Equifax 数据外泄后记：为金融机构及其客户加强网络安全和身份盗用防范措施

2017 年中发生的 Equifax 数据外泄事件是迄今为止最严重的数据外泄事件之一。数据外泄最近引发关注，也许最终各国会认真对待这个问题，开始采取全面、有效的解决措施。需要注意的是，此类数据外泄事件早在新闻报道频繁出现，网络犯罪和身份盗用行业发展成熟、高效之前，就已经时有发生。

事件经过

这起数据外泄事件是如何发生的，从中可以吸取哪些教训？网络犯罪分子可运用多种方式攻击机构，窃取数据。机构仅对最近新闻报道中提到的威胁采取对策远远不够；适当的网络安全计划需要评估所有风险，并按照优先顺序对症下药。也就是说，每个人都应从 Equifax 数据外泄事件中吸取教训。

Equifax 的网站存在漏洞，令消费者对其部分信用记录提出异议。消费者质疑记录的准确性，存储所提供信息和文件的数据库与其他包含消费者数据的数据库相连。Equifax 构建这个平台时，计算机程序员遵循了利用开源资源预编写部分代码的惯例。

开源计算机代码意味着可以免费查看和下载。“源代码”中每行代码都是可读的，并可根据需要进行修改。这些源代码组件可以与其余代码合成，然后将整个源代码“编译”成计算机可运行的格式，称为“机器代码”。相比之下，专用代码（可供购买的软件）则是已编译完成的代码，我们无法看到每行代码的具体细节。

程序员使用开源组件避免重新编制系统以及重写已经编写、使用和测试的代码。计算机编程需要整合预编写的部分代码，确保它们适合系统并可以协同工作，并确保程序可以与用户和数据库正确交互。Equifax 的网站使用的是 Apache Struts 开源组件，用来接受用户填写的网页表单，并将填写的信息传输到底层数据库。Apache Struts 由 Apache Foundation 维护，程序员可自由下载、检查和修改。

软件开发人员的工作就像承包商建造房屋。他们不制造木材、胶合板、砖块、石膏板、窗户或门，但会购买这些组件并组装。建筑产品成本高昂，但开源软件免费且可重复使用，但也需要确保合格。就像免费领养的小狗和小猫一样，需要耗费相当大的费用和精力来照顾它们。

建立面向消费者的网站过程中，Equifax 整合了开源软件组件，其做法完全可以接受。但是，他们未能跟踪组件的使用情况，及时发现漏洞并修补。所有软件都容易出现错误和安全漏洞，开源软件也不例外。程序员始终希望发布的代码是完美的，但始终会发现需要修复的错误，以及需要修补的安全漏洞。变化日新月异，操作系统和网页浏览器更新后，就可能需要更新相应的其他程序。因此，开源组件需要不断修复，来解决漏洞或错误，然后发布新版代码。仍在使用旧版本的任何人都会面临风险。

2017 年 3 月 7 日，Apache Struts 社区发现一个漏洞，攻击者可能会通过该漏洞突破软件组件，访问机密数据。攻击者可以

在网页表单中输入特殊内容，欺骗数据库执行命令并授予特殊访问权限。Apache Struts 发布了修复此问题的更新版，通知用户社群停止使用旧版本并将更新版合并到他们的软件中。

理想情况下，公司会保存一份软件清单，列明软件内容，包括所用组件的特定版本。在实际情况中，许多公司没有这样做。但定期评估漏洞，开展渗透测试，仍然可以发现这些缺陷。

这就像房子的锁。某种型号的锁失效了，用钥匙胚也能开锁，或者“智能家居”功能被黑客轻而易举地成功攻击。不幸的是，全国几千户房子（特别是新房）都安装了这种型号的锁。于是，制造商和承包商告诉房主，他们的锁不安全，需要修理，但同时窃贼也会知道这件事以及如何趁虚而入。解决方法很简单——找个锁匠换上新锁。如果锁匠不能立刻来换锁，房主还可以采取临时安全措施，例如在家中使用链锁、监控系统，甚至在外面配备保安人员。在信息安全方面，这种措施被称为“补偿控制”。

通过锁这一比喻，我们了解了安全漏洞，但与之相比，Apache Struts 补丁更加复杂。换锁十分简单，但更改软件组件并不易，它不像更新智能手机，按下提示的“更新”按钮即可。想一下 2004 至 2005 年的中国石膏板腐蚀事件。当时，卡特里娜等飓风造成严重破坏，随后大规模重建，导致美国生产的石膏板短缺。因此从中国进口大量石膏板，用于全美，尤其是东南地区的建筑

