時尚英语趣文

# Going Online on the Road

## 边旅行 边上网

网络时代

丛书主编：陈振东
本册主编：黄 樱

湖北辞书出版社

# Going Online on the Road

# 边旅行 边上网

## 网络时代

丛书主编：陈振东
本书主编：黄　樱
编　　译：奚菁颖
邹丽芳
万敏敏
王延水

湖北辞书出版社

(鄂)新登字 07 号

**图书在版编目(CIP)数据**

边旅行边上网:网络时代 / 黄樱编译. —武汉:湖北辞书出版社,2005.2

ISBN 7-5403-0863-X

Ⅰ.边… Ⅱ.黄… Ⅲ.英语—对照读物—英、汉 Ⅳ.H319.4

中国版本图书馆 CIP 数据核字(2005)第 005406 号

责任编辑:刘 丹
出版发行:湖北辞书出版社
(武汉市雄楚大街 268 号 B 座 430070)
印 刷:武汉市新华印刷有限责任公司
(武汉市江夏区纸坊古驿道 430200)
开 本:890×1240 1/32
印 张:5
版 次:2005 年 3 月第 1 版
印 次:2005 年 3 月第 1 次印刷
字 数:140 千字
印 数:0001—3000 册
定 价:14.00 元

# 前言

互联网的出现尽管只有短短二三十年的时间，其普及和发展的速度却是前所未有的。今天，互联网在我们生活中扮演着日益重要的角色，不仅是新新人类沉迷于网络世界中，我们大多数人在工作、生活中都享受着互联网带来的便利。可以说互联网使我们的生活产生了一场新的革命。

互联网在给我们带来通讯、交流的便利的同时，也对我们的生活产生了诸多影响。伴随着互联网的发展，出现了许多新的词汇，如“网恋”、“黑客”、“垃圾邮件”等等；也出现了诸多的新生事物及问题，如电子商务、电子图书馆、网络安全问题、网站管理问题等等。可以说，互联网本身就像一个小社会，和我们的大千世界一样有着种种轶事。本书选取了二十多篇近期外刊、外报上有关互联网的发展、现状及对我们生活的影响的文章，内容较为新颖有趣，兼具知识性和趣味性。读这些文章，就像是打开了互联网世界的窗口，对这一丰富多彩的世界得窥一斑。

我们在翻译的过程中尽可能做到既保持语言的准确流畅，又保留其原汁原味。通过全书，读者既能提高英语的阅读能力，又能掌握一些较新的互联网方面的词汇，同时还能了解一些有趣、有用的信息。

黄樱

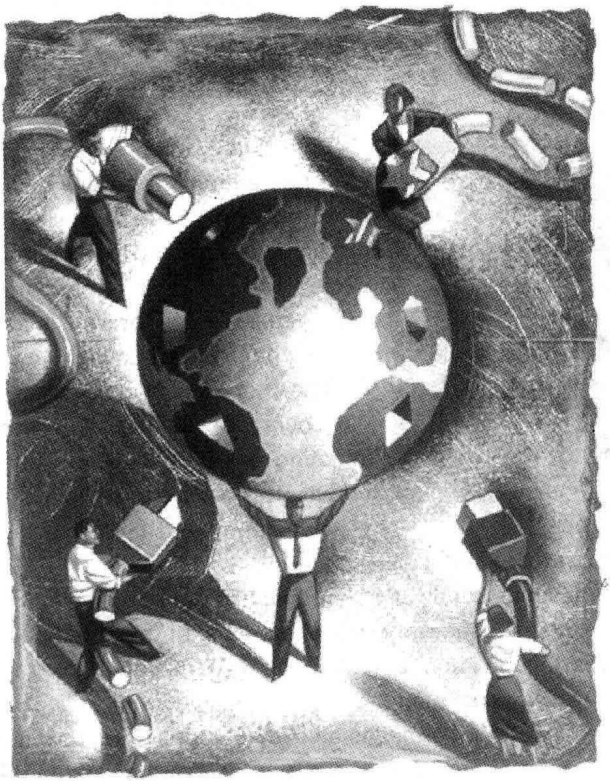
2004年11月

# CONTENTS 目录

# CONTENTS 目录



## After Thought 所思所想



# Banning E-mail —A Feasible Option?

# 禁止使用电子邮件——一个切实可行的选择吗?

John Caudwell, president of Phones 4U says he banned inter-office e-mail from his company and reaped an immediate productivity increase of three hours per day per employee. If we accept this claim at face value, we're forced to ask whether every organization should follow his lead.

