WILEY

反计算机犯罪

Fighting Computer Crime

一种保护信息安全的新构架

〔美〕Donn B. Parker 著
刘希良 吴艺霞 等译

電子工業出版社
Publishing House of Electronics Industry
URL:http://www.phei.com.cn

Fighting Computer Crime

反计算机犯罪——

一种保护信息安全的新构架

〔美〕 Donn B. Parker 著

刘希良 吴艺霞 译

电子工业出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 提 要

本书由计算机安全领域最具权威的专家编写，以全新、全面、深刻的视角剖析了计算机犯罪和信息安全保护，并辅以大量珍贵的真实案例。

全书共17章，从内容上可以分为两部分。第一部分通过大量的实例分析了计算机犯罪和普通信息安全保护技术目前存在的问题，第二部分进一步提出作者全新的信息安全模型，并对其进行全面深入的说明。

本书是IT行业的管理人员、技术人员、高校教学及科研人员，更是信息业、金融业、保险业等对信息安全有很高要求的企业主管、系统管理员的必读材料。

图书在版编目（CIP）数据

反计算机犯罪/（美）帕克（Parker, D. B.）著；刘希良，吴艺霞译. - 北京：电子工业出版社，1999. 10

书名原文：Fighting Computer Crime

ISBN 7-5053-5342-X

Ⅰ. 反… Ⅱ. ①帕… ②刘… ③吴… Ⅲ. 计算机犯罪 - 对策 - 研究 Ⅳ. C913.9

中国版本图书馆CIP数据核字（1999）第64864号

书　　名：**反计算机犯罪——一种保护信息安全的新构架**

著 作 者：〔美〕Donn B. Parker

译　　者：刘希良　吴艺霞

责任编辑：马树奇

印 刷 者：北京天竺颖华印刷厂

装 订 者：三河金马印装有限公司

出版发行：电子工业出版社　URL:http://www.phei.com.cn

北京市海淀区万寿路173信箱　邮编：100036

北京市海淀区翠微东里甲2号　邮编：100036

经　　销：各地新华书店

开　　本：787×1092　1/16　印张：18.125　字数：460千字

版　　次：1999年10月第1版　1999年10月第1次印刷

书　　号：ISBN 7-5053-5342-X

TP・2669

定　　价：31.00元

版权贸易合同登记号　图字：01-1999-0943

前　言

这本书会讲述许多故事，都是有关于计算机犯罪方面的内容。这些故事与许多犯罪分子和他们的犯罪动机有关，也是关于我们自身的故事，讲述我们对犯罪行为和犯罪动机的反应。书中的故事都彼此独立，反映了我们对系统、技术和社会的态度。我们就是这些故事的主人公，这些故事也是讲述发生在我们自身的事情。

一个流传很久的故事中讲到Donn Parker和Bob Courtney在一次参加国际会议时，乘坐的飞机座位相邻，他们都是应邀在会议上发言的人。Donn想利用这个机会来解决和Bob在思想方法上的一些分歧。Bob却不以为然，因为他觉得恰恰是因为他们之间的这些分歧才使他们能够应邀参加这些会议，并能够在会上发言。

我非常珍惜我同Donn之间的思想方法上的分歧。我的一个同事经常回忆我同Donn的一次思想方法方面的争论，发生在一次计算机协会会议中间喝咖啡休息的时候。他认为我们的争论给听众带来三个层次的深入思考，那并不是夸张。多年以后CSI举行了几次大型会议，对我们曾经争论的问题进行正式而深入的讨论。也许这本书的出版将使人们有机会重新讨论这个话题。

尽管我们达成共识的地方远远超过了我们之间的分歧，但这些分歧却显得不可调和。这么多年来，Donn一成不变地反对我的很有说服力的论点，简单地否认我的观点中的很明确的部分内容。他有礼貌地听我的看法但却坚持他原先的观点，丝毫不进行改变。尽管我确信我是正确的，但是我不愿意根据他同意我的观点的程度和范围来判断他的聪明程度，并且我也从来没有遇见过在任何事情都与我持同样观点的人。

我不敢断定Donn是否会同意我对这些分歧的描述，但Donn有关信息安全的观点确实值得商榷了。我们之间达成一致的是，都认为应该从预防犯罪开始采取措施。对于本书的标题和副标题，他也认为打击计算机犯罪是保护信息的正确方法。但我认为，还要防止信息被有意或无意地改动、破坏或泄漏。

