证券代码：002415　　证券简称：海康威视　　公告编号：2015-009 号

杭州海康威视数字技术股份有限公司

关于投资者电话会议沟通情况的相关说明暨复牌公告

本公司及全体董事、监事、高级管理人员保证公告内容真实、准确和完整，没有虚假记载、误导性陈述或者重大遗漏。

特别提示：公司股票将于 2015 年 3 月 3 日开市起复牌。

2015 年 3 月 1 日晚间，杭州海康威视数字技术股份有限公司（以下简称“海康威视”或“公司”）发布了《关于部分监控设备遭到网络攻击的情况说明》的公告，就近日部分媒体出现关于公司的相关报道进行说明。

为了对部分监控设备遭到网络攻击的事项作出进一步说明，保护投资者权益，保证公平信息披露，公司申请了自 3 月 2 日开市起股票临时停牌。

公司于 2015 年 3 月 2 日 9:45-11:00 在公司会议室召开了投资者电话会议，就部分监控设备遭到网络攻击的事项（以下简称“江苏事件”）作进一步沟通和说明。公司总经理胡扬忠，副总经理、董事会秘书郑一波，HSRC（安全应急响应中心）负责人工程师万里；国家互联网应急中心浙江分中心技术保障处副处长厉斌，工程师马骏野出席了会议。

经公司申请，公司股票（证券简称：海康威视，证券代码：002415）于 2015 年 3 月 3 日开市起复牌。

现就电话会议中投资者主要关心的问题进一步说明如下：

1、江苏省公安厅科技信息化处发文《关于立即对全省海康威视监控设备进行全面清查和安全加固的通知》中仅海康威视被点名，其他同类视频监控厂商是否也存在相似问题？

公司已在 2015 年 3 月 1 日晚间通过公告披露了相关情况。至于其他厂商是

否存在相似问题，公司并不了解，但暴露在互联网环境下的产品都有可能受到网络攻击。

2、江苏事件中暴露出来的设备安全问题，是否通过修改密码或者固件升级就可以简单解决，还是需要召回设备？另外，公司产品型号众多，解决问题的工作量是否很大？

江苏事件涉及的设备安全问题为弱口令漏洞，确实只需通过修改初始密码或简单密码，或者升级设备固件即可解决，并不需要召回或更换设备。

针对江苏事件，公司已组织专项应急技术团队帮助各地市公安局进行口令修改和固件升级工作。其实，类似的工作并不需要现场进行，可远程进行固件升级。

尽管公司的产品型号很多，但分系列管理，通常一个或几个系列产品使用同一类固件，因此升级固件的工作量并不大。

3、除了江苏省厅，是否有其他省公安厅会出现类似情况？

首先，江苏事件中流传在网上的图片是江苏省公安厅的一个通知，要求各地市公安局对设备进行排查，并不是正式文件。截至目前，公司并没有收到其他省公安厅或者其他客户的类似要求。如果今后有这样的需求，公司也会积极配合。

海康威视是一家负责任的公司，今后会更加主动和用户进行沟通哪些固件需要升级，哪些安全措施需要注意。

4、昨日公告指出，去年 8 月起海康威视产品就已遭到黑客攻击，而江苏省公安厅为何在 2 月才发文要求清查？

去年 8 月海康威视部分监控设备受到了网络攻击（以下简称“8 月事件”），公司认为是针对海康威视产品的恶意攻击行为，9 月 2 日公司已向属地公安局报案，公安机关立即立案侦查。但由于黑客使用的服务器在海外，攻击仍在继续，至今并无惩治措施。江苏事件中也有指出“设备被境外 IP 控制”（即攻击设备的服务器在海外），公司认为此事是 8 月事件在江苏省的呈现，监管部门发布电文要求排查也是其常规工作内容之一。其实，江苏省公安厅在 2 月 16 日通知了公司相关情况，公司支持省厅的行为，认为清查设备升级固件本身是对用户和厂家

来说很好的事情。

现在来看，8 月事件发生之后，虽然公司认为实际影响不大，但如果公司立即披露安全公告的话，可能对整个产业链的发展更好。

5、请问国家互联网应急中心浙江分中心的专家，弱口令问题是不是常态？

（国家互联网应急中心浙江分中心技术保障处副处长厉斌回答纪要）

我整体的看法是这只是一个网络安全事件，是信息化发展的产物。现在的视频监控设备相对计算机来说比较简单。据我中心统计，在过去的一周内，全国计算机感染病毒 62.6 万台，其中蠕虫病毒 11.4 万台。视频监控设备在互联网化后也需要面对这样的问题，需要企业和用户共同努力。企业需及时发布漏洞修复工具，病毒查杀工具，用户也需要主动更新固件。

海康威视自去年开始和我中心开展了相关合作，这次的弱口令漏洞也委托我中心在网上进行监测。海康威视作为业界龙头企业，对于产品安全的防范措施还是超前的。这次的事件，可能是公司产品销售范围较广，无法及时通知到所有用户进行密码修改或固件更新。

6、有外媒报道，海康威视有 31%设备被攻击，光江苏省就有 5 万多台。另有媒体报道，公司有数万设备中招，这是怎么一回事？

关于外媒报道，公司没有收到相关信息，不好评论。

至于媒体报道的“数万台设备中招”，是指从去年的 8 月事件至今，因为弱口令问题而被攻击的公司设备，这些设备的总数不超过 10 万台，且被感染的设备皆有通过线上和线下进行修复。