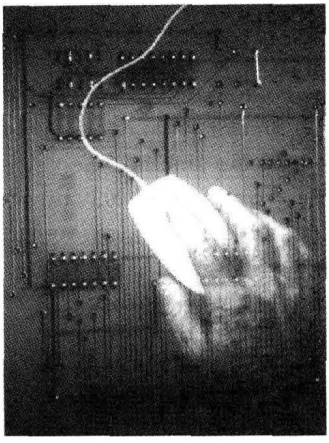
The short, and short-sighted, answer is, "Of course we should." The problem with initiating an automatic ban based on his results is that Caudwell's company isn't your company and therefore his solutions are not necessarily your solutions.

We should assume Caudwell did not impose the ban on a whim. He likely examined employees' usage of e-mail and decided they could better spend their time answering the phones. Without meaning to sound trite, e-mail didn't kill productivity–his people did.

The banning of internal e-mail is a valid solution if, and only if, the use of e-mail is causing a problem. The dozen queries I've received in the past few weeks asking. "Should we ban e-mail?" ignore this unsubtle point.

The timing of this e-mail banning discussion is perfect. Many organizations are currently sniffing around Instant Messaging (IM). What better time to ask "Why should we?"

IM is a growing hot topic. In the UK, Small Message Services (SMS) recently generated more than 30 million messages nationwide in a single day. Whether we like it or not, IM will undergo the same growth pattern, especially if the telecoms convince us that IM is the next silver bullet for productivity problems. The telecom strategy is to suggest that IM increases productivity



4U电话公司的总裁约翰·考得威尔说，他禁止在公司内部发送电子邮件，结果是每个员工每天的生产力立即增加了3个小时。如果我们按照表象接受这种做法，我们不得不问一下是否每个机构都应该学他这样做。

简短且目光短浅的回答是："我们当然应该这样做。"但问题是，考得威尔公司不是你的公司，因此他的解决办法不一定是适于你的办法。

我们应该能推断考得威尔实行禁令并不是一时的兴致。他可能检查了员工电子邮件的使用情况，确定他们花时间接电话可能更好一些。我并不想说老生常谈的话，但我想说电子邮件并没有扼杀生产力——扼杀生产力的是他公司的员工本身。

如果仅仅是由于使用电子邮件引起的问题，禁止内部电子邮件的使用当然是有效的解决办法。在过去的几个星期，我收到许多的询问，如"我们是否应该禁止使用电子邮件？"——这些询问都忽视了这个并不微妙的问题。

讨论电子邮件禁令的时机是很恰当的。许多机构对目前的即时信息嗤之以鼻，还有什么更好的时机来质问"为什么我们要这样做？"

即时信息是一个发展中的热门话题。目前在英国，通过短信服务商（SMS），全国每天会发出3000万条短消息。不管我们是否喜欢，即时信息都会经历相同的发展方式，特别是如果电信服务商让我们相信即时信息是解决生产力问题的又一剂灵丹妙药。电信服务商们试图暗示我们：即时信息能让我们随时随地联络到任何人，即时信息确实提高了生产力。

多么精彩又合人心意的事！从此以后繁忙的大人物们只要召唤一下最近的助手，马上就能得到需要的信息。毫无争议，如果我们能缩短需要信息和得到信息之间的时间，那么我们的工作就能变得更高效多产。