尽管他或许会认为对信息构成的更大的破坏来自于过失而不是犯罪，但他也认为研究犯罪分子的犯罪动机对保护信息安全至关重要。他强调的重点是侦察、调查以及对犯罪分子进行惩罚从而对潜在的犯罪分子进行威慑。我翻阅了他的许多有关计算机犯罪方面的文章，发现他已经沿这上方向独自研究得很久了。

他欣赏法律和法律秩序。例如，在他的书中讲到“如果让我从让犯罪分子在绝对秘密情况下滥用我的信息和FBI窃听我的信息二者之间进行选择，我会选择FBI”。我没有对这种选择的有效性发表评论，我同富兰克林博士进行讨论，他告诉我“那些想放弃关键的自由来换取短暂的安全的人既得不到自由也得不到安全”。我确实很珍惜我们之间的大多数分歧。尽管我可以依靠FBI在无法律状况下保护我，但我只能在法律状态下用法律来保护自己。

我关心秩序，但程度并不象法律那样强烈。另外，我也关心好的行为方式并欣赏自由。我认为，如果人们重视通过计算机和通讯获得的利益，就应该信任自己的系统。如果人们不

信任从系统得来的信息，那就如同没有它们一样。

我们之间的分歧非常敏感，也许这并不重要。无论我们之间有什么分歧，重要的是我们在必须做什么这个问题上是一致的。尽管我们可能在基本的犯罪动机和细节问题上有分歧，但我们一致认为应该有最低限度的安全标准，在实际当中应用，这主要是指作为“基本控制”和“细致工作标准”的措施。这些控制措施是指能够应用于所有的机构和系统中的控制和所有有责任感的职业人员和管理人员应该遵守的预防标准。

具体的系统很少能够满足这些标准，它们构成的总体则可能是一种灾难。这本书帮助我们理解为什么会出现这种局面，以及帮助我们进行改善和提高。

书中讲到，我们成功的标准并非是不允许失败，而是不能放任失败。同时书中讲到，并没有十全十美的安全系统，也承认实现安全经常或必须以牺牲一些其它方面为代价。在良性的环境中，必须实现两者之间的平衡。

我们正在以耗费巨大的花费开支和牺牲系统性能为代价来换取系统的安全。如果我们使系统畅通无阻，那我们的系统将达到完美的地步，或者在没有用户适用的情况下才是完美的。如果我们不把它连接到网络上，它将变得更加安全。现实中人们已经作了足够的工作和尝试、掌握了足够的专业知识、消耗了大量的时间进行研究，测试任何系统的防线。但幸运的是，并非任何系统都能被击破。

那么，人们如何衡量自己呢？人们如何知道自己什么时候做的是正确的呢？人们如何知道犯罪行为和报道的系统失败的复杂性？社会对计算机犯罪行为的态度是一种容忍的态度。

另一方面，社会往往带有很大的警惕性来看待防御措施的失败。社会对任何这种失败的容忍限度都是很低的。飞机可能会坠落，有时候还会撞机。但是，它们并不是简单地从天空中落下而无法解释。因此，尽管死于高速公路的人远远多于发生于空难的人，但是，公众对一件无法解释的空难反应出来的激烈程度比对同时发生的所有高速公路事故都强烈。根据每公里和每人来计算，高速公路死亡和意外事故发生率都远远高于飞机，但是更多的人却害怕乘坐飞机。

例如，通过因特网使用信用卡进行交易比面对面使用更加安全，但在普通公众的意识中却不这么认为；电子形式的交易方式比邮政方式更加安全，但在人们的意识中却恰恰相反。这种误解在一定程度上可以用事故的程度大小来反映，公众对事件的惨烈程度的反应要比对事件发生率强烈得多。

因此，我们如何对待传统系统和如何对待防御措施这些问题就提到了桌面上。系统失败可以归纳为六个方面的原因，主要包括劣质的硬件、脆弱的材料和维护、设计方面的缺陷、主人和操作员的误用以及犯罪分子的破坏。尽管本书的重点放在滥用这个问题上，但仔细阅读本书将会发现设计方面和操作方面的缺陷比滥用造成的危害更大。

尽管没有系统能够避免失败，但我认为防御措施的建设标准与普通系统的建设标准不同。防御措施在通常的下载和使用中不会失败，在意外事故和简单的、能够预测的误用中也不会失败。

