第一章 网络时代的商业秘密

20 世纪 70 年代初，我人生中第一次接触商业秘密问题，那时信息安全还只是各个企业的地方性事务，主要涉及经营场所和文件的物理访问控制，企业保密工作面临的最复杂的技术威胁来自复印机。

时过境迁，计算和通信技术的革命性发展提高了企业生产力，开启了万物互联；贸易全球化也开启了巨大的新兴市场。但信息泄露风险随之急剧飙升，而全球竞争的现实又要求企业将最重要的无形资产托付给世界各地数量和规模不断增长的网络经营者。

这就是当下企业面临的根本性的安全悖论：出于所有的传统原因，保密仍然很重要；但想取得成功，就要在瞬息万变、关系肤浅的扁平世界中分享信息与信任，而这个世界中风险无处不在。传统企业正在失去自身的独立身份，转而以不固定的形态存在，即一种由外部关系、互联网、社交媒体、移动设备和大数据定义的形态。与这个时代很多其他发展一样，这些因素能够带来价值增长的机会，但也是需要积极管理的薄弱环节。

目前，信息不安全的最大推手包括：业务全球化、互联网、其他通信和存储技术、流动办公的员工以及他们的移动设备。很多运营领域都面临管理上的挑战，需要制定和实施能够在不断变化、几乎不可预测的环境中发挥作用的各项战略。下文我们会详细探讨可以促进战略实施的因素。

开放式创新与全球供应链

创新史常以英雄人物的系列故事开篇，故事中的英雄们灵光乍现，作出了改变社会的革命性发明。但现实却没有这么富有戏剧性，发明创造通常需要团队协作，而非“灵光一闪”的瞬间。换言之，伟大的新发明很少完全脱胎于某个发明家的想法，几乎都有赖于一系列在先

的改良，逐步求索而得。亨利·福特（Henry Ford）就是通过这种方式一步步地完善了生产线。1913 年 12 月 1 日，福特汽车第一条大规模机械化生产线启用后，效率从此得到大幅提升，借助这条生产线，工人们可以通过 84 道独立的工序完成整车制造。但如果没有上一个世纪可替换零件的“美国制造方式”的发展，这条生产线也无从谈起。

福特汽车还有另一项知名的效率提升成果——全集成生产系统，也就是通常所说的流水作业线。福特并非只是将零件组装成整车，它还可以自己制造汽车零配件。福特生产汽车需要的橡胶来自于公司在巴西的种植园，煤和钢来自于公司的矿藏，木材来自于公司的森林；此外，公司还拥有自己的铁路和船队来保证运送。企业的这种“垂直整合”在一定程度上确保了风险控制和管理，符合当时的时代需求。

但 20 世纪下半叶全球化竞争和高速创新的出现，意味着在很多行业里，单一实体不可能处理设计和生产的各个方面。将业务灵活地外包给竞争对手逐渐成为了一项合理的策略。正如可替换零件让福特流水线成为可能，有了现代通信技术（包括互联网）的铺垫，外包逐渐扩展成为当今的“开放式创新”。

亨利·切萨布鲁夫（Henry Chesbrough）教授引火了“开放式创新”这个词，它指的是，多数大企业倾向于通过与他人（供应商、客户、甚至竞争对手）紧密协作进行创新，从而获得生存和发展的一种首选方式。在持续发展的外部驱动下，当代的全球企业不得不摒弃“非我所创”（not invented here）综合征，打破传统的管理孤岛，转而拥抱“最好最新的想法通常产生于公司围墙之外”的理念。如今，一些世界上最大且最成功的企业，以各种方式应用这一协作模式制造新产品，包括宝洁、通用、飞利浦、联合利华和福特，等等。

请不要受“开放式”一词的误导。为保护有价值的创新活动，某

些行业广泛采取了保密和专利措施，将“开放式”的说法适用于这些行业似乎存在矛盾。有时“开放式”一词会被错误解读为“自由”，如 Linux 的“开源”软件，或者创造了维基百科的公众合作。因此，可以考虑采用“协作创新”“协作工程”或“共同创造”等词汇来描述走出企业内部、接触未来创造性想法的这个过程。

