第一章　何谓信息安全

重点信息　保障资料安全就是让计算机确保你个人或公司的秘密不被泄漏或盗取，完整的资料不被篡改或遗失，让你有需要时可作存取，并为每次交易提供记录。

在我们的日常生活中，大多数人都知道使用门锁、防盗网及狼狗等工具来提高家庭或办公室的安全性，其实计算机系统也同样需要相应的防范措施来提高计算机系统的安全性。不过要将现实世界可以做得到的事情转移到计算机上，就必须先弄清技术名词的定义及业务本身的需求。如果你从来没有接触过信息安全，则你很快就会知道除了防止众所周知的“黑客”外，要令你的计算机系统达到“安全”，其实还有很多事情要做。

信息安全的种类

信息安全确实存在而且刻不容缓。那么，在解决信息安全问题之前，先让我们来弄清楚我们的计算机究竟潜藏着哪些安全问题吧。

病毒

病毒与计算机相伴而生，而互联网更是病毒滋生的温床。从早期的“小球”到引起全球恐慌的“梅丽莎”，病毒时刻是最直接的安全威胁。

内部威胁及无意破坏

事实上，大多数威胁来自内部，来自同事、被解雇的职员、受信任的顾客、咨询顾问等所有能进入系统的人 此外，一些无意的行为，如丢失口令、疏忽大意、非法操作等都可以对网络造成极大的破坏。据统计，此类问题要占网络安全问题总数的 70%左右。

系统的漏洞和“后门”

操作系统和网络软件不可能是百分之百无缺陷和无漏洞的，然而，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。另外，软件的“后门”都是软件公司的设计编程人员为了自便而设置的，一般不为外人所知，但一旦“后门”洞开，其造成的后果将不堪设想例如，微软公司的 Windows 产品就存在此类的严重问题。

网络上的蓄意破坏

好比说在未经他人许可的情形下窜改他人网页，作案动机多半是因为政治原因或仅仅为了炫耀自己的技术。在 2002 年和 2003 年，美国发生许多类似案件，一些著名的官方、新闻及商务网站皆遭到不明黑客的入侵破坏。 2002 年，我国一些站点也遭到来自国外的此类恶意攻击

侵犯隐私或者机密资料

很多人有这样的经验，当你从事网络购物或是信息的搜寻时，对方往往会要求你的信用卡资料作为注册的必要条件之一，并添加一大段文字确保此类个人资料的安全性。事实上，黑客并不需使用多么先进的技术便可获得此类资料通常只要用偷窥信息的封装（data packet）程序，即可得知使用者的注册名称及密码，然后间接使用这些数据输入上网，调出所谓的使用者资料（personal profile）

拒绝服务

当组织或机构因为有意或无意的外界因素导致无法完成应有的网络服务项目（例如电子邮件系统或是联机功能），即称为“拒绝服务”（Denial of service）问题。最近，YAHOO、HOTMAIL、CNN 等站点就受到此类攻击。虽然此类破坏并未直接威胁到信息的安全，然而公司本身却往往需要耗费大量的时间和精力来弥补错误。

信息安全的四个目标

重点信息　信息安全有四个目标，就是保密性、完整性、可靠使用性及不可否定性。

信息安全有四个目标：保密性、完整性、可靠使用性及不可否定性。需要特别指出的是，前三个目标对于负责信息科技的部门来说就如吃“糖果”一样，吃太多的“糖果”会令你生病，也可能令你超重。所以太严密的计算机安全水平对业务亦有负面的影响。此书能帮助你了解到信息安全应达到何等水平才适合你的业务。

保密性、完整性及可靠使用性是不可分割的，其定义及解决办法亦类似。但这不是重点所在，最重要的是，我们采取目标为本的方法：计算机应在我们需要的时候做我们需要它做的事—— 因为我们才是它的主人。当然，它不应为用户以外的人做任何事。

