CSA GCR cloud security alliance
GREATER CHINA REGION ®

基于NIST网络安全框架的勒索软件风险管理内部报告

目　录

致 谢

云安全联盟大中华区（简称：CSA GCR）隐私与个人信息保护法律工作组在2021 年 4 月成立。由原浩、方婷担任工作组联席组长，工作组专家来自竹辉律师事务所、西北大学、恩智浦、中伦文德事务所、美柚、中国工商银行、绿盟科技、美云智数、上海 CA、上海网综所、埃森哲、亚萨合莱、360 政企安全、软通动力信息、艾贝链动等十多个单位。

本报告由 CSA 大中华区隐私与个人信息保护法律 工作组专家翻译，感谢以下专家的贡献（排名不分先后）：

联席组长：原 浩

原创作者：高健凯　贺志生 张元恺 沈 勇

审核专家：郭鹏程　赵 晔　原 浩　姚 凯

研究协调员：高健凯

贡献单位：北森云计算有限公司

原文作者：William C. Barker、William Fisher、Karen Scarfone 和 Murugiah Souppaya 版权、专利和其他原始权利归属于 NISTIR 8374 中所指称的相关方。（出版物的声明部分从略）

关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c-csa.cn/research/） 上查看，如本白皮书有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正!

联系邮箱： research@c-csa.cn；

云安全联盟 CSA 公众号：

基于 NIST 网络安全框架的勒索软件风险管理内部报告（NISTIR 8374）

[中文版说明]

2022 年 2 月，美国商务部下设的国家标准与技术研究所（NIST）发布了最终版《基于 NIST 网络安全框架的勒索软件风险管理内部报告》，这是对 2020 年以来重大勒索攻击事件从技术和管理层面的整体策略回应，同时也是履行其基于 2014 年《网络安全促进法》和制定、完善《提升关键基础设施网络安全框架》（Framework for Improving Critical Infrastructure Cybersecurity，2018 年 1.1 版本，本文统称网络安全框架，下同）的行政职责。

CSA 大中华区隐私与个人信息保护法律工作组翻译了该文件（有删减），以及对国内的关键信息基础设施保障和提高应对勒索攻击的能力上有所借鉴，特别是在支持《关键信息基础设施安全保护条例》制度落地的方法论和策略方面，且在具体的应用场景上与网络安全等级保护的措施形成有益的补充和对照。

值得注意的是，本报告的风险控制主要是在组织层面实现，这与《关键信息基础设施安全保护条例》专章突出行业、领域的保护工作部门的机制有所不同，企业在参考时应予以关注和区别。

摘 要

勒索软件（攻击）是一种恶意攻击，攻击者加密组织的数据，并要求付款以恢复访问。攻击者也可能窃取组织的信息，并要求额外的付款，以换取不向当局、竞争对手或公众披露信息。

本报告确定了网络安全框架 1.1 版下的安全目标，支持识别、防范、检测，以应对勒索软件事件并从中恢复。本报告可作为管理勒索软件事件风险的指南，为衡量组织在应对勒索软件威胁和处理事件潜在后果方面的准备程度提供支持。

关键词

网络安全框架；检测；识别；保护；勒索软件；恢复；响应；风险；安全

1.引言

本报告可帮助组织和个人管理勒索软件事件的风险，为衡量组织在应对勒索软件威胁和处理事件潜在后果方面的准备程度提供支持；也可作为是改善网络安全的契机，帮助挫败勒索软件（攻击等威胁）。本报告确定了《提升关键基础设施网络安全框架》1.1 版下的安全目标，支持识别、防范、检测，以应对勒索软件事件并从中恢复。

1.1 勒索软件的挑战

勒索软件是一种恶意软件，它加密组织的数据，并要求付款作为恢复对该数据访问的条件。勒索软件还可以用来窃取组织的信息，并要求支付额外的费用，以换取不将信息披露给当局、竞争对手或公众。勒索软件攻击的目标是组织的数据或

关键基础设施，扰乱或中止组织的运营，给管理层带来两难选择：支付赎金并希望攻击者遵守恢复访问且不泄露数据的承诺；或者不支付赎金并尝试恢复运营。使用勒索软件进入某个组织的信息系统，在广泛的网络攻击中是很常见的方法，但其（特点）旨在强制（受害者）支付赎金。并且攻击者不断尝试采用新的手段向受害者施加压力，用于传播勒索软件的技术也在继续发生变化。

勒索软件攻击与其他网络安全事件不同。在其他网络安全事件中，攻击者可能会隐蔽（不会直接影响业务运营）的获取知识产权、信用卡数据或个人身份信息等资料，然后披露这些信息以获取收益；勒索软件却可能会对业务的运营产生直接影响。在勒索软件（攻击）事件发生后，企业可能没有充分时间缓解或补救影响、恢复系统，或通过必要的业务、合作伙伴和公共关系渠道沟通。出于这个原因，组织做出准备尤为关键。这包括教育网络系统的用户、响应团队和业务决策者，让他们在潜在勒索事件发生之前，了解预防和处理这些危害的流程和程序。

