国际商会企业网络安全指南

INTERNATIONAL CHAMBER OF COMMERCE

The world business organization

国际商会企业网络安全指南

致谢

国际商会（ICC）企业网络安全指南是受到比利时网络安全指南的启发，由比利时国际商会、VBO-FEB、安永比利时、微软比利时，与 B-CCENTRE 和比利时 ISACA 共同发起的倡议。值得称赞的是，在比利时该指南为国际商会数字经济委员会提供作为适应涉及全球资源权限的公司和机构的典范。

ICC 衷心表彰所有参与比利时指南的编制人员，以及参与全球指南编制工作的国际商会网络安全专家组所做出的贡献。

版权声明

国际商会出版号 No. 450/1081-5

ISBN: 978-92-842-0336-9

目 录

前　言

国际商会秘书长约翰·丹尼洛维奇

国际商会向企业提供管理工具和自律指导，进而促进良好的商业实践，已有近百年的光荣历史。作为全球性的商业组织，其成员由来自各行业和地区的企业组成，国际商会乐于为各种规模的企业提供一份简洁、明了的指导，从而帮助企业在日趋严峻的网络安全挑战中发挥各自的作用。

国际商会是一个致力于促进全球贸易和投资发展的国际性组织，包括鼓励数字经济为企业、客户、政府和社会带来日益巨大的发展机遇。网络的互联互通不仅改变了市场，也改变了社会的结构。互联网的全球性和开放性使人们能够获取更多的知识流、信息流、商品和服务。同时，互联网应该是可信的、安全的。因此，为了保护这些利益，网络安全策略的制定应该是恰当与合理的。

安全性是个令人望而生畏的话题，因为安全性就像完美性一样，其目标难以捉摸而又糅杂了各种权衡。对安全问题心存恐惧或缺乏意识，可能成为保障企业风险评估和采取适当措施的一个障碍。本指南会将安全意识转换成一整套简单的步骤以消除上述威胁和障碍。国际商会编订本企业网络安全指南，首先是为了助力 600 多万家会员，同时也希望惠及更广泛的读者。本指南并非局限于信息技术团队使用，而是更适用于企业所有者、员工和高管，此外，企业也应将本指南与其产品和服务供应链中的业务合作伙伴及公共管理部门分享，大力提高企业的应对能力。

本指南将通过全球范围的国际商会国家委员会、成员单位、商业协会和商会，国际商会世界商会联合会进行发布，发布范围将超过 130 个国家。国际商会坚信依托其广泛的网络与合作伙伴共同在全球商业活动中采取措施，将为有效降低企业和社会的网络风险发挥至关重要的作用。

网络安全始于你

现代信息和通信技术使得各种规模的企业均有能力进行创新、发掘新市场、提升效率，客户和社会亦从中受益匪浅。然而，越来越多的商业惯例和政策受到挑战，不得不适应由通信环境和网络信息流所带来的直接或间接的影响，而这些信息流往往会被用于商品和服务的所有交付过程中。许多企业采用了现代信息和通信技术，却没有充分认识到须同步加强对新型伴生风险的管控。本指南将解决这一现实问题，并概述各种规模的企业应当如何去识别以及管理此类网络安全风险。

人为恶意破坏企业网络安全的案例常常见诸报端，且不论企业规模大小，这些破坏看起来似乎都很随意和轻松。目前看，犯罪分子、黑客以及竞争对手利用现代信息通信科技漏洞的水平越来越高，导致企业面临越来越多的风险[1]。信息系统与多种外部设备[2]的结合增加了复杂程度并为企业信息系统带来了威胁。此外，企业面对的不仅仅是来自外部的威胁，同时也必须管理来自信息系统内部的威胁，因为组织内部人员也能够在自己的住所或者当地的咖啡馆来损坏企业数据或者利用企业资源。从业务的角度来说，无论是大型企业还是小型企业，能够及时地认识并有效地管控网络安全风险是至关重要的。同时，包括经营层和主管层在内的所有的公司经理们必须认识到网络风险管理是一个持续的过程，这个过程

[1] 越来越多外部网络的安全威胁包括恶意软件(如入侵软件、代码注入,漏洞、蠕虫、木马等)、拒绝服务、数据泄露等。相关更新请参考 2014 年 ENISA 威胁形势，2014 年（https://www.enisa.europa.eu）

[2] 例如移动手机、调制解调器、支付终端，软件自动更新、工业控制系统、供应商/客户交互、物联网。

中没有绝对的安全。

和许多业务上的挑战不同，网络安全风险管理始终是一个不容易解决的问题。它需要一个具有一致性的应用管理程序，来关注和清除存在的问题。网络安全需要持续关注，面对可能出现的问题，并且有明确的沟通原则。很多优质的资源可以用于解释和应对最严重的网络安全，但用来支持企业管理应对网络安全的合适材料仍然是稀缺的。本指南将帮助各种规模的组织管理层与他们的信息技术部门经理互动，同时为网络安全风险管理实践的发展提供指引。

风险管理程序可以提高一个组织的网络安全水平，其重点是“管理”。由于技术和威胁持续不断的变化，企业信息系统永远不会绝对的完善和安全。在变化的环境中进行有效运行需要坚持一种永无止境的风险管理方法。如果业务经理对手头的任务没有适当的预期，他们将会对网络安全措施产生挫败感。而且，如果没有适当的约束，企业在应对网络风险的过程中可能会迅速消耗掉所有可用的资源。通过一定流程帮助企业有能力认识并区分优先顺序（实物资产和信息资产），是实施网络安全风险管理的基础。

