well as educating users at all levels in the organisation, in order to break the vicious cycle of information security immaturity.

*“Good information security is reached through a good understanding of information security issues. Understanding and knowledge go together with procedural controls. This is how you achieve trust.”*

*“The best result is achieved by involving people in the process. The more you involve them, the greater the understanding they will have for information security.”*

6 Corporate Governance and Management Support

### 6.1 *Unidirectional Information Flow*

Recent research suggests that boards should ensure that they are proactively involved in risk and security management, even though implementation is delegated at the functional level within the organisation<sup>8</sup>. Whilst the majority of boards in the organisations that we interviewed received updates on the information security situation, few boards seem to be actually taking the initiative in this area.

Key findings:

- 68 % regularly communicated audit and review findings to the board.

<sup>7</sup> Adams, A., & Sasse, A. 1999. Users Are Not the Enemy. *Communications of the ACM*, 42(12): 40-46.

<sup>8</sup> Birchall et al., op. cit

- However, in only one case did we find evidence of pro-activeness on the part of the organisation's board

*"The board has a sub-committee ... which is responsible for audits. They receive and review audit findings and initiate actions to ensure that they have access to information of an audit nature. For example, they initiated the 'whistle-blower' line (a toll-free number that an employee can call and report anything that he or she feels is amiss)."*

Best practice suggests that an important criterion for successful implementation is that the management team should provide visible support and direction for information security. We found that the level of management awareness of the information security review process was even higher than board awareness. All but one organisation regularly reported audit or review findings to the management.

"We have very fast feedback. We also have written reports which are submitted to me and the CEO."

## **6.2 Investment in Information Security**

Whether or not an organisation views information security as an investment or cost can be seen as an indicator of an organisation's level of information security maturity.

In terms of budgeting and accounting treatment within the organisation, most of the organisations interviewed (92 %) regarded information security as a cost.

*"We definitely regard it as a cost. Most people want to avoid having security because it costs a lot and they can't see the concrete benefits."*

*"Today it's a cost. There is no culture of regarding information security as an investment – we don't do a ROI calculation, it is strictly considered at a technical level."*

Only two of the organisations that we interviewed explicitly stated that they performed return on investment (ROI) calculations or gave information security the same accounting treatment as, for example, information technology investments.

The quantification of risk was an area that a number of organisations (28 %) considered to be difficult. One organisation that was working with cost-revenue analysis, highlighted some of the difficulties in quantifying risk that other interviewees had expressed:

*"Usually, the consequences of an incident are huge and you can't predict all the consequences ... For example, if our main system stops for five hours, we lose revenue from our customers and have to work overtime. We could lose our customer – he might go to someone else. It might cost a lot of money to get him back. It's difficult to put a monetary value on a lost customer relationship – it's not only the cost of loss of revenue but the cost of getting the customer back."*

Paradoxically, 48 % of the same organisations that said that information security was treated as a cost in terms of accounting also said that they felt that they nevertheless viewed information security as an investment. This paradox can be explained by the fact that these organisations interpret investment in information security in different ways. None of these interpretations involved ROI calculations. Instead, interpretations ranged from information security as a necessary form of risk reduction, risk avoidance or protection to information security as an essential source of competitive advantage.

*"I think the organisation is aware that information security is something we have to do, that's why we see it as an investment, even though it's treated as a cost in the budget."*

*"It's an investment because it's an avoidance of risk."*

*"It's similar to insurance – investing in insurable events that don't adversely affect the company."*

*"Of course it's an investment. It's a part of our product. If we want the product to be good, it must be an investment ... There is no option to do things without security. Of course you can discuss the level of security and this is where the cost-benefit discussion comes in. But we have a lowest level and we can't go below this ... Customers must trust us."*

These varying interpretations indicate that expenditure on information security is risk-driven and/or business-driven. We found that taking an investment approach to information security does not necessarily include performing a ROSI (return on security investment) or ROI calculation in order to justify information security spending. In other words, investment in information security is a mindset, not a calculation.

*"Information security is about investing in finding out about risk and mitigating those risks before they have an opportunity to do detriment to the performance of the company."*

This lends support to the notion of a risk management mindset, which has also been reported by Ernst & Young<sup>9</sup>. Furthermore, it indicates that, for some organisations risk management, including information security risk, is an intrinsic part of business strategy.

The four organisations positioned as Centurions stand out in terms of their mindset. These four had all either already adopted a risk management mindset (although none are currently performing investment calculations for information security expenditure) or are in the process of rethinking their approach along risk management lines. A breach in security will have an impact on a company's reputation. Centurions, which not only have a high risk perception but are also at the cutting edge of information technology, are therefore tipping the scales in favour of risk management. For some Centurions, this means investing in reputation by investing in information security.

*"If customers don't think we're safe they won't use us ... The biggest risk is customers' perceptions of risk. The biggest risk is in the loss of reputation."*

## 7 Information Security Best Practice

For organisations whose information security needs are primarily driven by their business development needs, we identified interesting initiatives which seem to play an important role in ensuring the success of the information security policy and implementation plans in those organisations where they originate. These initiatives are listed below.

