Annual Report 2017-2018

Thomas Schreck, Chair

Serge Droz
Kate Gagnon
Aaron Kaplan
Koichiro Komiyama
Derrick Scholl
Damir ‘Gaus’ Rajnovic
Margrete Raaum
Maarten Van Horenbeeck
Adli Wahid

FIRST Annual Report 2017-2018

Dear reader,

This is the second year that the Forum of Incident Response and Security Teams (FIRST) publishes an annual report. Our Annual Reports provide a short summary of the activities of FIRST during the last year. The report covers the time between our Annual Conference in Puerto Rico, in June 2017, through our conference in Kuala Lumpur, June 2018.

FIRST made significant progress towards our goals in 2018, growing our membership to 86 countries. For the first time, we also organized a non-technical training aimed at policymakers and conducted it successfully during the Internet Governance Forum in Geneva. We also formalized a new Standards Development process, that will make it easier for our community to develop information security standards that are widely accepted across the world.

We appreciate your ongoing support as a member, event attendee, sponsor or grantor, and look forward to our ongoing cooperation during the next year. Thank you for being a part of our global community!

Best regards,

Thomas Schreck
Chair, Forum of Incident Response and Security Teams

Table of contents

Organizational goals

During the last year, FIRST has worked along the line of four main principles:

- 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.**
- We ensure member teams have a similar understanding of the incident response world, enabling them to quickly build trust and cooperation across organizational 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 hard problems.**
- 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 information and brainstorm at events.**
- We educate other communities about the work that FIRST and its members do, to make the world a place that's conducive to a global, effective incident response community. **We participate in policy forums and educate them on incident response and our community.**

A large focus of work conducted in 2017-2018 was ensuring our organization continues to grow in maturity. We engaged an outside consultant to help us understand the strengths and weaknesses, opportunities and threats ahead for FIRST. This is helping us develop a longer term view for our organization.

The FIRST Board of Directors during a Board meeting in Montreal, Canada

Major announcements and press

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

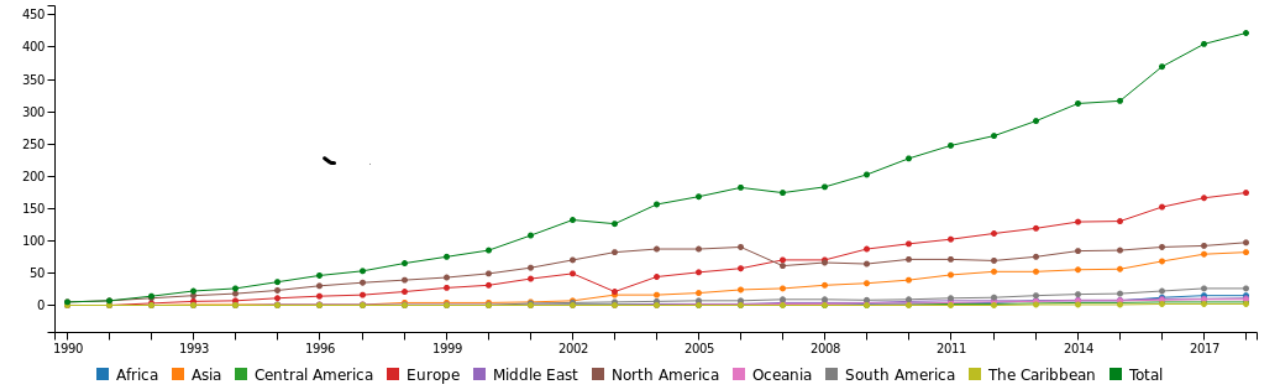
- In May 2018, FIRST announced having received a grant from the Australian Department of Foreign Affairs and Trade (DFAT) for a CSIRT project, consisting of a training and a regional event, focused on the Pacific Island countries
- On March 28th, 2018, FIRST launched a "Welcome kit", a document provided to new members that helps them understand the resources available to them as part of FIRST membership
- On December 18th, 2017, FIRST partnered with civil society organization Access Now to jointly organize a panel on "*critical issues in cyber security incident response*" during the Internet Governance Forum in Geneva
- On November 19th, 2017, we announced the FIRST and OASIS Borderless Cyber Conference and Technical Symposium at the Prague Marriott hotel
- On November 8th, 2017, we announced the release of our Incident Response training for Policymakers
- On August 15th, 2017, we announced the release of our FIRST Policy for Standards Development, a document to help standardize the development of standards within the FIRST community
- On July 24th, 2017, FIRST released its first Annual Report
- On July 11th, 2017, FIRST signed an agreement with APNIC to improve incident response capability in Asia Pacific, by enabling both organizations to benefit from each other's programs supporting CSIRT in the Asia Pacific region
- On July 6th, 2017, FIRST released the *Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure*, a set of guidelines and norms for vulnerability disclosure affecting multiple parties.

