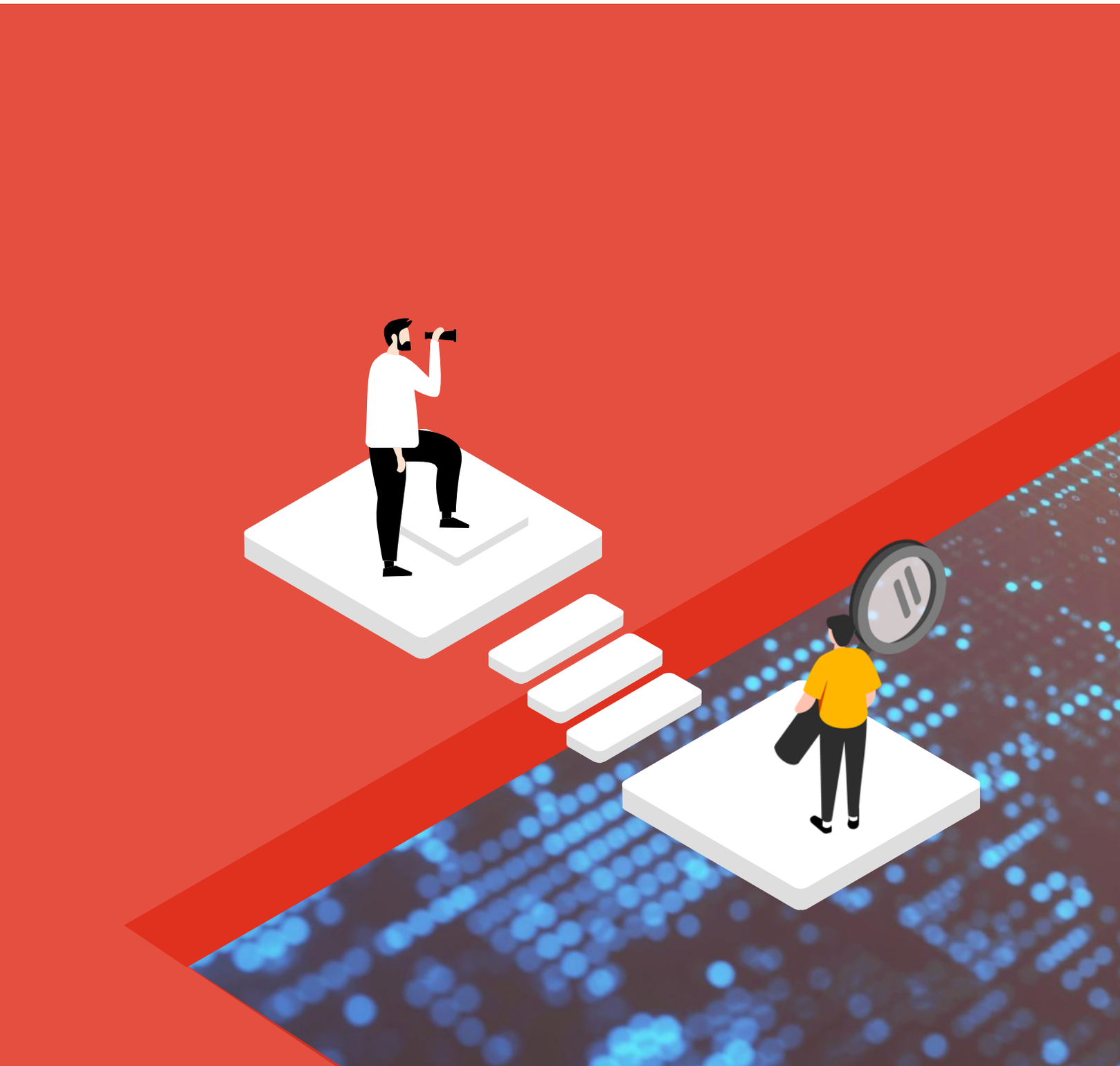
普华永道

2023年全球数字信任洞察调研中国报告

常备不懈 中国企业构筑未来网络安全防线



目录

前言

新冠疫情期间，人们由于封锁和隔离而不得不居家办公，商业世界也随之发生了重大变革。新冠疫情成为数字化转型的催化剂，加速了数字经济的发展。

随着全球数字化经济持续发展，中国正在加强网络安全实力，多年来稳坐世界第二大数字经济的地位。截至2022年6月，中国网民规模达到10.51亿，互联网普及率达74.4%。中国作为5G技术和标准的领导者，已建成全球规模最大的5G网络[i]。

从金融业到电信业，中国已经采取措施显著加强各主要行业的数据安全。2023年1月，中国工业和信息化部和国家互联网信息办公室等16个政府机构联合发布的重要指导意见提出发展目标，到2025年，数据安全产业规模超过1500亿元，年复合增长率超过30%[ii]。

企业和政府正在利用数字经济和新技术的发展，力图在后疫情“新常态”中保持竞争力并与时俱进。随着数字化的普及，企业需要进一步增强其安全能力来应对网络安全漏洞，同时防范或降低网络安全风险。同时，企业需要保持技术领先，避免在危机事件发生时由于不作为或违规行为而承担沉重的代价。

随着企业需要应对新技术和更加严格的法规，网络安全成为更加瞩目的焦点。公司不能承担成为数据泄露丑闻的中心并名誉扫地的后果。我们的2023年全球数字信任洞察调研的结果探讨了企业如何实现更全面的网络安全，以达到客户和监管机构的要求。