幸运的是，企业可以遵循建议的步骤准备和减少勒索软件攻击得逞的可能性。这包括以下内容：识别和保护关键数据、系统和设备；尽早发现勒索软件事件（最好是在勒索软件侵入之前）；并应对任何勒索软件事件和从中恢复。有许多资源可用 于协助组织开展这些工作。它们包括来自美国国家标准与技术研究所（NIST）、联邦调查局（FBI）和国土安全部（DHS）的信息。本文附录 A 中列出了 NIST 的其他资源。

本报告表 1 中的安全能力和措施支持预防和缓解勒索软件事件的详细方法。认识到采取所有这些措施超出了一般人员的能力范围，下面的文本仅包含了组织可以采取的基本预防措施，以防勒索软件威胁。并非所有这些措施都适用于所有组织的所有情况。本报告中的指导意见可视为最佳实践，但并非法律或监管要求。

【基本的勒索病毒提示】

即使不采取本报告中描述的所有措施，组织现在也可以采取一些基本的预防措施，防止勒索软件威胁并从中恢复。这些措施包括：

（1）教育员工如何避免勒索软件的感染。

不要打开来源不明的文件和链接，除非首先扫描病毒或仔细检查链接。

避免在办公计算机上使用个人网站和个人应用程序（如电子邮件、聊天和社交媒体）。

未经事先授权，不要将个人拥有的设备连接到工作网络。

（2）避免在系统中出现勒索软件可能利用的漏洞。

保持相关系统完全打好补丁。定期检查可用的补丁程序，并在可行的情况下尽快安装这些补丁。

在所有网络系统中采用零信任原则。管理所有网络功能的访问，在可行的情况下对内部网络分区，以防恶意软件在潜在的目标系统中扩散。

只允许安装和执行授权的应用程序。配置操作系统和/或第三方软件，使其只运行 授权的应用程序。可以建立审查机制予以支持，在可信应用列表中添加或删除授权的应用程序。

向技术供应商告知期望（如使用合同语言），推动供应链采取措施阻止勒索软件攻击。

（3）快速检测并阻止勒索软件攻击和感染。

无论什么时候都使用恶意应用检测软件，如防病毒软件，将其设置为自动扫描电子邮件和移动存储设备。

持续监测目录服务（和其他主要用户存储），发现疑似或主动攻击的迹象。

禁止访问不受信任的网络资源。使用的产品或服务屏蔽已知的恶意或疑似恶意的服务器名称、IP 地址或端口和协议。包括使用为地址的域名部分提供完整性保护的产品和服务（如 hacker@poser.com）。

（4）让勒索软件更难传播。

尽可能使用具有多因子认证的标准用户账户，非管理权限的账户。

引入认证延期登录或设置账户自动锁定，预防密码猜测。

为组织的所有资产和软件分配和管理凭证授权，并定期验证每个账户只拥有必要的访问权限，遵循最小特权原则。

以固定格式存储数据（这样，当有新数据时，数据库不会自动覆盖旧数据）。

只允许外部人员通过安全的虚拟专用网络（VPN）连接访问内部网络资源。

（5）更易于从未来的勒索软件事件中恢复存储的信息。

制定一个事件恢复计划。制定、实施并定期演练事件恢复计划，明确决策的角色 和策略。该计划应显示关键服务和其它商业基础服务，以便确定业务恢复的优先次序。事件恢复计划可以是业务连续性计划的一部分。

备份数据，安全备份和测试恢复。谨慎制定策略、实施和测试数据备份和恢复策略，并保护和隔离重要数据的备份。

保留联系方式。维护一份最新的勒索软件攻击的内外部联系人名单，名单包括执法部门、法律顾问和事件响应资源。

1.2 适用对象

本报告的适用对象是拥有可能遭受勒索软件攻击的网络资源的任何组织，无论所在行业或规模如何。任何组织：中小型企业（SMB）、小型联邦机构和其他小型组织，以及工业控制系统（ICS）或运营技术（OT）的运营商都可以利用本报告，

并鼓励他们进一步考虑查阅网络安全框架，其中许多措施可以在不耗费大量资源的情况下进行。以下两类组织均可获得相应参考价值：

熟悉 NIST 网络安全框架，以帮助识别、评估和管理网络安全风险，并希望通过解决勒索软件问题改善其风险状况。

不熟悉网络安全框架，但希望实施风险管理框架以应对勒索软件威胁。

1.3 其他指导性资源

除了前述引用的资源外，NIST 的国家网络安全卓越中心（NCCoE）还编制了支持、缓解勒索软件威胁的指南。NIST 还有许多其他资源，虽然不是专门针对勒索软件的，但包含了关于识别、防范、检测、响应勒索软件事件并从中恢复的有价值信息。有关参考资料的清单，请参见参考资料部分；有关 NIST 资源的更广泛清单，请参见附录 A。

2.勒索软件风险管理

本报告将组织的勒索软件预防和缓解要求、目标、风险偏好和资源与 NIST 网络安全框架的要素保持一致，帮助组织确定并优先考虑提高其安全性和抗击勒索软件攻击的能力。组织可以使用本报告作为分析自身准备度的指南。这样做将有助于组织确定当前的概况或状态，并设定一个目标概况以确定差距。

表 1 定义了勒索软件风险管理。前两栏列出了网络安全框架中的相关类别和子类别，组织可将其作为勒索软件风险管理计划的目标结果。第三栏简要说明了每个子类别如何帮助识别、防范、检测、应对勒索软件事件并从中恢复。

