CLAROTY

Cyberworld

调研报告

2024 年全球 CPS 安全状况：中断对业务的影响

网络攻击影响关键任务型基础设施，分析其造成的财务损失和运营后果

执行摘要

本项全球性调研对1,100名网络安全专业人员进行了访问，受访者的工作职责是保护网络化物理系统(CPS)，包括运营技术(OT)、物联网(IoT)、医疗物联网(IoMT)和楼宇管理系统(BMS)，这些系统是全球关键基础设施领域的核心。本项调研旨在了解网络安全负责人应对影响CPS的网络攻击的经验，尤其关注网络安全事件造成的财务影响和业务中断。主要的调研结果包括：

1. 影响 CPS 的网络安全事件造成巨额财务损失

- **45%**的受访者表示，在过去的12个月里，影响CPS的网络攻击造成了50万美元或更多的财务损失；**27%**的受访者的财务损失高达100万美元以上。
- 造成财务影响的因素有很多，其中常见的是收入损失（**39%**的受访者选择）、恢复成本（**35%**）和员工加班（**33%**）。
- 受财务影响最严重的行业是化学制造、电力和能源、采矿和材料，每个行业中有**54%**至**55%**的受访者表示，在过去的12个月里，网络安全事件造成的损失超过50万美元。

2. 勒索软件依然严重影响恢复成本

- **53%**的受访者支付了50万美元以上的赎金，恢复加密系统和文件的访问权限，从而恢复运营。
- 这一问题在医疗保健行业尤为严重，针对医院和临床环境的勒索软件与敲诈勒索攻击有增无减。**78%**的受访者支付了50万美元以上的赎金。

造成财务影响的主要因素：

- 收入损失
- 恢复成本
- 员工加班

78%

的医疗保健机构表示，在过去一年中，支付了50万美元以上的赎金。

©Copyright Claroty Ltd. All rights reserved

3. 全球范围内的企业受到不同程度的运营影响

- **49%**的受访者表示，在过去一年中，因网络攻击导致的运营停机时间超过12小时；**33%**的受访者表示，至少停机一天。
- **49%**的受访者表示，恢复需要一周或更长时间；**29%**的受访者表示，恢复需要一个多月。
- 常见的网络安全影响是流程操控（**38%**的受访者选择）和流程中断（**37%**），这些影响与运营停机息息相关。

4. 远程访问和供应链问题

45%的受访者表示，他们所在的企业至少有一半的CPS资产已连接到互联网。随着连接性和融合性的提高，对CPS进行远程访问的需求大幅增加。常见的连接方法是通过VPN（**36%**的受访者选择），但这种方法缺乏CPS专属的安全控制。

82%的受访者表示，在过去的12个月里，至少发生过一次网络攻击；**45%**的受访者表示，发生过五次或五次以上网络攻击。这些网络攻击源自第三方供应商对CPS环境的访问。然而，**63%**的受访者承认，他们对第三方与CPS环境的连接只有部分了解或完全不了解。

5. 弹性策略在降低风险方面取得成效

受访者对其企业的风险降低措施表现出越来越强的信心，表明其在CPS环境的防御技术日益成熟，并且对关键基础设施受到的影响有了更深入的了解。

相比于12个月前，**56%**的受访者表示，对其企业的CPS抵御网络攻击的能力更有信心。此外，**72%**的受访者预计，在未来12个月内，其CPS的安全性将得到量化改善。

49%

的受访者表示，在过去一年中，企业因网络攻击经历了超过12小时的运营停机，而恢复花费了一周或更长时间。

82%

的受访者表示，至少经历过一次源自第三方访问其CPS环境的网络攻击。

©Copyright Claroty Ltd. All rights reserved

调研报告介绍

网络安全负责人完全了解网络犯罪和高级攻击，对支持工业和医疗算力基础设施的CPS有哪些影响。无论是国家支持的网络攻击，还是营利性犯罪分子发动的攻击，都日益频繁地针对OT、IoT、IoMT和BMS。这些网络安全事件导致了业务中断、服务交付延迟、数据丢失和数据篡改等负面后果，还可能影响患者护理、公共安全、国家和经济安全等各个方面。

制造业、医疗保健、能源、石油和天然气等关键基础设施领域的首席信息安全官(CISO)在试图管理风险与缓解威胁时，经常发现自己陷入了攻击者和企业上级领导施加的压力之中。如果网络安全负责人要与高管、董事会进行交流，必须根据业务风险阐明威胁，即它们会造成多大的成本。

为了应对这种动态威胁，缓解这些威胁的压力，本调研报告旨在量化破坏性攻击对这些关键系统的网络安全和运营影响，并提供网络安全负责人可以利用的上下文，以制定能充分保护CPS的策略。

为了更深入了解关键基础设施领域CPS中断的潜在影响，Claroty将调查重点放在以下方面：

- 专门针对 CPS 的攻击对企业造成财务损失。
- 网络安全和运营影响，例如流程操控或中断，或者系统不可用，从而造成高昂的恢复成本。
- 过度连接和不受管理的第三方访问关键系统所带来的广泛风险。
- 企业在过去12个月内采取的风险降低措施，以及对措施有效性的信心。

©Copyright Claroty Ltd. All rights reserved

调研方法

Claroty委托研究公司Pollfish，对1,100名全职信息安全、OT工程、临床或生物医学工程、以及设施管理或工厂运营的专业人员进行了调研。受访者分别来自美洲、欧洲和亚太地区的40个国家，涉及汽车、化学制造、食品和饮料、医疗保健、制药和生物技术、电力和能源、运输等十几个行业。