本报告反映了133名驻中国内地和香港特别行政区的高管的观点。就本报告而言，“中国”包含了中国内地和香港特别行政区的数据。如果香港与中国内地的调研结果存在统计学上的显著差异，会将结果分别列示。

网络安全成熟度以及来自竞争对手的威胁

随着中国和全球各国进一步发展数字经济，数字和非数字业务都面临着网络安全威胁。技术以前所未有的速度快速传播，这意味着网络安全变得空前重要。随着科技公司数量增涨和行业的快速发展，监管也在迎头跟进[iii]。企业需要采取主动措施，了解其风险暴露情况，并根据行业最新动向发展其网络安全能力，比法规领先一步。

在调研的时间背景下，与中国高管 (40%) 相比，全球高管中只有较小比例 (25%) 表示其公司的收入在过去6至9个月内出现下降。反之亦然，在同一时间范围内，与中国高管（49%）相比，更高比例的全球高管（59%）表示其公司的收入呈现增长。展望未来，各地高管普遍预计其企业的收入将在未来12个月内增长（中国：77%；全球：72%）。这可能由于疫情之后经济逐步复苏，并且技术的发展和应用将推动收入增长。

图一: 请说明贵企业收入的实际和预期变化

在未来12个月里

	全球	中国	中国内地	中国香港
净减少	13%	14%	10%	27%
净增加	72%	77%	80%	67%

技术的发展将改变所有行业，网络安全保护成为全球国家及地区的重点关注领域，在此趋势下，中国通过立法等手段加强网络安全。中国的《网络安全法》自2017年实施以来，一直得到严格执行。随着整体网络安全态势的不断变化，中国正考虑对前述法律进行修订，可以预见，该法律将更加严格，对违规行为的惩罚将更加严厉，而关键信息基础设施运营商承担的责任将更加重大[iv]。

为了加强在网络安全方面的国家实力，中国还制定了一项网络安全国家战略，实施了一系列相关的法律和法规。于2021年9月生效的中国《数据安全法》要求外国和国内实体在中国境内收集处理数据时应当依照法律规定，采取相应的技术措施保障数据安全。《个人信息保护法》紧随其后，于2021年11月起实施，这是中国首部专门针对个人信息保护的法律。收集处理国内个人信息的中国企业和外国实体均需要遵循这些新的法规要求。

随着技术风险增多以及监管环境更加严格，与全球高管相比，更高比例的中国高管计划在2023年增加其企业的网络安全预算（中国：73%；全球：65%）。仅11%的中国高管预计将减少其预算（全球：17%）。31%的中国公司的网络安全预算将增加6-10%，而只有23%的全球企业预计有相同水平的增长。9%的中国企业预计出现15%及以上的增长。

图二: 贵企业2023年的网络安全预算将有何变化？

2023年贵企业网络安全预算的变化

	全球	中国	中国内地	中国香港
净减少	17%	11%	10%	17%
净增加	65%	73%	76%	63%
减少15% 或以上	2%	1%	0%	3%
减少11-14%	3%	1%	1%	0%
减少6-10%	5%	5%	5%	7%
减少5%或以下	6%	5%	4%	7%
不变	13%	10%	9%	13%
增加5%或以下	23%	21%	17%	33%
增加6-10%	23%	31%	35%	17%
增加11%-14%	11%	12%	15%	3%
增加15%或以上	8%	9%	9%	10%

就其网络安全活动预算分配的特征而言，绝大多数中国首席执行官表示他们的网络安全预算基于对网络风险的量化评估，反映他们的网络安全优先事项，并且有助于为其公司创造价值。与全球同行相比，持此观点的中国高管比例更高。

图三: 下列陈述在多大程度上准确反映了贵企业未来12个月的网络安全预算？

回答“在很大程度上/一定程度上”的受访者

	全球	中国	中国内地	中国香港
与企业战略保持一致	91%	93%	95%	87%
反映出我们的网络安全优先事项	92%	96%	96%	97%
提供充足的资金来支持网络安全工作，以便为企业创造价值	91%	96%	96%	97%
在我们当前和长期的需求之间寻求了平衡	91%	95%	96%	90%
基于网络安全风险量化评估	91%	97%	97%	97%
将企业的网络安全风险偏好纳入考量	91%	92%	92%	93%
针对企业所面临的网络安全风险进行合理的分配	92%	95%	94%	100%

自2020年以来，由于数字化进程的加速，无论是从云迁移、电子商务和数字服务交付方式、IT和运营技术的融合，还是其他全球企业数字货币的使用等方面，中国和国际企业面临的网络攻击风险都有增无减。在中国内地，披露网络安全事件和措施的外部要求不断增长，尤其是当前法律要求国内企业在网络事件响应和违规管理中做到披露和公开透明。与此同时，更多香港和全球高管在其公司的网络安全风险内部报告的质量方面遇到了挑战。

图四: 自2020年以来，贵企业经历了以下哪些情况？

自2020年以来企业所经历的影响（排名指数）

	全球	中国	中国内地	中国香港
由于数字化程度的提高（例如：云迁移、采用电子商务和数字服务交付方式、使用数字货币、IT与运营技术的融合等），企业遭受网络攻击的风险增加	**第一位**	**第一位**	**第一位**	**第一位**
在企业网络风险敞口内部报告的质量方面遇到挑战	**第二位**	**第三位**	**第三位**	**第二位**
外部对网络安全事件和措施的披露要求增多	**第三位**	**第二位**	**第二位**	**第三位**
我们的系统出现更多网络安全漏洞	第四位	第四位	第四位	第四位
地缘政治环境的变化导致我们企业成为目标	第五位	第五位	第五位	第五位
监管调查、执法行动或法律诉讼增加	第六位	第六位	第六位	第六位