本简介还引用了参考资料。这些是关键基础设施部门中常见的标准、指南和实践的具体部分，说明了实现每个子类别相关结果的方法。网络安全框架中的参考资料是说明性的，基于框架开发过程中最常用的跨部门指南，但并不穷尽。

例如，表 1 的第二栏引用了网络安全框架中包括的两个信息参考资料中的相关要求。这两个信息参考资料是国际标准化组织/国际电工委员会（ISO/IEC）27001:2013 和 NIST SP 800-53 第 5 版。

网络安全框架为每个子类别列出了额外的信息参考资料。这些参考资料将在本指导文件的在线版本中不时更新。

【五种网络安全框架功能类别】

识别——形成一种组织理解，管理系统、人员、资产、数据和性能的网络安全风险。识别功能中的活动是有效使用该框架的基础。了解组织业务背景、了解投入关键功能的资源以及相关的网络安全风险，使得组织能够聚焦和分级投入，与组织风险策略和业务（安全）需求一致。

保护——制定并实施适当的保障措施，确保关键服务的正常运行。保护功能的作用能够遏制潜在网络安全事件影响的蔓延。

检测——制定并实施适当的机制，识别网络安全事件的发生。检测功能能够及时发现网络安全事件。

响应——针对检测到的网络安全事件，制定并实施适当的应对活动。应对的作用能够防止潜在网络安全事件影响的蔓延。

恢复——制定并实施适当的活动，维护恢复计划，恢复因网络攻击期间受损的任何服务或性能。恢复功能支持及时恢复或重建正常运营，减少网络安全事件的影响。

表 1：勒索软件风险管理概况

类别	子类别和选定的信息性参考	应用资料	《关键信息基础设施安全保护条例》对应要求
NIST 的风险管理框架的功能要素	对应到具体的控制项，并通过 ISO 和 NIST 的其他标准进行补强	解释和详细组织任何进行相应控制	增加本列，建立在关键信息基础设施领域进行勒索风险管理的映射，以供国内 CII 运营者参考
识别			
资产管理（ID.AM）：根据数据、人员、设备、系统和设施对组织目标和组织风险战略的相对重要程度，识别和管理使组织能够实现业务目的的数据、人员、设备、系统和设施。	ID.AM-1：清查组织内的物理设备和系统 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 5 CM-8, PM-8. 5	应该清点、审查和维护物理设备，确保这些设备不会受到勒索软件的攻击。在勒索软件攻击后的恢复阶段，如果有必要重新安装应用程序，拥有一份硬件清单也是有益的。	保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。
	ID.AM-2：清点组织内的软件平台和应用程序 ISO/IEC 27001:2013 A.8.1.1,A.8.1.2 NIST SP 800-53 Rev. 5 CM-8, PM-8. 5	软件清单可以跟踪诸如软件名称和版本、当前安装的设备、最后的补丁日期和当前已知的漏洞等信息。这些信息支持补救可能被勒索软件攻击利用的漏洞。	

	ID.AM-3：绘制组织通信和数据流图 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 5 AC-4, CA-3, CA-9, PL-8	如果攻击者在一个环境中横向移动，有助于列举哪些信息或进程面临风险。	
	ID.AM-4：对外部信息系统编目 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 5 AC-20, SA-9	这对于规划与合作伙伴的沟通及为应对勒索软件事件而暂时断开与外部系统连接的可能行动非常重要。识别这些也将帮助组织规划安全控制措施的实施，并确定可能与第三方共享控制措施的领域。	
	ID.AM-5：资源（例如，硬件、设备、数据、时间、人员和软件）根据其分类、关键性和业务价值进行优先排序。 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 5 CP-2, RA-2, RA-9, SC-6	这对于了解勒索软件事件的真正范围和影响至关重要，而且对于未来勒索软件事件、应急响应和恢复行动的应急计划也很重要。有助于运营和事件响应者确定资源的优先次序，并支持应对未来勒索软件事件、采取应急响应和恢复行动的应急计划。如果有相关的工业控制系统（ICS），其关键功能也应纳入应急响应和恢复行动中。	
	ID.AM-6：为全体员工和第三方利益相关者（如供应商、客户和合作伙伴）确立网络安全	重要的是，组织中的每个人都要了解他们在防止勒索软件事件方面的作用和责任，以及	

	角色和责任 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 5 CP-2, PM-11, PS-7	在适用的情况下应对勒索软件事件并从中恢复。这些角色和责任应正式记录在事件响应计划中。需要明确规定事件响应计划定期演练（如至少每年执行事件响应桌面模拟）。	
商业环境（ID.BE）：了解组织的使命、目标、利益相关者和活动，并确定其优先次序；这一信息用于告知网络安全的作用、责任和风险管理决策。	ID.BE-2：组织在关键基础设施及其行业部门的地位得到确认和沟通 ISO/IEC 27001:2013 A.4.1 NIST SP 800-53 Rev. 5 PM-8	这使国家计算机安全事件响应小组能够更好地了解目标组织在关键基础设施环境中的地位，并允许他们在出现跨部门影响时及时作出反应。这也鼓励该组织及其外部利益相关者考虑勒索软件攻击的下游影响。	
	ID.BE-3：确定并传达组织任务、目标和 活动的优先次序 NIST SP 800-53 Rev. 5 PM-11,SA-14	这有助于运营和事件响应者对资源进行优先排序。它支持应对未来勒索软件事件的应急计划、应急响应和恢复行动。	
	ID.BE-4：确定提供关键服务的依赖性和关键职能 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 5 CP-8, PE-9, PE-11, PM-8, SA-20	这有助于确定在支持组织的核心业务功能方面至关重要的二级和三级组件。这对于确定应对未来事件的应急计划和对勒索软件事件的应急响应的优先次序是必要的。如果有相关的ICS，其关键功能应包括在应急响应和恢复行动	

