Enterprise Strategy Group | Getting to the bigger truth.™

ESG 白皮书

# 存储在确保网络复原能力的过程中发挥的作用

作者：
Scott Sinclair，ESG 实践总监兼高级分析师
Monya Keane，ESG 资深研究分析师

2022 年 01 月

This ESG White Paper was commissioned by IBM
and is distributed under license from TechTarget, Inc.

# 目录

## 执行摘要

数据作为一种会带来变革的商业资产，其作用正在不断增强。对应用开发的投资增加、全新的 DevOps 实践，以及商业智能、分析和机器学习需求的提升，几乎所有企业都在加速数据的创建和使用。同时，他们也在扩大使用数据的领域。这种数据的激增与加速运营带来的更大压力相互叠加，导致了 IT 基础架构和 IT 运营的变得尤其复杂。

上述因素致使企业及其基础架构面临着遭遇恶意攻击、人为错误和疏忽行为的巨大风险。不幸的是，传统的策略无法充分保证在发生这些类型的事件之后，业务运营能够持续进行。公司可以同时尝试各种方法，试图防止攻击或其他违规行为的发生，但功能的差距、整合缺陷以及管理的复杂性会使得安全目标的实现既费时、又困难。

将组织思维从预防转变为对事件的准备——例如，实施具有内置网络复原力的存储解决方案——这是保护关键数据资产，快速响应勒索软件和其他网络攻击，并从中恢复的关键。

## 简介

IT 部门面临着各种新的挑战。近一半（46%）的 ESG 调查对象表示，IT 部门今天面临的情况比两年前更加复杂。这种复杂性的增加可能是由于正在进行的数字化转型规划（29%），更大的数据量（35%），网络安全环境的快速演变（37%），以及努力遵守新的数据安全和隐私法规（32%）。[1]

同时，企业正在努力解决关键 IT 技能短缺的问题。事实上，48%的受访企业表示他们没有足够的网络安全专家，这是最常提到的短缺。此外，这些企业正在处理日益兴起的应用程序、设备以及远程和移动办公的问题，这扩大了 IT 部门负责保护的安全边界。[2]

鉴于现代 IT 的复杂性、不断扩散的数据和持续增长的网络攻击威胁，IT 团队往往难以跟上步伐。如果试图仅靠内部人员来解决复杂性的问题，这是一场注定失败的战斗。成功需要对基础架构本身进行现代化改造。而且在这过程中，IT 决策者不只是寻找一些用于满足应用需求或是简化操作的工具。要实现真正的成功意味着找到最适合的技术，同时改善应用环境的网络复原能力。

## 网络攻击和勒索软件的威胁不断上升

企业面临着越来越多的网络安全威胁，这可能是由于对网络犯罪分子的经济刺激越来越大而导致的。例如，2020 年美国公众对联邦调查局互联网犯罪投诉中心（IC3）的投诉比 2019 年增加了 69%，报告损失金额超过 41 亿美元。[3] 此外，在过去五年中，IC3 报告的损失金额共计为 133 亿美元。[4] 截至 2020 年第四季度在美国，勒索软件攻击企业后的平均中断时间为 21 天。[5] 很显然，勒索软件对企业运营的负面影响巨大。

IT 的复杂性与其面对网络攻击的脆弱性之间存在着强烈的关联性。伴随着 IT 日益复杂，网络攻击的频率会变得越来越高，所造成的损失代价也会越来越大。

勒索软件是一种普遍性的威胁，而且有针对性攻击企业最宝贵的资产——数据。IC3 在 2020 年确定了 2474 起报告的勒索软件事件，ESG 发现，调查中 63%的组织在过去一年中都经历过勒索软件攻击。事实上，9%的企业每天都会遭遇勒索软件的攻击（见图 1）。[6]