网络安全披露在企业方针中发挥关键作用

随着数字经济的进一步发展，世界各国政府正在不断努力跟上新的发展趋势，并实施法规以保护公众。例如，美国的2022年《关键基础设施网络事件报告法案》要求公司报告重大网络安全事件，并为上报行为提供激励措施。中国的《网络安全法》包含发生网络安全事件向主管机构披露漏洞的强制性要求和对违规的处罚[v]。

在新冠疫情爆发后，人们花费更多的时间使用移动设备，更多的公司采用混合工作模式，加快了全球转向数字经济的步伐。在这种背景下，自2020年以来，中国企业经历了许多挑战，包括网络风险内部报告的质量，以及外部对网络事件和措施披露需求的增加。一方面，一些企业可能采取了“预防胜于治疗”的思路，试图建立一套全面的政策，以确保详尽的内部报告既能比法规领先一步，又能预防那些可能需要披露的网络事件，从而避免公司声誉受损。另一方面，一些企业可能正尝试跟上最新的法规，并确保其流程符合规定。

自2020年以来，企业正在加强其网络安全工作并保持谨慎的态度。在中国和全球企业所面临的影响中，“监管调查、执法行动或法律诉讼”排名最末。

在中国公司对利益相关者的优先级排序方面，首席执行官和董事会占据前两位，而负责网络安全对策的政府机构和消费者权益保护监管机构排在第三和第四位。这印证了自《网络安全法》、《数据安全法》和《个人信息保护法》等法规实施以来，中国企业所面临的披露要求日趋严格。

图五: 请思考向以下各类利益相关者进行报告的情况，然后按照贵企业在未来12个月内的报告优先级对这些利益相关者进行排序

企业对待利益相关者的优先级（排名指数）

	全球	中国	中国内地	中国香港
董事会	**第一位**	**第二位**	**第二位**	**第一位**
首席执行官	**第二位**	**第一位**	**第一位**	**第二位**
价值链参与者	**第三位**	第八位	第八位	第八位
消费者权益保护监管机构	第四位	第四位	第四位	**第三位**
负责国家或联邦网络安全对策的机构	第五位	**第三位**	**第三位**	第七位
行业监管机构	第六位	第六位	第五位	第五位
消费者和其他私人倡议团体	第七位	第七位	第六位	第十位
财务报告监管机构	第八位	第五位	第六位	第四位
负责当地网络安全对策的机构	第九位	第十位	第六位	第六位
执法机构	第十位	第九位	第六位	第九位

与全球同行相比，中国企业往往对法规变化作出更有力的反应，并更加严格地遵守法规。更高比例的中国高管同意或十分同意，他们的企业有能力对外披露网络安全措施、战略和事件。特别是，86%的中国企业表示能够在报告期限内提供有关重大或重要事件所要求的信息，88%的企业能够有效评估网络事件的重要性以便报告。

图六: 下列陈述与贵企业对外披露网络安全实践、策略和事件的能力有关。请问您在多大程度上赞同或反对这些陈述？

贵企业向外界披露网络安全实践、策略和事件的能力
回答“非常同意/同意”的受访者

	全球	中国	中国内地	中国香港
我的企业能够在报告期限内提供有关重大或重要事件所要求的信息。	81%	86%	85%	87%
我的企业能够出于报告的目的而有效评估网络安全事件的严重程度。	80%	88%	88%	87%
我的企业能够出于报告的目的而说明董事会成员具备的相关网络安全专长。	78%	82%	82%	83%
我的企业已经制定一项政策，规定哪些网络安全事件的相关信息可以披露，哪些不得披露。	76%	84%	87%	73%
我的企业能够提供第三方网络安全风险管理的相关信息。	75%	85%	85%	83%

在研究企业如何管理和披露内部风险时，随着托管服务的普及，企业有必要深入了解其风险暴露范围。随着全球加强对风险的关注，公司和涉及第三方实体的价值链上的风险透明度更加明晰。85%的中国高管表示，他们的企业可以提供有关第三方网络风险管理的信息，这比全球高管高出10个百分点。这一点非常重要，因为41%的中国企业预计，相比2022年，2023年的第三方违规事件会显著增加。

图七: 对手可能通过以下哪些途径侵入贵企业的系统，请选择那些您预期会在2023年对贵企业造成更加重大影响的途径

对手将显著影响企业的途径

	全球	中国	中国内地	中国香港
移动设备	41%	32%	33%	27%
电子邮件	40%	27%	25%	33%
云端途径	38%	44%	43%	47%
网络应用	37%	45%	43%	53%
人员或用户（内部人员或社交工程）	37%	37%	39%	30%
第三方/第n方	34%	41%	38%	53%
终端（台式机、笔记本电脑）	33%	42%	44%	37%
软件供应链或访问	32%	37%	35%	43%
远程访问门户	32%	34%	33%	37%
物联网	29%	34%	36%	27%
运营技术	26%	44%	45%	43%

