Gamutsoft
Gamutsoft Corporation

IT堂速递 CIOEXPRESS

金道 12

金道视点–黑客大战

黑客大战及IT管理责任

–金道服务战略顾问 加藤恒雄先生

嘉宾访谈

马克华菲CIO左敬东

促业务发展的优雅圆舞曲

利丰IT经理陶龙

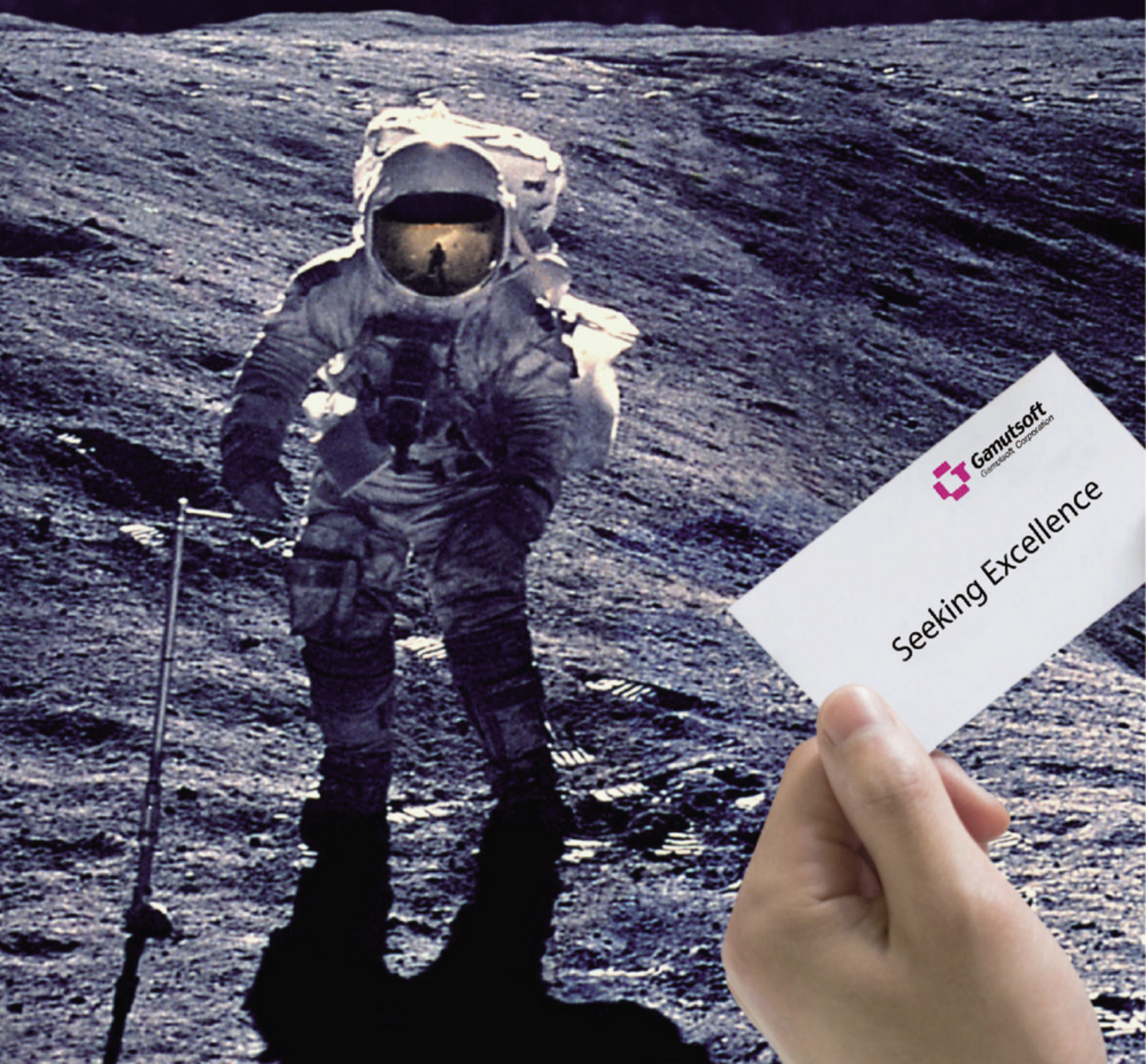
IT价值在技术之外

IDC:2012年唯一确定的就是其不确定性

WPM 金道 服务无所不达

金道，中国本土第一的IT运维外包服务商。

金道致力于为客户提供世界级品质的IT管理服务，总部位于北京，在上海、广州、成都设有分公司，目前，金道拥有600人工程师团队，服务覆盖包括台湾的200座城市，为110余家企业提供以：IT服务台，WPM，数据中心运维等IT专业服务，涉及金融、制造、互联网、医药、零售、汽车、物流、化工等多个行业。



目 录
Contents

希望阅读更多金道专家文章？请登陆金道官网www.gamutsoft.com三人行栏目。

Gamutsoft
Gamutsoft Corporation

北京金道天成信息系统服务有限公司
地址：北京市海淀区中关村东路66号
甲1号世纪科贸大厦A座6层
电话：010-58737222

北京金道天成信息系统服务有限公司
上海分公司
地址：上海市广中西路777弄88号
华清大厦8层
电话：021-60899800

IT堂速递
CIOEXPRESS

金道IT堂俱乐部会刊 编辑部：李金金
主编热线：021-60899800-7526
投稿热线：8008200017
投稿邮箱：marketing@gamutsoft.com

黑客大战及IT管理责任

Cyber War and IT Management Responsibilities

■ 金道服务战略顾问 加藤恒雄先生

黑客大战已经从电影故事沿袭到我们真实的工作及生活。
那谁是你的白客?

7月中旬，美国宣布“除了传统来自陆、海、空、以及太空的4种入侵外，美国承认存在第五种威胁（网络攻击），并将反击任何对美国发起网络攻击的国家”。

在当今的网络时代，如果没有连接到网络的PC或智能手机，我们无法开展生意，也无法享受生活。因此，倘若网络访问中断或数据被窃取，那可真是事关重大。今天，我想通过向你介绍一些今年发生的事件，来谈谈我们该如何保护自己。

DDoS攻击及BOT

2011年3月3日，韩国总统办公室、军事机构及多家证券公司网站收到大量数据（俗称DDoS攻击），导致系统被挂起且一连持续了3天。约10万台电脑向这些站点发出海量数据，导致用户无法进行正常Web访问。而这些电脑的机主大多却并不知道参与了这一犯罪。

这10万台PC由来自70个国家的750台PC及服务器远程控制，其中3台安装在日本。此程序被称为BOT，名称来源于“被远程控制的机器人”。韩国政府通过国际刑警组织要求日本调查这3台肇事PC及服务器。日本警方发现2台服务器来自两家中小型企业：一台位于北海道，一台位于香川县；他们都是小公司，缺乏对安全系统的投资。第三台是一名东京男子的个人电脑，它并未安装有效的病毒安全程序，并且始终保持联网状态。而所有这三位主人对于自己就是网络攻击者一事一无所知。

基于网络日志数据，警察发现这些病毒来自于北朝鲜。虽然朝鲜可能会拒绝承认，说他们也可以是受害者（即有人用BOT控制了在朝鲜的服务器），但是除非他们打开日志数据，证明病毒原始发件人不是在朝鲜，否则他们不能说“我们不是攻击者”。

一段时间以后，日本警方发现了另一个攻击源。他们来到一间便利店，对那里的经理说：“你的店通过DDoS攻击了朝鲜”。无疑，这对

2011年3月3日，韩国总统办公室、军事机构及多家证券公司网站收到大量数据（俗称DDoS攻击），导致系统被挂起且一连持续了3天。

那位经理来说是个大“惊喜”。该问题设备是一个安全摄像头，这种安全摄像头将视频/图像数据发送到保安公司，它可以随时进入摄像头监控店面，这就意味着该摄像头有一个可能感染外部计算机病毒的内置操作系统。

McAfee的董事之一表示：“可以连接互联网的电视、视频/HDD、录像机和甚至高科技咖啡壶都应具备内置的安全程序包”。他说：“如果你认为那些只是简单的家用电器，那将是一个巨大的错误”。因此，你应当明白有这样一种可能，“（或许）某天，由于你的家用设备被外人控制，你将可能成为一名网络攻击者（黑客），而你自己却毫不知情。”

由于海量数据的发件人可以轻松地被检测到，因此即使袭击者可能不是攻击的发起端，追查源IP地址现在也并不是难事。尽管国家之间针对网络恐怖主义的合作规则尚未牢固确立，追查本身也可能需要花费不长不短的时间，但国家之间警察网络（例如国际刑警组织）的合作依然能关闭任何服务器或电脑。

特洛伊及多种病毒

三菱重工几个月前就意识到有病毒入侵，并开始对其进行分析。由于其业务遍及原子装置、潜艇、护航船、拦截导弹和火箭发动机等，所以数据被窃取一事非常严重。他们宣布至少有9个场所和80台服务器感染了8种类型病毒。

他们最近公布的病毒种类数量达50多个。其中一个工作站就有28种不同的病毒。

2004年的数据窃取病毒“Worm_Agobot”、篡改网站并向访问站点的计算机发送病毒的“Gumblar”，甚至连盗取银行帐户信息的“Spy-eye”都已被成功揪出；然而，实际上这些病毒大多都可以通过定期更新安全包来阻止，这也就意味着，这些中招的公司其IT安全管理实在太差劲，他们的CIO都应被立即开除！哈哈！

他们还发现了另一个不能通过常规安全软件检测到的病毒。这种病毒入侵之后立即创建另一种病毒。一名雇员从他的朋友那里收到一封新年问候邮件，并打开了里面的贺卡。这卡就是病毒，但它比较隐蔽，因此当事者并不知道感染了病毒。发件人（服务器）来自台湾，但我们不知道他们是否就是始作俑者，抑或是BOT程序。

