研究洞察

新冠病毒疫情加剧网络战争：如何保护企业

疫情肆虐之时，网络攻击不断升级 — 加强安全措施之行动指南

IBM 商业价值研究院

IBM

IBM 如何提供帮助

如果遇到网络安全问题或事件，请联系 X-Force IRIS 以寻求帮助：

美国服务热线：1-888-241-9812

全球服务热线：(+001) 312-212-8034

请在此了解更多信息：https://www.ibm.com/security/covid-19

扫码关注 IBM 商业价值研究院

官网　微博　微信　微信小程序

作者：Wendi Whitmore 和 Gerald Parham

要点

新冠病毒疫情与网络犯罪

世界各国全力应对新冠病毒疫情之际，网络犯罪分子发现自己有了可乘之机。2 月份以来，IBM X-Force 监测到的以新冠病毒为主题的垃圾邮件增幅高达 4,300%。*行动建议：运行模拟，针对最大的潜在威胁进行建模，立即采取措施堵住漏洞。*

拨开迷雾，积极改进

倘若平日里准备不足，那么疫情期间势必会措手不及。事实上，根据 2019 年度报告显示，76% 的企业并未在整个组织范围实施统一的事件响应计划。[1] *行动建议：制定或更新网络安全事件响应计划 (CSIRP)。*

在颠覆性危机期间实施有效管理

危机期间，业务连续性计划成为一项重要的战略资产。即使企业未做好准备，也可以采取措施减轻影响，同时利用相关经验，制定未来的危机应对计划。*行动建议：快速执行“侦查、判断、决策、行动”环。*

从极端事件中汲取经验

最近几周，恶意分子借新冠病毒疫情之机乘虚而入，网络安全威胁持续升级。疫情当前，企业在员工福利、资金链以及运营和供应链连续性等方面已经应接不暇，焦头烂额，因此对于网络安全的关注度有所下降，导致风险不断升级。

如果企业只是在危机期间临时做出决策，只会加剧数据泄露风险，甚至危及业务运营。由此引发的潜在影响也更加危险。例如，同样是应对分布式拒绝服务 (DDoS) 攻击，容量已经捉襟见肘的运营环境所遭受的破坏要比备用容量充分的环境要大得多。

在本报告中，我们为企业的负责人提出了一些关键措施建议，帮助他们应对此类环境中可能发生的各种影响力巨大的事件，以及其他不可预见的情况。每个网络安全危机的生命周期均由三部分组成：

- 规划和检测
- 即时响应和补救
- 恢复。

首先，负责人要确定自身所处的生命周期阶段，并计划相应的行动优先顺序。我们针对每个阶段提出行动建议，希望大家以此作为指导。尤其是当前疫情肆虐全球，亟需进一步加大对响应和补救工作的关注力度。从安全运营中心 (SOC) 和网络靶场（测试安全能力的虚拟环境）的事件响应演练中汲取经验教训后，我们发现安全永续能力较强的企业往往在以下三个方面表现出众：组织和部署资源；定期沟通；协调响应。

50 多种

不同的恶意软件通过各种以新冠病毒疫情为主题的宣传活动分发到世界各地 [2]

1/4

的企业未制定事件响应计划 [3]

#1

事件响应 (IR) 团队与 IR 计划测试的组合所节省的成本高于其他任何安全补救流程 [4]

新冠病毒疫情对网络安全格局造成的影响

2020 年，全球几乎每一家企业的业务都经历了翻天覆地的变化。随着新冠病毒确诊人数的不断增加，一些地区的传播速度加快，另一些地区的传播速度则在放缓，企业的运营格局每天都在变化，甚至每小时都不同。波及范围史无前例。

投机性威胁分子

自 2 月全球疫情爆发以来，IBM X-Force 监测到的以新冠病毒为主题的垃圾邮件增幅高达 4,300%。网络犯罪分子趁着新冠病毒的爆发大发横财，在暗网中销售以病毒为主题的恶意软件资产，甚至还有与病毒相关的折扣代码。[5] 他们还在快速创建域名：与新冠病毒相关的恶意域名的比例较同期注册的其他非恶意新冠病毒域名高出约 50%。[6]

不计其数的网络钓鱼欺诈邮件接踵而至。例如，IBM X-Force Exchange 正在跟踪一种垃圾邮件，这种邮件利用小企业主渴望向美国小企业管理局申请贷款的心理实施诈骗。这种邮件并未提供任何帮助，而是通过附件安装了远程访问木马 (RAT)。另一种大规模垃圾邮件威胁称，如果收件人及其家人不支付比特币赎金，那么将会感染新冠病毒。[7]

