Annual Report 2018-2019

Thomas Schreck, Chair

Forum of Incident Response & Security Teams

Board Members

Serge Droz
Javier Berciano
Alexander Jaeger
Dave Schwartzburg
Derrick Scholl
Damir 'Gaus' Rajnovic
Margrete Raaum
Maarten Van Horenbeeck
Adli Wahid

FIRST Annual Report 2018-2019

Dear Reader,

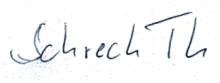
Welcome to the third Annual Report of the Forum of Incident Response and Security Teams. This report provides a short summary of the activities of FIRST during the last year. The report covers the time between our Annual Conference in Kuala Lumpur, in June of 2018, through our conference in Edinburgh, June of 2019.

FIRST made significant progress towards our goals in 2018-2019, growing our membership to over 480 teams in 92 countries. In terms of creating maturity in specific technical areas, we released several new trainings, including a technical training focused on DDoS mitigation, and released materials around how to mature Product Security Incident Response Teams.

This year, I am reaching my term limit and will be stepping down as Chair. It has been a pleasure working with the entire FIRST community and helping our organization further its goals.

The entire Board of Directors is deeply appreciative of the support we get from our members, sponsors, grantors, and the wider security and incident response communities throughout the year. Thank you for your support, and we look forward to continuing to partner with you in the future to further and mature cybersecurity incident response maturity around the world.

Best regards,



Thomas Schreck
Chair, Forum of Incident Response and Security Teams

Table of contents

Organizational goals **3**

Major announcements and press **4**

Organizational updates **5**

Membership 5
Events 7
Training and Education 8
Special Interest Groups 9
Standards 10
Internet Governance and Policy 11
Financials 12
Infrastructure 13

Organizational goals

During the last year, FIRST has continued to work along the line of four main principles:

1. During an incident, it is important that incident response teams have immediate contacts at their counterparts in the world, whether they manage the network where the attack originates, or support software, devices or systems which help defend against the attack. **We grow our membership to enable these relationships.**
2. We ensure member teams have a similar understanding of the incident response world, enabling them to quickly build trust and cooperation across organizational, municipal and national boundaries. **We develop and maintain a services framework that defines typical CSIRT services – developing and providing training, and enabling working groups where teams can work together on complex problems.**
3. We help teams automate where possible, enabling computers to do the heavy lifting, while human talent is inspired to solve the hard problems. **We develop standards, provide guidance on information sharing, and enable teams to share strategies and brainstorm at events.**
4. We educate other communities about the work that FIRST and its members do to make the world a place that is conducive to a global, effective incident response community. **We participate in policy forums, and educate participants on incident response and our community.**

A large focus of work conducted in 2018-2019 was to continue ensuring our organization grows in maturity. We brought in a new attorney, a new accounting firm and a new public relations firm. We also retained an additional specialized attorney specifically to help us work through issues involved in our international growth. Additionally, we launched additional trainings and a Hall of Fame to help drive recognition and awareness of those who have contributed significantly to the Incident Response discipline.

Last, but definitely not least, FIRST also hired an Executive Director. Chris Gibson, a former Chair and Board Member of the organization, is joining us in a full-time capacity to help build out our operational capability. Working closely with our Chair, Board and professional staff, he will work to implement the Board's strategy.

Chris brings with him over 15 years leadership experience and knowledge of the cyber security industry. He is well versed in FIRST's mission having spent nearly ten years on the Board of FIRST, five years as Chief Financial Officer and two as Board Chair. He joins FIRST from Orwell Group where he was Chief Information Security Officer. Chris also built and ran CERT-UK, the UK's first national Computer Emergency Response Team within the UK Government's Cabinet Office.

Chris Gibson, Executive Director of FIRST, 2019

Major announcements and press

During the last year, FIRST made the following major announcements:

- On May 22nd, 2019, we announced the new Product Security Incident Response Team (PSIRT) and Cyber Insurance SIGs;
- On May 17th, 2019, we announced hiring Chris Gibson as FIRST's first Executive Director;
- On March 5th, 2019, FIRST released its DDoS mitigation training course;
- On December 6th, 2018, FIRST announced the Incident Response Hall of Fame, a new recognition for visionaries and leaders in Incident Response;
- On September 22nd, 2018, FIRST published an address to the Global Commission on the Stability of Cyberspace covering the needs of the Incident Response community on global cybersecurity norms;
- On June 21st, 2018, FIRST released training to help companies respond to product vulnerabilities.