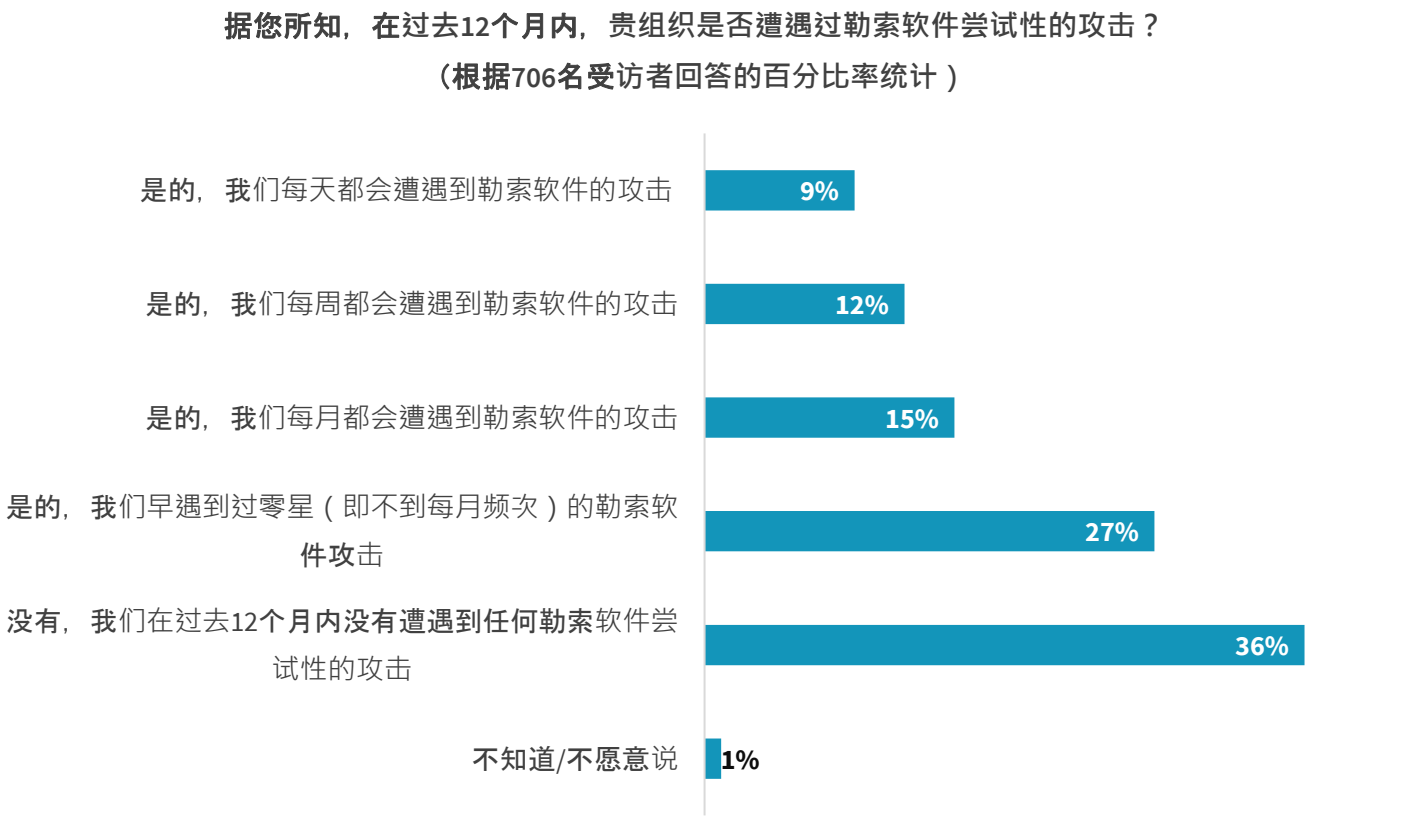
[1] 数据来源：ESG 完整的调查结果，*2022 年企业技术开支意向调查*，2021 年 11 月。
[2] 同上。
[3] 数据来源：联邦调查局互联网犯罪投诉中心，2020 年互联网犯罪报告。联邦调查局互联网犯罪投诉中心，*2020 年互联网犯罪报告*。
[4] 同上。
[5] 数据来源：Coveware 博客，*随着越来越少的公司支付数据渗透勒索要求，勒索软件的支付量下降*，2021 年 2 月。
[6] 数据来源：ESG 完整的调查结果，*2022 年企业技术开支意向调查*，2021 年 11 月。