图 1-1　信息安全的四个目标

保密性

信息安全的第一个目标就是保密性——让信息远离不应获取资料的人。要达到此目标，我们就必须先要清楚分辨什么资料需要保护，及什么人有权存取该等资料。而且必须定义资料储存于计算机中，及于不同网络传送时的保护机制。我们亦必须知道用什么应用程序操控数据及如何控制该等程序。通常这都是计算机安全总监及信息科技部门的工作，只要我们表明什么人士应有何等程度的存取资料及应用程序的自由，有关部门就会负责执行。

“保密性”的定义已扩展至与隐私保护有关。对于某些行业，例如医疗及金融服务，隐私保护已成为法律上的问题。美洲、欧洲、澳洲的许多国家都已对隐私保护成立了不同程度的法律，某些在其他地区拥有客户或雇有员工的美国公司都已受该等地区的隐私保护法律所监管。公众对私人资料保密的需求亦迫使公司制定清晰的隐私保护政策。

完整性

信息安全的第二个目标乃“完整性”，即确保计算机内的资料不会受不良影响或被不合适的方式改变。保密性及可靠使用性均有助于资料的完整性。让信息远离无资格获取资料的人、确保有资格存取资料的人可顺利获得资料，乃确保资料完整性的最基本方法完整性的机制可确保储存于电脑的资料不会受影响，或以不合适的方式改变

不过，严格规定不同人士的存取权并不能百分之百保证资料的安全性。有时候我们信赖的人其实并不可信，有时我们迫不得已将电脑系统进入权及重要资料披露予我们所知甚少的人，如临时员工、业务伙伴、顾问等。因此有关完整性的限制并不能只限于人的身份，而应将存取权的程度亦考虑在内。如某人拥有存取权，则他或她可在其计算机中进行什么操作？所以用户必须在计算机系统内详细界定不同程序的存取权有什么限制，因而令现代的商业计算机系统变得复杂假如所有用户均可改变系统或网络的行为的话，则公司内的任何人均可令业务停顿——无论是有意或无意。

对资料完整性的需求使计算机安全与业务延续计划及数据恢复机制联系在一起数据会因软硬件失效、人为错误或安全上的问题而受损或摧毁，因此数据恢复机制在任何信息科技的计划中都是不可或缺，而必须由有关部门严格监

控的

可靠使用性

信息安全的第三个目标乃可靠使用性，亦即确保储存于计算机内的资料可由有存取权的人士在重要的时候可及时存取资料。可靠使用性涉及的范围广阔，包括错误容许的弹性，以确保有存取权的人士不会因不小心造成的错误而未能存取资料，大多数的计算机都可分为两个类别的使用者：系统管理员及一般使用者。惟一的例外是桌面上的操作系统。

只要翻开信息科技类书籍，你就会发觉大部分都会认为微软窗口 95/98 所有的版本都是不安全的。原因之一是，作为一个操作系统，它没有分别系统管理员及一般使用者的权限。事实上，大多数的桌面操作系统均有此弊端。任何使用计算机的人都能改变其安全环境，甚至将安全设置关掉，虽然某些使用者一可开启网络及觉察安全环境的改变当然，即使安全环境正常，亦不代表一定安全，因该等操作系统均有其他安全上的弱点。

资料存取的授权不应只按照系统管理员及一般使用者来分类。在一个安全的计算机系统里，使用者一般都由人事部按其职位描述而获指派某些公司内的角色，而计算机则按照角色的分配而决定该使用者的存取权。此方式能限制每一个使用者对计算机的控制程度，包括系统管理员在内，因此获普遍采用，以避免系统管理员权力过大而随便改变安全环境，甚至获得比雇主更大的、不合理的控制权

在互联网的世界里，“ 可靠使用性 ”的意义已不断扩张。在互联网应用程序上，“ 拒绝服务 ”的袭击是最大的安全问题网上的攻击者有两种方法可以蓄意令计算机系统及数据不能使用：一是损毁目标计算机或其网络部件；二是向目标计算机传送大量信息，令其不能处理所有信息，从而令合法的使用者因计算机过于繁忙而无法使用。

