2017 中国互联网安全大会
China Internet Security Conference

勇敢的面对网络威胁

Koichiro Sparky Komiyama

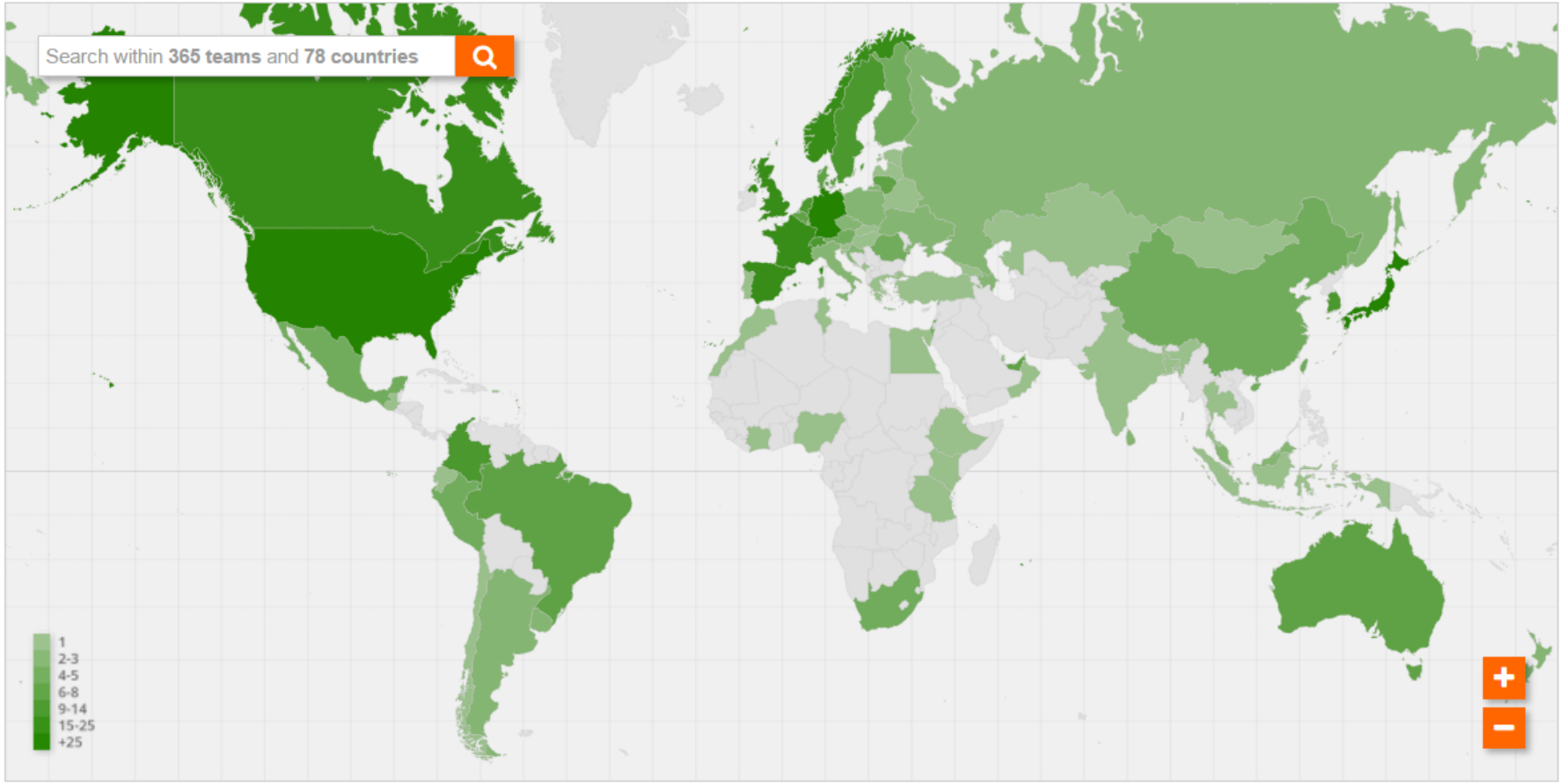
FIRST 董事
JPCERT/CC 副主任

关于 FIRST
事件响应与安全组织论坛

- 将事件响应和安全小组结合到一起的协会。提供最佳实践、工具和与成员小组的可信赖沟通。
- 是第一个事件响应论坛，创立于 1989 年，在第一个 CERT （为了应对 Morris 互联网蠕虫）成立之后成立。
- 加入该协会使事件响应小组能够更有效地应对安全事件。

