没有准备就是准备失败

克里斯·吉布森
FIRST.Org 执行主管

我是谁？

- 我为什么有资格谈论这个主题？

克里斯·吉布森 （Chris Gibson）

在花旗集团工作19 年，负责全球事件管理和计算机取证工作

在FIRST.Org 董事会任职10年，其中5年任首席财务官，两年任主席

建立并运行了英国第一个正式的全国性计算机应急响应小组

在金融服务行业任首席信息安全官两年

近期开始担任FIRST.Org的执行主管

电子邮件：chris@first.org

机构网址：www.first.org

历史告诉我们什么？

胜利者未上战场已获胜利，
而战败者先上战场再设法取胜。

历史告诉我们什么？

或者说……

5P法则

适当的规划可避免糟糕的表现

（Proper Planning Prevents Poor Performance）

最佳做法告诉我们什么？

网络安全成熟模型

美国国家标准技术研究所（NIST）

识别　了解你的环境、任务和风险承受能力

保护　保护好你的环境

发现　通过监测发现事件和异常活动

响应　以有计划、风险可控的方式对事件作出反应，从而最大限度降低风险

恢复　回归完全正常运转的状态

政府怎么说？

国家网络法

第55条

当发生网络安全事件时，应立即启动网络安全事件应急响应计划，对网络安全事件进行评价和评估，要求网络运营商采取技术和其他必要措施，消除潜在的安全风险，避免威胁扩大，并迅速公开发布相关警示。

监管机构怎么说？

英国金融服务领域的网络和技术复原力

负责监督的执行主管梅根·巴特勒的讲话 （2018年11月）

截至今年10月的一年内，各公司向金融行为监管局报告的技术故障数量增长了187%，收到报告的所有事件中有18%与网络袭击有关。

不过，在此我想强调几点：第一，报告事件数的增多并不仅仅反映了网络袭击和故障数量的大幅增加，它也表明企业开始更为积极地进行相关报告了。不过，我们仍高度怀疑隐瞒不报的问题依然存在。

第二，金融行为监管局并不期待“零故障”的局面。这点在七月份金融行为监管局与英格兰银行关于运行弹性的讨论文件已有说明。 那份文件中谈到设定“影响容忍度”的问题，还谈到企业中断运行后恢复和戏曲教训的能力问题。

相关内容如果换一种更适合今天这个场合的方式来说就是：真正能反映英国金融业复原力强弱的，不是没有事件发生，而是我们的事件管理做得好不好。

https://www.fca.org.uk/news/speeches/cyber-and-technology-resilience-uk-financial-services

市场怎么看？

波耐蒙研究所

- 就全球来看，如果一家公司能够在30天内将一次故障控制住，那么与持续时间更长的情况相比，它至少节省了100万美元。
- 一家公司若设有事件响应小组，则每次课节约14美元。

英国技术研究公司

- 有关数据破坏的新闻爆出后，公司的股票价格会震荡几周至几个月，不过最剧烈的震荡通常出现在消息披露后的14个交易日内。然后实际股价就会回升，消息披露一年后，平均上涨8.53%，但与纳斯达克相比，这些股票平均下跌3.7%。到披露后两年时，股价会上涨17.87%，但与纳斯达克相比则下跌11.35%。

有哪些众所周知的事实？

达信/微软（2018）

- 70%的受访者认为IT部门是网络风险管理的负责和决策部门，37%认为应有高管负责，32%选择了风险管理部门。
- 75%的受访者认为业务中断是潜在财务影响最大的网络损失场景，只有不到50%的人确实会估算损失数额，而这部分人中又只有11%会对网络风险进行量化。
- 有五分之一的机构目前没有或网络保险或没有购买计划，四分之一的人不清楚网络保险的情况。

- 负责风险与技术的管理人员中有45%表示他们会将网络安全信息发给董事会。
- 18%的董事表示，他们会收到网络安全方面的信息。

- 62%的企业将网络安全列为五大风险之一，比2016年翻了一番。
- 19%的人对管理和响应相关问题的能力具有“高度自信。
- 30%有相关计划。

那么，我们该怎么做呢？

事件响应需作为网络战略的一部分。

- 最好假设会出现故障。
- 我们往往是事后才考虑防御系统。
- 必须有计划，并且有记录，并且经过测试。

那么，我们该怎么做呢？

- 信领导
- 管理息缺口
- 建立关系
- 确保具备适当的技能
- 明确你的义务
- 演练、演练、再演练

领导

如果故障严重，高层领导的响应就至关重要了。管理人员必须与企业的宣传、法务、审计和合规团队，以及人力资源和技术部门相互协调。出现的故障可能非常复杂，而且我们也常能见到故障发生后管理层行事不当而引发的伦理和法律问题。