没有任何夸张，黑客大战的确成为当下的一个严重问题。每个人都应该考虑如何在这个黑客大战时代中保护他们的公司和国家免受故意攻击。

此外，他们发现SJAC（日本航空宇宙工业会）也卷入到攻击三菱的数据窃取事件中。病毒是藏在一封假冒从SJAC某高管十个小时前发出来的邮件里面。接收方认为是真正的邮件，也就丝毫没有怀疑地打开了它。

下面是一些发生在世界各地的重大事件：

2003年，美国核电站计算机：安全监控系统停止了5个小时。

2003年，美国华盛顿附近铁路系统：系统崩溃。

2005年，美国一汽车厂5万名职工：生产短时中断。

2006年，美国水净化厂：监控系统被远程控制。

2007年，爱沙尼亚政府和银行系统：访问中断。

2008年，波兰铁路点交换系统：14岁的男孩制造了脱轨事故。

2008年，美国五角大楼：网络被入侵，数据被发往其他国家。

2009年，能源行业：中国黑客团体发起夜龙行动。

2009年，谷歌：约30家公司被入侵，民间维权的邮件被复制。

2010年2月，伊朗核电站：为西门子专门调整的Stuxnet搞砸了 30,000台电脑 。

2011年，14个国家政府及相关机构被意想不到的Shady-rat窃取数据。

以上只是冰山一角。过去十年有成千上万大小不一的入侵事件，而且毫无疑问，这些数字还在不断上升。这可没有任何夸张，黑客大战的确成为当下的一个严重问题。每个人都应该考虑如何在这个黑客大战时代中保护他们的公司和国家免受故意攻击。

IT安全的提升

我谈论黑客大战的原因之一是因为金道所属的正是IT服务产业。

去年（2010年）一家跨国企业（金道客户之一）决定让其雇员自由访问网页，即雇员可从自己办公室访问他们喜欢的任何网站。我相信，这只是

在员工休息时才被允许。自然，每月数百例的病毒感染在急剧上升。金道服务团队被要求每天清理众多被感染的电脑，一些是可以直接清除病毒，另一些则需要完全重新安装操作系统。

尽管这种清洁服务增加了我们的额外收入，金道依然建议客户加强防火墙措施，尤其是为中国定制防病毒程序。我们说过，除了全球标准的体系结构和员工培训外，还可能需要建立一个双安全功能，因为大部分的英语防病毒软件包（全球标准）不可能完全检测出用中文编写的特洛伊程序。但客户CIO友好地拒绝了我们的附加服务报价，而是只支付受感染部分设备的服务费用。

由于大部分病毒感染都来自于可疑网站和不假思索打开邮件中的附件，所以我们需要做到以下几点：

1)随时随地注意培训每一位员工，这非常重要。不过，正如我在上一篇文章中提到的，如果邮件来自于你的老板或你的朋友发送的贺卡，你可能毫不怀疑无辜地就打开了。这是人类的天性。

2)我们必须让他们及时更新Windows和防病毒程序。然而，如之前所述，一些间谍软件无法被普通的防病毒软件检测出。

上述培训是有效的，但有人类天性存在，就不能防止每个感染。所以我们还有如下建议：

1.该公司的IT部门应限制员工仅访问授权的网站。员工不应使用公司电脑访问作个人用途的站点。此限制措施可显著减少公司里的病毒感染机会。

2.由网络专家做常规/定期检查是必不可少的。能做这种工作的人被称为“白色黑客”（用犯罪行为反击黑客）。这些检查可能包括入侵测试（针孔检测）。

3.至于防火墙反病毒架构，我们建议您为了安全起见考虑冗余保护。

我之所以这么说是因为BOT。

如果您不完全保护您的服务器和您员工的个人电脑，这些设备可能会从外部被控制，比如被人恶意用于攻击其他公司或国家。也许您公司的PC就被用于了攻击韩国或三菱重工。如果您是IT部门的主管，但却不能保护您的网络免遭病毒，那您就是一名同犯，尽管您不一定会被国际刑警组织逮捕，但您不能说“我是无辜的受害者”。

就职于IT行业之外的多数智能手机用户，都不知道自己手机的潜在能力和病毒风险。关于安卓系统的智能手机增速迅猛，据一项技术报导，迄今已发现的恶性病毒数量已经接近200个。

智能手机及移动终端

智能手机现在已经席卷了世界的每一个角落。除Apple手机外，Android手机也正急剧加速智能手机的应用，它不仅迅速占领了个人市场，也同时占领了商业市场。目前，Google和Apple两家的智能手机应用相加已经有75万个之多。

就职于IT行业之外的多数智能手机用户，都不知道自己手机的潜在能力和病毒风险。去年8月，在美国一个安全大会上有个演示，他们使用一部智能手机‘渗透’汽车的电脑并启动了引擎。

关于安卓系统的智能手机增速迅猛，据一项技术报导，迄今已发现的恶性病毒数量已经接近200个。而这也在我看到的电视节目中被再次证实。黑客将手机设置成静音状态，然后拨打这部手机，黑客就可以听到这部手机旁边的任何声响，比如，一个商业会议。

黑客同样可以通过远程操控盗取图片。他们可以盗取手机用户昨天在确认其项目损益时刚从公司数据库中下载的数据文件夹。你的手机通讯录，通话记录，以及图片库都可以很容易的被盗取。我们必须意识到，“智能手机=PC=可能被远程控制的高风险”。因此，在日本，所有网络服务供应商（比如Softbank和Docomo）现在都在致力于如何加强对其用户的安全服务。

日本移动通信运营商多科莫公司已经发布了4款智能手机机型及2款平板电脑机型；这些都基于长时间的技术演变，因此被称为超级3G。而被韩国三星所代工生产的最新机型“Galaxy SII LTE”已经达到了峰值75兆每秒，比基于3G的机型快了5倍，但价格却只有2000人民币。虽然这个速度已经足够于商业用途，但你或许也已经知道LTE将很快成为下一代全球通信技术标准（目前已有70个国家同意使用），因此1GB每秒的下载速度在1到2年内将不再是梦想。

总结

几年前“云计算”还只是在IT从业人群中流传，但如今，每个人都知道它已融入我们日常生

下为本文英文版本

Cyber War and IT Management Responsibilities

■ T. Kato, Strategy Consultant, Gamutsoft Corporation

活，也可以为个人所用！由于各种应用和数据存储空间遍布于网络中，使用者无法确定其确切位置，它也被冠以“云服务”的称呼，就像苹果的i-cloud。由于这种服务的提供只能基于高速通信连接，因此许多企业开始使用ICT（信息通讯技术）来代替IT也变得情理之中。

在网络年代，保护终端用户信息及数据的重要性愈发突出。基于此原因，即为了改进手机、电脑以及通讯网络的安全，无论是对个人、公司或国家，我们所需要的都是真正卓越的工程师。在未来10到20年里，“白客”们将在世界范围内无数私有组织或政府机构中成为最受欢迎的资源，因为好的“白客”知道如何抵御“黑客”们的系统攻击。

早在2010年，金道就意识到人们的工作场所将不再限制于工厂或办公室，而是延展到几乎你能想象到得任何场合，比如在客户的办公地点、机场、火车、咖啡店、甚至家里，你都能通过智能IT设备连接高速无线/有线网络来工作。基于此，金道2010年即推出了WPM（工作环境管理）服务，其中以解决移动终端用户需求的“IT服务台”及“IT安全性管理”是WPM里最关键的组成部分。

在这个急剧变化的生活和快速发展的网络环境中，信息系统安全应该成为任何一个CIO的首要关注点。这也是金道致力于为我们的客户提升相关服务技能的原因。

—加藤恒雄，金道服务战略顾问

Middle of July, the USA announced that “In addition to the 4 kinds of traditional intrusions to land-sea-and air, and from Space, the US recognizes the 5th threat and would fight back to the country who initiated Cyber attacks to the US”.

In this network era, we cannot do any business and/or enjoy our life without connecting PC or smart phones to the network. Hence, it is truly a big problem if the network access is disturbed or the data is stolen by somebody. Today, I would like to talk how we should protect ourselves by showing you some incidents recently happened.

DDoS Attack and BOT

March 3, 2011, Web sites of Korea President Office, Military organizations, and many Stockbrokerage firms received massive data (known as DDoS attack) and many of their systems hanged up. This continued for 3 days. About 100,000 PCs sent massive data to the sites so that normal access to the Web became impossible. Most of those PC owners were not aware of the involvement to the crime.

Those 100,000 PCs were remotely controlled by 750 PCs/Servers in 70 countries including 3 servers/PCs installed in Japan. The programs are called BOT. The name comes from Robot because of remotely controlled. Korea government asked Japan to investigate those 3 via ICPO. Japan police found that 2 servers are in SMEs; one in Hokkaido and the other is in Kagawa prefecture. They are small companies and their security system was poorly invested. The third one is a PC of a man in Tokyo who did

not install effective virus security program and also left the PC permanently connected to internet. All three owners never knew they are assailants.

Based on the network log data, the police found the virus was sent from North Korea. Although the North Korea may deny the crime and say they could also be a victim, i.e. somebody controlled the servers in North Korea as BOT, unless they open the log data and prove the virus originators are not in North Korea, they cannot say "we are not assailants".

A while later, the Japan police found another one. They visited a convenience store and said to the manager "your store attached Korea by DDoS". It was a big surprise for the manager. The problem equipment was a security camera. Such security cameras send video/picture data to the contracted security company, and the company can also access to the cameras to monitor the store at any time. This means the camera has a built-in OS that can be affected by computer virus from outside.