换锁十分简单，但更改软件组件并不易，它不像更新智能手机，按下提示的“更新”按钮即可

金融机构和企业需要识别其平台上与身份盗用和网络犯罪相关的风险

项目。但很快发现这些石膏板有毒，对于居住者而言是不安全的，甚至可能会破坏电线等建筑构件。屋主意识到他们房屋使用的是危险的中国石膏板，但更换起来难度高，价格也昂贵。基本上，房屋的内部必须全部拆除并重建：拆除所有石膏板、安装新的石膏板、接缝、抹腻子、微调和涂漆。

有时发现漏洞后，公司没有足够的资源来修复漏洞。一些房东可能觉得没有必要换锁或更换石膏板，认为窃贼不太可能闯入，或石膏板释放的气体不太可能伤害租户或损坏建筑物。事后看来，Equifax 在风险分析和反应方面似乎存在类似的缺陷。他们应该重写网站代码，融入 Apache Struts 的更新版本。在构建、测试和部署新网站的几天、几周或几个月内，他们应该通过添加过滤器（或解析器）来进行临时补偿控制，防止 Apache Struts 漏洞遭到攻击。该漏洞让用户可以在网页表单中恶意输入，可能会导致网站授予攻击者控制权和访问权。补偿控制可审查输入内容，防止有害文本进入易受攻击的 Apache Struts 代码。

黑客正是利用这一漏洞，攻击 Equifax 并窃取了 1.5 亿受害者的个人信息，Equifax 于 2017 年 7 月 29 日获悉数据外泄，于 9 月 7 日向公众披露。这似乎是有史以来最大的数据外泄事件之一，引发了诉讼、监管行动、立法以及对内幕交易的起诉。

个人应如何做？

个人如果知道采取哪些措施应对数据外泄事件，就能保护自己、家人，以及为客户提供更好的建议。此次数据外泄事件的罪魁祸首尚未查清，但众所周知，他们现在拥有一份全面的个人身份信息数据集，可以将之出售，用于身份盗用或其他恶意用途。

一些罪犯将利用此次外泄导致的恐惧。他们将实施网络钓鱼攻击或其他欺诈计划，让个人误认为他们成为了身份盗用的受害者，欺骗他们提供个人信息或做出暴露其计算机或云数据的行为。

企业也会利用大众的恐惧销售产品。Equifax 等公司出售信用相关的产品和服务。数据外泄有利于他们开展业务。他们通过广告和恐惧策略，说服消费者每月支付一定费用，换取安全感。信用报告机构的商业模式令其有多个谋利渠道：销售消费者数据的访问权，在数据外泄后销售安全服务，以及让消费者为保护他们的数据和身份付费。

根据此次数据外泄引发的内幕交易案件相关事实，公众了解到 Equifax 对数据外泄的态度。数据外泄事件发生后，一些 Equifax 员工被告知该公司可能即将面临数据外泄事件，但他们并不知道 Equifax 即是数据外泄的主体。据称，一名员工发现后，迅速出售了他所持的 Equifax 股票，预计一旦数据外泄事件公布后 Equifax 股价将会下跌，因此被指控内幕交易（相反，几名高层员工在数据外泄发生几天后抛售股票，但经 Equifax 内部调查后被证明无罪，称他们抛售股票时并不知晓数据外泄事件）。因此，Equifax 通过数据外泄谋利，但外泄对公司估值不利。

从消费者的角度来看，个人应鼓励政府加强监管，提升对隐私权的保护，并改变企业存储、使用和销售消费者数据的规则。也可以呼吁政府妥善处理网络犯罪，而不仅仅是要求企业加强安全，也不是简单地将其视为执法问题，而是全面解决这一国际普遍面临的问题。

执法方面，可以采取更多措施，解决身份盗用和网络犯罪的危害。身份窃贼通常依赖于通过 Equifax 式数据外泄手段窃取数据，但检察官难以对身份盗窃案件立案，需要数月艰辛工作，跨司法管辖区调查，还需要企业和金融机构的协助。地区检察官 Robert Morgenthau 在意识到打击这一犯罪的重要性后，创建了美国首个反身份盗用部门。所调查案件很快证明身份窃贼和网络犯罪分子之间存在联系。缺乏资源或仅寻找可快速引起新闻界关注案件的检察官无法提起相关案件的诉讼，打击这一罪行。