在日益数字化的经济中，首席信息安全官 (CISO) 被指定负责管理第三方风险。由于企业日常管理涉及敏感客户数据，公众欣慰地看到企业已经制定管理和治理客户数据的相关政策。在这些实践中，大多数企业会审查与其共享客户数据的第三方和合作伙伴；然而，更高比例的中国企业更加频繁地采取这种第三方审查（中国：82%；全球：78%）。考虑到最近实施的《个人信息保护法》，这样的行动预计将持续，因为数据隐私将成为所有CISO的首要任务。

图八: 贵企业在多大程度上实施了以下与客户数据管理和治理有关的政策和实践？

回答“总是/经常实施”的受访者

	全球	中国	中国内地	中国香港
我们只在获得明确许可的情况下使用客户数据	79%	78%	83%	60%
我们审查与我们共享客户数据的所有第三方和合作伙伴	78%	82%	83%	77%
在推出新产品和服务前对其进行数据安全和隐私评估	79%	83%	83%	80%
我们运用道德框架来指导我们在各种用例中对客户数据的使用	77%	74%	75%	70%
对于客户围绕我们持有的个人信息所提出的数据请求，我们制定了具体的响应时限	77%	74%	76%	70%
如果没有可依据的法规，我们通过政策、指导原则和价值观约束自我行为	77%	77%	82%	63%
我们在营销工作中遵循客户自愿选择、以保障隐私为先的策略	77%	80%	83%	73%
我们对通过物联网/传感器/智能设备收集的数据进行限制、匿名处理和删改	70%	73%	75%	67%
我们使用最新的技术（例如：差分隐私）来对客户数据进行假名化处理	72%	73%	76%	63%
我们检查客户端应用程序设计方式中是否存在黑暗模式	68%	76%	82%	57%

网络安全韧性亟待提升

多年来，网络安全已经成为一个日新月异的动态领域，以适应创新的商业实践。作为运营的重要组成部分，企业需要确保拥有足够的网络安全韧性来管理突发情况。如果缺乏韧性，网络事件可能会破坏大多数甚至所有的商业成功计划，导致财务损失、声誉损害和信任丧失。

如何评估和应对2023年的风险，这考验高管们团结协作、制定缓解大规模危机和避免业务中断的计划能力。在韧性计划所预计和考虑到的一系列威胁中，全球企业将灾难性网络攻击排在第一位，而中国高管则将这个威胁排在第三位，仅次于新冠疫情的复发或新的公众卫生危机，以及全球经济衰退的迫近。然而，随着中国内地于2022年12月重新对外通关并开放经济，取消大多数疫情控制措施，排列顺序可能会发生变化。

中国受访者优先考虑新的公众卫生危机计划，这并不出人意料，因为在过去三年中，新冠疫情深刻影响了中国的经济格局和数字转型的路径。为了在防疫政策调整和经济重启后应对短期国内挑战，中国企业不仅需要在其风险计划中考虑预期事件，还需要通过这些计划建立韧性，包括抵御突如其来的网络攻击的能力。

图九: 请展望贵企业在未来12-24个月内可能面临的总体风险，然后选出前五种被您正式纳入贵企业韧性计划的风险场景并对其进行排序

正式纳入企业韧性计划的前五种场景（排名指数）

	全球	中国	中国内地	中国香港
灾难性的网络攻击	**第一位**	**第三位**	**第三位**	**第二位**
全球经济衰退	**第二位**	**第二位**	**第一位**	第八位
新冠疫情卷土重来或出现新的公众卫生危机	**第三位**	**第一位**	**第二位**	**第一位**
通货膨胀环境	第四位	第五位	第五位	第四位
供应链瓶颈	第五位	第六位	第六位	**第三位**
新的地缘政治冲突	第六位	第八位	第十一位	第五位
商品市场波动	第七位	第四位	第四位	第九位
信贷紧缩/资本获取途径显著减少	第八位	第十二位	第九位	第十三位
大量员工流失	第九位	第九位	第八位	第十位
社会不稳定	第十位	第七位	第七位	第十二位
自然灾害或极端天气	第十一位	第十位	第十位	第十位
制裁的执行	第十二位	第十一位	第十二位	第六位
粮食危机	第十三位	第十三位	第十三位	第六位

值得欣慰的是，企业在中国网络安全法规的指导下，在建立网络安全韧性方面持续努力，并且取得阶段性成果。在过去的12个月中，网络安全在多方面取得了进展。在此时间范围内，与全球同行一致，中国高管同意或十分同意，他们的网络安全团队在增强网络安全韧性方面取得了众多成就，如提高了运营技术安全性（86%）、提升了网络安全资源的价值和利用效率（84%）以及协调各职能部门的工作以遵守新法规（84%）。超过77%的中国企业感受到了这些成就，高于全球水平。

图十: 请指出贵企业的网络安全团队在过去12个月内是否完成了下列工作

过去12个月中网络安全团队的成就（回答“是”的受访者）

	全球	中国	中国内地	中国香港
提高运营技术安全性	79%	86%	90%	73%
提高我们对勒索软件的防御能力	77%	82%	83%	77%
帮助企业将“安全和隐私”纳入新产品和服务的设计	75%	83%	83%	80%
提高网络安全资源的价值和利用效率	75%	84%	83%	87%
改善与运营技术/工程团队的协作	73%	83%	85%	77%
有效应对漏洞或攻击，同时确保不对我们的业务造成重大干扰和/或损害	72%	83%	89%	63%
预测到与数字计划有关的新的网络安全风险，企业因此能够预先管理该风险，防止其影响我们的合作伙伴或客户	71%	83%	86%	73%
改善供应链风险管理	70%	77%	81%	63%
协调各职能部门的工作，以遵循新法规的规定	70%	84%	87%	73%
检测到针对我们业务的重大网络安全威胁，并阻止其影响我们的运营	70%	81%	83%	77%

