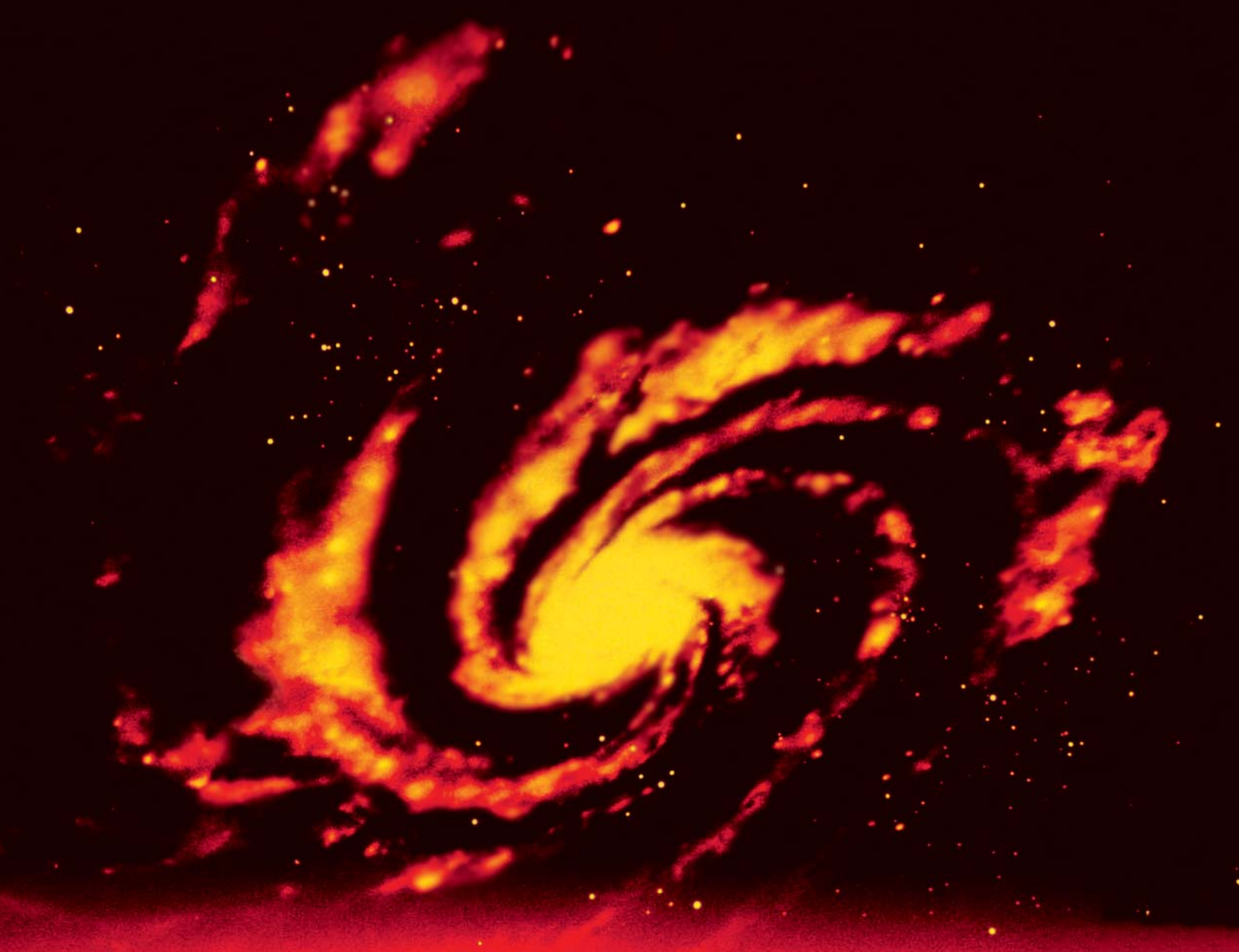


MARCH 2002

# Global Information Security Survey 2002

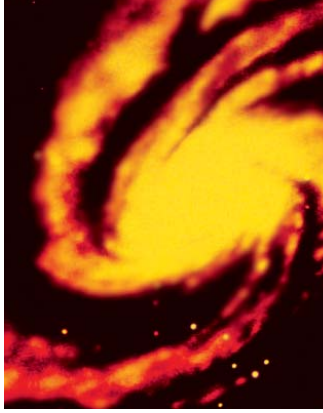
 **ERNST & YOUNG**  
*FROM THOUGHT TO FINISH.™*