另一些欺诈邮件暗示与某些合法卫生机构有牵连。一种电子邮件网络钓鱼攻击声称由世界卫生组织 (WHO) 总干事发起。这种电子邮件随附的文档中安装了 Agent Tesla 恶意软件变体，充当键盘记录器和信息窃取器。[8] 还有一种类似的攻击以美国疾病控制和预防中心 (CDC) 作为诱饵。[9] IBM X-Force 新冠病毒疫情安全公告板罗列了一系列威胁分子和新冠病毒疫情漏洞，确定了数百个攻击示例。[10]

报告指出，有些国家可能利用疫情入侵美国公共卫生机构，特别是美国卫生与公众服务部。[11] 美国参议院情报委员会委员 Ben Sasse 评论道，“这是 21 世纪冲突的真实写照：网络攻击是乘对手陷入困境时发动攻击的强大武器。”[12]

洞察：网络犯罪严重打击公众信任

恶意分子之所以能够顺利实施网络犯罪，是因为他们利用了疫情期间人们被放大的恐惧、焦虑、迷茫和愤怒情绪。更令人担忧的是，疫情期间，无论个人还是企业，生计都受到不可预知的颠覆性影响。世界经济论坛的公报指出，人类社会对数字基础架构的依赖度越来越大，一旦这种架构崩塌，代价势必非常巨大。[13] 此次公共卫生疫情的社会和经济代价无可估量，会对个人造成独特而又深远的影响。高价值资产 (HVA) 尤其容易受到攻击。根据美国网络安全与基础架构安全局 (CISA) 的定义：“信息或系统至关重要，一旦丢失或损坏，必然会对组织履行使命或开展业务的能力造成严重影响。”倘若网络犯罪分子的目标在于摧毁组织的公信力，那么势必优先选择破坏 HVA。[14]

远程工作面临的新型风险

匆忙转变为远程工作，也给网络犯罪分子带来可乘之机。根据《纽约时报》报道，截至 2020 年 4 月的第一周，美国有 3.16 亿人被要求待在家中。[15] 全球数字更是要高出一个数量级。例如，印度就地避难指南就覆盖 13 亿人。[16]

许多人尽管待在家中，但仍在家工作。然而，很多远程工作者缺乏保障数字安全的安全设备或协议。大量初次尝试远程工作的员工通过个人设备访问企业网络，黑客则通过刺探 Wi-Fi 配置和 VPN 连接来寻找安全漏洞。人们出于工作和个人原因而集中使用基于云的生产平台 — 恶意分子同样使出浑身解数，利用这个千载难逢的机会，比如入侵及干扰实时会议。[17]

不只是员工没能做好准备 — 企业也是一样。Threatpost 近期开展的一项在线调研表明，70% 的受访者表示所在组织过去基本未尝试过远程工作。40% 的受访者报告称，开展远程工作后，网络攻击有所增加。[18] 美国参议员 Mark Warner 在电子邮件中指出：“在联邦政府着手筹备史无前例的远程工作的过程中，也为恶意分子发动攻击创造了更多的机会，很可能会造成关键的政府服务中断。”[19]

疫情期间发生持续中断的可能性比较高，组织的危机响应负责人务必时刻保持警惕，保证组织的敏捷性。

安全永续能力较强的企业往往能够高效地调配资源、进行沟通和协调响应。

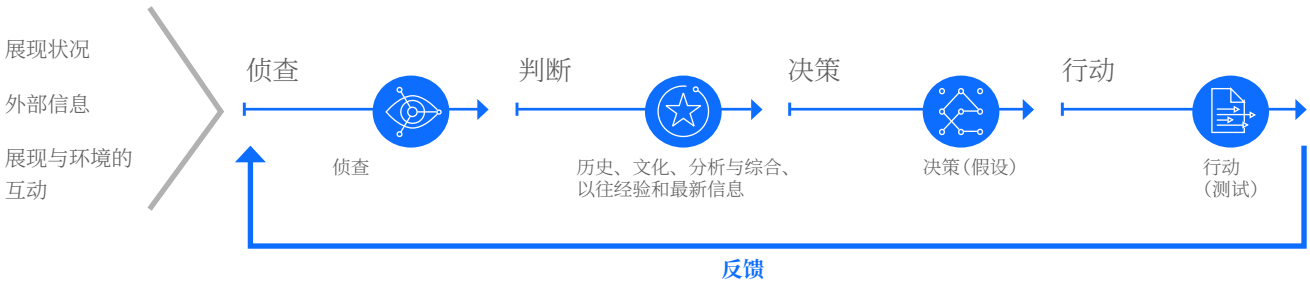
快速决策的重要意义

危机期间，安全团队的高管和成员必须过滤可用信息，迅速做出最优决策。组织可借鉴由军事战略家首创的原则，综合运用“侦查、判断、决策、行动”（也称作“OODA 环”）等战术行动方法，从中受益。[20]