针对勒索软件的保护需要一个超越传统网络安全领域的技术战略——同时，这应该充分利用数据存储和数据保护领域的技术进步。

## 数据存储应对网络威胁过程中的作用

存储系统和存储管理员在防范勒索软件方面都发挥着重要作用。当 ESG 询问 IT 决策者，他们的组织有哪些措施来打击勒索软件攻击，或者降低其影响时，67%的受访者表示会使用网络工具来主动避免勒索软件，53%的受访者谈及到数据恢复能力，如物理隔离（见图 2）。[7] 这两项普遍的答复选项强调了不仅要实施避免攻击的措施，而且

图 1. 63%的受访者在过去 12 个月中遭遇过勒索软件的攻击

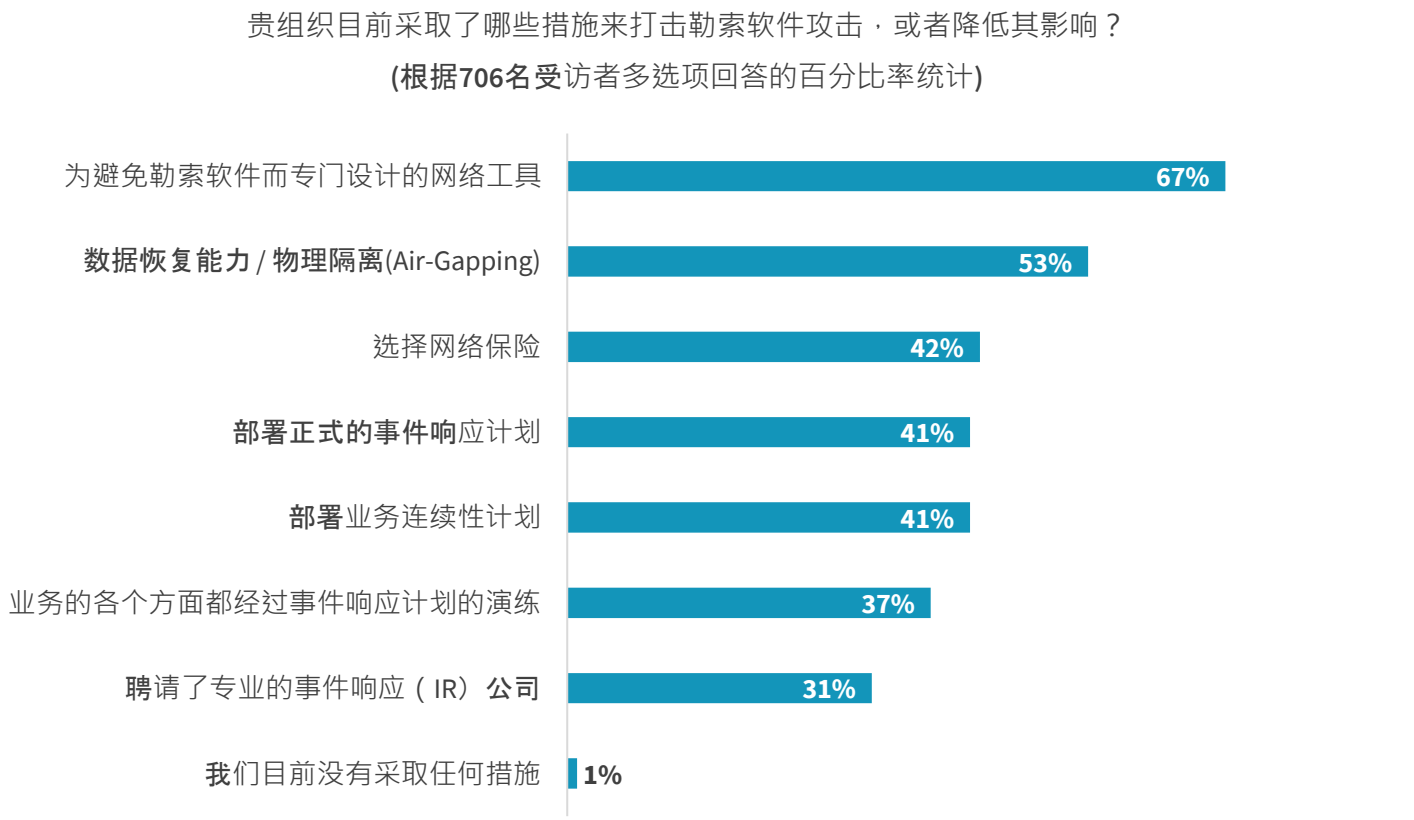



*数据来源：TechTarget 有限公司，ESG 事业部*

要投资于那些能够确保企业在攻击不可避免地发生时做好恢复准备的解决方案。重要的是，要避免单纯设定规则政策来打击勒索软件，或缓解其影响，然后就此止步。这种“以偏概全”的方法创造出一种错误的安全感。在努力减轻攻击影响的同时，实际上还应该建立一个有效的数据恢复计划，以便不时之需。

[7] 数据来源：ESG 完整的调查结果，*2022 年企业技术开支意向调查*，2021 年 11 月。

图 2. 打击勒索软件，或缓解其影响的常见措施




*数据来源：TechTarget 有限公司，ESG 事业部*