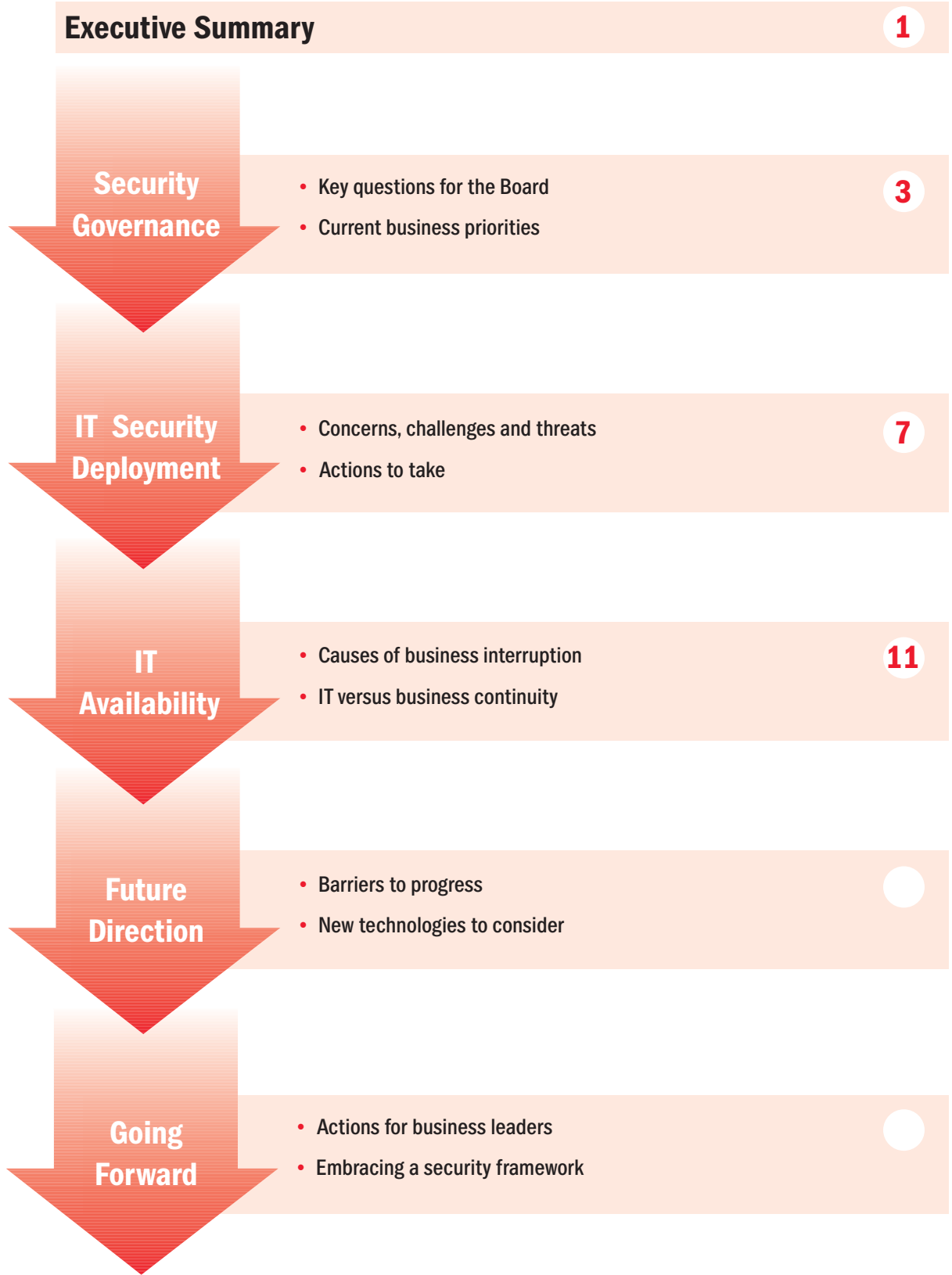
# Issues at a glance

- Only **40%** of organisations are confident they would detect a systems attack
- **40%** of organisations do not investigate information security incidents
- Critical business systems are increasingly interrupted - over **75%** of organisations experienced unexpected unavailability
- Business continuity plans exist at only **53%** of organisations
- Only **41%** of organisations are concerned about internal attacks on systems, despite overwhelming evidence of the high number of attacks from within organisations
- Less than **50%** of organisations have information security training and awareness programmes

There are some **alarming gaps** and some organisations could be judged **irresponsible** in their approach to information security, the management of which is now critical to **business survival** and **competitive advantage**



# Survey Route Map



# Executive Summary

Ernst & Young's Information Security Survey 2002 has been conducted against a background of economic uncertainty, continued media headlines of security breaches and virus infections, and the terrorist events of 11 September 2001. The timing of the survey has allowed alarmist rhetoric to subside in favour of reasoned responses to changing risk probabilities. We have spoken to leading IT Directors and business executives to understand where they see the biggest threats, how they are responding to those threats and what barriers they see going forward.

Current expectations are that economic uncertainty will continue, as will cyber threats and increasing connectivity. This means organisations need to be alert to some key issues such as:

- opportunities for disaffected staff to damage systems,
- over reliance on fewer individuals,
- increased pressure on budgets creating increased vulnerabilities,
- short term decisions on cost cutting,
- third party service providers looking for cost savings at your expense, and
- likelihood of increased fraud.

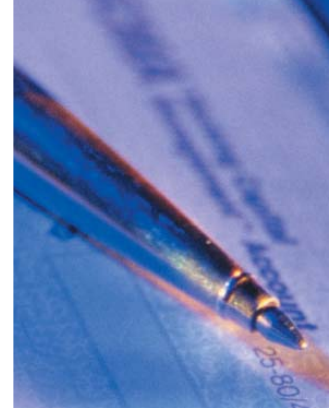
The survey examines some difficult questions. Have the events of 11 September combined with economic uncertainty pushed IT security on to the Boardroom agenda and provided the opportunity to drive good practice and discipline? Or have they resulted in short term and possibly shortsighted financial decisions? Have events triggered greater interest in piloting or implementing new technologies, such as biometrics, to address some immediate issues such as authentication? Whatever organisations are doing, is it in the right areas and is it enough?

In this report we explore the implications of some of the key findings from our survey. In summary, there are some potentially worrying indications:

- **Critical business systems** are being increasingly interrupted and yet only 53% of organisations have business continuity plans. 40% of organisations do not investigate information security incidents. In the current environment, essential basics seem to be missing.
- **The speed of change** and increasing sophistication of threats are cited as the biggest challenges to achieving the required information security. 60% of respondents expect to experience greater financial and reputational vulnerability as connectivity increases. Yet only 40% of organisations feel 'very confident' in their ability to detect attacks on systems, and less than half are carrying out security assurance activities.
- **Employee awareness** is cited by 66% of respondents as a barrier to achieving effective security, yet less than half of organisations have a security training and awareness programme in place.
- **Sourcing of internal specialist skills** is a challenge to over 50% of organisations.

In setting their priorities business leaders need to ensure that bridging the gap between the recognition of security risks and the implementation of remedies is a high priority for someone with both a broad business perspective and a solid technical understanding of the threats and vulnerabilities. Achieving recognition of the challenge is an important step, but it is only the first of many.

# ... executive summary



## How confident are you about your organisation?

Information security is still often regarded as a technical issue to be left to the IT department alone, resulting in:

- implementation of the 'bottom layer' alone,
- technology solutions without supporting business processes,
- 'point solutions' such as firewalls or virus protection.