主要调研结果

1. CISO 应对因影响 CPS 的攻击造成的严重财务影响

瞄准 CPS 的攻击不再罕见。俄罗斯 Sandworm APT 和伊朗革命卫队等攻击组织，分别对乌克兰的电力基础设施、美国和以色列的水处理设施发动了高度公开的网络攻击。同时，勒索软件依然对医院和患者护理造成明显且现实的威胁，数百起攻击影响了医疗保健服务机构(HDO)。最值得关注的是，Change Healthcare 在 2 月份检测到的攻击事件。Change Healthcare答应了攻击者的勒索要求，支付了数百万美元赎金，希望能重新获得受影响的患者数据和医疗设备的访问控制权限。

此类网络安全事件会给企业带来严重的财务影响，其中许多网络安全事件始于针对IT基础设施和企业网络的普遍攻击，最终影响工业生产或患者护理等。**45%**的受访者表示，在过去的12个月里，影响CPS的网络攻击造成了50万美元或更多的财务损失；**27%**的受访者表示，网络攻击造成的财务损失达到或超过100万美元。

受访者指出了许多具体的财务影响，包括收入损失、与赎金支付相关的恢复成本、或重新映像服务器和终端等其他技术费用，以及一些难以量化的成本，例如对企业品牌和声誉的影响。

在全球范围内，**39%**的受访者认为，最大的财务影响是收入损失；**27%**的受访者表示，在过去的12个月里，网络安全事件造成的财务影响达到或超过100万美元；**12%**的受访者表示，网络安全事件造成的损失达到或超过500万美元。

©Copyright Claroty Ltd. All rights reserved

在过去的12个月里，您所在的企业因网络攻击造成的财务影响（以美元计算）：

少于 100,000 美元	19%
100,000 美元 — 499,999 美元	22%
500,000 美元 — 999,999 美元	18%
1,000,000 美元 — 4,999,999 美元	15%
5,000,000 美元或以上	12%
无财务影响	14%

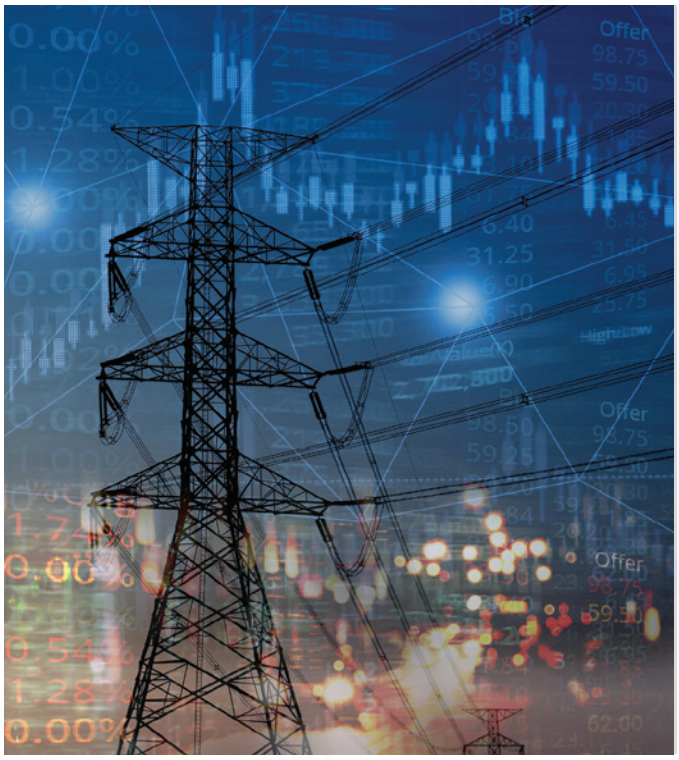
各行业称，
损失金额在 100 万美元或以上的百分比：

电力和能源	38%
采矿	32%
运输	30%
食品和饮料	29%
化学制造	26%
医疗保健、制药	26%

与此同时，造成财务影响的因素多种多样：

哪些因素造成了财务影响？（可多选）

收入损失	39%
恢复成本	35%
员工加班	33%
法律费用	31%
失去客户或合作伙伴关系	30%
事件响应和取证	29%
勒索赎金	28%
监管罚款	28%
品牌声誉恢复成本	27%
无财务影响	4%



©Copyright Claroty Ltd. All rights reserved

2. 企业遭受勒索软件攻击后的恢复成本

受访者认为，除了收入损失，财务影响的第二大因素是恢复成本。例如，影响制造业、电力和能源业或医疗保健机构运营的网络安全事件，往往需要较长的恢复时间。若是遭受破坏性勒索软件攻击、或由国家支持的网络攻击，企业通常面临着从已知的、良好的备份中恢复的问题，必须对服务器进行重新映像、应用缓解措施，并采取修补和固件更新等补救措施。

在某些情况下，这会导致长时间停机或系统不可用。对于医疗保健机构而言，这会影响公共安全或患者护理。**49%**的受访者表示，恢复需要一周或更长时间；**29%**的受访者表示，恢复需要一个多月。

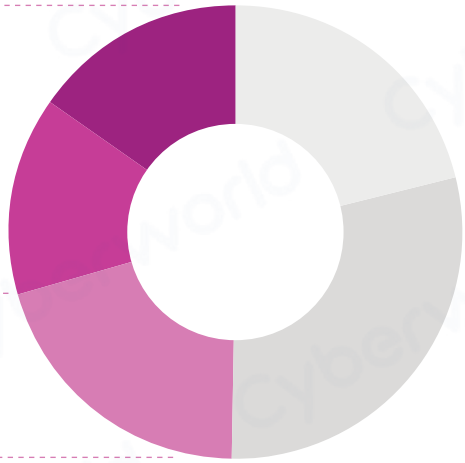
恢复花费了多长时间?

