

Real Time Club

The place for impassioned discussion about the information society

[HTTP://WWW.REALTIMECLUB.ORG.UK](http://www.realtimeclub.org.uk)



ICT Banana Skins 2004

A survey of the risks facing the industry

RTC is supported by



Report sponsored by
Mishcon de Reya

ICT Banana Skins 2004

Preface

Towards the end of 2003, the Real Time Club, as part of its normal program of debates on key issues facing our industry, organised a meeting with the theme of "ICT Banana Skins". We asked Kiran Sandford of Mishcon de Reya, to lead this discussion.

As we progressed with our preparation, it became clear that we would have at the end a wealth of information, from many of the leaders in the IT industry, and that if we were to follow the successful model of the CSFI's Banana Skins report for the banking industry, we could potentially have a valuable vehicle to assist the industry in its future planning. We would like to thank CSFI for the generous advice and guidance as we developed this report, and for the permission to use the same format as their survey.

Following our debate, at which we had collected a significant amount of input, we asked our Secretary, Stephen Aitken, to conduct a survey of our membership, and of others associated with the RTC, in order to present as comprehensive a view as possible of the potential traps and pitfalls. This report is the result of this work.

It is obvious to us that the first version will provoke a number of reactions from the readership including "Why didn't they include xxx". For that reason amongst many others we decided to follow the lead of CSFI, and have decided to make this an annual report. We therefore will in the fourth quarter of 2004, repeat our survey work, and subsequently publish our second edition. We welcome your comments, which should be addressed to Stephen at stephen.aitken@theStrateg-e.com

We hope that you find this report thought provoking, and even contentious. If we alert some of you to potential problems, which you may not have considered, and which you take steps to avoid, then our efforts will have been worthwhile.

John Gallop, Chairman. Real Time Club

Foreword

We are pleased to be able to sponsor this survey. As a law firm, we are very aware of the fact that law has a bearing on many IT related issues. This is borne out by the results of the survey.

It is not surprising that the top four banana skins are all security or attack related. We have noticed that businesses have increasingly become concerned about vulnerability to outside attack over the past few years. International cybercrime is becoming much more organised. Hackers are banding together in groups and the financial gains to be made from interfering with transactions such as Internet banking can be significant.

The perception that organisations are concealing cyber attacks is very interesting. It may be that those organisations are not deliberately setting out to conceal attacks but that they consider that they have nothing to gain (and everything to lose in terms of reputation) by reporting them. Current legislation is ineffective in dealing with many attacks. Where such legislation exists, it differs from country to country. Even if the perpetrators can be tracked down, it is often difficult to bring them to book (especially if they are outside the UK).

Organisations must have the incentive to report cyber crimes and know that the report will be followed by effective action. This will only come about if there is international cooperation, as cybercrime knows no territorial borders. Businesses should consider setting up an international body to whom reports can be made. Such a body would need the backing of effective international legislation which enables criminals to be tracked down and punished accordingly. If criminals are brought to book, attacks may diminish. The European Convention on Cybercrime is a good starting point but so far has only been ratified by four countries. Much more is needed if the widespread perception that cybercrimes are being concealed is to be dispelled.

Kiran Sandford, Mishcon de Reya

January 2004

About this survey

The survey was conducted in December 2003 and is based on 28 responses from 150 members and some friends of the Real Time Club. The questionnaire (reproduced in the Appendix) was in four parts. In the first respondents were asked to describe in their own words their main concerns about the future of the ICT industry for both suppliers and customers over the next two to three years. In the second they were asked to rate a list of potential banana skins, both by severity (1 = low, 5 = high) and whether they were rising, steady or falling. In the third they were asked how prepared their own and other organisations were to handle the main risks identified. In the fourth they were asked whether they were a supplier, customer or observer of the industry and whether they wished to be identified with any remarks they had made.

Some respondents did not feel able to rate every risk. Where this occurred the response was not counted in calculating the average for that risk which determines the order of risks shown in the table in the Introduction and Summary.

This report was compiled and written by Stephen Aitken, Secretary of RTC

About the Real Time Club

Some 150 entrepreneurs from the IT community are members of the Real Time Club. The Club meets for discussion, debate and dinner on a regular basis and has done so continuously since 1967, indeed our very name derives from the work done on Real Time computers in the early UK software industry. Our meetings are stimulating, challenging and enjoyable whilst always addressing key issues of the day.

The Club has been described as a "Dining/Debating Society with attitude". Our speakers are leaders of a diverse range of sectors including Finance, Business, Education, Computer/Telecommunications industries and Government. A proportion are entrepreneurs who have or are developing highly successful, frequently international hi-tech businesses. Whilst having a strong interest in technology, the Club prides itself on being business focused. Indeed some of our earlier members created the very first companies in the world that provided "Real Time" computing. Membership is open to IT professionals and others interested in keeping closely in touch with the commercial and social impact of IT and to those who wish to contribute to and influence the development of our industry for the benefit of the whole community. To find out more about the club and forthcoming meetings please visit www.realtimeclub.org.uk

This report does not reflect the views of Mishcon de Reya, the Sponsors

Table of contents

Preface	1
Foreword.....	1
About this survey	2
About the Real Time Club	2
Introduction and Summary	5
Risers and Fallers	6
New Risks identified during the survey	7
Preparedness.....	8
THE BANANA SKINS	9
1. Concealment of attacks (rising).....	9
2. Phishing undermines Internet banking (rising)	9
3. Unexpected attacks (rising).....	10
4. Cyber Terrorism (rising)	10
5. National Grid fails (rising)	10
6. Data protection too onerous (rising).....	10
7. Offshore outsourcing hits UK employment (rising).....	11
8. Users vs IT professionals (rising).....	11
9. Personal ID card fails (rising)	12
10. SPAM halts the Internet (rising)	12
11. Hackers unite (rising).....	13
12. Extra-territorialism escalates (rising)	13
13. Disaster recovery found wanting (steady).....	13
14. Disgruntled IT employee (steady).....	14
15. Non-resilient systems - insufficient redundancy in systems (falling).....	14
16. IT Governance (steady).....	14
17. Copyright law litigation hits UK corporates (rising).....	14
18. System suppliers in court (rising).....	15
19. Intellectual Property Rights Enforcement Directive (rising).....	15
20. Systems demographics disasters (steady).....	15
21. Wireless systems setback (rising).....	15
22. Websites damage global brands (steady)	16
23. SCO suit succeeds (steady)	16
24. The Disappearing IT Director (steady)	16
25. Knowledge economy fails (steady)	17
26. Legacy systems halt (falling)	17
27. Outsourcing put on hold (steady)	17
28. European Software Licensing (rising).....	18
29. Drive by wire (or wireless) accidents (steady)	18
Appendix: Survey Questionnaire	19