我们应时刻意识到，如果没有适当的预防措施，互联网、企业信息网络和设备都是不安全的。现代企业信息系统往往被一些恶意破坏者作为攻击目标。如何设定网络安全风险管理的预期，这里可以引入一个有用的观念：“有价值的东西只要联网，就会处于危险当中，并且很可能招致破坏”。幸运的是，对于恶意破坏者来说有价值的东西并不一定是企业认为有价值的资产（比如：钱、商业机密和客户信息）。虽然技术和处理措施可以降低损害的风险，一个坚定的恶意破坏者会从互联系统中最薄弱的环节获益。企业的信息系统在组织结构层面、人员层面以及技术层面等都存在大量的潜在漏洞。

尽管企业拥有最好的技术供应商、服务供应商以及员工，也不会拥有绝对的安全。网络安全风险管理过程必须对企业的薄弱环节和可能会遭受的特别威胁进行评估，并把这些弱点及威胁与企业的优先资产进行隔离。

尽管上述现状不容乐观，各类企业仍然能通过培养关键的组织技能，成功实现网络风险管理。

- 首先，企业必须进行风险分析，找出企业中最需要优先保护的资产。
- 其次，领导层要采取必要的行动，确保企业运用了最好的信息安全保护措施。
- 最后，企业必须通过制度化的组织流程，及时做好网络事件的检测和内外部应对工作。

需要增强与同事、相关政府部门、客户甚至竞争对手之间的沟通交流应对措施。需对可能发生的网络事件提前制定预案，以避免因仓促应对而犯错（这原本是可以避免的），而导致问题复杂化。最后，建立从网络事件中学习与调整应对措施的机制至关重要，这可以有效促进制度改革，进而在全公司推广优秀的网络安全风险管理实践案例。

在过去的十年里，各国政府、组织以及个人发布了许多应对网络信息安全挑战的内容。文档和指南太多，以至于让你不知该从哪里读起，也不知道哪种更适合你的组织。现有的材料内容相当广泛，内容也越来越具体。

- 指导方针——提出网络安全问题的高水平目标声明，并为组织和个人提供行动纲领。例如：经合组织的安全指导方针等。

- 国家战略——通常是在指导方针的基础上，进一步阐明在特定国家或法律体系下的网络安全保护途径。例如：国际网络安全战略[3]，欧洲及其他国家的国家战略[4]等。

- 框架——是对国家战略的进一步细化。框架中收集形成一份按重要性排序的或需评估的资源目录，协助组织对标衡量其应对网络风险的成熟度与水平。例如：美国国家标准与技术研究所（NIST）的网络安全框架[5]等。

- 实践标准——这些文件用来指导或者管理组织流程，从而确保最好的网络安全流程能够强有力地、持续地得到执行。例如：ISO 27001、27002、27032工艺标准，PCI安全标准等。

- 技术标准——是针对处理特定类型互操作性要求的接口实现的详细规范。例如：HTTPS、AES、EMV、PCI支付标准等。

首先，本指南依据全球网络安全指导方针和各国国家战略，为企业评估在线安全问题提供了一个简明框架，提出五项重要原则，为各种规模的企业解决网络安全风险提供指导。其次，本指南提出了六项关键举措，以确保企业获取广泛的资源并借鉴最好的经验。进而，提出了如何将五项原则应用到企业制定政策和管理活动中。

---

[3] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[4] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[5] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

使用说明

随着相关资料的进一步开发，本指南还将补充一份持续完善的配套电子附录，该附录将从实践标准到技术标准等方面提供更具体的建议。虽然没有绝对的安全，但是网络安全风险管理的概念将帮助企业在不断变化的环境中应对信息安全挑战。本指南不仅对企业自身有指导意义，还应分享给与企业有关的各方，这样才能为你的企业体系和运营活动中涉及的所有入口与交换节点提供更好的保障。

由于受一系列因素的影响[6]，不同公司之间维护信息安全的方法可能不尽相同，然而无论规模大小及所处行业，所有的企业均可遵循一些通用的高级原则来构建可靠的信息安全体系。本指南提出的五项关键原则可以分为两大类：

A：目标和思维模式；

B：组织和流程。

这些原则辅以六项安全举措，然后将五个初始元素应用到这些原则当中，进而形成公司的信息安全策略。

总而言之，本指南中建议的原则和活动会增强公司对网络威胁的应变能力，并减少安全漏洞造成的破坏。

A.目标与思维模式

原则一：重点着眼于信息，而不是技术

你是防御网络威胁的第一道防线，也将协助企业定下信息安全方案的基调。因此建议要更广义的来看信息安全，而不仅仅是指信息技术这一方面。

信息安全涉及到人员、流程和技术各个方面，是一个企业整体范畴的问题，而不仅仅是信息技术（IT）问题。信息安全措施的落实不应局限于信息技术部门，而应反映到全公司的各个环节。因此，信息安全的范围和目标应包括：人员、产品、工厂、流程、政策、程序、系统、技术、设备、网络和信息。

人是关键。对信息资产的漏洞和威胁识别、管理是一项艰巨任务。然而，攻击造成的安全事故中，如果人们能以更安全的方式来处理，其中一半以上的安全

[6] 包括业务性质、风险水平、环境因素、互连级别,监管要求以及公司规模等。

事故原本是可以避免的。[7]

信息安全保护应聚焦在保护你最有价值的信息和系统上，一旦这些信息与系统的机密性、完整性和可用性遭到破坏，将会对公司造成巨大的损失。当然，这并不意味着可以对其他信息资产的安全置之不理。这表示在信息安全管理实践中，关注组织内的“拳头部门”的风险控制才是行之有效的方法。同时，我们必须意识到，100%的风险消除既不可行，其巨大的成本也是不可取的。