FIRST was highlighted in several media articles over the last year. Chair Thomas Schreck and Member Trey Darley published an article in Infosecurity Magazine on the value of Threat Intelligence sharing. Damir 'Gaus' Rajnovic was interviewed by Global Partners Digital on multi-stakeholder approaches to cybersecurity. HostingAdvice, a site focused on the challenges of web hosters and their clients, wrote a detailed article about the operations of our organization and how we contribute to global information security.

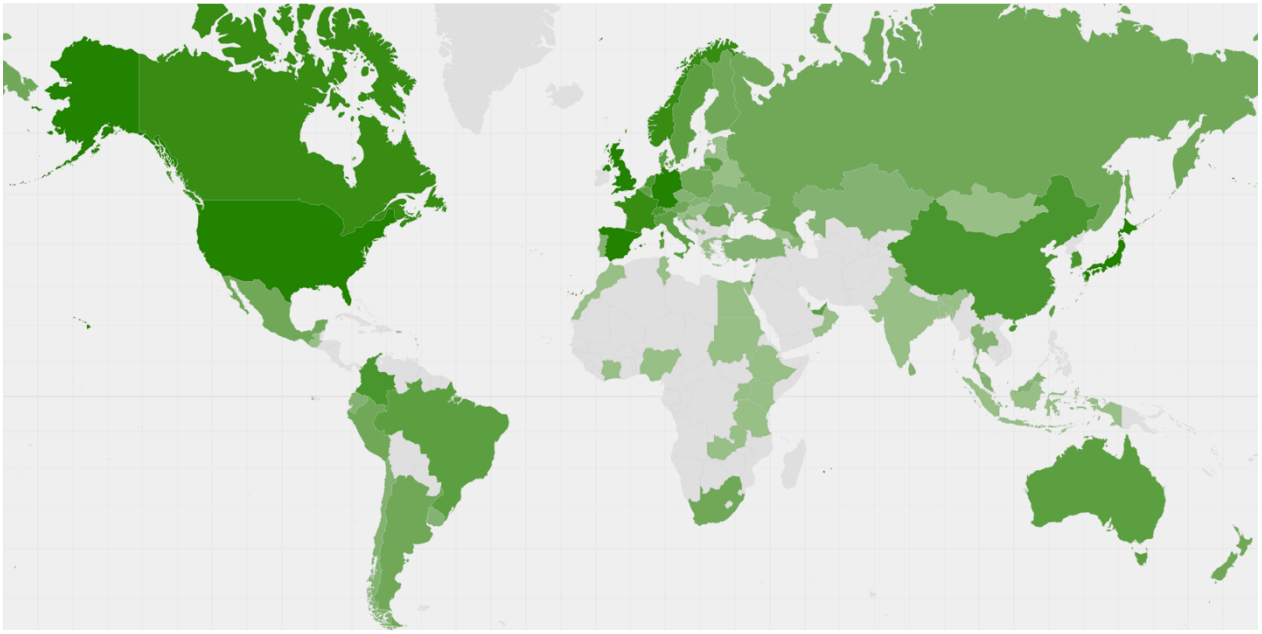
Finally, various outlets, including El Vocero, CarribeanBusiness and El Nuevo Dia wrote articles about the FIRST conference, taking place in Puerto Rico.

Organizational updates

Membership



FIRST continued to grow in 2017, with over 425 member teams by the 2018 annual conference. Membership grew mostly in Europe and Asia. FIRST membership is also increasingly becoming international for we now have members in a total of 86 countries, compared to 81 last year.



FIRST membership across the world, colored by membership density

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 from developing countries to competitively apply for financial support from FIRST to assist in their membership. In 2016, four teams from Bangladesh, Myanmar, Côte 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, four have joined as full members.