Introduction and Summary

ITC Banana Skins 2004 are ranked in descending order of severity of the risk. Severity is defined as the likelihood of it happening times the cost to the industry if it does.

Five of the top eleven risks are related to attacks on information and communication systems via the Internet or otherwise. Concealment of attacks is seen as the most severe, closely followed by Phishing, then Unexpected attacks and Cyber terrorism, then Hackers unite at 11. Also in the top ten at 10 is SPAM halts the Internet – which could be considered an inadvertent or direct attack. Most of these are relatively new phenomenon and are new risks we have to accept and manage if we are to enjoy the benefits of ubiquitous computing and communications.

The National Grid fails is in at 5 probably because of recent and predicted failures in Electricity supply in UK, USA and Europe, which have an effect on transport systems as well as businesses and households.

Data protection too onerous is in at 6. Although we want more protection for the individual the new laws are seen as preventing the effective conduct of e-commerce.

Offshore outsourcing hits UK at 7 is seen as a serious and growing risk to the ICT industry and the UK economy although there are recent signs of a reversal in call centre outsourcing.

In at 8 is the perennial problem of Users Vs. IT professionals – we still don't communicate effectively and this leads to unsatisfactory systems, failing systems and end users developing their own systems.

At 9 Personal ID card is seen as having a high risk of failure and if it does expensive consequences for users trust in IT and the development of systems, mainly public services related, that would use it.

Combinations of these risks, “bunches of banana skins”, can occur e.g., Offshore outsourcing and Data protection. If companies transfer personal data outside Europe they should ensure appropriate safeguards are in place enabling the same levels of data protection, or the individuals concerned have consented to the transfer of their data abroad. Also the company must ensure that the offshore outsourcing service provider meets other key criteria, such as guaranteeing levels of security and employee reliability. Similarly Outsourcing may exacerbate the problems between Users vs IT professionals, which may have a knock on effect on IT Governance.

ICT	Banana Skin
1	Concealment of attacks
2	Phishing
3	Unexpected attacks
4	Cyber Terrorism
5	National Grid fails
6	Data protection too onerous
7	Offshore outsourcing hits UK
8	Users vs IT professionals
9	Personal ID card fails
10	SPAM halts the Internet
11	Hackers unite
12	Extra-territorialism
13	Disaster recovery found wanting
14	Disgruntled IT employee
15	Non- resilient systems
16	IT Governance
17	Copyright law litigation
18	System suppliers in court
19	IPR Enforcement Directive
20	Systems demographics disasters
21	Wireless systems setback
22	Websites damage brands
23	SCO suit succeeds
24	The Disappearing IT Director
25	Knowledge economy fails
26	Legacy systems halt
27	Outsourcing put on hold
28	European Software Licensing
29	Drive by wire accidents

Risers and Fallers

Although offshore outsourcing is only seventh in the risk table it is the fastest riser being seen as a significantly increasing danger to the UK ICT industry and economy.

Copyright law litigation is also seen as rising fast although only 17th in severity – due to the new laws.

Others on a rising trend like Concealment of attacks, Cyber terrorism, Phishing, Personal ID card fails, SPAM, Unexpected attacks, Hackers unit and Data protection too onerous are also seen as high risk.

Users vs. IT professionals and National grid fails are just rising here although both are in top 10 of risks.

Only Non-resilient systems and Legacy systems halt are seen to be falling – so we think we have got some of the basics onto a falling risk trend.

ICT Banana Skin	Trend
1 Offshore outsourcing hits UK	Rising
2 Concealment of attacks	Rising
3 Cyber Terrorism	Rising
4 Copyright law litigation	Rising
5 Phishing	Rising
6 Personal ID card fails	Rising
7 SPAM halts the Internet	Rising
8 Extra-territorialism	Rising
9 IPR Enforcement Directive	Rising
10 Unexpected attacks	Rising
11 Hackers unite	Rising
12 Data protection too onerous	Rising
13 System suppliers in court	Rising
14 European Software Licensing	Rising
15 Wireless systems setback	Rising
16 Users vs IT professionals	Rising
17 National Grid fails	Rising
18 Websites damage brands	Steady
19 Systems demographics disasters	Steady
20 Drive by wire accidents	Steady
21 Outsourcing put on hold	Steady
22 Disaster recovery found wanting	Steady
23 IT Governance	Steady
24 Knowledge economy fails	Steady
25 Disgruntled IT employee	Steady
26 The Disappearing IT Director	Steady
27 SCO suit succeeds	Steady
28 Non-resilient systems	Falling
29 Legacy systems halt	Falling

New Risks identified during the survey

The survey questionnaire was designed following several planning meetings and a debate on 25th November 2003, which identified 29 banana skins. Question 1 in the questionnaire asked respondents to describe their main concerns about the future of the ICT industry for both suppliers and customers as they looked ahead over the next two to three years. Where possible these risks were linked with the initial 29 risks and are discussed in the main body of the report: for instance complexity is discussed under Knowledge economy fails. Respondents identified the following additional risks.

U.K. Government stifling innovative solutions.

