勒索软件：我们如何爬出泥沼

付佳伟，海洛德·辛博贝，徐文渊，闫琛

医疗信息安全专家呼吁，医院必须像预防和治疗疾病一样确保医疗设备与信息系统的高可用性，因为勒索软件只是表面症状，而非根本病因。

以 WannaCry 勒索软件为例的计算机恶意软件严重地扰乱了临床工作的连贯性。美国国土安全部就此事件发布警报，受该勒索软件漏洞影响的医疗设备产品多达数十款，包括肿瘤放疗设备、移动式 X 线摄片机、超声检查与麻醉监护设备等。虽然该恶意软件在世界范围的传播因为一位好奇的 22 岁年轻人花 11 美元注册了一个域名而暂时停止（并非玩笑），下一轮攻击仍然会在毫无预警的情况下再次发生。

勒索软件本身并非造成我们面前问题的罪魁祸首，它是我们医疗基础设施中固有的设计缺陷所表现出来的症状。这些问题的根源是充斥着老旧医疗设备软件的脆弱的基础设施。

当我们了解了一种疾病之后，我们只是看看新闻然后希望自己永远不要得病吗？不是的，我们接种疫苗，避免前往高危地区，洗手，在与病原携带者接触后立刻寻求医疗帮助。总之，我们为了风险管理而未雨绸缪。

所以，什么策略可以有效地规避医疗设备信息安全风险，保护临床操作不再被恶意软件干扰？

只是采用新技术并不是答案。把不可维护的旧电脑换成不可维护的新电脑同样也不是答案。一套有效的方法必须顾及医疗供应链的五个核心部分：制造、采购、法规、培训、监管。

首先，医疗设备生产商必须设计在网络安全风险下也能够保持安全有效运行的医疗设备。美国食品药物管理局已经认可了 AAMI TIR57 等相关社会标准和最佳实践，在医疗设备的设计环节构建信息安全。微软公司在计划淘汰 Windows XP 系统的第一天就警告了设备生产商。事实上，该操作系统被终结的命运在多年前就已经非常明确，其后的危险已被预先警告过。尽管设备生产商可能卖出了不可维护的产品，医院在购买它们的时候同样犯了错误。医院积累了数十年的老旧设备，却没有财政机制来淘汰这些无法确保安全的设备。

医院在做出采购决定时应当将网络安全作为重要因素进行考虑，并参考例如梅奥医学中心发布的网络安全“厂商名录”这类采购实践。医疗设备应该配备软件物料清单以便医院做出基于风险的采购决定。医院需要通过更好的服务合同来购买和维护更好的设备——他们需要跟踪到库存设备的端口数量、以太网 MAC 地址和软件版本以更好的管理风险。设备生产商需要向供应商提供将医疗设备序列号与 MAC 地址映射的数据库，使基于网络的库存跟踪成为可能。

政府应该考虑建设一个国家试点医院，进行医疗基础设施的网络攻击承受度测试。类似汽车制造业的汽车耐撞性测试，消费者从这类测试中可以了解产品的风险。尽管对于患者来说，有医疗设备远比没有更安全，患者和医院有权利在使用和购买一套医疗设备时了解他们所需要面对的风险。

监管机构必须考虑到恶意软件的非地域性问题，即它们不受国境的限制。相同的核心网络安全问题无处不在，不同国家的医疗信息技术日常运作出乎意料地受相似的计算安全难题困扰。医疗设备监管机构，例如美国的 FDA、英国的 MHRA 和中国的 CFDA，需要拥有知情权威和立法职权来保证医疗设备在网络安全威胁下保持安全有效。

谁该对这些问题负责？谁处于经济原因有动力解决这些问题？不幸的是，正如我们最近在勒索软件上的惨败所揭示的，去应对安全根本问题的人并不具被足够的能力。政府可以强制淘汰无法确保安全的设备和操作系统，并由卫生与公众服务部的民权事务办公室评估处罚（以美国为例）。

如果没有连贯合理的监管策略，我们与受暴利刺激的国际犯罪分子的斗争将会是旷日持久的败仗。例如，英国的《刑事司法法》假定信息技术不会出现安全错误。这种欠妥的法律敞开了误导诉讼的偏门——出于好意的医生和护士却要为医疗系统和设备自身的缺陷担负法律责任。立法本应推动厂商生产安全可靠的医疗设备，而不是处罚那些向厂商和监管机构合情合理地报告问题的无辜的医护人员和患者。

人力短缺一直是网络安全的巨大阻碍。计算机科学专业的学生很少会选择在医疗领域工作。需要注意，计算机科学的学生在帮助改进医疗卫生行业上能够起极大作用，特别是生物医学工程双专业是很好的选择！设备厂商和政

府应该通过提供卓著的研究生奖学金将最优秀的学生吸引到这个领域，这样厂商、医院和政府就能够填补他们在网络安全方向上的职位空缺。

最后，医院亟需有效的监管体系以控制医疗设备的软件安全风险。一个医院应当指派一位管理高层，全权、全责负责包括生物医学工程与信息技术部门的网络安全，并拥有预算支持，实现对医疗安全的保障。

没有任何医疗设备是绝对安全的，但一个医院在遭受网络攻击后应该正常恢复，而不是承受数天的全系统中断。在任何时候，患者都不应该被迫怀疑医疗卫生服务的可用性与可信性。安全只是为了实现目标的一条途径，而那个最终的目标就是安全、有效的医疗卫生服务。

勒索软件近期在全球范围的爆发只是症状，是时候该我们采取建议和行动来改进制造、采购、法规、培训、监管这些环节的网络安全了。除非网络安全意识已经变成了像洗手一样的第二天性，否则网络安全问题的发生频率与影响只会有增无减。

如果说这次事件能够给我们一丝慰藉的话，也许就是促使厂商、医疗卫生组织和政府开始战略地思考如何改进医疗信息安全，而不再只是被动的应对了。

付佳伟博士，现为医疗网络安全公司 Virta Laboratories 的首席执行官和首席科学家，以及密歇根大学阿基米德医疗设备安全中心的主任。

海洛德·辛博贝博士，现为威尔士斯旺西大学计算机科学教授。他是皇家内科医学院的荣誉院士，研究医院信息技术问题。

徐文渊博士，现为浙江大学电气学院教授，博导。

闫琛，现在为浙江大学电气学院博士生。