FIRST – 一个全球社区

Members around the world



FIRST follows the International Olympic Committee (IOC) country name listings.

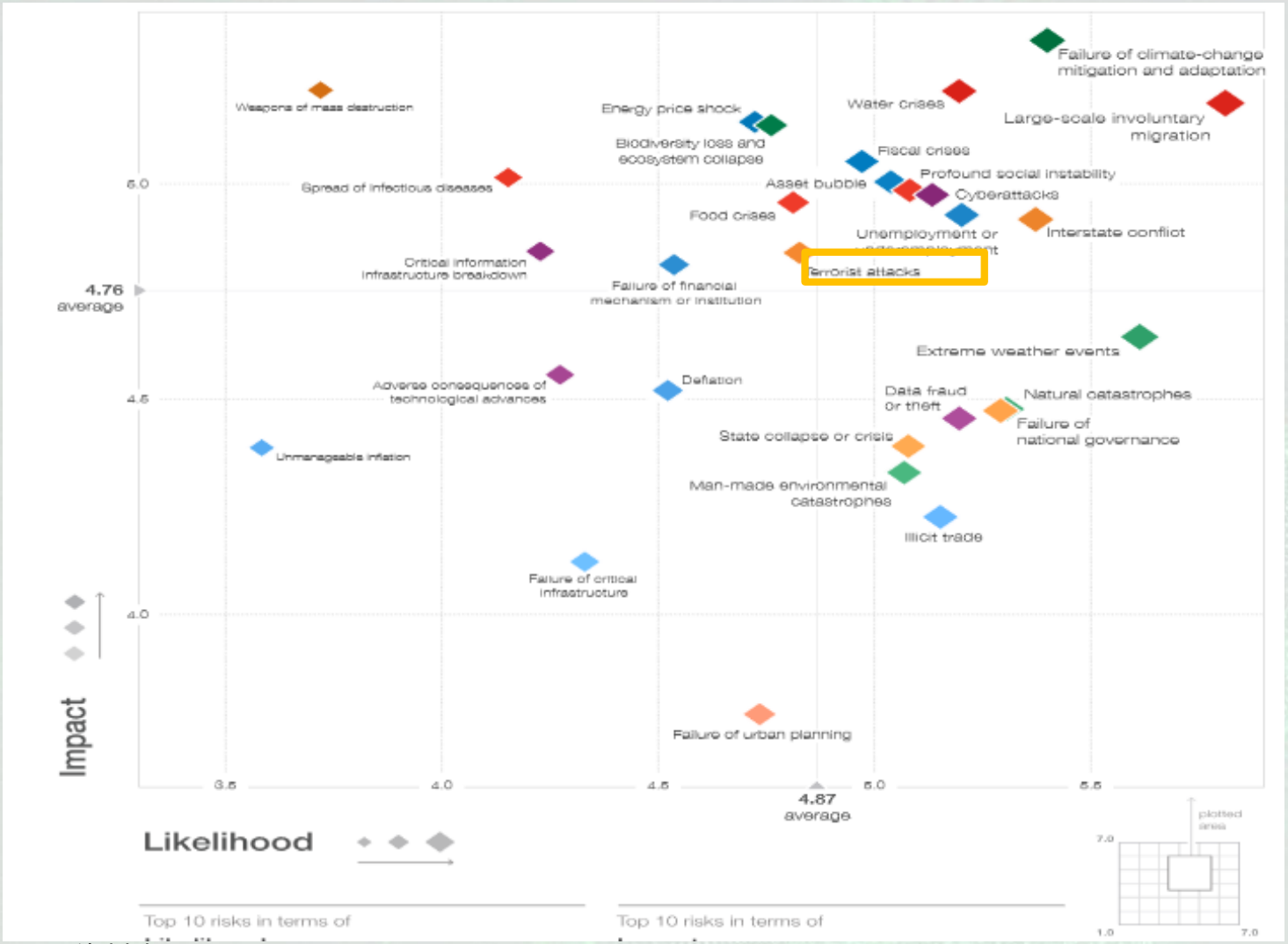
[credits]