书中讲到的应用标准与我们传统的建造信息系统的标准不同。我们认为人们现在所做的目的并不十分明确，结果系统已经变得十分脆弱。这并不是说相对其系统本身而言它们已经完全遭到破坏。这些系统并没有表现出能够抵抗书中讲述的简单滥用类型破坏的能力。

这个问题大多由设计的材料失败导致，到目前为止这些材料依然十分昂贵，以致于只有最有效的应用才能使用。材料最有意义的特征是它们的表现、普遍性和灵活性。为了评判昂贵的硬件设施，我们需要多用户和多方面使用的操作系统，这些操作系统是根据性能而不是根据安全来选择的。这并不是简单地说这些系统没有考虑安全性，而是因为使用过程中安全性会遭到毁坏。实际上，似乎没有什么产品的安全性不能被危害，没有什么安全功能不能被误用，也没有什么特点不能被滥用。

我们在设计中犯的另一个大的错误是没有能够对未授权的使用者（犯罪分子和其他人）充分掩盖最敏感的控制。这么做需要管理人员和操作人员使用强大的确认和加密技术。部分原因可能是系统管理人员希望他们可以使用系统而别人不能使用。实际上，人们是根据责任来评价自己，使其控制的对象不与别人发生接触。

这些设计问题主要是由态度造成的。大多数的IT管理者认为计算机的硬件非常昂贵，维护硬件是他们的职责。在他们看来，尽管安全性值得注意，但是并不一定表明可以危害其性能。甚至那些最了解安全性的职员也持有这种观点，认为安全性是一种不可思议的奢望。当他们确信这种思想时，也会把失败归结于材料问题。在一次对话中，一位安全管理人员说，任何没有使用最小数量、最便宜的材料的设计都是一种“过头的设计”。换句话说，作为设计标准，安全性并不能与代价和成本相提并论。

Netscape公司的Jim Barksdale喜欢把因特网的安全性与商业飞行中的安全性相比较，两者的技术成功都十分关键。他指出1937年DC-3开始投入使用时，飞机只能飞到有限的地方。如果保持1937年的飞行安全水平但是交通水平升高到今天的状况，那么我们的事故水平就将每天杀死两架波音747飞机的乘客，这个道理对于因特网同样适用。

阅读以前的事故报告，可以知道我们并没有停留在1937年的安全水平。只有尽量向前发展才能获得今天的成绩。在比较宽松的环境中，航空公司与有关方面共同合作，以生产最安全的交通运输工具。

许多人可能看过PBS nova，它记载了波音777的测试资料。在一次最为令人惊奇的地面测试中，为了使机翼断裂，他们装载了机身最大载荷的1.54倍。但是，真正使人们感到吃惊的是机翼同时断裂。人们对全过程进行了录像，并反复用慢镜头播放。

在另一次测试中，他们给波音777装载了它能够起飞和在飞机跑道上加速的最大重量。在应该起飞时，驾驶员尽力踩刹车装置，飞机在跑道的尽头停了下来，所有的刹车装置和大多数的线路都起火了。不必担心，他们已经预测到了这一点，消防队员已经全体整装待发，进行救火行动。但是，既然在大多数事故中，消防队员不可能在事故发生时就已经准备就绪，那么装备时间应该扣除五分钟，这时火势不会传播到机身（或油料），而在这段时间中，消防队员应该能够作出反应。

信息技术人员认为他们面对的问题比航空器和桥梁建造者面对的问题要困难得多。信息领域的自由空间更大，问题更复杂，所以人们更容易出错和失败。实际上，其它领域的工程人员在开始的时候与信息技术人员具有相同的自由空间，但在他们有一定的依赖性时便会放弃一定的自由，这就是这本书所要讨论的内容。在信息技术领域中，我们必须勤奋、精力充沛，并且与其它行业和领域的同事加强合作，不使用较低的标准。

我们现在使用最新、最脆弱而非常容易遭到破坏的防御技术来运行和调整其它系统。社会和经济各领域的防御系统都由通讯系统来运作。我希望读者能够从本书获得对责任感全新的感受，而不仅仅是有一种紧迫感。