OODA 环有利于迭代（见图 1）。如果可以提前行动而不是被动补救，就能够获得一定优势。加快响应速度，在更广泛的团队中协调工作。不一定要做出最终决策。哪怕出现一些小差错，也总比不做事要好。

图 1

侦查、判断、决策、行动 (OODA) 环



来源：“OODA 环。”Wikipedia；访问时间：2020 年 4 月 1 日。https://en.wikipedia.org/wiki/OODA_loop

制定事件响应计划

许多组织准备不足，难以应对重大网络安全事件，更不用说遭遇新冠病毒疫情这样的全球危机了。Ponemon Institute 近期的一项调研表明，76% 的组织未制定统一的事件响应计划。1/4 的组织表示，未制定任何网络安全事件响应计划 (CSIRP)。[21]

行之有效的 CSIRP 需说明各团队的治理和沟通实践（请参阅“洞察：CSIRP 剖析”）。同时，还要定义响应模型，详细规划整个组织的响应负责人及其职责，如战略、技术、运营以及社区和政府关系。如果组织还未制定 CSIRP，则必须加快步伐，迎头赶上。即使在新冠病毒疫情爆发之前，随着全球有关数据泄露通知的法律法规日趋严格，业务连续性规划成为一项长期性的战略能力，用于确保组织为各种突发事件做好充分准备。

然而，即使企业已制定了 CSIRP，仍需要立即采取措施加以巩固，防范新冠病毒疫情带来的种种特定风险。危机管理计划因以下因素而异：威胁性质和范围；组织类型和规模；与信息披露、数据隐私和数据存放地点相关的法规要求的差异。随着企业吸取越来越多的经验教训，他们可以调整 CSIRP，并快速应用学到的知识。

洞察：CSIRP 剖析

网络安全事件响应计划 (CSIRP) 通常包含以下信息：

- 如何确定危机事件的性质并进行分类；
- 内部和外部团队成员的角色和职责，包括通过分层视图说明决策权限和上报路线；
- 用于规范内部和外部利益相关方沟通的危机沟通计划；
- 组织 HVA 和任务关键型能力清单，以及为这些能力提供帮助的关键支持服务；
- 与上述各项有关的法规和披露要求；
- 补充性运营支持能力清单，例如与社区 / 计算机应急响应 / 准备小组 (CERT)、联邦执法机构或其他各方共享的威胁补救服务和威胁情报。