幸运的是，消费者可以免费行使一些权利。每年都可以从三家信用报告机构 Equifax、Experian 和 TransUnion 中分别获得免费信用报告。此项操作可在 www.annualcreditreport.com 网站完成。不要被其他网站欺骗，为此类服务付费。如果有任何信用信息不准确，可以提出异议并纠正。讽刺的是，Equifax 的异议汇报网站遭数据外泄，因此对其信用记录提出异议并提交身份证明及相关文件的

消费者损失最大。无论如何，纠正信用记录是一项需要时可以行使的权利。

这三家信用报告机构也有权“冻结”信用，这将阻止他人获取信用记录以及开立新账户。无疑，此前这三大机构会收取费用，但新法律规定消费者可免费享受这一服务。这些机构还提供信用“锁定”服务，可能与其他付费服务捆绑，但即使没有免费“冻结”的法律规定，也建议消费者选择“冻结”，而非“锁定”。

金融机构和企业应该做些什么？

金融机构和企业需要识别其平台上与身份盗用和网络犯罪相关的风险。美国联邦贸易委员会危险信号规则 (Federal Trade Commission Red Flags Rule) 要求制定此类身份防盗制度，并且机构应努力超越最低合规标准。

其中一项风险是企业将为此类犯罪提供渠道，欺诈者可以以受害者的身份接触企业。由于市场上可能会出现一批新的被盗个人身份信息，可能会导致此类欺诈事件增加。在线开立账户时，网络犯罪分子和身份窃贼可以完美伪装，欺骗在线验证工具。他们可以很轻易地在市场上购买个人信息，因此提供虚假的姓名、出生日期和社保编号等信息并不难。即使是在现场开立的账户也容易遭受这种欺诈行为，身份窃贼可以很熟练地出示伪造身份证明的文件。

金融机构和企业应采取更积极的方式处理与身份盗用相关的欺诈行为。显然，网络犯罪数据外泄与使用此信息进行身份盗用之间存在关系。因为身份盗用有利可图，所以数据外泄也有利可图。金融机构和企业会遭遇成千上万的欺诈行为，这些都能为建立刑事案件提供宝贵信息。

私营部门开展欺诈和反洗钱调查对于减少网络犯罪和身份盗用至关重要。然而，有些可以容忍其平台上发生身份盗用行为的企业和金融机构，将开展相关调查视为商业支出、额外成本，而不是良好的企业公民应承担的重要责任。当然，有许多专门的专业人员负责调查此类欺诈行为，但他们有时会缺少相关资源或支持。

信息安全至关重要，因为金融机构和企业收集、存储与客户和员工相关的大量数据，许多外泄事件仅仅是因为未能采取基本的安全措施。每个员工都是潜在的外泄点，缺乏知识或意识会带来重大风险。公司需制定成熟的事件响应计划，培训高级管理人员。Equifax 在事件中 缺乏对策、沟通不畅，因而进一步损害了公司声誉，也危害了消费者利益。

金融机构和企业应采取更积极的方式处理与身份盗用相关的欺诈行为

适当的风险分析首先要评估潜在的威胁、危害和成本，然后按照优先顺序采取补救措施。如果 Equifax 采取适当举措，他们就会投入资源解决问题。公司需制定强大的网络安全和反欺诈计划，这需要不断改进并将其融入企业文化中。网络安全的责任不能推脱给较低级别的员工（作为事件的替罪羊），而应该由最高级别的管理层来承担。预防比事后补救成本更低，而且针对网络犯罪和欺诈行为采取强势态度也将有益于企业发展。

结语

为保护自己，消费者可以从三家信用报告机构获取免费的年度信用报告，冻结信用，提升自己的网络安全意识，支持致力于保护安全和隐私的机构，以及鼓励政府更全面地解决这些问题。

金融机构和企业必须尽自己的努力来加强所保存的数据的安全，并防止落入网络犯罪分子手中。他们还需要投入资源，调查网络犯罪分子和身份窃贼，减少他们的非法利润。

最后，政府需采取更多措施，保护民众免受犯罪的威胁。如果受害者对威胁毫无控制措施，攻击者居住在异国，那么公众将更依赖政府。A

John Bandler，CAMS，
律师事务所 Bandler Law Firm PLLC
创始人，美国纽约州纽约市，
johnbandler@BandlerGroup.com