“协作”和“走出来”意味着分享和承担风险：我必须将我的部分产品路线图托付给你，以便我们可以共同高效地在最佳道路上行进。乍一看，这似乎产生了信息安全困境：保证信息安全通常意味着限制访问。确实，当你把秘密告诉他人时，必须确保他们会努力避免对信息的进一步传播。如下文所述，商业秘密法律和政策可以保护“开放式”创新的安全——只要披露和误用的风险得到良好管控。

与协作创新的过程相似，当代的全球供应和经销网络带来了规模和效率的新机遇。然而，这些网络上数以千计“终端”的存在，意味着企业对其信息的控制力更低（与自己生产零件或派遣自己的销售人员相比）。此外，这些终端——携带笔记本电脑和智能手机的人——散布在世界各地，所处的国家对信息安全和所有权的执法制度、文化态度通常大相径庭。事实上，部分美国公司正在“重新收回”他们之前的外包业务，不仅仅是因为外国薪资成本不再具有绝对优势，或是因为疫情大流行期间经历的供给短缺，他们还认为在美国本土对信息的控制更容易、更有效。

但底线是：即使在贸易紧张时期，大多数现代商业都是通过全球协作完成的，他们必须分享有价值的信息，优化供应链效率。具备完善的商业秘密管理，才能确保这种商业背景下的利益，控制其中固有的风险，并对如何部署最重要的资产做出明智的决定。

互联网

毫无疑问，过去 25 年商业秘密领域中最大的变化是互联网。以往泄露商业秘密的方式通常是粗心的员工将保密文件副本带出办公室，然后不小心遗忘在酒店或者飞机上（下文我们还会讨论到粗心的员工仍然是最有可能的信息泄露源）。但现在，只需要粗心的员工错误点击笔记本电脑上的按键，甚至只是使用酒店或飞机上的 wifi 网络，就会在不知不觉中被网络窃贼植入“中间人攻击”设备，这类设备可以匿名读取通过本地路由器传输的每条信息，扫描有价值的数据和密码，从而更深入地渗透到公司的网络。

机遇：大数据和物联网

首先，好消息是，与没有互联网相比，互联网能够以更快的速度引导创建更多有用的信息。以“大数据”为例。大数据涉及数据和信息之间的差异。IBM 估计，全球 90% 的互联网数据是 2016 年起生成的，当时的日使用量是 440 亿千兆字节，这一数字预计在 2025 年前将增长 10 倍。大海捞针无疑是一项巨大的挑战，非人力之所及，但计算机却非常擅长这项任务——在数据海洋中自动冲浪，然后定位最终可能会有意义的模式。“数据分析”这一新兴领域由人工智能驱动，有望提高人类对复杂系统的工作方式和原理的理解——从天气到疾病，再到人工智能本身——并为各种问题提供创新性和有价值的解决方案平台。以气候公司（Climate Corporation）为例，该公司总部位于旧金山，于 2010 年引入了一项服务——从公共渠道收集数十年来的天气、农作物产量和土壤的数据，以自有算法进行分析，并向农民和农作物保险公司出售由此得出的建议。三年后，该公司以超过十亿美元的价

格被收购。这类新财富的基础是什么？就是将所有这些数据转变为信息的秘密算法，以及由算法所生成的信息，而这些都属于商业秘密保护的范畴。

其他的例子不胜枚举：比如亚马逊的顾客信息库，推动了数十亿美元的销售额；或者谷歌的搜索引擎，每年处理万亿次的搜索。这些系统采用了“机器学习”，从巨量的小额交易中挖掘其背后的价值。（有趣的是，这类秘密所创造的价值并未完全反映在这些公司的账簿上，因为会计师还在为如何评估信息等“无形资产”绞尽脑汁，但这些价值会体现在公司的股价上。）

大数据之所以如此宝贵，是因为它经常会利用为其他目的收集的已有信息，创造出新的有用信息。大多数企业都会记录出售的产品和购买的客户；而一旦汇总这些记录并挖掘出其中蕴含的模式和趋势，便可以提高利润、扩大效率和创造更多销售额。大数据还可以服务公共利益——斯坦福大学的科学家曾使用软件，分析了人们为查找特定药物和自身症状的信息所进行的 8200 万次匿名搜索，并从中准确得出了同时服用这些药物产生的副作用。