One of the McAfee's directors says "Internet connected TVs, video/HDD recorders, and even a high-tech coffee maker should have built-in security packages". He says "It is a big mistake if you think those are simple home apparatus". Therefore, you should consider "one day, you may be an assailant in a Cyber War without knowing that one of your home equipment is controlled by somebody else".

The massive data sender can be easily detected so that tracing back the source IP Addresses is not difficult although the assailants may not be the originator of the attack. The collaboration of police network, e.g. ICPO, between countries could work to stop the servers/PCs, although it may take so-so lengthy hours and the collaboration rule between countries againstcyber terrorism has not yet firmly established.

Trojan and Various Viruses

Mitsubishi Heavy Industries realized the virus penetration since some months ago and started to analyze them. Their divisions develop atomic plants, submarines, escort ships, interceptor missiles, and rocket engines. Hence, the stolen data is a serious issue. They announced that at least 9 locations and 80 servers were affected by 8 types of viruses.

This is not any exaggerations but true that the Cyber War is a serious on-going problem. Everybody should think how to protect their company and their country from willful attacks in this Cyber War era.

They recently updated that the number of kinds of virus is more than 50. One of their work stations had 28 different viruses.

The data stealer "Worm_Agobot" (2004), "Gumblar" that modifies web site and send virus to the machine who accessed the site, and even "Spy-eye" that steals the bank account information were found; however, most of them can be blocked by regularly updating security packages. This means, their IT security management is very poor so that CIO(s) should be immediately fired! Ha! ha! ha!

They found another one that could not be detected by regular security software. This virus creates another virus after the penetration. One employee received a New Year message from his friend and opened the card. That card was virus but very quiet for a while so that the person was not aware of the infection. The sender (server) was from Taiwan, but we do not know whether they are the assailant or a BOT.

Furthermore, they found that SJAC (Society of Japanese Aerospace Companies; was involved to attack Mitsubishi for stealing data. The virus mail was forged by using an actual mail with attachment sent from an executive in SJAC 10 hours ago. The receiver thought it is a real mail so that opened it without doubt.

Some of the major incidents around the world are as follows:
2003, nuclear plant computer in the US: security monitoring system stopped for 5 hours.
2003, railway system around Washington DC, USA: system was messed up.
2005, automobile factory - 50,000 workers in the US: production stopped for a while.
2006, water purifying plant in the US: monitoring system was remotely controlled.
2007, government and banking systems in Estonia: access blocked.
2008, railway point switching system in Poland: 14

years old boy caused derailment accident.
2008, US Pentagon: network was affected and the data was sent to other countries.
2009, energy industry: the Night Dragon operation began by a China hackers group.
2009, Google: about 30 companies were affected and mail of civil-rights activists was copied.
2010, nuclear plant in Iran: Stuxnet specially tuned for Siemens screwed up 30,000 PCs.
2011, government and related organizations in 14 countries: revelation of Shady-rat operation that steals data.

The above are a tip of the iceberg. There are thousands of penetrations; some are big and some are small in the past decade, but undoubtedly, the numbers are increasing.
This is not any exaggerations but true that the Cyber War is a serious on-going problem. Everybody should think how to protect their company and their country from willful attacks in this Cyber War era.

IT Security Improvement

One of the reasons why I talk about Cyber War comes from the IT service industry where Gamutsoft belongs to.

Last year (2010), the global headquarters of a multi-national company (one of Gamutsoft customers) decided to make free the web access for their employees, i.e. employees can access any sites as they like from their office. I believe they are allowed to do so during their recess time. Naturally, virus infection dramatically increased at several hundred cases per month level. Gamutsoft service team was requested to clean up so many affected PCs every day; some to remove the virus, and some to completely reinstall the operating system.

Although such cleaning service generated additional revenue, Gamutsoft proposed the customer to strengthen the firewall especially the China specific anti-virus programs. We said that, in addition to the global standard architecture and employee trainings, it may be required to build a double security feature since most of English based (global standard) anti-virus packages may not perfectly detect Trojan written in Chinese. The customer CIO kindly rejected our additional service offer, but only pay for troops to firefight with infected devices.

Excluding we who are working in IT industry, most of the smart phone owners do not know the hidden capabilities and virus risks of their phones.

Since most of virus infections come from doubtful web site accesses and unconsidered opening of files attached to incoming mail,

1)It is very important to train every employee about when and where they must pay attention. However, as I wrote in the previous article, if a mail is from your boss, or a greeting card sent from your friend, you may innocently open the file without doubt. This is a human's nature.

2)We must let them promptly update windows and anti-virus programs. However, as I mentioned before, some of spyware cannot be detected by normal anti-virus software.

The above trainings are effective but cannot prevent every infection because of human's nature.

1.The company IT department should limit employees to access authorized sites only. Employees should not use company PC to access the sites for personal purposes. This restriction dramatically decreases the chance of virus infection in business.

2.Regular/periodical inspection by network specialist is indispensable. The people who could do such job is called "white hacker"; against black hacker who does criminal act. This inspection may include a penetration test (pinhole detection).

3.Depending on the firewall/anti-virus structure, we recommend to consider redundant protection for the sake of safety.

Why I say this is because of BOT.
If you do not perfectly protect your servers and your employees' PCs, these equipment may be controlled from outside, i.e. used by willful people to attack other companies or countries. Maybe your company's PCs were used for attacking Korea or Mitsubishi Heavy Industries. If you are in charge of the IT

department and did not protect your network against virus, you are one of the assailants, and you cannot say I am an innocent victim although it is a question whether or not you may be arrested by ICPO.

Smart Phone and Mobile Terminals

Smart phone is now very popular everywhere in the world. In addition to Apple, Android has dramatically accelerated the use of smart phone not only in personal use, but in business as well. There are over 750,000 smart phone applications for Google and Apple.

Excluding we who are working in IT industry, most of the smart phone owners do not know the hidden capabilities and virus risks of their phones. In August last year, there was a demonstration in a security conference in the US. They used a smart phone to penetrate in the computer of a car, and started its engine.

In regard to the Android based smart phones rapidly increasing, one technical report says there are almost 200 very harmful viruses found to date so far. I also saw the virus demonstration on TV. The hacker sets the phone to silent mode, and then calls the phone. The hacker can now listen to what is going on around that phone (e.g. a business meeting).

They can even take a photo remotely. They can steal a data file that was downloaded from the company DB yesterday when the phone user confirmed profit and loss on his/her project.Your phone directory, call history, and photo library are easy to steal. We must understand that "smart phone = PC = a high risk to be remotely controlled". Hence, in Japan, all the network service providers (such as Softbank and Docomo) are now chasing on how to strengthen the security services for their users.

NTT Docomo in Japan already released 4 smart phone models and 2 tablet PC models; those are LTE (Long Term Evolution) technology based, so called Super 3G. The latest model "Galaxy SII LTE" OEMed by Samsung Korea achieved maximum 75MBit/sec that is about 5 times faster than the 3G based models, but the price is 2,000RMB only.Although this speed is high enough for business use; however, you may know that LTE will soon become the next global communication standard (70 countries are so far agreed to use it) so that 1GB per second (downloading) is not a dream within two years.

"Cloud Computing" was a buzz word only in IT business guys since a decade ago, but now, every body knows it is in our daily life for personal use also!

Summary

"Cloud Computing" was a buzz word only in IT business guys since a decade ago, but now, everybody knows it is in our daily life for personal use also! As far as the application and data storage space are in the network somewhere the user does not know exactly where, it is called "Could Service", like Apple's i-Cloud for example. This type of service cannot be provided without high speed communication link. Hence, it is quite understandable that many companies started to use ICT (Information and Communication Technology) instead of IT.

The importance to secure end user's information/data is dramatically increasing in this network era. For this reason, i.e. to improve phones, PCs, and communication network security regardless whether it is for your personal or company or country, what we need is so called excellent engineers. In the next 10 to 20 years, the white hackers are one of the most welcome resources in many private or government organizations in the world, because good hackers know how to defend the system from any attack of black hackers.

Early 2010, Gamutsoft announced WPM (Work Place Management) services since we know the work place will not be only factory or office but any place including your customer site, airport, on train, coffee shop and your home by using smart IT equipment connected through the high speed wireless (or wired) network. The Service Desk that solves issues on mobile terminal users and the IT Security Management are the most important ones in WPM services.

In this dramatically changing life and rapidly advancing network environment, the information system security should be the greatest concern of any CIO, so that Gamutsoft is keen to improve its service skills for our customers.