原则二：建立应变思维

本原则的目标是公司对于信息损失或损害的风险应变能力。公司需要遵守各种法律法规，其中一些要求企业实施相应的安全措施。一方面，遵守这些法律、法规和标准能够提高企业的信息安全水平；另一方面，一旦符合这些合规要求，企业会误以为可以高枕无忧了。事实上，安全威胁的变化速度远远超过法律法规的修订速度，这需要我们制定一个动态的风险管理目标。因此，在实际使用中，现有业务政策和程序有可能是过时或者无效的。

定期评估公司抵御网络威胁和漏洞的能力，这对衡量风险管理目标的达成情况和网络安全措施的充分性来说至关重要。评估活动可以通过内部和独立评审来完成，包括渗透测试和入侵检测等方法。

网络安全的责任决不能仅仅局限在技术部门，制定决策的利益相关者也应当参与问题的分析，此外，长远来看还应在组织内建立一个健康的生态系统。然而，只有当与网络风险管理相关的公司文化及思维模式得到了改善，定期商业评论的价值才得以真正实现。

[7] 安永，《2012 全球信息安全调查—缩小差距》

当企业引入新的解决方案和设备时，一定要提前考虑信息系统的适应性。在此情形下，在引入阶段就应当尽早考虑该采取哪些适当的安全措施，最理想的是在业务需求识别阶段就开始考虑。这种“以安全为核心理念的设计”可以使热衷创新的员工，更多地关注信息安全风险管理。

B. 组织和流程

原则三：做好应对准备工作

即使采取周全的保护措施也会遇到信息安全漏洞。我们所处的环境中只有“何时发生”而不是“如果发生”。因此，一个企业如何应对漏洞就是你需要评估的了。

为了最小化网络安全事故对企业的影响，除了技术应对措施外，企业还必须制定组织应对计划。通过设立组织规划路标，来帮助企业管理人员清楚应该在何时请专业的第三方介入并协助控制和解决安全事故，以及在什么样的情况下来联系其他外部资源（包括执法部门或政府监管机构）。请牢记，向有关当局报告是一种改善整体安全局面的方法，并且在某些情况下这是强制性要求，否则就会违反监管条例或面临罚款。成功的网络安全事故应对管理还应包括内外部沟通策略，不同的策略会产生截然不同的结果，可能是上报纸头版头条尴尬收场，也可能成为大学相关课程的成功案例。

尽管内部风险管理活动是最关键的，但也要记得花一些时间广泛地与业内同行、合作伙伴、执法方进行沟通，这将帮你及时了解当前和未来新的威胁，同时建立起可靠的关系以便在突发事件中寻求帮助。

原则四：管理关注，责权对应

为有效管理信息安全，企业管理层必须理解和支持风险管理活动，这是成功的基本要素。你和你的管理团队应该更多地参与到公司的网络安全风险策略的管理与监督中来，并确保在公司资产保护上投入了充足的人力与财力资源。但仅投入资源还远远不够，无论企业规模大小，确保信息安全时应有权限调动全公司资源共同应对网络威胁和漏洞。

公司信息安全措施的有效性和充分性应当正式地报告给最高业务管理者，并且至少每年向管理团队、审计和董事会汇报一次。这些基于各种安全指标和数据的定期报告将有助于为信息安全策略的制定和投资提供决策依据，并帮助你理解公司是怎样保护信息资产的。

尽管人员常被认为是信息安全体系中最薄弱的环节，你还是应该通过培养大家的安全意识、掌握有效技巧，积极地将你的团队打造成为优秀的安全体系中最宝贵的资产。

原则五：基于目标而行动

仅仅阅读本指南是不够的，你必须通过创建（或修改）各种信息安全策略来实现公司独特的网络信息安全目标。公司信息安全策略提供了一个准绳，来引导整个公司所有业务单元和人员的安全活动，同时在业务过程中强化安全意识。

通常情况下，安全策略文档及其配套指南和标准将共同构合成一份信息安全策略框架，随后被转化成一般的操作程序。然而，随着企业在业务价值链中越来越多地采用和集成第三方供应商的服务，企业必须清楚自己的信息资源是如何流向和依存于各类外部合作伙伴的。如果第三方没有充分保护你的信息（或者是你赖以使用他们的信息系统），**他们**的安全事故或许会**成为你**企业经营、声誉和品牌价值的严重威胁。鼓励供应商至少采用你公司的信息安全原则。如果条件允许的话，建议要在适当的地方进行审计或要求服务提供商将他们的信息安全实践细化，从而在商务活动中获得额外的保障。

第三方不仅是风险的来源——有些可能有助于减少风险，甚至能够帮助你实现网络安全风险管理的关键目标。信息技术服务提供商可以帮助你改善网络安全风险管理的基础设施，比如帮你进行安全评估和审计，以及通过现场的、或外部托管的、或基于云[8]的方式向你提供信息安全设备和解决方案或服务。

[8] 云服务是通过网络（例如因特网）使用外部服务器存储、运行和管理数据，具有很高的灵活性，并能做到实时监控。

六项基本安全举措

这是一套实用举措，各种规模的企业均可以通过采取这些举措降低网络安全风险。虽然不够全面详尽，但能确保企业通过这些举措在信息安全方面取得优异成果。

举措一：备份商业信息，有效恢复程序

网络安全管理是一个持续进行的过程。如果你对所采取的初步措施比较满意，可到与本指南有关的门户网站查找相关标准和资源，帮助你采取进一步措施，以提高信息安全程序的恢复能力。