我对即时信息有不同的看法。中途打断会很大程度上降低我们的效率和生产力水平，可能更严重的是降低我们的工作质量。如果我们是理性的、合乎逻辑的人类，我们必须断定这结论对每个人而言都是正确的。

还有一个针对信息质量的问题。我们每天收到多少与我们工作无关的电子邮件？有多少封电子邮件的内容就像孩童时期消遣时光而传递的小纸条一样无关紧要？有什么东西能表明我们的即时信息有所不同？电子邮件会不会堕落到用于交流体育比赛的得分、谁被投票出局和传播笑话？

by allowing us to contact anyone, anywhere, anytime.

What a wonderful and desirable thing! Busy, and hence very important people need information now. Just call out to the nearest assistant and get our informational needs filled immediately. There is no argument. If we can reduce the time between informational need and gratification, then we have become more efficient and productive.

I have a very different perspective on IM. Interruptions significantly reduce our effectiveness, productivity levels and, perhaps most importantly, the quality of our work. If we are rational, logical human beings, we must assume this is true for everyone else.

There is also a question about the quality of messages. How much of our daily e-mail is non-work-related? How many mimic nothing more than the childhood pastime of "passing notes" in school? Is there anything to suggest we will IM differently? Will it degenerate into the communication of sports scores, who got voted off island, and jokes?

Trying to hold it back is a pointless exercise. IM will edge its way into our organizations, simply because it's new and fashionable. So what, if anything, can we do to minimize the negative and maximize the positive benefits?

Plan ahead, create usage standards before we find ourselves surrounded by a white noise with zero content. Define in advance the types of messages we'll send on IM. Set reasonable guidelines on when we can send messages. What is a "timely" response? Must we respond immediately, regardless of who we are speaking with at time the machine chirps?

Preliminary guidelines, created during pilot projects, might help us avoid operating under the belief that the beeping machine ("expletive deleted" coincidental, but probably appropriate) is more important than the hand we were warmly shaking.

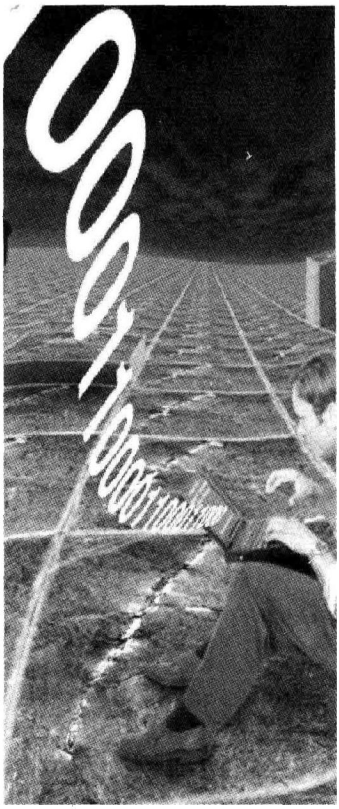
We will inevitably embrace IM. The irony is that we complain people resist change, but when we should resist change, we don't.

试图阻止它是毫无意义的行为。即时信息会慢慢地进入我们的机构，只因它是全新的，时尚的。因此，是否我们所能做的只是使它的负面效应最小化、积极效应最大化?

在发现我们被毫无内容的白色噪音包围之前，要提前规划，创造使用标准，事先定义我们将通过即时信息发送的消息类型，建立何时发送信息的合理指导方针。什么是“及时”的回复？难道不管我们在跟谁说话，当机器发出唧唧的声音时，我们就必须立即回复吗?

在试验性方案中建立初步的指导方针，可能会帮助我们避免认为“嘟嘟”作响的机器（“垃圾信息删除”也许是巧合，但或许是适当的）比我们正在热情握手的人更重要。

我们不可避免地会被即时信息包围。具有讽刺性的是我们常抱怨人们抵制变化，但是当我们自己应该抵制变化的时候，我们却没有这样做。



# *Disaster Planning* **Requires New** Thinking

需要重新思考

# 灾难应对计划

Corporate silo mentality has to end but doing so is no easy task, say experts.

