专家洞察@IBV

顺利度过 Boom 事件危机

提高安全危机决策水平

IBM 商业价值研究院

应对安全危机

不时有影响数百万人的数据泄露事件见诸新闻头条，引发高度关注。一些大型企业的首席执行官被迫前往政府委员会接受立法人员的讯问。席间不免提出很多严苛问题，堪称首席执行官的噩梦：安全防护为何如此松懈？为什么没有意识到发生问题？为什么反应如此迟钝？大部分企业都将 IT 资源集中在检测和预防工作方面，却不够重视响应和补救。

了解违规事件时间表

最近几次重大安全漏洞事件表明，许多企业的准备措施不够充分。在指定的 2 年期限内，企业有 25% 的概率遭受重大威胁。[1] 然而，有相当一部分企业根本无法应对重大安全事故。事实上，Ponemon Institute 开展的一项调研发现，75% 的企业并未全面统一实施事故响应计划。[2] 鉴于全球有关违规通知的法律法规日益严格，向政府和公众通报的时间要求越来越短，这项缺陷尤其令人担忧。

在安全漏洞的整个生命周期，将会发生若干关键事件。首先，出现漏洞。其次，数据被截获或销毁。第三，外部或内部机构发现漏洞。最后，公布漏洞。通常出于事故响应的目的，人们将时间表中的各关键环节称为“Boom”事件。而在本文中，Boom 事件的定义为漏洞被媒体公诸于众，企业已无法控制事态的时刻（见图 1）。

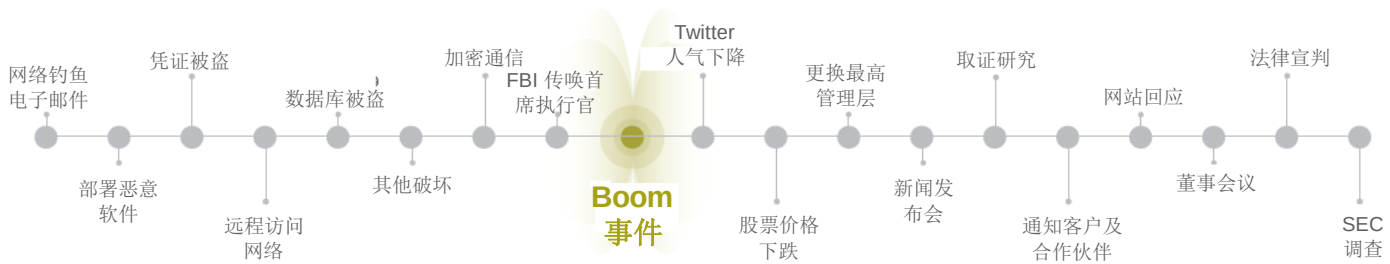
尽管新闻媒体通常只关注事件本身，但漏洞往往持续数月。

人们将披露或发现漏洞前的一段时间称为“Boom 前期”。在此期间，网络窃贼会伺机获取凭据，实施深入访问，窃取可以牟利的数据，攻击关键知识产权或准备发动毁灭性攻击。通常，恶意用户会秘密潜入，甚至很长一段时间根本不会发现他们访问系统。对于企业而言，针对 Boom 前期的活动可能包括安全规划和实施检测工具。

“Boom 后期”则是指响应并处理目前已知的安全漏洞。过去，大多数企业都主要关注“Boom 前期”而非“Boom 后期”，但时间表的两端都很重要。

图 1

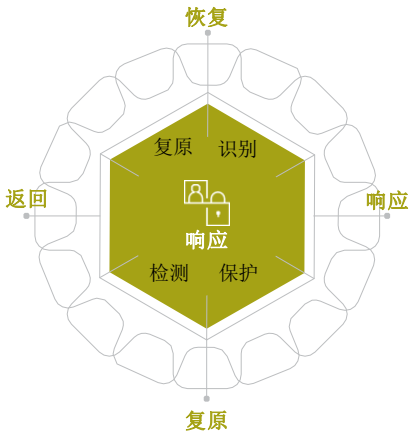
假设性安全漏洞的时间表



来源：IBM 安全事业部

图 2

为有效应对危机，整合业务流程和内部安全流程至关重要。



来源：IBM 安全事业部

改善 Boom 事件决策

发生 Boom 事件期间，企业可能应对得当，也可能决策失误或完全失控。一旦发生安全漏洞或网络攻击，高管必须督促做出有效应对。必须快速增强客户以及其他利益相关方的信心，说明自己将竭尽所能解决问题。对于许多最高层主管而言，这种快速直观的响应运用得并不那么自然。尽管他们可能清楚如何从技术层面堵住漏洞，但往往并未做好应对人为因素的准备。在危机情形下，最高层主管面对的主要是人类对手，往往令他们应接不暇。电话响个不停，既有愤怒客户投诉，又有记者质问，很可能令他们措手不及，往往导致心理防线崩溃或者无暇采取应对措施。发生危机期间，采取措施总比什么都不做好，即使有些措施从长远角度而言并不恰当，但聊胜于无。