FIRST 董事会

FIRST SC 成员由协会在年度大会上选出，任期为两年。每年将重新选举一半的董事会成员。

- Thomas Schreck，西门子，德国（主席）
- Damir (Gaus) Rajnovic，松下公司，英国（首席财务官）
- Margrete Raaum，Statnett，挪威
- Maarten Van Horenbeeck，Fastly, Inc.，美国
- Adli Wahid，APNIC，澳大利亚
- Derrick Scholl，Juniper，美国
- L. Aaron Kaplan，CERT.at，奥地利
- Koichiro Komiyama，JPCERT/CC，日本
- Serge Droz，OpenSystems，瑞士
- Katherine Gagnon，世界银行，西班牙

为什么网络安全是一个复杂的政策问题？



资料来源 http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf

日本的现状

- 过去 **4** 年里，JPCERT/CC 协调了 **30,000** 起网络安全案例。**14,000** 起案例来自日本以外，需要与 **98** 个经济体协调。
- 当前**排名前十**的国家和地区是美国、中国、德国、法国、中国台湾、俄罗斯、波兰、荷兰、巴西和土耳其。

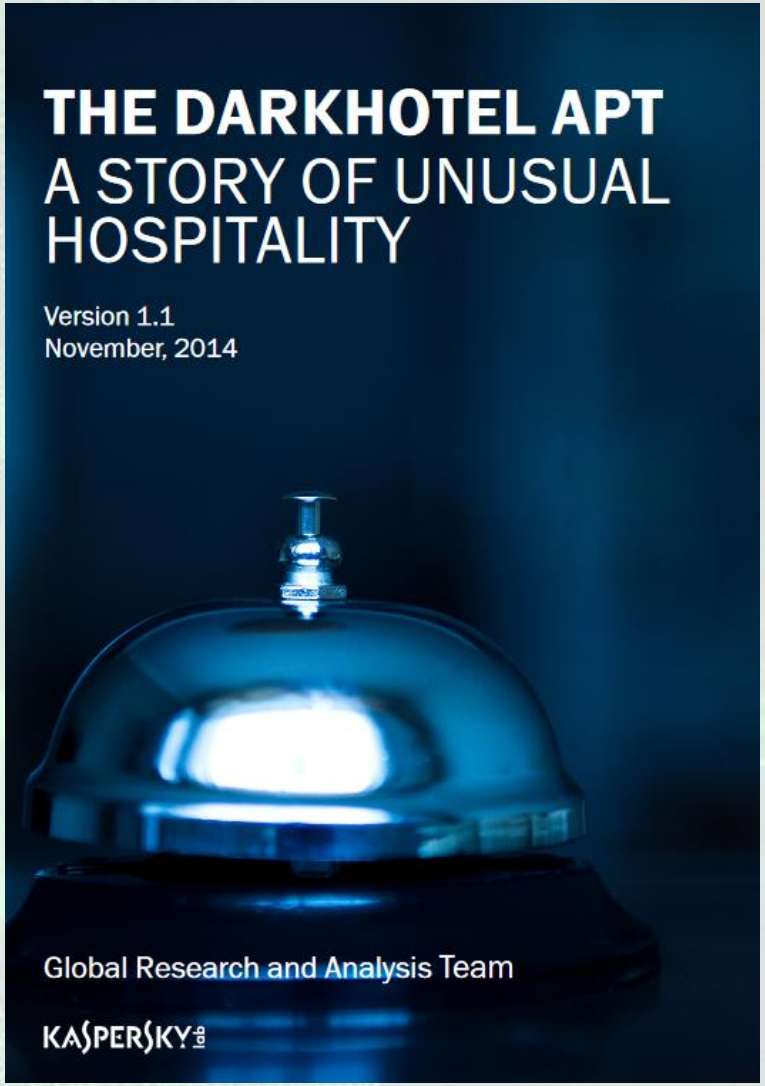
酒店行业

a Hilton Hotel Photograph by Roberto Machado Noa—LightRocket/Getty Images

HILTON

Hilton is the Latest Hotel Chain to Confirm a Data Breach

Robert Hackett
Nov 25, 2015

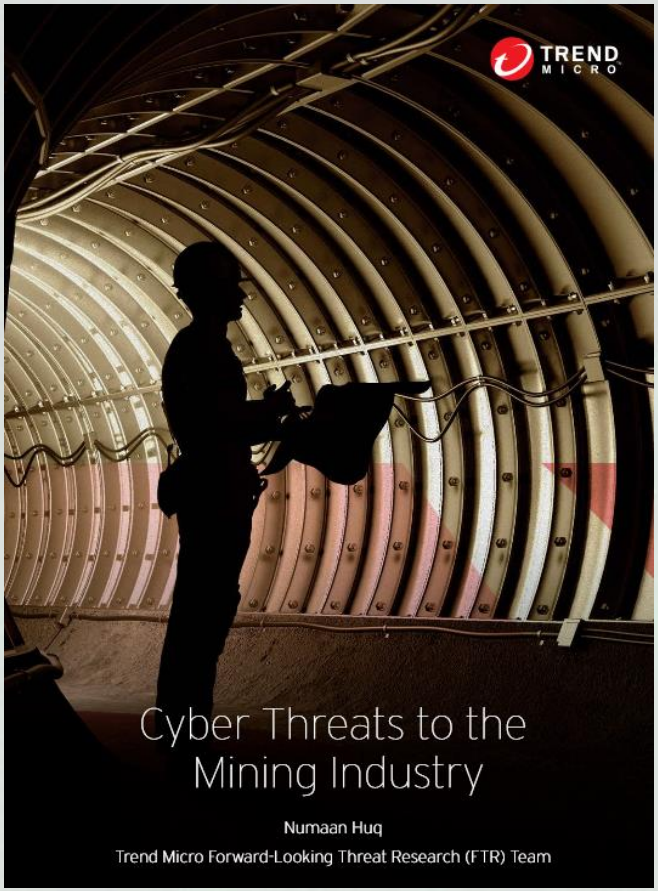


Here's How The CIA Allegedly Hacked Samsung Smart TVs -- And How To Protect Yourself

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms. FULL BIO

采矿业



Date	Victim(s)	Description
February 2015	Nautilus Minerals and Marine Assets Corporation	Canada's Nautilus Minerals and Dubai-based marine solutions company Marine Assets Corporation (MAC) were victims of a cyber scam that resulted in Nautilus paying a $10-million deposit intended for MAC into an unknown bank account.[60]
April & May 2015	Detour Gold Corp.	Canadian gold mining company, Detour Gold Corp. was hacked by a group that calls themselves the Angels_Of_Truth. 100GBs+ worth of data was stolen from the Detour Gold networks. 18GBs of compromised documents were shared on a torrent site.[61, 62]