“In order to “reduce risk” government tenders have a series of tender pre-qualifications that effectively preclude small (or even quite large private) companies from being considered for tenders other than as a very ‘junior’ partner in a ‘partnership’ or as part of a ‘consortium’ bid. The problem is that the main considerations now seem to centre around size of balance sheet, turnover, number of employees, profitability and of course ‘salesmanship’ rather than asking, can they actually do the job? As government buyers have all heard about an IT disaster they all operate a ‘herding’ mentality when taking these decisions. Most good IT solutions over the years have been designed and built by a small number of highly committed people rather than an amalgam of available fodder! The ‘low risk’ purchasing strategy, is actually very high risk!” Denis Saunders, a supplier

And in a similar vein

“HMG/Commission and their regulators preserve current suppliers/industry structures (whether by accident or design) rather than helping/expediting the transition to those needed for the UK to be a serious player in the global knowledge economy” Philip Virgo, an observer

Failing to achieve a Strategic Vision for Mobile Access

“The pace of new technology in mobile access is increasing. Numerous alternative mobile or tetherless access technologies are coming to market. The WiFi business is evolving, raising issues of access security and charging as it progresses and a multitude of broadband wireless access technologies are being deployed by various companies – some such as IP Wireless with claims of mobility. However what the mobile worker wants is access anywhere, at high speed, using light, high performance devices and without the need for multiple accounts to be set up or different or difficult connection procedures to be learnt. For me there are three essentials for success, which will be required:
A single closely linked set of standards – think GSM
Inter-operator business linkages to enable the all-important single account/ single access.
Global vision – it’s no good if Europe goes one way, Japan another, USA another and China a fourth. So where’s the banana skin? It lies in the path of the multiple companies who to-day are appearing to push a particular access technology as the basis for a business, rather than working from fundamental customer needs and then deploying the business systems, partnerships and technology to meet those needs. Start with the right strategic vision and work to meet it and you will succeed.” Hugh Collins, a supplier

And a risk for government and industry where organisations are failing to make necessary business process changes to remain competitive

“Short term priorities especially around share price and quarterly results will delay fundamental re-alignments of industry verticals/stovepipes, making the ultimate adjustments (which will have to be made in order to survive) more painful than if they were grasped early on. Essentially there is still a gulf between technology driven business process re-engineering, and the senior line-management in many corporates. So my concern is that there may be casualties before such change is made. My other concern is that undue delay may mean that the initiative is seized by major emerging economies in Asia, writing the business processes for the rest of the world to follow- that may be good, or it may not be”. A supplier

Preparedness

We asked respondents to say how well prepared they thought their own and other organisations were to handle the main risks they had identified. No one thought they were fully prepared for all risks, some thought they were better than others and some recognised there was no contingency for things like Internet failure. As the industry continues to develop and to develop new products and services it will need to assess and contain the new risks it exposes. The following are some responses:

“We are reasonably well prepared. As a law firm, we do not face many of the risks faced by ICT companies. Our own security procedures are fairly good, but not excellent. The ICT industry as a whole is only moderately prepared to deal with the broad array of risks it faces. Commercial incentives to roll out new products continue to trump security concerns, although this situation appears to be improving somewhat. There is no easy solution to the commercial risks and competition facing the industry.” Maury Shenk, an observer

“Some risks we have no contingency for (eg internet failure). On security issues we believe we are on top of these.” A supplier

“I am confident that technology will win, though we need better than some major players are prepared to sell us.” A customer

“I think most organisations including my own are poorly prepared. There were some risks we hadn’t even considered and new ones are arriving all the time as well as ‘sea-changes’ occurring in the existing risks” Denis Saunders, a supplier

“These risks (and growing awareness of them) will power the next round of recruitment to both PITCOM and EURIM. Over the past year I have seen both my ISPs off-air for 8 hours or more (albeit not at the same time) and suffered a 16hour power cut. I now plan on the basis that my main system could be put out of action in such a way that I would have to rebuild on new equipment from back-ups at 24 hours notice. In this context I would also like an easy to use and reliable, off-the-shelf Linux system (whether for regular use or as a standby) which will handle my Word and Excel files and e-mails so that I can diversify my technology risks.” Philip Virgo, an observer

THE BANANA SKINS

The banana skins are listed highest risks first with some discussion, followed by any relevant quotes from the respondents and then the definition of the risk taken from the questionnaire.

1. Concealment of attacks (rising)

The refusal of organisations to admit they have been successfully attacked is seen as the highest risk and is one of the fastest risers. Concealment means the criminals are probably not pursued and may be encouraged to repeat their attack on other systems. Other organisations trying to protect their systems are less likely to be aware of the type of attacks from which they are potentially vulnerable and to be able to take pre-emptive action. Under the current legal regime it is difficult to bring attackers to book and, if they are outside the UK, it may be impossible so there is little incentive to report when all it will do is damage reputation.

“There is a widespread feeling among my City contacts and others that there is a high or even a very high level of concealment and cover up by financial institutions and others particularly of successful attacks and frauds. By its very nature, this is unproven but nevertheless is felt to be highly prevalent. Brand and career protection are frequent motivations. What is needed is the creation of the type of ‘No Blame’ open reporting regime, which the airline industry introduced with great success to determine and resolve causes of air incidents.

Regarding attacks, we should expect them as part of the natural model, which looks increasingly like a competitive biological evolutionary model exploring underlying inherencies. The natural competitive biological model has been filled with viruses from the start – in fact they are among the engines of evolution. We need to begin to understand the nature of the ‘Information Organism’ and the process of building an immune system. This can only really be done in a fully transparent environment such as is provided by the open communitarian approach of Open Source.” Basil Cousins, an observer

“Only new legislation allowing companies to prosecute attacks will ensure that concealment doesn’t rise. The stigma of such an attack has to be addressed also”. Anthony Parker, a supplier

"It is not that most users actively conceal attacks. It is that they do not know who to report them to. If they did, they would not get through most of the time and would not get a sensible response most of the time that they did raise a human being, as opposed to an answer phone e-mail or website black hole. They have therefore do not bother. Meanwhile those who publicise telephone lines or e-mail addresses for reporting quickly get swamped - including by spammers and/or those responding to phishing attacks." Philip Virgo, an observer

Definition used in the questionnaire.