在企业遭受诸如信息被窃取、篡改、删除或丢失的安全漏洞损害前，确保商业信息已经备份。单纯的备份还远远不够[9]，有效的备份程序还应包括验证包含在备份文件中的商业数据和信息以及测试还原过程。如使用第三方进行信息存储（例如云服务），确保同样适用上述备份规定。

物理媒介，诸如用来存储备份数据的磁盘、磁带及驱动也是很容易存在风险。备份数据必须采用与源数据相同级别的保护方式，尤其是涉及易被移动的物理媒介。

[9] 备份过程是一个技术过程，必须正确进行。例如，只用几个在同一站点同时链接的存储库是不足以正确进行备份的。一个行之有效的备份需要考虑多种类风险，包括数据丢失和运行站点的丢失，结合其它原因，通常要求数据备份要放在不同的物理位置。

举措二：更新信息技术系统

各类系统和软件，包括网络设备和装置，应当在补丁程序和固定升级软件可用时及时进行更新。这些升级和安全补丁可修复易受攻击的系统漏洞。许多成功的攻击是由系统漏洞造成的，然而在被攻击事件发生甚至一年多前，系统就已经可以进行升级了。

如果可能的话，使用自动更新服务；尤其是诸如反恶意软件应用程序、网络过滤工具和入侵检测系统的安全系统。自动更新程序可以保证用户直接从源供应商处获取有效的安全软件更新。

举措三：增加员工培训投资

在整个公司的员工队伍中培养保护信息安全的意识是必不可少的，并且应当不断重复强调。培训[10]能够保证所有接触信息和信息系统的工作人员了解自己日常工作中的职责，保护并支持公司的信息安全活动。如果没有适当培训，员工可能很快成为企业内部的风险源，制造安全事件和漏洞，给对手以可乘之机来破坏你的信息安全系统。

[10] 终端用户如需了解一般网络安全信息，可查询欧洲网络信息安全局（ENISA）的网站（www.staysafeonline.org. http://www.enisa.europa.eu/media/multimedia/material）。为达到公司内部教育目的，所有该网站上的信息、视频和图标均被授权使用。

建议在企业内部培养信息安全风险管理文化。随着时间的推移，培训投资可以加强员工的商业信息安全意识，并使得员工的安全技能得到提升。

举措四：监控信息环境

企业必须事先部署系统和流程，以确保在企业内部发生信息安全事件时，能够及时得到警告。很多时候企业并没有意识到安全漏洞；一些企业在检测到入侵前已经遭受了数月甚至数年的信息泄露或病毒感染[11]。各类技术解决方案包括入侵检测、预防系统和安全事件管理可以协助解决上述问题。然而，仅仅简单地实施这些解决方案是不够的。要想真正从这些技术方案中获益，对上述解决方案输出信息的持续检测和分析是必不可少的。

许多企业或许没有用来监控重要系统和流程的专业技术和资源。不同的服务商可根据不同的商业模式提供现场和托管安全服务，包括基于云的技术和服务。如果有这方面需求的话，可以寻找符合自己组织的模式，寻求有经验方的建议，并将需要的条款写在合同中。

如果公司正在遭受网络安全事件，需考虑向相应的政府机构[12]和行业协会报告这一事件——与他人沟通可以帮助确定公司是在遭受一个孤立事件，或者是一个更大的网络安全事件[13]的一部分。通常，跟外界联系可以获取一些信息和建议，帮助企业采取有效的应对措施。

---

[11] http://www.verizonenterprise.com/DBIR/

[12] 网络安全受害者需向有关执法机关提起诉讼，当地警方往往是传统犯罪的最佳联络方式，但更多专门的执法机关专门打击于网络犯罪（黑客、蓄意破坏、谍报）。

[13] 网络攻击可以是横向的（同行业之间）或者纵向的（针对分包商）或者专门针对特定的软件或硬件的安全威胁。

举措五：用分层防御降低风险

网络边界安全和传统的访问控制已经不足以抵御风险，尤其是企业的信息系统已经连接到互联网、网络服务提供商、外包和云服务、供应商和合作伙伴以及便携设备，这些均超出了公司的控制范围。针对黑客，病毒、恶意软件和装置需要用分层防御降低风险。结合多种技术[14]来处理网络安全风险会显著降低一个小破坏发展成为一个全面网络安全事件的风险。

分层防御措施能限制黑客或对手的自由访问并能增加企业监控系统监测到攻击的几率。

网络安全保险不仅可以减少因网络安全事故遭受的财务损失，而且能够主动管控风险，强化企业内部的风险管理。

举措六：做好网络事件应对准备工作

风险管控不仅包括减少发生概率，还包括降低事件发生时的潜在损失。这就需要做好迅速调查事件的准备，确保拥有足够的资源，利用系统和流程来获取关键信息。如果破坏是由恶意软件导致，需将恶意软件删除。充分准备还需要有组织的计划方案，在安全事件发生时，迅速做出适当的决定，采取必要措施并加以控制。至于由谁来响应以及如何响应，可通过团队精心设计和有效沟通得出结论。

[14] 包括网络过滤、反病毒保护、主动恶意软件保护、防火墙、强大的安全策略、用户培训等。

最后，事先准备可最大程度减少最具破坏力的后果——如遇到失去操控权、无法访问数据、无法及时恢复业务。在业务的连续性设计和恢复计划中重点关注优先事项并事先做好准备，将会最大程度的减少损失。

将以上原则应用于公司的信息安全策略

企业管理的一项频繁的任务就是把本文中提供的信息安全原则转化成与之匹配的公司政策与具体实践。本章节的主旨为使此任务简单易行。根据本指南所列举的五个关键安全原则，以下因素将成为公司网络安全风险管理策略与操作的出发点。