单单要达到保密性、完整性及可靠使用性，已令计算机安全成为一个大课题因商业上的需求，用于达到此等目标的相关科技同时亦应使用在第四个目标——“ 不可否定性 ”的实现上；有关技术能透过计算机生成有法律约束力的合约而无需使用任何纸张及签名，安全性相关科技的使用及对以安全、可靠的工具制造电子签名的需求，令“ 不可否定性 ”成为计算机安全方面的另一新目标。

不可否定性

“不可否定性”有众多重要的目标，包括确保传送的信息不会在途中被更改此等机制的其中一个正面作用乃令传送信息的人不能否认该信息乃由其发出，而此点对商业活动来说极为重要。

举个例子：在“企业对顾客”（Business to Customer）的交易中，顾客在发出订单后可能改变主意而声称并无发出该信息，或所订购的并非该货品，试图否认该订单。“不可否定性”的机制就能禁止此情况，确保顾客的忠诚度，及保护有关公司的利益。

另一个“不可否定性”对之非常重要的行业就是网上拍卖。各类型不同忠诚度、不同目的的客人均可透过网上拍卖进行交易，因此确保用户忠诚度的机制是不可或缺的。

信息安全的责任

大多数的企业、政府或非牟利机构都成立有其信息科技部门，大型企业甚至有员工或部门专门负责信息安全方面的事宜。近来不少公司均增设信息安全总监（Chief Security Officer，简称 CSO）一职，而 CSO 大致可分两种：一种是全权负责及处理计算机信息安全的问题。虽然公司自聘专业人士负责可减轻管理层不少的负担，但由与业务无直接关系的信息科技人员作出影响全公司的信息科技政策或决定，亦产生一定的问题；另一种 CSO 则是清楚用户需求并能给予不同权限的定义。这些定义与公司业务及其员工息息相关，而此种 CSO 可挑战对计算机或信息安全缺乏认识的人，但亦同时是能为公司想出解决办法的人。

概括起来，信息安全的责任，主要有：①明确企业的哪些关键数据和资产需要保护，并根据其价值设置相应的安全级别；②对企业关键数据和资产进行威胁识别和风险评估，确定企业在具体环境下到底存在哪些安全漏洞和安全隐患；③在前面工作的基础上，制定并实施安全策略，完成安全策略的责任分配，设立安全标准。

只有政府国防部或非常小型的公司才能由一个中央的机构或人士去制定资料安全政策，而无需咨询管理层。在现时架构复杂的公司或机构里，如 CSO 尝试强制执行有关政策或律例，结果必然是失败 CSO 的其他信息科技同事很

可能反抗有关规定，而中层管理人员及其他同事则可能不主动配合

信息安全人员的目的只是改善公司资料的保密性、完整性及可靠使用性，理应与所有同事及部门提供互惠互利的方案信息科技人员与其他同事的紧密及和谐的合作对公司的成功至关重要。

信息安全的相关性

信息安全系统并非因能配合公司需要或因公司花了大量的时间和金钱而一定产生效用；相反，基于种种原因，安全系统实际上可能并无产生实际效用。因为作出决定要投资在系统安全上后，随之而来的问题就是究竟多少安全措施才是足够？太严密的措施只会影响业务，因此公司的安全系统应是对业务需求及安全水平的平衡点。

有时我们甚至忘记了公司需要有安全措施但安全措施对公司盈利有好有坏，在于你怎样控制。要减低风险自然需要一定的成本，而多数的情况都是最后两成的风险要用八成的金钱去消除。因此，一旦公司已达到基本安全需求，平衡减低风险的成本及安全措施失效时所带来的潜在损失就变得异常重要。很多公司都在其预算中加入安全措施成本一项，但如成本超出预算，则应分析个别情况而决定是否投入资金。

信息安全执行上的困难

一般公司的资料存取守则均规定员工在获得存取权前必须通过背景资料调查（如是否有案底或不良雇用纪录等）。但如公司因业务需要而聘请短期员工，则此守则就产生执行上的困难，背景调查所需的时间可能比雇用期更长。同样，如公司守则规定由专责部门统一于系统内加入新用户，亦会出现类似问题

