6 网络安全

从互联网APP到胰岛素泵，医疗设备正越来越多地连接到互联网。到2020年，连接到互联网的医疗产品的经济价值预计约为2850亿美元。[32]但互联网的方便快捷并不是没是代价的－它极易受到黑客和犯罪分子的攻击。

由于安全漏洞变得越来越普遍且系统维护成本越来越高，医疗设备的网络安全将在2016年成为一个重要问题。这便要求设备厂商和医疗机构采取先发制人的措施，以维护消费者对医疗设备的信任，并防止任何可能对医疗行业造成破坏的黑客行为。

这并不是空穴来风。2015年政府曾对此做出了第一次警告，认为医疗设备易于受到黑客攻击。一位输液泵的官员警告说，该类设备可能会被远程修改，以输出致死剂量的药物。[33]医疗器械被黑客入侵，其后果将是灾难性的：患者可能因为设备的原因受到伤害甚至死亡；设备可能会允许其他医院和医疗供应商网络的不当访问；商业价值巨大的研究数据也可能会被从临床试验中使用的设备中偷走。

监管机构已对此进行了风险通知。FDA已发出关于网络安全的警告和指导性文件，并表示希望(但不强制要求)医疗设备制造商和医疗供应商只确保“受信任”用户对设备的访问。34此外，FDA还要求将网络安全漏洞进行及时地纠正和报告。35

虽然至今还没有出现因设备被黑而导致患者受到伤害的事例，但最近从保险公司到零售商的一系列遭遇来看，黑客入侵会使相关机构遭受诉讼、收入损失和名誉损害之苦。2014年，约85%的大型医疗机构经历过数据泄露，其中的18%修复费用高达1亿美元。[36]

“归根结底，这关乎于网络体系结构和设计，”Armor Inc.的首席安全官、退役上校Jeff Schilling说道，“医疗设备需要有其单独的网络。如此一来，即使黑客黑进了设备系统，也不能很快造成伤害。”

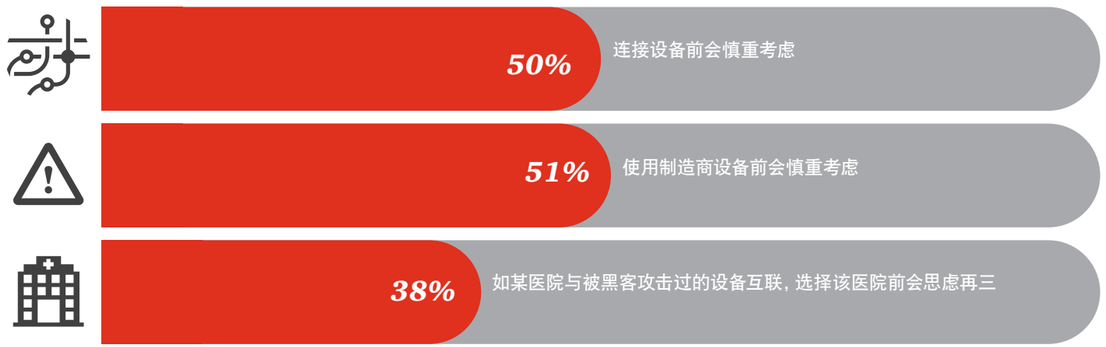
网络安全状况不佳会给医疗系统和设备制造商带来巨大的损失。(见图5)。62%的消费者表示，比起设备的易用性，他们更在乎设备的安全性。[37]那些没有内嵌安全功能的设备，特别是面向消费者的APP或可穿戴设备，可能会在竞争中处于不利地位。

影响：

- 设备制造商应先发制人。企业应定期对设备漏洞进行评估，并制定激励政策，鼓励“白骇客”，即安全研究人员查找并报告未知漏洞。银行业在这方面树立了良好的榜样：他们开发了数据提交协议，即专门为每一种产品与流程设置安全协议，并限制设备连接范围。[38]如果医疗行业不能捍卫设备安全，则监管机构可能会介入其中。
- 对供应商而言，网络分离与设备管理至关重要。供应商应及时更新设备，并为设备安装防火墙，且设备连接的网络应与关键医疗数据和个人数据网络相互独立，并限制医疗设备的用途(这样做会给设备互操作带来严峻挑战)。密码管理也是一个不容疏忽的问题。医院通常不会修改默认设备密码，这让入侵设备变得轻而易举。很多医院根本不知道哪些设备正在为医院医生所使用。
- 新兴公司具备更大优势。可靠的安全协议是出售产品和服务的一大优势。从一开始便采用最佳安全实践的新兴企业可省去高昂的设备更新费用，故而占得市场先机。制药公司通过APP促进销售，因而一旦出现设备被黑事件，其销售额、名誉与患者可能遭到十分消极的影响。
- 监管机构同样是黑客攻击目标。政府也需要维护自身设备安全。人力资源管理办公司数据泄露可能会置无数员工记录于风险中。同理，监管机构数据一旦被窃，也可能会对众多设备与其用户造成巨大威胁。[39]

设备被黑将导致客户流失

一旦某医疗设备出现过被黑事件，消费者对连接该设备通常都十分谨慎



来源：普华永道2015年度HRI消费者调查

Megan Haas

普华永道香港法务会计服务合伙人

随着网络安全漏洞的发生率和所造成的损失越来越大，医疗领域的网络安全在2016年将在全球范围内成为一个重要话题。

例如，针对网络的破坏行为将成为一个重大挑战。很多人认为，这样的破坏比网络犯罪和网络间谍有更大的威胁，因为它很难通过传统的网络安全防范措施来阻止。

越来越多的人开始相信，医疗设备制造商在网络安全方面必须具有一定的前瞻性。在中国，网络安全在很多时候并没有完全跟上制造业技术的高速发展。制造商和供应商为了实现新的产品理念，在很多时候把安全和隐私放在了次要的位置。然而，我们有必要作出改变，不仅仅只关注网络安全事件的事后的应变，更要让网络安全成为产品战略的核心要素。

根据普华永道2016年全球CEO调查，许多CEO对网络安全漏洞表示了关注。然而，他们中的很多人并没有意识到，网络安全也可以成为他们业务战略的一个优势。

在中国，医疗健康领域的网络安全已经引起了政策制定者的关注，并在今年的全国人大和政协会议（即“两会”）上成为议题之一。

两会代表们认为，政府需要加大对于患者信息安全的监管力度，包括医疗大数据背景下的患者隐私保护以及明确电子诊疗档案的归属权。同时，政府应当在医疗数据安全保护方面投入更多资源并增加预算。

普华永道认为，网络安全的重点在于设计方面。优秀的网络安全措施是扎根于产品理念并始终贯穿于整个产品设计和制造过程中，而不仅仅是一个独立于产品之外的附加部分。这样的设计理念需要企业从高管层面发起和推动。