重要的是要记住，打击勒索软件的攻击与传统的数据恢复是完全不同的两件事。通常情况下，企业几乎总是希望通过使用最新的副本来恢复他们的数据。但对于勒索软件，IT 部门通常不知道该使用哪个副本是“良好的”；因此，恢复风险往往会更大，而且可能需要更长的时间。一些勒索软件的攻击不仅针对数据，而且还针对备份基础架构本身。这就是为什么先进的数据存储能力是有效恢复勒索软件的基础。

采取图 2 中措施无疑是明智之举，应该尽量增加这些举措。同时企业还必须明白，没有任何一种防御措施对勒索软件的恢复是 100%有效的。虽然专门用于识别和避免勒索软件以及恢复数据的工具很重要，但这只是努力的一部分。即使有最好的防御，也有可能被攻击绕开。企业必须为这种情况做好准备，并评估如何通过尽可能快地恢复方法来减少对业务影响。为了最大限度地减少勒索软件的整体风险，企业应该寻找方法来加快他们识别攻击的速度，如何快速地减轻各种损害，以及如何快速地用已知的良好的副本加以恢复。

这就是强大的网络复原力发挥作用的地方，考虑到所有的数据处理组件，即硬件、软件、人员和流程。在制定网络复原策略时，企业应该从问 "*我们如何保护？*"转向 "*如果我们被勒索软件击中，我们能多快恢复？我们的业务能多快恢复正常？*"

## 数据存储与数据保护：明确重点，最大限度地减少勒索软件的风险

勒索软件的恢复是灾难恢复的一种形式，但勒索软件的影响与火灾或洪水的影响完全不可同日而语。毕竟，通常来说，你会知道火灾何时被完全扑灭。勒索软件更像是墙内隐藏的火花，有可能在任何时候重新点燃。存储管理人员需要专注于某些领域，以帮助减少与勒索软件相关的风险。因为速度是至关重要的，他们应该确定所在的组织可以多快响应：