重点着眼于信息，而不是技术

- 公司上上下下、方方面面都要对信息安全负责，还要设立专职和任命专员主导与协调全公司的信息安全措施。
- 在规划如何实现信息安全目标的时候，公司应该确定以下几点：
  - 做什么
  - 需要什么资源
  - 谁负责
  - 什么时候完成
  - 结果如何评估[15]
- 当公司内部缺乏丰富的信息安全经验的时候，需要获取外部经验，聘请外部网络安全专家参与公司的信息安全系统的设计与构建。

[15] ISO/IEC 27001:2013

建立应变思维

- 信息安全活动应当协调一致，可能的话可与其他风险控制活动进行整合，以减少重复的举措和责任。
- 不要“因噎废食”，对风险的厌恶不应该妨碍新科技的引入。信息安全措施不仅可以帮助公司实现网络安全风险管理的目标，还可以让公司在引入创新技术时找准定位。
- 确保公司的每一个项目，特别是新项目，都充分考虑了安全问题。如果在项目伊始就统一筹划，安全工作并不会显著地增加项目成本和期限。 但是，如果等项目启动后甚至是已造成破坏时再考虑安全问题，届时的财务成本、时间成本及其他负面影响就会比当初要高出几个数量级。
- 判定何种设备——尤其是公司员工和合作伙伴的移动设备——可以访问公司的网络和信息[16]，同时还应考虑如何管理公司设备上的软件及安全设置。
- 评估数据访问以确保有效的控制，保证信息的保密性、完整性和可获取性。
- 管理者应当接收、审阅和确定哪些内外部用户可以访问本部门的数据和应用程序。访问权既是责任也是风险，因此，建议对员工访问系统数据和信息的权限加以合理控制。
- 建立设备丢失或被盗的报告制度，如果可以的话，远程操作删除丢失或被盗的设备中的全部公司信息。

[16] 这需要用户自己将移动设备做相应的设置，以阻止犯罪分子远程盗取该设备上的信息。

做好应对准备工作

- 人非圣贤，孰能无过。当信息安全事故发生后，公司应把不幸转化为机会，就此在内部进行开放式讨论，从而营造出员工勇于报告安全事故的文化氛围。
- 授权专员与同僚以及行业的利益相关方进行信息分享，相互帮助构建可行的操作方案以及彼此警示潜在的网络安全攻击。
- 在处理网络安全事故，特别是网络犯罪[17]事件中，授权相关方确保从一开始就保全证据。
- 判断如何、何时将信息安全事故向网络紧急响应团队（Cyber Emergency Response Teams，CERTs）、政府机构或执法人员进行报告。

管理关注，责权对应

- 公司负责信息安全的人员应有权限联系最高管理层、使用相关工具及接受培训，只有这样，他们才能有效履行职责并在遇到信息安全威胁时应对自如[18]。
- 小公司也应当在公司内部或外部指定专人对信息安全的充分性进行日常监测，确保有人正式承担信息安全的职责。尽管可能不是一个全职角色，但对一个公司的“生死存亡”起到关键作用。
- 大公司中，职能、角色以及责任的分配交织在员工个人、（虚拟）工作组以及

[17] ICT 人员可访问以下网址，了解当发生信息安全事故时，如何获取数据、保全证据：http://cert.europa.eu/cert/plainedition/en/cert_about.html

[18] 培训中应当让员工了解一项重要的信息安全威胁——社交工程学，是指通过（网络社交）来操控人们的行为并导致他们泄露自己的敏感或保密信息的技术。

委员会之间。每个成员应当清晰地知晓其责任和职责。恰如其分的文字记录和沟通是至关重要的。

基于目标而行动

- 对外部访问公司内网或从公司内网访问外网的操作进行控制，并按照最基本的业务与员工需求[19]优先分配相应的服务与资源。
- 建议使用安全等级高的密码，还可考虑采用“密码+其他信息”的多重认证方法[20]。
- 通过加密来确保静态数据与动态传输数据的安全[21]，此外还应特别关注公共网络连接及那些如笔记本电脑、USB 和智能电话等容易丢失或被窃的移动电子设备。
- 设立详尽的备份手段和档案制度，使其符合法律和法规中关于信息保存的规范要求：
  - 备份什么样的数据以及如何备份；
  - 备份数据的频率；
  - 谁来负责备份数据和检查内容的有效性；
  - 何地以及如何储存备份数据；

[19] 公司可以考虑过滤对公司资源构成安全风险的服务与网页，例如，员工之间的文件共享和色情网站访问。过滤规则应当对所有的用户透明，同时也应明确为被误禁的业务网站解除阻断设置的流程。

[20] 多重验证方法是指多种认证信息的组合，比如所知识别（密码或 PIN 码），外物识别（智能卡或 SIM 卡），以及自身识别（指纹和虹膜识别）。

[21] 例如，电子邮件在互联网的传输过程中通常是纯文本，公司应该考虑在传输敏感信息时将电子邮件加密。

- 谁有权解除这些备份数据；
- 数据恢复过程如何操作以及如何测试的。

■ 开发提高信息安全防范意识的培训课程，包括以下课题：

- 如何保持安全有效的沟通；
- 慎用社交媒体；
- 采用安全的手段传输数字文件；
- 正确使用密码；
- 避免丢失重要的信息；
- 确保只有经过授权的人才可以接触你的信息；
- 远离电子病毒和恶意软件；
- 意识到潜在的信息安全威胁时向谁预警；
- 如何防范被他人骗取信息。