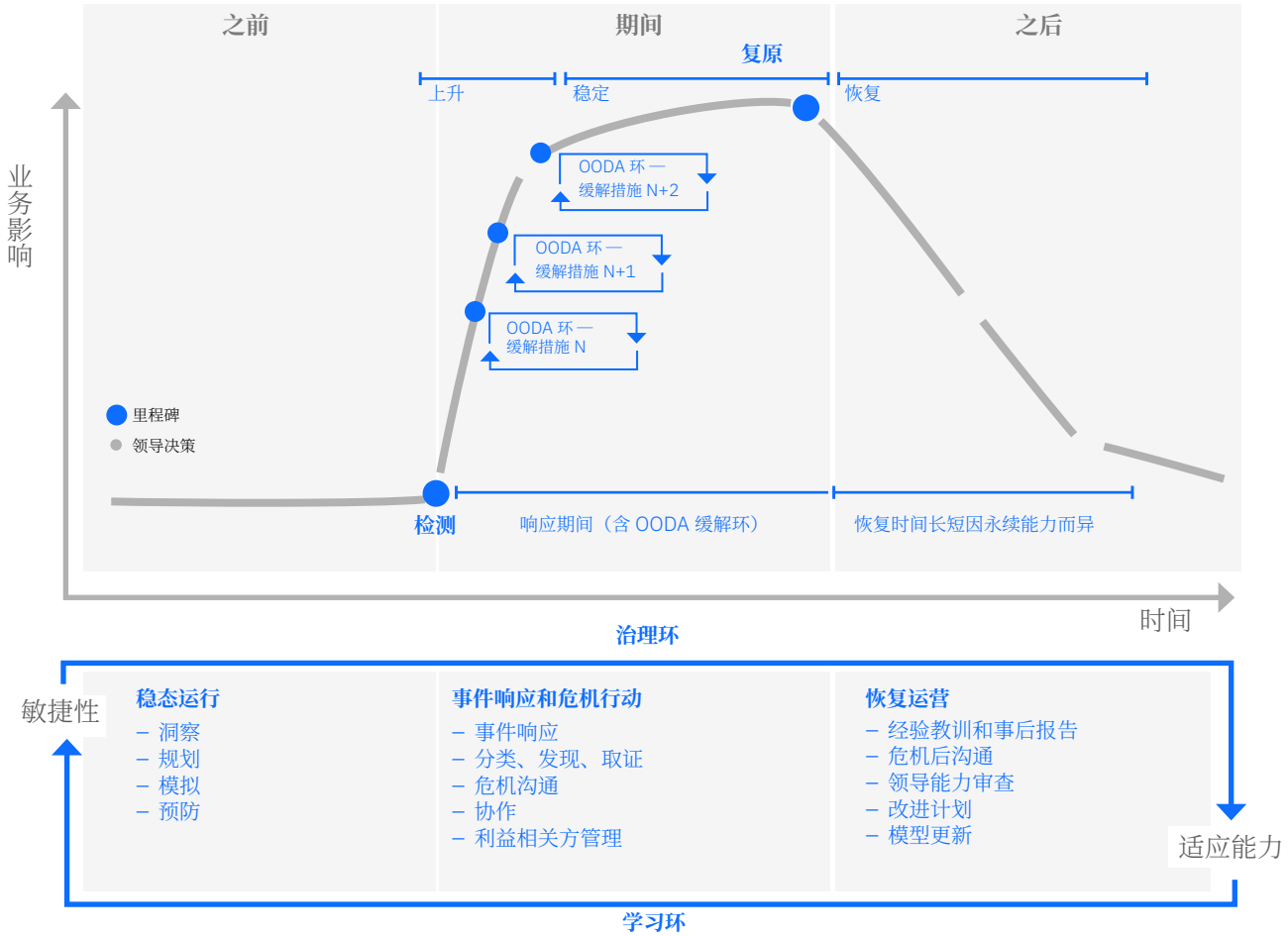
哪怕出现一些小差错，也总比不做事要好。

危机生命周期，第 1 阶段：稳态 / 规划

新冠病毒疫情危机日益蔓延，如果组织尚未遭遇网络威胁，那么仍有时间进行准备 — 务必明智地把握这一时间窗口期。（见图 2）

最重要的是，如果组织尚未制定 CSIRP，务必立即采取行动。如果领导者已完成规划阶段，应立即抓住机会，根据新冠病毒疫情期间的安全形势评估 CSIRP，确定是否存在任何不足。即使是在像新冠病毒疫情这样的“黑天鹅”事件已成长期现实的情况下，也存在应对之策。[22] 关键在于设法改进方案，争取时间做出更明智的决策。

图 2
危机生命周期



来源：IBM 商业价值研究院分析。

此外，还可通过模拟，优化组织在灾难期间的执行力。尽管无法替代现实生活中的亲身经历，但演练和重复模拟有助于发现风险管理和风险缓解模型的不足。团队实践经验越丰富，认识越深入，越有利于在实际发生安全事件时做出预测和响应。团队可以实时查看各种可变因素和依赖关系，针对响应措施建模，并不断改进。

定义风险管理

网络安全永续能力是指组织预防和应对网络攻击、重新恢复运营以及维持内部和外部运营完整性的能力。威胁、漏洞和风险是三大核心问题：

- *威胁：*任何有意或无意利用漏洞以及强占、损害或破坏信息或运营资产的行为。威胁属于离散的战术或事件。
- *漏洞：*安全计划的弱点或不足，很可能被威胁所利用，从而能够未经授权地访问资产。
- *风险：*因漏洞被利用所引发的威胁造成损失、损害或破坏的可能性。[23]

