**升级对数据安全的认知 | 医院数字化转型路线图 (五）**

吴恒 / 健康界

数据安全只有起点，没有终点！

医院数字化转型后最大的资产就是数据，同时也意味着要面对更大的数据安全风险！对于任何组织来讲，安全和效率都是一对矛盾，解决这一矛盾的关键在于找到一个平衡点，在保证安全的情况下兼顾效率，这也是医院数字化转型必须要面对的一项挑战。

下面就从外部和内部两个方面来谈谈医院数据安全面临的挑战。

**医院数据安全的外部挑战**

医院数据安全的外部挑战主要是防范攻击和应对风险，保证数据和业务的连续性。

**一、一张地图——安全作战地图**

具体要从哪些方面开展数据保护工作？华为的安全作战地图值得借鉴，总结起来即“五不两可”。“五不”是指攻不进，看不见，看不懂，拿不走，毁不掉，“两可”指的是可追溯和可恢复。具体来讲就是：

“攻不进”，是指采用防火墙等边界防护技术使外部攻击无法入侵医院的系统，并且在发现入侵时立刻阻断。

“看不见”，是指采用深度隔离和动态脱敏技术，即便万一发生不合规访问，访问到的数据也是脱敏后的数据，使攻击者看不到医院核心数据和患者的隐私数据。

“看不懂”，是利用加密和伪装技术对核心数据进行处理，即便攻击者看到了某项核心数据，也不会认为这项数据很关键。

“拿不走”，强调的是防御系统能时刻感知数据资产的异常，一旦感知到数据有被转移或者挪动的情况，立即启动阻隔程序防止数据被盗。

“毁不掉”，是针对比较敏感的操作命令（比如删除、修改等）进行实时告警与阻隔，防范勒索加密，防止误操作、恶意操作造成的严重后果。

“可恢复”，是信息安全的最后一道防线，一旦出现网络安全灾难性事件或者数据丢失以最快的速度恢复数据，确保业务的稳定运行。数据库复制、数据实时保护和传统的定时策略备份，三种手段共同组合成医院的数据灾备解决方案。

“可追溯”，是指医院要建立一套溯源机制，发生数据泄露事件后，利用水印技术来确认哪个环节发生了泄露并进行追责。

**二、一个安全观——“知白守黑”**

“知白守黑”来自《道德经》，原文是“知其白，守其黑，为天下式”，这个观点是某数据安全企业在应对防勒索病毒时提出的。该企业负责人柳遵梁的原话是这样的，“我们不关心病毒的特征，勒索病毒没什么特征，就是正常的应用。我们是把在服务器上运行的应用进行特征化，不符合这个特征的就是不正常的。通俗来讲就是‘知白守黑’。”首先对正常的访问进行特征化分析，建立用户访问数据的规则，然后根据规则建立白名单体系并设置好访问路径，在白名单体系之外的访问全部阻断。“知白守黑”就是不纠缠于外部攻击的多样性，只专注于外部访问的合规性，变被动为主动。疫情防控中健康码的应用就是典型的“知白守黑”，把健康码异常的挡在门外，只允许正常的进入。

**三、一个提醒——紧急情况下的数据安全**

医院特别要注重紧急急情况下的数据安全，比如突发的公共卫生事件、突发的极端天气事件。2021年7月20日河南郑州突然遭到特大暴雨，市内多家医院不同程度受灾，其中有数据中心机房被淹的情况。此类情况下恢复数据和系统运行是当务之急，但越是紧急越是不能忘记数据安全，特别是抢修时给外部人员开通的特权账户，一定要进行权限控制并在抢修完成时及时收回。

**医院数据安全的内部挑战**

医院数据安全的内部挑战主要是建立内部使用者的管理体系，保证数据采集、处理、利用各环节合规合法，重点防范使用者用合法身份去做不合规的事情。

**一、与时俱进的制度建设**

各家医院都有关于信息网络安全的制度，但是在实际工作中还存在对于制度建设不重视的情况，要么制度知晓率不高导致制度上墙不落地，要么制度更新不及时跟不上形势变化，要么制度执行缺乏奖惩不具备震慑力。

数据安全管理体系的前提和基础是系统完备、科学规范、运行高效的数据安全制度体系，为此要注意以下三点：

一是制度更新的及时性。密切关注数据安全领域的新动态，及时补充、修订和完善新制度，及时废止已经过时以及与国家新规定相抵触的制度。

二是制度发布的全面性。利用新媒体、自媒体和医院内部办公软件发布数据安全制度，提高制度的知晓率，做到日常工作中使用者可以随时查阅以便执行。

三是制度执行的严格性。对于“不准”或“禁止”类目标要求，配以相应的处罚机制，增大违反制度的成本和保证制度的执行力。

**二、敏捷动态的权限管理**

敏捷动态的权限管理就是保证相应类型相应级别的使用者，在相应的数据区域内进行合规访问，防范他们用合法身份去做不合规的事情。医院内部人员根据数据使用权限可以分为三类，一是数据管理者，包括数据库管理员、安全管理员、审计管理员；二是数据生产者，包括医护人员、医技人员、医疗辅助人员（后勤、财务）；三是数据维护者，包括运维人员、病案管理人员、医院各级管理者。

