FIRST

Improving Security Together

Board Members

Serge Droz
Javier Berciano
Andrea Dufkova
Alexander Jaeger
Dave Schwartzburg
Derrick Scholl
Thomas Schreck
Damir 'Gaus' Rajnovic
Masato Terada
Maarten Van Horenbeeck

ANNUAL REPORT

2019 - 2020

Serge Droz, Chair
Forum of Incident Response & Security Teams

FIRST Annual Report 2019-2020

Dear Reader,

Welcome to the Forum of Incident Response and Security Teams (FIRST) Annual Report. This is our fourth report and provides a summary of our activities between our Annual Conference in Edinburgh in June 2019 and July 1 2020.

Despite the pandemic shaking up our routine in the middle of this reporting period, FIRST is happy to report on much good news. We have grown to over 530 teams in 96 countries, confirming that Incident Responders see value in FIRST.

Again, we have conducted many events, training courses, Symposia and others. FIRST has been increasingly asked by policymaking bodies to advise on topics such as responsible vulnerability disclosure, capacity building and even norms for responsible state behaviour, demonstrating that we are recognized as an important stakeholder when it comes to global cybersecurity issues.

COVID-19 has had a profound impact on the way we meet as a community. We have managed to move many of our important events online which has allowed members to continue to share thoughts, ideas and queries. Going forward we will continue to experiment with formats that will allow us to interact online. This may also help us in the long run to reduce our impact on rising CO_2 levels.

Our Special Interest Groups have been pretty unaffected by COVID-19. Driven entirely by volunteers working virtually, they have been enormously productive, creating for example a Code of Ethics, or an online Capture the Flag with record participation.

2019-20 has been a challenging year but we have risen to the occasion. As incident responders we are familiar with performing under adverse conditions. Our ability to overcome challenges makes me very proud to be the chair of FIRST.

The Board of Directors is grateful for the support we get from our members, sponsors, grantors, and the wider security and incident response communities. Thank you for your continued enthusiasm, and we look forward to continuing to collaborate with you in the future to further the maturity of cybersecurity incident response around the world.

Serge Droz

Serge Droz
Chair, Forum of Incident Response and Security Teams

* Front page photo source: 2019 Beijing Cyber Security Conference

Table of Contents

Organizational Goals

During 2019-20, FIRST continued to mature and make progress on its four main missions:

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.

The new Board formed in 2019 has faced several challenges. In the fall of 2019, the cooling global political climate led to increasing export restrictions and sanctions, forcing us to suspend teams in good standing, and otherwise increasing the administrative effort involved in being an organization with global membership. 2020 has been dominated by one topic so far: the global COVID-19 pandemic, which has had a great impact on our operations. We quickly responded by moving activities including Board meetings, conferences, the AGM and the annual general meeting online. Fortunately, we were able to launch our new single sign on Portal this Spring which has allowed us to provide many existing activities online and also offer new channels for engagement such as Slack for FIRST members.

Behind the curtain much work was, and continues to be, needed to make the Portal happen. Due to rapid expansion of FIRST’s member teams in the past five years, our previously manually recorded processes needed to be streamlined and integrated into the Portal to help us to manage and collaborate more effectively with users.

FIRST has not only grown in terms of members during 2019-20, but our influence also increased with policymakers. We are regularly consulted by international organizations to help and advise on best practices to make the Internet a safer place. We continue to build mutually beneficial relationships with policymakers to ensure that they understand what Incident Responders do and what they need. This initiative has led to FIRST building important, strategic partnerships with organizations such as Internet Corporation for Assigned Names and Numbers, the Cyber Peace Institute and the World Economic Forum, to name but a few.

Public Relations and Marketing

With the aim of increasing our global reach and engaging incident responders worldwide, FIRST continues to deliver an integrated communications strategy which involves building relationships with the media, keeping our members informed and providing global stakeholders with regular updates across our social media channels.

Relationships were built between FIRST and journalists from Business Insider, China Daily, CISO Magazine, Cyber Risk Security, Help Net Security, Hong Kong Economic Times, Security Magazine, Security Week, Tech Babble, The Daily Swig in media across the world. Our media database was increased too, widening our reach globally.