-T. Kato, Strategy Consultant, Gamutsoft Corporation

IDC:2012年唯一确定的就是其不确定性

2011年11月22日--国际数据公司（IDC）公布其对于亚太区（不含日本）2012 年度信息通信产业十大预测，2012 年经济形势的不稳定前景和不确定性成为其基调。

尽管市场波动空前剧烈，但各公司仍期待在这个地区取得增长。业界领袖将不得不直面艰难的投资决策，为保持增长，企业将寻求以更新颖、更稳健的方式利用信息通信技术。更多观点将在即将出版的《IDC 亚太区（不含日本）2012 年信息通信产业十大预测》报告中发表。

“即将到来的2012 年似乎将是动荡不安的一年，唯一能确定的就是其不确定性。虽然亚太地区正逐渐摆脱困扰其他地区的经济困境，但各公司似乎对于信息通信技术投资有些举棋不定。尽管审慎，但也雄心勃勃，各公司仍将争取在本地区实现利润增长。但伴随着消费者和劳动者的日渐精明和富裕，要求也日渐提高，各公司将需要明智地进行投资，避免在全球范围新的经济危机冲击下吃亏。”IDC 亚太区新兴技术研究负责人 Claus Mortensen 如是说。

尽管 IDC 承认 2012 年全球经济衰退的风险依然存在，但同时也预计其对亚太区的信息技术支出不会产生重大影响。鉴于2012年全球经济前景充满不确定性，IDC 预计，本地区的企业会在即将到来的一年采取谨慎的态度对待信息技术方面的支出。IDC 预计，2012 年度亚太区（不含日本）信息技术行业支出将达到 6530 亿美元，同比增长 10.4%。IDC 预期增长将低于 2011 年同期。增长率将在未来 4-5 年间有所降低，但是到 2015 年，仍将保持在 9%以上。

根据 IDC 最新研究以及 IDC 各地区和各国的分析师们的内部头脑风暴会议结果，IDC 做出了2012 年度信息通信产业十大预测，如下所述。IDC 相信，与其他趋势相比，这些发展趋势将对亚太区（不含日本）信息技术市场产生更大的商业影响。

1. 从新兴到新兴：亚洲新兴企业不同于传统的商业和交付模式将在 2012 年推动新一波ICT支出。

IDC 认为，一种新型企业正左右着市场：“亚洲新兴企业”。这些企业积极寻求挑战传统的跨国公司，渴求增长和地域扩张，与来自成熟经济体的公司有着本质的不同。这些新兴企业的首席技术官们正设法寻找新的途径展开更有效的竞争，缩短其IT投资用于推动业务发展的时间。IDC 预测，亚洲新兴企业将推动新一波突破性IT技术投资，例如：移动化、云计算、业务分析和社交媒体。

2. “1”的价值：亚洲企业推崇IT产品单一化的价值。

由于亚太区的市场环境十分复杂，企业开始推崇产品“单一化”，并意识到单一化的产品可以为厂商/供应商创造成功、可持续的商业模式。典型的例子就是苹果，它致力于简单性：只生产一种手机产品，以及一种媒体平板产品。在苹果出现之前，许多企业曾将差异化奉为移动设备行业的重要成功要素，而 IDC 预计，信息技术公司普遍会在 2012 年以及往后数年采用“单一化”的模式。

3. 使2+2=1：云整合服务推动外包进入 3.0 时代

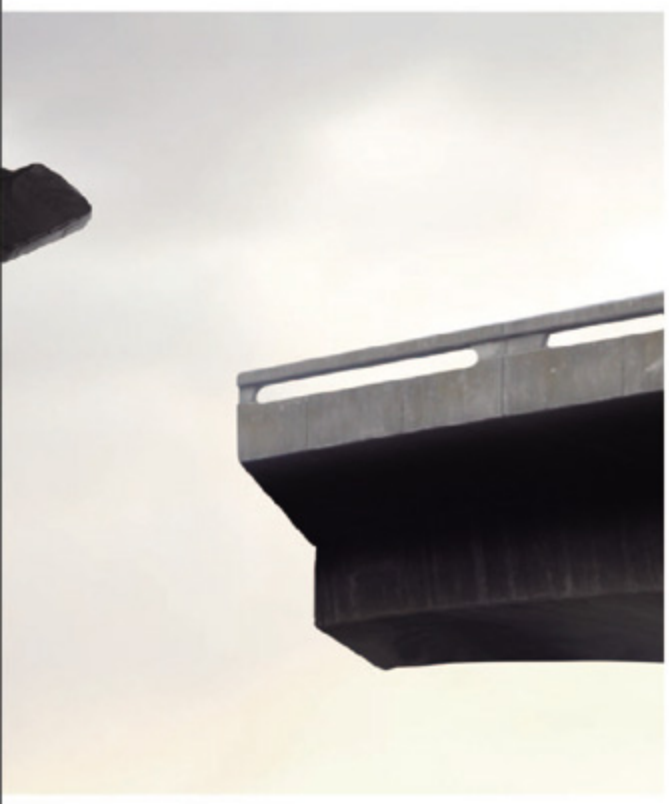
2011 年，IDC 预测，企业新增应用开发的80%将基于公共云平台，到 2015 年，将占到企业应用支出的20%将采用“云包”。因此，云服务的购买者将不得不与更多的服务和厂商打交道，增加了上马原本应该更易于操作的新服务的管理难度。为解决这一问题，在 2012 年及之后，云服务提供商将对分散的云服务进行流程整合管理，即云整合。到 2015 年，市场将不再热议云服务，而会将其视作外包服务的自然演变，即外包 3.0。

4. 首席数据师将把“大数据”与业务挂钩

IDC 预计，2012 年亚太地区将迎来“大数据”时代。社交媒体互动、实时传感器数据、地理空间信息和其他数据来源，不但给企业制定下一代信息战略带来大量挑战，同时也给企业带来重大的机遇。最为有用的见解将来自于高级分析，或者大数据分析。这类分析能对日渐海量、迅速、复杂多样的企业数据进行分析。但大数据分析的各种参数和模型可能是全新的，需要采用多种新的分析技术，IDC 相信，2012 年将出现“首席数据师”职位，他们将制定企业“大数据”战略。

5. 新的云工作负载将出现：需自动化引领

IDC 预计，基于当前经济形势的不确定性，2012 年 IT 业将朝着适应不断变化的业务需求方向发展，迅速提供 IT 服务和 IT 资源的能力将成为在市场竞争中获得优势的关键因素。IDC 相信，随着新一波云工作负载浪潮的出现，IT 流程标准化和自动化将日益重要，自动化将成为 2012 年首席信息官们关注的焦点。对标准化和自动化的投资将促使公司充满活力的设计，加速其业务服务的交付和管理，从而使公司能灵活适应关键业务流程的要求，确保 IT 技术更深地融入整体业务运营之中。



6. 应用整合者：电信运营商的创新先锋队服务于个人和企业用户

通过多样化的终端、及固定和移动网络承载的数字内容和应用的爆炸式增长，给电信运营商带来新的机遇。现在，他们有机会整合各种应用和内容，为最终用户提供互联互通、个性化、以客户为中心的解决方案。然而，这需要电信运营商建立专门的团队发掘、捆绑、整合并发布“正确”的业务应用或个人应用。IDC相信，在2012年，具有远见的电信运营商将建立专业化的创新团队，为家庭用户、企业用户和热点用户发掘和提供适合的应用和内容。

7. 故障预测将成为建设战略平台选项之一

不可预测的IT系统对于企业绩效会产生巨大的影响，为消除这一影响，企业投入大量资金为服务器、系统、数据和网络制作备份，亦称之为冗余。而IDC预计，富有远见的公司在2012年的想法会有所不同。幅度，只要平台故障在误差幅度内，企业就不必依赖冗余了。IDC预计，上述概念将在2012年获得广泛关注，成为企业在未来几年部署大型虚拟化X86环境时的优先选择。

8. 企业将回归以客户为中心的IT服务

由于经济前景的不确定性，IDC预计，“以客户为中心”将成为2012年亚太区企业的首要工作。此外，企业还将关注有助于提高对客户的关注、增强客户参与度、加强对业务贡献最多的客户的了解的技术。如果经济形势向好，“以客户为中心”到了2013年或许就不会再受到同样重视，但IDC预计，到2015年，坚持“关注客户”对大多数IT企业而言都是不可或缺的工作重点。

9. 移动业务和IT的融合将为新的工作空间铺平道路

IDC预计，2012年各企业将围绕移动性、云和数据服务，开始建立新的工作空间架构。IT消费化对工作环境提出了新的要求，IDC预计，2012年企业将利用桌面更新、绿色部署以及远程/小站点操作等机会，测试新的移动服务和解决方案。

10. 成为“中产阶级”：价格低于100美元的智能手机将成为新的收入来源

智能手机的出现宣告新的个人计算时代的来临。2012年，预计亚太地区智能手机的出货量将超过PC机的出货量，这一趋势很可能无法再被逆转。IDC预计，2012年市场中将出现低于100美元的智能手机，将为新兴亚洲市场的服务提供商创造巨大的机遇。IDC还相信，新兴亚洲市场的消费者对于移动应用的依赖程度很快将赶上成熟市场的消费者。

—来自互联网

关于IDC的预测

IDC的亚太区（不含日本）年度预测根据最新的IDC研究和IDC遍及全球各地的1000多位分析师们的头脑风暴结果总结得出。紧随预测报告的是一份全面的地区性评论，内容包括重要业内事件、用户趋势、供应商战略以及对有望明确界定特定技术发展趋势、从而对2012年的亚太区（不含日本）市场产生推动性影响的各项经济措施。在全球各地，随着IDC全球十大预测的发布，IDC的地区团队、技术团队和行业团队也会在随后几个月发布其专项预测报告。

Gartner预测2012年十大IT技术发展趋势

Gartner 副主席David Cearley称，组成IT系统的的技术处于关键发展阶段，在未来五年，移动设备，服务器应用和社交网络应用将从各个方面影响IT，因此各大公司从现在起就要做好准备。

例如，企业需要投资改善网络容量和可靠性。他们还需要改进无线监管从而提升服务水平，在参加本周Gartner Symposium IT/Expo大会时，Cearley对与会者如是说。下面是Gartner对十大IT技术趋势的预测以及就各相关事项做出的解释：

1. 多媒体平板电脑等：

研发核心技术已经成为企业生存准则，因为这涉及到IT需要面临的安全问题和管理挑战。到2015年，多媒体平板电脑的销售将达到笔记本销售的一半，而Windows 8则会成为安卓与Apple后的第三大系统。Cearley说，微软在用户平台的市场份额将减少到60%甚至是50%。Windows为主流PC系统的时代将会被后PC时代所取代，这意味着Windows将成为多样化IT环境的一种选择而已。在智能手机领域，2012年入门级智能手机的价格会降至75美元，且这样的手机还配备了双核甚至四核的处理器，屏幕更大更亮，分辨率更高，同时还兼有3D，HD视频和更多传感技术，如gyros，指南针和气压计等。而Gartner认为目前虽然iOS主导平板市场，但2015年iOS/Android的市场份额将占到80%。