June 2015	Codan	Australian communications, metal detection, and mining technology firm Codan reported sales and prices of the firm's metal detectors have collapsed after hackers stole its designs and began manufacturing counterfeit metal detectors.[63]
November 2015	International Mineral Resources	International Mineral Resources (IMR) filed a lawsuit claiming rivals EuroChem Volga-Kaily hired New York City law firm Salisbury & Ryan to dig up information on IMR after a mining business deal went bad. Salisbury & Ryan allegedly hired a former Soviet military counter intelligence officer to conduct a hacking campaign against IMR.[64]
February 2016	The New South Wales Department of Industry, Resources and Energy	Hackers targeted the New South Wales Department of Industry, Resources and Energy. They unsuccessfully attempted to access confidential information related to mining approvals.[65,66]
February 2016	Ukrainian mining company	BlackEnergy and another APT campaign, Sandworm, were discovered as the likely perpetrators behind outages at two power generation facilities in Ukraine in December 2015. BlackEnergy and KillDisk were discovered in attempted similar cyber attacks against a mining company and a large railway operator also in Ukraine.[67]
April 2016	Goldcorp	The Canadian gold-mining firm Goldcorp suffered a major data breach. The hackers leaked 14.8GBs of data online by publishing a document on Pastebin with a URL address to a full torrent download. The archive includes employee PII and financial data.[68]