针对以上三类人员的工作性质，细化权限管理，保证每个权限都有固定访问的数据区域和数据类型，防止越级使用和跨界使用。比如运维管理人员只能访问运维体系内的日志性数据，无法访问业务数据；同样，业务部门人员只能访问业务数据，没有其他数据的访问权限。特别要注意对离职人员权限的收回，消除利用此类权限进行非法访问的隐患。

**三、融入血液的安全意识**

实际工作中，职工经常出现这样的行为：不小心点击垃圾邮件中的恶意链接、使用脆弱的密码、访问不安全的网站、提取数据时不注意保护患者隐私等等。因为教育不到位，许多人根本就没有意识到这样的行为存在安全隐患。

我一直认为，只有加强数据安全教育，才能提升数据安全防范意识，树立融入血液的安全意识。

数据安全教育要树立“人人参与 人人有责”的理念，数据安全不仅是领导的事，不仅信息部门的事，更是每一位使用者的责任。

数据安全教育要与时俱进，照本宣科式的宣讲效果不大，多利用数据安全典型案例、数据安全周报、情景重现式短视频等形式，普及数据安全最佳实践，防范技能知识点和数据安全新动态。

**数据安全的认知升级**

爱因斯坦说过，问题不可能由导致这种问题的思维方式来解决。面对瞬息万变的数据安全威胁，只有改变固有思维方式进行认知升级才能以不变应万变。接下来谈谈三个数据安全的认知升级。

**一、没有绝对的数据安全**

没有绝对的数据安全，只有相对的数据安全，数据安全是一种以安全为目标的持续的不均衡过程。持续的不均衡是凯文·凯利在《失控》一书里提出的一个概念。什么叫持续的不均衡？以走路为例，我们都有这样的经验，单脚立地的时候不好保持平衡，但走路时感觉很稳定。走路其实就是一个个单脚着地瞬间的连接，只不过这种不均衡由于两条腿着地的周期很短，我们意识不到而已。

数据安全也是这样一种追求安全的持续的不均衡过程。不断变化的业务场景迫使你调用既有的安全认知和技术来应对，当发现既有的认知和技术不足以应对时就要进行升级，如此循环往复保持一段时间内相对安全。

只有持续投入才能保证比攻击者快半步，就可以为自己争取一段时间，利用这段时间把未知的风险转变为已知的风险，再去寻找抵御风险和提升防御能力的方法。

**二、数据安全要有系统化思维**

航空界关于飞行安全有一条经典法则——海恩法则，即每一起严重事故的背后，必然有29次轻微事故和300起未遂先兆以及1000起事故隐患。

这条法则同样适用于数据安全。对于医院核心数据的攻击也有大量的先兆，人们感觉不到是因为这样的攻击分布在边缘业务或者非核心数据上。因此数据安全要有系统化思维，必须系统化作战，只确保核心数据资产的安全是远远不够的，必须要形成一个系统，把与患者、合作伙伴、供应商等对接的账号等周边最容易被忽略的元素全部纳入进来，实行系统化防范。特别注意外包服务相关系统的防范，黑客攻击的突破点往往是安全防范力量最薄弱的地方。

**三、数据安全最重要的是人**

对于数据安全，不少医院的管理者一直以来都有一个错误的认知，认为只要购买安全设备就能做好数据安全。殊不知数据安全最重要的因素是人，再好的设备和系统如果交给能力不足的人，使用效果会大打折扣。这就是我们常说的拿着AK-47当烧火棍来用。

检验这个认知误区的方法很简单，只需问一个问题。如果有两个选择，一个是花费数百万买一套安全设备，一个是花费一万培训数据安全工程师，请问怎么选？

改变这个认知误区需要从两个方面入手。

一方面，厂家要加强对医院信息部门人员的技术培训提高使用者的能力，工欲利其器必先善其事。

另一方面，医院要加大对数据安全工程师培训的投入，建立起一支技术过硬的信息安全技术队伍，随时应对可能出现的安全挑战。

医院数据安全始于与时俱进的制度建设，行于敏捷动态的安全体系，成于不断升级的安全认知！

数据安全只有起点，没有终点！

*本文作者吴恒是河南大学淮河医院党委委员、党办主任，中国研究型医院学会医疗信息化分会青年委员会副主任委员，河南省医院协会人工智能与临床大数据管理分会副秘书长、常务委员。曾获第四届中国行业互联网大会“2018年度中国优秀CIO”、2017-2018年度（第三届）中国医药健康信息化十佳CIO。*

本文为健康界原创，任何机构或个人未经授权均不得转载和使用，违者将追究法律责任！