2. 移动应用和接口：

触摸，手势和语音搜索都将改变移动应用的工作方式。到2014年，每年应用商店的移动应用下载量将超过七百亿。到2014年，至少有一半在2010年进行了优化的App Store的应用程序将被收购或不复存在。

3. 社交与文本用户体验：

据Gartner透露，文本感知型计算使用的是与终端用户或与对象的环境，活动连接以及偏好等相关的信息来改进与终端用户或对象的互动。文本感知型系统可预知用户需求，然后提供最合适的内容，产品或服务。预计到2015年，全球40%的智能手机用户会选择能追踪其操作的文本服务供应商，因为谷歌，微软，诺基亚和苹果到2015年的时候将能追踪到全球10%人口的操作习惯。

4. 应用商店和市场：

企业应用商店数量的上升是关键，这些商店可以为用户开发指定应用。这也可以让IT部门参与特定应用的管理与控制。但是Cearley称，IT企业或许比较难接受用户的选择。企业应该使用托管多样化的方法关注应用商店的努力并通过根据风险和价值区分应用。应用的商业价值较低而潜在风险很高时，应将应用完全拦截。

5. 物联网：

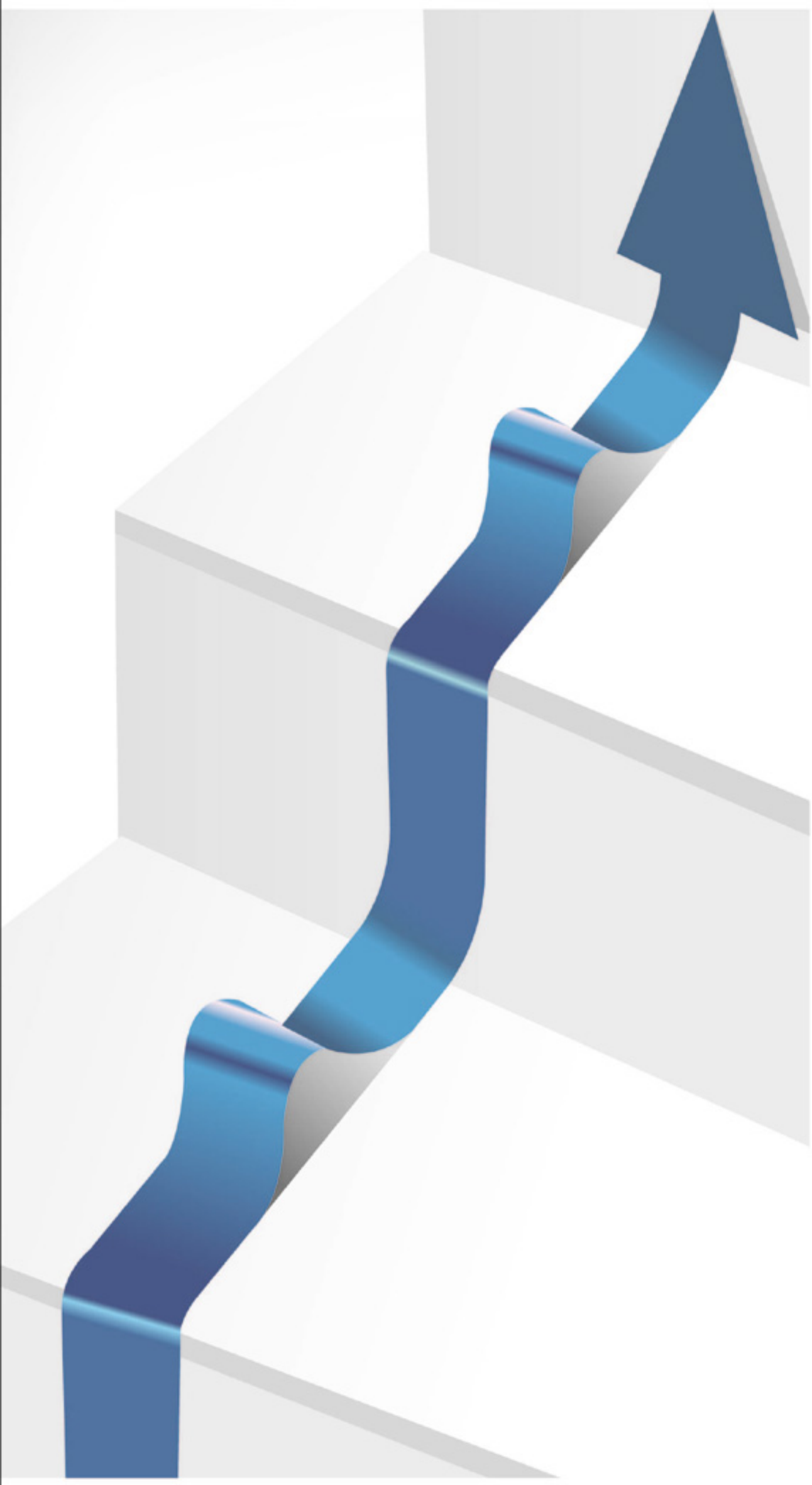
我们正在创建无处不在的运算环境，在此环境中，摄像头，传感器，麦克风，图像识别等都只是组成部分。现在，遥感技术的使用也是物联网的一部分。此外，不断增长的智能设备还带来了隐私问题。Cearley称，IT部门需要对所有设备提供集中式统一管理。

6. 下一代分析：

大多数企业都达到了性能与成本的改进，因此他们可以对业务中希望采取的每项行动进行分析与模拟。不仅仅是数据中心系统可以做到这一点，移动设备也需要访问数据，以及拥有足够的能力执行分析。IT部门可以集中精力开发有助于决策的分析技术。

7. 大数据：

大数据作为IT管理者一项很重要的挑战快速涌现，尽管这个词只是在2009年才开始流行。到2011年2月，谷歌有关“大



数据”的搜索词条已达290万，而供应商现在都宣传自己的产品可以应对大数据带来的挑战。企业必须意识到他们无法存储所有信息。有新技术可以处理极限数据值，如Apache Hadoop，但是企业也要开发出新技能才能有效使用这些技术，Cearley说。

8. 缓存运算：

我们将看到闪存广泛使用于消费电子设备，娱乐设备及其它嵌入式IT系统中。此外，闪存也为服务器和客户电脑中的缓存级别提供了新一层次。与服务器和PC中的主要存储RAM不同，闪存更为持久。因此，它更像是磁盘驱动，因为我们在断电和重启都不会对其产生什么影响。只不过闪存的读取速度快于磁盘驱动。一分钱一分货，闪存用于数据中心，可以优化闪存使用和延长闪存耐用性的软件成为关键。用户和IT供应商应该将缓存运算视为长期技术发展趋势，而且这种趋势与云计算相比可能有着干扰性的影响。

9. 低功耗服务器：

如果你可以把一个盒子中的10台虚拟机转换成40台比较慢，能耗很低的物理服务器，你会怎么做？其实客户对这类处理大数据的运算类型也有需要。例如，数以千计的小型处理器可以执行Hadoop进程。Gartner认为10%—15%的企业工作量适合这样的操作。服务器技术将得到发展以便处理大数据。

10. 云计算：

这个话题的热度将从去年的第一名降至第十名，但是它仍是一个很重要的趋势，它将成为谷歌与Amazon的竞争领域。IT企业将考虑如何开发混合云以便改善安全和监管问题。

—来自互联网

Voice

左敬东

马克华菲信息管理部总监

马克华菲Mark Fairwhale，一个以“鲸鱼”命名、以原创为灵魂的服装企业，在中国的发展亦如其名般游弋稳健。自1999年创立以来，马克华菲门店已分布全国30多个省市自治区，门店数量超过700家。对于以“结合业务扩张的门店管理”为IT特点之一的零售连锁企业，马克华菲是不折不扣的典型。

促业务发展的优雅圆舞曲

笔者将全面解析马克华菲的IT建设及管理的重点和现状，另外你将看到左敬东在带领IT部门推动整个业务部门的发展过程中，又是如何从内部管理工作完美阐释“马克华菲”品牌含义的。

马克华菲，在其名字中就融入了飞翔、智慧、责任、和谐、青春、想象等美好寓意的中国本土企业，自成立以来一直以其优雅、时尚、简约的风格傲立于服装市场。一直喜欢关于马克华菲的一个介绍：一个以深海鲸鱼命名的时尚品牌，如同一个奇迹般的慢乐章，宁静而优雅的奏起了令人心荡神驰的中国圆舞曲。

记者走进马克华菲，采访其信息管理部总监左敬东，从他身上感受更多的是其对于整个IT团队独特的建设思路，以及在与业务部门的沟通、协作过程中的智慧。左敬东在接受记者采访时，指出马克华菲的IT团队不仅仅是关注技术，“我自己个人就会偏向参加更多业务层面的交流活动，以更了解企业业务的需求。”

不同的IT团队架构 不同的思路推动业务发展

在采访左敬东时，马克华菲的IT部门刚刚搬迁到新的办公楼。左敬东也告诉记者，其个人也是半年前刚加入马克华菲。“从马克华菲信息化建设的情况来看，从上服装行业的POS、分销软件，到上财务、OA以及电子商务，其还是比较典型的批零兼营的建设思路。”

