简译版

物联网安全事件日益猖獗且成本高昂

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	IoT Security Incidents Rampant and Costly		
原文作者	Dawn Kawamoto	**原文发布日期**	2017 年 7 月 18 日
作者简介	Dawn Kawamoto 是 Dark Reading 的副主编，主要关注网络安全新闻和趋势。https://www.darkreading.com/author-bio.asp?author_id=2382		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/vulnerabilities---threats/iot-security-incidents-rampant-and-costly/d/d-id/1329367		
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。		

物联网安全事件日益猖獗且成本高昂

Dawn Kawamoto

2017 年 7 月 18 日

最近的调查结果显示，在使用物联网设备的公司中，近一半遭遇了攻击事件，而且处理这些攻击的成本通常超过传统攻击。

两份独立的研究报告均显示，物联网设备攻击导致 46%的受访者遭受了攻击事件。

IDC 本月发布的一项调查采访了大约 100 名 IT 安全人员、IT 运营人员和高管。而另外一项调查是由咨询公司 Altman Vilandrie 在今年 6 月份发布的 ,他们采访了 19 个国家的大约 400 名 IT 高管。

根据 Altman Vilandrie 的报告，在未来的几年内，保护 IoT 设备的成本将会增加，甚至高达 IT 预算的三分之一。绝大多数 IDC 受访者表示，处理物联网攻击的成本往往超过传统攻击。

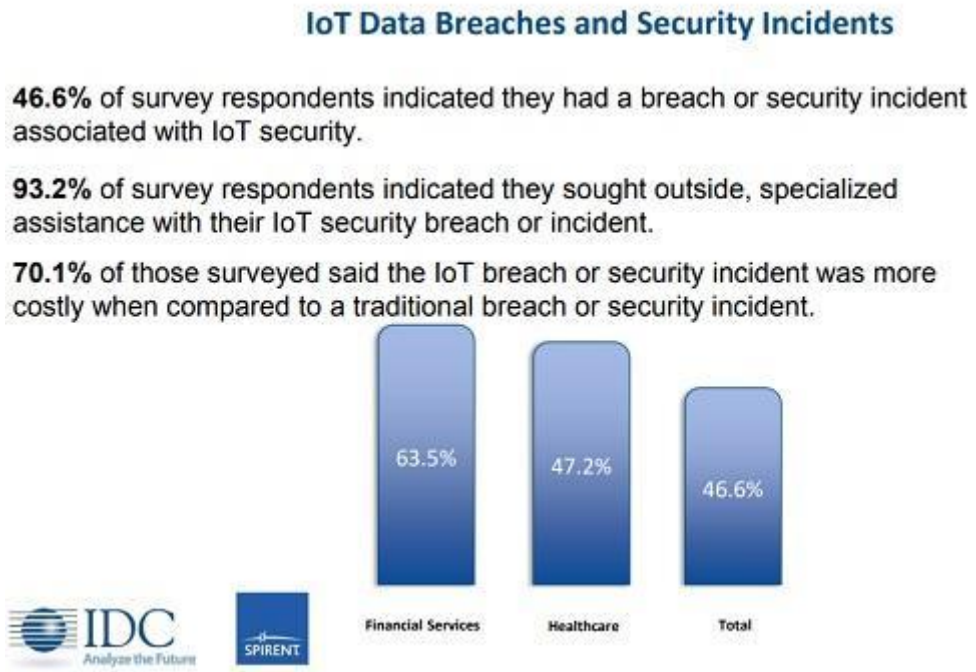
IoT 安全和公司规模

根据 Altman Vilandrie 的报告，在年收入低于 4.99 亿美元的公司中，物联网攻击导致超过一半的公司面临高达 25 万美元的经济损失。报告说，这对年收入低于 500 万美元的公司影响特别大，经济损失约占年收入的 13.4%。

同时，调查显示，九家年收入超过 50 亿美元的公司的损失至少达到 2000 万美元。

Altman Vilandrie 负责人兼报告作者之一的瑞恩·迪恩（Ryan Dean）表示："在我们的研究样本中，年收入超过 50 亿美元的公司只有 5%。总的来说，最大规模的企业遭受的经济损失可能会有很大的不同，这取决于攻击类型和影响。"

