网络安全保障做法

2022-2025年
研究期

第3/2号课题

保护信息和通信网络：发展网络安全文化的最佳做法

2023年中期交付成果

内容提要

2022年在基加利召开的世界电信发展大会审议了侧重于分享网络安全实践经验的第3/2号研究课题的职责范围。网络安全威胁是全球关注的一个重大问题，对技术的依赖性日益加大导致网络攻击风险和后果的升级。网络安全保障做法已成为保护网络、系统和数据免受恶意活动干扰的关键因素。

本报告反映了第3/2号课题会议以及网络安全保障做法专门讲习班的文稿和讨论意见。以下介绍讨论的六个关键要点：

1. 不同程度的危急性和风险需要不同程度的保障。风险评估有助于确定适当的保障水平，同时考虑到受保护数据和资产的敏感性、违规后果以及威胁环境。
2. 与合作伙伴组织、行业和利益攸关多方进行接触是推动网络安全保障的有效途径。政策制定机构、民间团体组织和业界之间的合作可以促进对安全和信息政策及监管发展的需求。
3. 考虑通过对话和磋商实现不断演进的知情监管方式。网络安全保障做法在成为强制性措施之前可自愿引入，这取决于为防止网络攻击是否有必要采取更有力的措施。
4. 鉴于动态的威胁格局和不断演进的网络安全风险，网络安全保障做法应不断得到重新审视和随着时间加以调整。定期的内部审计和订阅威胁情报被认为是好的做法。
5. 正在努力向消费者和制造商宣传网络安全的重要性以及选择更安全的产品的好处。网络安全标签方案和意识宣传活动可以帮助用户了解技术产品的安全性。
6. 互惠协议有助于缓解跨多个市场操作的行业参与方的合规性，同时统一基本安全要求可减轻产品和服务提供商的监管负担。

引言

2022年6月在卢旺达基加利举行的上届世界电信发展大会上，审议了第3/2号课题“保障信息和通信网络的安全：培育网络安全文化的最佳做法”的职责，其中一个具体研究问题为“分享网络安全保障的实践经验”[1]。

经批准的第3/2号课题的职责范围认识到，网络安全威胁仍然是全球各国政府、组织和个人关注的主要问题。随着对技术的日益依赖，网络攻击的潜在风险和后果也在升级，且网络攻击也越来越有利可图[2]。网络罪犯经营着一项利润丰厚的业务，据估计，全球耗资8万亿美元[3]。

网络安全保障做法[4]已成为保护网络、系统和数据免受恶意活动干扰的关键因素。这些泛指用于确保保护电子设备、系统、网络和数据机密性、完整性和可用性的相关控制程序。虽然它们不直接防止网络攻击，但如果实施得当，其目标是将此类攻击的风险降至最低。根据具体的安全控制、导则和标准，可以对网络安全保障做法进行检查，这些做法既可由监管实施，也可由业界自愿采用。但是，没有放之四海而皆准的方法，国家主管部门和行业监管机构经常采用不同的做法，从自我评估和自愿导则到贴标方案以及严格的合规检查。

虽然没有一种单一的方法可以推荐，但很明显，在最近的几年和几个月里，随着若干国家和地区的不同发展，在全球范围内采用网络安全保障做法已取得了持续进展。例如，经济合作与发展组织于2022年12月推出了理事会有关产品和服务数字安全的建议书，该建议书推荐通过相关政策，增强与风险相称的产品和服务的数字安全性，首先采用基于自愿政策措施的宽松方法，并探讨强制性措施的必要性[5]。

本报告反映了第3/2号课题会议以及关于网络安全保障做法的专门讲习班的文稿和讨论意见。2023年5月23日在日内瓦举行的全日公众讲习班，通过展示一系列全球正在进行的做法和声音，为探讨全球各领域（物联网（IoT）、电信等）网络安全保障格局提供了机遇。会议汇集了成员国、业界、技术机构以及民间团体的代表。