据了解，马克华菲的核心是做品牌和渠道建设，公司的业务重点更多的是在直营、加盟以及电子商务层面。

左敬东结合企业的核心业务，对于自身IT团队建设的思路也有着自己的特点。“在IT团队架构上，我们分为零售部门、支持部门和服务部门，这区别了多数企业的应用、基础架构和服务这样的分类。”其中，零售部门集中体现了马克华菲的行业特色，支持部门的服务对象为公司所有后台部门，包括了财务、供应链、HR等，服务部门就主要体现在基础架构、安全及IT服务等。

在采访中，记者也了解到左敬东对于自己的团队成员的能力要求比较全面，特别强调资源整合能力。“对于应用开发人员来说，一要懂业务、二要懂将业务需求转化成IT语言、三要懂测试、四要懂立项。”左敬东总结到。基础架构和服务部分由于基本都采用了外包，自己人员只需具备基础知识，此外更为重要的是要有出色的项目管理能力，要会与业务部门打交道。左敬东对员工的要求也全面迎和了IT部门服务业务部门的需求。

目前马克华菲的IT团队只有10几个人，而面对业务部门的繁杂、实时的业务需求，马克华菲的IT部门选择将部门的IT服务进行外包。选择外包需要明确一些概念，尤其对于CIO而言更需要用足够的理由说服上级领导。“可能更多的CEO会认为自己做没有成本，但是事实是这其中也会存在机会成

本。员工成长需要投入资源培养。另外，一家企业的IT部门的服务水平和专业化水平也是有限的。”左敬东强调到，目前马克华菲也在考虑Helpdesk外包。

与此同时，左敬东也指出选择IT外包在前期需要做好充分的准备，才能真正达到外包的目的。选择适合本企业特色的外包商、选择适合外包的服务、做好外包管理工作，才能让外包发挥最大价值，随时、灵活地满足业务需求。

“除了IT组织里面所需要的能力外，其他都可以外包。如在马克华菲，基础架构的工作基本是外包的，自身的IT团队成员需要做的是管理工作，需要与外包服务供应商、业务部门进行沟通”同时左敬东也特别指出，与公司业务战略结合的工作是绝对不可以外包的。

无论是IT团队分类，还是选择性地进行IT外包，都离不开左敬东对于其所带领的IT部门的定位和自我要求：“成为最佳的客户导向团队；与业务充分融合；交付卓越的运营品质、信息服务和创新技术。”

灵活调整流程制度
轻松应对业务部门百变需求

任何国家、任何行业、任何企业的IT部门都无法避免来自业务部门的一些抱怨，IT部门与业务部门的关系也总是理不清、缕还乱。从乙方到甲方，从软件开发、咨询到信息管理部总监，左敬东对于如何处理与业务部门的关系、如何应对来自业务部门的抱怨，也有着更多自己的想法。

在接受采访时，左敬东指出IT首先要做到尽量地与业务进行融合。“CIO需要站在公司的层面考虑问题，需要考虑如何用IT手段去促进公司业务发展。”

虽然IT部门的特长在IT方面，但是其主要职能并不只是给业务部门提供工具，而是需要了解这个工具的意义。IT最终需要将技术与业务流程相结合，做成业务解决方案。

左敬东告诉记者，目前来说多数企业的IT还都是不断满足业务需求，还没完全做到引领业务的发展。这对于整个IT部门而言，在处于被动地位时，需要足够的技巧和智慧去与业务部门进行沟通。

任何一个CIO都有收到来自业务部门抱怨的经历，而如何面对这种抱怨、减少这种抱怨呢?

“业务部门有抱怨很正常，首先从心态上来说，IT部门需要放平心态。”左敬东还特别强调指出流程制度规范的重要性。“定SOP（标准运作流程），用流程制度来规范，可以实现更加标准化的管理。”

而同时，流程制度也需要符合双方部门的共同需求，“要制定双方都能接受的SOP。”左敬东还指出，流程制度也需要不断地变化，根据业务部门所提供的信息不断修正自己的服务重点，“可能今天的重点是加强客户满意度，过两天则是控制成本，那就需要降低服务水平了。”

从团队建设、员工培养，到选择性IT外包，从明确IT部门定位，到不断修正流程制度，左敬东向我们讲述了一名CIO在面对众多业务需求时该如何优雅应对，而马克华菲的品牌精神在IT部门与业务部门的整个协作过程中也表现的淋漓尽致。

Voice

陶龙

利丰贸易公司

经过100年及三代管理层的刻意经营，利丰集团已经演变成为国际性大型跨国商贸集团；中国大陆对利丰来说不仅是采购中心，而且还将成为一个有待发展的庞大消费市场。作为贸易型企业，多重供应链管理的深入性和灵活性，成为IT管理一大特点；如何结合这一业务特点，体现IT价值?

IT价值在技术之外

IT的价值在哪里？每个IT从业人员时不时都会问自己。“帮助企业提升工作效率，加速业务运转，让各个办公室和部门之间有效协作与沟通，并提升这一过程的效率。这些工作，能够让企业面对市场变化时，有快速的响应。”作为国际性大型跨国商贸集团利丰贸易的IT运营支持经理，陶龙如是给出了他的答案。

助业务快速反应方能体现IT价值

“很多人谈IT，往往都会谈节约成本，降低开支。”陶龙认为，IT帮助企业降低成本，是很重要的工作，但这并没有带来真正的价值。在利丰贸易，IT真正的价值，是帮助公司实现了快速的响应。

“很多时候，我们的客户并不是追求低成本，而是要求能够把握住市场的节奏和变化，快速推出市场需要的产品，帮助他们有效地认准趋势，甚至驾驭市场。”

陶龙口中的客户，并非利丰贸易的客户，而是公司内部的业务部门。

“成熟公司的一个标志是，IT是作为一种服务，其客户就是业务部门。”陶龙表示，他所在团队的愿景，是树立服务意识，然后努力提升IT服务质量。

利丰贸易，起源于1906年，由冯柏燎和李道明在广州创立，是当时中国第一家华资对外贸易出口商。现在则是全球知名的贸易公司，经营出口贸易、零售和经销批发三大核心业务。这家公司拥有出众的供应链管理能力，曾经入选过哈佛商学院案例。

利丰贸易在IT建设上最大的两部分是E-System和统一通信平台。

通过E-System这套系统，利丰实现了大部分业务的IT化。这家公司有自己核心的order system和ERP system，给供应商也会有一个叫做total shopping的一个vendor portal。针对大的客户，利丰则通过EDI实现双方ERP系统的对接，生产进度、安排货运、验货等双方之间进行的主要互动流程，都可以通过各自的系统看到。

和制造业不同的是，利丰是一家贸易公司。制造业通常主业比较稳定，一条生产线和一款产品的变化不会很大，生命周期也许长达10年，直到它终结。但利丰做的东西比较多，变化比较大，产品和业务模式变化也会比较多。在这个基础上，利丰贸易在ERP系统上还实现了很多创新。

统一通信平台则帮助利丰内部实现了快速沟通。利丰在中国有深圳和上海两个办公室，为了加强企业内部的有效沟通，利丰正力求建设一个统一、高效的通信平台。主要包括对原有邮件系统、PC/IP电话，还有视频等系统进行升级改造，并上线一个新的即时通讯系统和网络会议系统。

实现了上述的两大系统，对大部分公司而言，IT基础设施建设都已经完成。陶龙认为，这只是IT万里长征的第一步。公司的IT基础架构搭建成功，其实并未体现出IT的价值。

“我们跟业务部门工作的非常紧密，我们IT都会设一些与业务沟通的岗位，以便业务部门和IT这边非常紧密的沟通和协作。这些人现在是跟业务部门坐在一起的，这样是为了更深入的了解他们的业务，从而能够最大化的体现出IT的价值。”陶龙这样描述他是如何带领团队发掘IT的“价值”。

在利丰做IT的一个特色就是随时应变，根据业

务的需求，IT部门去做及时的反应。

“我们很多项目都是IT与业务携手形成的。”陶龙介绍到，IT会全程去做相关的项目，也会将项目内容提交给业务部门，去求证这些是不是业务部门真正想要的。

业务部门只要做一个新的business，IT一定会参与进来，因为现在的信息化程度很高，业务对IT依赖很深。

为了避免需求理解错误的情况，陶龙要求IT团队和业务团队交流时要walk stepping，这样大家能够有充分的交流和理解，将业务语言和IT语言之间的沟通鸿沟降低。

“这是一种常态的沟通机制。”陶龙强调，IT团队如果只是在项目来临时才和业务进行沟通，容易出现很多问题。往往IT谈论的业务不懂，业务的需求反馈IT也不理解。

如果不是常态沟通机制，大家相互之间不了解，都不清楚对方是做什么的，也不了解他们做的具体产品以及对应的区域市场和客户。

正因为如此，陶龙更加看重那些既懂IT又懂业务的通才。对利丰IT部的员工，陶龙会要求他们把大部分的精力放到业务中去，IT的知识和技能主要是靠供应商项目来做。

“我们大部分的项目都是由相应供应商来做，我们自己的IT人员更多是扮演了项目经理的角色。”陶龙的想法中，IT部门员工最后应该两条腿走路，一方面管理服务商，一方面不定期拜访业务部门了解需求，尽可能多的去了解业务的实际状况并给予定制化的服务。

“这样，我们就让IT部门与公司的业务目标能够保持高度一致。”但陶龙自己的体验，要想实现这个目标，IT部门还面临更多挑战。

利丰公司最大的特色就是“变”，特别是在中国市场，业务增长速度快并且常常会有很大改变。对IT而言，需要在服务上有一个很大的提升，比如说快速响应、快速解决，还要更有柔韧度。要和我们的客户要有充分的沟通，这样才可以去真真正正的把IT服务给到我们的客户，包括外部客户和内部客户。