With a series of events hitting corporate Canada over the past 12 months, from SARS and the massive blackout to attacks from the SoBig and Blaster worms, companies are intensifying their disaster preparedness but finding that a siege mentality often exists between departments.

At a Conference Board of Canada corporate security conference held in Toronto last month, Robert Gerden, director, corporate security with Nortel Networks Ltd., spoke of the need for corporate silos to be broken down if companies want to successfully address security and business continuity shortcomings.

But Gerden admitted the task is not an easy one, "It is difficult to break down the barriers, there is not a lot of communication between them." He said. People are often "Protecting political turf." The silos vary from IT and physical security to emergency management and business continuity departments. "You have all these departments that may not be working together," he said.

Rex Pattison, director, business continuity management with the Bank of Nova Scotia, agreed that the silo factor is a hindrance to successful security implementations but that silo existence is often the result of the way companies were traditionally designed.

The key to solving the silo mentality is creating an enterprise risk council comprised of representatives from each department. Later, if a companies chooses to do so, they can take the process a step further and create what Gerden calls the four pillars of security:asset security, business continuity,

专家们认为公司中的无形壁垒应该打破，但是这并非易事。

在过去的12个月里，一系列的突发事件袭击了加拿大的公司，从SARS病毒的传播，大规模的停电事故，到计算机网络遭SoBig和Blaster蠕虫的侵袭。各个公司都在加强他们的抗灾难准备，但却发现各个部门之间都存在着围城心理。

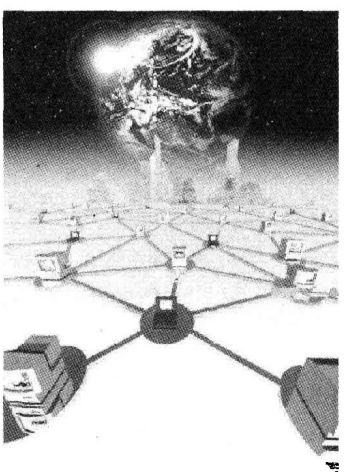
加拿大会议局上个月在多伦多召开了公司安全会议，诺泰尔网络公司负责安全事务的主任罗伯特·格顿说，如果公司想成功地解决安全和业务连贯性的问题，公司内的壁垒就应该被打破。

但是格顿承认这项任务并不轻松。他说："很难打破壁垒，因为他们之间缺乏沟通。"人们经常"保护政治地盘"，这个内部壁垒存在于从负责IT安全和人身安全到负责应急管理和业务连贯性的各个部门。他说："你拥有所有这些部门，但是不一定能保证他们齐心协力地工作。"

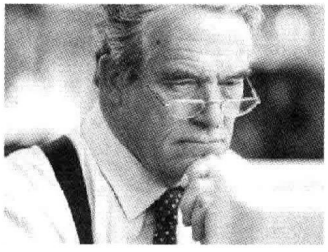
挪瓦·斯考提阿银行的管理业务连贯性的主任雷克斯·派忒逊同意这一说法——内部壁垒妨碍了成功地执行安全体系，但是内部壁垒的存在通常是公司传统设计方式的结果。

解决内部无形壁垒问题的办法是成立一个由公司各个部门的代表组成的企业风险委员会。这样做了之后，他们还可以再向前迈进一步，建立格顿所提出的"安全的四大支柱"：资产安全、业务连贯性、服从安排和财政保护。这四大支柱的负责人分别向企业风险管理专员汇报，再由专员向企业高层汇报。

格顿说，对于风险委员会和风险专员的这两种解决办法，都有赞同和反对的意见。风险委员会的解决办法对现存的组织机构影响较小（公司里不用建立额外的管理层）；但是，因为委员会的性质，没有人须为所有的安全问题负责，所以还存在责任落实的问题。



风险专员的解决办法被格顿视为未来公司解决安全问题的发展方向，为了成功推行，这个办法在公司里存在的可能性必须先通过行政议程的讨论。如果管理不当，各个部门之间会缺乏完整的风险调和。格顿补充说，在上述的基础上，由于一人在上负责，所以要有更强大的安全制约和责任制，要有一个更为简单的组织和报告结构。



compliance and financial protection. These four pillars in turn report to an enterprise risk officer, who in turn reports to the top of the corporate structure.