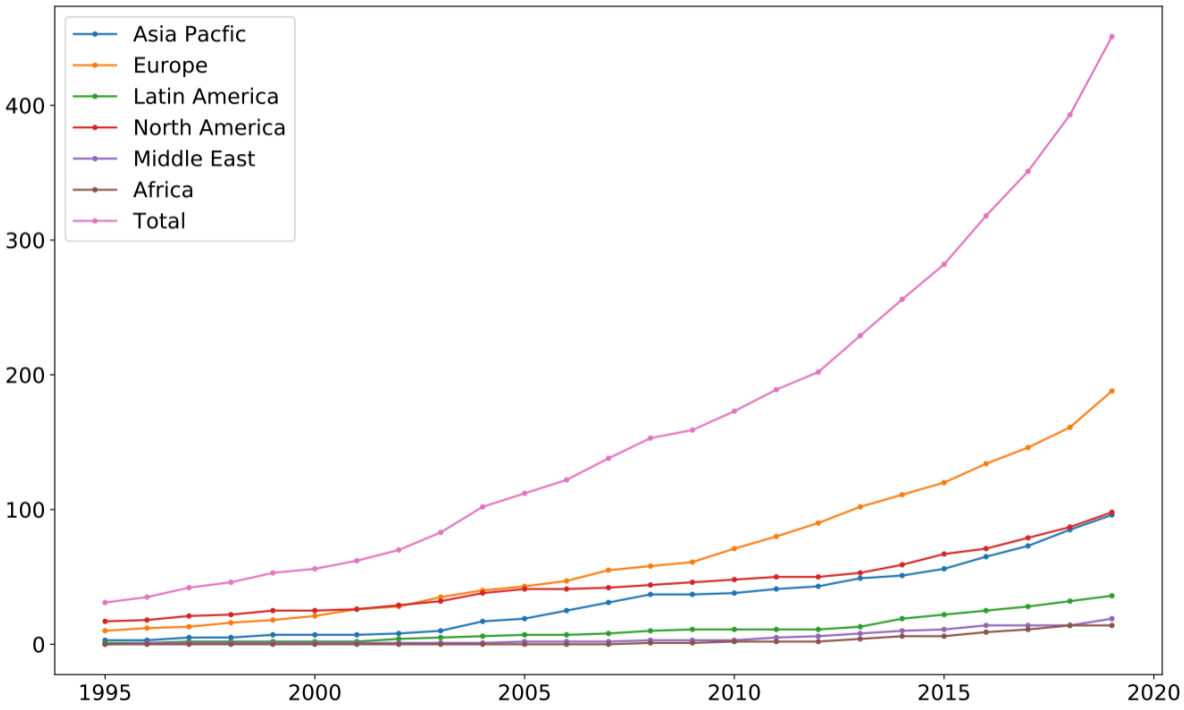
FIRST was highlighted in several media articles over the last year:

- Board member Maarten Van Horenbeeck was published in High Growth Scotland, sharing guidance for corporations on how to best prepare for data breaches.
- May 1st of 2019, Digital Guardian named FIRST one of the "top Infosec Networking groups to join."
- January 3rd, 2019, Tripwire named the FIRST conference one of the "top information security conferences of 2019."