对某些公司来说，在中央系统纪录中为新的员工开户，所需时间可能比其雇用期更长因此，一些管理层宁愿订立省略此手续的机制，试图简化程序；但这种另立例外机制而非重新检讨原有守则的做法正损害了资料的安全性最典型的做法是设立数个无须辨识的用户户口，可以按需要自由指派使用者。此举令不应拥有存取权的人拥有户口，而公司亦难以监察或控制其资料存取，令资料安全严重失效

信息安全水平的平衡点

重点信息 80% 的利益可由 20% 的信息安全成本所获得。

企业需要保护的信息到底值得企业投入多少？想必此一问题是大多数企业决策者所关心的。安全水平太低会增加对业务的危机，但过高的水平亦会对业务带来负面的影响。因此管理层及专职计算机安全的人需在数据保护及对业务的影响两者中寻找一个平衡点。图 1－2 显示信息安全的成本及所带来利益的相互关系。在多数情况下，80% 的利益可由 20%的成本所获得，但余下 20% 的利益则成本高昂。世上是没有绝对的计算机安全的。一般良好程度的安全水平成本不高，但要达到更高水平则须支付昂贵的代价

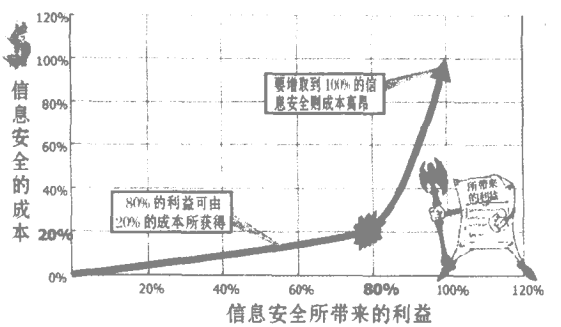

图 1－2 信息安全的成本及所带来利益的相互关系

如何组织信息安全

要确保信息安全，须使用到多种技巧及知识；通常公司都会就所有的技巧及知识而安排工作，但可惜在信息安全上，一般公司都只注重科技其实信息安全与业务密不可分，因此应从业务的角度而非科技的角度去处理。

小型公司一般都不会聘请额外员工负责计算机安全，而是依赖具备有关知识的员工兼任。在大型企业则需了解计算机安全方面有哪几种角色，或可安排需要相近知识的多个角色予一个专职员工担任

计算机安全有一最基本的原则，就是权力分立——即制定守则与执行的人必须分开。如所有权力集中在一个人或机构手上，就做不到权力分立。就算将

权力放在整个信息管理部门又过于集中某些角色可轻易从信息科技分开，例如内部核数师及资源拥有者

在信息科技方面，最重要的是将制定信息安全制度（即主任及经理）的角色与执行有关机制的角色，即网络及系统工作人员分开。计算机安全操控员及法律分析员则是近年新增设的职位由于监控守则合规的工具已趋成熟，因此这些角色已发展为透过安全控制台去操控有关工具，分析工具所提供的资料，并确保系统受袭时能成功修复。

要在公司架构中安排计算机安全方面的位置，一般视乎其行业是否有政府监管而出现两种情况须遵守政府计算机安全规定的行业如医疗、金融服务行业，省级及中央政府机关等，均须将计算机安全与其信息科技作同等对待。一般而言，安全总监（CSO）须向有法律方面知识的合规主任汇报。而其他政府和并无规范的行业，CSO（有时亦称 CISO，即信息安全总监）则须向集团的信息总监（CIO）汇报，与信息科技的主管（CTO）同级。

某些不注重计算机安全的公司不会聘请 CSO 或 CISO，只由信息科技部门的同事兼任此种做法在上市公司已越来越少见，因外部的核数师及负责信息科技基建的政府机构不断向其施加压力。

小型公司并不会开设“主任”级的中层职位。这种情况就更加需要将守则制定及执行的角色分开。虽然其信息科技部门——无论规模有多小——仍可负责计算机设备的配置、安装及维修等，但守则的制定则绝对需要从执行的部门分开。