组织面临的挑战（尤其是新冠病毒疫情时期的挑战）具有动态、突发及不可预测等特点，而且往往相互依存。在风险管理过程中，需发现风险并进行建模，预测运营影响等级和发生概率。这就是为什么危机响应是网络安全、技术和运营团队跨职能（而且将来还将跨组织）的协作活动。

风险一旦变为现实，各团队就必须调整业务重心，从规划和建模转到事件响应、灾难恢复和业务连续等工作上来。最重要的是，务必确保规划 / 模拟流程与行动 / 响应流程保持一致。快速协同决策能力往往决定成败。

第 1 阶段：行动计划

协调运营团队，积极开展实践，完善行动方案

1. 制定计划，建立团队。制定 CSIRP 并定期更新，反映最新运营环境状况。检验并测试危机警报人员名单，完善团队成员资格。考虑每半年或每季度更新计划并开展危机响应演练，人员更迭频繁的大型组织尤其要注意这一点。

2. 将决策转变为敏捷实践。先前制定并经过检验的流程和程序可以帮助负责响应计划的主要利益相关方快速做出决策。主要领导有权做出重要决策，而且不必经过漫长的审批流程。

3. 消除依赖关系，全方位扩展可视性。供应链的可用性和完整性是一个时常被忽视的风险因素。实施透明机制，消除摩擦，加速决策，避免受到供应商的影响。反思采购依赖关系（按地理位置或供应商划分），探寻维持业务运营的替代来源。重新审视提供商 / 供应商合同的不可抗力（包括不可避免的重大事件）条款。检查供应链网络，确定是否存在第四方和“第 n 方”风险。

4. 切实推行计划。桌面演练和违规模拟是验证网络危机管理计划各关键功能流程和程序的一种有效途径。定期开展全方位的模拟演练，对团队、领导层和沟通机制进行压力测试。最终目标是培训团队“建立肌肉记忆”，能够像急救人员或军队一样快速做出响应。危机规划必须适应各种运营中断和社会影响，这就需要采取不同方法缓解和应对危机。

5. 从错误中汲取经验教训。与其真正面临危机时措手不及，不如提前进行危机模拟，哪怕模拟失败也会带来无尽的价值，而且代价也要低得多。了解系统性依赖关系、过时的假设或决策偏差在应对危机方面带来的不利影响。每次演练均引入意外事件，学习如何达到均衡效果：既遵循标准实践和危机治理机制，同时充分发挥团队在合作解决问题方面的优势和智慧。

危机生命周期，第 2 阶段：事件响应

尽管我们总觉得计划周密，准备充分，但显而易见，危机总是让我们措手不及。当危机（如新冠病毒疫情）势不可挡地席卷各行各业的组织时，很可能引发系统性崩盘。一旦形成系统性风险，企业的日常运营能力很可能与关键基础设施发挥同等重要的作用，因此需要大幅调整到稳态运营模式。

当真正爆发危机时，经过模拟演练的团队在更新响应计划及优化实施措施方面通常表现更佳。因为团队知道该做什么，领导也有能力密切关注形势发展。同时，还可以根据需要做出决策和调整，从而实现以下目标：保障员工、客户及其他利益相关方的安全；保护数据完整性；应对事件，帮助缓解特定危机。

倘若危机肆虐各行各业并引发严重的社会动荡，企业必须采用全新方法，充分利用运营资源，提供援助，帮助社会恢复信心。经过精心规划，响应计划可以综合考量各个可变因素，帮助领导选取有利于增进善意、诚信和信任的响应措施。

危机运营

在应对危机的过程中，务必兼顾治理原则和创意智慧，使二者达到适当的平衡。为关键沟通制定治理原则，有利于在解决问题的过程中发挥更多创意，协同开展更棘手的危机缓解工作。尽管问题看似专业而神秘，但解决方案总不免牵涉人类情感和团队合作。

一旦发生安全违规或网络攻击，高管必须迅速向客户及其他利益相关方灌输信心，表明正在尽全力解决问题。许多最高层领导无法顺势做出这种快速直观的响应。尽管他们可能了解如何从技术层面控制安全违规事件，但往往并未做好处理人际关系的准备。

危机当前，行动方案和模拟演练可以帮助全体人员（包括安全团队、沟通人员、公共关系专业人员一直到首席执行官）了解自身角色，凭借适当的软硬技能组合采取妥善措施，使团队抢先一步做好准备。