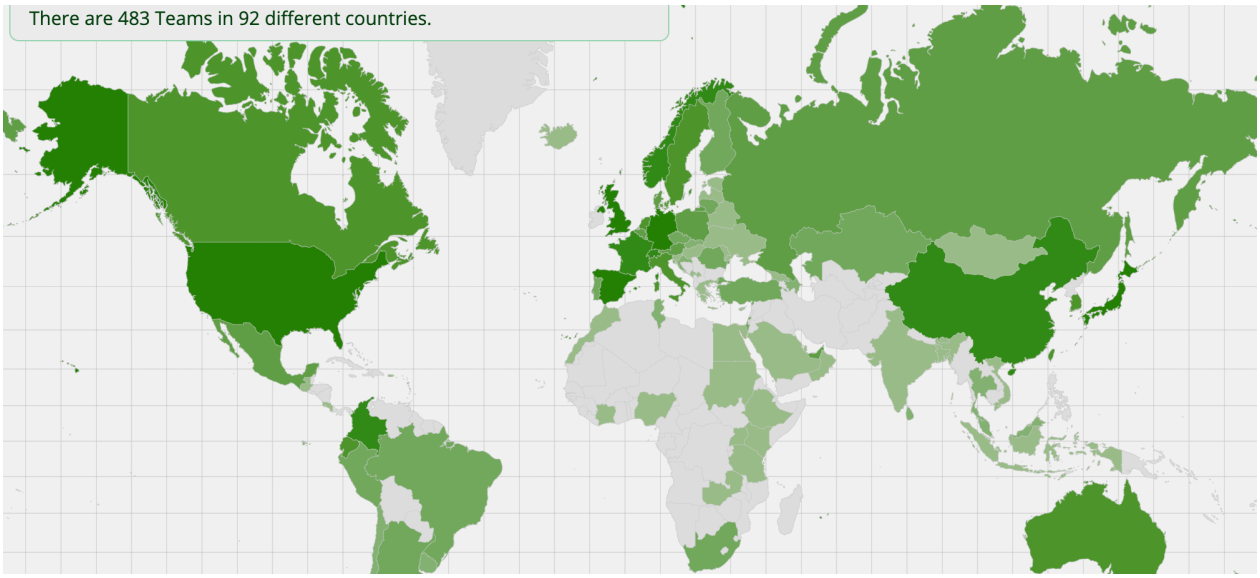
Finally, various outlets, including Digital News Asia, Malaysia's The Star, ASEAN Tech & Sec and Cybersecurity ASEAN wrote articles about the FIRST conference which took place in Kuala Lumpur in 2018.

Organizational updates

Membership



FIRST saw healthy growth in 2018-2019, with over 480 member teams by the 2019 annual conference. Membership grew mostly in Europe and Asia. FIRST membership is also increasingly becoming international – we now have members in a total of 92 countries, compared to 86 last year.



As Internet use grows across the world, there is an increased need to bring incident response teams from developing economies into our community. We continue to challenge ourselves to have all countries and industries represented within FIRST.

The **Suguru Yamaguchi Fellowship Program** helps us towards this goal by enabling teams to join our community more readily. In 2016, four teams from Bangladesh, Myanmar, Cote d'Ivoire, and Ghana participated in the program while in 2017, teams from Vietnam, Panama, Ecuador and Moldova joined. In 2018, we welcomed representatives from Tonga and Costa Rica. The full roster of Fellowship teams is now 13 teams, though three teams have dropped from the program. So far, three have joined as full members.

Read more about our membership at https://www.first.org/members.

Suguru Yamaguchi Fellowship Program participants and Board Members, Kuala Lumpur Conference 2018

Events

FIRST activity across the world: Training classes TC's Symposia Annual conference 2019

FIRST organized 4 Symposia, 11 Technical Colloquia and 11 trainings (4 taking place during an existing FIRST event around the world). These events are opportunities not only to exchange ideas and know-how, but also to grow trust and meet peers. Our events and training sessions would not be possible without volunteers, and we invite interested parties to contact us about opportunities to contribute.

Read more about our events at https://www.first.org/events/first.

Training and Education

FIRST has recognized “Training and Education” as one of its key priorities. By increasing educational opportunities available to our members, we can truly help make the incident response community more effective.

In 2018-2019 FIRST volunteers continued development of our services framework. The PSIRT group not only put the finishing touches on a services framework for Product Security Incident Response, but it also published an easy to read “PSIRT maturity” document, accompanied by a series of blogs. Making formal standards accessible in an easy-to-use way helps teams get started. The CSIRT Services framework was also updated to fill gaps and to align it with its PSIRT counterpart. An interim version 1.1.1 has been published, fixing some minor issues while the final version 2.0 of the document is being prepared.

The popularity of services frameworks has exceeded our expectations. Several organizations, such as the ITU, use them as the basis for their capacity building programs.