29%

的受访者表示，恢复需要一个多月的时间。

49%

的受访者表示，恢复需要一周或更长时间。



不到 1 天	21%
1-6 天	29%
7-30 天	20%
31-90 天	14%
超过 90 天	15%

勒索软件依然是关键基础设施领域的心头大患。财务损失和停机时间迅速增加，在最紧张的情况下，备份等恢复工作也面临考验。尽管执法部门和网络安全专家都提出了建议，但企业往往在艰难的商业决策下与攻击者协商，满足其赎金要求。

同时，勒索攻击也发生了变化。它们不仅仅是加密关键系统和信息的攻击，还是经常伴随数据泄露和知识产权盗窃而发生的二次攻击。攻击者利用被盗数据来威胁受害者，扬言要泄露患者数据或商业机密，试图进一步勒索受害者。

尤其是针对CPS的网络攻击，赎金要求和相关的恢复工作会造成巨大的财务压力。

©Copyright Claroty Ltd. All rights reserved

在全球范围内，**53%**的企业满足了超过50万美元的赎金要求，**16%**的企业支付了500万美元或更多的赎金，恢复加密系统和文件的访问权限，从而恢复运营。

在医疗保健行业，勒索软件和敲诈勒索攻击有增无减，**78%**的受访者表示，支付了50万美元以上的赎金。

您所在的企业支付了多少赎金？

	所有行业	医疗保健行业
少于 100,000 美元	14%	—
100,000 美元 — 499,999 美元	21%	11%
500,000 美元 — 999,999 美元	20%	39%
1,000,000 美元 — 4,999,999 美元	17%	39%
5,000,000 美元或以上	16%	—
没有支付赎金	13%	11%

在欧洲，59%的企业支付了至少50万美元的赎金，
其中23%的企业满足了100万美元至500万美元之间的赎金要求。

同时，网络保险正日益受到关注，企业试图以此抵消与网络攻击相关的部分成本。然而，经纪人和保险公司变得越来越严格，在提供保险前，会要求企业具备某些控制措施。如果企业的网络安全计划中存在缺口，例如缺乏标准化实践、缺乏事件响应计划以及其他不足，就会导致无法投保。尤其是中小型企业，它们通常因为这些缺口，而无法购买网络保险。

在全球范围内，受访者表示，网络安全事件发生后，通过网络保险获得了巨额赔付，帮助抵消了一些较高的恢复成本。

©Copyright Claroty Ltd. All rights reserved

在过去的 12 个月里，网络保单给您所在的企业支付了多少赔偿金？

少于 100,000 美元	**17%**
100,000 美元 — 499,999 美元	**20%**
500,000 美元 — 999,999 美元	**19%**
1,000,000 美元 — 4,999,999 美元	**19%**
5,000,000 美元或以上	**14%**
没有购买网络保险	**11%**

3. 不同程度的运营影响

CPS安全对于公共安全、国家安全和经济稳定非常重要。但如今，CPS经成为了勒索者、黑客和攻击者的主要目标，这些网络犯罪分子试图利用传统技术和过度连接的漏洞，以获取利润或地缘政治利益。

去年年底，美国和以色列的水处理设施遭到入侵。攻击者利用以色列制造的工业控制系统中的漏洞，让一群被认为与伊朗革命卫队有关的人员访问了这些系统。虽然仅是这些集成的Unitronics可编程逻辑控制器(PLC)和人机界面(HMI)控制器遭到破坏，但攻击的目标是破坏水质控制系统的完整性，制造混乱和恐惧。

针对医院的勒索软件攻击已经广为人知。患者突然被转移到其他医疗机构；重要的患者数据或连接的医疗设备不可用，导致预定的手术被迫推迟或取消。

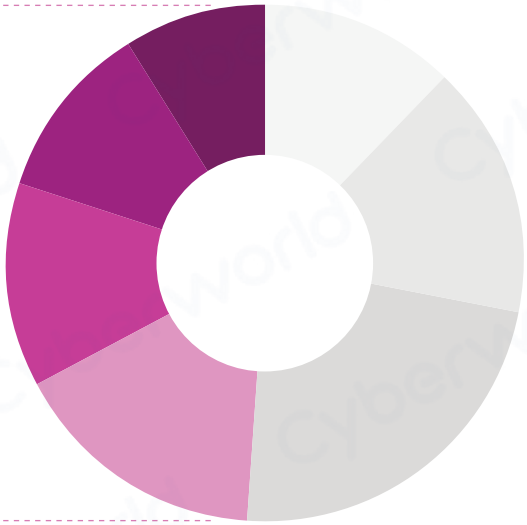
受访者坦诚地谈论了针对CPS的攻击对运营和网络安全的影响。CPS环境是无法容忍停机。**49%**的受访者表示，网络攻击导致的运营停机时间超过12小时。**33%**的受访者表示，至少停机一天。