当然，还有金融领域

TECHNOLOGY NEWS | Thu May 19, 2016 | 1:57pm EDT

Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat

为什么网络安全是一个复杂的政策问题？

由于担心会出现攻击性网络能力，各国需要保护其社会安全，这个问题随之变得越来越复杂。

为什么小组要加入 FIRST

获得全球安全专家社区的支持

- 小组专业知识帮助更有效地对事件作出响应
- 快速、全球性的信息交流与合作
- 与来自全球各行各业的安全专家建立可信赖联系

从可信赖论坛中受益

- 国际性的可信赖论坛有助于安全小组之间的互动
- FIRST 的基础设施可帮助在成员之间安全地共享信息
- 我们齐心协力解决安全问题

加入 FIRST 的额外权益

专题讨论会和技术研讨会

- 全年在全球各地举办各种区域活动
- 专属讨论论坛
- 面向 FIRST 成员小组的培训

最佳实践、展示和播客

- 与同行合作
- 交换想法和最佳实践
- 为您的团队下载资源

沟通与讨论列表

- 与安全事件有关的洞察
- 学习和分享经验
- 多种渠道 – 电子邮件、IRC

近期活动

FIRST 亚太地区专题讨论会，台中市，9 月 9-11 日 – 由 APNIC 主办

蒙得维的亚技术研讨会，9 月 18 日 – 由 LACNIC 主办

巴厘岛技术研讨会，9 月 28-29 日 – 由 ID-SIRTII/CC 主办

布加勒斯特 2017 年 FIRST 技术研讨会，10 月 16-19 日 – 由 Dell SecureWorks 主办

CS3/FIRST ICS 安全会议 – 斯德哥尔摩，10 月 24-26 日 – 由 CS3 主办

UNDP 2017 技术研讨会 – 波德戈里察，ME，11 月 7-9 日 – 由 UNDP 主办

奥斯陆 2017 年 FIRST 技术研讨会和 TRANSITS 培训，11 月 28-30 日— 由 Telenor CERT 和 KraftCERT 主办

毛里求斯 2017 年技术研讨会与培训，11 月 30 日 - 12 月 1 日 – 由 CERT-MU 主办

拉斯维加斯 2017 年 FIRST 技术研讨会，12 月 5-6 日 – 由 Sands CERT 主办

无边界网络和技术研讨会，布拉格，12 月 6-7 日 – 由 FIRST 和 OASIS 主办

第 30 届 FIRST 年会之计算机安全事件处理，2018 年 6 月 – 吉隆坡

请访问 http://www.first.org/events/first 查看我们的活动

FIRST 年会

该会议提供了一个论坛，让大家汇聚一堂，分享目标、想法、信息以及对如何改善全球计算机安全的看法。这个为期五天的会议包括：

- 学习事件管理方面最新的安全策略
- 增长安全问题与解决方案方面的知识和技术洞察
- 了解最新的事件响应和预防技术
- 增加网络漏洞分析方面的洞察
- 聆听行业专家如何管理安全问题
- 与来自全球各地的同仁交流互动，交换事件响应方面的想法和建议
- 赢取 26 个 CPE 学分，获取专业证书
- 将影响扩展到我们全球受众的赞助机会