Most dangerous of all, the Board may feel confident that the organisation is adequately protected, when in reality significant technical investments are undermined by:

- inadequate business processes,
- lack of awareness or training,
- third parties and business partners,
- absence of testing and assurance processes.

Look beyond your immediate organisational boundaries to the **extended enterprise** - their contribution and reliability (or not) is critical to achieving effective and enabling information security.

- Availability of systems and business continuity are critical to **customer** loyalty
- **Employee** awareness can make or break your investment in security technology and processes
- **Suppliers** and service providers have employees too - their lack of security awareness can seriously compromise their security - and yours
- Security threats and incidents can seriously impact share price and **stakeholder** confidence



**Engagement from the extended enterprise is critical to achieving effective and enabling information security**

# Security Governance

Security governance focuses on strategic alignment, delivering value while managing risk and measuring overall performance. In an environment where IT is both strategic and operationally critical to many organisations, what are the current information security priorities and is this view reflected in organisations' investment?

## Survey findings

**74%**  
**of respondents believe they have an information security strategy**

74% of respondents believe they have an information security strategy. If this is indeed the case, this is a very encouraging statistic, since it would provide a framework within which IT can plan and prioritise to meet strategic and operational business needs. However, as discussed later, implementation concerns do bring into question whether these strategies provide a sufficient vision to deliver a secure environment.

A key element of governance is monitoring performance. A prerequisite to monitoring is measurement. Survey responses around the cost of IT, and security in particular, indicate concerns. Information security expenditure may appear in the overall IT budget or in the business unit budget. However, organisations identified several components that were not monitored nor easily identifiable in either budget, typically application security design and management, and intrusion detection services. In addition, some expenditure, including security headcount, security specific application operations, and business continuity appears in business unit budgets as well as in IT budgets, which can make it hard to see the full picture and ensure efficient use of scarce skill sets. 73% of respondents felt the budget to be sufficient for short term needs.

61% of respondents said that IT projects overall are being rationalised, but IT security seems to enjoy some protection currently - only 34% are rationalising IT security projects and only 7% plan a decrease in security personnel. 51% believe that information security is viewed as a priority compared to other IT related projects and 35% see it as at least an equal priority. Only 13% expect to see cuts to the IT security budget, although 41% said they did not know.

70% of organisations stated they plan to enhance business continuity and IT disaster recovery plans. While this is encouraging, it is disturbing that only 29% treated business continuity planning as a business unit expenditure and 45% said it is within the IT budget, indicating perhaps, that many organisations still perceive business continuity as a responsibility of IT and not the business. Alternatively, these organisations may not recognise the wider risks of business continuity compared, to traditional recovery of hardware and software.

## What might this mean for your business?

An information security strategy provides a framework for making decisions and agreeing priorities. Many businesses develop technical plans. These may include policies, procedures and some indication of technologies - in other words, focus on technical specification. For a security strategy to be of real value it must be driven and embraced by line and functional business leaders across disciplines, and include sound consideration of the nature of the business risks and the organisation's

**51%**  
**believe IT security is currently a priority compared to other IT projects**



# ... security governance

culture. It must be a living document which drives tactical and operational decisions in all business areas. Components often overlooked are training and awareness, sourcing strategy, and performance and assurance measures.

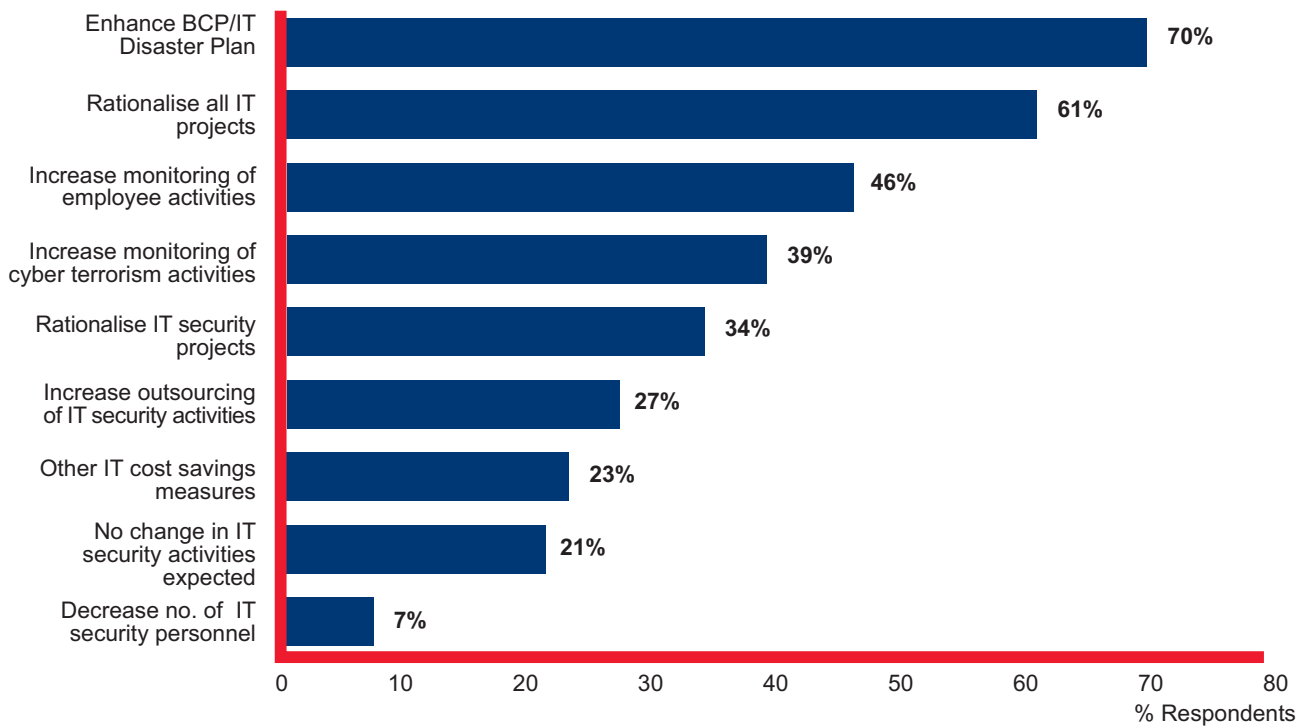
Wherever the budget sits, it must be communicated and monitored if proper control and return on investment is to be achieved. If this is not the case, there may be a lack of visibility of the overall commitment and spending priorities and spend may be duplicated unnecessarily. In addition, it can result in unexpected additional expenditure during the year. For

example, implementation spend may be in the business unit budget, but support and maintenance is expected to come from the IT budget, yet neither include security related elements.