因此，这本书讲述一些故事也是讲述一些道理，这些道理及时、有用并且重要，值得我们学习、注意和借鉴。

William Hugh Murray
新坎纳　康涅狄格

序　言

这本书是我28年研究计算机犯罪分子和帮助世界各地的受害者的总结。现在保护信息和计算机通讯安全的紧迫性空前迫切并不断增长，因特网的商业和个人应用以及我们对脆弱的互联信息系统的过分依赖，最终使人们认识到保护信息的安全在维持我们社会的生存和发展方面具有重要的意义。

这本书的前半部分着重介绍计算机犯罪分子和信息的误用以及他们给信息所有者带来的挑战，同时我还介绍被我称作信息安全“folk art”的可怖情形，包括我们经常失败地去理解我们的对手以及他们滥用和误用信息属性的情况。我不赞成现在通行的原则，即只保护信息的秘密性、完整性和可用性，因为它过于简单并且不能起到实质的作用。计算机犯罪是一个非常复杂的问题，加上经常发生的非理性行为使这些技术的复杂性变得更加难以理解。为了解决这个难题，我们需要对信息安全进行更详细、清楚地从总体上分析。

这本书的后半部分介绍我关于保护信息和信息所有者的框架和新的基础。并不仅仅是尝试去降低风险，新的方法是实现更加重要的目标，即符合细致工作标准以避免疏忽大意，进行细致的保护。我会通过简单、完备和实用的术语来解释如何使用新的模型实现更高水平且并不繁重的安全保护。

本书与许多关于信息保护的书有所不同。它建立在我从实际的信息滥用者和误用者以及受害者得到的第一手资料的基础上。资料的渊源和课题来自于我多年的安全研究和咨询工作，也来自于对计算机犯罪案例、文章、报道、书籍和录像资料。这段经历包括采访超过200多个计算机犯罪分子和他们的受害者，以及我在SRI咨询公司工作期间为超过250家不同公司进行的咨询服务，覆盖信息滥用和误用的各个方面，并不仅仅限于对计算机中信息的无意地改动、破坏或泄漏，还包括信息的保存和发送。我涉猎了所有类型的保护，并不限于系统和通讯的安全。另外，这个领域的大多数技术专家把注意力集中在对计算机内部信息的保护，而忽视了存储在人脑中的信息、打印在纸上并留在没有上锁或不设防的办公室中的信息。这些技术人员并没有直接面对真实的敌人，因此他们难以理解什么是真正的信息安全。他们从提高计算机系统性能着手，而我们从同计算机信息的滥用和误用者进行斗争着手。

在这本书中我将讲述一些真实的计算机犯罪案例。具体的细节描述可能不是非常精确，因为这毕竟是来自同犯罪分子、受害者有限的交谈和并不详尽的报道，并且其中的部分内容也难以完全证实。但是这一切已经足以证明和支持本书对必须制止的信息滥用和误用所持的观点。有一些案例非常经典而且我在早期的文章中已经进行了详细介绍，在这本书中它们仍然在有关的章节中出现。我没有列出犯罪分子和受害者的名字，除非他们已经为广大公众所熟悉。对他们当中的许多人应该以匿名方式介绍，这样能够给他们机会改过自新。我同样在书中的例子中隐去了特殊信息所有者的名字。

为了能够清楚、准确地阐述案例，本书避免使用一些令人困惑的、不确切的或通常在技术文章中使用的术语。例如，我没有使用access，它是指使用计算机，risk是指可能的信息丢失，professionals是指安全执行人员。access可以用来表示人们能够进入房间，但应用到计

算机中容易引起误解。risk可以用来描述商业投资，但在讲述预测未知的信息丢失时，却并非如此。professionals一词，在信息安全领域中的真实含义我们也很难准确把握，尽管我们中很多人都可以称得上是信息技术专业人员。正确使用单词和准确把握它的意思在信息安全中非常重要，因为我们的对手非常狡猾，并且许多人必须充分理解如何保护自己的信息安全。单词integrity、confidentiality、privacy、computer hacker、crime需要我们认真对待。

这本书的编写得到了人们的大力支持。感谢我的家人的理解和妻子Peggy的建议。非常感谢华盛顿大学著名专业作家Anne Meadows的大力支持，他帮助我提高了本书的质量；Wiley公司的高级编辑Bob Elliott鼓励我写这本书并赞助它的出版。我非常感激我的同事们的鼎力相助，尤其是Bill Murray（编写了前言），Douglas Webb博士、Wallace Bruschweiler、Susan Nycum、Bruce Baker博士，所有的SRIC I-4成员，以及SRI咨询公司帮助我的管理人员。最后，我还要感谢配合本书编写的所有计算机犯罪分子、阴险的黑客以及他们的受害者，他们向我透露了曾经十分痛苦的经历。