Early 2019, we released our latest training course: DDoS Mitigation Fundamentals. The course quickly has become popular and has been taught a number of times in locations around the world. FIRST trainers delivered a number of courses at various locations, attracting ever more students, in both English and Spanish. The training courses not only build capacity but also form a platform to welcome new teams into FIRST. As has been the case historically, FIRST releases all of its training materials under a Creative Commons license, to maximize their usefulness. FIRST is happy to deliver exclusive Incident Response trainings to ITU members at their Cyber Drills.

We have also contributed to third party training development. Board member Serge Droz participated in a GEANT Training materials retreat to help facilitate the update of the existing TRANSITs materials with a view towards moving them to be open source in the future.

FIRST is happy to see its course “Incident Response for Policymakers” become more popular. During this reporting period it was taught at the 2018 Meridian conference, as well as to members of the NATO Cooperative Cyber Defence Centre of Excellence and diplomatic staff in Tallinn, and in Lima, Peru.

Read more about our training and education program at https://www.first.org/education.

56th TF-CSIRT meeting & FIRST Regional Symposium Europe in Tallinn, Estonia, January 2019

Special Interest Groups (SIG)

FIRST organizes Special Interest Groups by request of membership, and provides them with support, such as web site infrastructure, a conference bridge, a Program Manager, and meeting space at our events.

During the year, the following new SIGs were implemented:

- **Product Security Incident Response Teams** – The PSIRT SIG is developing learning materials to support evolution of PSIRTs at all maturity levels;
- **Cyber Insurance** – This new SIG will coordinate data sharing and provide a feedback mechanism between CSIRTs and cyber insurance organizations.

Several SIGs published work efforts during the year, including the PSIRT SIG, which published a PSIRT maturity document.

Most SIGs held face to face meetings during the 2018 FIRST conference and the same is scheduled for the 2019 FIRST conference. This is an important opportunity for those working in the SIGs, and it is also a chance for attendees at the conference to collaborate with those groups.

Read more about our Special Interest Groups at https://www.first.org/global/sigs.

FIRST SIG Planning Checklist

The SIG checklist is required for any proposed new SIG. Please complete and submit this form to the FIRST Secretariat at first-sec@first.org.

Proposed Charter for: [Special Interests Group Name]

Submitted By: [Name] **Date:** [Day Month, Year]

Mission (required)
Briefly state the reason for chartering this subgroup in general terms (what problem are you trying to solve)?

Goals & Deliverables
Describe the goals and deliverables of what you hope to accomplish in the next year (please explain if a longer approach is needed).

Initial Chairperson(s) and Members
Chairperson(s) and Team Affiliation (needs to be a FIRST member or liaison)

Please list anyone that has already shown interest in participating and their email. The Secretariat will also assist with a call for participants to the teams list once the SIG is approved.

Ever considered launching your own SIG? Find our SIG template at first.org/global/sigs!

Standards

FIRST supports the development of standards and maintains several cybersecurity standards:

- **ISO 29147 "Vulnerability disclosure"**: This standard was updated and the new revision was published in 2018. ISO has made this updated standard freely available for download as it did with the previous version from 2014.
- **ISO 30111 "Vulnerability handling process"**: The second revision of this standard is being finalized and should be published in 2019.
- The **Common Vulnerability Scoring System (CVSS)**: develops and maintains the CVSS standard, a robust and useful scoring system for IT vulnerabilities that allows organizations to prioritize them across their networks. CVSSv3 has also been published as an ITU recommendation in X.1521:2016. FIRST released an interactive training “Mastering CVSSv3” through our learning platform.
- The **Traffic Light Protocol (TLP)**, a set of designations used to ensure a common expectation in audience for (non-automated) iterative sharing of sensitive information between entities. The initial version of this standard, building on the original TLP, was released in September of 2016.
- The **Information Exchange Policy (IEP)**, a framework for defining information exchange policy, and a set of common definitions for the most common sharing restrictions. It addresses information exchange challenges and promotes information exchange more broadly, primarily for machine automated communications. The first version of the standard was released in September of 2016.
- **Passive DNS exchange:** a common output format for Passive DNS servers. Released in 2015, this standard is made available as part of an IETF RFC, and is seeing continued development within the FIRST community.