To avoid damage to their reputations companies, particularly in financial services and retail, prefer to conceal cyber crime incidents and not to pursue the criminals in the courts. Meanwhile the cost of these attacks continues to escalate. The first person in the UK has been sent to prison for an internet attack but usually it is difficult and expensive to track down the culprits as attacks can be made from anywhere in the world.

2. Phishing undermines Internet banking (rising)

Phishing is seen as having a very high risk of undermining Internet banking and e-payments and it is seen as increasing. Globally it has reached more than one incident a day see <http://www.antiphishing.org> affecting banks, credit card companies and retailers.

“ The success of Phishing (to bypass most of the current technology-based security models for browser-based e-transactions) could collapse e-commerce later this year, unless organised crime is content to limit its take so as to milk the vulnerabilities and not kill the scared cow.” Philip Virgo, an observer

Definition used in the questionnaire.

Users lose confidence in Internet Banking as Phishing becomes endemic, leading to collapse of e-commerce. Phishing is fraudsters sending fake emails to trick customers into revealing account names and passwords that

they use to transfer money or make payments. These emails look like the real company sent them, and include their web graphics, logos, etc.

3. Unexpected attacks (rising)

The unexpected attack is by definition hard to prepare for so it is seen as very high risk although steady.

“Fear of the Internet killer attack -- There may be a new type of attack on the Internet that actually disables it. This could (in worst case) bring down the global economy.” A supplier

Definition used in the questionnaire.

Protesters from minority anti-establishment groups attack the IT operations of their unsuspecting target organisations damaging business. The LIFFE building was invaded by Swampys intent on bringing trading to a halt.

4. Cyber Terrorism (rising)

Although there are no reported successful cyber terrorist attacks, there are a great number of international and domestic cyber terrorists that are capable of seriously damaging the communications and information systems of government, financial and industrial. This would then affect the systems they control - defence, water, food, pharmaceuticals, transport, energy, health care, emergency services, stock markets and the economy. These terrorist groups may increasingly rely on cyber terrorism to accomplish their social and political goals because of the numerous advantages of cyber terrorism – low cost, relative anonymity, remote, large number of targets, large impact. . Although these cyber terrorists may attack, there are agencies on an international, national, and local level, led by the USA, which are developing counter cyber terrorism abilities. Furthermore, although expensive and difficult to implement, there are protective measures that private corporations can implement in order to protect themselves. However, to quote

“Operating systems are protected by ad-hoc'ery from the outside rather than by design from the inside. And this means that, sooner or later, a virus, or some other attack, will spread quickly enough and widely enough to cause major economic disruption and, possibly, physical damage to life and other structures. (I am talking about disruption an order of magnitude larger than that that has already been experienced). This is one weapon of mass disruption against which little concerted action is being taken.” A customer

Definition

Technical terrorists attack computers controlling energy and water supply systems in the developed world bringing chaos in Europe and USA. More likely, and more devastating, would be co-ordinated terrorist attacks on the handful of communication centres (six for the UK, 14 for the US) through almost the whole of the communications of most western nations now flow.

5. National Grid fails (rising)

Failure of the grid and its consequential impact is seen as very severe risk but is only just rising as the big public failures have caused investment in standby generators and more resilient power systems.

“As experience teaches from the power failure in Italy and London, the whole industry relies on the integrity of power. Without power, as I witnessed in Charleston when Hurricane Hugo struck, the whole system collapses.” Peter Millard, an observer

Definition used in the questionnaire.

A software failure disrupts the UK national Grid and cascades throughout Europe, which was expected to provide us with backup power. Most IT systems are shut down. This may happen anyway with out a software failure, as the energy generators are not capable of responding to peaking and increasing demand.

6. Data protection too onerous (rising)

This was seen as a high risk and rising as the new legislation gives more protection to the individual, giving them the right to "opt in" before receiving e-marketing. It also restricts the use of Cookies and other invisible tracking devices that collect user information on Internet. These may only be used if the web site user is given clear information about the purpose of any such invisible activity and is offered the right to refuse the cookie.

This will allow the web site user to decide when access to their computer is acceptable and when it is not. The use of Location Data generated by mobile phones can only be further used or passed on by network operators with the explicit consent of the user. Then there is the other aspect of confusion in the existing application of the law.

“Civil liberties - Recording and keeping unproven criminal allegations vs Freedom of information – how do we keep important data without impairing innocent people? Denis Saunders, a supplier

Definition used in the questionnaire.

It becomes impossible to conduct IT backed marketing and customer relations management and support because of the Data Protection act and its interpretation. Being open with customers will no longer work – customers must positively opt in and there will be a new regime for cookies.

7. Offshore outsourcing hits UK employment (rising)

Offshore Outsourcing, seen as a high risk and the fastest riser and generated a lot of comment, particularly from suppliers, who think more should be done to point out the risks.

“The Internet has now truly created a global IT market with the emergence of India and China as vast powerhouses of IT resources.” A supplier

and

“The biggest threats to the ICT industry appear to me to be the commercial threats from slower increases in demand and foreign competition.” Maury Shenk, an observer

Who should take the lead to defend us?

“My main concerns for the ICT industry in the UK centre round the competitive threat from India and the Far East. This issue is self-explanatory but I do feel that UK representative bodies such as Intellect and the BCS should take a lead in pointing out the pitfalls in outsourcing work to locations 6,000 or 9,000 miles away, such as cost of project management and cost of “Chinese whispers”! Outside London and the South-east UK firms can actually be competitive on price with these companies.” Denis Saunders, a supplier

and from a supplier, who is affected by this and other factors

“As a small consultancy I have 3 competitive concerns: Competition from cheap labour offshore; Foreign workers being granted work permits for working in IT; British legislation like IR35. Competitive tendering -- up until 2 years ago the big names wouldn't bid for contracts less than £1million. Now they do, and we have to compete with them.” A supplier

and from a supplier giving a customer perspective

“There is an ever growing choice of products and services now able to be supplied from all corners of the Globe, how do you find the right product at the right price and carry out effective due diligence to ensure your company's cost base, brand and assets are protected.” A supplier

Definition used in the questionnaire.