		中。	
治理（ID.GV）：管理和监测组织的监管、法律、风险、环境和运营要求的政策、程序和流程得到理解，并告知（内外部相关者）网络安全风险管理政策和策略。	ID.GV-1：制定并 传达组织网络安全政策 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 5 AC-01,AU-01, CA-01, CM-01, CP-01, IA-01.01，ir-01，pe-01,pl-01，pm-01，RA01、SA-01、SC-01、SI-01	建立和沟通预防或缓解勒索软件事件所需的政策是至关重要的，也是所有其他预防和缓解活动的基础。在实际情况下，应定期审查这些政策，以反映风险的动态性质和需要不断调整的现实。	专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责： （一）建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划……
	ID.GV-3：了解并管理有关网络安全的法律和监管要求，包括对隐私和公民自由的义务 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 NIST SP 800-53 Rev. 5 CA-07, RA-02	这对于制定网络安全政策和确立应对未来勒索软件事件的应急计划的优先次序尤为必要。	
	ID.GV-4：治理和风险管理流程应对网络安全风险 ISO/IEC 27001:2013 A6 NIST SP 800-53 Rev. PM-53, PM-7,9, PM-10, PM-11, SA-2	必须将勒索软件的风险纳入组织风险管理治理，以建立适当的网络安全政策。	

风险评估（ID.RA）：组织了解网络安全对组织运作（包括任务、功能、形象或声誉）、组织资产和个人的风险。	ID.RA-1：识别和记录资产的脆弱性 ISO/IEC 27001:2013 A.12.6.1,A.18.2.3 NIST SP 800-53 Rev. 5 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	识别和记录组织资产的漏洞对于制定缓解或消除这些漏洞的计划并确定其优先次序至关重要。这些行动也是评估和应对未来勒索软件事件的应急计划的关键，将减少勒索软件攻击成功的可能性。	专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：…… （二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估…… 运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。
	ID.RA-2：从信息共享论坛和来源获得网络威胁情报 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 5 PM-15,PM-16, SI-5	从信息共享源接收和使用网络威胁情报，可以减少对勒索软件攻击的暴露，并促进对新威胁的早期检测。	
	ID.RA-4：确定潜在的商业影响和可能性 ISO/IEC 27001:2013 A.16.1.6, 6.1.2 NIST SP 800-53 Rev. PM-59, PM-11, RA-2, RA-3, SA-20	需要了解潜在勒索软件事件的业务影响，支持网络安全的成本效益分析，并确定勒索软件响应和恢复计划中的活动重点。了解潜在的业务影响也有助于在发生勒索软件攻击时做出应急响应决定。	

	ID.RA-6：确定风险应对措施并排定优先次序 ISO/IEC 27001:2013 A.6.1.3 NIST SP 800-53 Rev. PM-54, PM-39	应对勒索软件事件并从中恢复的相关费用，直接受到应对预计风险的应急计划的有效性的影响。	
风险管理战略（ID.RM）：建立组织的优先事项、约束条件、风险容忍度和假设，并用于支持运营风险决策。	ID.RM-1：组织利益相关者建立、管理并同意风险管理程序 ISO/IEC 27001:2013 A.6.1.3, 8.3, 9.3 NIST SP 800-53 Rev. 5 PM-4, PM-9	建立和执行组织政策、角色和责任取决于利益相关者是否同意并实施有效的风险管理流程。这些流程应考虑到勒索软件事件的风险。应定期审查这些政策，以反映风险的动态性质和随着时间推移需要调整的现实。	运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。 运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。
供应链风险管理（ID.SC）：组织的优先事项、约束条件、风险容忍和假设已经确立，并用于支持与管理供应链风险 相关的风险决策。该组织已经建立并实施了识别、评估和管理供应链风	ID.SC-5：与供应商和第三方供应商一起进行响应和恢复规划和测试 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. CP-52, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9	勒索软件应急计划应与供应商和第三方供应商协调，并应包括测试计划活动。该计划应包括组织、其供应商和第三方供应商都受到勒索软件影响的情况。	运营者采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