**70%**  
*of organisations plan to enhance business continuity and IT disaster recovery plans*

If budgets are perceived to be sufficient for the short term, the questions to ask are:  
1) whether this view is based on an informed and objective business-based assessment of threats and vulnerabilities; and  
2) whether there is true visibility of the spend and its relevance to business needs.

## Actions considered in current environment



# ... security governance

**Effective security must be directed and co-ordinated at Boardroom level. Security governance is the responsibility of the Board and discussion at this level should not be avoided because of discomfort with the subject.**

**How do you ensure your security agenda is based on business requirements and not just reaction to media headlines?**

***Ask the right questions, challenge the answers and measure the results.***

1. Does your Board recognise that information security is a Board level issue and cannot be left to IT alone? Is your information security strategy aligned with your business strategy?
2. Is there clear accountability for information security in your organisation?
3. Can your Board members articulate an agreed set of threats and critical assets? How often do you review and update this?
4. Do you know how much is spent on information security and what it is being spent on? Can you measure your return on investment?
5. What would be the impact on the organisation of a serious security incident (Reputation, Revenue, Legal, Operational Performance, Investor Confidence)?
6. How does your organisation see information security as an enabler (for example, by implementing effective security, could you enable your organisation to increase business over the internet)?
7. Has your business assessed the risk of getting a reputation for slackness in security?
8. What steps have you taken to satisfy yourself that well intended (or not) third parties will not compromise the security of your organisation?
9. How do you obtain independent assurance that information security is managed effectively in your organisation?
10. How do you measure the effectiveness of your information security activities?

# ... security governance



## What can you do about it?

If you believe you have an information security strategy, challenge whether it is business risk based (versus technology alone) and is truly understood and implemented. Ensure you are getting objective assurance that it is effective. If you do not have a strategy, now is the time to act.

**1. Whether challenging an existing information security strategy, or developing a new one from the start, make sure the final strategy creates a positive response to these questions.**

- Does it consider the organisation's wider business strategy, maturity and culture?
- Is it consistent with the organisation's overall IT and business security strategies?
- Does it provide a framework for establishing security awareness, sourcing strategies, funding, priorities, resourcing, technologies and tools?
- Does it provide direction for decisions on key third parties, whether service providers or other stakeholders such as suppliers or customers?
- Is there an articulated and agreed set of threats and critical assets, prioritised and reviewed regularly?

**2. Once you have the strategy, look at IT security plans and budgets across the organisation.**

- Do you have a framework within which you can make investment decisions and determine the impact of cutting expenditure or curtailing projects?
- Do you know how much you are spending and on what?
- How do you measure your return on investment?

**3. If IT security is not on the Board's agenda, make sure it is, and not just when there is a problem. Information is an asset and information security is too important to be left to IT alone. An organisation's capability and appetite for risk management comes from the top and effective IT security can create competitive advantage.**

- Do you have visible and measurable Board support?
- Is the organisation clear where it sees itself in its approach to security and risk?
- Is information security importance reflected in investment and programmes?
- How do you ensure that technology, people and process activities related to information security are linked?

**4. Ensure accountability for information security is clear and recognised.**

- Do you have performance goals and metrics to measure effectiveness?
- Are there mechanisms to achieve independent assurance that information security is effectively managed?
- Is there organisation-wide recognition of security accountability and responsibility?

# IT Security Deployment

This section identifies our survey respondents' key concerns and challenges in achieving the required level of information security. Where do they perceive the real threats to be, based on their own experience, and what steps have been taken to address concerns?

## Survey findings

Our survey found that less than half the respondents have deployed an IT security training and awareness programme, although a further 31% plan to address this key activity. This

indicates a critical gap in effective security implementation, that is all the more surprising because three quarters of respondents stated they have an explicit and well-understood security strategy.

We regard a security training and awareness programme as a fundamental component of an effective information security strategy. This is borne out by 66% of respondents citing employee awareness as a barrier to achieving the required level of security.

**53%**  
see the internal availability of specialist skills as a challenge to effective security

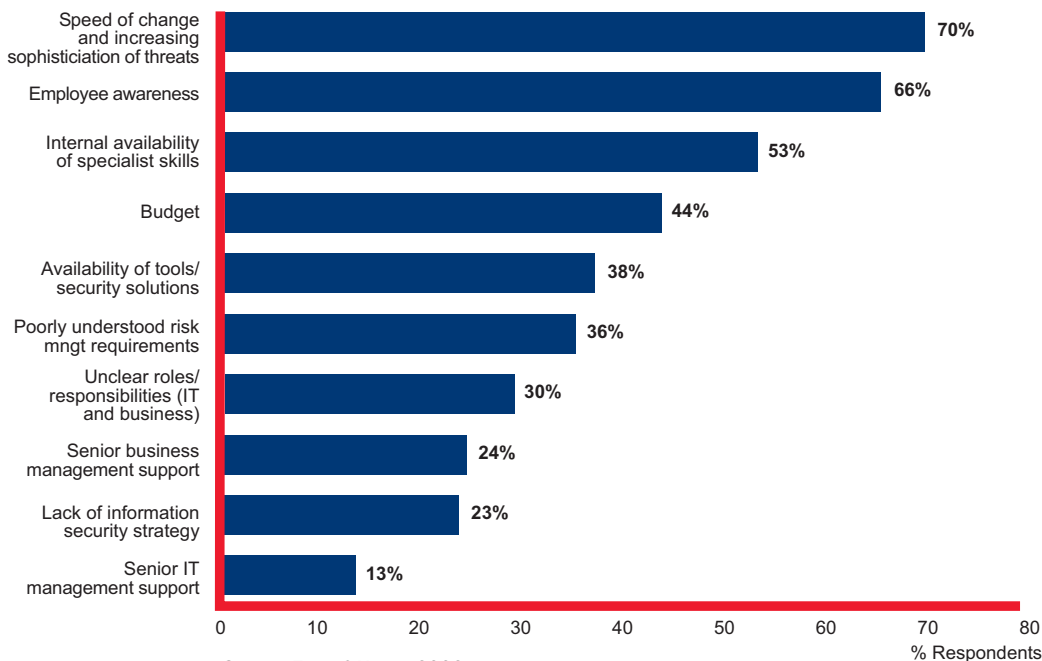
The highest level of activity seems to take place in what we regard as the 'minimum' of information systems security, for example,