Offshore outsourcing of IT systems development and maintenance and call centres to lower cost economies becomes a serious problem causing significant unemployment in the UK.

8. Users vs IT professionals (rising)

Seen as a high risk, and just rising – it has always been a problem and one aspect of it, users doing their own thing, may be getting worse because of free software like Instant Messaging. In many cases, employees have downloaded from the Web and are IM-ing clients, competitors, and colleagues without management's knowledge, without written rules and policies to guide usage, and without IT-approved technology to help prevent security breaches and control overall risk. If it's not approved it affects another risk area – IT Governance.

It continues to happen with falling hardware prices.

“Employees can buy the cheap colour screen mobiles, LCD screen, theatre quality sound, the digital camera and the photo quality printer that can turn every PC into a high quality multimedia workstation. Or it might leave your company having to catch up with the competition with a very expensive desktop/laptop/palm/personal digital assistant/phone refresh program.
This could also lead to a return to the early PC days when companies IT departments could not keep up with IT developments and business units went off and bought their own IT equipment because it was cheap and helped them do their job” A supplier

And it is worse in the UK/EU.

“The major UK/EU suppliers appear to have become increasingly out of touch with user priorities and consequently unable to handle the changes now inevitable as Asia/Pacific changes cost structures, business models and expectations of ease of use and reliability - let alone the technology platforms (e.g. data mobile and inter-active digital TV merging to provide seamless video-telephony in place of PC and browser).” Philip Virgo, an observer

And some users feel misled

“My main concern is that the rising cost of annual upgrades will begin to bring the industry into disrepute. Furthermore the tactics used to market broadband will be seen by many users as being economical with the truth for the basic user does not realise the need for greater protection as their computer is on open access to the web.” Peter Millard, an observer

Definition used in the questionnaire.

IT professionals continue to use a different language, fail to understand the users and to get users to understand them. At the same time people sponsoring projects need to understand the project and not just be managing the process. Local computer systems developed independently by end users need to be banned to avoid exposures but this stifles innovation and may have a direct negative impact on the business. There needs to be a process for identifying and evaluating them and legitimising them if valid and supportable.

9. Personal ID card fails (rising)

Failure of the ID card project is seen as high risk and rising fast. It is clear that the Government needs to adopt more secure technologies for the card but they will still need constant upgrading.

“There are now over twenty ID cards and all the biometrics have now been successfully spoofed. It will be like Swipe Cards - a slow path to convergence and then a never-ending evolution cum arms race between criminals and banks - with the rest following on their coat-tails.” Philip Virgo, an observer

“Pet hate. Very likely to fail & set back e-government a decade.” An observer

Definition used in the questionnaire.

Fingerprint and Iris codes systems fail to be secure as criminals replicate and personal identification and information is stolen more easily. NB low-tech methods for spoofing them have already been demonstrated.

10. SPAM halts the Internet (rising)

The risk of SPAM halting the Internet is seen as high risk and rising even with the impact of new data protection laws – will they be ignored without global controls.

“Until we have truly global legislation or police force, SPAM will continue to invade our email systems until they become unusable.” Anthony Parker, a supplier

A new danger is emerging as virus writers have started to use spamming techniques. A recent virus, SoBig, infected hundreds of thousands of computers worldwide, but the initial virus also installed open proxies on compromised machines, which were then used to send spam.

In the USA the CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act), without banning unsolicited email, enables Internet users to have their email addresses removed from mailing lists and also calls for heavy fines and prison terms for those sending messages of a fraudulent or pornographic nature without warning recipients.

Definition used in the questionnaire.

SPAM is already threatening to halt ISPs and new legislation by country may not work, as it has to be controlled globally. Firewalls, which can be used to control SPAM, get fooled by new Spamming techniques.

11. Hackers unite (rising)

This is assessed as a high risk and rising and it is now real. There is a hackers' peer to peer network, Sinit, where there is no central server that can be shut down. It uses encryption technology to prevent antivirus companies from tracking development activity or modifying the virus codes. It seems likely that the primary motive of the virus writers is changing from intellectual challenge or simple-minded cyber-vandalism to financial gain. This is partly reflected in our respondents' views.

“Also, I was surprised that the list did not identify the individual virus/worm attacks and security breaches that are already a major problem for the industry”. Maury Shenk, an observer

“Hackers are not the main threat: criminals are”. Maarten Botterman, a customer

“Given the nature of the (hacker) community this is more likely to happen by accident than by design. Organised crime is more concerned to milk the system than kill it”. Philip Virgo, an observer

Definition used in the questionnaire.

A group of hackers link to make simultaneous attacks on the Microsoft Operating System and UNIX bringing world trade to a standstill. The MS OS is now being patched monthly via the Internet and someone may have embedded a Trojan horse into the UNIX compiler, which activates - it could happen to the SCO kernel.

12. Extra-territorialism escalates (rising)

This is assessed as a medium risk but a high riser probably because the US economy has been worsening and they seem most likely nation to take action.

Definition used in the questionnaire.

USA controls the world's software, controlling the distribution of patches and upgrades –this could be used as an economic weapon against individual countries. Alternatively the USA makes overseas outsourcing of IT and call centre jobs less attractive by applying punitive taxes at the point of transaction – deemed to be in USA. This has a serious impact on some US vendors who are unable to honour their support contracts. US and then EC places taxes on SW and HW imports. Islam moves to attempt to place controls on the use of images worldwide.