During the last year, FIRST issued eight press releases, including these major announcements:

- FIRST released ethics guidelines to deepen trust among incident response teams (Dec 2019)
- FIRST publishes updated CVSS for worldwide security teams (July 2019)
- FIRST releases updated Computer Security Incident Response Team (CSIRT) Services Framework – Version 2.1 (March 2020)
- FIRST aims to update the Traffic Light Protocol standard to increase global adoption (May 2020)
- FIRST updates coordination principles for Multi-Party Vulnerability Coordination and Disclosure (May 2020)

Various outlets wrote articles about our Edinburgh conference including Digit, Future Scot, High Growth Scotland, Professional Security and The Daily Swig.

A timely FIRST opinion piece written by Board member Maarten Van Horenbeeck entitled ‘11 vital steps towards cyber security resilience in 2020’ achieved widespread interest globally in Australian Cybersecurity Magazine, Cyber Risk Leaders, Help Net Security and The Cyber Wire.

In addition FIRST was mentioned in a number of articles: Businesses must prepare to welcome Generation Alpha (July 2019); Qatar pays special attention to Cybersecurity (Dec 2019); Cybersecurity Forum Begins (Dec 2019); and, New code of ethics for cyber security professionals – Guidelines applicable for all sectors, including European NRENs (Jan 2020).

The aggregated reach of all the media coverage (opportunities to see and hear news about FIRST) was in excess of 600 million - mostly due to the coverage generated in China by Chris Gibson’s presentation at the 2019 Beijing Cyber Security Conference.

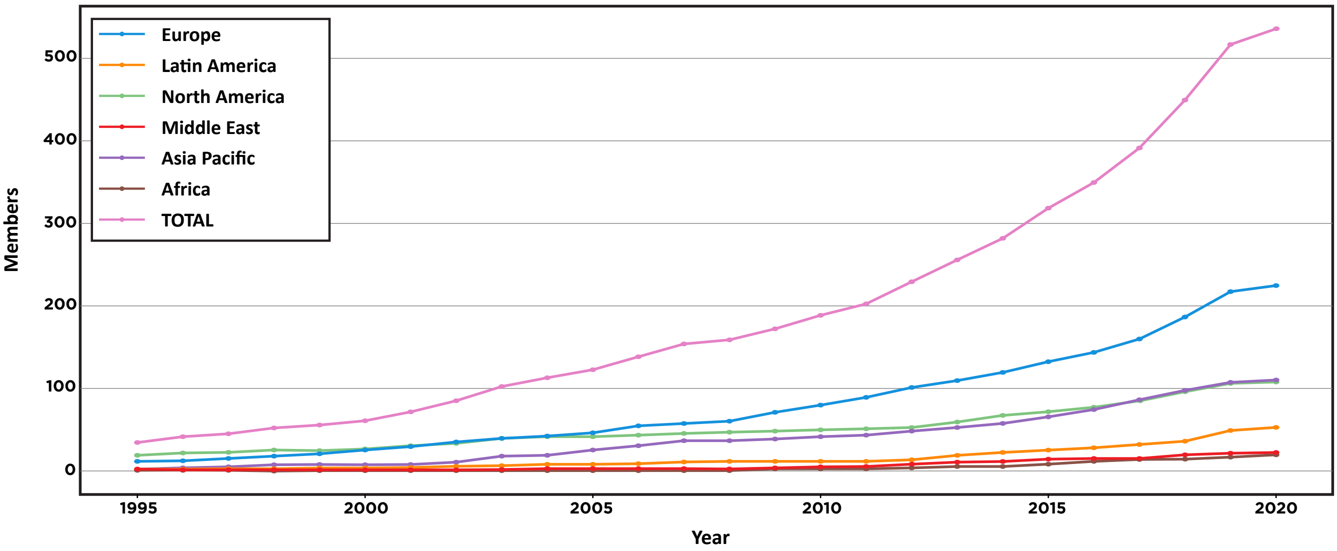
We have moved to a quarterly newsletter with the aim of keeping our members regularly informed and up to date. The newsletter features major announcements by FIRST, invitations to participate in projects, stories on members and infrastructure updates.

We saw a substantial increase in followers across our social media channels in the past 12 months. Total number of followers are now at 12,195 with LinkedIin looking particularly healthy with 2,717 followers - 28% increase.