送给我的孙子们：Scott, Daniel、Rose、Laura、Allison、Andrew，祝愿他们在这个强大的计算机世界中能够万事如意。

Donn B. Parker
1998年6月26日

目　录

第1章　信息安全的起源

我很讨厌为安全性而担忧，大多数人也厌烦锁门和锁抽屉的事情，没有人喜欢给文件做备份和牢记口令。当面临信息安全性的问题时，对需要保护什么内容和为什么，我们常常会不知所措。

大家都知道，信息既宝贵又脆弱——容易被多种途径地滥用和误用。为保护信息，我们制订了版权法、商标法、商业机密法等法律。进入计算机时代以后，我们又通过了新的法律来保护个人隐私和信息的所有权。同时，我们制订了许多类似于口令和密码的安全措施，使犯罪分子更难获得这些信息。

现在我们关心的是各种各样的电脑世界，这个无形的领域包括书面、口头和电子信息。它们无处不在且传播共享，给人们带来了很多便利，但同时也带来了许多负面作用。

本书讲述的是电脑世界中的信息滥用和误用——姑且称之为计算机犯罪或计算机犯罪。虽然我们很难区分一个事故究竟是有意的还是无意的，但是大多数的信息丢失都是因为偶然事件而不是有意造成的。通过多年的研究，我认为防止有意破坏造成信息丢失的保护措施也能防止无意事故造成的损失，这就是我在本书中强调计算机犯罪的原因。

政府的态度

对于所有的计算机用户来说，信息安全都非常重要，而白宫对这方面的考虑或许已经到了无以复加的地步，因为美国对信息技术极其依赖，所以必须以防止攻击国家基本信息设施的“信息战”的方式来保护自己。正是因为认识到这方面的危险，克林顿总统在1996年7月15日签署了行政命令，其部分内容如下：

> 由于信息设施的能力不足或被破坏可能使得美国的国防或经济安全遭受损害，因而它们的作用至关重要。这类关键设施包括电子通信、电力系统、石油、天然气的储存、运输，金融、交通、供水系统，紧急事故服务（医药、警察、消防和救护）和政府的连续性。对这些设施的威胁可以分成两大类：一类是对有形财产的物质性威胁，另一类是基于电子、无线电、计算机，对控制重要基础设施的信息和通信等关键机构的威胁。

这个行政命令是由包含政府和私人的40个高级专家和权威人士组成的保护关键基础设施总统委员会（PCCIP）制订的。委员会的职责是评价构成关键基础设施威胁的范围和性质，决定法律和政策以排除这些危险，以及推荐解决这些问题的综合性策略。

现在的确是发展信息安全的黄金时期。从60年代末期开始对一些年青的计算机黑客和高技术入侵者的出现而担忧到现在，我们为此付出了长期的巨大努力。

经验之谈

除了造成国家安全的潜在危险之外，电子犯罪同样危及商业和个人，我们每个人都是潜在的侵犯目标。不幸的是大部分人没有引起足够的重视，如同我们锁紧门却打开了窗户。举例来讲，虽然安全保护专家告诉计算机用户设定难以猜测的口令，但恶意的计算机黑客仍然可以通过电脑网络，利用功能强大的自动搜索词典对口令进行解密，实施偷窃。一些人心存不会成为电子犯罪受害者的侥幸心理，而不愿花费防止犯罪必须的时间和精力。

没有一种简单的方法能够预防全部形式的犯罪——如一把足够大的锤子，可以毁坏任何事情。我们不能全面保护信息，但并不意味着我们应该放弃某种形式的保护。除了可能成为电子犯罪的受害者的考虑之外，我们想避免疏忽，就应该通过达到一致的标准，来小心地保护我们的信息。这正是那些小心谨慎的信息拥有者所做的努力。信息拥有者可以采纳许多著名的信息保护措施、手段以达到相应的保护水平。例如，我们可以设定进入口令、锁好计算机房门，妥善保管重要信息的备份，以及各人承担相应的责任（这不要求进行复杂的风险评估）。