在一个日益复杂的互联世界中，风险可能来自任何领域。由于不可能完全免于遭受网络风险[vi]，因此采取“全灾害”方法来识别破坏来源对于每个企业都是必要的。超过七成的中国企业（73%；全球：62%）接受调研时表示已经对自身面临的风险有了广泛的了解。同时，与全球水平（ 52%）相比，更高比例的的中国企业（ 65%）已经正式协调和整合了业务连续性与业务恢复。尽管如此，企业仍然需要更多的灵活性，在当前水平之上进一步促进网络安全韧性。

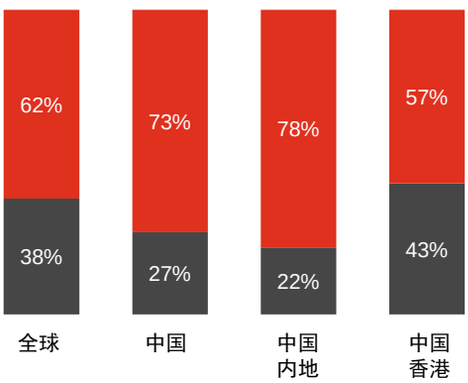
在瞬息万变的数字世界中，速度和适应性对于企业实现其目标至关重要。面对更加艰难和越来越不寻常的网络挑战，企业需要保持一定的灵活性，以便进行迅速和恰当的反应。只有44%的中国企业正在推广一种整合的、灵活的运营模式，可以应对各种业务中断事件。这意味着大多数企业使用的是孤立的、预先设定的计划和策略流程，这些流程旨在响应特定的业务中断场景，但可能无法以整体方式考虑大规模意外业务中断的情况。

网络安全韧性仍有可以提升的空间。中国企业需要加快开发预案，使企业能够主动而非被动地应对网络安全事件，同时考虑高优先级关键系统之外的风险。与全球同行类似，只有约一半的中国企业（52%； 全球：53%）采取预测性和预防性的方法，假设事件将会发生，嵌入包括威胁情报的韧性能力，以预测和抵御业务中断的发生。只有不到一半的中国企业（47%；全球44%）不仅考虑了持续运营所需的高优先级关键系统和操作，还考虑了第二和第三级依赖关系。

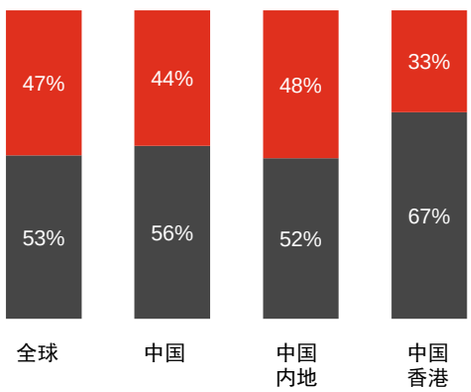
图十一: 超过六成的企业对他们面临的风险有了广泛的了解，但要推广集成、敏捷的运营模式，不仅要考虑网络韧性中的高优先级关键系统，还有更多工作要做

当前在网络安全韧性方面的方法和能力

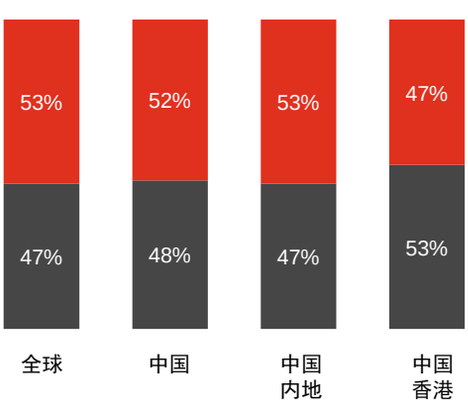
- 全面了解企业当前面临的风险，以及如何在整个企业同时面临多种风险时维持运营
- 专注孤立的风险情景，以及如何从该特定业务中断事件中恢复过来



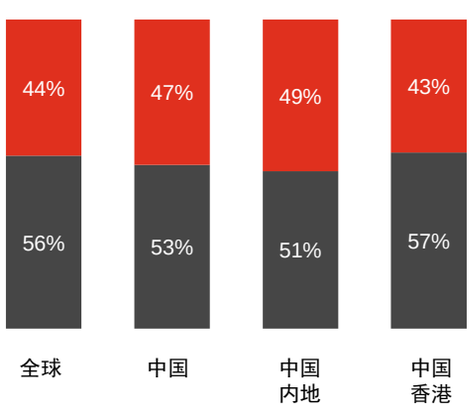
- 推广一种整合的、灵活的运营模式，可以应对各种业务中断事件
- 针对各类具体的业务中断事件分别预先确立和落实防范计划和流程



- 采取预测性和预防性的方法，假设事件将会发生，嵌入包括威胁情报的韧性能力，以预测和抵御一旦发生的业务中断
- 实施计划来应对已经发生的业务中断事件，并在发生故障或业务中断事件后专注于恢复企业运营