IoT 攻击成本 vs 传统攻击成本



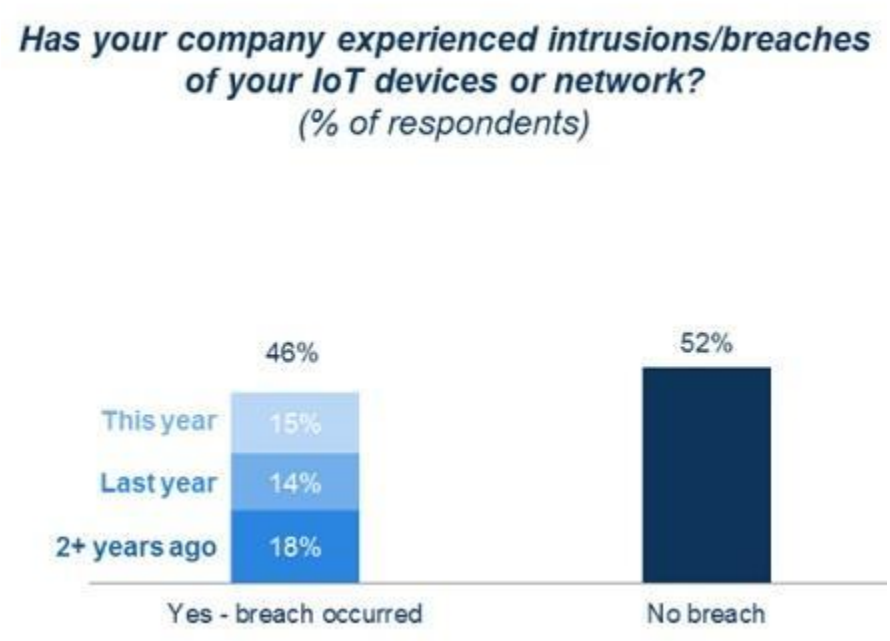
IDC 报告显示，将近一半（46%）的调查对象遭遇了物联网设备攻击。

IDC 信息安全分析师罗伯特·韦斯特韦尔（Robert Westervelt）表示："这远远超出了我的预期。IoT 还处于初期阶段，我预计这一比例会在 10%到 20%左右，而不是 46%。"

同时，近三分之二（63.5%）的金融服务行业受访者和近一半（47.2%）的医疗行业受访者表示，他们的组织经历了物联网安全事件。

由于绝大多数（93.2%）调查对象依赖于第三方服务机构或厂商（如物联网取证专家）帮助他们修复或评估物联网攻击事件，报告发现 70.1%的受访者表示与传统攻击相比，物联网攻击的成本更高。

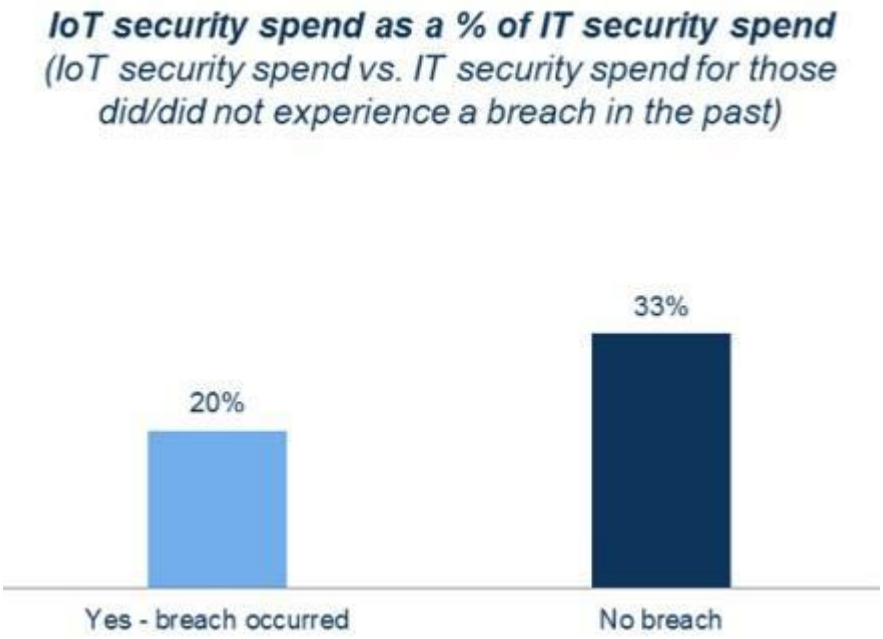
两年内 IoT 安全情况



在两年的调查时间里，46%的 Altman 受访者表示其物联网设备或网络遭遇了攻击。Altman 公司的迪恩表示，他对这一高比例感到很吃惊。

迪恩表示，首席信息安全官（CISO）应该意识到三大物联网安全隐患。首先是缺乏物联网安全投资，这可能会导致物联网攻击。其次是没有意识到物联网攻击不仅会损坏设备及其周围环境，而且还可能导致经济损失、品牌声誉损失和其他损失，如法律费用和争取客户的费用。第三点是，如果 CISO 不愿意将成熟安全厂商与 IoT 安全创业公司进行权衡比较，那么他们可能会面临风险。