网络安全自我评估

以下章节提供简单的检查清单作为管理工具，有助于指导公司检查内部的网络安全应变能力，同时，帮助他们向参与这些网络安全工作的团队提出适当的问题。工具中的问题可以帮助企业去分辨自身所具备的特定优势和劣势并确定内部整改路径。

与此同时，对于那些刚开始引入信息安全措施的企业，或者希望以本指南信息为基础来规划他们的网络应变能力的公司，可以把这些自我评估调查表作为一个检查清单。

对下面的每一个问题，企业应该从所提供的选项中选出能够准确反应目前企业现状的一项，每一选项用不同颜色的投票符表示，如下：


这是最不希望看到的反应，显然应该考虑改进；


要想更好地保护企业，还有改进的空间；


充分反映了对网络威胁的应变能力

调查问卷的答案是每一个评估者的独特的反应。每一个问题都将对应*一份更详细的检查清单*，旨在帮助企业识别并记录企业现行的一整套基本信息安全控制的状态。在这个提问的过程中所采集的信息将有助于掌握企业信息安全管理中的缺口或漏洞，因此通过使用本指南，企业能够知道下一步需要采取何种行动。

公司对处理敏感信息行为如何评估？

没有，但是我们公司设置了防火墙，以防数据被盗；

是的，我们公司了解信息的重要性，并实施了通用安全措施；

是的，我们公司对信息进行分级处理，并且知道我们的敏感信息在哪里存储和运行。我们实施了基于敏感信息的安全措施。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
敏感数据是否被识别和分级？		
是否知道自己对已识别的敏感数据的责任？		
敏感度最高的数据是否被高度保护或加密？		
敏感数据保护规程中是否包含个人隐私信息管理？		
是否所有的员工都能区分敏感数据和非敏感数据并采取正确的保护方式？		

2

公司是否进行信息安全相关的风险评估？

我们公司不开展任何风险评估。

我们公司开展风险评估，但是不针对任何特定的信息安全相关的主题。

我们公司针对特定的信息安全主题开展安全评估。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否按照风险由高到低的顺序解决网络安全问题？		
是否已经识别那些可能导致业务流程中断的事件？是否对业务中断引起的潜在影响进行了评估？		
是否有一套现行的业务连续性计划并定期测试和更新？		
是否定期执行风险评估？并定期更新需要保护的数据和信息的级别？		
是否对贯穿所有业务流程的风险进行了识别，以防止信息处理崩溃或信息恶意使用？		

公司在什么样的管理级别下执行信息安全管理？

- 没有适当的信息安全管理。
- 信息安全仅限于IT部门，因为这里才是信息需要安全保护的地方。
- 实施公司级的信息安全管理，以确保其对整个公司产生影响。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
董事会和CEO是否制定信息安全预算？		
信息安全是否在董事层的风险管理范围之内？		
管理层是否支持公司的信息安全策略并通过适当的方式传达给了（所有的）员工？		
是否定期向董事层或管理层汇报网络安全策略、标准、流程和指南的最新进展？		
公司的管理架构中，是否至少分配了一个管理者负责保护数据和个人隐私信息？		

公司内是否有信息安全管理团队或者专门的信息安全管理职责？

- 关于信息安全，我们公司没有一个信息安全团队，也没有特定的角色去负责。
- 我们公司没有信息安全（管理）团队，但公司明确定义了特定的角色去负责信息安全。
- 我们公司有信息安全（管理）团队或者公司专门界定了一套信息安全（管理）职责。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否指定专门的信息安全专家或者团队去协调内部信息安全意见并在信息安全方面为决策层提供管理帮助？		
所指定的信息安全专家或团队是否负责修订和系统地更新基于重大变更或重大事件的信息安全策略？		
所指定的信息安全专家或者团队是否有足够的预见性来支撑其参与公司任何与信息相关的举措？		
是否有不同的经理负责不同类型的数据？		
（现行的）信息安全策略是否可行且有效？除此之外，信息安全团队的效力是否有独立的机构或者审计人员对其进行定期审核？		

如何应对来自于拥有公司敏感数据访问权限的供应商的信息安全风险？

- 我们和供应商之间有基于双方相互信任的关系。
- 我们在一些合同中包含了信息安全相关的条款。
- 我们有相应的流程来验证第三方供应商的登录，并与供应商沟通具体的安全指南且由供应商签字确认。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
承包商和供应商是否可以通过含有近期照片的ID标志进行识别？		
是否有针对承包商和供应商进行背景调查的措施？		
当承包商或者供应商完成了他的任务之后，其对设施和信息系统的访问权限是否会自动中断？		
当信息丢失或者被盗时，供应商是否知道在你公司的应对方案怎样以及谁负责？		
是否能够确保供应商保持其对软件和应用的安全补丁更新？		
在与承包商和供应商的合同协议中，是否明确地定义了安全需求？		

公司是否定期评估计算机和网络安全？

- 我们公司不进行安全审查或者入侵测试来评估我们的计算机和网络安全。
- 我们没有系统化的途径去开展安全审查和入侵测试，但是会通过一些特定的措施评估计算机和网络安全。
- 定期的安全审查和入侵测试是我们公司系统性评估计算机和网络安全的一部分。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否定期测试并记录所发现的风险？		
是否有规程来评估公司信息系统面临的人为风险，包括欺诈、社交工程和信任滥用？		
是否要求其信息服务提供者出具相应的安全审查报告？		
在安全审查期间，是否对每种类型存储数据的用途都进行了评估？		
是否会审查信息流程及规程与其他公司政策和标准的匹配度？		