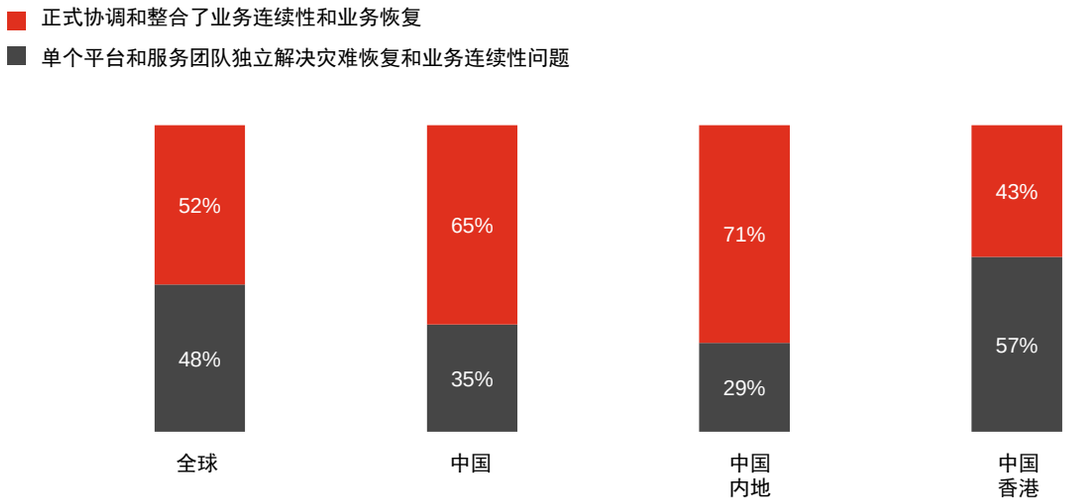


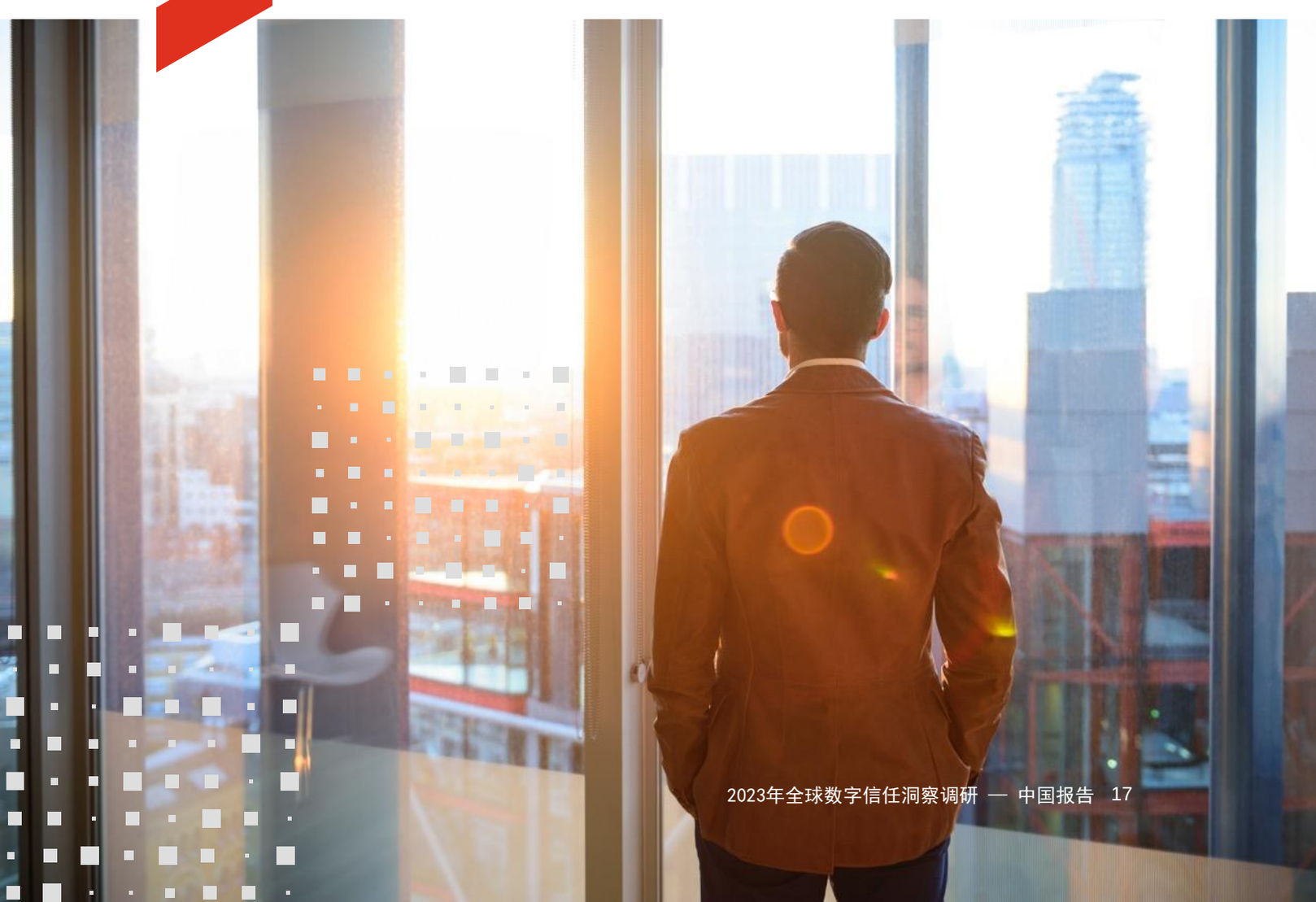
- 不仅考虑高优先级的关键系统和流程，还考虑第二和第三级依赖关系
- 考虑持续运营所需的高优先级关键系统和操作