In addition, FIRST continues to be represented as a sector member in the ITU as a standards body and is a Category C liaison to ISO. FIRST also signed a Memorandum of Understanding with standards organization OASIS to permit closer cooperation on threat intelligence specifications such as STIX and TAXII.

Read more about our Standards work at https://www.first.org/standards.

Internet Governance and Policy

As a member of the Internet Technical Community, FIRST continues engaging with policymakers and Internet governance bodies to provide technical expertise where appropriate. While FIRST does not engage in policymaking efforts, we do contribute to technical discussions contributing to the wider Internet governance debate. In particular, we educate policymakers and other stakeholder communities about the challenges of the Incident Response community.

During the last year:

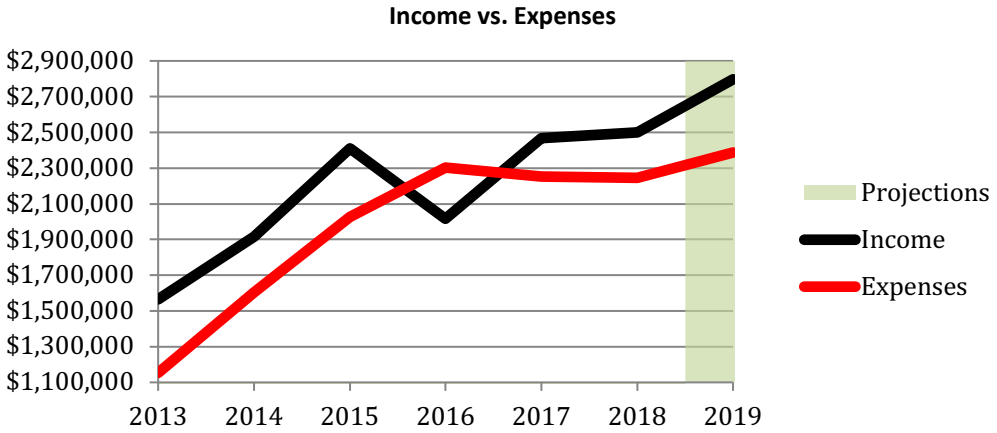
- Board member Serge Droz actively participated in the **World Economic Forum's Center for Cybersecurity** annual conference;
- Board members Maarten Van Horenbeeck and Serge Droz participated in the Swiss Governments "**Geneva Dialogue,**" a multi-stakeholder platform discussing the consequences of cyber norms;
- Board Member Serge Droz participated in two events organized by the **International Committee of the Red Cross** exploring the consequences and the possible need for changes in humanitarian law due to cyber operations;
- Board member Serge Droz represented FIRST at the **OECD Global Forum of Digital Security and Prosperity** as a follow up the Paris call. Board member Maarten Van Horenbeeck is contributing as Lead Expert to the **IGF's Best Practices Forum on Cybersecurity**, which is working to operationalize part of the Paris Call and other agreements by collecting best practices on areas of agreement within international cybersecurity.
- Board member Maarten Van Horenbeeck participated in a UNIDIR meeting on the value of **regional associations in cybersecurity**, and is further working to understand how we can contribute to international UN processes such as the OEWG and UNGGE, which are starting up this year.
- Board member Serge Droz was invited by the renowned Stockholm International Peace Research Institute (SIPRI) and the Swedish Civil protection Agency to participate in a high level workshop on "De-Escalation of Cyber incidents"

Read more about our Internet governance and policy work at https://www.first.org/global/governance.

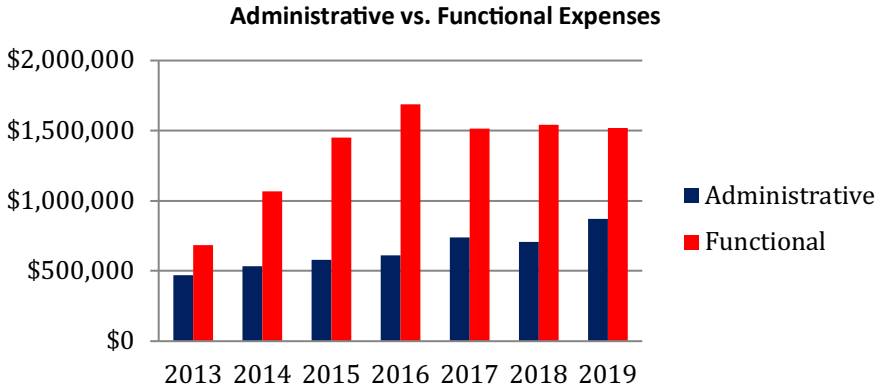
Serge Droz and Maarten Van Horenbeeck teaching the "Incident Response for Policymakers" course in Lima, Peru

Financials

In 2018 FIRST realized profit of around $166,000 in line with the budget predictions. As the organization grows and matures, our expenses are growing but, more importantly, our income is also growing, as shown in the graph below. Please note that the figures for 2019 are only predicted values.



