新规之下，你的网络安全事件处理“跑得赢”时间吗？

2025年9月28日

The better the question. The better the answer.
The better the world works.

EY安永

Shape the future with confidence

聚信心 塑未来

新规之下，你的网络安全事件处理“跑得赢”时间吗？

2025年9月28日

2025年11月1日起，**《国家网络安全事件报告管理办法》（以下简称《办法》）**正式施行。《办法》对所有网络运营者提出了明确要求：在发生安全事件后，应当按照《办法》规定**及时、准确**地将事件情况上报给监管机构。

这不仅仅是“写一份报告”那么简单。它对企业的应急响应能力提出了终极考验，因为这份“报告”的背后，是对企业在危机时刻从技术到管理，再到合规的全链条掌控能力的严苛要求。

安永洞察：合规报告背后的三大硬核挑战

《办法》的出台让企业在面对真实网络攻击时面临着三大挑战。

挑战一：时间极限下的判断与上报

《办法》对重大级别的上报要求十分严格。现实中，从“发现异常”到“能否判定影响等级、组织有效信息、提交合规报告”，往往需要跨部门的确认和取证。时间窗口一压缩，问题就暴露：

- 技术能发现问题，但不知道哪些必须上报
- 管理层要拍板，却拿不到清晰结论
- 合规、公关在等，但缺乏同步信息

挑战二：跨部门协同的“真空带”

网络安全事件的处置，绝不是技术部门的“独角戏”。《办法》要求报告事件处置的详细情况，这需要技术、法务、公关、业务等多个部门协同作战。

想象一下：当勒索软件攻击发生，技术团队在抢救数据，法务需要评估支付赎金的法律风险，公关团队要准备对外声明。如果各部门平时没有磨合、没有清晰的流程，在危机时刻将各自为战，陷入混乱。

挑战三：报告，是“事后总结”还是“战时前置”？

《办法》强调的“及时报告”，意味着它不再是一个在事件平息后慢慢撰写的“事后总结”，而是需要融入整个应急响应流程的“战时前置”环节。

这要求企业必须在日常安全运营中建立一套能够快速触发、无缝衔接的报告机制。从事件监测、告警、处置到最终上报，整个流程须环环相扣，才能满足《办法》针对时限的严格要求。

安永观点：合规，是检验你应急能力的“试金石”

《办法》出台的目的并非增加企业负担，而是推动企业将网络安全从“被动防御”提升到“主动响应”的实战水平。合规本身不是目的，而是推动企业能力建设的最佳契机。

应对这些挑战，仅仅采购更多的安全设备是不够的。企业需要提升团队的实战能力，通过体系化的演练和培训，将流程固化到团队的肌肉记忆中。这些挑战归根结底都指向一个核心问题：**当事件真正发生时，你的团队能否高效协作，快速决策，并在规定时限内完成所有必要步骤？**

要回答这个问题，最好的办法就是进行应急响应演练。它不是“纸上谈兵”，而是将团队置于模拟的实战压力下，通过反复演练，发现流程中的盲点，磨合团队的协作机制，从而将事件响应的动作，转化为团队的本能反应。

安永服务：主动“预见”，未雨绸缪——剧本杀式网络安全应急响应演练（Cyber Wargame）服务

传统的网络安全应急响应演练往往对参与者的反应和行动进行了事前定义。为了让演练更具实战性和吸引力，我们摒弃了传统的生硬模式，引入了沉浸式的“剧本杀”形式，让参与者“做自己”。为了全方位考验参与者的**团队协作、应变能力、策略运用**及**决策水平**，在演练过程中，关键信息会在特定时刻揭示，让参与者在短时间内进行密切协作与关键决策。同时，通过各种工具和技术，提升互动性和趣味性，让整场网络安全应急响应演练变得更加生动与沉浸。

剧本杀模式颠覆传统演练方式，融合卡牌和安永wavespace™的技术，提升真实感、强化合作与沉浸体验。

1.参与者**扮演日常工作中的角色**，身临其境地体验模拟的网络攻防情境。

2.定制化的故事线图驱动情节发展，**模拟真实攻击与应对过程**，提升演练的互动性和挑战性。

3.借助**虚拟现实**技术，增强演练的互动性和真实感，让参与者**全方位体验**网络攻防场景。

4.用视觉化工具**提升团队协作**，实时更新和共享信息，提高演练的协同性和效率。

安永提供的网络安全应急响应演练，涵盖了四大考察层面，帮助你的团队在实战中找到薄弱点，优化流程，最终将合规要求转化为企业的核心安全能力。

类型	关注点	受众群体
应急响应执行演练	应急响应流程的执行有效性，聚焦跨团队的沟通、协作能力的考核。	首席信息安全官（CISO）、事件协调员、法务合规代表、技术负责人（应用、基础架构）、业务团队执行层（如客服、市场营销、公关）等。
应急响应领导决策演练	聚焦网络安全危机事件，重点考察决策制定和对外沟通策略。	管理层（CXO），首席信息安全官（CISO）、法务总监、公关部门总监、政府事务负责人、业务部门负责人等。
技术应急响应演练	评估信息科技部门在应对安全事件的技术检测、遏制、响应和恢复能力。	首席信息安全官（CISO）、安全团队、基础架构团队、应用团队、运维团队。
红蓝对抗演练	通过模拟真实黑客攻击，让组织在“被攻击”的环境中验证技术与流程的有效性，发现盲点，提升安全运营的能力。	应急团队负责人、安全运营（SOC）团队

无论是网络攻击、系统中断、供应链中断，还是声誉危机、自然灾害，我们都能为企业匹配最贴近业务的演练场景—既可以直接选用成熟案例，也可以根据企业的行业、组织架构和风险特征量身定制。

常见安全威胁类型	
远程办公安全	内部人员威胁
勒索软件、网络钓鱼与语音钓鱼	供应链风险
开发安全与风险	数据泄露
零日漏洞威胁	关键业务系统宕机
云安全威胁	人工智能威胁

常见业务影响示例	
隐私合规风险	社交媒体热点
监管关注、调查或处罚	消费者/客户投诉
公司内部数据在暗网被出售	与名人/代言人相关的负面舆论
业务中断	经济损失（薅羊毛、优惠券刷单）

最有效的演练总是源于最真实的挑战，通过深度定制化剧本、沉浸式体验、专业引导与深度复盘等，我们致力于为企业模拟高压、逼真的网络安全应急响应演练。多重事件实时注入，制造真实危机下的信息轰炸，全面检验团队的应对方法、决策效率与沟通协作，帮助企业精准识别改进空间，将合规要求转化为真正的应急响应能力。

如需了解更多信息，欢迎联系我们：

高轶峰

主管合伙人
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
kelvin.gao@cn.ey.com

王瑾

合伙人
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
lena.wang@cn.ey.com

薛淼

经理
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
miao.m.xue@cn.ey.com

汪子婷

高级顾问
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
emma.zt.wang@cn.ey.com

安永 | 建设更美好的商业世界

安永致力于建设更美好的商业世界，为客户、员工、社会各界及地球创造新价值，同时建立资本市场的信任。

在数据、人工智能及先进科技的赋能下，安永团队帮助客户聚信心以塑未来，并为当下和未来最迫切的问题提供解决方案。

安永团队提供全方位的专业服务，涵盖审计、咨询、税务、战略与交易等领域。凭借我们对行业的深入洞察、全球联通的多学科网络以及多元的业务生态合作伙伴，安永团队能够在150多个国家和地区提供服务。

All in，聚信心，塑未来。

APAC no. 03023924
ED None

ey.com/china

关注安永微信公众号
扫描二维码，获取最新资讯。