图十一: 超过六成的企业对他们面临的风险有了广泛的了解，但要推广集成、敏捷的运营模式，不仅要考虑网络韧性中的高优先级关键系统，还有更多工作要做

当前在网络韧性方面的方法和能力





掌握网络安全转型的主导权

网络安全转型涉及众多方面和各种利益相关者，其中CEO和董事会优先级最高。由于员工对CEO负责，而CEO则对董事会负责，因此网络安全团队将公司的网络风险策略纳入董事会和高级管理层的讨论至关重要。

中国的《网络安全法》强调了企业领导者在其各自企业内维护网络安全的问责制和责任制的重要性。被确定为对违反网络安全保护义务负直接责任的企业领导人可能会因个人责任而被罚款。

调研表明，高管对各种网络安全问题负有责任。全球范围内，虽然CEO参与网络安全事务，但CISO对网络安全的多个领域具有最大的影响力。就职责而言，尽管中国和全球趋势基本相一致，但香港的情况与之不同。

在全球和中国内地的企业中，CISO主要负责多种网络安全行动，包括向董事会和高级管理层报告网络和隐私风险（香港：CIO）；协调网络安全事件响应（香港：CDO）；网络安全解决方案和技术的购买决策（香港：CIO）；与外部利益相关者沟通网络安全事项（香港：CEO）；管理第三方风险（香港：CIO）；评估与业务决策相关的网络安全风险（香港：CIO）；对并购目标进行网络安全尽职调查（香港：CIO）；网络安全保险覆盖和政策（香港：CIO）；以及运营技术/工业物联网的安全保障（香港：CIO）。

与全球和中国内地的同行相比，香港的CIO负责更多的网络安全领域。此外，全球和中国内地的CISO获得更多授权，得以倡导、协作和协调更好的网络安全未来。

图十二: 谁主要负责贵企业内部以下各个方面的网络安全事务 ？

*显示前三个答案

向董事会和高级管理层报告网络和隐私风险

全球	中国	中国内地	中国香港
CISO	CISO	CISO	CIO
21%	30%	34%	27%
CIO	CIO	CDO	CEO
16%	14%	13%	17%
CEO	CEO	CEO	CISO
13%	12%	11%	17%
CFO	CDO	CIO	CDO/CPO
7%	11%	11%	7%

保障软件开发的安全性（由DevSecOps保障DevOps）

CIO	CISO	CISO	CIO
19%	29%	29%	30%
CISO	CIO	CIO	CISO
17%	19%	16%	27%
CTO	CTO	CTO	CTO
11%	13%	14%	10%
CEO	CEO	CEO	CFO/工程/运营主管
10%	8%	9%	7%

图十二: 谁主要负责贵企业内部以下各个方面的网络安全事务 ？

*显示前三个答案

协调网络安全事件响应

全球	中国	中国内地	中国香港
CISO	CISO	CISO	CDO
25%	32%	37%	17%
CIO	CIO	CIO	CIO
17%	17%	17%	17%
CEO	CEO	CEO	CISO
11%	12%	12%	17%
CDO	CDO	CDO	CEO
8%	9%	7%	13%

决定网络安全预算

CFO	CFO	CFO	CIO
20%	26%	28%	20%
CEO	CISO	CISO	CISO
17%	23%	24%	20%
CIO	CIO	CEO	CFO
14%	11%	10%	17%
CISO	CEO	CIO	CTO
14%	10%	9%	13%

图十二: 谁主要负责贵企业内部以下各个方面的网络安全事务 ？

*显示前三个答案

管理数据治理和隐私

全球	中国	中国内地	中国香港
CIO	CIO	CDO	CIO
16%	21%	20%	30%
CDO	CISO	CISO	CISO
15%	18%	19%	13%
CISO	CDO	CIO	CEO
15%	17%	18%	10%
CEO	CPO	CPO	CPO
12%	11%	12%	10%

网络安全解决方案和技术的购买决策

CISO	CISO	CISO	CIO
20%	27%	30%	27%
CIO	CIO	CFO	CTO
17%	15%	16%	20%
CEO	CFO	CIO	CISO
13%	14%	12%	17%
CFO	CTO	CEO	CFO/COO/CRO
11%	11%	10%	7%

图十二: 谁主要负责贵企业内部以下各个方面的网络安全事务 ？

*显示前三个答案

与外部利益相关者沟通网络安全事项

全球	中国	中国内地	中国香港
CISO	CISO	CISO	CEO
19%	20%	21%	27%
CIO	CIO	COO	CIO
17%	16%	16%	23%
CEO	CEO/COO	CIO	CISO
16%	14%	14%	13%
CDO		CDO	CFO
8%		11%	10%

管理第三方风险

CISO	CISO	CISO	CIO
18%	20%	24%	30%
CIO	CIO	CEO	CRO
15%	17%	14%	17%
CEO	CEO	CIO	CDO
12%	13%	14%	10%
CRO	CDO/CRO	CDO	CEO
10%	11%	11%	10%