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

Suguru Yamaguchi Fellowship Program participants and Board Members, Puerto Rico Conference 2017

Events

FIRST activity across the world: Training classes TC's Symposia Annual conference 2018

FIRST organized 5 Symposia, 13 Technical Colloquia and 5 training sessions around the world. These events are opportunities not only to exchange ideas and know how, but also to grow trust and meet peers. In 2016 FIRST also published a site selection guideline to help us finding suitable and safe venues for our activities. Our events and training sessions would not be possible without volunteers, and we invite interested parties to contact us if interested in contributing.

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

The FIRST Regional Symposium for Arab and Africa Regions in Dar Es Salaam, Tanzania, November 2017

Training and Education

FIRST has recognized Training and Education as one of its key priorities.

In 2017 and 2018 work on the PSIRT Services Framework continued and the group, sponsored by Microsoft, created an Online Training for PSIRTS. This is an important step towards creating more visibility for these teams with a very specific function, to provide security for product development teams. These Service Frameworks, developed by experts from the FIRST community, systematically describe the services delivered by teams. The work continues to attract the attention of third parties who seek to better understand what CSIRTs and PSIRTS do.

Last fall Maarten Van Horenbeeck and Serge Droz, both members of the Board, developed a new training: "*Incident response for policymakers*". A first training, given during the IGF 2018 in Geneva attracted members from the diplomatic community, NGOs, civil society and academia. The feedback was very encouraging. A next training was scheduled for New York, targeting UN missions. Many volunteers from the community contributed to the materials, for which we are grateful.

Another highlight were two advanced trainings in Africa. The material was custom made especially for these events by the trainers. We are currently looking into how we could make it available to the wider FIRST community. Finally, the Board has been working on more formal procedures for training delivery: The goal is to create a self-sustaining and scalable training program. We also agreed to intensify our collaboration with ITU in delivering training courses during their Cyberdrills.

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

FIRST Training: Incident Response for Policymakers, Geneva, December 2017

Special Interest Groups

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:

- **Academic Security** - Creates a new space for discussion to reflect on academia's collective experiences, focus on current challenges and envision strategies on how we could work together to improve security in academic environments, including Research & Education, NREN & University CERTs, and Infrastructures.

- **Big Data** - Leverages the collective knowledge of teams who have deployed scaled IR capabilities to share reference architectures and best practices for detection and response at scale. It also will create containerized environments based on those architectures for teams that would like to get started.

- **Cyber Threat Intelligence** - Discusses common applications of threat intelligence capability with a view to agree best practice in the context of supporting effective digital forensics and incident response (DFIR) operations.

- **"Capture the Flag"** - Designs, develops, and conducts security competition exercises for the FIRST.org community including the flagship CTF event is held during the FIRST annual conference and is referred to as the FIRST.org Security Challenge.

Several SIGs published work efforts during the year, including the Vulnerability Coordination SIG, which worked with the National Telecommunications and Information Agency (NTIA) of the United States to publish a draft *Guidelines and Practices for Multi-Party Vulnerability Coordination* for public comment in late 2016. A final draft was released just after our Annual Conference in July 2017. On November 10, 2017 the Information Sharing SIG released a new version of MISP 2.4.82. Updates include the following:

  - An improved publish-subscribe ZMQ format
  - Improvements in the feeds system
  - Sightings are now ingested and synchronized among MISP instances
  - Improvements in many bug fixes and export

Two SIGs held face-to-face meetings: VRDX SIG held a 2.5 day summit at the Osaka TC to develop a global vision to improve multiple aspects of the vulnerability response lifecycle while the Red Team SIG held a face to face meeting at the Amsterdam TC that focused on facilitating current red team participants to exchange information about their practices.

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

Standards

FIRST supports the development of standards and maintains four different cybersecurity standards:

- 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. In the first half of 2017, FIRST released an interactive training "Mastering CVSSv3" through our learning platform. In response to regular inquiries to the CVSS SIG regarding what was planned for CVSS v3 improvements, the SIG published a list of work items they are working on for CVSS v3.x on November 15, 2017.
- 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 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 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. FIRST also signed a Memorandum of Understanding with standards organization OASIS to permit closer cooperation on threat intelligence specifications such as STIX and TAXII.