第3/2号课题管理班子希望借此机会感谢所有发言人和撰稿人就此议题提出的宝贵输入意见。没有他们的承诺，这项工作不可能完成。

基于收到的宝贵输入意见，本报告主要通过介绍六个要点，说明迄今为止在考虑和实施网络安全保障做法方面所面临的挑战、对影响的评估和吸取的经验教训。

这些要点可作为国际电联成员的重要输入意见，用于评估现有做法，并评估是否需要采取更多或不同的方法，同时考虑到其他主管部门和组织汲取的经验和教训。

要点1：不同程度的危急性和风险需要不同程度的保障

在考虑实施网络安全保障做法时，至关重要的是首先确定一个实体正在试图保护什么以及确定的资产所面临的风险。希望防止网络攻击的国家和公司应优先确定哪些系统和资产需要保护，并评估其漏洞。在此方面，制定开展风险评估的蓝图是一种有益的工具。最知名的框架之一是国家标准技术局（NIST）的网络安全框架[6]，该框架目前正在进行更新[7]。这是一种广泛使用的方法，用于帮助确定和尽量减少组织风险。它制定了非监管导则，使全球各组织能够确定其自身的风险状况，并对此实施适当的网络安全控制。将于2024年初最终确定的经修订的框架基于与使用这些导则的利益攸关方的广泛和长期接触，并继续与其它国际标准保持一致。

在讲习班上，NIST代表强调，该组织作为一个非监管机构的有利地位已使其与来自世界各地的行业利益攸关方进行更深入的接触，从而了解实际的挑战并收到反馈意见，这些已被纳入新导则[8]。这些要求具有适应性和灵活性，并适用于所有组织和部门。ITU-D部门中的一个私营部门成员BitSight谈到了其平台，该平台嵌入了NIST网络安全框架，并已被负责网络安全的不同政府机构（如应急计算机响应团队（CERT）、国家网络安全机构、电信监管机构）所使用[9]。通过该平台，各国可对其认为的关键基础设施和资产进行风险评估，并衡量其风险因素。

风险评估还有助于确定适当的保障水平，同时考虑到被保护数据和资产的敏感性、违规的后果以及威胁环境（即实体是否易受网络攻击）。在某些情况下，保障水平取决于监管要求。保障级别越高，安全控制越严格。例如，较低的保障级别可能只需要一个

1 https://www.itu.int/en/ITU-D/Study-Groups/2022-2025/Pages/reference/SG2/ToR/Q3-2.aspx#Question
2 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090023PDFE
3 https://www.einnews.com/pr_news/606505844/cybercrime-damages-to-cost-the-world-8-trillion-usd-in-2023
4 操作安全与网络安全保障做法密切相关，因此操作安全可为保障做法提供良好基础。ITU-T第17研究组副主席Broadcom介绍了良好条件的模型，强调该模型由四个关键要素组成：人员和流程、知识、安全产品（外源安全）和资产安全（内源安全）。见“降低风险和保护声誉”，https://www.itu.int/md/T22-SG17-C-0214/en
5 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481
6 https://www.nist.gov/cyberframework
7 https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20
8 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090017PDFE
9 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090024PDFE

系统密码或防火墙，而更高级别的保障需要增加更先进的控制，如先进的加密和多因素认证。

尽管网络安全保障做法增加了信息技术预算，但未能落实安全控制可能会付出更高的代价。在讲习班期间，代表们敦促听众不仅从财务角度思考遭受网络攻击带来的成本，而且额外声誉成本的危害要大得多。失去客户和公民的信任具有一种长期的影响，超出了金钱的范围，组织必须能够从战略上理解这一点。同样，对于公共部门而言，攻击如果成功，可能会影响公共服务和关键活动的提供，其破坏力也不能仅从财务角度进行评估，因为它影响到公民的生活。

要点2：与合作伙伴组织、行业和利益攸关多方接触可成为推动实现网络安全保障的有效途径

首先，重要的是将举措与其它做法进行对比，了解最佳做法，并在举措制定过程中从他人的成功和错误中吸取教训。第二，重要的是与包括业界在内的利益攸关多方进行接触，以获得对作为发展组成部分的举措本身的重要见解。

尽管在欠发达国家网络安全保障做法越来越必要，但可能仍然难以实施。多哥网络防御非洲（CDA）的代表解释了本地市场在向基本业务运营商（ESO）提供网络安全保障方面面临的挑战[10]。需要应对的部分因素包括缺乏资金、对政府作为服务提供商缺乏信任以及缺乏本地人力和设施等。为支持ESO遵守新公布的网络安全控制要求，多哥政府与大型知名网络安全提供商建立了公共私营伙伴关系，为公共和私营部门提供网络安全服务。通过这一模式，多哥创建了CDA，作为一个自给自足且高质量的本地网络安全提供商，在非强制性的基础上向ESO提供支持。自给自足的模式使多哥能够应对上述诸多挑战，并鼓励培养网络安全领域的本地人才，推动当地市场的发展。该代表指出，CDA作为竞争市场中的私营实体，对于确保适应性、高质量服务和竞争性定价十分重要。