恰当的领导有助于避免类似情况发生。

管理信息缺口

预先进行计划并指定专人负责信息沟通。此人将与事件响应负责任密切配合，满足本组织内各第三方的信息需求。在事件过程中，人们会要求得到大量的信息，而实际负责调查情况并提供信息的人员却很少。

经常被忽视的一个环节是，要详细记录每一项决策是如何做出的。

贯穿事件全过程的良好沟通可能是决定成败的关键因素。

建立关系

等到事件发生时再建立信任和关系为时已晚。要让你的团队在并不需要他们帮助的时候就预先与业务合作伙伴、全国各计算机安全事件响应小组，以及服务供应商建立关系。

加入相关的组织，在相关的会议和行业工作组中与他们的安全团队会面，或使用现有的供应商审查程序等机制来预先确定适当的联络人并与其保持联系。

事件过程中要想开展有效的合作，信任是关键。

确保你具有适当的技能

保留外部的法务、公关和技术支持，他们能够提供一些内部团队不具备的技术技能，包括法务、公关和技术支持等，比如危机管理或磁盘取证。

找好这类服务的供应商，事先与其签订含有预付款项的协议。

明确你的义务

你也许对客户做出了承诺，保证一旦发生数据破坏，将在很短的时间内告知。即使你不做出这类承诺，也有越来越多的现行法规对此做出要求，比如欧盟的《通用数据保护条例》。按其规定，组织要在72小时内收集相关信息并依据监管要求，也就是《欧盟网络与信息安全指令》进行报告，具体的数字服务供应商不得延迟报告。

要提前了解所有相关要求，这样才能保证事件响应程序按照这些要求进行。

演练，演练，再演练

人们常常认为安全演练只有在达到一定的成熟度之后才重要，这是一种误解。选取其他机构遭遇的一次事件，进行一次桌面演练，看看如果相同的情况发生在你所在的机构，你们会怎样应对。这样至少可以发现还有哪些缺漏需要弥补。演练应该定期进行，广泛参与。上至高管，下至普通技术员工都要参与，这很重要。

这会建立一种“肌肉记忆”，当一次事件真正发生时发挥难以估量的巨大作用。

最后一环（一）

研究并记录这次事件。

处理安全事件的过程中最重要的阶段就是“事后”阶段。我们基本上不可能杜绝所有事件，所以有事件发生正是我们反思为何会出现这种情况的好机会，也是发现改进相关程序办法的一个机会。要问“五个为什么”：每当你认为自己已经明白一次事件为何会发生时，就再深入一步，多问一个为什么，找到深层的原因，至少要问五遍为什么，层层深入。

在每个层面上都要有所行动，对更深层次的原因给予更多的关注。因为这些深层原因如果不能妥善处理，将导致下一次事件。

最后一环（二）

研究并记录这次事件。

不要浪费任何一次事件的良机。一次事件会带来两方面的好处：

首先，事件可以非常清楚的体现需求和影响，因此往往是争取追加投入以避免下一次事件的最佳时机。一定要清楚地说明目前的安全程序还需要哪些改进才能更加有效，制定跟进计划让高管能够有所投入。

其次，你处理的每一次事件都会让你更加了解你所在的机构，了解内部各系统之间是如何互动的，不过更重要的是，机构内的人员是如何互动的。

最后一环（三）

研究并记录这次事件。

与他人分享你学到的东西。作为一个共同体，我们只有积极分享我们所经历的网络安全问题的相关信息，才能做得更好。

飞机很安全，但这恰恰是因为每一次出现故障后都会展开详细的调查，并与其他航空公司共享相关详细信息，而且各航空公司都会制定相关的行动计划，无论最初出现的问题影响的是哪家公司。

与他人分享你学到的东西，你就为共同体内部的其他人提供了一次学习的机会，互联网也会因此变得更安全，更适合人们社交和经商。

FIRST.Org能做什么？

我们的宗旨

全球协调：出现紧急状况时，你总能在我们的全球社区找到你需要的支持团队。

全球语言：全世界的事件响应工作者有着同一种语言，了解彼此的意图和方法。

自动化：无聊的计算让机器去完成，这样人才能专注思考更困难的问题。

政策与治理：确保别人了解我们是做什么的，让他们帮助我们，而不是限制我们。

FIRST.Org能做什么？

全球协调：每个FIRST都可以在危机发生时找到另一个FIRST成员与之合作，这个合作者可以来自其他国家，其他行业。

FIRST组织了四次研讨会、11次技术座谈会、11次培训（其中四次安排在世界各地的FIRST活动期间）这些活动不仅是交流想法、交换技能的好机会，也是培养信任，认识同行的机会。志愿者对我们的各项活动和培训至关重要，我们欢迎所有对此感兴趣的朋友联系我们了解详情。