一旦出现安全漏洞或网络攻击，您一定会觉得时间不够用。安全团队主管和成员亟需筛选可用信息，掌握事件的来龙去脉，以便快速做出最佳决策。可以借鉴军事战略家首创的应对原则，企业通常必须“观察、定向、决策并行动”。为顺利完成这一过程，人们往往采用迭代方法。核心理念在于，如果可以抢先对手一步完成循环过程，势必能够占得先机。通过快速执行一系列应对措施，就能够协调各方面的工作，避免被动应付局面。任何决策均不应作为最终决策，即使犯些小错误，也好过什么都不做。

积极开展 Boom 后期工作

Boom 后期阶段不仅要缓解攻击产生的破坏，还要在客户和媒体了解情况后引导公众舆论。Boom 后期阶段采取的措施可能决定企业的未来命运。发生危机时，高管必须充分表现出熟练的领导能力，绝不能给公众留下企业试图隐瞒事态的不良印象。

在发生网络攻击或安全漏洞期间和事后，快速决策能力至关重要。我们的研究发现，目前及不久的将来，人们面临的首要网络安全挑战在于缩短平均响应和解决时间。[3] 为快速处理事故，企业不仅需要制定规程，还必须反复演练应对措施，以便在发生事故时自动做出反应。

主要经验教训和建议

在与全球众多客户开展数百次模拟并积累大量经验后，我们总结出三项主要经验教训。

1. *以成果为导向。*行之有效的安全文化是关键所在。必须保护企业的品牌、声誉和未来发展。在这样的安全文化中，在事故期间应广泛传达并清晰理解“企业管理层的意图”。究竟怎样才能算作成功度过安全危机？
2. *切实落实安全计划。*仅仅制定细致的安全计划和操作手册还远远不够。计划可能看起来很棒；然而，一旦面临压力，很可能土崩瓦解。如不经常运用和磨练技巧，肌肉记忆将逐渐衰退。整个企业必须始终如一地贯彻和完善计划实施，并检验训练成果。
3. *充分发挥不同的背景优势。*具有急救医学和军事背景的员工往往比具有传统业务或技术背景的员工更善于进行安全模拟。由于此类员工习惯于持续练习、规划和准备应对大量不同的情况，通常可以在重压下快速做出决策。

拳不离手，曲不离口

倘若一个人只是在书中读到过急救知识，一旦心脏病发作，绝不能指望这个人实施心肺复苏术。在生死攸关时刻，只有练习过心肺复苏术并且具有发达“肌肉记忆”的人员才能有效进行胸外心脏按压。只有勤习不辍的专业人员才能挽救病人生命，因为他们学习过心肺复苏术，即使不是以人为模拟对象也不受影响。

同样，高管光有应对危机的理论知识也是不够的。他们必须勤加练习，熟悉实际发生安全事件时可能会出现的状况。获取现实生活实践经验绝无捷径可走。通过模拟，可以练习在特定情况下如何做出反应。在模拟过程中，您可以亲身体验受控环境下发生的意外状况并研究响应方法，可以不断重新尝试以提高应对水平。

设想一下，如果可以像飞行员进入飞行模拟器那样体验网络安全模拟，了解如何最有效地应对紧急情况，该有多好。

模拟安全事件的关键在于尽量保持真实性，让人们学会相互配合。在模拟过程中，全体成员（包括安全团队、沟通和公关专业人员以及首席执行官）都能切身体验网络攻击场景。经历过这种身临其境的安全体验后，就可以检验并改善整个企业的员工技能、安全流程和领导能力。除了帮助员工应对事件本身及 Boom 后期影响以外，实施模拟还有助于主管和领导根据真实事件和经验制定更具战略意义的长期措施计划。

改进响应成效

一旦出现危机，必须进行规划和演练，除此别无选择。员工在体验过模拟网络攻击后，必定能在实际发生事件时信心满满地发挥领导能力和快速决策能力。为最有效地做出应对，首先应重点保护员工和客户的安全，其次要保护数据，最后才是企业品牌。问题不在于*是否*会发生危机，而是*何时*发生危机；因此，在前进的过程中，务必花些时间仔细思考下面这些问题：

- 在事故响应方面，我们是否反复演练制定的计划？我们是否建立了反馈周期，用于整合所学到的经验教训？
- 我们是否具备适当的技能？我们需要更多地练习哪些“肌肉”？
- 我们的高管团队是否知道发现入侵后需要立即采取的关键行动以及要做出的关键决策？

主题专家

Caleb Barlow

IBM 安全事业部 XForce 威胁情报副总裁
cbarlow@us.ibm.com
https://www.linkedin.com/in/calebbarlow

Christopher Crummey

X-Force Command Cyber Range 执行董事
chris_crummey@us.ibm.com
https://www.linkedin.com/in/chriscrummey

关于专家洞察@IBV 报告

专家洞察代表了思想领袖对具有新闻价值的业务和相关技术主题的观点和看法。这些洞察是根据与业界领先的主题专家的对话总结得出。要了解更多信息，请联系 IBM 商业价值研究院：iibv@us.ibm.com。

New Orchard Road
Armonk, NY 10504

美国出品
2018 年 1 月

备注和参考资料

1 Ponemon Institute.“2016 Cost of Data Breach Study:Global Analysis.”Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC.2016. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

2 Ponemon Institute and IBM.“The 2016 Cyber Resilient Organization.”2016. http://info.resilientsystems.com/ponemon-institute-study-the-2016-cyber-resilient- organization

3 “Cybersecurity in the cognitive era:Priming your digital immune system”, IBM Institute for Business Value, November 2016

26012626CNZH-01