©Copyright Claroty Ltd. All rights reserved

在过去的 12 个月里，您所在的企业是否遭受过因网络攻击导致的运营停机，影响了企业生产商品或提供服务？如果是的话，停机持续了多长时间？

49%

的受访者经历了12小时以上的运营停机。



否，运营未受影响	12%
是，不到 1 小时	16%
是，1-12 小时	23%
是，12-24 小时	16%
是，1-2 天	13%
是，2-7 天	11%
是，超过 7 天	9%

一旦工业、制造和其他流程被中断或被操控，会严重影响系统的可用性，还会影响操作人员和公众的人身安全。这还可能迫使生产停工或产品交付延迟，从而造成高昂的财务损失。

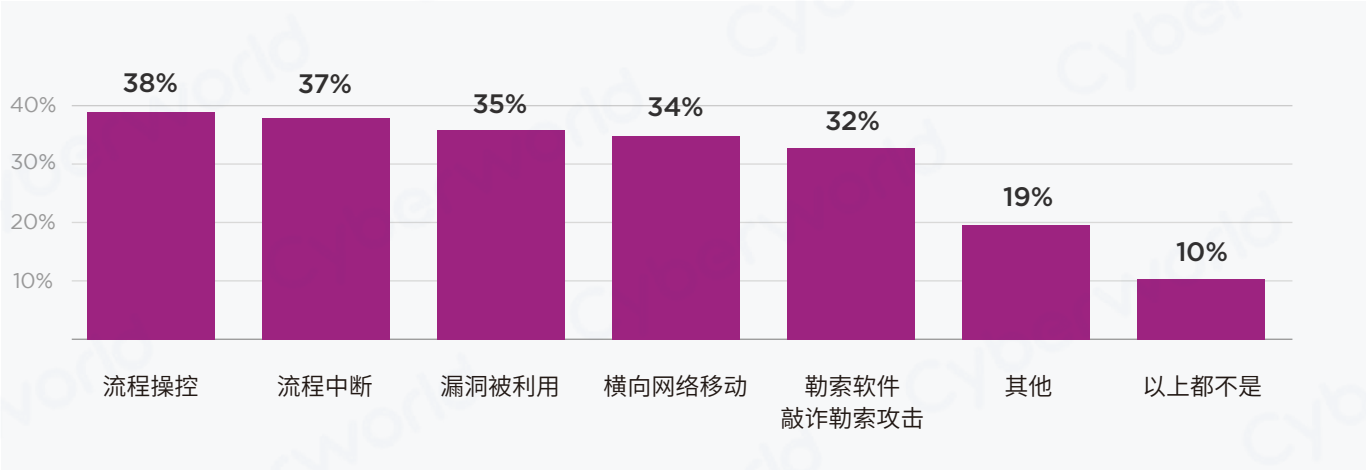
针对 CPS 的网络攻击对运营产生哪些影响？(可多选)

财务损失	38%	法律影响	23%
声誉受损	32%	人员变动	22%
产品发货停止	30%	公共安全	21%
生产停工	28%	患者护理中断	20%
失去客户或合作伙伴关系	28%	人身伤害	17%
知识产权损失	27%	其他	15%
监管影响	25%	以上都不是	5%

©Copyright Claroty Ltd. All rights reserved

令人不安的是，**38%**的受访者表示，网络攻击带来最严重的影响是流程操控；流程中断以及与之伴随的停机是第二大影响，占了**37%**，高于攻击者成功利用已知和未知漏洞、从CPS到企业网络的横向网络移动、勒索软件与敲诈勒索攻击。

网络攻击对网络安全有何影响？(可多选)



以下哪种网络攻击的后果对您所在的企业产生了最持久的影响？

数据泄露或数据被篡改	19%
数据隐私被侵犯	15%
无法访问系统和信息	13%
无法恢复系统和信息	13%
泄露PHI或PII	10%
敲诈勒索	9%
以上都不是	8%
违规	7%
其他	6%

©Copyright Claroty Ltd. All rights reserved

4. 第三方和远程访问暴露的问题

企业正面临满足远程访问CPS需求的压力。**45%**的受访者表示，至少有一半的CPS资产是在线连接的。无论是来自员工，还是来自第三方供应商和合作伙伴，在某些情况下，企业这样做的方式会给业务带来暴露的风险。

本项调研报告揭示了一些不太好的做法。在全球范围内，**32%**的受访者承认，通过暴露的开放端口和其他不完善的网络安全措施将CPS直接连接到互联网。**36%**的受访者表示，通过VPN解决方案进行连接，但大多数VPN不足以远程连接到工业控制系统或医疗设备。

VPN、跳板机和非企业级远程访问解决方案缺乏会话记录、审计和基于角色的访问控制，而这些对于正确保护OT环境是必不可少的。有些解决方案缺乏基本的安全功能，例如多因素身份验证(MFA)选项，或者已被各自的供应商停用，不再接收功能或安全更新。

Claroty Team82 于 2024 年 5 月和 9 月发布的研究结果，从两个方面展示了不安全连接所造成的潜在弱点，攻击者可能会利用这些弱点。例如，在OT方面，关键的、基于Windows的工程工作站和HMI经常会直接连接到互联网，而不是通过安全的远程访问解决方案。

这种连接方式会引入不必要的风险。因为这会让攻击者轻易地发现互联网上存在这些设备，并发动暴力攻击以访问它们。许多设备还包含了已知的、可利用的漏洞，从而成倍地增加了其暴露风险。

您所在的企业的 CPS 是如何连接到互联网？(可多选)