- 识别风险。
- 量化已经造成的损害。
- 通过确定一个已知的良好的副本，使用该副本进行恢复，并最终恢复正常运行，从而减轻损失。

采取“这不会发生在我们身上”的方法无疑是一种将有风险隐藏起来的鸵鸟心态。企业必须主动出击，在真正需要之前，制定一个有效的数据存储和保护解决方案。

## 与 IBM 携手，从网络安全转向网络复原力

凭借在网络安全和风险管理方面的丰富经验，IBM 是行业内公认的网络复原力的领导者，并提供一套全面的高级存储和数据保护解决方案，这包括：

- IBM FlashSystem、IBM Cloud Object Storage 以及 IBM Spectrum Scale，这些初级存储解决方案具有数据防篡改和加密功能。
- IBM **磁带存储**支持数据的防篡改和加密，并通过物理隔离提供保护。
- IBM Spectrum Copy Data Management 软件管理和保护数据的副本。
- IBM Spectrum Protect **套件**提供额外保护。Spectrum Protect 软件定义的存储可以将数据放在闪存、磁盘、对象存储和物理或虚拟磁带上。然后，通过识别与正常访问模式的巨大偏差来检测恶意软件和勒索软件活动。
- QRadar **和** Storage Insights **解决方案**利用人工智能增强的功能帮助加速检测潜在威胁。

## 发挥 IBM Cyber Vault 的网络复原能力

存储在防止勒索软件方面的作用怎么强调都不为过。存储软件可以看到对主数据所做的更改。因此，存储软件处于一个很好的位置来识别攻击开始的时间。同时，这也是获取和保护二级副本的技术——这使得存储在数据恢复方面发挥着至关重要的作用。考虑到这些事实，在 IBM 的网络复原工具箱中最有用的工具之一就是 IBM Cyber Vault。