投资回报率

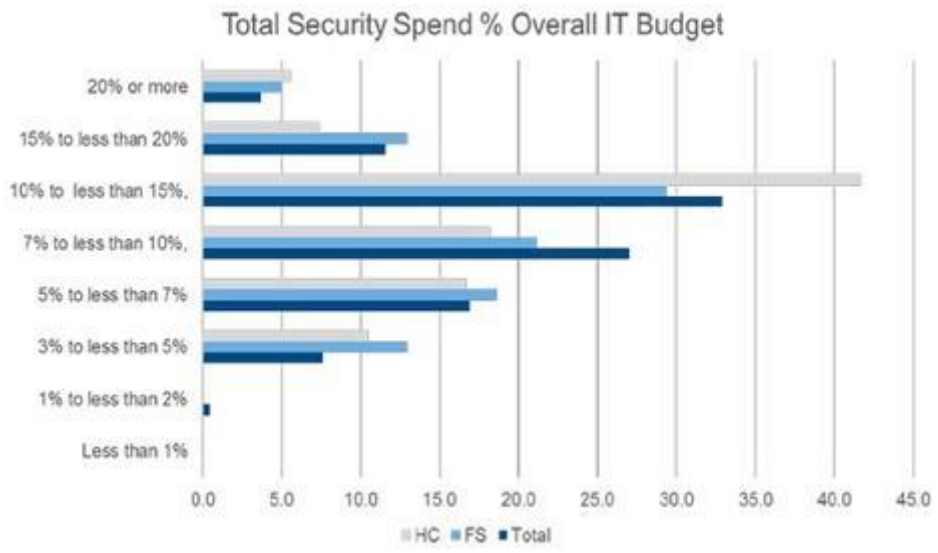


调查结果显示，将物联网安全纳入 IT 安全预算的公司更不容易遭遇物联网攻击。

报告显示，超过一半（52%）的受访者表示其组织在两年内没有遭遇物联网攻击，三分之一（33%）表示其 IT 安全预算涵盖物联网安全。在那些遭受了 IoT 攻击的公司中，只有 20%为 IoT 设备分配了预算。

迪恩说："IoT 安全投资较少的公司，在本案例中是 20%的 IT 预算，更容易遭受 IoT 攻击。相反，对 IoT 安全投资更多的公司，在本案例中是 33%的 IT 预算，更不容易遭到攻击。"

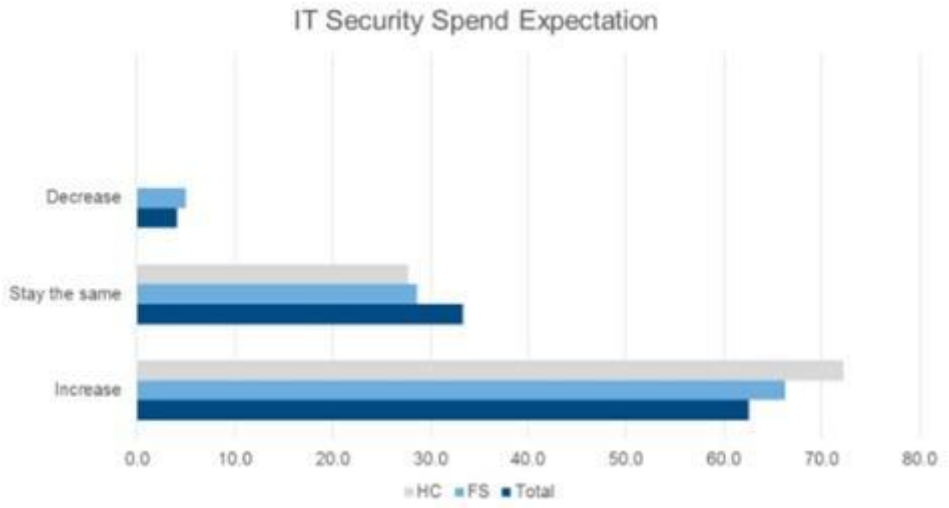
IoT 安全支出



IDC 发现，物联网市场虽然年轻，却在快速成熟，40％的受访者表示，他们的公司已经实施了六到十项物联网安全措施。金融服务和医疗机构预测，物联网安全成本将会增加。

IDC 的韦斯特维尔特表示，目前 IoT 安全占 IT 预算的 15％或更少。他指出，随着公司添加端点、网络和 Web 安全解决方案，他们将需要扩展到物联网环境中。