信息安全上的遗漏

重点信息 大部分与信息安全有关的损失均由内部人员蓄意或不小心造成。

很多公司因没有计算出由于信息安全失效而导致损失的实际数据，公司一定会认为他们的计算机已经够安全而事实上要令计算机完全安全则非常烦琐。即使已将计算机的安全措施做妥，仍然会发现有所遗漏。这里有一个很好的例子：有公司在做了一个安全素描后甚至发现其电邮乃经其竞争对手的服务器传送的，竞争对手可获得所有其公司的商业计划、库存报告、新的订单等资料，亦无从知悉此情况由何时开始、由谁造成。

信息安全并不应只侦测外来的黑客。大部分与信息安全有关的损失均由内部人员蓄意或不小心造成。当我们在讨论如何确保计算机资料的保密性、完整

性及可靠使用性的时候，并非单指外部的人。不论任何身份，只要他对资料作出错误的改动，都得及时制止：纵使我们不能利用科技去迫使所有人都输入正确的数字，但至少可以令所有人都是以完全合法及假设已受适当训练的方法输入数字。

一些公司只顾避免外来人士对计算机的袭击，这是策略上的重大错误。严重的计算机袭击通常都是由一些假装为雇员的外部人士作出的。外部人士可以盗取或猜测公司雇员的用户名称及密码，然后轻易假装为公司员工的一员。所以，所谓的计算机安全必须要对所有活动均有所监控，不论是外部的人士还是最信任的员工。

必须谨记的是所谓的安全是相对的，在计算机安全中是并无“绝对安全”的所以问题是：“我们要有多安全？”最普遍的答案是：“要与其他公司一样安全或更安全一点。”这表示要令自己的计算机达到“安全”，就必须先要了解竞争对手的系统有多安全。

很多公司将计算机安全当作不重要的一种姿态而懒得去讨论研究，让不太专业的第三者去评估自己公司的安全水平是否足够。这些第三者通常都是电脑或软件公司，他们的工作主要是通过卖他们的产品来赚取利润。因此有时这些公司并不能为客户的计算机提供足够的保护或太多的保护。因此，正确的做法是如同一些大型的公司所做的那样，他们雇用独立的第三方去找出合适公司的安全水平，或技术分析，公司如 META Group、Burton Group 、中国博扬企业管理顾问公司（www.byemcc.com）等。

业务部门经理的责任

业务部门经理在计算机安全中的角色举足轻重。如果你是该经理的话，那么你就是资源拥有人。信息科技的同事不会明白储存于计算机中的资料对公司业务有多重要，因他们不了解业务运作。因此，只有了解业务的人才能判断各项资料的重要性负责计算机安全的人（如 CSO）及负责信息科技的人可向业务经理提供意见及指引，但不能替公司作最后决定。安全程度要多高才足够？这完全视乎资料的价值及风险——而这些都是你才能决定的。

决定安全方面投资的过程称之为风险评估。在大型的公司里， CSO 就会请你做这方面的决定。如公司属中小型，则你得自行解决。毫无疑问，评估信息资产的价值与风险乃 21 世纪的重要管理技巧。

信息安全要订立目标及行动

重点信息　信息安全并不是一厢情愿的空想，或单靠技术人员就可以达到。

信息安全并不是一厢情愿的空想，或单靠技术人员就可以达到。安全是一个相对性的概念，因此只能订立目标，然后评估是否能达到。而这些目标亦等于计算机安全守则。正式来说，守则应是由行政人员签署的通知，向所有员工提出清晰而具弹性的指引，定出技术、操作上的标准及步骤。

计算机安全执行技术

计算机安全执行技术是以防火墙及辨认与鉴定技术来保护业务资产，图1－3是形容如何执行安全措施、保护资料、防止不合法存取的方法。达至信息安全所使用的技术一般于计算机的基础建设内进行，然后扩展至网络、服务器及桌上型计算机等。