VPN	**36%**
自有的CPS专用的安全远程访问工具	**32%**
远程桌面协议(RDP)	**32%**
直接连接到互联网（开放端口）	**32%**
TeamViewer或远程管理工具	**32%**
第三方提供的CPS专用的安全远程访问工具	**28%**
跳板机	**27%**
以上都不是	**8%**

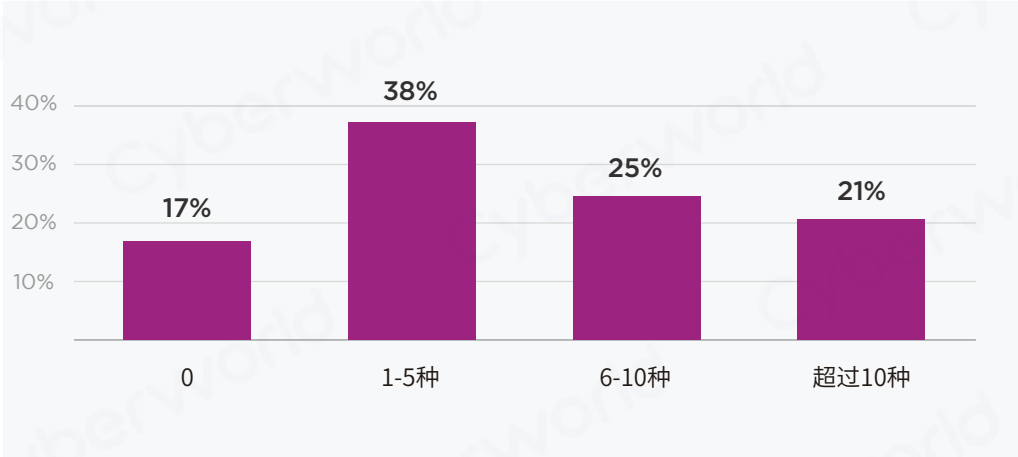
©Copyright Claroty Ltd. All rights reserved

企业为了应对远程访问的需求，采用了大量技术，其中许多技术并没有考虑到安全性。Claroty Team82 的数据集显示，**55%**的企业正在运行四种或四种以上远程访问工具；**33%**的企业运行六种或六种以上远程访问工具。同时，**79%**的企业在OT网络中运行的设备上安装了两种以上的非企业级工具。这些非企业级工具包括TeamViewer和AnyDesk。今年，这两款工具都遭遇了入侵。Claroty Team82 的数据集显示，**89%**的企业在其环境中部署了TeamViewer；**63%**的企业部署了AnyDesk。

这会扩大攻击者可利用的攻击面，也增加了管理和保护这些工具的巨大运营负担。

这些远程访问需求既源于支持融合环境的需要，也源于需要访问这些系统、进行维护和应用功能或安全更新的众多合作伙伴和上下游供应商。在全球范围内，本项调研结果与Claroty Team82的调研结果一致。

当前的 CPS 环境中使用了多少种远程访问工具?



45%

的CPS直接或间接连接到互联网。

许多远程连接都是第三方关系要求的。**63%**的受访者表示，他们对第三方与CPS环境的连接只有部分了解或完全不了解；**21%**的受访者表示，他们对访问方连接到CPS环境的控制有限。

通常，企业对供应商的网络安全实践知之甚少，或者在这些关系中，合同权力有限，无法提出某些要求。还有，如果第三方受到攻击，例如 Change Healthcare 攻击、SolarWinds 、NotPetya 和其他网络安全事件，就会对整个行业造成毁灭性后果。

Change Healthcare称，在 2024 年 2 月检测到了一起入侵和勒索软件攻击。Change Healthcare是医疗保健行业最大的理赔支付处理商，其系统离线数周，导致理赔未得到处理，一些医疗服务提供商因无法获得所提供服务的补偿而陷入财务困境。事实证明，整个医疗保健生态系统中这一枢纽的入侵会带来重大的财务影响。

©Copyright Claroty Ltd. All rights reserved

美国医学协会在4月份发布的一项调研描述了此次攻击所造成的混乱局面，指出**80%**的医疗机构因未支付理赔或无法提交理赔而损失了收入。受访者还讲述了理赔付款延迟或无法查验福利资格的问题。

本项调研结果显示，**82%**的受访者表示，在过去的12个月里，至少发生过一次网络攻击；**45%**的受访者表示，发生过五次或五次以上网络攻击，这些攻击源自第三方供应商对CPS环境的访问。在全球各行业，**38%**的受访者表示，因第三方访问环境而遭受过一至五次网络攻击；**27%**的受访者表示，遭受过五至十次网络攻击；**17%**的受访者表示，遭受过十次以上网络攻击。