- Integrate information security into the business development process.

*"We're always thinking about information security ... Every development project involves a review of information security --- It's the person running the development project [who is in charge of the review]. The IT technical manager is always involved."*

- Make an information security survey an intrinsic part of the review process.

*"For information security audits we do a GAP analysis and a questionnaire-based survey. We survey 10% of the employees and they get almost immediate feedback in terms of results. When they have answered the questionnaire, participants receive information on how they are positioned compared to the rest of the group."*

- Raise awareness of information security in the extended organisation, including partners and customers.

---

<sup>9</sup> Ernst & Young, op. cit

*“We’re working on spreading awareness on these issues when top managers are visiting remote sites and in dialogue with customers and partners.”*

- Make information security a part of the performance appraisal process.

*“Sometimes responsibility for ensuring that corrective action is taken after an audit, can be directly related to performance appraisal in the case of senior or executive managers.”*

## 8 Conclusions

There seems to be a strong relationship between the importance of information systems and business strategy, organisational perception of risk and the way an organisation develops its information security strategy. Our interviews have also shown that an increased perception of risk – due to a number of factors, such as general awareness of incidents elsewhere, virus attacks, audit findings and information misuse – triggers changes in information security in some organisations.

As Section 4 shows, some organisations did not do enough to protect themselves from the risks that they were exposed to while Section 5.2 shows that others may be overemphasising controls. Finding the right balance will involve reviewing the strategic importance of information security and IT in general. Organisations that seem to be the most ‘at ease’ with their information security environment are those that understand that over-restrictive controls can be as damaging for business as lax attitude to security. These are the organisations that have also spent time carefully balancing the trade-offs resulting from this equation.

Finally, the research presented here also shows that information security cannot be solved by technology alone, since technology is only one of several components in an organisation’s defence of its information assets and IT infrastructure. Organisations need to recognize that information security strategy and implementation is a social process. A key factor driving this process is a substantial but complex human element in the form of different types of stakeholders interacting at different levels within the organisation. A critical success factor in managing information security effectively is therefore skill in managing and including these stakeholders in the information security process.

## The Authors

**Jean-Noël Ezingard, PhD and Chartered Engineer, is a senior member of faculty at Henley Management College, UK. He can be contacted at [jean-noel.ezingard@henleymc.ac.uk](mailto:jean-noel.ezingard@henleymc.ac.uk)**

**Monica Bowen-Schrire, MBA, is a Research Fellow at the Centre for Business in the Digital Economy, Henley Management College, UK. She can be contacted at [monica.bowen-schrire@henleymc.ac.uk](mailto:monica.bowen-schrire@henleymc.ac.uk)**

## **Henley Management College**

Henley was founded in 1945 as a place for the development of senior managers in British industry, and as such was the first business school in the UK.

Our service to industry and commerce has grown and developed over the years both in the UK and overseas, and we are now working extensively with many international companies and with companies headquartered in several countries world-wide. In the 2002 Financial Times rankings of Executive Education providers Henley was listed in the top 30 business schools world-wide and the top three in the UK. It was ranked second in the world for the amount of repeat business from satisfied customers.

Henley has developed extensive expertise as a provider of the MBA degree. The College was one of the first to provide the MBA degree through distance learning in 1984, after ten years of previous experience in masters' level provision. From the start of our MBA programme, we have stressed the importance of combining learning at a distance with learning face-to-face with tutors and fellow participants.

We now deliver the MBA in four different modes - Executive Full-Time (one year), Modular - over two years, Flexible Evening (in the City of London and in Frankfurt), and Distance Learning. In all of these we blend face-to-face learning with the use of our course materials available either on the Internet, on CD-ROM or as texts. In the EIU 'Which MBA?' Guide 2002, Henley's full time MBA was ranked 1st in the UK, 2nd in Europe and 11th Globally. Henley has also been a pioneer in the delivery of the MBA to companies, tailoring the learning mode and application of the ideas to company needs. There are currently close to 7,000 people world-wide working on the Henley MBA degree.

Henley has also pioneered the DBA degree, and now has one of the largest and most respected professional doctoral programmes in the world.

Henley Management College (UK)  
[www.henleymc.ac.uk](http://www.henleymc.ac.uk)

Henley Management College (Sweden)  
[www.ihm.se/henleymba](http://www.ihm.se/henleymba)

## **Dataföreningen i Sverige**

Dataföreningen was founded in 1949 and is Sweden's largest organisation for individuals within the IT-business. Dataföreningen got more than 30 000 members.

Computers, the Internet, and mobile phones truly shape the IT revolution. But the real revolution evolves through human beings – from their thoughts, desires, and visions. New technologies emerge from the human drive to simplify and improve.

That's why Dataföreningen wants to bring people together. We learn and develop together through our courses and network. Professionals within IT meet through our activities; they come from different industries – with different areas of expertise. People with leading technical competence, people with outstanding user competence. Meetings that enormously benefit professional and private life.

Dataföreningen i Sverige  
[www.dfs.se](http://www.dfs.se)