- anti-virus procedures,
- access management, and
- firewall management.

40% of organisations do not investigate incidents, yet failure to investigate systems incidents increases the likelihood of undetected damage and creation of 'back doors' for later malicious use.

Only 40% of respondents admitted to having experienced a network, data or internet security attack in the past six months. This seems at odds with the statistics appearing with almost every security breach headline, which suggest that the incidence of attack is much higher. However, it is also recognised that many organisations do not admit openly to experiencing information security breaches or attacks.

## IT security challenges



# ... IT security deployment



Additionally, only 40% (up from 33% last year), of respondents felt very confident they would detect an attack. It is almost certain that some of those who are not entirely confident that they would detect an attack have actually been attacked, but were not aware of it.

Less than half of organisations are carrying out security assurance activities. How, therefore are organisations getting the confidence to know the real source of threats and that their security policies and procedures are being deployed effectively?

Yet again we see greater concern about vulnerability to external attack (57%), than internal (41%), and yet leading research groups continue to confirm that more than three quarters of attacks originate from within organisations. The other key concern is attacks on code, for example, viruses and worms (59%).

Just over 50% of respondents indicate a concern about the loss of confidentiality of data. Data confidentiality may not be critical to all

organisations, however, security and privacy concerns are still seen as the top barrier to further connectivity.

Surprisingly perhaps, only one third of organisations were very concerned about compliance with legislation and industry regulations. This is despite increased attention being paid to privacy and data protection issues, such as those evidenced by the EC Directive in Europe and Gramm-Leach-Bliley Act in the US, and expected industry pressures to improve identification and authentication measures.

The major challenges in achieving the required level of security are:

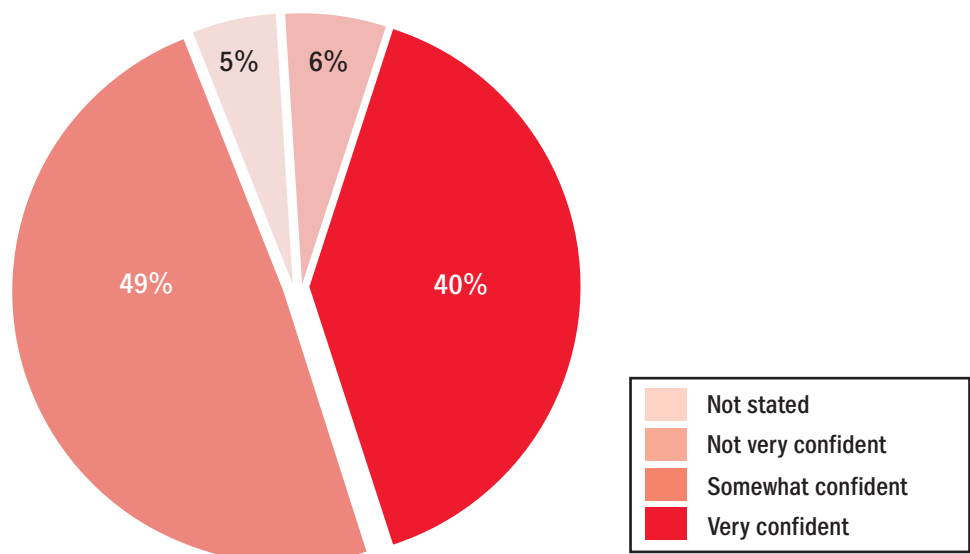
- speed of change and sophistication of threats (70%),
- employee awareness (66%), and
- internal availability of specialist skills (53%).

Only 13% see lack of IT management support as a challenge to improving information security; a higher percentage see lack of business support as a challenge (24%).

Top activities currently being outsourced to third parties are IT Internal Audit (21%), and security

**Only 40% of organisations are confident they would detect a systems attack**

## Confidence in detecting a systems attack



Source: Ernst & Young 2002

# ... IT security deployment

assurance processes (20%). There is mixed satisfaction with outsource delivery, which is not surprising given the number of variables in each situation.

## **What might this mean for your business?**

Our survey indicates progress has been made in some areas, such as virus protection. However, an alarming amount of evidence remains that

organisations are lacking fundamental management information about security breaches. This challenges the basics of decisions about IT security spend and investment, relative to business need and hard evidence.

Even for the 40% who said they were confident they would detect an attack, the key questions to ask are 1) when are attacks detected (during or afterwards, and how long afterwards), and 2) can you measure the impact?

It would be encouraging to think that the two thirds of respondents who are not very concerned about compliance with legislation and industry regulations are in this position because they have a high level of awareness of the IT implications and sound action plans to address them. The concern is that many organisations may not be aware of the regulations themselves, or of the risk in not complying with them. Business partners as well as regulators are likely to seek confirmation that organisations take these issues seriously.

The statistics about security activities seem to indicate many organisations are taking a somewhat piecemeal approach to information security. For example, anti-virus procedures and access management processes are in place, but little training and awareness activity exists to help ensure they are effectively implemented and there is limited assurance activity to help ensure compliance.