如何做到快速？

为了更好地支持到业务部门，利丰加强了IT内部流程管理，这也是苹果的管理理念。将工作内容分解成一个个IT服务，针对这些服务制定KPI，对外部则通过SLA（服务水平协议）来确保IT部门的服务。

SLA都是事先和客户部门达成一致，以满足他们的需求，同时也便于IT部门自己监控服务的执行情况，真正确保服务能够帮助到客户部门，让他们体验到IT服务。

“这就有点像五星级酒店，无论客人入住那家酒店，都能够享受到非常优质、高效、标准的服务。”陶龙非常看重IT部门员工的服务意识。他有两个要求：第一，要customer focus （以客户为中心）。

第二，要尽最大的努力去提升客户的体验。

后者，是他规划未来三年致力提升的部分，即“experience our customer”。

“体验不单是你的harvest（结果），你的facility（灵活性），更重要的是你的人。”陶龙阐述到，“就好像我们去饭店去消费的时候，菜非常可口，环境、装修很好，但服务员态度很差，我们的感受就会有很大的折扣。”

陶龙回忆到，很久以前一次会议进行到一半时，有一些内容无法播放，需要IT部门的支持。但是支持的IT工程师到达时间太慢，而到了之后又一时找不到解决方案，就很武断的说这个需求无法实现。这些给客人的感受都不太好，客户对IT的满意度就会下降很多，本来事情不顺利，情绪上就很焦虑，而支持的IT工程师态度不好，则会大幅降低客户部门对IT部门的预期和评价。

所以利丰IT部门很注重服务的感受，会有大量的沟通和培训让IT部门员工提升服务意识，这样可以促进他们在技能知识上的积累。

“客户体验是一个整体感受，没办法量化。”谈到客户体验的方方面面，陶龙感触很深，“还是用吃饭的例子，也许我们去的是一家简朴的小店，但是服务员让客人感受到被重视和尊重，那么他就会觉得服务很好。”

陶龙认为，适合客户是最重要的，因为适合的才是最好的，所以在利丰任何业务部门活动都会有IT去支持和追踪。为了帮助部门员工能够快速累积经验，利丰还建立了问题库——将用户的需求收集起来，下一次再发生同样地问题，立刻就可知道怎么做了。这样IT部门可以在不断发现问题、解决问题的过程中，逐步形成新的服务和标准。

借力外包

将IT导向支持服务外，陶龙还选择了IT服务外包以帮助IT部门更好地完成各项工作。

“服务外包更具弹性和连续性，因为利丰的扩展比较大，可以通过借助外包供应商的力量，快速的增加所需求的各类人力或资源。无论是在高峰还是低谷都可以保证服务在比较稳定的水平。”陶龙介绍，利丰将服务台和桌面支持的项目外包给了专业IT运营管理服务商金道公司。

IT通常会有一些日常的基础服务，例如电脑操作系统和Office办公软件的维护。这些事务性的服务都是通用的，几乎每家公司都在用，并且和业务的关系并不是很紧密。

同时，由于采用金道管理服务（Managed Service）外包模式，还可以让陶龙减少人员管理的精力。他只需要和外包服务供应商达成一个共识，制定一些SLA，然后确保服务的质量。那么外包团队的内部管理基本上不用参与，这样可以从原本很多人力资源管理，内部的工作分配，人员备份等等琐碎且事务型的工作中解放出来。

选择将这些事务外包，能够让利丰的IT将更多的精力放在和IT部门客户的沟通工作上，去做一些跟业务结合更紧密的工作。同时可以避免IT团队过大而增加的管理难度。

“以前我们的一个IT工程师可以支持100台桌面终端需求，引入外包项目经理后，通过管理优化，可以提升至150台。但是人员并没有增加，这样可以产生一个额外的红利，而这个红利则可以由我们和服务商双方去共享。”陶龙还道出了使用金道管理服务（Managed Service）外包的另外一个好处。

用好外包商有学问

用好外包商，在陶龙看来也是一门学问。并非随便找到一家外包商都可以有同样不错的效果。

“外包是一把双刃剑，用得好帮助很大，用得不好则负面问题很多，就像被别人卡住了脖子一样。”对外包，陶龙感触颇多。“如果外包没有真正帮助你，你甚至会觉得做事情非常的麻烦。”

想要用好外包，陶龙首先看的是外包供应商对利丰IT团队的重视程度。

“这其实也是一种态度。”陶龙非常重视客户感受。外包团队虽然承担的是事务性的IT工作，但是往往是要直接和内外客户打交道，因此服务态度同样重要。

外包并非代表完全放手不管，需要每个月去审核、沟通服务绩效。并且还需要有一个项目经理来管理外包团队，灌输利丰的服务理念，将其传达至外包供应商，形成双方的共识，最终完成客户服务

支持。

这个项目经理，是代表利丰IT部门来管理外包团队。主要承担常规人员的管理工作，例如考勤、绩效，同事还要涉及外包团队和利丰IT部门之间的沟通协调，积极地参与用户的沟通，了解用户对服务台、现场工程师的满意程度。

通过收集用户对外包团队技能、态度的反馈，和利丰的IT部门形成有效、良性的沟通。

“通过这样一个沟通机制，外包团队用好了，甚至就像自己的团队一样。”这是陶龙心目中外包团队的理想状态。

要想达到这个状态，则一定要建机制和外包团队充分沟通，并加强IT内部沟通。外包团队主要职责是IT设备更新维护和简单应用支持，但是同样需要了解利丰公司整体的大方向。否则在很多问题上，无法看的更全面。

“例如我们要向用户交付一个服务或者去提升外包团队理念，如果他对利丰公司整体的背景不了解，就会有瓶颈。”陶龙分享他使用外包团队的经验，对公司大背景有了解，外包团队才知道为什么需要这样做，认同了公司的方向，他内心潜意识才会真正形成伙伴意识，尽自己最大的努力去完成各种任务，而不会随便说“这个我们做不了”。

“这样才是外包团队和IT部门真正形成共识。”陶龙的理念中，双方达成共识，是长期合作的基础。陶龙还希望外包团队满足利丰的理念，针对利丰涉及的不同行业特性制定相应策略。因为利丰不同业务之间差异很大，只有快速响应、快速解决、快速支持才能满足业务需求，否则就会出现各种问题。

在共识下面，即便真正出现一些问题暂时无法解决，也会有一个服务框架在。陶龙举例，在为业务部门客户提供服务时候，IT人员即便知道真的无法实现，也不能一下子去拒绝。他可以说“我也许无法完成，但是我先来帮你看一下。”，或者“我帮你问一下，是否有其他方式去实现。”。

他可以将遇到各种问题，反馈给项目经理、然后通过项目经理和IT部沟通，那么用户的体验就会好很多。

“我们在酒店里时常会遇到问题，服务员无法解决。但是如果这时候他态度非常友好地表示，愿意帮你向大堂经理进行反馈，看看是否可以解决。随后派出你专属的客户经理和你沟通，有可能最后问题还是没有办法解决。但是用户觉得我是上帝，我的需求得到了重视。”陶龙笑言，在利丰IT部门和外包团队，首先需要的就是服务的意识。

陶龙希望不断推进IT服务的标准化，将很多服务做深做细，然后提升整个IT团队的服务意识，这样每个工程师和项目经理在执行项目时才会有内容去参考和执行。

“这是一个长期的过程。”陶龙觉得，当利丰IT部门的服务到了一个高标准后，IT部门的价值会自然得到最好的呈现。

细小处见真功夫

■ 金道服务经理 王晓隆

如何衡量“无形”服务的“有形”价值？而对于纯粹卖IT服务的金道来说，服务人员是如何在日常工作中实践这看不见摸不着的服务精髓的呢？就让我们走进一线，来看看“三头六臂”的金道客户服务经理们是如何各显神通的。

IT服务中如何实现较高客户满意度？

“态度、技巧，以及良好的团队管理是必要条件。”金道客户服务经理王晓隆给出他的总结。“IT服务中的客户满意度，同其他服务一样属于感性度量，但总结来说，也有道可循：首先是服务质量，它包括响应时间、解决时间等指标，这是客户满意度的基本要件；其次，也是最重要的是服务态度和技巧，就像前段风靡的海底捞火锅，能将服务做到众口称赞，就在于他们强调用心服务来提高客户体验。”

用心服务，运维无小事

IT运维服务工程师平常的工作大多是繁琐而细小的，在王晓隆看来，如果没有一个良好工作态度，效果就会大打折扣。“机会是给有准备的人，小事情也是机会，付出一定有回报”这是王晓隆坚守的信念。

一次，客户一业务部门需要大面积更换工位，要求IT工程师们在下班之后完成25台PC的迁移工作，这种加班对于王晓隆所在的团队来说已经是司空见惯，工程师们的思想工作不用费太多精力，但所涉及的细节就不容忽视了——在迁移之前，他们需要将所有25台PC的资产信息整理出来，迁移时则要求工程师们帮用户换好座位后尽可能恢复原样，帮用户把网线电源线等整理好。总之，用晓隆的话来说就是要“神不知鬼不觉”中完成“乾坤大挪移”。而完成迁移之后，还要将更改的IP整理出来，将资产变动更新到CMDB中。听上去一次容易的“挪移”，实际执行起来并不简单，从迁移之前的数据导出到迁移之后的数据更新，都不能出丝毫差错，这就对工程师的耐心和细心都提出了不小要求。

“其实这些都是举手之劳的小事，但就是这些人性化的举动，可以最大限度的提高我们的用户体验。搬家是所有运维工作中最复杂最繁琐的工作，搬家就是由很多件小事组合起来的项目，如果中间的小事都不能做好，那整个项目肯定会失败，而让我们持续做好这些小事的动力就是付出肯定有回报。”王晓隆说。