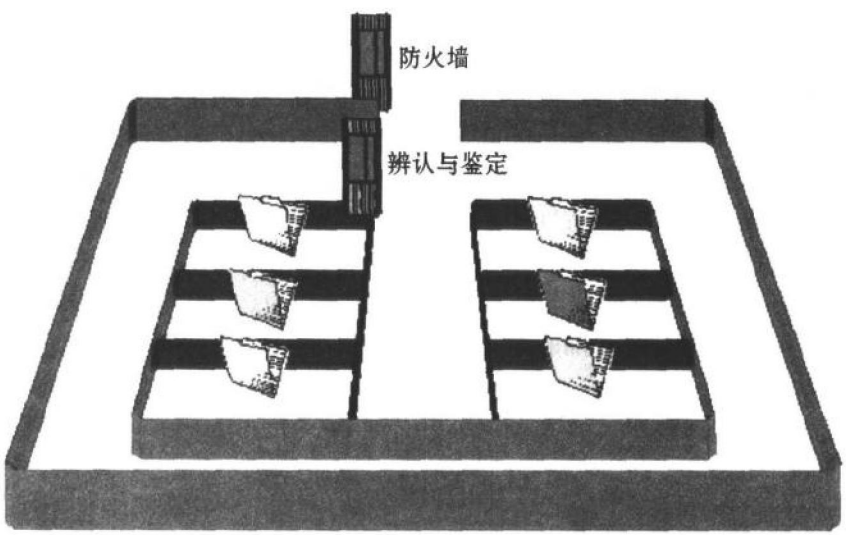

图1－3　计算机安全执行技术是以防火墙及辨识与鉴定技术来保护业务资产

存取控制

“存取控制”乃一概括性的用词，泛指所有限制不同入士存取权的计算机安全技术。此书中所提及的“存取控制”所指的是已由计算机商建立于操作系统中的存取控制机制，如微软窗口、UNIX 及 MVS 等

辨识与鉴定

辨识与鉴定两个名词常可交替使用。虽然技术人员可能不同意，但我们只讨论此两项栏目下可标识身份的技术。可辨识身份的技术有很多。例如输入用户名称及密码，则已是启用标识与鉴定系统以获得计算机或应用程序的存取权其他还包括大小如信用卡的“智能卡”，同样使用了用户名称及密码的技术；生物识别技术，即以指纹、声音甚至外表作为辨认用户的基准等。不过目前最常用的还是密码，每个人可能单是密码就有好几十个。

防火墙

防火墙选择性地过滤网络间的通讯。如果你的公司可上网的话，那么差不多肯定设有防火墙。在任何情况下如怀疑你公司的计算机系统没有防火墙，请立即翻阅有关书籍并纠正。防火墙是必备的、最基本的安全设施，在与互联网有关的侵害上提供最基本程度的保护，亦可为公司分隔不同安全需求的范围。例如研究部门对上网的要求有高有低，视乎其所研究的范围而定。而销售及市场推广部一般对存取权计算机安全的需求都是中度的。因此内部的防火墙就是将两个部门对安全需求分隔的方法

虚拟私有网络（VPNs）

于计算机间传送的信息均可被拦截或读取，更可改变信息而不被察觉。当然，如所有的信息传送均在公司内进行，则容易倾向于忽视这方面的危机，但当要与外界接触而令内在环境变得不稳定及不安全的话，就必须要确保计算机间的信息传送的安全。员工使用非公司的计算机从外部存取公司系统内的资料时，我们更须确保计算机间的往来是安全的。对这种计算机间传送的要求日渐

增加，令对 VPN 技术的需求亦相应增长 VPN 使用先进的加密技术令往来于计算机间的信 f1 不被读取，亦确保信息不会在不察觉的情况下被更改或伪造

公钥基础建设（PKI）

这是在大型、开放的系统（如互联网）间确保计算机安全的工具，令素未谋面的用户也可以互相信任。 PKI 需在大型的基础建设中使用，但可惜不同公司出品的 PKI 均不尽相同；如能充分利用 PKI，则可确保辨识所有用户，而并清楚知道每个信息或所使用的应用系统。 PKI 最多可容纳过百万的用户。当然你现在可以计划使用 PKI，但距离充分使用及实现 PKI，则尚有数年之遥。