公司在引进新技术时是否会评估潜在的信息安全风险？

- 评估信息安全不是新技术引进流程中的一部分。
- 在新技术引进的过程中，信息安全只会在特定的基础上实施。
- 新技术实施的流程中包含信息安全。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
考虑推行新技术时，是否会评估其对已经制定的信息安全策略的潜在影响？		
推行新技术时，是否有保护措施降低风险？		
推行新技术的流程是否文档化？		
推行新技术时，是否可以依赖合作伙伴关系，促使协同合作以及共享重要安全信息？		
现行的信息安全策略是否通常被看作是技术机遇的障碍？		
是否会在系统的生命周期内用安全系统开发方法去管理新技术？		

公司是否组织信息安全方面的培训？

我们公司完全信任我们的员工，并不认为信息安全指导有更多价值。

我们公司只有IT人员会接受特定的培训以保障我们的IT环境。

我们公司会在全员范围内组织定期的信息安全培训。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否有适用于活动现场员工的一些信息安全知识普及会议？		
是否教育员工要警惕信息安全漏洞？		
是否有关于上报系统和服务的安全漏洞或安全风险的用户指南？		
员工是否知道如何正确管理信用卡数据和个人隐私信息？		
第三方用户（相关方）是否也能接受相应的信息安全培训，并且能定期更新组织政策和程序？		

公司内部如何使用密码?

- 公司内同事间共享密码和公司内没有关于如何安全使用密码的策略或定期更换密码的相关规定。
- 包括管理层在内的所有员工都有单独的密码，但对密码复杂程度没有要求，可以更换密码但不是强制性的。
- 包括管理层在内的所有员工都有个人密码，该密码要满足一定要求且须定期更换。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否已经建立并且强制实施一个针对于所有公司资产的、全球通用的密码管理规定？		
是否确保所有的密码能满足以下要求：未将密码保存在可以轻易接触到的文件中；密码设置不会过于简单、空白或者是干脆是默认设置；这些密码不会长期不变或很少变更，尤其对于移动设备来说？		
针对未授权的物理访问是否做了很好的保护？		
所有的用户或分包商是否清楚地知道如何保护那些无专人看管的设备（比如及时退出登录）？		
针对那些诱骗大家泄露安全信息的社交工程陷阱，是否对员工做过专门的培训，告诉他们如何识别与应对？		

10

公司内是否制定了关于合理使用互联网及社交媒体的政策？

公司没有关于如何合理使用互联网的相关政策。

是的，公司制定了相关政策，并且所有员工均可在集中办公地点获取，但并未要求大家签署。

是的，公司有相关政策，且是员工劳动合同的一部分，所有的员工专门签署过。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否为员工制定了处理与新闻、社交媒体关系等通用传播指南与流程。		
一旦员工违反了公司的传播指南，是否有纪律处分流程？		
是否有指定的通信经理或专门团队负责互联网监控，以便评估公司网络声誉的风险与状态。		
当员工、其他内部用户或黑客滥用公司系统执行非法操作时，是否评估公司应承担的责任？		
是否采取措施防止员工或其他内部用户攻击其他网站？		

公司是否对信息安全相关事件进行过评测、报告或跟进？

公司对所实施的安全措施的效率及适用性从未进行过监控、报告或跟进。

公司采用一些工具与方法，对公司部分现行的安全措施的效率及适用性进行监控、报告和跟进。

公司采用必要的工具与方法，对公司所有的现行安全措施的效率及适用性进行监控、报告和跟进。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否审查维护信息安全事故的流程与日志，并采取积极措施预防类似信息安全事故的再次发生？		
是否检验数据隐私等方面的合法性、合规性？		
是否开发一些工具来协助管理安全状况评估，以优化降低潜在风险的能力？		
是否制定包括目标、进度评估、潜在合作机会分析等内容的信息安全路线图？		
是否将信息安全监控报告与事故报告提供给官方或者行业协会等其他相关组织？		

12

公司如何更新内部信息安全系统？

公司基本上是依托供应商的自动补丁管理来更新系统。

公司采取按月系统化更新安全补丁的方式。

公司已有漏洞管理流程并可持续检索可能产生漏洞的信息（比如通过订阅新漏洞自动警告服务），同时安装相应补丁包以降低风险。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否将漏洞扫描纳入定期系统维护计划中？		
在操作系统发生改变后，是否对应用系统进行检验与测试？		
用户能否自行检测是否存在未打补丁的应用程序？		
用户是否清楚他们应将个人移动设备中包括安全软件在内的操作系统和应用程序更新为最新版本？		
用户是否接受过相关培训并能够识别合法的警告信息，比如权限更新请求（不同于假冒杀毒请求），并且一旦发现可疑的情况能以正确的方式通知安全团队？		

13

公司是否对应用程序及系统的用户访问权限进行定期检查与管理？

公司对应用程序及系统的访问权限从来不进行删除或检查。

只有当员工离职时公司才会对应取消其应用程序及系统的访问权限。

公司制定了访问控制策略，对所有相关业务应用程序及配套系统所分配的用户访问权限进行定期检查。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否制定相关政策和流程来限制电子信息系统及设施的访问权限？		
是否根据隐私政策明确所搜集的信息（比如客户的物理地址、电子邮箱、浏览历史等）及其用途？		
是否制定相关政策和程序详细说明物理访问的控制方法，比如门锁、访问控制系统或视频监控系统？		
当团队成员结束雇佣关系时，是否切断其对公司设施及信息安全系统的访问权限？		
是否对敏感数据实行分级管理（高度机密、敏感、仅供内部使用）？并对拥有相应访问权限的用户也进行分类登记？		
是否开发了专门的流程来控制公司电子信息系统的远程访问？		