险的程序。			
保护			
身份管理、认证和访问控制（PR.AC）。对物理和逻辑资产及相关设施的访问仅限于授权的用户、流程和设备，其管理与（被非授权访问的）风险评估结果保持一致。	PR.AC-1：发放、管理、验证、撤销和审计授权设备、用户和流程的身份和凭证。 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-4, IA-5，IA-6,IA-7, IA-8, IA-9, IA-10, IA-11	大多数勒索软件的攻击都是通过网络连接进行的，勒索软件的攻击往往从凭证泄露开始（如未经授权分享或捕获登录身份和密码）。适当的凭证管理至关重要，尽管不是唯一需要的缓解措施。	专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：……（七）对关键信息基础设施设计、建设、运行、维护等服务实施安全管理……
	PR.AC-3：远程访问得到管理 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev.5 AC-1, AC-17, AC-19, AC-20, SC-15	大多数勒索软件攻击都在远程进行。管理与远程访问相关的权限可以帮助保持系统和数据文件的完整性，防止恶意代码的插入和数据的渗出。使用多因子认证是减少账户被破坏可能性的一个关键而且容易实现的方法。	
	PR.AC-4：访问权限和授权的管理，包括最小特权和职责分离的原则。 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3,	许多勒索软件事件通过攻破用户凭证或调用对系统有不必要的特权访问的进程而发生。这是预防此类事件的一个非常重要的管理步骤。	

	A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. AC-1, AC-2,3, AC-5, AC-6, AC-14, AC-316、AC-24		
	PR.AC-5：网络完整性得到保护（例如网络隔离、网络分段）。 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 5 AC-4, AC-10, SC-7	网络分割或隔离可以防止恶意软件在潜在的目标系统中扩散，从而限制勒索软件事件的范围（如从商业信息技术网络转移到运营技术或控制系统）。将 IT 和 OT 网络分开并定期验证其独立性至关重要。这不仅降低了 OT 系统被破坏的风险，而且还可以在业务 IT 系统从勒索软件中恢复时继续进行低级别的关键操作。这对包括安全仪表系统（SIS）在内的关键 ICS 功能特别重要。	
	PR.AC-6：身份被证明并与凭证绑定，并在互动中被断言。 ISO/IEC 27001:2013 A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. AC-1、AC-2、AC-3、AC-16、AC-19、AC-24。 IA-1,IA-2,IA-4, IA-5, IA-8, PE-2, PS-3	被破坏的凭证是勒索软件事件中常见的攻击媒介。身份应该被证明，然后与凭证绑定（如正式授权个人的双因素认证），以限制凭证被破坏或发放给未授权个人的可能性。	

意识和培训（PR.AT）：向组织的人员和合作伙伴提供网络安全意识教育，并对其进行培训，以便根据相关政策、程序和协议履行与网络安全有关的职责和责任。	PR.AT-1：所有用户都应告知并接受培训 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 5 AT-2, PM-13	大多数勒索软件的攻击是由从事不安全行为的用户、实施不安全配置的管理员、或安全培训不足的开发人员造成的。	专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：……（四）认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议； （五）组织网络安全教育、培训；……
数据安全（PR.DS）：信息和记录（数据）的管理符合组织的风险战略，以保护信息的保密性、完整性和可用性。	PR.DS-4：保持足够的容量以确保可用性 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. AU-54, CP-2, SC-5	确保数据的充分可用性可以减少勒索软件的影响。这包括保持异地和离线数据备份的能力，在必要时测试平均恢复时间和系统冗余度。	专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：……（六）履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度……
	PR.DS-5：防止数据泄漏的保护措施得到实施 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. AU-54, CP-2, SC-5	双重勒索：既要求付款以恢复数据访问，又要求不在其他地方出售或公布数据是很常见的，所以数据泄漏预防解决方案很重要。	
	PR.DS-6：使用完整性检查机制验证软件、固件和信息的完整性 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4	完整性检查机制可以检测到被篡改的软件更新，这些软件可以被用于插入启用勒索软件事件的恶意软件。	

	NIST SP 800-53 Rev. 5 SC-16, SI-7		
	PR.DS-7：开发和测试环境与生产环境是分离的。 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 5 CM-2	将开发和测试环境与生产环境分离，可以防止勒索软件从开发和测试系统发布到生产系统。	
信息保护过程和程序（PR.IP）：安全政策（涉及目的、范围、角色、责任、管理承诺和组织实体间的协调）、流程和程序维护并用于管理信息系统和资产的保护。	PR.IP-1：创建和维护信息技术/工业控制系统的基线配置，并纳入安全原则（如最小功能概念）。 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 5 CM-2,CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	基线对于建立一套系统需要执行的功能很有用，这样就可以对任何偏离该基线的行为评估，确定潜在的网络风险。未经授权的配置变更可以作为恶意攻击的一个指标，可能会导致引入勒索软件。	运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。 专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责： （一）建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；……（七）对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；
	PR.IP-3：配置变更控制流程已经就绪 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev.	适当的配置变更流程可以帮助执行软件的及时安全更新，维护必要的安全配置设置，并阻止用含有恶意软件或不满足访问管理策略的产品替换代码。	

	5 CM-3, CM-4, SA-10		
	PR.IP-4：备份、维护和测试信息 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. CP-54, CP-6, CP-9	定期维护和测试的备份对于及时和相对无痛地从勒索软件事件中恢复至关重要。备份应该是安全的，确保不会被勒索软件破坏或被攻击者删除。备份应离线存储。	
	PR.IP-9：响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）已经就绪并得到管理 ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 NIST SP 800-53 Rev. 5 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	响应和恢复计划应包括勒索软件事件。响应计划的副本应保持离线状态，以防事件发生时取消了对目标网络内的软拷贝的访问。在事件分级过程中，应适当地对勒索软件事件进行优先排序，目的是立即遏制勒索软件的传播。	
	PR.IP-10：测试响应和恢复计划 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 5 CP-4, IR-3, PM-14 •	应定期测试勒索软件的响应和恢复计划，确保风险和响应假设及流程在不断变化的勒索软件威胁方面是最新的。响应和恢复计划的测试应包括任何相关的ICS。流程需要更新和维护，以适应不断变化的组织需求和结构，以及新的勒索软件类型和策略。测试培训了需要执行该计划的人员。	