13. Disaster recovery found wanting (steady)

A medium risk not expected to change – are we being complacent or have we done relevant and comprehensive tests. Two views:

“Unfortunately just good enough seems to have got most organisation through in the past”. A supplier

“Risk falling as firms (large and small) reduce critical dependence on UK city centre sites - either decentralising or off-shoring with 24 by 7 mirrored sites”. Philip Virgo, an observer

Definition used in the questionnaire:

Most Disaster Recovery sites are untested and in unsuitable places. Rarely has anyone tested it with real end users at the site. Back-up systems must have read and write access to all data, including confidential and secret data. These systems are normally controlled by a person and not by a process so are an open door for attackers from both inside and outside the organisation. At same time all organisations face an increasing risk of terrorist attack.

14. Disgruntled IT employee (steady)

This was assessed as a medium risk and holding steady although a recent survey of all types of employees by HR consultancy Watson Wyatt found that the number of people that say they are happy at work has fallen from 25% to 7% over recent years. One would expect the level of satisfaction to be lower in ICT related activities.

Definition used in the questionnaire

IT staff are becoming disgruntled and sometimes less competent. Salaries have stagnated, employment opportunities are still in decline in the industry and a lack of training has reduced competence. There is a lack of loyalty following poor treatment of employees during transitions to outsourcing. Consequently there is a rash of damage to corporate systems, some malicious, some incompetence.

15. Non-resilient systems - insufficient redundancy in systems (falling)

Seen as a lowish risk and just falling – has everyone installed resilient systems where they are needed?

Definition used in the questionnaire

Disasters occur when several things go wrong simultaneously. If systems have built in redundancy they can go on working if there are several failures – if not they stop.

16. IT Governance (steady)

IT Governance was seen as a medium risk and steady despite the increasing emphasis on Corporate Governance which is meant to enable active participation by shareholders in organisations. This cannot happen without effective IT Governance.

Definition used in the questionnaire.

Since we spent a lot of time and money auditing our systems for Y2K we have been complacent. We have downsized IT departments and are now at risk if staff leave or we have outsourced to vendors who have also downsized and don't now have the skills to support the systems. There needs to be the right governance in place to avoid things going wrong. CEOs have a responsibility to ensure that IT goals align with those of the business, it delivers value, its performance is measured, its resources properly allocated and its risks mitigated. Specifically, global organizations, or non-US-based companies that are required to comply with Sarbanes-Oxley, need to examine their IT operations and determine if they are significant to the organization as a whole. The assessment of whether an IT business unit is significant can be impacted by the materiality of transactions processed by the IT business unit, the potential impact on financial reporting if an IT business unit fails and other qualitative risk factors.

17. Copyright law litigation hits UK corporates (rising)

This new law designed to protect the UK media industry operating in a global marketplace is seen to create significant new litigation risks for other UK organisations as they unwittingly infringe copyright - but by others is seen as much needed. It aims to take account of new technological developments but it fails to tackle the growing practice of P2P file sharing and downloading. At the same time it makes it more difficult for organisations, like educational establishments, to make sensible and limited use of copyright materials.

“The problems of piracy today and loopholes in copyright and international law serve only the ISP and hardware manufactures who have no obligations to prevent copying. Today's file sharing programs are so advanced that they have used the Internet to form vast networks of file sharing users. One of the most popular programs is so exceptional in its ability to distribute files that users are encouraged to share; the more they share the more credit they acquire and with it the right to carry on downloading. The client/server relationship is so smart that it even tracks the ability to give the user better download rates depending on their credit and what their upload speed is set too. Currently there is no means of controlling these communities. The radical reform that I suggest would point towards a counter attack to stop this plague in its download. Copyright law is in dire need of radical reform to protect a vulnerable industry. The effect of a failure to act will mean serious problems for the long-term evolution of IT.” A customer

Definition.

The Copyright and Related Rights Regulations 2003, drafted by the UK's Patent Office, came into force at the end of October 2003. It is the UK's implementation of the European Union Copyright Directive (EUCD), which strengthens copyright protections. The UK adopted what many consider to be Europe's toughest digital copyright law, with the stated aim of protecting a media industry that exports many of its works to overseas audiences.

Most companies believe their internal copyright guidelines will protect them from unwittingly engaging in copyright infringement. In fact, the regulations place new limits on privileges, which previously allowed individuals and organisations to use copyrighted materials without obtaining a licence or paying a fee. In most cases, using any copyrighted work will now require a licence.

18. System suppliers in court (rising)

This is viewed as a medium but rising risk. IT suppliers and users need to move away from a confrontational approach to negotiating and implementing IT systems. Both suppliers and users need to be more open with their requirements and lawyers need to be seen to facilitate the process rather than to put up barriers.

It would be nice to see an evolution towards paying a realistic price for products that are fit for purpose - but that also means defining the purpose, which will always be difficult as it needs detailed and accurate specifications under well managed change control.

Definition used in the questionnaire

Systems suppliers find themselves in court defending alleged under delivery. In a world of increased litigation and blame allocation, often coupled with reduced IT staff numbers in large corporations, how do system suppliers protect themselves against alleged under delivery? Tight specifications only go so far, are expensive to produce, and are still open to interpretation when things go wrong. In this customer centric world, clients have rights and suppliers have responsibilities, but clients need to contribute to the success of a project, too. Project management within the IT world is almost a dead art. How do we best draw the line between what it is reasonable for a bespoke system supplier to provide, and what a customer can reasonably expect to receive? And what is the customer's responsibility in making the project work?

19. Intellectual Property Rights Enforcement Directive (rising)

This was seen as a medium risk, rising and less of a risk than Copyright law litigation. As you will see from the definition below the risk was about the possible collapse of support for current western copyright and patent regimes. The view is the legislation is more likely to increase litigation than collapse.

