网络弹性研究：事件响应计划和安全自动化技术

简译版

非官方中文译文•安天技术公益翻译组 译注

文档信息			
原文名称	Cyber Resilience Study: Incident Response Plans and Security Automation Set High Performers Apart		
原文作者	Larry Ponemon	**原文发布日期**	2019 年 4 月 11 日
作者简介	Larry Ponemon 是 Ponemon Institute 主席兼创始人。 https://securityintelligence.com/author/larry-ponemon/		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/cyber-resilience-study-incident-response-plans-and-security-automation-set-high-performers-apart/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

网络弹性研究：事件响应计划和安全自动化技术

Larry Ponemon

2019 年 4 月 11 日

今天，波耐蒙研究所（Ponemon Institute）发布了第四届年度《网络弹性企业报告》。这项全球性研究始于 2015 年，由 IBM Security 公司赞助。

随着时间的推移，网络弹性对企业的重要性显著增长。安全领导者正在努力对其“准备就绪程度”（preparedness）和安全级别进行基准测试，并衡量其抵御网络攻击的弹性恢复能力。

在今年的研究中，Ponemon Institute 采访了 3655 名 IT 和安全专家，涵盖了 11 个不同的市场：美国、加拿大、印度、德国、日本、巴西、英国、法国、澳大利亚、中东和东南亚。

对网络弹性进行基准测试以确定最佳实践

回顾去年的研究，企业网络弹性的最大障碍是缺乏对“人工智能”（AI）和“机器学习”（ML）等重要技术的投资。而今年，我们发现了一个重大变化：23%的受访者已经广泛采用了包括 AI 和 ML 在内的安全自动化技术。

在今年的研究中，我们将最具网络弹性的企业单独列出来，分析他们的方法和习惯，并据此创建了衡量网络弹性的基准。我们将这些企业称为“表现优异者”（high performer），有 960 名受访者（占总样本的 26%）被认为是“表现优异者”。接下来，我们来分析这些企业为实现网络弹性所采取的措施。

首先，这些企业具备事件响应计划。55%的“表现优异者”在整个企业中部署了“网络安全事件响应计划”（CSIRP），而其他企业中只有 23%部署了 CSIRP，另外 77%则缺乏 CSIRP。自该研究启动以来的四年里，这一数字没有发生太大的变化；但是，大量的企业缺乏实现网络弹性的基本构建模块，这一点令人震惊。

今年，我们首次跟进这些受访者，以期了解他们面临的障碍。一些受访者表示，他们缺乏推动网络弹性所需的人员配置或强有力的领导；而另一些受访者则指出，他们的组织结构存在障碍，无法采用集中式的方法。

近一半（46%）的受访者表示，虽然《通用数据保护条例》（GDPR）自 2018 年 5 月就生效了，但是其企业至今尚未完全实现 GDPR 合规性。在未来的研究中，我们计划探讨公司缺乏一致的事件响应计划的原因。

“表现优异者”的独特之处

很明显，较好的网络弹性会给企业的安全态势带来积极的影响。这些企业遭受的数据泄露事件较少（41% vs 55%），网络攻击造成的破坏也较小。进一步研究发现，他们具有较大网络弹性的原因在于人员、流程和技术的融合。

在“人员”方面，技能差距仍然是大多数企业面临的主要障碍。受访者指出，人才短缺、难以招到和留住高技能人才是主要障碍。“表现优异者”能够更好地解决这些问题，更重要的是，这些企业的领导层重视人才和网络弹性。

在“流程”方面，超过 55%的“表现优异者”部署了 CSIRP，他们更有可能参与威胁情报和数据泄露共享合作伙伴关系（69% vs 56%[平均值]）。

最后，“表现优异者”认为 IT 解决方案过于复杂也会带来挑战。因此，这些企业很可能部署更少的安全解决方案（39 个 vs 45 个），并相信他们拥有适当的技术来实现网络弹性。

采用安全自动化技术降低数据泄露成本

企业需要制定策略来应对这些挑战，并考虑如何在遵守 GDPR 和其他法规的前提下处理安全事件。

网络攻击的数量和严重程度持续上升，但研究表明，采用安全自动化技术的企业可以节省高达 155 万美元的数据泄露成本，而不采用安全自动化技术的企业则需要承担更高的数据泄露成本。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*