维护（PR.MA）：根据政策和程序，维护和修理工业控制和信息系统组件。	PR.MA-2：组织资产的远程维护得到批准、记录，并防止未经授权访问。 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 5 MA-4	远程维护提供了一个进入网络和技术的渠道。如果管理不善，违法或犯罪人员可能会利用这种访问改变配置，允许引入恶意软件。组织或其供应商对所有系统组件的远程维护必须得到验证，确保这一过程不会为 OT 或 IT 网络提供后门访问。	专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：……（七）对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；
保护性技术（PR.PT）：管理技术安全解决方案，确保系统和资产的安全和复原力，与相关政策、程序和协议保持一致。	PR.PT-1：根据政策确定、记录、实施和审查审计/日志记录 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. AU-1, AU- AU-2,3, AU-4, AU-5, AU-6, AU-7。A-8、A-9、A-10、A-12、A-13、A-14、A-16	审计/日志记录的可用性可以帮助检测意外行为，支持取证响应和恢复过程。	运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。
	PR.PT-3：通过配置系统，只提供必要的功能，体现最小功能原则 ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 5 AC-3, CM-3 7	保持最小功能原则可能会阻止潜在目标系统之间的移动（如从管理网络移动到操作过程控制系统）。	

检测			
异常活动和事件（DE.AE）：检测异常活动，了解事件的潜在影响。	DE.AE-3：从多个来源和传感器收集事件数据并关联 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 NIST SP 800-53 Rev. AU-56, CA-7, IR-4, IR-5, IR-8, SI-4	多个来源和传感器协同安全信息和事件管理（SIEM）解决方案提高了网络的可见性，有助于在早期发现勒索软件，并有助于了解勒索软件如何通过网络传播。	专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：…… （二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；…… 保护工作部门应当定期组织开展本行业、本领域关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。
	DE.AE-4：事件的影响得到确定 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 5 CP-2, IR-4, RA-3, SI-4	确定事件的影响可以为确定勒索软件攻击的响应和恢复优先级提供信息。	
安全持续监测（DE.CM）：监测信息系统和资产，识别网络安全事件并验证保护措施的有效性。	DE.CM-1：监测网络以检测潜在的网络安全事件 NIST SP 800-53 Rev. 5 AC-2, AU- CA-12,7, CM-3, SC-5, SC-7, SI-4	网络监测可能会在恶意代码被插入或大量信息被加密和泄露之前检测到入侵。	

	DE.CM-3：监测人员活动，发现潜在的网络安全事件 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 NIST SP 800-53 Rev. 5 AC-2, AU- AU-12,13, CA-7, CM-10, CM-11	监测人员活动可能会发现内部威胁或不安全的工作人员行为或泄露的凭证，并阻止潜在的勒索事件。	
	DE.CM-4：检测到恶意代码 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 5 SI-3, SI-8	检测可能表明，勒索软件事件正在发生或即将发生。恶意代码通常不会立即执行，因此在勒索软件攻击执行之前的插入恶意代码和激活恶意代码阶段之间可能有时间检测到恶意代码。	
	DE.CM-7：监测未经授权的人员、连接、设备和软件 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	未经授权的人、连接、设备和软件是发动勒索软件攻击的潜在资源。监测可以在勒索软件攻击执行之前发现。	
	DE.CM-8：进行漏洞扫描 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev.	勒索软件攻击期间可能会利用漏洞。定期扫描可以让组织在执行勒索软件之前检测并缓解大多数漏洞。	

	5 RA-5		
检测程序（DE.DP）：维护和测试检测过程和程序，确保了解异常事件。	DE.DP-1：明确检测的角色和职责有助于明确责任。 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 5 CA-2, CA-7, PM-14	明确理解角色和职责是可问责的关键，鼓励遵守组织政策和程序，帮助检测勒索软件攻击。	
	DE.DP-2：检测活动符合所有适用的要求 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 5 AC-25, CA-2, CA-7, PM-14, SI-4, SR-9	探测活动应按照组织政策和程序进行。	
	DE.DP-3：检测过程经过测试 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 5 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4	测试为基于勒索软件的攻击提供了正确检测过程的保证，但并不是说 所有的入侵尝试都会被检测到。 测试是对需要执行计划的人员的培训。	
	DE.DP-4：沟通事件检测信息 ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 NIST SP 800-53 Rev. AU-56, CA-2, CA-7, RA-5,	为了能够在勒索软件攻击完全实现之前采取补救措施，必须及时沟通异常事件。	