In 2017, FIRST published a Policy for Standards Development. The new policy will help provide guidance to FIRST SIG chairs and participants, as well as to the wider public, on the process to be followed for FIRST to formally publish a new standard. It covers topics such as how standards are agreed upon, how common terminology is maintained across standards, and how to deal with non-consensus proposals. It also implements a uniform approach to Intellectual-Property Rights management, ensuring FIRST standards remain free for implementation and unencumbered by patent restrictions.

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

Internet Governance, Policy and Outreach

As a member of the Internet Technical Community, FIRST has engaged 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:

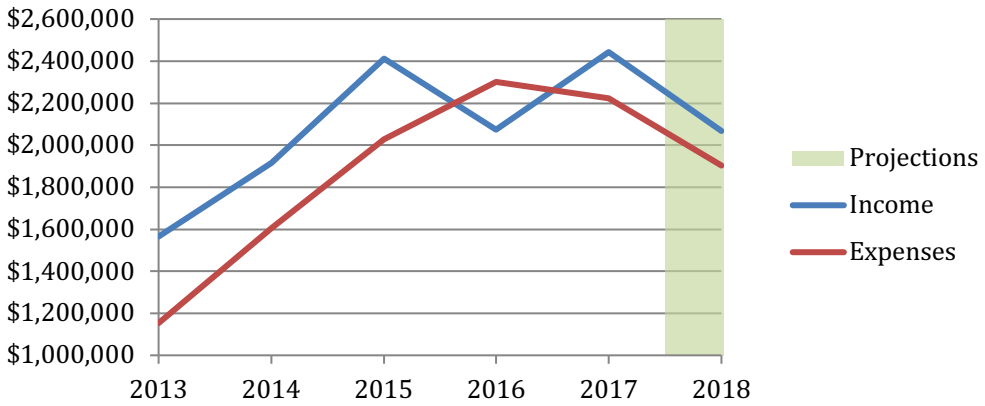
- Board member Adli Wahid participated in the ICT4Peace Cybersecurity Policy and Diplomacy initiative in Vietnam.
- Board member Serge Droz represented the Incident Response community and FIRST as an official expert in the ICT4Peace NGO. The latter is working on norms for IT security and AI.
- Board member Maarten Van Horenbeeck functioned as lead expert to the Best Practices Forum on Cybersecurity, organized by the Internet Governance Forum in Geneva, Switzerland.
- Board Member Serge Droz, on the invitation of Interpol, participated in an Expert Workshop of Project Stadia in Doha, Qatar. The meeting included presentations and one to one talks with government officials.
- FIRST continues to engage with ICANN and EU authorities to keep or reopen access to WHOIS information for security researches and incident responders. FIRST has teamed up with the Anti-Phishing Working Group (APWG) and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) to make a strong case.
- Board member Serge Droz presented FIRST's vision of global incident response during the 4th Annual Middle East Cyber Security Summit in Muscat, Oman in September 2017.
- Chair Thomas Schreck keynoted the OIC-CERT Annual Conference in Baku, Azerbaijan.
- Board member Maarten Van Horenbeeck participated and shared some of the cybersecurity implications of Lethal Autonomous Weapons Systems during Rightscon Toronto, in May of 2018.

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

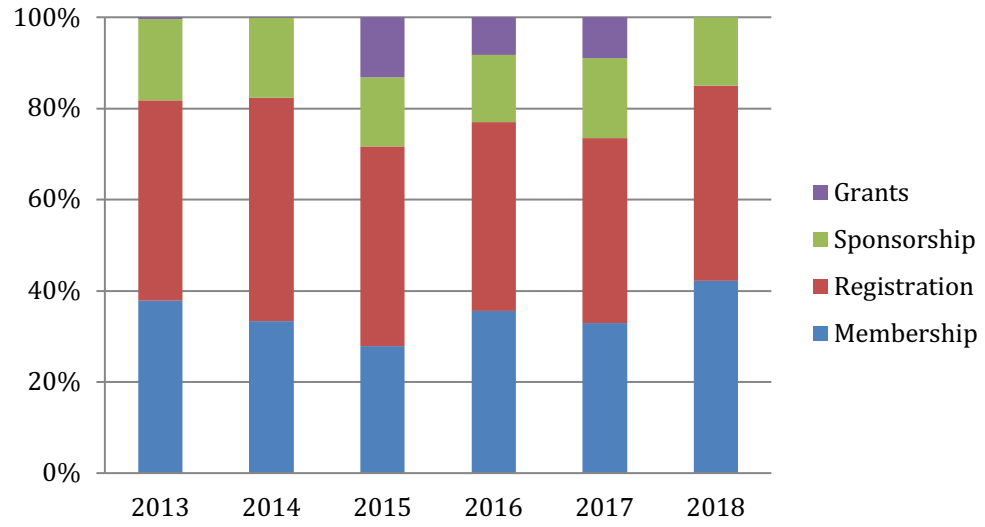
FIRST presenting during the Internet Governance Forum 2017 Main Session on Cybersecurity