第 2 阶段：行动计划

执行行动方案、持续调整并开展协作

1. 接受无法尽善尽美的事实 — 因时制宜。认识到分类的必要性，初步成果可能不是完美的。快速执行 OODA 环，未雨绸缪。将复杂问题分解为多个组成部分。

2. 尽量减轻认知负荷。采用标准化术语和通信协议，使团队成员保持同步，加快发现和评估过程。过滤信息，尽量简明直接地表现可变因素。利用可视化效果呈现重要的关系和依赖性。

3. 以身作则。领导者需综合发挥软硬技能。展现出成熟的思想、同理心和技术敏锐度。紧跟形势变化，寻找适当的行动与分析组合。鼓励团队成员警惕事实与臆断之间的区别。

4. 优先开展团队合作 — 不提倡个人英雄主义或自我牺牲。盘点团队优势，发挥团队的多元化优势。根据求知欲和能力分配职责。让合作伙伴像核心团队成员一样享有权利并肩负责任。发挥全局观念，启发思考，不要事无巨细都亲历亲为。

5. 本着诚实透明的态度进行沟通，与高层领导和利益相关方沟通时尤其要注意这一点。严格定义威胁对企业造成的具体影响。哪些衡量指标表明取得进展？投入更多的专业资源、预算或时间会取得更好的效果吗？此次危机与其他危机有哪些相似（不同）之处？哪些可变因素会导致形势恶化（或好转）？了解何时应逐级上报决策，准备一套方案并说明预期效果。

危机生命周期，第 3 阶段：恢复和改进

一些安全专家认为，新冠病毒疫情可能对未来的网络攻击产生指导性作用，继而引发类似规模的社会动荡。[24] Brian Finch 在《国会山报》专栏中写道：“华盛顿的网络思想家应当好好研究哪些措施能够成功缓解新冠病毒疫情对经济的影响。这样，一旦发生不可避免的网络病毒传播，就可以借鉴这些措施，避免不必要的慌乱和应急解决方案。”[25]

新冠病毒疫情无疑是当前全球的关注点。与所有大动荡一样，可以从这些灾难中吸取经验教训，改善未来的应对之策。有一点似乎确定无疑：沟通、协调和协作能力与命令和控制能力同等重要，有助于最终战胜疫情。

企业一方面要加强规避和防范措施，另一方面要开展事件响应演练和模拟，这样，安全领导不仅可以增强企业抵御危机的信心，还能通过诚信运营提升企业公信力。网络安全公司 BlackCloak 的首席执行官 Chris Pierson 指出，“本次全球疫情期间，网络犯罪分子并没有在睡大觉，防御者或供应商同样也没有懈怠，因此我认为前景十分乐观。”[26]

第 3 阶段：行动计划

投资培养新型技能，增强企业的永续和适应能力

1. 实施安全遥测和分析。要提前检测并做出响应，首先需要具备自动化数据收集能力。借助现代遥测和日志文件捕获解决方案，即使危机结束后也能对攻击模式进行建模，确定攻击特征以及复盘违规事件。

2. 培养安全措施自动化能力。实现安全措施自动化后，专家团队就可以解放出来，将精力集中在需要深入分析的威胁上面。Ponemon 的研究表明，自动化投资物有所值：如果组织未部署安全措施自动化能力，一旦发生安全违规，面临的损失将比全面部署该能力的企业高出 95%（未部署自动化技术的企业平均损失为 516 万美元；全面部署自动化技术的企业平均损失为 265 万美元）。[27]

3. 利用威胁情报，贡献威胁情报。基于云的安全服务对于运营足迹的监控超过任何一个组织个体。企业贡献威胁情报数据有助于增强所有组织的网络安全永续能力，而企业利用威胁情报中的洞察可以加快威胁检测和响应速度。[28]

4. 优先开展协作和持续学习。网络安全永续能力较强的组织采用“发现、学习、适应和迭代”的持续循环，开展运营工作。危机时刻，高效的威胁补救措施取决于人们能否携手应对复杂（而且往往十分棘手）的问题。[29]

5. 提高安全意识。网络安全永续能力较强的组织将安全视为自己的优先战略能力。但许多组织并未将安全的优先级定得如此之高：2019 年 IBM 与 Ponemon 联合开展的网络安全永续能力调研显示，仅有 25% 的受访者认为所在企业的网络安全永续能力较强，仅有 31% 的受访者认为发生网络攻击时组织的恢复能力较强。[30]