	SI-4		
	DE.DP-5：检测过程不断改进 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 5 CA-2, CA-7, PL-2, PM-14, RA-5, SI-4	勒索软件攻击中使用的策略在不断完善，因此检测过程必须不断发展 以跟上新的威胁。	
响应			
响应规划（RS.RP）：执行和维护响应过程和程序，确保对发现的网络安全事件作出响应。	RS.RP-1：在事中或事后执行响应计划 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. CP-52, CP-10, IR-4, IR-8	立即执行响应计划的公共关系和通信响应部分是必要的，可以阻止恶化或持续的数据外流，阻止感染扩散到其他系统和网络，并及时地传递信息，以尽量减少进一步的损害，包括声誉或法律方面的损害。	专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：…… （三）按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；……
沟通（RS.CO）：与内部和外部的利益相关者协调响应活动（如来自执法机构的支持）。	RS.CO-1：需要响应时，人员应知道角色和行动顺序 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1 NIST SP 800-53 Rev. CP-52, CP-3, IR-3, IR-8	对勒索软件事件的响应包括技术和业务响应。有效和高效的响应需要所有各方了解其角色和责任。通信响应角色应正式记录在事件响应和恢复计划中，并应通过演练计划加强。	关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。

	RS.CO-2：事件的报告符合既定标准 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. AU5-6, IR-6, IR-8	对勒索软件事件的响应包括技术和业务响应。有效和高效的响应需要预先建立的报告标准，并在事件发生期间遵守这些标准。	
	RS.CO-3：根据响应计划共享信息 ISO/IEC 27001:2013 A.16.1.2,A.7.4, A.16.1.2 NIST SP 800-53 Rev.5 CA-2, CA- CP7,-2, IR-4, IR-8, PE-6, RA-5, SI-5 4	信息共享的重点包括阻止感染扩散到其他系统和网络，以及高效的信息传递。	
	RS.CO-4：根据应对计划与利益相关者协调 ISO/IEC 27001:2013 A.7.4 NIST SP 800-53 Rev. 5 CP-2, IR-4, IR-8	与关键的内外部利益相关者的协调对于阻止错误信息的传播和建立高效的信息传递等优先事项非常重要。	
	RS.CO-5：与外部利益相关者自愿分享信息，以实现更广泛的网络安全态势感知。 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 5 PM-15, SI- 5	信息共享可能会对取证带来帮助，并减少勒索软件攻击的影响和利润。自愿共享是对任何监管或其他合规性要求的报告和共享的补充。	

分析（RS.AN）：进行分析以确保有效的反应并支持恢复活动。	RS.AN-1：调查来自检测系统的通知 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 NIST SP 800-53 Rev. AU-56, CA-7, IR-4, IR-5, PE-6, SI-4	应及时和全面调查来自检测系统的通知，因为这些通知往往表明勒索软件攻击处于早期阶段，可以预先阻止或减轻影响。	
	RS.AN-2：了解事件的影响 ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 5 CP-2, IR-4	了解影响将决定恢复计划的实施。 企业应设法了解勒索软件攻击的技术影响（如哪些系统不可用），然后了解由此对业务产生的影响（如哪些业务流程无法交付）。这将有助于确保响应和恢复工作有适当的优先次序和资源，同时可以实施业务连续性计划。	
	RS.AN-3：取证 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev.5 AU-7, IR-4	取证有助于确定遏制和消除攻击的根本原因，包括重设被攻击者盗取的凭证密码、删除攻击者使用的恶意软件、删除攻击者使用的持久性机制等。 取证也可以为恢复过程提供信息，并协助报告和分享行动。	

	RS.AN-5：建立程序，接收、分析和应对从内外部来源（如内部测试、安全公告或安全研究人员）织披露的漏洞。 NIST SP 800-53 Rev. 5 PM-15, SI-5	分析过程可以防止未来的成功攻击和勒索软件扩散到其他系统和网络。它还可以帮助恢复利益相关者的信心。	
缓解（RS.MI）：为防止事件扩大，减轻其影响，并解决事件而开展的活动。	RS.MI-1：事件得到控制 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. IR-54	必须立即采取行动，防止勒索软件扩散到其他系统和网络，减轻其影响，并解决该事件。遏制勒索软件包括任何相关的 ICS。	关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。 发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。
	RS.MI-2：事件得到缓解 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. IR-54	必须立即采取行动隔离勒索软件，尽量减少对数据的损害，防止感染在网络内和其他系统和网络中扩散，并尽量减少对任务或业务的影响。	

	RS.MI-3：新发现的漏洞被缓解或被记录为可接受的风险 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. IR-54	漏洞管理使勒索软件攻击成功的概率降到最低。如果漏洞不能被修补或缓解，记录这种风险至少可以将其纳入未来的决策中，并为可能受到勒索软件事件影响的利益相关者提供透明度。	
改进（RS.IM）:通过吸收从当前和以前的检测/响应活动中获得的经验教训，改进组织的响应活动。	RS.IM-1：应对计划中体现了经验教训 ISO/IEC 27001:2013 A.16.1.6, A.10 NIST SP 800-53 Rev. 5 CP-2, IR-4, IR-8	最大限度的减少了未来勒索软件攻击成功的概率，并有助于恢复利益相关者的信心。	
	RS.IM-2：更新应对策略 ISO/IEC 27001:2013 A.16.1.6, A.10 NIST SP 800-53 Rev 5 CP-2, IR-4, IR-8	最大限度地减少了未来勒索软件攻击成功的概率，并有助于恢复利益相关者的信心。	
恢复			
恢复规划（RC.RP）：执行和维护恢复过程和程序，确保恢复受网络安全事件影响的系统或资产。	RC.RP-1：在网络安全事件发生时或发生后执行恢复计划 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev.	在确定勒索攻击根本原因后立即启动恢复计划可以减少损失。	保护工作部门应当按照国家网络安全事件应急预案的要求，建立健全本行业、本领域的网络安全事件应急预案，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组