Organisations could therefore be placing a wholly inappropriate degree of reliance on some less than effective security activities, to provide corporate protection. The piecemeal approach seems to have extended to the concerns about the sources of threats. Perhaps because external hackers and security breaches continue to hit the headlines, organisations see the external threat as of greater concern than the internal.

In addition to published data suggesting a very high level of attacks originate from within an organisation, we are in a period of economic uncertainty. Difficult economic climates usually see greater motivation for individual gain, and risk of frauds or sabotage by employees. There is also the disaffected employee to consider, who may simply want to cause damage to an organisation and its reputation.

The varying levels of satisfaction with outsource delivery may indicate to some organisations that this area would seem to be a bit of a lottery. The reality is more likely to be that those who are satisfied went into the arrangement with clearly agreed and communicated expectations, and a plan which recognises the number of variables which can impact satisfaction, for example;

- understanding of business needs,
- culture fit,
- service levels,
- skills and experience, and
- technically competent in-house management of outsourcers' activities.

The mix of activities outsourced supports the view that information security outsourcing is typically driven by either 1) the need for skills and expertise that are recognised not to be a core competence of the organisation, or 2) the need for an independent view. These drivers may, of course, be supplemented by 'traditional' reasons such as cost control or improved services.

**Less than 50% have an IT security and awareness programme**

# ... IT security deployment



## What can you do about it?

**1. Know what is important to your organisation. It may be your strategic plan, financial information, product research and pricing information, personnel information, supplier details, etc.**

- Have you conducted a proper threat and vulnerability analysis including an assessment of others' capability and incentives to launch attacks?
- Have you assessed your ability to deal with the threats?
- Do you have a process to re-assess threats and vulnerabilities regularly?

**2. Agree the priorities and get the basics in place. People, process and technology combine to achieve effective security.**

- Are you confident that your anti-virus technologies and policies, for example, cannot be undermined by inadequate training and awareness activities?
- Is your firewall protection, for example, being undermined by the absence of clear policies and standards to control connectivity into the organisation?
- Do you budget and plan for effective and regular assurance activities?

**3. Once you have agreed your priorities, assess your core information security competencies.**

- Do you have qualified in-house talent who can provide robust management of security activities across the business, IT and third parties?
- What is reasonable to do in-house and what might be better done by others, either because they have greater depth and breadth of expertise and experience, or because independence is needed?
- If you are using a third party, have you conducted a rigorous assessment of their skills and capabilities, culture and their understanding of your business?

**4. Ensure you have appropriate management information to enable you to make decisions and manage information security effectively.**

- Are you receiving information on a regular basis that allows you to assess the suitability of continued connectivity with third parties?
- How are you measuring and monitoring the staff awareness aspects of your information security framework?
- What was the impact of the latest virus? Did the organisation handle it better than previous incidents?
- How recently have you reviewed your approach to detecting and monitoring both internal and external incidents and attacks?

# IT Availability

Late 2001 changed the set of probabilities that businesses face in preparing for business interruption. Respondents' views are outlined around several key questions in this section:

- What are the major causes of unavailability of critical business systems?
- Do organisations know the business impact whether financial or reputational?
- What plans are in place to address business continuity and how likely are they to be effective when needed?

## Survey findings

The top causes of business interruption failures were cited as hardware or software failure (56%) and telecommunications failure (49%). Around a quarter of failures were due to operational errors, system capacity issues and third party failures. Respondents regarded the operational impact of failures as higher than the financial or reputational impact.

Just over half the respondents have business continuity plans. Of those who have plans, many have not gone through the expected activities to develop the plan. For example, only just over 40% of organisations have carried out a business impact analysis and prioritised their critical business processes and 21% have not tested the plan. In addition, just under half the organisations surveyed have not agreed recovery timescales with the business, which could mean a wide expectation gap between what the business needs and what IT might be able to provide.

A higher number of organisations said they have IT disaster recovery plans (71%) although 16% have not tested them. Management may wish to challenge whether recovery of hardware and software is of value, if the work force lacks facilities and procedures to allow revenue-generating activities to resume.

## What might this mean for your business?

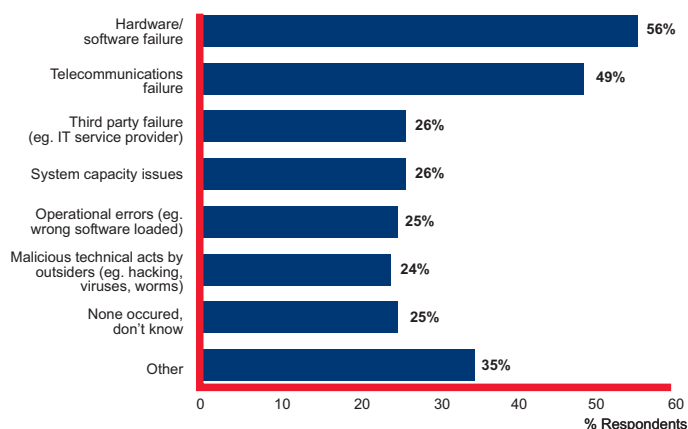
Aiming to prevent disasters is at least as important as knowing what you will do afterwards, which is why we were interested to understand the key causes

of failure. The fact that top causes were cited as hardware and software, and telecommunications failures is not of itself surprising. What is disturbing is the number of failures attributed to operational errors, system capacity issues and third party failures. These could be the result of poor management of operational basics, such as sound operational procedures for loading new software, change management and capacity planning.

The results also pose the question of whether organisations are able to quantify the financial and reputational impact of operational downtime, compared to simply recognising operational impact. Also of concern is that most respondents could not articulate the operational loss in business terms, for example, the opportunity cost or financial cost of 10,000 employees without access to systems for four hours.

Evidence abounds about the number of 'IT dependent' businesses without tested business continuity plans which fail to survive a disaster. It is hard to identify those organisations that are not IT dependent in today's world and this makes the recurring statistics about the number of organisations without plans all the more alarming. Even where they have been developed, many plans may not be effective if they have been developed in isolation of the business, or have not been tested.