安全编码技术（SSL）

在需求上与 PKI 有些细微分别的 SSL，即万维网（WWW）安全协议，能以 PKI 作为基础鉴定服务器及客户，加密与鉴定万维网的通讯。通常于万维网中使用，并已证实有效。SSL 有多种，其中最简易的一种（SSL2）是最广为使用的 SSL3 安全程度更高，但所涉及的双方（最终用户及服务器）均需于使用前证明其身份，因此使用亦较困难

单一登录

每个用户都想凭一个密码就能使用所有工具，而每个计算机或制造商均承诺此点。然而，事实上单一登录是非常困难甚至不可能的，因为我们使用的计算机系统太多。如果公司只使用一种计算机，则要营造一个单一登录的环境是没有问题的；但很少公司会这样做，因为计算机系统由于经营上的需要和经费上的限制，不可能让所有部门每次都同时更新所有计算机系统，同时，各部门对硬软件的要求也不是全部一样的，单一登录其中一种是“互联网单一登录”，由于所有网络的服务器均以一些普遍的技术为基础，因此可以在所有以互联网为基础的应用系统制造单一登录环境，但必须是应用系统本身已设计成可支持单一登录方可

安全系统所用科技与操作

除了运用这些科技，亦应对安全系统作出管理、监控及维护。

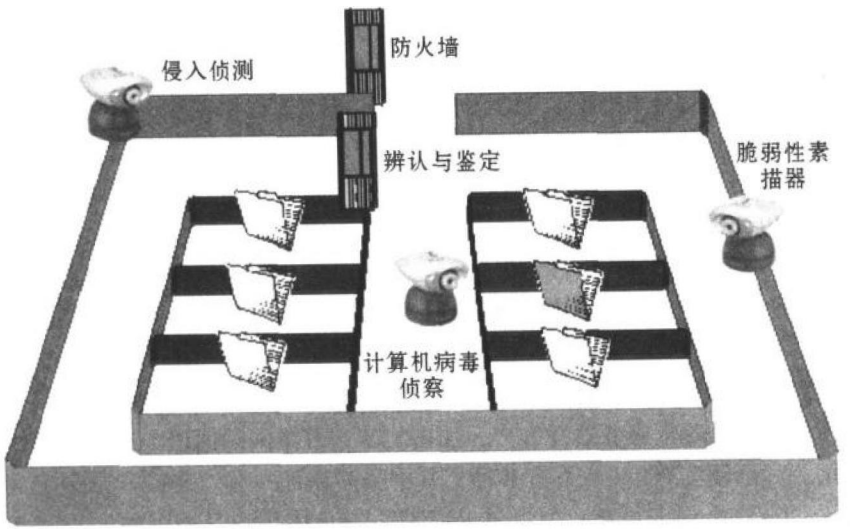

图 1－4　安全系统所用科技与操作能帮助监控和管理你的网络

用户管理

大部分的公司均会使用已安装于计算机内的工具来新增用户；对大型机构来说，一个员工可能有数百个与他有关的新增或消除户口的指令。很多缺乏中央控制机制的公司都不会消除已离职的员工的户口，对计算机安全造成极大的危险。离职的员工可能是对公司或工作不满而选择离职，又或者是在离职后对公司产生怨言。因此这些离职员工很可能并不会再小心保护如用户密码等重要资料。

侵入侦测

如果不是特意侦测，基本上很少会发现计算机系统有侵入者。但其实很多计算机安全系统均不能侦测到侵入者进入系统。侵入侦测工具可在有怀疑时通知你。

脆弱性素描器

计算机都可以在配置时决定其安全设置，因此在制造时可轻易有意或无意地影响计算机的安全设置。脆弱性素描器能侦测计算机的配置并通知用户有关的安全漏洞。

计算机病毒控制

计算机病毒乃一蓄意编造的计算机程序，能快速入侵你的计算机，及造成一定程度的破坏。这些程序就像人的病毒一样，能迅速从一部计算机扩散到与之有关联的计算机，一直延伸出去。破坏性有强有弱，而要避免受感染就得利用抗计算机病毒的工具。