迅速发展的“物联网”（IoT）是大数据分析的另一种应用。工业互联网——连接了机器、在途商品和人员——是我们监控事物方式的第一波巨变。工业互联网结合了低成本传感器和无处不在的网络，生成有用信息，提高了效率。我们不仅连接了智能手机和工业设备，还连接了汽车、家用电器、运动器械和各种“可穿戴”设备，生成关于我们自身的数据，包括我们所处环境以及健康状况的数据。截至 2019 年，活跃的物联网设备总数已超过 260 亿，相当于地球上几乎每个人拥有四台设备。

所有这些不断增长的连接会产生惊人的数据量。正如《经济学人》指出，一个燃气涡轮传感器每天可以创造 500 千兆字节数据；全世

界有 4 万台，假设每台燃气涡轮上只有三个传感器，这意味着每天会产生 60 万亿字节数据，大约相当于 2000 年整个互联网产生的日流量的 24 倍。（目前的互联网协议 IPv4 即将陷入困境，因为它只支持 430 亿个地址；而新协议 IPv6 则可以容纳超过 300 万亿个地址。）数据分析因此迎来用武之地，它意味着大海捞针过程中捞到那根神秘的针可以创造的价值。

风险：有百万种方式可以获得你的数据

好消息先说到这里。虽然互联网为开发有价值的新信息（以及由此产生的财富）提供了无限机遇，但也给信息安全带来了特殊威胁。我们会在第七章更为深入地探讨网络间谍的具体问题以及如何管理相关风险。现在需要记住的要点是：互联网不只改变了我们工作和通信的方式，也改变了我们对工作和通信方式的看法。而这一改变，对大部分依赖人类信任的商业秘密系统而言具有深远影响。

不经意间，互联网已成为个人和商业生活的重要部分，也是我们获取地图和食谱等各类信息的首要手段。多数情况下，信息是免费的（但可能需要观看一些广告）。如前文所述，我们正以惊人的速度将设备接入互联网。对企业而言，不仅要考虑计算机和智能手机，还要考虑闭锁系统和打印机。此类“终端”越来越多，带来的风险也越来越大，就像给一栋楼装上越来越多的门。但实际情况比这更糟糕，因为很多设备用的都是老版的简单软件，很容易被黑客利用。一旦攻击者侵入打印机，就可以轻松连接到公司的其他网络。最近一项针对接入互联网的商业设备的调查发现，有 4000 万到 5000 万台设备仍然使用着存在已知漏洞的旧协议。

只要可以通过互联网远程操作，即使是监控摄像头也能为窃贼

打开方便之门。比如，某个品牌的无线摄像头被发现装有存在漏洞的软件，远程攻击者可以借此提取设备的全部内存，包括摄像头的安全证书以及用于访问摄像头的网站和账户。德克萨斯的一户人家发现了这个漏洞，当时他们听到婴儿房传来喊声，发现有人侵入了他们的婴儿监控器，对孩子们大喊脏话。

敌人就是我们自己

这个问题涉及更深层次的东西。我们不仅创造了安全性非常脆弱的基于互联网的系统，还拒绝承认该系统的风险程度。因为互联网已经融入我们的日常工作，并且可以保证在99%的时间内都能正常运行，我们很可能没有注意到它的危险性。以电子邮件为例，我们对它又爱又恨，因为光是每天浏览邮箱就要花掉很多时间。我们会删除明显的垃圾邮件，但稍不留意，可能会打开一个很久没有联系的人发来的邮件，告知我们某个感兴趣的消息，比如即将召开关于某个主题的会议。我们打开邮箱中的链接，却没有意识到已经把一位不速之客请进了自己的系统，而这位“客人”会在我们毫不知情的情况下植入恶意软件，控制设备的运行，并通过“受信任”的路径进入我们工作企业的网络。

根据2018年赛门铁克（Symantec）发布的互联网安全威胁报告，大约55%的电子邮件是垃圾邮件，即使安装了过滤器，用户平均每月仍会收到16封恶意邮件。将这个数字乘以系统使用的人数，就可以看到人们多么容易受到误导，尤其是在注意力不集中的时候。有些黑客还会采用“延时”技术，使电子邮件躲过传统筛选，在几小时或几天后才变成恶意邮件。而且，越来越复杂的“鱼叉式网络钓鱼（spear-fishing）”已变得越来越普遍，这些程序会把从社交媒体网站上“抓取”来的关于你的信息加入到电子邮件的信息中。而此类程序