## Causes of unavailability of critical business systems



Source: Ernst & Young 2002

# ... IT availability



## What can you do about it?

**1. Know what is important to your business and the threats it might face - this is key to achieving a consistent understanding of business priorities.**

- Do you know what would be the impact on the organisation of a serious security incident or loss of availability in terms of reputation, revenue, legal, operational performance and investor confidence?
- Have you identified and assessed the major threats to your business?

**2. Ensure you have good operational procedures supporting your critical IT services.**

- Do you know what has been the cause and impact to date of systems operational failures?
- How robust are your procedures for making changes to operational software?
- How confident are you that data backups work and are genuinely being taken off site in accordance with

**3. Review your approach to business continuity planning (including consideration of third parties).**

- Have you followed a formal approach to develop your recovery plans?
- Have you done enough to identify and minimise the risks to your business operations?
- Have you considered the full end-to-end business process? Was the business involved in assessing what is needed for recovery and agreeing recovery timescales?
- Are the plans robust enough to deal with a range of disasters?
- Have you challenged assumptions used in developing plans?
- Are your plans over reliant on key individuals to manage the crisis?
- Will you be able to access both your recovery and offsite data storage locations following a disaster?
- Are you confident you know what your service providers will supply if you need to call on them?

**4. Test regularly and update arrangements accordingly.**

- How will you communicate, test and review business continuity plans regularly? Consider using a range of disaster scenarios in the testing of the plans (for example, inability to access a key building, a supplier failure, or enterprise wide virus attack). Review and update plans accordingly following tests.

# Future Direction

Do organisations see an increase in vulnerabilities going forward as connectivity increases? What are the barriers to growth and what use can organisations make of new technologies?

**Security and privacy concerns are the top barriers to further connectivity**

Information security should be built into the design of new systems. Therefore watching the security horizon and preparing for the future is a critical part of an information security strategy. Our respondents provide views on vulnerabilities as connectivity increases, outline their plans to make greater use of technologies as they develop, and predict the barriers they expect to face.

### Survey findings

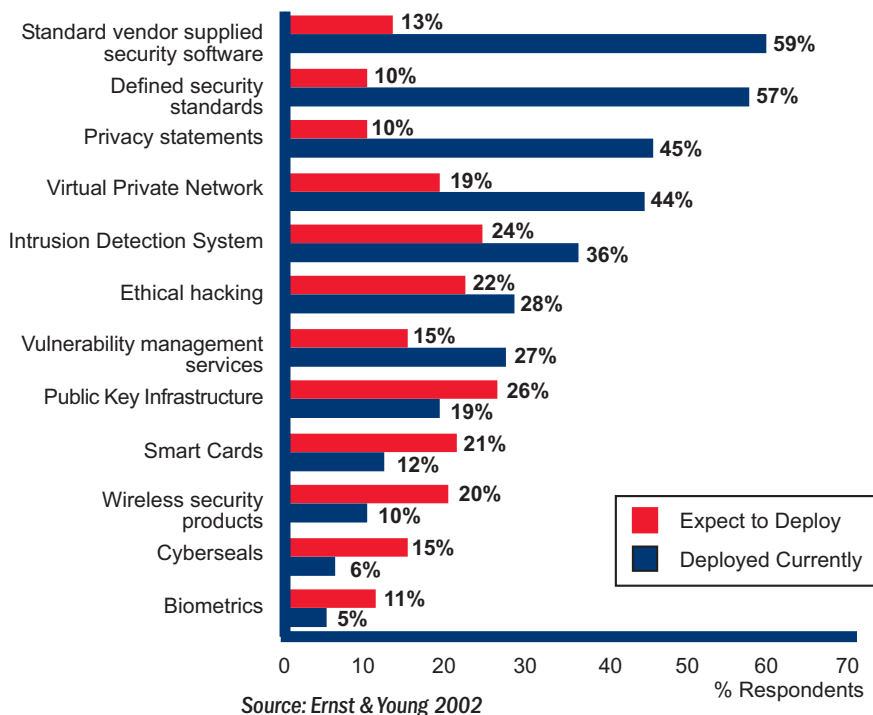
Two thirds of organisations believe risks will increase due to increased connectivity and as last year, security and privacy concerns are seen as the top barrier to further connectivity. Only 22% cited confidence in business partners or third parties as a barrier and yet effective information security is

critically dependent on major stakeholders including employees, suppliers and business partners.

Top technologies in use are standard vendor supplied software and defined security standards. Current take-up of advancing information security technologies is still relatively low. 19% are piloting or widely deploying Public Key Infrastructure (PKI) and a further 26% are planning to pilot it. Biometrics is in use at only 5% of organisations and only a further 11% plan to pilot it. Given the increased interest in authentication in recent months, this number is surprisingly low. 36% of organisations are making use of Intrusion Detection Systems (IDS) with a further 24% expecting to deploy.

A number of barriers to increased use of these technologies are cited. Cost is stated by 38% as a major barrier, although lack of skills, lack of understanding of potential technologies and technical issues are also seen as barriers.

### Current and planned use of technologies



# ... future direction



## What might this mean for your business?

**60%**  
of organisations  
expect to  
experience greater  
vulnerability as  
connectivity  
increases

Reduced interaction with business partners is not an option.

Increased connectivity is here to stay and will increase risk.

Efforts to demand and prove agreed levels of assurance on an on-going basis should be a top priority for business and IT leaders.

Since security and privacy concerns are still the top barrier faced by survey respondents, organisations need to find accelerated means to understand risk, the risk profile for the

organisation and the necessary actions to address risk. Results appear to indicate some continued resistance to the deployment of new technologies such as biometrics, wireless, and cyberseals, with a number of reasons given for non-deployment. These may indicate a lack of clarity and understanding about where the various technologies are in terms of maturity and market implementation and their potential applicability to resolve current top concerns such as identification and authentication.