关于作者

Wendi Whitmore

IBM Security 的 X-Force 威胁情报副总裁

wwhitmor@us.ibm.com

linkedin.com/in/wendiwhitmore2

@wendiwhitmore

Gerald Parham

IBM 商业价值研究院安全和 CIO 领域的研究负责人

gparham@us.ibm.com

linkedin.com/in/gerryparham/

Wendi Whitmore 是 IBM X-Force 威胁情报副总裁，也是网络安全领域公认的权威专家。她在事件响应、战略性的主动信息安全服务、情报和数据泄露调查等领域拥有超过 15 年的丰富经验，客户遍及各个行业和世界各地。

Gerald Parham 是 IBM 商业价值研究院安全和 CIO 领域的全球研究负责人。Gerald 的研究重点是网络生命周期和网络价值链，尤其侧重研究战略、风险、安全运营、身份管理、隐私和信任之间的关系。他在高管领导、创新和知识产权开发领域拥有 20 多年的丰富经验。

选对合作伙伴，驾驭多变的世界

在 IBM，我们积极与客户协作，运用业务洞察和先进的研究方法与技术，帮助他们在瞬息万变的商业环境中保持独特的竞争优势。

IBM 商业价值研究院

IBM 商业价值研究院 (IBV) 隶属于 IBM Services，致力于为全球高级商业主管就公共和私营领域的关键问题提供基于事实的战略洞察。

了解更多信息

欲获取 IBM 研究报告的完整目录，或者订阅我们的每月新闻稿，请访问：ibm.com/iibv

访问 IBM 商业价值研究院中国网站，免费下载研究报告：
https://www.ibm.com/ibv/cn

相关报告

新冠疫情行动指南
https://www.ibm.com/cn-zh/services/insights/report-covid-19-action-guide

应对极端挑战之 CIO 指南
https://www.ibm.com/downloads/cas/WRNRKVGJ

CISO 如何确保战略合作关系
ibm.com/thought-leadership/institute-business-value/report/ciso-strategic-partnership

备注和参考资料

1 “The 2019 Cyber Resilient Organization.” Ponemon Institute and IBM.2019. https://www.ibm.com/downloads/cas/GAVGOVNV

2 XF-IRIS internal data analysis.Additional COVID-19 data insights are available at https://exchange.xforce.ibmcloud.com/collection/Threat-Actors-Capitalizing-on-COVID-19-f812020e3eddbd09a0294969721643fe

3 “The 2019 Cyber Resilient Organization.” Ponemon Institute and IBM.2019. https://www.ibm.com/downloads/cas/GAVGOVNV

4 “2019 Cost of Data Breach Study: Global Analysis.” Ponemon Institute.Benchmark research sponsored by IBM independently conducted by Ponemon Institute LLC.2019. https://www.ibm.com/downloads/cas/ZBZLY7KL

5 Whitney, Lance. “Cybercriminals exploiting coronavirus outbreak with virus-themed sales on the dark web.” TechRepublic.March 19, 2020. https://www.techrepublic.com/article/cybercriminals-exploiting-coronavirus-outbreak-with-virus-themed-sales-on-the-dark-web/

6 “Update: Coronavirus-themed domains 50% more likely to be malicious than other domains.” Check Point blog post, accessed March 27, 2020. https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/

7 “U.S Small Business Administration Spoofed In Remcos RAT Campaign.” IBM X-Force Threat Intelligence.IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Small-Businesses-Seeking-Disaster-Assistance-Targeted-By-Remcos-Infostealer-e8b9f4f5e9d8c98f51e2ee09ac632ef8; “Holding Your Health For Ransom: Extortions On The Rise.” IBM X-Force Threat Intelligence.IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Holding-Your-Health-For-Ransom-Extortions-On-The-Rise-1fc43fac1cf1b72a4245f0107da283e3

8 “Covid-19 Drug Advice From The WHO Spoofed to Distribute Agent Tesla Info-Stealer.” IBM X-Force Threat Intelligence.IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826

9 Vergelis, Maria. “Coronavirus phishing.” Kaspersky Daily.February 7, 2020. https://www.kaspersky.com/blog/coronavirus-phishing/32395/

10 Whitmore, Wendi. “IBM X-Force Threat Intelligence Cybersecurity Brief: Novel Coronavirus (COVID-19).” March 17, 2020. https://securityintelligence.com/posts/ibm-x-force-threat-intelligence- cybersecurity-brief-novel-coronavirus-covid-19/

11 Stein, Shira, and Jennifer Jacobs. “Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak.” Bloomberg.March 16, 2020. https://www.bloomberg.com/news/articles/2020-03-16/u-s-health- agency-suffers-cyber-attack-during-covid-19-response