同样重要的是，应加强那些可能确定监管环境的政策制定者与民间团体组织之间的合作，这些组织可以促进安全需求，同时根据现有的和确定的区域和国际做法，为政策和监管的发展提供信息。例如，DiploFoundation是一个国际组织，就与网络安全相关的主题向政府、监管机构、企业、民间团体提供培训项目和能力建设，并参与有关网络空间负责任行为对话（日内瓦对话）[11]。2020年，日内瓦对话产生了一系列良好做法[12]，其中包括建议对安全设计和漏洞管理、良好行业做法、威胁建模、第三方和供应链安全、安全开发、漏洞管理和披露以及组织文化做出的定义。全球网络专业知识论坛（GFCE）是一个国际平台，支持项目的协调，促进知识和专业技术的共享，将提供能力建设支持的请求与开发研究项目相互匹配[13]。GFCE在太平洋岛屿、非洲、美洲和加勒比以及东南亚建立了四个区域中心。鉴于其全球足迹和在发展中国家得到的各种支持，该论坛完全有能力就网络能力建设的需要和需求提出更多区域性的多元观点。GFCE拥有一个在线门户网站，作为全球已落实的、当前网络能力建设项目以及资源和工具的存储库。这一门户网站还有助于减少重复工作并确定一些项目或能力建设方面的差距和模式。

要点3：通过对话和磋商，考虑不断演进的知情监管方式

在许多情况下，网络安全保障做法在成为强制性之前是自愿引入的。这种转变通常发生在政府认为行业在确保产品安全方面做得不够，消费者不一定掌握评估产品是否安全的知识。这可导致政府和国家主管部门采取行动并规定他们期望行业满足的保障做法。例如，巴西电信监管机构Anatel已在国内建立了认证机构和测试实验室系统，用于客户驻地设备（CPE或家庭网关）的认证。传统上，Anatel的做法是为电信行业提供自愿网络安全导则。然而，通过进行风险评估，Anatel发现，考虑到此类设备的脆弱性和威胁，建议不足以满足CPE的需求，因此有必要为此类产品制定强制性的最低安全要求。通信服务提供商（CSP）的强制性要求于2023年初公布，重点解决密码不安全和不必要启用的服务部件等漏洞。这些要求将于2024年初生效，作为产品获批的强制性实验室测试的一部分[14]。Anatel解释说，只有与该部门进行全面讨论之后，才能从非强制性方法向网络安全强制认证要求演进。

同样，沙特阿拉伯王国的国家网络安全局（NCA）介绍了其创建独立验证和检验（IV&V）生态系统[15]的举措，以便在沙特阿拉伯从网络安全保障的角度测试和认证产品。该举措亦旨在确定对网络风险和威胁高度敏感的硬件和软件并进行分类。此外，其还寻求为IV&V中人力的发展做出贡献。该举措路线图考虑从自愿计划开始，然后再将其作为强制性义务。监管机构还提到，这一生态系统最终实现“自我可持续”十分重要，这向NCA通报了鼓励市场利益攸关方进行此类评估的方法。

10 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090025PDFE
11 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090020PDFE
12 https://genevadialogue.ch/goodpractices/
13 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090021PDFE
14 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090018PDFE
15 https://nca.gov.sa/en/news?item=535

在IoT安全领域，英国还提供了从自愿方式向强制方式演进的案例研究。近年来，英国决定通过立法，根据欧洲电信标准协会（ETSI）EN 303 645标准（全球首个适用于消费者物联网设备的网络安全标准）为IoT消费品制定基本安全要求。在英国，制造商、进口商和分销商必须遵守13条ETSI安全导则中的3条，法律授权政府在必要时根据定期的威胁评估采用附加要求。在自愿通过一段时间后，决定强制规定一个安全要求基准。2018年，英国制定了消费者物联网安全的自愿行为准则[16]，但行业合规性并未达到预期。通过磋商活动收集的证据表明，消费者重视安全，并愿意为安全产品支付溢价。然而，安全威胁不受与产品安全同等程度的强健监管，导致制造商缺乏透明度并延缓采用安全政策。证据还发现，消费者可连接的产品市场抑制了基本安全功能的采用，因为消费者绝大多数认为产品已经是安全的。该机制旨在通过强制规定行为准则中的要素来弥补这一差距，以确保制造商了解漏洞并采取措施减轻这些漏洞的影响。PSTI（产品安全和电信基础设施）制度将于2024年4月生效，并将适用于可连接到互联网的任何消费产品[17]。