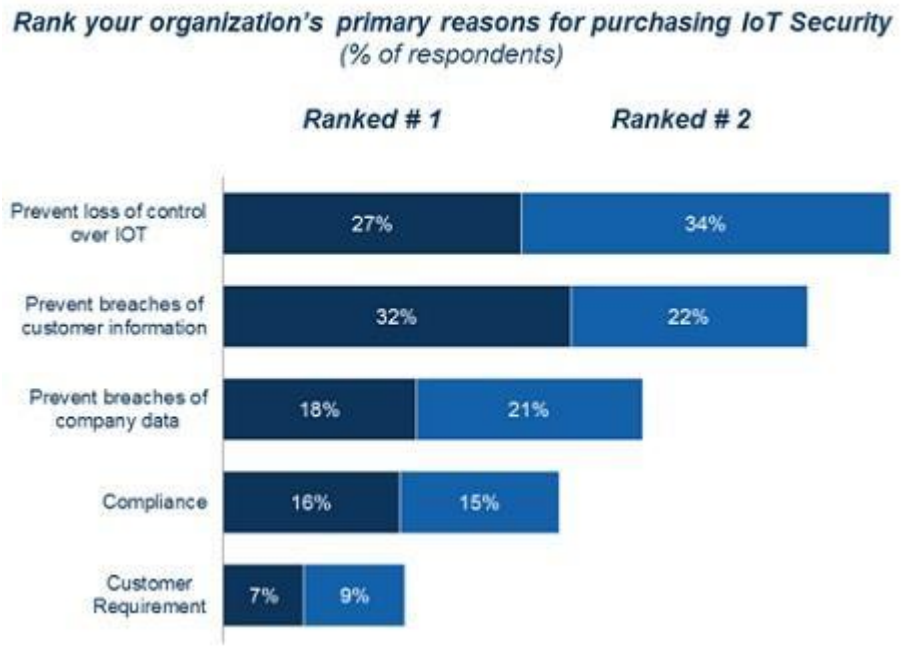
金融与医疗行业 IoT 支出增加



IDC 调查发现，62％的受访者预计 IT 安全支出将会增加。金融服务和医疗机构预测，他们将会采取安全分析、数据丢失预防和其他传统 IT 解决方案来减轻物联网风险。

韦斯特维尔特说："IoT 医疗设备使用传感器进行通信，医疗行业的很多 IoT 安全支出源于需要遵循合规性。"

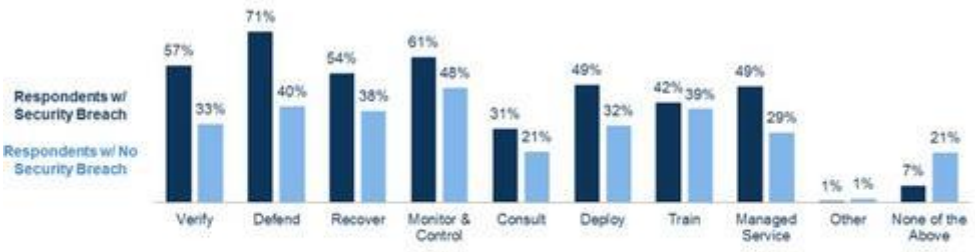
购买 IoT 安全解决方案的主要原因



根据 Altman Vilandrie 的报告，失去对 IoT 设备的控制是 IT 高管购买 IoT 安全解决方案的主要原因之一。迪恩说，这是由公共安全问题驱动的，例如吉普切诺基的远程控制。

排名第一的是 No. 1 原因（保护客户信息）和 No. 2 原因（失去对 IoT 设备的控制）的组合。在解释为何将这两个原因进行组合时，迪恩表示这样做是为了广泛地反映 IT 高管需要关注的重要问题。

IoT 安全解决方案购买清单



Altman Vilandrie 公司查报告结果显示，一家公司是否遭受了物联网攻击能够影响他们在未来一到两年内购买物联网安全解决方案的决策。

调查发现，在遭受了物联网攻击的企业中，71%将“防御技术”列为他们在未来几年内最想要购买的解决方案。对于尚未遭受物联网攻击的公司而言，最想要购买的 IoT 安全解决方案是监控和控制产品。

“我们认为，购买‘防御产品’是一种应对型措施，”相关专家表示，“这些受访者已经遭遇了物联网攻击，尚未部署足够的安全防御解决方案。相反地，其他受访者可能已经部署了良好的安全方案，他们更加注重购买‘监控和控制产品’来管理端点和系统。”