一个自身造成破坏的案例

知道自己应该做什么是一回事，按要求去做则是另一回事。几年以前，我曾经是自身破坏行为的受害者。在纽约时代公司（Time Incorporated）董事参加的信息安全会议上，我发表了一次自我满意的动人演讲，着重强调对信息文件进行经常复制、消除原始文件的重要性。在飞回旧金山的路中，我认识到自己也没有遵循这些建议。在我的家用电脑上存储着包含我大半生心血的文件，而最近一次备份已经是4周前的事情了。

回到家里，我来到计算机前，打开计算机，插入软盘。当我键入A字母命令磁盘驱动器对A盘进行格式化时，我无意中却键入了“C”，计算机按照指令对硬盘进行格式化，并非对我的软盘进行操作，破坏了所有的数据。我静坐着等待了20分钟，在黑暗中凝视着不停闪烁的红灯，听着驱动器发出的声音，想着我一个月的工作瞬间消失得无影无踪，却无能为力。我花费了1星期的时间对文件进行恢复，相信此后我永不会再犯同样的错误。

当然，如果有足够的理由，我们可以对信息文件不做任何维护。有些人已经考虑到了这种情况并准备为此付出代价（假定我们的行为不伤害任何人）。面对追求目标，我们必须做出决定。例如，为了实现诱人的商业目的，我们必须承担相应风险而不能一味谨慎。毕竟，商业是一种具有风险的赢利性行为。

但是，疏忽大意仅仅是问题的一个方面，尽管我们小心谨慎，仍然可能跌入犯罪分子精心布置的陷阱，请看下列旁白中的案例。

发生在后院中的生动一课

我曾经对一个名叫Kevin Mitniek的黑客进行了长达20年的研究。他非常孤独、却沉溺于计算机，从十多岁时成为黑客，是70年代旧金山臭名昭著的“罗斯科（Roscue）”黑客组织中的一员。几次定罪以后，因为假释期间在北卡罗莱那因偷盗信用卡号被再次定罪，并被当作逃犯抓获。现在，他在卡罗莱那州等待审讯。

当因特网用户成为电子空间的先锋时，我成了Kevin犯罪的受害者。1988年的一天，Kevin的声音从电话里传出来："Donn，我认为你需要帮助，给我一份信息安全顾问的工作如何？"那时我正准备扩充员工队伍，但他如何得知？一年以后，我得到了问题的答案。从一个在计算机公司工作的朋友处得知，Kevin肯定曾经读过我的e-mail信件。在FBI调查Kevin从公司计算机上盗窃价值数百万美元的电子程序的时候，他们找到了我在USC的一台计算机上储存的e-mail信件（Kevin作为黑客的一种签名技巧是用他人的计算机储存偷窃的赃物）。很明显，Kevin能够假冒我所在公司的计算机管理者，用未经修改的缺省超级口令进入系统，得到我所有的e-mail信件。尽管我对自己的私人秘密遭到侵犯感到惧怕，但是，这却使我的雇主下定决心抓紧安全保护工作了。

信息安全控制的不足

有些受害者采用的防护措施数量虽多，但看起来与犯罪实施的成功与否却不相干。有效防护的关键在于有效措施的正确使用，以及人与人之间、系统之间形成紧密的联系。在这些联系中，信任和防护措施带来的相互制约并存。

经过28年的事实案例研究，以及同二百多个罪犯和他们的受害者的访谈中，我发现绝大部分公司的安全措施远远不足。从一个部门经理在18个月内在银行中侵占了2000万美元的案例我们可见一斑。 他原来在数据传递部门工作，并知到当从另一帐户转入超过100万美元数额时，主机会通知审计员，在帐户的收支帐目出错超过5天时，审计员也会收到通知。所有这些限制都被细心操作的每个银行所接收、采纳，但是这个聪明的部门经理保证任何一次偷窃行为不会超过数额限制，任何帐户的不足情况不超过5天的时间（我称这种方法为"意大利腊肠"技巧，每一次偷窃较少数额，且不被发现，最后得到了整个腊肠）。但是一个星期五的下午，他在移动一笔短缺帐目以逃避5天限制的时候犯下错误，移动数额超过了100万美元，审计人员在下个星期检查帐目时发现了他的偷窃行为并抓获了他。