The EU's draft Directive on the enforcement of intellectual property rights sets out to make it dramatically easier to enforce copyrights, patents, and trademarks in Europe, and to punish people who tamper with technical mechanisms designed to prevent copying or counterfeiting. The directive has been welcomed by the music and film industries but not by the communications industry, universities and libraries. Larger software firms may now be in a better position to collect royalties from the smaller firms who want to make their products compatible. Designers and manufacturers of branded products will now be in a stronger position as they can use RFIDs (embedded radio chips) to identify their products to consumers and it will be much harder to sell fake or imitation products.

Definition used in the questionnaire.

A lose - lose confrontation for the proposers which will lead / help trigger the collapse of support for current western copyright and patent regimes.

20. Systems demographics disasters (steady)

This is seen as a low, steady risk that we seem to be managing.

Definition used in the questionnaire

For convenience of installation, training and routine maintenance companies have purchased large numbers of identical hardware items from the same manufacturing batch and loaded up identical software and patches. If a hardware or software component is intrinsically faulty all the items may fail simultaneously – a simultaneous death of the population of components including back-up systems.

21. Wireless systems setback (rising)

Not seen as a serious risk but just rising as wireless systems proliferate. About 25% of businesses have installed wireless networks and maybe 10 – 15% are doing mission critical work in USA. The initial security standard, WEP, uses a static encryption key. A better standard is emerging called WPA, WiFi Protected Access, which fixes the encryption problems of WEP but is not as secure as other current systems such as SSL used to encrypt secure Web transactions. The next stage is the official IEEE 802.1X, which is expected to be finalised in Spring 2004.

“So what’s new in a hundred years of wireless, this is the one area where encryption is of unequivocal value”. Philip Virgo, an observer

Definition used in the questionnaire.

The limit of wireless channels means they are open to interference, snooping and hacking and these risks, once experienced, outweigh their convenience, so causing a halt in wireless systems implementation. Systems have been penetrated using a Pringles packet and a coat hanger and buildings have been marked by hackers to show best locations to access systems. Hackers can flood a wireless system from outside the building so bringing an IT enabled business operation to a standstill. End users are now being issued with WiFi enabled laptops and can send files and macro based systems to each other without the knowledge of the IT department.

22. Websites damage global brands (steady)

This is a medium to low risk, holding steady, but still a risk for those underestimating the importance of brand.

“Websites of major brands will become front line. Only companies taking a serious look at security will save face. Many will believe that brand doesn’t mean anything and will be open to attack.” Anthony Parker, a supplier

Definition used in the questionnaire.

Malfunctioning and insecure websites and back-office systems damage the brands of major retailers. IT and service suppliers face massive consequential damage claims and the demand for new systems falls dramatically.

23. SCO suit succeeds (steady)

This is seen as a medium risk and steady, almost falling. Initially it is causing doubt in the Open Source world but SCO will find it hard to win the case.

“Litigation is rarely in the users interest. For example the SCO v Linux litigation has caused Fear Uncertainty and Doubt in the corporate Linux world. The Microsoft Explorer Litigation nearly meant that users would have to purchase this free software. A supplier

The risk is being reduced by Novell’s move to offer its SuSE customers a Linux Indemnification Programme which will protect them against copyright infringement claims made by third parties and Open Source Development Labs launch of a legal defence fund to meet costs of end users threatened by The SCO Group

Definition used in the questionnaire:

The suit by SCO over Unix code in LINUX is successful and invalidates the business case for LINUX and affects confidence in Open Source. This causes changes in IT strategy for many organisations with consequential delays in systems delivery and increased costs for customers.

24. The Disappearing IT Director (steady)

This is a low risk and steady on trend. Probably not perceived as happening. But is the IT Director getting more risk averse?

“Regulation appears to be forcing IT Directors to be more conservative, they must be able to demonstrate they are actively managing the IT risks and protecting the company’s digital assets, not a bad thing in itself. But is this creating a breed of risk adverse IT Directors supporting a return to the period when you never got sacked for buying IBM (for IBM read Microsoft today). But by relying on the traditional suppliers they may be not carrying out proper risk assessments”. A supplier

Definition used in the questionnaire.

Companies are removing the post of IT Director. Many IT directors are not properly qualified, vendors have downsized and companies have outsourced, but complexity is increasing. Who will they blame when it goes wrong?

25. Knowledge economy fails (steady)

Clearly respondents do not expect the knowledge economy to fail in the UK and it is not seen as an increasing risk. However there was some comment on risks and issues connected with the knowledge economy such as the avoidance of complexity,

“Unnecessary Complexity is the breeding ground for error, and for ‘killer’ faults. So far as we understand, the natural biological model is constructed on very simple units, which combine together in huge diversity. Systems designers and programmers should strive to follow this model to avoid major disasters”. Basil Cousins, an observer

the use of inappropriate measures to drive the knowledge economy

“My secondary concern relates to the increasing use by government of computer generated performance measures, especially in health care and in education, for political purposes. In health care underlying mistakes were made early on such as calculating bed occupancy in hospitals at midnight, yet counting it as days. There is now a gradual recognition by professionals that many of the calculations used are numerically correct, but are practically flawed. Peter Millard, an observer

and the politicisation of education

“Education – This country needs to buck up its ideas on school education and focus on what industry requires rather than on what politicians deem suitable. The politicisation of education is a wicked practice that has been in force for decades in this country.” A supplier

Definition used in the questionnaire.

Companies in an effort to protect their intellectual property and aided by lawyers increase the complexity of their procedures so that no one in the business has relevant experience and no one knows what they are allowed to do. They forget that 90% of corporate knowledge is in unstructured emails, which no one is managing. It has always been difficult to specify a human task in computer terms. Interviewing managers who only intervene to manage the exceptions, gives the wrong specification. Computer systems to support the processes can no longer be analysed, designed and successfully implemented because of the complexity and constant change. End users used to understand the business and could work round poorly specified IT systems, but now they can't because they don't know how it is supposed to work. Similarly Government continue to implement new legislation overlaying old legislation without fully analysing and knowing the implications. In their efforts to create a sustainable inclusive society they create an unsustainable economy with new inequalities where expert benefits claimants have a better lifestyle than many of those working.