的变体——“对话式网络钓鱼（conversational fishing）”，会通过一系列相关电子邮件，让消息看起来更真实。考虑到我们对电子邮件漫不经心的态度，如此多的攻击取得成功也就不足为奇了。（据估计，三分之二的钓鱼邮件在周一和周五发送，一般认为在这两个时间点人们的注意力会不大集中。）

但更糟的是，不但网络让我们不太关注自己的通信，还“教会”我们主动交出自己的数据。我们创造出了全新的“脸书一代”，人们被悉心培养使用社交媒体进行联系、向大量观众分享私人信息。如前文所述，这为通过电子邮件进行有针对性的鱼叉式网络钓鱼提供了素材。而且，分享私人问题的冲动会渗透到个人的商业活动中，即员工在为解决雇主（或雇主的客户）的问题而寻求帮助时，可能认为将相关问题发布到网络空间完全没问题，但实际上却造成了无法挽回的保密信息泄露。

互联网和保密活动给我们的教训是：敌人就是自己。对信息丢失的防御必须是多方面的，我们需要能够实时分析威胁，并对许多不同类型的行为做出应对。

移动设备：U 盘、笔记本电脑、平板电脑和智能手机

技术进步最大的讽刺之一是：在我们创造出越来越有价值的信息之时，我们也在创造更有效地盗取这些信息的工具。过去，窃贼青睐的信息工具是复印机，现在则是无所不在的 U 盘（现在有数十亿计的具备 USB 功能的设备），只需几秒，就能加载几千份文件，然后放入口袋或钱包中带走。U 盘也是公司网络“内部污染”的主要媒介；有时候，数据窃贼会将受病毒感染的 USB 设备故意丢在一家公司的停车场，希望有员工捡到并插入他们的电脑看看里面有什么内容。我

们可以采取很多措施降低这类风险（请见第五章），但有些安全措施会令人沮丧，比如，许多企业通过软件或环氧塞的方式关闭了所有电脑上的 USB 功能。

1982 年，在本书的前身出版之时，笔记本电脑还不是放在膝盖上的便捷电脑。如今，笔记本电脑已是每位出差高管或经理用来存储竞争必备的所有信息的工具。很多公司都制定了政策，要求员工出差时只携带存有旅程必要信息的“精简”电脑。但即使员工使用公司笔记本电脑或平板电脑在家工作，如果个人信息和公司信息混放且登录了不安全的网络，同样会增加信息泄露的风险。

同时，计算设备的尺寸不断缩小。对世界上大多数人来说，智能手机是他们访问互联网的主要方式，智能手机比 20 世纪 60 年代的大型计算机拥有更强的数据存储和计算能力。过去公司 IT 部门可以屏蔽个人移动设备进入公司网络，黑莓的独特成功就可以追溯到对通讯进行严格控制的渴望。但多数关注该问题的人认为，这场斗争已结束，员工最终胜出。人们甚至还为此造了一个词：BYOD（自带设备办公）。当前，手机、平板和个人笔记本电脑等员工自有连接设备激增，而且其中大多数设备都越过了公司的物理防线，使得信息保密工作比以往任何时候都更加困难。

无论精心设计的间谍活动是否还像我们以前认为的那样普遍，互联网已经开放了许多途径，交易工具也变得更小、更便宜、更有效。精密设备可以通过远距离测量会议室窗户的微小振动来窃听会议室中的讲话。如果将传声器（窃听器）和摄像头安装在小型无人机上，有时甚至都不必隐藏起来。正如《经济学人》的打趣，如果你真的需要确保对话不被偷听，解决方案是“找一个狂风呼啸的夜晚，在新犁过的田地里，赤身裸体地召开重要会议。如果做不到这一点，那就拉上窗帘，清理窃听器，轻声低语，避免直接引用事实”。

员工：仍然是最大的泄露源

在商业秘密的世界里，几乎不变的一点是：无论互联网或恶意软件入侵会带来何种风险，对公司数据安全的最大威胁来自于两耳之间的“湿件”，即大脑。安全专家称为“内部威胁”，尽管这种威胁有时会通过个人的故意行为表现出来，但目前为止最常见的信息泄露原因是员工的粗心大意。