然而，一些受访者在数据泄露后，能够改善与第三方的关系。

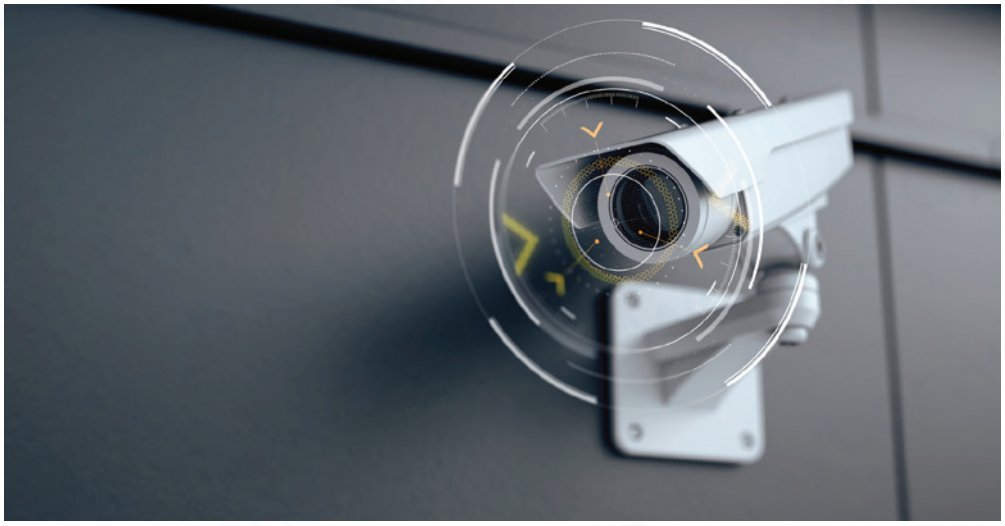
这些网络攻击是否对企业与相关供应商或合作伙伴的关系产生负面影响?

是 —— 与相关供应商或合作伙伴建立新的安全协议	**26%**
是 —— 与相关供应商或合作伙伴重新协商条款或定价	**25%**
是 —— 结束合作关系	**15%**
否 —— 合作关系不变	**15%**
不适用 —— 没有源于第三方访问的网络攻击	**19%**

涉及第三方的网络安全事件也会对上下游供应商产生影响。**40%**的受访者表示，一至五次攻击对第三方供应商环境产生了影响；**19%**的受访者表示，有十次以上的攻击产生了此类影响。

26%

的受访者表示，在攻击影响到供应链合作伙伴的环境后，他们与第三方建立了新的安全协议。



©Copyright Claroty Ltd. All rights reserved

5. 对风险降低措施的信心日益增强

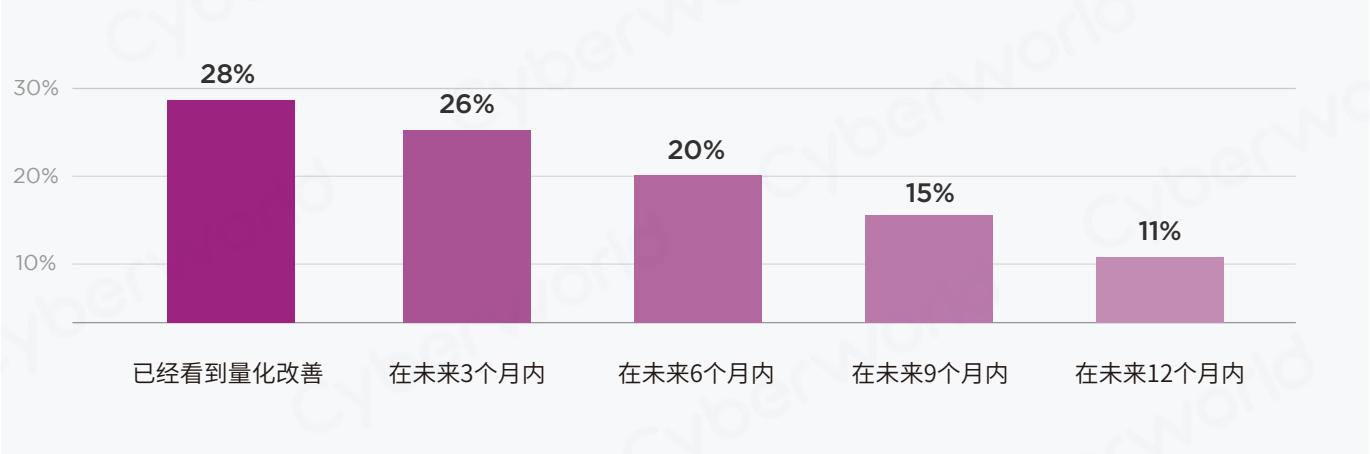
受访者承认网络安全事件是不可避免的。保护CPS免受网络攻击需要采用不同于IT安全管理的方法。企业正在制定策略来构建弹性系统，并设计能够抵御攻击的系统和网络，而不是试图修补每一个漏洞、解决每一个已知和未知的威胁。

大多数CPS环境都需要准确且持续地厘清资产，了解所连接的资产，检测威胁和对系统的异常访问，根据系统重要程度和已知漏洞来确定补救措施的优先级，并遵守行业法规与遵循公认的标准。

在被问及他们在过去的12个月里缺少哪些安全功能时，**34%**的受访者认为是风险评估，它能更有效地管理风险；其次是漏洞管理（**32%**）和资产、变更或生命周期管理（**31%**）。