换位思考，化解矛盾误会

除了良好的工作态度，服务技巧同样不可或缺。在现场服务过程中，工程师难免会与客户发生误会和矛盾。对此，王晓隆的心得是“将心比心，换位思考”，他

王晓隆来自于金道一个20人的客户IT服务团队，常年在客户现场负责客户公司整个IT基础架构的运维，包括网络、桌面、语音、应用系统支持等。

常常要求工程师在遇到问题时首先学会体谅用户心情，尽量满足用户要求，而对于超出规定或能力范围外的，则要事先明确提出，争取获得谅解和支持。“实际证明，积极的双向沟通确实是解决问题的不二法宝”。

奇妙关联：“团队内部建设”与“用户满意度”

“还有两天才到周五啊！”在驻现场工程师的工位上偶尔会听到这样的叹息。但别误会，对大多数金道驻现场工程师来说，这不是在期待欢乐的周末，而是期待周五下午王晓隆组织的例会。

“我们就喜欢参加这样的例会。除了工作总结之外，王经理每次都会组织对我们进行工作技巧培训，工作心得分享，有时候还会向我们讲述金道又发生了哪些大事。”刚进入这个项目组半年的工程师小李直言不讳地说：“我们驻现场工程师，除了当初应聘和入职的时候，基本上没有机会回到金道公司总部，对公司感觉多少还是陌生的。王经理就是用这样的方式，让我们感觉到我们和公司是在一起成长。”

“‘客户满意度’和‘金道团队内部建设’乍一看没关联，事实上却舟水相承。”晓隆表示。对于外包团队来讲，培训好、建设好至关重要；如果缺乏培训和建设沟通，成员极易出现缺乏公司认同感（同时表现在服务企业认同感和公司自身认同感），从而带来“高人员流失/变更=影响服务质量可能”的后果。“团队培训与建设已经变成考验IT外包企业的重要标准”，晓隆表示，“打造一支用心服务、长期服务/低流失率的团队，已经成为客户认可团队的重要原因之一。”

—金道《CIO EXPRESS》专稿

真知出自实践，卓越源于用心

■ 金道服务经理 刘平

在50人的服务团队里，月度考核3次排名前3，半年内3次获评优秀现场主管。即使在人才济济的金道服务团队，这样的成绩也不多见，这就是今天故事的主角——服务经理刘平。

提到刘平和他的团队，最不得不提的就是“客户满意度”。IT外包中SLA达标，但用户体验却差强人意的情况并不少见，如何能在SLA达标的同时，给用户带来数字之外的优质体验？关键在于“找到平衡点”，“按轻重缓急处理”，刘平给出他的两条服务心得。

客户满意度，平衡的艺术

“这95%的资产准确率太低，你们想办法给提到100%吧”——客户IT负责人如此说。

“我这邮件怎么总发不出去？我着急给客户发个报价呢，请赶紧帮我恢复”——客户最终用户如是说。

作为专业提供IT支持的金道服务人员，满足客户需求是天然使命，但是当现有资源与客户期望产生冲突时，该如何应对？对此，刘平在实践中摸索出来了独特的客户满意度公式：客户满意度=客户期望值--实际所得结果，在实际工作中，他也是据此来指导和要求工程师的。

首先，是尽一切努力改进服务结果。这里刘平列举了多项举措，包括：

用过硬技术和专业态度建立客户信任，这是服务的基本和前提。

按照SLA，提高请求响应速度，这是服务技巧。

在原则基础上适当注意人性化关怀，如遇果真火烧眉毛之事，在不影响大局的前提下，可加以优先考虑。这是灵活变通，急客户所急。

每周例会工程师们交流经验心得，由主管和经理加以指导、纠正。

刘平甚至对工程师自己的工位干净整洁程度也有要求，“试想如果你是用户，找到工程师发现其工位乱糟糟一团，你会信任他能帮你解决好问题吗？”

其次，与客户事先达成合理的期望值。“做好了以上几点，如果还不能令客户满意的话，那说明有可能是客户期望值过高。”刘平说。作为在运维领域比客户还要专业的金道服务人员，此时会提前向客户进行分析和建议。比如，一个地域分布广泛的大型集团公司，做资产清查统计耗时长，如果客户希望在现有资源条件下（人力财力等）提高准确率，那么金道工程师就会告诉客户，每提高一个百分点，所要额外增加的资源是多少，客户在经过权衡之后，也会定出自己合适的期望值。

“前期获得理解，执行中努力超越，在客户期望与服务结果间取得最佳平衡点，始终保持较高客户满意度，我想这就是我们能连续几年都收获金道优秀服务团队称号的重要原因”刘平自豪地表示。

分清轻重缓急，提高服务效率

运维支持工作，各种状况都可能碰到，每天面对纷至沓来的大小事件如果没有良好的统筹安排和管理，工程师们就会像无头的苍蝇，越忙越乱，处理不好就可能带来用户满意度的下滑甚至SLA不达标。“在我们团队，对各种事件是依据重要紧急程度来区别对待的，并且我们对每一个关键节点都设定有时间点和检查点，此外，如遇不能解决的问题，则会及时升级上报。”刘平说，运用时间管理的理论，能轻松把精力从繁琐中分解出来。

具体来说，就是将同一时间段内的事情分别放入四个象限：重要且紧急、重要但不紧急、不重要但紧急、不重要也不紧急。比如，日常数据备份与机房服务器宕机相比，显然后者更紧急，而普通员工和VIP遇到同一事件其重要性也不一样。

未雨绸缪，事先预防矛盾

“昨天我申请买的新笔记本怎么还没到？你们效率也太低了！”最终用户有时会对IT支持人员有此抱怨，类似投诉服务工程师们在日常工作中没少遇到。

在刘平所服务的这家客户公司里，硬件由IT统一购买，用户如有需要可填表申请，IT接到需求后开始订购，但一般来讲用户不清楚具体到货时间，超过预期用户就会怪工程师效率不高。为了解决这一问题，刘平带领团队事先确定了双向沟通流程，告诉用户整个过程大概需要多长时间，每一步做什么，并且制作了详细的流程图，定义每个环节的关键时间点和责任人，涉及工程师、供应商等相关人。并且还会定期进行总结，分享经验。这样双方就能对进程一目了然，如有问题，能做到及时发现及时处理。

事先建立明确流程和风险意识，不仅能对可能结果进行预估，还可事先想好解决方法，通过这种方式，刘平的团队成功减少了多种潜在矛盾，也赢得了客户的充分信任。

—金道《CIO EXPRESS》专稿

金道服务经理刘平

《故道白云》

作者：一行禅师

如果你成功了，你是否会为下一个目标的意义而迷惑？
如果你还在沉浮，你是否会停下脚步凝视自我？
而立之年的你应该读的书

年少时，常常看到、常常期待的是，在合适的时间遇到合适的人或机遇，成就一生；而立之后，褪去了少年的浮华与娇嗓，读书的指向性更明确，也大致形成了自己的阅读风格。于是，在合适的时间遇到一本合适的书，也如年少时在合适的时间遇到合适的人一样，是人生的另一种大幸福。《故道白云》就是在合适的时间遇到的一本合适的书。

起初只是在当当毫无目标的搜书，直到《故道白云》进入视线。看到书名就已心动了，买入，等待有时间的时候细看。买书常常是这样，买的时候很急切，买来之后却又静置柜中许久忘记翻看。

《故道白云》也象很多书一样，买来之后在办公室的柜子里静静的等了一年多，才因为前一阵的病休，终于细细读完。回忆从求学到工作这许多年的阅读经历，除了金庸的武侠，还没有哪本书让我这样牵心挂肚的想一气读完，不为别的，只为它能解我心中的惑。虽然年龄愈来愈大，但心中的迷惑、纠缠一刻也不曾少，只是跳脱出最初的小我，进入大我的范畴。常常为无可追回的过往懊悔，也常常为不可测的未来忧惧，更常常费力的去思索无解的生命谜题。一切的执著与思索都在读过《故道白云》后豁然开朗。往者不可追，来者不可控，重要的是活在当下，把握当下。佛陀与摩诃迦叶拈花微笑的心意相通，一粒沙里看世界的大美无言。生命无常，而生活无时无刻不有大美存在。我们唯一能做的，只是把握、珍惜当下、眼前。

金道概述：

金道专注于为中国本土及海外客户提供以管理服务为核心的IT运营外包服务。公司总部位于北京，并在上海、广州、深圳和成都设有分支机构。

十多年来，通过结合我们在50多家世界500强企业客户中的IT外包服务实践，和自身国际化团队的IT运营及管理经验，金道不断完善以ITIL为基础的服务方法和流程，及多种自动化、可视化服务管理工具。目前，金道可以为客户提供100个坐席，7×24小时、多语种的可视化IT服务台，服务网络覆盖大陆、香港、台湾共200座城市，专业服务团队超过600人。我们承诺以富有竞争力的价格为客户提供世界级品质的IT外包服务，并致力于与客户共同建立持续发展的长期商业伙伴关系。

金道服务：

通过以质量控制和效率提升为核心任务的 IT服务台，以及200个城市的服务网络，我们为客户提供涵盖桌面端、移动终端、服务器、网络及应用等IT环境的运营和管理服务。

金道客户：

高品质的服务和专业化的管理，使金道成为众多客户信赖的外包伙伴。我们的110多家客户遍布制造、物流、零售、银行、保险、医药、化工等多个行业，其中50多家为世界500强企业。

北京总公司
地址：北京市海淀区中关村东路66号甲1号世纪科贸大厦A座6层
电话：（010）58737222

上海分公司
地址：上海市广中西路777弄88号华清大厦8层
电话：（021）60899800

网址：www.gamutsoft.com
热线：800 820 0017
Email：marketing@gamutsoft.com