信息安全服务

找寻及留住能管理计算机安全的员工并不容易。如果处理得宜，则可外判予服务供货商负责。无论如何，员工与技术人员都能在信息安全中发挥重要作用。

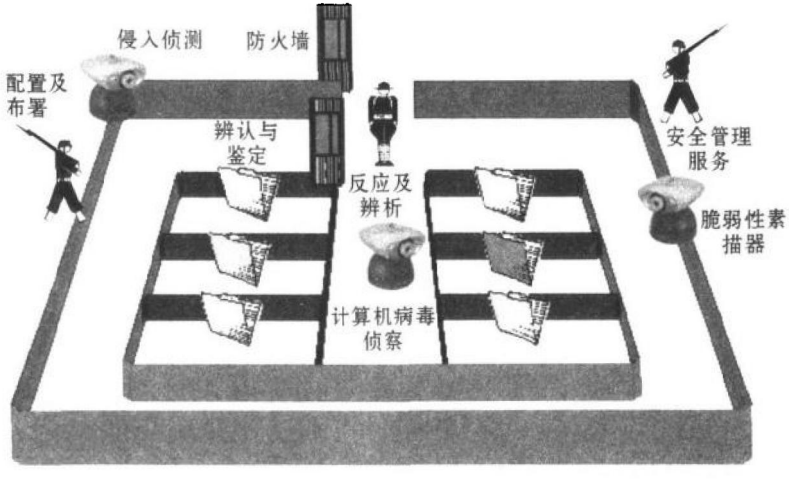

图 1－5 “计算机安全执行技术” + “安全系统的鉴察技术” + “良好的安全的技术员” = 业务资产的安全保证

风险评估

评估信息财产的价值及其潜在风险乃工作的一部分。但这不是一次性的，而是一个漫长的工作，需要负责的信息科技人员与业务方面的同事紧密合作，定期作风险评估。外部的公司则可派出顾问为信息科技部提供短期或持续的协助。请谨记：如果你是属于医疗或金融服务行业，则必须按法律规定定期进行风险评估。

信息价值不太好量化，有些信息对企业来说是致命的，比如那些有关产品生产的科研数据，如果被竞争对手掌握，并很快抢占市场，那么这些数据对企业来说就非常具有价值。另外，企业的财务信息、人事信息、业务信息，也是需要保密的。一般来说，在一个企业的网络建设中，在信息安全方面需要 15%～20% 的投入，对不同的行业，这个比例可能会有所不同，这主要取决于企业需要保护的信息价值到底有多大。

提供安全架构

要了解所有安全技术非常烦琐。具备安全架构方面知识的外部顾问就能为信息科技部及应用程序开发的同事提供最基本的文档，以营造安全的计算机系统。

配置及部署

安装及配置安全软件不是一件简单的工作。如果没有聘请信息科技方面的人员，则可将大部分工作外判予具有相关经验的系统整合公司。

安全管理服务

安装了安全软件后，就需要有人负责其操作。控制房通常需要每天 24 小时、一周 7 天的全天候管理，而外部的公司通常更能有效地提供此类服务，一般包括防火墙、VPN 及入侵侦测等。

反应及辨析

一旦发现入侵者你会怎样处理？在现实世界里最直接的解决办法就是报警。虽然你也想报警捉拿计算机入侵者，但更重要的是作出实时反应，制止损失及揪出原凶。因此公司一定要指派固定人选知道有关安排，而外判公司则可提供人员执行有关安排。

计算机安全就如人生一样，是一个过程而非终点。你可能以为只要安装防火墙、过滤计算机病毒、培训工作人员已经能够做到让计算机安全。但事实是，公司是活动的、不断变化的，因此对计算机安全的需求亦会随之而改变。计算机安全需要不停的维护，令你不断改进。