已确定的挑战之一是对小微企业可能产生的影响，这些企业在遵守新制度方面面临困难。英国执法机构正在制定指南，以减轻任何不相称的影响。除了与业界合作外，英国还表示，计划中必须满足的三大要求已经确定并透明地传达了数年。多年来，英国对该制度的实施过程进行了演练，包括密码要求、产品基本架构、漏洞暴露和安全透明度要求。影响评估表明，减少针对消费者和企业的网络攻击量的总体益处有望超过与制度相关的成本。由于《2022年PSTI法案》是世界上第一项强制性网络安全产品立法，执行这一制度的成本尚不确定，但初步估计，划拨的资金将足够。

在某些情况下，用户或客户的身份决定了保障做法是强制性的还是自愿的。例如，大韩民国推出了云安全保障计划（CSAP），这是一项云计算服务的安全认证[18]。通常，CSAP认证是自愿的。但是，公共部门的客户（即公共机构）需要使用已根据相关规定获得CSAP认证的云服务，因此，云服务提供商在向公共机构提供云服务时需要获得认证。

要点4：鉴于不断变化的威胁格局和不断演进的网络安全风险，网络安全保障做法不能一成不变，应随着时间的推移重新审视和调整

开展定期内部审计有助于确定控制和风险暴露方面的差距并了解威胁情报，这被认为是一种良好做法。即使产品获得认证，也可能在其生命周期内受到安全缺陷的困扰。接受认证方案的过程要求在特定的时间提交信息，而这并不考虑未来威胁的动态变化。BitSight最近的一项研究表明，漏洞“打补丁节奏”不佳与发生网络安全事件[19]的可能性之间存在很强的相关性，这表明了一旦有安全补丁可用就必须立即更新系统的重要性，同时要铭记据报补丁在全球各地的不同分布情况。

渗透测试或“笔测试”是一种安全保障活动，有助于评估IT系统的安全性，并确定可能被用来利用的系统漏洞。英国通信监管机构Ofcom自愿与电信提供商共同实施TBEST计划，这是一项笔测试，旨在刺激网络攻击，以发现安全漏洞，然后通过补救程序加以解决，以改善运营商的网络安全态势[20]。监管机构概要介绍了这一进程以及所涉及的不同利益攸关方。从更广泛的意义上讲，这一计划是Ofcom采用的监督体制方法的一个范例，它强调了与监管机构监管的行业建立协作关系的重要性。迄今为止，英国所有通信提供商都已经或正在自愿接受TBEST计划，并因此实施了变革。TBEST既不是一个“标准”，也不是一个认证程序。其目标是使通信提供商能够意识到网络威胁并及时实施适当的变革，以提高其网络防御能力。通过意识到和解决这些漏洞和薄弱环节，运营商在保护其网络方面将处于更加有利的地位。

要点5：正在努力教育消费者和制造商了解网络安全的重要性和选择更安全产品能带来的好处

为使公众了解网络安全的重要性以及选择安全产品的好处，已付出了努力。

为此采取的一种方法是制定网络安全标签方案（CLS），以新加坡为例，经过认证的产品可以附有标签。标签方案主要是为消费者提供信息工具。新加坡网络安全局（CSA）讨论了一项网络安全标签方案，旨在帮助消费者区分安全程度较高和较低的物联网设备[21]。该方案是自愿性的（Wi-Fi路由器除外，因为它是强制性的），分为四个级别，第1级是安全基线。第1级和第2级基于制造商的自我评估，第3级和第4级由

16 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf
17 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E00000090014PDFE
18 https://isms.kisa.or.kr/main/csap/intro/index.jsp
19 https://www.bitsight.com/press-releases/study-finds-significant-correlation-between-bitsight-analytics-and-cybersecurity
20 https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience/our-work
21 https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E00000090016PDFE

经认可的实验室进行第三方评估。该方案分为多个级别，以激励制造商在基本要求之外采取额外的安全措施。CSA还讨论了强制执行网络安全标准所涉及的权衡问题，包括制造商因合规成本增加而绕过市场的风险。相反，我们的目标是改变制造商的心态，将网络安全视为一种促进因素和市场差异化因素，而不是一种成本。关于网络安全标签方案在新加坡的影响，目前仍处于初期阶段，鼓励制造商参与该方案并改善其网络安全的工作仍在进行中。今后将再次开展公众调查，以评估消费者的意识和行为。1级和2级制造商的合规成本已降至最低，消费者的产品成本也没有显著增加。随着自愿计划的实施，市场力量有望推动制造商提高网络安全水平。