然而，受访者对过去12个月采取的风险降低措施充满信心。这表明CPS环境的防御成熟度在不断提升，并了解其对关键基础设施的影响。

根据企业在过去 12 个月采取的风险降低措施，预计何时会看到 CPS 安全性的量化改善？



受访者表示，为了最大限度地减少CPS中断，勒索软件或敲诈勒索攻击是优先考虑的威胁。此外，受访者还高度关注国家支持的网络攻击以及营利性犯罪分子实施的攻击。

©Copyright Claroty Ltd. All rights reserved

为了最大限度地减少 CPS 中断，您会优先考虑以下哪种威胁？
（按重要程度 1 到 5 级排序，1 为最重要）

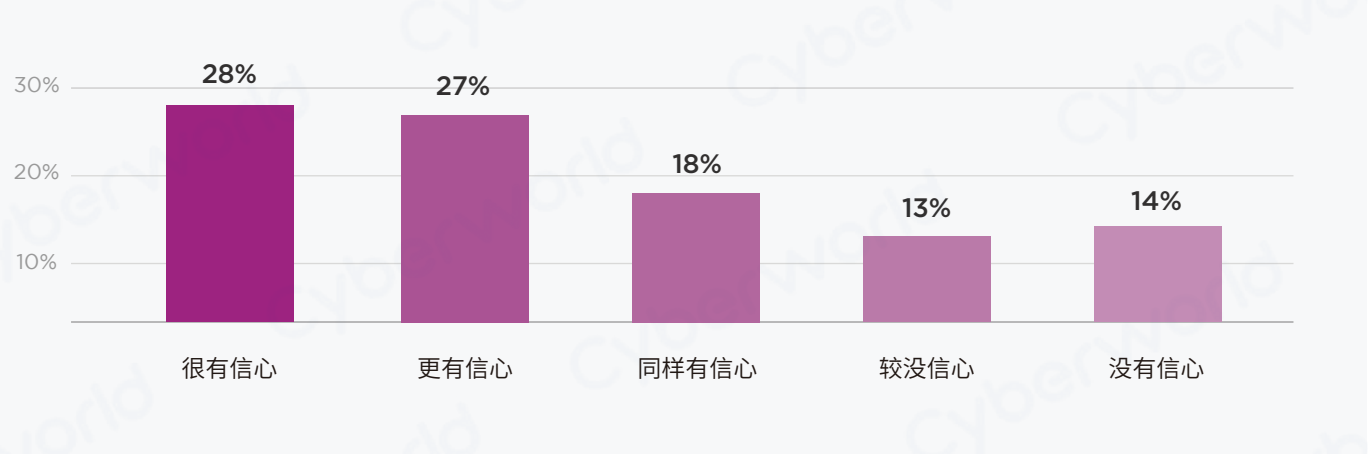
1	勒索软件或敲诈勒索攻击	3.79
2	国家支持的网络攻击或蓄意破坏	3.81
3	营利性犯罪分子发动的攻击	3.89
4	拒绝服务攻击	4.03
5	国家支持的间谍活动	4.09
6	内部威胁	4.16
7	人为失误和操作错误	4.23

对于国家支持的、高级的、瞄准CPS的攻击，68%的受访者表示“中度”到“极度”担忧。

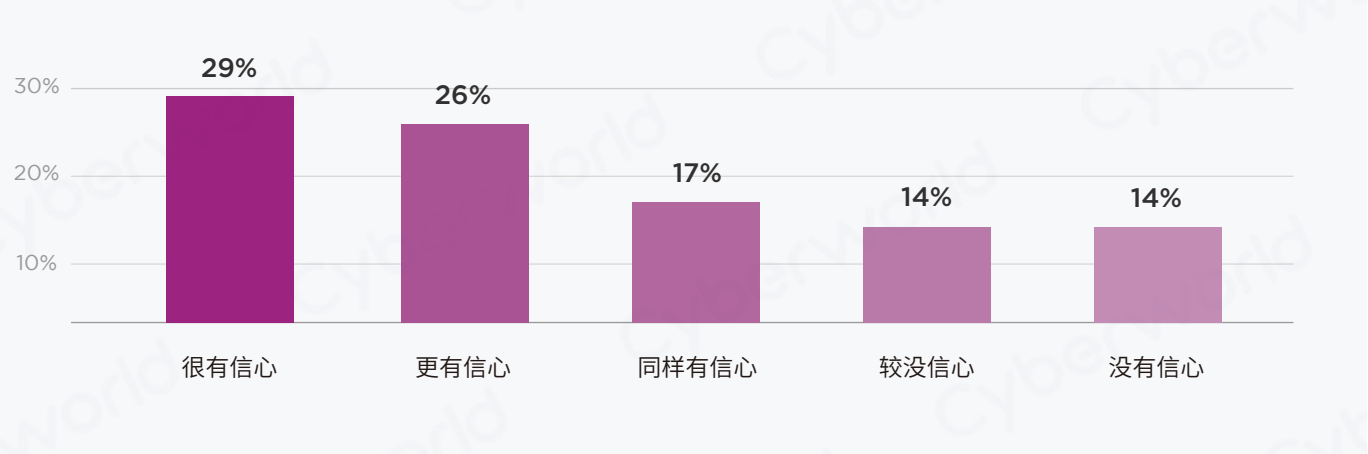
©Copyright Claroty Ltd. All rights reserved

56%的受访者表示，对采取的风险降低措施充满信心。

与 12 个月前相比，对于企业构成 CPS 所有资产的可视化，您现在有多大信心？



与 12 个月前相比，对于企业 CPS 抵御攻击的能力，您现在有多大信心？



©Copyright Claroty Ltd. All rights reserved

建议

在日常工作中，CISO面临着越来越多的新监管和个人法律压力。与网络攻击相关的任何业务中断都可能对网络安全计划的有效性产生严重影响。鉴于工业控制系统、智能设备和系统、以及联网医疗设备的连接性不断提升，若CPS受到攻击，可能会对物理世界产生影响，降低CPS的风险是所有网络安全负责人的首要任务。