Gerden said both the risk council and risk officer solutions have their pros and cons. The risk council solution disrupts the existing organization less (there are no additional management levels created in a company), but, because of the very nature of a council, there are accountability issues, since no one person is responsible for all security matters.

The risk officer solution, which is where Gerden sees corporate security going in the future, has to get past the political agendas which may exist within a company in order to succeed, and can lack full risk co-ordination between departments if it is not managed properly, he said. On the upside, there is greater security alignment and accountability, and a simpler organization and reporting structure since there is one person at the top, Gerden added.

Telus Corp., the Burnaby B.C.--based telco, is going through similar security growing pains. Over the past several months it has created a "partnership in governance," said Gene McLean, vice-president and chief security officer at Telus. The partnership is between the company's CIO, CSO and chief information security officer.

"It is working very well," he said, "but it wasn't an easy (stage) to get to." The difficulty was getting everyone " thinking on the same page." Mclean agreed with Gerden that job protectionism and turf wars are common.

Another hurdle is getting all participants to look at security from the company's perspective, not their own department's. Mclean said the ultimate goal of any security practice is protecting the corporate brand.

Gerden added that one often overlooked department is IT. "We need to have a better understanding of what IT security is all about."

And if disaster strikes, not jumping to conclusions is paramount to success, Pattison said.

Reacting too quickly leads to over-simplification, which leads to poor decision making. Pattison said for things to run smoothly in disaster situations, a company needs a good team in place, solid planning and continual testing.

泰勒斯公司（位于加拿大不列颠哥伦比亚省伯纳比市）正在经历类似的安全发展时期的困难。泰勒斯公司的副总裁兼首席安全执行官吉恩·麦可林说，在过去的几个月，公司创建了“管理上的合作伙伴关系”。这是公司的首席信息执行官、首席安全执行官和首席信息安全执行官之间的合作关系。

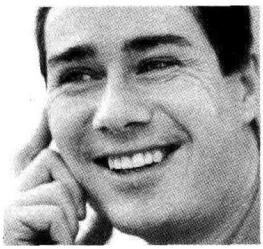
他说：“一切都进展顺利，但是达到这个阶段并不是件容易的事。”困难使每个人“站在同一立场上思考问题”。麦可林同意格顿的观点，认为工作保护主义和派系斗争是普遍存在的。

另一个难题是要让所有的参与者都站在公司的角度而不是站在各自部门的角度来看待安全问题。麦可林说，任何安全措施的最终目的都是是保护公司的品牌。

格顿补充说，经常被忽视的是IT部门。“我们需要对IT安全有更全面的了解。”

帕提逊说，如果灾难降临，对于成功极为重要的是不要急于下结论。

反应太快会导致过于简单化，从而导致作出糟糕的决定。帕提逊说，在灾难来临时，为了使事情平稳地进行，公司需要一个良好的团队，有可靠的计划和经得起持久的考验。



# IT Directors List Cyber Threats as Top Priority

# IT领导者们眼中的首要威胁

Firms failing to report attacks on their IT, phishing, unexpected cyberattacks and cyberterrorism are the four biggest "banana skin" risk areas for IT leaders in 2004, according to a report by the Real Time Club based on a debate and membership survey at the end of 2003.

With the rise in awareness of IT risk as part of overall corporate risk management, the Real Time Club, many members of which are City-oriented IT professionals, aimed to set out a prioritized list of risk areas. This list was influenced by the annual Banana Skins Report from the Centre for the study of Financial Innovation, which identifies broader finance sector business risks.