Expenses are divided into two groups: administrative (running the organization) and functional (accomplishing the FIRST mission and vision). The graph below shows that most of our expenditures are toward furthering FIRST goals:



2018 was a year of changes with some having a direct impact on finances. While the introduction of AMS was aborted, we have to maintain $40,000 in reserves in case of a dispute with the AMS vendor. These reserves will have to be in place until 2021. We modified sponsorship packages for the Annual Conference and are expecting a record sponsorship income in 2019. Growing demands of FIRST, as an organization, led us to select a new CPA. Greg Brink, our former CPA, helped FIRST grow tremendously to where we are today. As of early 2019, CPA services are now delivered by CliftonLarsonAllen company (CLA).

FIRST is a financially sound organization and a 501c3 non-profit incorporated in North Carolina, USA. Detailed financial information is made available through our members portal or can be provided upon request to interested parties such as grantors and sponsors.

Infrastructure

During this year, FIRST continued to heavily invest in infrastructure to support our growth. The following significant changes were made as a result:

1) Significant effort has been committed to supporting FIRST's financial needs. We migrated our dues server payment processing from on-premise javascript to a hosted iFrame, reducing PCI complexity from SAQ-A-EP to SAQ-A. The plan moving forward will be to leverage FIRST's existing services of Bill.com or Quickbooks Online, or another payment processor, to best facilitate secure collection of dues.

We also completed our migration from Quickbooks enterprise desktop edition to Quickbooks Online. This streamlined the integration between Quickbooks and our FIRST database so we can better track member dues invoices and payments. This has helped to:

- Reduce costs to FIRST
- Eliminate the need to run a Windows VM
- Lay the groundwork for services to be used by FIRST's new financial services provider (CLA)

2) FIRST also deployed an interface for the FIRST Incident Response Hall of Fame (https://www.first.org/hof) which supported the nomination process of the candidates for the inaugural award. Volunteering with FIRST now is also supported by a directory of volunteers and contribution record features (https://www.first.org/volunteers).

3) The FIRST Technology team is also working on an Identity Project, which will help make FIRST services easier and more universally accessible:

- The tech team has refined requirements and criteria. An evaluation has been completed of open source and commercial SSO solutions with strong MFA to complement FIRST's existing user directory. A pilot is currently underway with Gluu & Casa (https://www.gluu.org).
- Successful outcome of the pilot will result in a rollout of improved SSO experience across FIRST's services, which would begin after the 2019 conference.

4) A subset of SIGs have been on-boarded into a pilot of SIG-specific channels within the FIRST Slack Workspace. The tech team has applied for a non-profit license for, and intends to deploy Mattermost due to Slack non-profit pricing being cost prohibitive for our size and intended use.

5) Several enhancements were made to the website and internal FIRST portal:

- New development has facilitated the CAPS team to better manage FIRST program content and agendas;
- Call for Papers: The Bangalore and PSIRT TCs were the FIRST events to adopt new CfP functionality;
- The capability to add speaker photos was added to FIRST event programs.

6) An agreement was reached with Tenable to provide FIRST with complimentary licensing for Tenable.sc. This will facilitate better securing FIRST's infrastructure. Deployment is still in progress.

7) The FIRST Bug Bounty Hall of Fame (https://www.first.org/about/bugs) was updated with 11 new entries. Some of the resulting improvements and fixes that were made as a result include:

- Cipher updates
- Removal of deprecated services
- DNS configuration (SPF)
- DoS / Brute force hardening

https://www.first.org
first-sec@first.org

Forum of Incident Response and Security Teams
PO Box 1187
Morrisville
North Carolina 27560-1187
United States of America