7、公司昨日公告中说明 2014 年 3 月底以前出厂的设备才有漏洞，但最近网络上“凯奇哥”视频演示的却是 2014 下半年的设备，这是什么原因？

江苏事件和 8 月事件涉及的都是弱口令漏洞，至于网络视频涉及的则是 RTSP 漏洞。这是两个完全不同的漏洞，而昨日公告主要是针对前者的相关说明。

至于 RTSP 漏洞，公司安全应急响应中心已于 2014 年 12 月 5 日披露了安全公告，进行安全预警，并同时发布固件升级程序。升级固件可以修复该漏洞。

8、公司 2014 年 12 月 5 日在官网公布 RTSP 漏洞，是否是一个常规做法？公司是想让用户升级固件，但同时黑客也获取了漏洞信息，更方便攻击没有升级的设备。

在公司官网发布安全公告是 IT 行业的国际惯例。至于后面提到的问题，基于安防行业产品的特点，公司不知道最终用户在哪里，即使在 HIKDDNS 上能查询接入设备的 IP 地址，也不能代替用户远程修改密码，只能在用户要求下帮助用户远程进行固件升级。目前来看似乎还没有更好的方式。

9、此次江苏事件对公司业务有何影响？国内政府采购订单是否会放缓？

从目前来看，这次事件对公司的品牌和声誉是有一定影响的，但对公司整体业务无实质性影响。至于是否会影响国内政府的采购趋势，目前公司并未得到相关部门的看法。公司产品主要应用于专网、局域网，接入互联网产品数量很小，因为接入互联网的用户主要是小微企业，大型企业一般有内网。由于目前没有确定的统计口径，所以无法披露接入互联网产品的比重，但预计不超过 10%，而其中受到攻击的设备比例更小。

公司认为，江苏事件发生在海康威视身上，将为整个产业带来更多积极影响，因为这些问题在整个行业都存在。厂商需提高产品安全意识，安装商、集成商也应该在安装设备后及时修改初始密码，优化基础的 IT 网络设计，合理配置路由器、设置网管，最终用户也应加强使用初始密码的危害性意识。

10、海外媒体也有报道，是否会对出口有一定影响？

公司已通知海外销售关注当地新闻，也有和海外的专业媒体沟通，坦诚本次事件的真实情况。是否影响出口暂不得知。

11、对于加强网络安全建设，海康威视对此有何具体措施？

2014 年 3 月，公司已成立安全应急响应中心（HSRC），负责接受、处理和公开披露公司产品的安全漏洞。同时，也主动与行业专家、实验室发起合作，例如国家互联网应急中心、杭州安恒信息技术有限公司等，旨在进一步加强网络安全

建设，推动公司上下对产品安全问题的关注。公司多次邀请互联网安全专家对员工进行培训。此外，公司近期也将启动优化研发管理流程的项目，加强研发人员的产品安全意识，针对研发和测试的每一个环节进行优化。

在中国 IT 企业国际化的过程中，必然会面对产品安全问题，如华为在打入欧洲市场时，路由器曾被攻击。这次的事件对于公司是危机也是转机，公司也将以行业巨头为榜样，坦然面对，在探索中坚定地走下去。解决产品安全问题是一项永久的课题，但公司将以此为契机，在 2015 年走上一个新台阶。

12、海康威视旗下萤石系列产品有没有遭受到网络攻击？

目前公司还没有收到萤石系列产品出现安全问题的消息，但黑客行为肯定存在，因为自萤石服务器建立以来，一直有监测到被网络攻击。

13、产品接入萤石云，是否对设备安全性的提高有帮助？

应用在专网或者局域网上的产品，固件升级需要用户主动完成。而萤石系列产品拥有手机推送功能和/或设备信号灯提示功能，固件升级等安全信息更容易获取，从这个角度来说，产品接入萤石云确实对安全性能的提高有帮助。

目前公司已在新加坡建立萤石云平台，欧洲则正在进行，计划未来将在海外 6 处构建萤石云平台。

产品暴露在互联网上的风险比接入专网和局域网中高很多，因为在互联网上的设备易遭到远程攻击，而后者环境封闭危险不大。在互联网环境中，萤石云可以帮助与用户沟通，及时修复漏洞。

14、萤石产品在弱口令问题上的安全性很好，有 2 个密码：用户本地有个密码，查看视频有个密码。海康威视的其他产品是否有能做到这样的安全防范措施？

针对不用的网络应用，有不同的解决策略。近期会重新梳理和评估海康威视的安全策略，可能会在海康威视部分产品上取消通用密码。

15、在产品互联网化过程中，海康威视和其他互联网公司相比，有何优劣

势？

做一个产品要考虑方方面面，网络安全问题只是其中一个环节。海康威视的行业产品从专网、局域网做起，公司对互联网所带来的风险意识还不足。2013年公司成立萤石团队，用互联网的架构来规划产品和平台。凭借公司在视频监控领域的经验，公司相信可以取长补短，做好产品互联网化。

特此公告。

杭州海康威视数字技术股份有限公司

董 事 会

2015 年 3 月 3 日