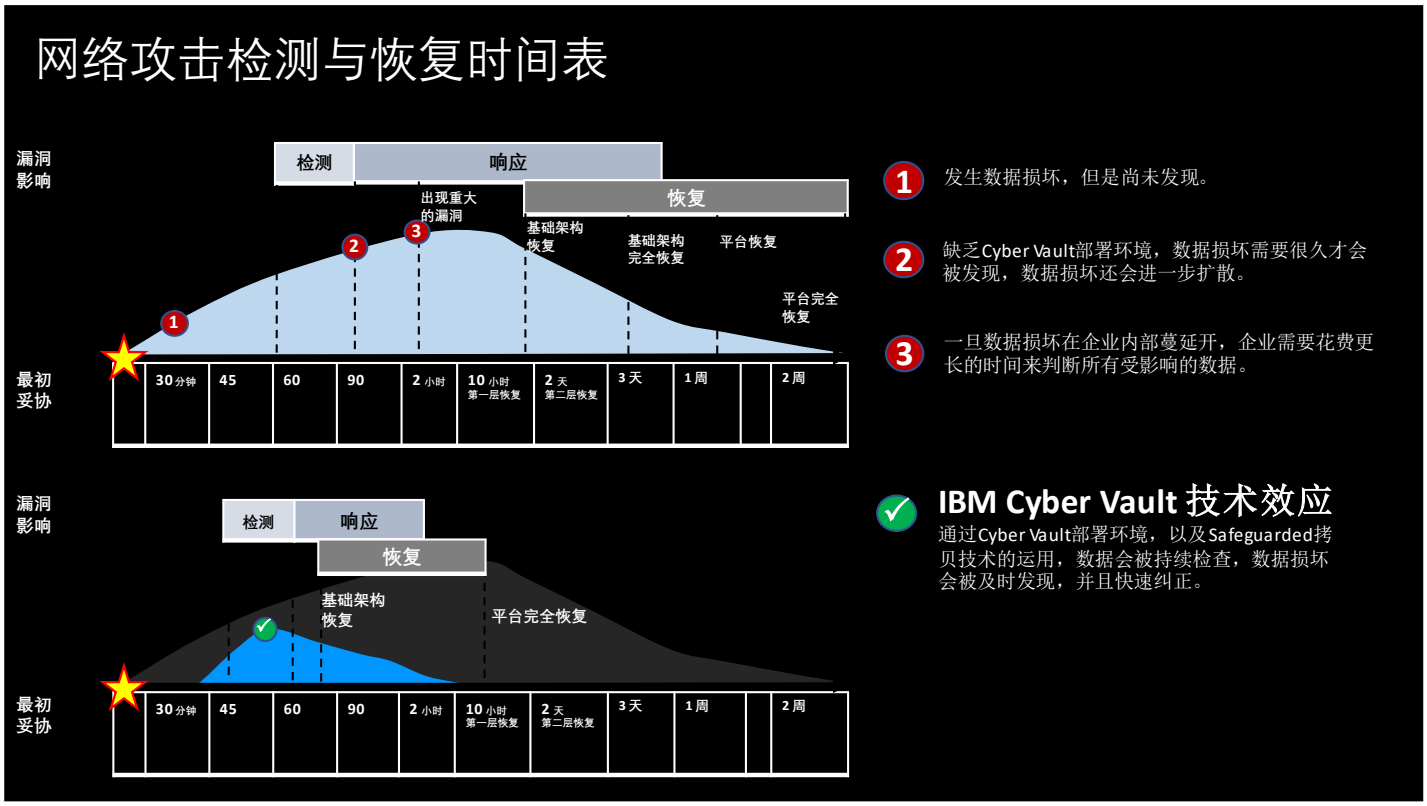
IBM Cyber Vault 是一种安全方法，用于从网络攻击中快速恢复。它建立在 IBM Safeguarded 拷贝之上，这是一种定期创建隔离的、防篡改的快照技术。Cyber Vault 分析这些快照，寻找潜在的恶意变化，从而指向可能存在的勒索软件。IBM Cyber Vault 还与 IBM QRadar 与 IBM Storage Insights 集成，以便实现更快地检测。它对防篡改的副本的验证使管理员能够快速识别一个良好的副本，对其进行测试，然后用它进行恢复。

特别在提高速度方面，IBM Cyber Vault 能够帮助存储管理员加快响应：

- **发现识别**——QRadar 和 Storage Insights 的整合提供了增强的检测和监控。

- **量化并降低损害**——这是一个自动化过程。对攻击的早期自动检测显然能够实现更快恢复。
- **识别已知的良好的副本**——假如检测到威胁，就会自动生成防篡改的数据副本。
- **恢复运行**——实现在几小时内快速恢复的可能性，而非等待数天甚至数周时间（见图 3）。

图 3. 如何通过 IBM Cyber Vault 加速网络恢复




*Source: IBM*

## 更大的真相

IT 基础架构正在继续变得日益复杂，增加了发生人为错误、系统故障或疏忽的可能性。同时，组织内部和外部的恶意行为者都在不遗余力地寻找和利用薄弱环节。

毫无疑问，安全事件将会不可避免的发生。这一事实应该迫使组织的思维方式从被动变为主动——从执着于试图防止攻击转变为在安全故障发生时做好准备和应对工作。这就是组织在从网络安全到网络复原力的过程中必须进行的转变。

许多企业和组织正在按照 NIST 网络安全框架提供的指导来制定他们的网络复原战略，该框架建议组织确定关键资源，保护这些资源，检测故障和漏洞，并计划从网络事件中进行响应和恢复。领先的组织正在特别关注 IT 基础架构能力，这些能力可以通过数据发现、副本管理、加密、访问控制和不可改变的存储等能力来增强其网络复原力，同时保持多种数据恢复选项。

对于 IT 和商业领袖来说，网络复原力就是要做出正确的技术决策和正确的商业决策——最终目的是保障业务的正常运作。

**Enterprise Strategy Group** is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188