除标签外，投资于技术控制与建立意识和教育民众了解各组织和国家所面临的网络安全风险同样重要。目前，勒索软件攻击是最令人担忧的趋势。对于这些类型的攻击，攻击的主要载体 – 即犯罪分子进入网络或系统的方式 – 是通过网络钓鱼电子邮件[22]。在这种情况下，网络犯罪分子往往只需点击网络钓鱼电子邮件，就能绕过安全控制。因此，让普通公民和员工了解此类问题对网络安全保障至关重要。

要点6：必须寻求国际协同/统一和互惠协议

网络安全保障模式（即认证和标签方案）之间是否存在互惠协议，可成为这些做法能否推广的决定因素。正如利益攸关方所强调的那样，互惠协议可以帮助在多个市场上运营的行业参与者更容易地遵守规定。然而，考虑到互惠协议是一种正式机制，有许多国家限制，而且批准和签署需要时间，网络安全保障做法需要与符合国家需求和优先事项的现有国际方法找到协同效应。这将减轻产品和服务提供商的监管负担，以避免相互矛盾的要求。

CSA强调了在制定和实施网络安全标签方案方面开展国际合作的重要性。新加坡已与芬兰和德国签署了相互承认安排，并正在努力扩大在此领域的伙伴关系。新加坡回顾了其经验，认为政府需要积极主动地建立认可，尽管制造商也有兴趣支持认可进程，因为它可以减轻重复测试和认证以及不同管辖区市场准入的负担。这一进程涉及将相关各方汇聚一堂，统一要求并制定现实且不过于繁琐的共同标准。

在欧洲层面，欧洲网络安全机构（ENISA）负责开发三种认证方案，这些方案将在内部市场得到认可，从而在整个欧盟（EU）实现自动“相互认可”。这些方案是：欧盟ICT产品的通用标准方案，目前正处于起草立法法案的阶段，目标是获得通过；云服务方案，正在进行广泛讨论；5G方案，正在制定中[23]。

除互惠外，考虑到国际市场行业的运作，统一基本安全要求也是一项重要考虑。有关IoT消费产品的ETSI标准是此类努力的一个示例。主要问题是不同监管框架在多大程度上是同步的，以及它们将在多大程度上通过相同的国际标准相互连接。在此方面，加强对话，甚至找到适当的对话场所是一项挑战。为了协调统一，ENISA在网络安全标准化和5G方面的活动需要CEN、CENELEC、ETSI、ISO、IEC GSMA、3GPP、GlobalPlatform的协作。该机构的主要输出成果之一是将不同标准开发组织（SDO）的5G安全控制整合到一个存储库中[24]。

[22] 网络犯罪分子的常见策略，用来诱骗人们泄露敏感信息或下载感染目标系统/网络的恶意软件。

[23] https://www.itu.int/dms_pub/itu-d/oth/07/2e/D072E0000090019PDFE

[24] https://www.enisa.europa.eu/publications/5g-security-controls-matrix

附件：网络安全保证做法实例

国家或组织	实践的名称	实践的类型	实践的范围	方法类型	参考
澳大利亚	面向制造商的物联网设计安全指南	指导	物联网	自愿	链接
澳大利亚	行为准则：为消费者保护物联网	实施规程	物联网	自愿	链接
巴西	77/2021法案 电信设备的网络安全要求	认证方案的要求	电信设备	自愿	链接
巴西	2436/2023法案 – 客户驻地设备（CPE）符合性评估的最低网络安全要求	认证方案的要求	CPE	强制	链接
沙特阿拉伯王国	独立验证和确认（IV&V）	产品的测试和认证。设备和软件的识别和分类	产品	最初为自愿	链接
大韩民国	云安全保证计划（CSAP）	认证方案	云	组合 – 通常是自愿的。对于向公共机构提供云服务是强制性的。	链接
新加坡	网络安全标签计划	认证和标签计划	物联网	组合 – 通常是自愿的。仅适用于Wi-Fi家用路由器。	链接
大不列颠及北爱尔兰联合王国	产品安全和电信基础设施（产品安全）制度	最低安全要求	可连接的产品	强制	链接
大不列颠及北爱尔兰联合王国	TBEST方案	渗透测试	电信网络	自愿	链接

ITU出版物
瑞士出版，日内瓦， 2023

国际电信联盟
Place des Nations, CH-1211 Geneva Switzerland