将重点放在以下五个方面，将有助于引导网络安全负责人达到他们期望的最终状态：
具有抵御攻击能力并维持生产和服务的完整性与可用性的弹性系统。

1. 资产管理

成功的网络安全计划依赖于厘清资产和资产可视化。任何CPS安全计划所产生的价值都取决于其资产可视化的质量。企业必须识别网络内的所有资产，包括硬件、软件、应用程序和数据。这有助于了解需要保护的内容。

适当的可视化可以帮助了解CPS环境的复杂性、以及支持OT、IoT和联网医疗设备的专有技术。它还可以更好地确定风险管理的优先级，及时修补风险最高的软件和固件漏洞，降低整体风险。

2. 风险管理

风险管理是现代网络安全计划的关键。高度互联的企业必须了解其弱点所在，并根据多种因素，从可利用性、系统的重要程度、宽松的访问控制等开始排定优先级。风险评估和业务影响评估是这一策略的核心，网络安全负责人应了解漏洞被利用的潜在影响和可能性，并根据其对企业风险进行优先级排序。

网络安全团队应根据是否用不安全的方式连接到互联网、是否包含已被广泛利用的漏洞等因素重新分类高风险设备。这样可以识别出被利用风险最高的设备和系统，并大幅减少需要优先处理和缓解的设备的数量及百分比。

©Copyright Claroty Ltd. All rights reserved

3. 安全访问

为第三方提供安全的远程访问是当今CPS网络安全计划不可或缺的，旨在确保用户与机器之间的通信安全。企业比以往任何时候都向互联网暴露了更多的技术和基础设施。分析师正在获得更好的业务指标并提高效率，以降低成本、改善流程效率、患者护理和其他关键服务。

然而，网络的入口点增多，高级攻击和常规攻击的风险也随之增加。适当的可视化有助于制定安全访问策略，并让网络安全负责人了解控制系统和其他关键设备是否安全地连接到互联网、是否受专为远程访问设计的解决方案保护、是否由强大的访问控制和特权访问管理功能守护。正如前文所示，受访者表示，由于第三方访问控制不佳以及网络上部署了过多的非企业级远程访问工具，导致网络安全事件频繁发生。

安全访问必须被严格管理，以确保尽量减少业务中断、高昂的收入损失和监管不合规。许多企业寻求建立所有供应商使用的单一CPS安全访问中心，从而创建一个标准来维护控制和身份治理。

4. 网络保护

CPS已被频繁用于提高运营效率。确保机器对机器、云工作负载对机器的通信安全，成为了缓解各类网络风险的重要功能。正如前文所示，横向网络移动是攻击者的主要手段，他们在初始接入点站稳脚跟后，试图访问其他系统，提升权限，以窃取数据、部署恶意程序和勒索软件等。

在CPS环境中，企业历来将物理隔离作为一种隔离方法。但是，这些物理隔离一般是形同虚设。因为操作人员在紧急情况下或为了更有效地完成工作，会将资产连接到外部。当企业想获得数字化转型的效益时，将资产连接到IT或公共云是必需的。此外，IT与OT融合需要更强大的连接性。无论是在融合环境，还是在非融合环境，网络安全负责人都应该利用网络分段来确保通信安全。虽然网络分段是一项艰巨的任务，但它可以有效地限制攻击者横向网络移动。安全的网络分段还可以帮助隔离敏感数据和系统。这种隔离也可以带来合规性方面的好处，使企业或客户信息远离攻击。

CISO和其他网络安全负责人应该先根据安全性要求、合规性要求和机密性来定义网络段，然后相应地调整防火墙和访问控制列表，以帮助实施安全策略。最后，还可以根据特定网络段的机密性，对流量监察和威胁检测进行优先级排序。

5. 威胁检测

厘清资产和CPS资产可视化提供了宝贵的基准，不仅可以正确调整防火墙和访问控制，还可以识别关键系统中可接受的网络流量和活动的任何偏差。将威胁检测功能与上述建议事项搭配运作，一旦检测到潜在的有害活动，企业就可以根据警报采取行动，隔离受影响的系统，或采取措施实时降低风险。

手段高明的攻击者和网络犯罪团伙逐渐将攻击目标对准CPS，以造成中断，或在最坏的情况下进行破坏性活动。至关重要的是，工业企业和医疗保健机构不仅要检测已知威胁，还要了解网络和系统行为中的异常，这些异常可能表明存在以前未被发现的威胁，例如，对已知漏洞的利用。

安全运营中心(SOC)可集成大多数威胁检测技术，并分析警报，以通知事件响应活动。具有CPS的可视化非常重要，这样才能自信且集中地管理对环境的威胁，以满足正常运行时间的业务要求，并维护核心数据和系统的完整性。

©Copyright Claroty Ltd. All rights reserved

关于 Claroty

Claroty凭借无与伦比的、以行业为中心的平台重新定义了网络化物理系统(CPS)防护，该平台旨在保护关键任务型基础设施。Claroty平台提供市场上最深入的资产可视化和最广泛的CPS安全解决方案，包括风险管理、网络保护、安全访问和威胁检测，可以搭配 Claroty xDome 在云端使用，也可以搭配 Claroty CTD 在本地部署使用。Claroty平台以屡获殊荣的威胁研究和技术联盟为后盾，让企业能够有效地降低CPS风险，以最快的时间实现价值并降低总体拥有成本。在全球范围内，已有数百家企业在数千个站点部署了Claroty。

Cyberworld
广州科明大同科技有限公司
中国区
总代理
官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792

©Copyright Claroty Ltd. All rights reserved