银行因为部门经理犯了错误才抓获他，长时间以来，这个经理尽量避免触动安全保护措施，这些措施也难以发挥作用。银行的防卫措施造成了他的堕落，并使他每个星期五的下午非常忙碌（使他难以有喘息之机），但是直到他犯下错误这些防护措施才发挥作用。

另外一个案例说明了相同的道理。 很多公司利用称作防火墙的计算机来筛选在因特网和公司内部局域网自由传送的数据，通过监测进出的数据包和限定可接收的信息类型、内容、资源地址、目标和频率，这种防火墙在防止黑客试图使用公司计算机方面能够提供很强的安全保护作用。当计算机黑客反复猜测正确的口令时，防火墙能够监测到这种行为并进而阻止他的成功。但是如果黑客从朋友哪儿得知公司的工程师的个人计算机同电话相连，而计算机又同公司的局域网相连，恶意的黑客拨通工程师办公室的电话，逃避防火墙的监测，实现个人计算机同工程师计算机的连接，以这个工程师的身份进入公司的内部网络，就可以破坏与此相连的大量数据。

每一个实例中，原本强大的防护措施都很难发挥作用，这是因为犯罪分子了解他们并能够成功地绕开他们。换句话，这些防护措施能够被预测和规避。当这些措施难以被预测时，犯罪分子的行为就难以成功。

人为因素

在保证安全方面，人为因素不可低估。公元13世纪末期成吉思汗和他的蒙古游牧部落试图打破、穿过或绕过长城，无奈长城太坚固、太深、太长。通过收买守卫的士卒，他征服了这道障碍，并征服了大半个中国。从那时起，这种状况没有得到很大改善。事实上，当强大的技术防护措施促使犯罪分子蓄意发现它的脆弱之处时，相比较而言，受害者往往要遭受更大的损失。

在一个案例中，一名早期计算机黑客想探访一位医药器材经销商的计算机，却被安全防护系统拒之门外。他只有希望欺骗轻信的员工，使他们透露所必需的关键信息。黑客用最正式的语言，给公司中心的夜间操作员打电话，谎称是计算机维修工程师，如果有正确的口令，就可以解决公司的缓冲器不足问题（他知道公司的计算机正遇到这种问题）。他解释说，可以通过电话线路对操作系统控制程序进行直接修改，运行整个程序，使问题得到纠正，并使这位操作员便可立下大功。

操作员透露了口令，黑客发送代码修改了操作系统程序，也消除了这个棘手的问题。这些修改发生于控制计算机的内部秘密指令上，进而作用于计算机的操作系统，因此黑客可以在将来随意地修改进入口令。这个黑客向储存于计算机中的产品目录文件灌入大量脏话，并在计算机控制台显示器称呼操作员母亲的名字。黑客的行为导致经销商产品的全球销量在几天内大幅度减少。公司难以修改操作系统，因为黑客的代码同样改变了操作系统的唯一备份。在这一经典的黑客攻击案中，技术防护措施性能优越，但是人员控制却失败了。

如何应付这种混乱局面

因为我们难以理解犯罪分子思考问题的方式，所以尽管我们在操作系统中放置控制措施，他们还是在我们的周围出现。我们的技术专家并不理解犯罪分子的聪明、坚韧，也不理解我们的系统中存在的弱点和人为因素，这些专家提供技术控制措施不能满足需求。

我们现行的信息安全基础不够完备、前后脱节、很多情况下也不充分，必须补充一系列的控制措施；为有效地利用控制措施，我们需要理解保护的原则、策略。

CIA信息安全基础的不足

我们对现行信息安全基础的考虑着眼于信息的机密性（confidential）、完整性（integrity）和可用性（availability），许多保护专家把它缩写为CIA。炼金师认为世上的元素只包括火、水、土和气，与此观点相类似，CIA基础反映我们对信息保护的认识水平。虽然我们大大地提高了技术保护措施，但是我们基本的认识却没有超过最初的原始阶段。

因为计算机专家主要考虑保护信息的机密性，早期的控制措施基本上是为了限制信息的可读性。许多计算机犯罪不仅仅涉及观测和泄漏信息，还包含变更、读取、误用或者破坏机密信息等行为。计算机的看护者——审计员的最初职责是保证计算机信息的安全防护，而往往他们缺乏足够的计算机知识来检测控制措施的有效性（他们的方法是对输入的数据进行抽查，并与预期的结果进行比较——在目标计算机的外围，而不是通过或者在计算机内部实