全球语言：FIRST团队知道，其他FIRST团队是靠得住的。所有FIRST成员对方法和问题有着共同的理解。

我们致力于确保FIRST成员具备最基本的能力，值得其他FIRST成员信任。我们会投资举办培训和教育活动，确保开展有效、全面的知识共享，并对所有成员一视同仁。

FIRST.Org能做什么？

自动化：FIRST成员间彼此信任，具有一整套工具可用于自动共享。

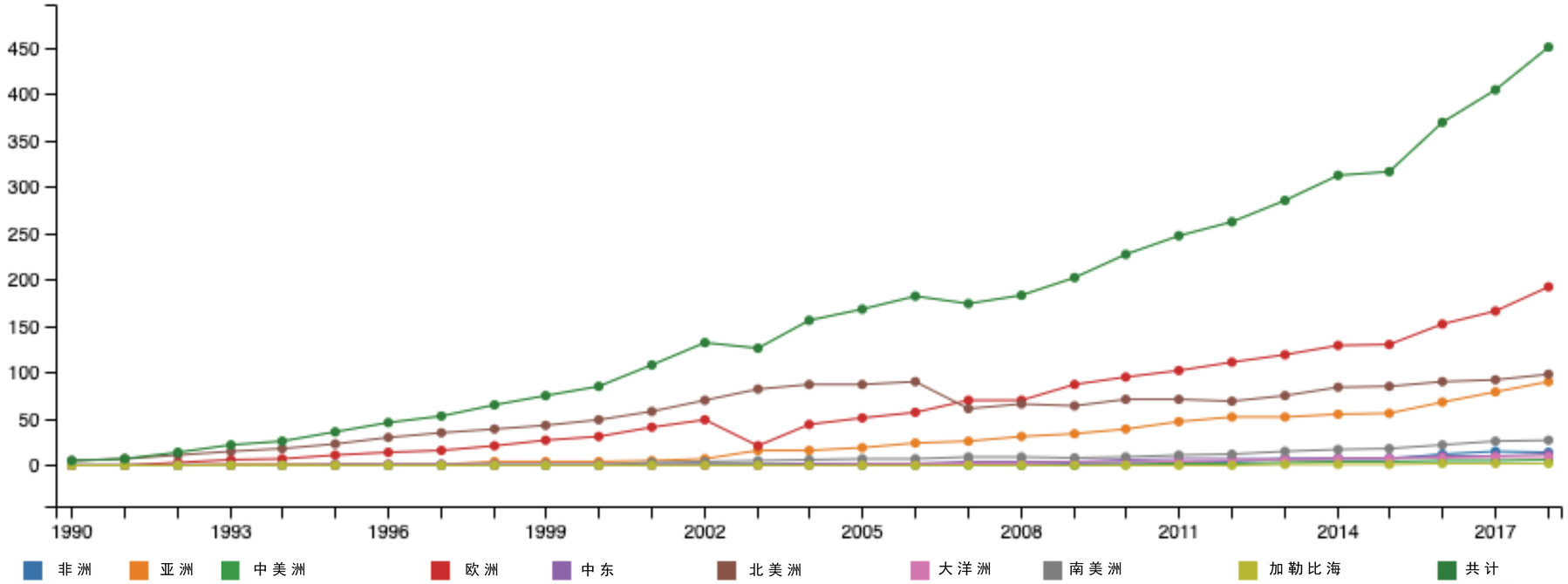
为促进协同，FIRST 支持其成员开发共享工具和标准，以便以高效、可靠的方式共享信息。

政策与治理：FIRST可以在有助于实现其宗旨的良好环境下工作。

作为互联网技术社区的成员，FIRST一直与政策制定者和互联网治理机构共同努力，在适当时候提供技术支持。FIRST并不直接参与制定政策，我们会参与各种技术讨论，而这些讨论有助于更大范围的互联网治理问题的讨论。而且，我们还设法教育政策制定者和其他利益相关者社区，让他们了解事件响应领域面临的挑战。

FIRST.Org能做什么？

FIRST 成员年增长*



谢谢！