The World Economic Forum (WEF) report, which looks at how much world economies are facilitating and reaping the rewards of ICT access. The UK is rated 15th out of the 102 economies studied -- a large drop from seventh position last year.

26. Legacy systems halt (falling)

This is seen as a low risk and falling. What was a problem with old mainframe systems is less of a problem with networked systems and there are still people around with the skills to do the work – living longer, retiring later?

Definition used in the questionnaire.

A lot of legacy systems are based on OS/2 and older systems with non-GUI interface. Soon there will be no one around who knows how to use them, no one able to maintain them and no one who wants to learn.

27. Outsourcing put on hold (steady)

Putting outsourcing on hold is not seen as a serious risk and is steady, almost falling. However there is concern about the oligarchy of major outsource vendors which is reducing competition, sometimes providing poor service to trapped customers, and moving vendors one more step away from the real business customers.

Definition used in the questionnaire

Organisations have not automated and documented the business process Definition used in the questionnaire used in the questionnaire prior to outsourcing and now find they didn't specify properly what they wanted when things go wrong. Meanwhile vendors of outsourcing, having bid low to win business, will now want to make money from add-on projects to recover their profitability. However customers do not want to spend more and put outsourcing and in some cases all IT spend on hold.

Following the massive overspend on the Libra Magistrates system and an anticipated failure to outsource the NHS contract the Government puts further outsourcing on hold. The government has already scrapped PFI for IT projects as their changing requirements prevent any risk being transferred to the supplier.

28. European Software Licensing (rising)

This is seen as a low risk but rising - and by some as irrelevant.

“The EU software industry is dying and Asia is beginning to overhaul the US so this will soon cease to be relevant.” Philip Virgo, an observer

It is a fallacy to think that there is an "EU Law" - even where the EU implements EU-wide Directives there will always be country to country differences. What is core to licensing and other contractual arrangements are the commercial elements that underpin those arrangements, such as delivering the user what it wants, pricing and so forth. What is needed is a good lawyer who understands that these commercial issues will be common throughout the EU and who can incorporate those key elements in commercial contracts clearly and concisely. The technical legal differences in terms of copyright etc will have less relevance than the core commercial terms.

Definition used in the questionnaire.

Ignorance of European Software Licensing slows exports to Europe. For UK software authors selling their products in Europe, to what extent do they need to invest in specialist EU legal advice, particularly in support of their European resellers? Most UK trained lawyers are specialists in UK, rather than EU law, and EU specialists are expensive. With the exception of such obvious differences as the position on reverse engineering, are there significant variations in contract formation, IPR, copyright protection, etc. And have the differences in law been tested? If software were sold as a product and not a service it must be fit for purpose – the industry would collapse.

29. Drive by wire (or wireless) accidents (steady)

This was assessed as a low risk and holding steady. Although computers are now incorporated in most control systems the technology is well known and tested.

“Until the industry agrees a way forward and gets the current Health and Safety Executive plans, still in their drawer because not replaced, merely batted back, there is a real risk”. Philip Virgo, an observer

Definition used in the questionnaire.

A spate of road accidents and a major shipping accident is caused by coding errors / systems conflicts / interference in the many computers that now control the engine and drive systems of expensive executive cars and modern ships like the Queen Mary. For example the Thai Prime Minister would have been suffocated when the computer of his BMW failed and they were trapped inside - his chauffeur had to smash a window so they could breath while waiting to be rescued!

Appendix: Survey Questionnaire

ICT Banana Skins 2004

An RTC survey of the risks facing the ICT industry

“Banana Skins - unexpected things we must avoid in next few years, but if we don't we will probably get the blame and pay the costs”

Dear Members of RTC

For the first time we are asking you to describe your main worries about the ICT industry as you look ahead. We would be very grateful if you would take a few minutes to fill out this form and email it to Stephen.aitken@theStrateg-e.com, Secretary of the RTC. If successful we will make this an annual survey. We would like to thank the CSFI for their advice and their permission to copy closely their Banking Banana Skins Survey which has now be running successfully for eight years.

Question 1. Please describe your main concerns about the future of the ICT industry for both suppliers and customers as you look ahead over the next two to three years

Question 2 Below are some of the areas of risk for the ICT industry suggested by RTC club members at meetings leading up to and including the Banana Skins debate on 25th November 2003. The risks are explained in the subsequent pages. Please rate their severity on a scale of 1-5 (5 high) and whether you believe they are Rising, Falling or Steady (indicate R, S, F) and add any comments in the right column. You may add more risks at the bottom – if you do please explain them on the previous page.

No	Banana Skin	Severity 1 = low 5 = high	Trend <u>R</u> ising, <u>S</u> teady, <u>F</u> alling	Comments about severity. Severity is measured as the likelihood of it happening times the cost if it does. Please add further comments in answering question 1
1	Concealment of attacks			
2	Copyright law litigation			
3	Cyber Terrorism			
4	Data protection too onerous			
5	Disaster recovery found wanting			
6	Disgruntled IT employee			
7	Drive by wire accidents			
8	European Software Licensing			
9	Extra-territorialism			
10	Hackers unite			
11	IPR Enforcement Directive			
12	IT Governance			
13	Knowledge economy fails			
14	Legacy systems halt			
15	National Grid fails			
16	Non- resilient systems			
17	Offshore outsourcing hits UK			
18	Outsourcing put on hold			
19	Personal ID card fails			
20	Phishing			
21	SCO suit succeeds			
22	SPAM halts the Internet			
23	System suppliers in court			
24	Systems demographics disasters			
25	The Disappearing IT Director			
26	Unexpected attacks			
27	Users vs IT professionals			
28	Websites damage brands			
29	Wireless systems setback			

Question 3. How well prepared do you think your own and other organisations are to handle the main risks you have identified

--

Question 4.

Your Name:			
Organisation:			
Are you mainly a supplier	customer	Or observer	Of the ICT industry
Replies are in confidence but if you are willing to be quoted in our report, please tick here			