2018 年网络安全预测

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Analyst Perspective: 2018 Cybersecurity Forecast		
原文作者	Adam Meyer	**原文发布日期**	2017 年 12 月 1 日
作者简介	Adam Meyer 是 SurfWatch Labs 首席安全策略师。他曾在防御、技术和关键基础设施领域担任领导职务超过 15 年。		
原文发布单位	SecurityWeek		
原文出处	http://www.securityweek.com/analyst-perspective-2018-cybersecurity-forecast		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

2018 年网络安全预测

Adam Meyer

2017 年 12 月 1 日

又到了我们回顾过去一年并展望未来一年威胁状况的时候。我花了大部分时间来分析大量的威胁数据、寻找威胁趋势并创建威胁情报，希望能够为客户提供重要的见解，帮助他们更好地应对即将到来的网络威胁。为了这一愿景，我将对 2018 年的网络安全情况进行预测。

1. 2018 年，个人和组织将会付出惨痛的代价，个人识别信息不应该被用作验证信息。

尽管大多数组织长期以来对识别信息（identifier）和验证信息（authenticator）两个概念比较模糊，但是两者之间存在着重要的区别。作为个人识别信息的信息可以是诸如社保号、驾照号甚至地址之类的信息。验证信息可以是一个问题，当被正确回答时，能够证明你就是本人。基于知识的验证包括一系列问题，如你的高中吉祥物是什么？你的第一辆车是什么牌子？或者，这些验证可以基于信用报告数据和许多其他信息，相对于成本更高但更安全的验证方法（如双因素认证/2FA）来说，这些验证成本较低。

不幸的是，太多的组织将识别信息用作了验证信息，导致诸如 Equifax 这样的大规模数据泄露事件屡屡发生，在 2018 年这会带来更加严重的问题。Equifax 存储了数百万客户的个人身份信息（PII），这些信息被攻击者窃取，导致每个人的身份信息都面临被滥用的风险，特别是在那些将识别信息用作验证信息的组织中。举例来说，你打电话给银行，他们要求你提供社保号后四位、姓名、出生日期等.....所有这些都是识别信息，而不是验证信息。Equifax 事件发生后，有多少黑客得到了这数百万客户的识别信息呢？在 2018 年，个人和组织将会再次以惨痛的代价认识到这一点。要解决这一问题，最重要的是让组织停止将识别信息用作验证信息。

2. 2018 年，伙伴关系、供应链和“即服务”（as-a-service）关系将会引发更多的泄露事件。

业务越来越数字化，精明的组织正在通过伙伴关系、供应链集成和“即服务”功能扩展其业务范围并为客户提供便利。虽然这种广泛的外包正在成为日益流行的业务加速方法，但

它也可能是一个危害安全的噩梦。在 2017 年，德勤（Deloitte）和博思艾伦（Booz Allen）都在这方面栽了跟头。明年，我们将会看到更多由于合作伙伴网络攻击引发的数据泄露事件。

在合作中，组织共享数据和品牌声誉。公司应该开发网络安全最佳实践，并要求所有伙伴遵守；应根据任何适用的监管要求拟定书面合同，在合同达成和/或续订之前，应限制与合作伙伴的业务范围。不幸的是，这可能会给采购部门带来难题。由于这些最佳实践可能会影响预算，以满足新的要求并加以执行，因此组织需要在明年建立这一要求并相应地管理成本。

3. 2018 年，小型医疗机构将成为勒索软件攻击的首选目标。

勒索软件将继续作为全球黑客的一条业务线，但是其攻击目标将会更加有侧重性：防御措施不够完善的中小企业。因此，赎金金额可能会比较低，以便较小的组织有能力支付。明年，地区诊所和医院将会成为重灾区，这主要是因为很多黑客认为它们易于攻击。以最少的投入获取最高的回报是这些“商人”所追求的目标。

4. 组织会将泄露响应的优先级排在事件响应之前。

在公司认真对待数据泄露之前，我们还要收到多少来自 CEO 的道歉信呢？随着网络安全在各地的董事会会议上成为优先处理事项，组织意识到这不仅仅是一个技术问题。这是一个组织的优先事项，虽然公司肯定会有失误，但我们将会看到更好的泄露响应计划。

事件响应是 IT 运营和安全工作，旨在防止安全事件并在事件发生后进行补救。泄露响应远不止于此——它涉及整个企业如何应对影响客户数据的泄露事件，涵盖从受补救成本影响的底线数字到未来公司声誉的所有内容。泄露响应包括首席执行官、董事会、法律部门、市场营销和公关团队等的行为。

在泄露响应方面，Equifax 做了最糟糕的示范。该公司在全世界的目光下，出现了一个又一个的失误。该事件为一些组织敲响了警钟，他们必须优先考虑、计划和实施泄露响应计划。

5. 机器学习技术作为一种能力将会更加清晰和成熟。

机器学习是一个流行词，对每个人来说它的意思都有些微不同，但是我认为在 2018 年这种能力将会变得更加清晰。机器学习技术的目的是减轻人们的负担，提高处理和理解大量数据的速度。安全技术不断进步，我们将会看到更好、更高质量的数据。我们正在改进数据

处理，届时创建更智能的人类响应将成为可能。在 2018 年，机器学习或自动化将会继续改善，威胁情报数据的质量也将不断提高。将机器学习威胁情报功能与可以提供分析、见解和建议的人类专家相结合将是两全其美的选择。

安天实验室简介

安天是引领威胁检测与防御能力发展的网络安全国家队，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。

安天智甲终端防御系统面向政企用户网络安全需求，同时支持传统企业反病毒和白名单+安全基线两种防御模型。通过安天自主研发的反病毒引擎和主动防御模能有效防御感染式病毒、蠕虫、木马、僵尸网络、格式文档攻击等针对主机的安全威胁。针对高级威胁能够进行网内威胁追溯和定点查杀。安天在智甲产品中形成了一套独有的针对勒索软件及各家族变种的检测、防御和阻断方法，可帮助企业用户免受勒索软件骚扰。