图十二: 谁主要负责贵企业内部以下各个方面的网络安全事务 ？

*显示前三个答案

评估与业务决策相关的网络安全风险

全球	中国	中国内地	中国香港
CISO	CISO	CISO	CIO
23%	30%	34%	27%
CIO	CIO	CEO	CISO
15%	17%	15%	17%
CEO	CEO	CIO	CRO
12%	12%	15%	13%
CRO	CDO	CDO	CDO/CIRO/GC
8%	10%	11%	7%

对并购目标进行网络安全尽职调查

CISO	CISO	CISO	CIO
17%	23%	27%	27%
CIO	CIO	CIO	CDO
17%	18%	16%	10%
CEO	CEO	CEO	CFO
13%	11%	13%	10%
CFO	CDO/CFO	CDO/CFO	首席审计执行官(CAE)/没有单一的负责人/CCO/CEO/CISO
8%	8%	7%	7%

图十二: 谁主要负责贵企业内部以下各个方面的网络安全事务 ？

*显示前三个答案

网络安全保险覆盖和政策

全球	中国	中国内地	中国香港
CISO	CISO	CISO	CIO
17%	28%	32%	23%
CIO	CIO	CIO	CFO
14%	18%	17%	17%
CFO	CFO	CFO	CISO
14%	11%	10%	13%
CEO	CDO/CRO	CDO	CRO
13%	7%	7%	13%

运营技术/工业物联网的安全保障

CISO	CISO	CISO	CIO
18%	29%	31%	30%
CIO	CIO	COO	CISO
17%	15%	12%	20%
CEO	COO	CIO	CTO
10%	11%	11%	10%
CTO	CDO/CFO	CDO	CFO/COO/CRO/工程/运营负责人
9%	8%	9%	7%

企业领导者在确保其企业站在更高的安全性立场方面发挥着重要作用[vii]。世界千变万化，高管需要掌握网络安全转型的主导权，使企业能够快速识别和降低安全风险，从而自信地采用支持其战略目标的新数字技术[viii]。

就在未来12-18个月内推动网络安全转型而言，中国的前三项举措与全球同行有所不同。在全球范围内，头号举措是确保所有非网络安全员工了解其行为可能带来的潜在安全后果。而在中国，提升企业在网络安全和隐私活动上的数据分析能力（全球：第二）被认为是转型的关键驱动因素，其次是整合企业技术解决方案，以实现更简化的技术架构。中国受访者还认识到领导力对于推动整个企业网络安全的重要性。

	中国	全球
1	提升对网络和隐私活动的数据分析能力	确保所有非网络安全领域的员工了解其行为带来的潜在网络安全影响
2	整合企业技术解决方案，以实现更简化的技术堆栈/基础架构	提升对网络和隐私活动的数据分析能力
3	在整个企业推进网络安全的领导力	在整个企业推进网络安全的领导力

结语

展望未来，随着中国数字经济蓬勃发展，中国网络安全市场将迎来进一步增长，其驱动因素包括：云服务的广泛采用；对先进安全解决方案的需求不断增长；对网络安全威胁的高度关注；以及在中国内地本地化和保护系统、技术基础设施和数据的需求。此外，政府正在增加对数字技术的使用并加强关键领域的机构开放计划，预计将为面向未来、做好网络准备的企业提供更多机遇。

鉴于当前的动态环境，中国企业必须开发一种整合的、灵活的运营模式，能够应对各种业务中断事件。这种模型应该具有灵活性，能够使企业作出快速、有效的响应，而非依赖于那些缺乏前瞻性、静态的威胁响应计划和流程。此外，企业在确定潜在的业务中断来源时必须采用“全灾害”方法，包括收集威胁情报信息和对已识别的威胁采取行动，以保持对网络安全风险的韧性。在急速发展的数字世界中，企业必须努力保持敏捷性，开发和测试预案，用以协助主动处理事件。为成功实现这些目标，高管必须将网络安全转型倡议整合到其业务战略中，并使企业能够自信地采用新的数字技术。

[i] http://english.scio.gov.cn/m/pressroom/2022-11/07/content_78506468.htm

[ii] https://www.scmp.com/tech/policy/article/3206997/china-unveils-plan-boost-data-security-key-industries-bet-data-driven-economic-growth

[iii] https://pro.bloomberglaw.com/brief/regulation-and-legislation-lag-behind-technology/

[iv] https://www.pwccn.com/en/issues/cybersecurity-and-privacy/china-cybersecurity-data-legal-developments-implications-businesses-oct2022.html#:~:text=October%202022&text=The%20Cybersecurity%20Law%20has%20been,at%20the%20end%20of%202021.

[v] https://www.tiangandpartners.com/en/news-and-activity/china-cybersecurity-law-mandatory-breach-notification.pdf

[vi] https://www.globalgovernmentforum.com/on-the-front-line-how-can-governments-safeguard-against-cyberattacks/

[vii] http://www.cisa.gov/shields-up

[viii] https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/transformation.html

联系我们

黄景深

普华永道中国内地及香港地区网络安全和隐私服务主管合伙人
+852 2289 2719
kenneth.ks.wong@hk.pwc.com

李睿

普华永道中国网络安全和隐私服务中国内地主管合伙人

+86 (10) 6533 2312
lisa.ra.li@cn.pwc.com

编辑和写作

Shivia Ganglani

雷国锋

吴俊怡