我们都看到过机场里疲惫不堪的出差人士，他们无法接入公司的VPN（虚拟专用网），但需要向总部发送包含重要文件的消息，不得不使用免费的公共网络（Wi-Fi），却没有意识到有“中间人攻击”设备正在钓鱼。在对虚拟窃听毫不知情的情况下，员工通过免费的Wi-Fi 发出了信息，但消息在传输途中遭信息窃贼拷贝。更糟的是，窃贼还顺便掌握了员工的网络密码，可以直接登入公司系统，安装软件工具查找更多密码，监控按键输入，转发电子邮件，发送令人产生兴趣的文件。另一种可能的情况是，加班回家后还有重要工作需要处理的员工，在离开公司前，用 U 盘拷了些非常敏感的公司文件，回到家后用私人电脑继续完成相关工作；这时，公司的信息与早已侵入员工电脑的恶意软件一起被存储到硬盘驱动器中，之后恶意软件采取行动，将雇主信息发送给窃贼。此外，恶意软件蠕虫病毒还会进入 U 盘，第二天上午员工把这个 U 盘插入公司电脑后，感染的病毒会在公司整个网络中传播扩散。自从新冠疫情大流行，越来越多的员工在家网络办公，这种个案很可能会扩大范围演变成灾难。（关于如何降低在家办公的固有风险，我们将在第五章探讨。）

公司治理

我们会在第五章和第八章讨论公司董事会和管理层面临的关于无形资产的信义责任。对于大部分企业，特别是上市公司，网络攻击（包括网络间谍）带来的威胁对公司治理提出了重要议题。2018 年，美国证券交易委员会发布了最新的网络安全指引，尽管形式上是一个自愿采用的指引，但很多人认为这实际上是强制性指引。2013 年，欧盟委员会发布了一项立法建议，要求企业评估信息安全风险并采取行动，并指出：“行业应反思让 CEO 和董事会承担更多确保网络安全责任的方法。”2014 年 2 月，美国商务部发布了《NIST 网络安全框架》，详细说明了保护关键性基础设施的最佳实践方法，经 2018 年更新后，安全专家认为《NIST 网络安全框架》会成为所有公司对信息进行审慎风险管理的事实上的标准。

随着信息日益成为公司最具价值的资产，信息管理也遇到了前所未有的挑战。在日新月异的环境中，信息资产不断面临新的威胁，企业本能地投入所有资源进行防御：警戒周边、控制移动设备、保持高度戒备。但上述举措忽视了一个细微但非常重要的转变——这是我对成熟公司如何履行信息管理职责的观察所得——信息最灵通的企业不再假定上述措施有用或是最应该做的事，也不会只注重把自己的信息封锁好并防止感染。在一个高度互联的商业世界，要达到近乎完美的安全标准非常困难，全球化竞争的需求使得这一挑战难上加难。“完全控制住”信息似乎是一种无用功，还可能是一种浪费，因为在当今环境中，把信息封锁起来就像把钱藏在床垫里，可能会剥夺企业通过他人的开发利用（无论是合作还是许可）获得额外收入的机会。

确实，管理层面临的一大问题是，如何最好地利用公司在已经开发的信息中可能具备的竞争优势。从纯技术角度看，这涉及如何处理

那些值得采取严格知识产权保护的创新。传统的专利委员们会选择那些被认为值得投入成本和时间的发明，并在相关市场取得专利。但问题可能更复杂，部分原因是专利法已经修订，而且与过往相比，在为一项发明申请专利或作为商业秘密（全部或部分）保护的取舍上，人们的分歧更大。（商业秘密和专利之间的区别，以及如何选择适当的保密形式，请见第四章。）这意味着管理层需要更多地参与其中，首先要针对公司信息资产的开发利用制定一项优化策略，确定将公司信息资产作为商业秘密还是其他知识产权进行保护，以及直接使用还是对外许可。

信息管理的基本理念是：当代的信息管理不仅仅是保障公司信息不丢失和不受污染，尽管这些是至关重要的一部分。审慎的信息治理要求动态化的企业策略，可以识别出全部信息资产并设置确保信息资产得到适当利用的程序。完全的信息纯洁目前不可能实现，不仅因为技术原因，还因为共享或销售也是审慎管理的一部分。信息管理首先要了解你所拥有的信息资产，以及如何有效地使用信息资产并从中获利。你可能会惊喜地发现，信息管理可以为公司的业绩增色不少。