参会人员

- 决定安全产品需求和实施解决方案的**技术人员**
- 承担整体安全职责的**政策和决策者**
- 从事网络犯罪调查的**执法人员**
- 与政策和决策者共同确立安全政策的**法律顾问**
- 直接负责保护基础设施的**高级管理人员**
- 负责保护系统和关键基础设施的**政府管理者和高管**

工作组

就特定主题和问题进行合作的，规模更小、联系更紧密的工作组

工作组包括：

- **标准制定**：通用漏洞评分系统 (CVSS-SIG) 和 Passive DNS (pDNS)
- 互联网基础设施供应商（供应商 SIG）
- 指标 SIG
- 僵尸网络 SIG
- VRDX SIG （漏洞报告和数据交换）
- ACAN BoF （学术和 NREN BoF）
- 能源 BoF

工作组

就特定主题和问题进行合作的，规模更小、联系更紧密的工作组

标准组：

- 通用漏洞评分系统 (CVSS-SIG)
- Passive DNS (pDNS)
- 红绿灯协议 (TLP-SIG)

工作组：

- 互联网基础设施供应商（供应商）
- 能源 SIG
- 僵尸网络 SIG
- VRDX SIG （漏洞报告和数据交换）

讨论组：

- 互联网基础设施供应商
- 恶意软件分析
- 指标
- 僵尸网络规避和修复
- ACAN （学术和 NREN）

FIRS 教育计划

- FIRST 为全球计算机安全事件响应组 (CSIRT) 制定教育课程框架
- 根据 CSIRT 服务框架与全球安全社区进行通力合作

– CSIRT 参与者来自 6 大洲 15 个国家和地区的国家机构和教育社区

- 自启动以来，FIRST 已经主办了 3 场教育峰会
- 更多信息：https://www.first.org/global/education

FIRST 培训活动

FIRST 坚持在教育和培训方面的合作

- 邀请主题专家在 FIRST 会议上进行培训
- 与 ISC^2 在 2013 年能源研讨会上合作进行取证培训
- 制定 FIRST 培训内容和材料

培训通常在 FIRST 活动中进行，或者与 AfricaCERT 等区域合作伙伴合作开展（例如 2017 年 5 月的培训）

申请成为 FIRST 成员

- **小组**成员和**联络**成员
- FIRST 要求小组在成为成员之前到现场参观以评估 CSIRT 容量
- 小组可免费使用文档，将其用于自我评估 https://www.first.org/membership/site-visit-v2.5.pdf

- 容量很**重要**
  - 使小组能够成功地互操作
  - 确保通用词汇和理解
  - 确保提供最低数量的工具

- 更多信息：https://www.first.org/membership

FIRST 成员申请流程

FIRST 成员申请

1. 申请人确定两个 FIRST 正式成员为其申请担保。
2. 申请人填写成员申请表，可在 www.first.org 上找到。
3. 写一份申请书，说明想加入 FIRST，并列出您能够带给组织的好处。
4. 其中一位担保人必须进行现场参观并提交一份报告。
5. 两位担保人都要写一封信，介绍并推荐申请小组成为 FIRST 正式成员。
6. 担保人还必须签署申请小组代表 PGP 密钥和小组密钥。
7. 两位担保人将整个申请文件包提交给 FIRST。
8. FIRST 审核申请并提交给 FIRST 会员委员会 (MC) 审核和审批。如果有问题，MC 会与您的小组联系。
9. 整个申请将公示出来，听取 FIRST 成员反馈，FIRST 指导委员会拥有最终审批权。一旦申请成功，您将会收到董事会主席的通知和会费发票 – ***800 美元申请费和 2,000 美元的 2017 年年费。***

总结

- **全球合作对于有效响应至关重要**

- **需要三种级别的合作：**
  1. 信任和社区
  2. 教育
  3. 技术数据共享

- **FIRST 的计划**
  1. 扩大 CSIRT 小组的全球社区
  2. 推动教育培训工作
  3. 通过标准促进分享和沟通

如欲了解更多信息，请联系

www.first.org

Koichiro Sparky Komiyama
koichiro.komiyama@first.org

FIRST Secretariat
first-sec@first.org

谢 谢