So far, the Real Time Club's embryonic list is qualitative, drawing on responses from 26 members, but all are well placed to understand the state of the IT industry.

Five of the top 10 risks relate to internet-based attacks on information systems. Concealment of attacks was viewed as the most severe risk, closely followed by phishing–the use of spoof websites and e-mails to elicit confidential information from users.

The danger of unexpected attacks and cyberterrorism followed. At number 10 on the list was the risk of spam halting the internet. Hackers uniting to hit systems with multiple attacks was taken seriously in 11th place.

"Most of these are relatively new phenomena and are new risks we all have to accept and manage if we are to enjoy the benefits of ubiquitous computing and communications," said the report.

The risk of the National Grid failing was in fifth place reflecting IT leaders concern over the power outages experienced in London last autumn.

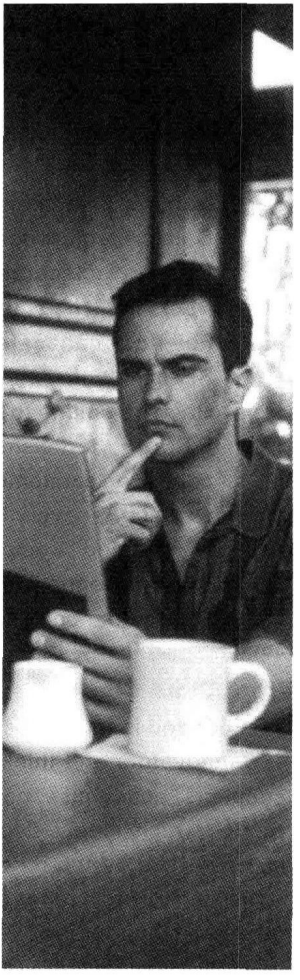
The demands of data protection were racked sixth, with fears they could prevent the effective conduct of e-commerce.

The impact of offshore outsourcing on the UK economy, in seventh place,

“实时”俱乐部在2003年底以辩论和会员调查结果为基础写了一份报告。根据这份报告的内容，在2004年，对IT领导者来说，四个最大的“香蕉皮”风险区域是：公司没能报告他们的IT系统所受到的攻击、网络诈骗、突如其来的网络袭击和网络恐怖主义。

随着越来越多的人把IT风险视为整个公司风险管理的一部分，“实时”俱乐部打算开始对风险区域按照风险的大小列表，而俱乐部的许多成员都是以城市IT方向为职业的。这份列表受到来自金融改革研究中心的年度“香蕉皮报告”的影响，该报告证实了更广泛的金融部门的商业风险。

迄今为止，“实时”俱乐部的调查列表是定性的，收集了来自26个成员的反馈信息，但是已能让人了解当今IT产业所处的现状。



10个最大的风险中的5个都与通过因特网对信息系统的袭击有关。袭击的隐蔽性被视为最严重的风险，紧接下来是网络诈骗——使用欺诈性的网站和电子邮件诱出用户的秘密信息。

再接下来是突如其来的网络袭击和网络恐怖主义。列于表上第十位的是阻塞网络的垃圾邮件，它们会使网络陷于瘫痪。黑客联合起来采用多种手段袭击网络则被认为是居第十一位的风险。

报告上说：“其中大多数相对来说是新现象和新风险。如果我们想从无处不在的计算机运用和通信中获益，就必须接受并管理它们。”

由于全国高压输电网所存在的缺陷而产生的风险被排在第五位，这反映了IT领导者们对去年秋天在伦敦发生的电力中断事件的关注和担忧。

对数据保护的要求被列在第六位，因为害怕丢失数据会阻碍电子商务的有效操作。

海外采购对英国经济的影响列在第七位，这被看作是对IT产业来说不断增长的风险。

列在第八位的是令人头痛的用户使用未经授权的软件或是把他们自己的IT挂在公司的网络上。问题通常是由于IT员工与终端用户缺乏有效的沟通，导致终端用户对系统不满而自己去寻求