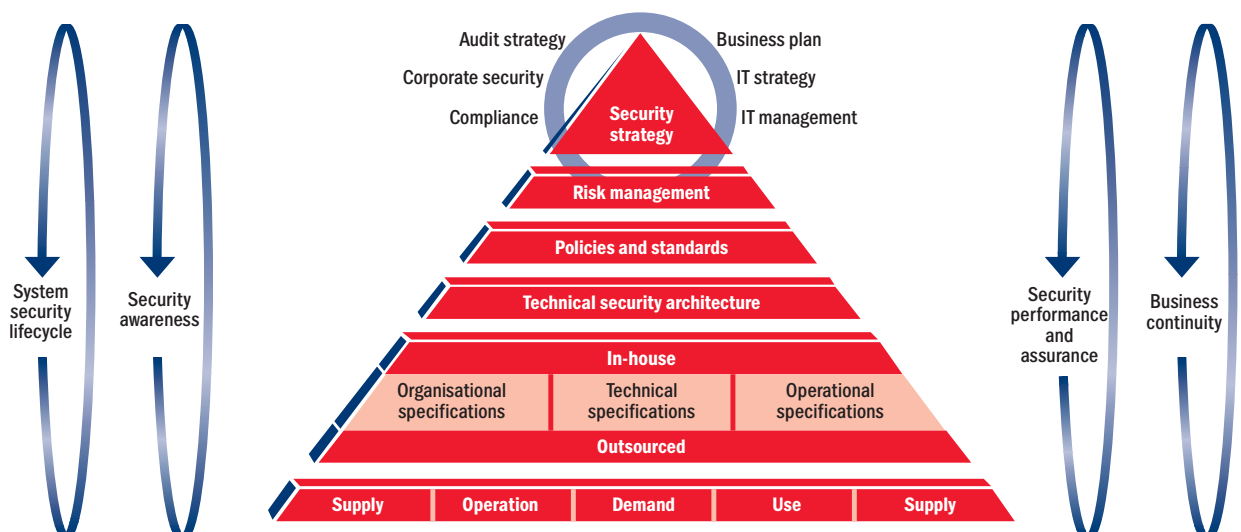
Security is a priority for IT investment in many industries and recent events have heightened this. Organisations that are not assessing how new technologies can help are likely to be missing a huge opportunity to address security issues.

## What can you do about it?

- 1. Assess (or re-assess) where your organisation will need to be in the future in terms of security and risk within the context of your business strategy.**
  - When making major organisational changes to gain competitive advantage, do you take into account whether your security organisation is capable of supporting your plans?
  - Has the money you have spent on security reduced your organisation's risk? Do not assume it has.
- 2. Consider the aspects of security which are critical to your organisation, for example, identification and authentication.**
  - Have you performed a risk assessment? Consider whether you have too much or not enough security to support your organisation.
  - Are your employees aware of the need to protect corporate information, systems and facilities?
- 3. Consider what technologies could provide you with more effective security whether in terms of cost, service, reliability etc. As with all technologies, assess your needs first.**
  - Have you integrated security requirements from the beginning when you are developing new systems? Retrofitting security is always more expensive.
  - Are your organisation's future needs taken into account when purchasing new supporting technologies? Technology cost tends to go up when planning is inadequate.
- 4. Implement a rigorous information security investment appraisal programme.**
  - Does the programme provide for portfolio assessment, prioritisation and identification of dependencies?
  - Does it include rigorous post-investment appraisal?

# Going Forward

- Despite awareness and recognition of threats, there are some alarming gaps in organisations' responses.
- Many organisations appear to be wrestling with increasing interruptions to critical business systems; uninvestigated security incidents; lack of business continuity planning; gaps in employee awareness and the challenge of increasing sophistication of threats.
- Addressing these gaps in isolation exposes organisations to all the risks associated with short term thinking.
- Effective information security requires a framework which looks to the future. This enables organisations to incorporate security into business strategy and planning, manage investment and build consumer and investor confidence.
- Using a framework ensures that the development and implementation of any security related activity incorporates consideration of the critical elements of business.



Copyright: Ernst & Young

## Information Security Framework

# ... going forward



- **Given the widely known body of threats and vulnerabilities and the accepted criticality of systems and information, a reactive strategy can appear irresponsible.**
- **Without a tick in every box, business leaders, prospective alliance partners, non-executive directors and security professionals would be well advised to take action.**

- ✓ **A consistent, integrated view across the organisation of the importance of information security**
- ✓ **A balanced approach between technology, process and people**
- ✓ **A clear view of spend and measured return on investment**
- ✓ **Regular and robust assurance activities**
- ✓ **Performance goals and metrics to measure effectiveness**
- ✓ **A plan for regular reassessment of risk and security**

**The time has arrived for business leaders to understand, anticipate and manage information security and availability as a business-wide priority for both survival and competitive advantage.**

## **Methodology**

During October and November 2001, Ernst & Young conducted a number of face-to-face and telephone interviews using a structured questionnaire among a representative sample of CIOs, IT Directors and business executives in countries worldwide. A total of 459 interviews in 17 regions were completed and responses were analysed on an anonymous basis by IDA, a recognised market research agency, to produce aggregated, tabulated results.

The main survey findings have been analysed in full for each question, profiled by country and a range of industry sectors. In statistical terms, the sample achieved will provide 95% confidence limits of plus or minus four percentage points at the 50% level, on average.

In analysing the results, we have referred to Ernst & Young security surveys carried out previously with the aim of identifying trends and change rather than direct comparison.

ERNST & YOUNG LLP

[www.ey.com](http://www.ey.com)

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member practice of Ernst & Young Global.

© Ernst & Young LLP 2002. Published in the UK by Presentation Services.  
All rights reserved. 9597 2/2002 (UK)

Further information can be found at [www.ey.com](http://www.ey.com) or your usual Ernst & Young contact.

### ***Ernst & Young – solutions for the issues that matter***

Ernst & Young's worldwide organisation is a global business committed to being the trusted business adviser who contributes most to the success of people and clients by creating value and confidence. Ernst & Young's broad range of services and solutions is delivered on an integrated basis in more than 130 countries.

Ernst & Young's network of information security professionals worldwide offers unparalleled depth of security and control experience and expertise.