Financials

After posting a loss in 2016, FIRST had a successful year in 2017, realizing a profit of $213,773. The profit is in line with the average of the realized profit in the covered period. The graph below shows total income and expenses for the period 2013 to 2017 with an estimate for 2018.



FIRST's income for 2017 was distributed across membership fees (33%), conference registration (41%) and sponsorship (18%). Though we did receive one grant during the reporting period, these funds were not yet received at the time of this report. The final spending for a grant received in 2016 did also extend until April 2017. It was earmarked for training development.



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 heavily invested in infrastructure. The following significant changes were made as a result:

- FIRST continued to move services to a new hosting provider, competitively selected through an RFP process. This led to cost savings and increased abilities to manage our wide set of services. This migration also consisted of a complete rebuild of most services and virtual machines, taking place in the background without much user impact.
- The infrastructure rebuild, ongoing between 2014-2018 led to some of the following benefits:
    - Clear alerting & monitoring
    - Automatic updates (and patch management cycle) for every service operated
    - Central syslog services
    - Proper incremental backups
    - Proper internal network design was needed
    - Stricter PCI requirements as part of PCI DSS 3.2 demanded more attention to CC handling
    - Implementation of a vulnerability reporting and bug bounty program
    - Advanced DDoS mitigation
- Other major service updates include:
    - A solid and up to date mail infrastructure (smtp.first.org, mx.first.org) which follows best current practices (DMARC, SPF, …) as well as provides IMAP services
    - The new CMS supports a new blog feature. This gives FIRST members a clear voice on the FIRST.org website and has featured several guest blogs through 2017-2018
    - Integration of the mailing list management into a centralized management system, api.first.org
    - A new and updated Certificate Authority (CA) server: the handling of TLS client certificates used by our members to authenticate against the portal was significantly automated, replacing scripts which previously had to be run for every membership change
    - A file sharing platform based on Nextcloud
    - An updated dues management server, to comply with PCI DSS 3.2
- FIRST established its “learning.first.org” platform which is covering some online courses (Mastering CVSS). These offerings are being expanded.
- The API service became a core component of our day-to-day operations, offering internal services to our secretariat to manage membership effectively.
- FIRST moved towards a single sign on solution – with the intermediate step of establishing an LDAP single password and user management system. Authorization and Authentication were re-architected.
- FIRST continued to improve, with the support of CIRCL, a Malware Information Sharing Platform (MISP) instance operated by the Information Sharing Operations SIG.
- FIRST created a Bug Bounty program. The bug bounty program helped the infrastructure team to discover vulnerabilities in FIRST’s web presence. In 2017 FIRST issued 21 bug rewards and thanked the reporters.
- FIRST is moving towards having its web services hosted via a Content Delivery Network in order to become more resilient in case of DDoS attacks or similar.
- FIRST installed a Nessus instance to do a weekly internal security scan and act upon alerts. As another security measure we hardened its servers periodically and checks if it follows best current practices.
- In order to comply with GDPR, FIRST did an internal data and process inventory, carefully checking for privacy implications. We also spent significant effort updating our internal documentation.

An initiative launched during 2017, the implementation of a member-wide Malware Information Sharing Platform (MISP) threat intelligence platform, saw significant success. As of May, 2018, over 700 users across the FIRST community, across more than 240 organizations, participated in the network.

One project was cancelled. During 2016, FIRST initiated the implementation of an Association Management System (AMS), with as goal to automate several of our management processes and optimize reporting. During the deployment, significant issues were identified with the solution chosen, and how it could support our specific needs as an organization. In May 2018, FIRST decided to no longer pursue this implementation. During its deployment, significant automations were achieved using our current systems, and FIRST is not currently planning to consider other AMS systems. We will continue to invest in existing systems developed by our technology team.

The FIRST blog, a new feature launched during the 2017 conference

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