14

公司是否允许员工使用手机、平板电脑等个人设备来存储和传送公司信息？

是的，员工无须采取任何额外的安全措施就可以使用个人设备来存储和传送公司信息。

公司有政策不允许员工使用个人设备存储与传送公司信息，但是从技术层面上，员工可以无须采取任何额外的安全措施就可以这么做。

只有在采取了相关安全措施或提供了专业解决方案的前提下，员工才能使用个人设备存储与传送公司信息。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否采用被广泛认可的“使用个人设备办公”的政策？		
未授权用户是否不得使用移动设备？		
是否所有接入公司网络的设备与连接都会被永久识别？		
是否对每个移动设备加密，以确保数据的安全性与完整性？		
公司层面是否清楚，即使员工对其个人设备负有责任，公司仍需为数据负责？		

15

公司是否已经采取措施防止存储信息丢失？

公司目前尚无数据备份/可用性流程。

公司有数据备份/可用性流程，但没有执行过恢复测试。

公司已有数据备份/可用性流程，且该流程包含了恢复/弹力测试。公司将备份信息存储在其他的安全地点或者采用其他的高可用性解决方案。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否有足够多有能力的团队成员创建可检索备份及归档副本？		
是否通过多电源供电、永不间断电源（UPS）或备用发电机等方式确保设备永不断电？		
是否经常测试备份媒介，以确保能够在恢复程序所要求的期限内恢复数据？		
针对丢失或失窃的移动设备，是否有相关的报告程序？		
是否对员工进行专门培训，告诉他们误删信息时如何应对以及如何恢复信息？		
是否采取措施确保存储地点备份数据的安全性与完整性？		

16

公司是否已经做好了处理信息安全事故的准备？

公司不会出现信息安全事故。即使出现了，公司员工也完全有能力处理。

公司有事故管理程序，但不适用于处理信息安全事故。

公司有专门的信息安全事故处理程序，包括必要的升级与沟通机制。公司努力提升事故处理效率，以便在未来能更好自我保护。

下述问题为一份基本的信息安全检查清单，旨在协助公司进行自身信息安全管理水平评估。	是	否
是否对不同类型的事故（比如从拒绝服务到违反保密要求）进行分级，并采取不同的方式处理？		
是否有事故管理沟通计划？		
万一发生事故，是否清楚应该通知哪些部门以及如何通知？		
针对不同类型的信息安全事故，是否分别明确对应负责人的联系方式？		
是否有内部沟通经理负责与员工及其家人的联系？		
信息安全事故发生后，是否能积累经验教训，不断提升公司的事故管理水平？		

本指南附有配套电子版附件，提供从操作标准到技术标准更详细的资料。你可进入网址 www.iccwbo.org/cybersecurity 查询。该网站纳入了一系列相关的全球框架、资源、联系方式，以及由国际商会各国家委员会和成员陆续提供的本地框架。目前纳入的仅仅是已发布的相关资源概览，相信随着时间的推移，相关资料会进一步更新和充实。

www.iccwbo.org/cybersecurity

本国际商会企业网络安全指南亦在 www.iccwbo.org/cybersecurity 有在线版本，该网站为一站式资源门户网站，提供针对信息安全技术与功能方面的国际相关的、本地化的标准、实操及相关建议。

网站特点：

- 下载《国际商会企业网络安全指南》
- 提供该指南的不同翻译版本
- 提供全球公认的优秀实操、标准及框架的链接
- 提供活跃于网络和信息安全领域的全球公共机构与组织清单
- 提供由企业、政府机构或其他实体开发的具体国别资源的链接

国际商会:

国际商会是全球性商业组织，是全球工商界的权威代言机构。

国际商会的宗旨是促进开放的国际贸易与投资，助力企业迎接全球挑战与机遇。国际商会于 20 世纪初由一群富有远见的“和平商人”创立。自成立以来，国际商会始终坚信，贸易是保证世界和平与繁荣的重要力量。

国际商会主要有三大职能：规则制定、争议解决及政策建议。由于国际商会的会员企业及协会本身均从事国际业务，因此国际商会在制定跨境业务行为规则方面具有较强的权威性。尽管这些规则属于自愿性质，但实际上每天发生的无数交易都在遵循这些规则并且成为国际贸易中不过或缺的一环。

国际商会同时提供各种基本服务，其中最重要的是国际商会仲裁院——一家世界领先的仲裁机构；另一项服务是世界商业联合会，该联合会依托国际商会遍布世界各地的商会网络，促进最佳商业实践的互动与交流。此外，国际商会还提供专业培训与论坛，同时也是国际商务、银行业务与仲裁方面的实践、教育参考工具的业界领先出版商。

国际商会会员中的商业领袖与专家围绕国际贸易、投资政策及相关技术领域的广泛问题展开讨论并确立商业立场，包括反腐败、银行业务、数字经济、营销道德、环境与能源、竞争政策及知识产权等。

国际商会与联合国、世界贸易组织及包括 G20 在内的政府间论坛组织保持密切合作。

国际商会成立于 1919 年，目前拥有来自 130 多个国家和地区的 600 多万家企业、商会及商业协会会员。国际商会依托其国家委员会与各国会员开展工作，阐述他们关心的问题并向当地政府传达国际商会的商业观点。

33-43 avenue du Président Wilson, 75116 Paris, France
电话：+33 (0)1 49 53 28 28 F +33 (0)1 49 53 28 59
邮箱： icc@iccwbo.org www.iccwbo.org
国际商会出版号:450/1081-5
ISBN: 978-92-842-0336