12 Miller, Maggie. “Top US health agency suffers cyberattack.” The Hill.March 16, 2020. https://thehill.com/policy/cybersecurity/487756-top-us- health-agency-suffers-cyberattack-report

13 Pipikaite, Algirde, and Nicholas Davis. “Why cybersecurity matters more than ever during the coronavirus pandemic.” World Economic Forum.March 17, 2020. https://www.weforum.org/agenda/2020/03/coronavirus- pandemiccybersecurity/

14 “CISA Insights.” US Cybersecurity and Infrastructure Security Agency website, accessed March 29, 2020.https://www.cisa.gov/insights

15 Mervosh, Sarah, Denise Lu, and Vanessa Swales. "See Which States and Cities Have Told Residents to Stay at Home." The New York Times.March 29, 2020.https://www.nytimes.com/interactive/2020/us/coronavirus-stay-at-home-order.html

16 Gettleman, Jeffrey, and Kai Schultz. "Modi Orders 3-Week Total Lockdown for All 1.3 Billion Indians." The New York Times.March 24, 2020. https://www.nytimes.com/2020/03/24/world/asia/india-coronavirus-lockdown.html

17 Miller, Maggie. "Zoom vulnerabilities draw new scrutiny amid coronavirus fallout." The Hill.April 2, 2020. https://thehill.com/policy/cybersecurity/490685-zoom-vulnerabilities-exposed-as-meetings-move-online

18 Seals, Tara. "Coronavirus Poll Results: Cyberattacks Ramp Up, WFH Prep Uneven." Threatpost.March 19, 2020. https://threatpost.com/coronavirus-poll-cyberattacks-work-from-home/153958/

19 "Federal employees may soon be ordered to work from home." The Washington Post.March 13, 2020.

20 "OODA loop." Wikipedia, accessed April 1, 2020. https://en.wikipedia.org/wiki/OODA_loop

21 "The 2019 Cyber Resilient Organization." Ponemon Institute and IBM.2019. https://www.ibm.com/downloads/cas/GAVGOVNV

22 Black swan events describe entirely unexpected situations outside the realm of normal expectation that have extreme consequences.Taleb, Nassim Nicholas. "The Black Swan: The impact of the highly improbable." 2007.

23 "Threat, vulnerability, risk—commonly mixed up terms." Threat analysis Group website, accessed April 1, 2020. https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly -mixed-up-terms/

24 Kallberg, Jan, and Col. Stephen Hamilton. "What COVID-19 can teach us about cyber resilience." Fifth Domain.March 2020. https://www.fifthdomain.com/opinion/2020/03/23/what-covid-19-can-teach-us- about-cyber-resilience/

25 Finch, Brian. "Cyber planners should be carefully watching the coronavirus." The Hill. March 2, 2020.https://thehill.com/opinion/cybersecurity/485391-cyber-planners-should-be-carefully-watching-the-coronavirus

26 Ferguson, Scott. "Cybersecurity Sector Faces Reckoning After Coronavirus Hits." BankInfoSecurity. March 10, 2020. https://www.bankinfosecurity.com/coronavirus-hits-wall-street-cyber-survive-slide-a-13913

27 "2019 Cost of Data Breach Study: Global Analysis." Ponemon Institute.Benchmark research sponsored by IBM independently conducted by Ponemon Institute LLC.2019. https://www.ibm.com/downloads/cas/ZBZLY7KL

28 For example, the annual IBM X-Force Threat Intelligence Index. https://www.ibm.com/security/data-breach/threat-intelligence

29 "High-Stakes Hiring: Selecting the Right Cybersecurity Talent to Keep Your Organization Safe." IBM Smarter Workforce Institute.2018. https://www.ibm.com/downloads/cas/X47BR759

30 "The 2019 Cyber Resilient Organization." Ponemon Institute and IBM.2019. https://www.ibm.com/downloads/cas/GAVGOVNV

关于研究洞察

研究洞察致力于为业务主管就公共和私营领域的关键问题提供基于事实的战略洞察。洞察根据对自身主要研究调查的分析结果得出。要了解更多信息，请联系 IBM 商业价值研究院：iibv@us.ibm.com。

国际商业机器中国有限公司
北京朝阳区北四环中路 27 号
盘古大观写字楼 25 层
邮编：100101
美国出品
2020 年 4 月

44031444CNZH-01