	5 CP-10, IR-4, IR-8		织提供技术支持与协助。
改进（RC.IM）：通过将吸取的经验教训纳入未来的活动，改进恢复规划和进程。	RC.IM-1：恢复计划体现所学到的 经验教训 ISO/IEC 27001:2013 A.16.1.6, A.10 NIST SP 800-53 Rev 5 CP-2, IR-4, IR-8	最大限度地减少了未来勒索软件攻击成功的概率，并有助于恢复利益相关者之间的信心。	
	RC.IM-2：更新恢复战略 ISO/IEC 27001:2013 A.16.1.6, A.10 NIST SP 800-53 Rev. 5 CP-2, IR-4, IR-8	这对保持应对未来勒索软件攻击的应急计划的有效性是必要的。	
通信（RC.CO）：与内外部各方（如协调中心、互联网服务提供商、受攻击系统的所有者、受害者、其他 CSIRT 和供应商）协调恢复活动。	RC.CO-1：管理公共关系 ISO/IEC 27001:2013 A.6.1.4, A.7.4	通过公开和透明将业务影响降到最低，并恢复利益相关者的信心。	保护工作部门应当按照国家网络安全事件应急预案的要求，建立健全本行业、本领域的网络安全事件应急预案，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。
	RC.CO-2：事件发生后声誉得到修复 ISO/IEC 27001:2013 A.7.4	声誉修复将业务影响降到最低，并恢复利益相关者的信心。	

	RC.CO-3：向内外部利益相关者以及执行和管理团队传达恢复活动的信息 ISO/IEC 27001:2013 A.7.4 NIST SP 800-53 Rev. 5 CP-2, IR-4	有关恢复活动的沟通有助于最大限度地减少业务影响，并恢复利益相关者的信心。	

参考文献：

1、美国国家标准和技术研究所（NIST，2018 年）《改善关键基础设施网络安全框架》，1.1 版。https://doi.org/10.6028/NIST.CSWP.04162018

2、国际标准化组织/国际电工委员会（ISO/IEC）ISO/IEC 27001:2013，https://www.iso.org/isoiec-27001-information-security.html

3、联合任务组（2020）信息系统和组织的安全和隐私控制。(国家标准与技术研 究所，马里兰州盖瑟斯堡），NIST 特别出版物（SP）800-53，Rev.5。包括截至 2020 年 12 月 10 日的更新，https://doi.org/10.6028/NIST.SP.800-53r5

附录 A

除了本文引用的其他资源外，NIST 国家网络安全卓越中心（NCCoE）还制作了额外的指导以支持缓解勒索软件威胁。这些指导包括：

NIST 特别出版物（SP）1800-26《数据完整性 检测和应对勒索软件和其他破坏性事件》，说明组织在攻击发生时如何处理，以及需要具备哪些能力检测和应对破坏性事件。

NIST SP 1800-25《数据完整性 识别和保护资产免受勒索软件和其他破坏性事件的影响》，说明组织如何在攻击发生前努力识别资产和潜在的漏洞，并对发现的漏洞进行补救以保护资产。

NIST SP 1800-11《数据完整性 从勒索软件和其他破坏性事件中恢复》，说明数据完整性受到攻击后的恢复方法。

《保护数据免受勒索软件和其他数据丢失事件的影响》，是管理服务提供商执行、维护和测试备份文件的指南，对从勒索软件攻击中恢复至关重要。

NIST 有许多其他资源，虽然不是专门针对勒索软件的，但包含了关于识别、保护、检测、应对勒索软件事件和恢复的宝贵信息。以下是几个重点介绍的资源。如需更完整的资源清单，请访问 NIST 的勒索软件保护和响应网站：https://csrc.nist.gov/ransomware。

（1）提高远程工作、远程访问和自带设备（BYOD）技术的安全性。

• 远程工作：任何时间、任何地点的工作项目

• NIST SP 800-46 企业远程工作、远程访问和自带设备（BYOD）安全指南，修订版 2

（2）对软件进行修补，以消除漏洞。

• NIST SP 800-40 企业补丁管理技术的指南，修订版 3

• 关键网络安全：企业项目补丁

（3）使用应用控制技术防止勒索软件的执行。

• NIST SP 800-167，应用程序白名单指南

（4）寻找关于安全配置软件以消除漏洞的一般层次指导。

• 国家检查列表计划

（5）获得关于已知漏洞的最新信息。

• 国家安全漏洞数据库（NVD）

（6）网络安全事件的恢复规划。

• NIST SP 800-184，网络安全事件恢复指南

（7）在勒索软件造成的中断后恢复业务的应急计划。

• NIST SP 800-34 联邦信息系统应急计划指南，修订版 1

（8）处理勒索软件和其他恶意软件事件。

• NIST SP 800-83 台式机和笔记本电脑的恶意软件事件预防和处理指南，修订版 1

（9）处理一般的网络安全事件。

• NIST SP 800-61，计算机安全事件处理指南，修订版 2

（10）进行网络安全风险管理。

• 开始使用 NIST 网络安全框架：快速入门