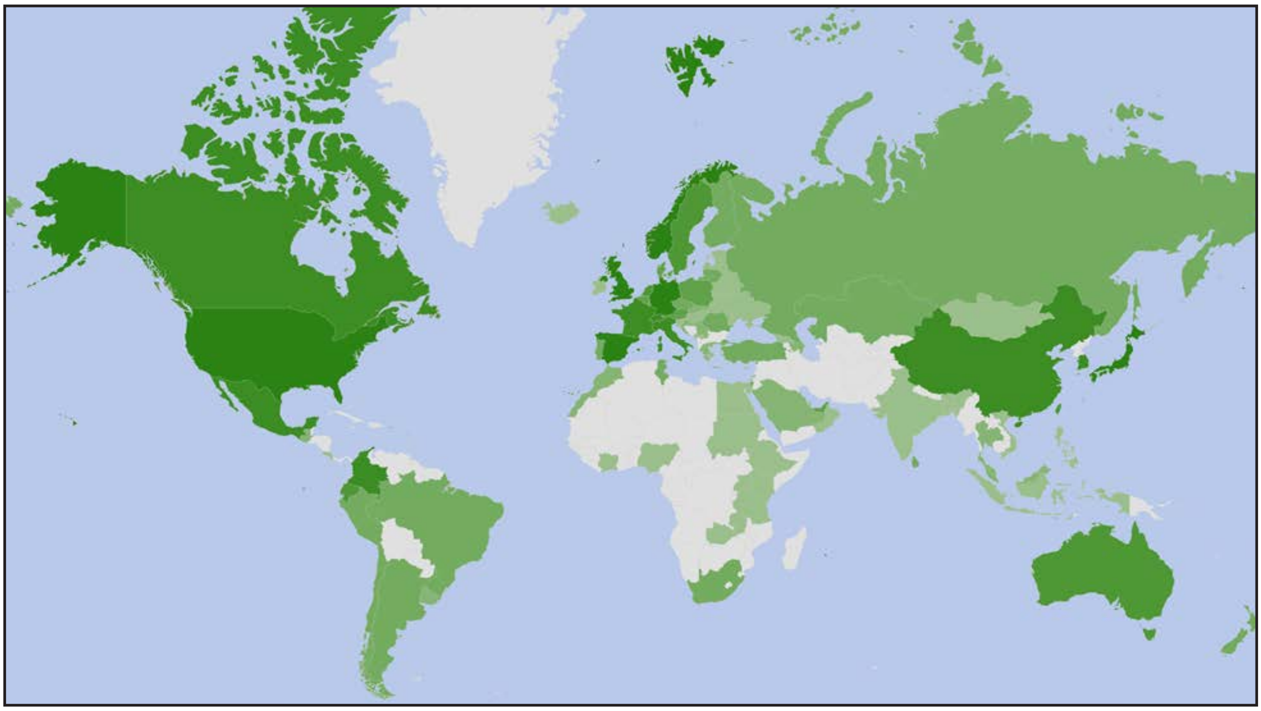
Organizational Progress

Membership

Membership continues to grow. Over 530 member teams held active membership as at July 2020 - a 10% year over year increase. Membership grew mostly in Europe and Asia, but we also saw growth in teams from across Latin America.



Membership continues to grow. Over 530 member teams held active membership as at July 2020 - a 10% year over year increase. Membership grew mostly in Europe and Asia, but we also saw growth in teams from across Latin America.



Fellowship

With the purpose of making the Internet safe for everyone across the world, FIRST actively encourages incident response teams from developing economies to join our community. The Suguru Yamaguchi Fellowship Program achieves this goal by making it easier for teams to join FIRST. In 2020, we accepted teams from Albania, Bolivia, Cameroon, Vanuatu, Republic of North Macedonia and Mozambique. Due to complications resulting from COVID-19 and the postponement of our annual conference, the new teams will start their Fellowship at the 2021 Conference in Fukuoka, Japan.

They will join existing Fellowship members from (2016) Bangladesh, Myanmar, Cote d'Ivoire, and Ghana, (2017) Vietnam, Panama, Ecuador and Moldova, (2018) Tonga and 2019 (Burkina Faso, Uzbekistan, Benin, Serbia and South Africa).

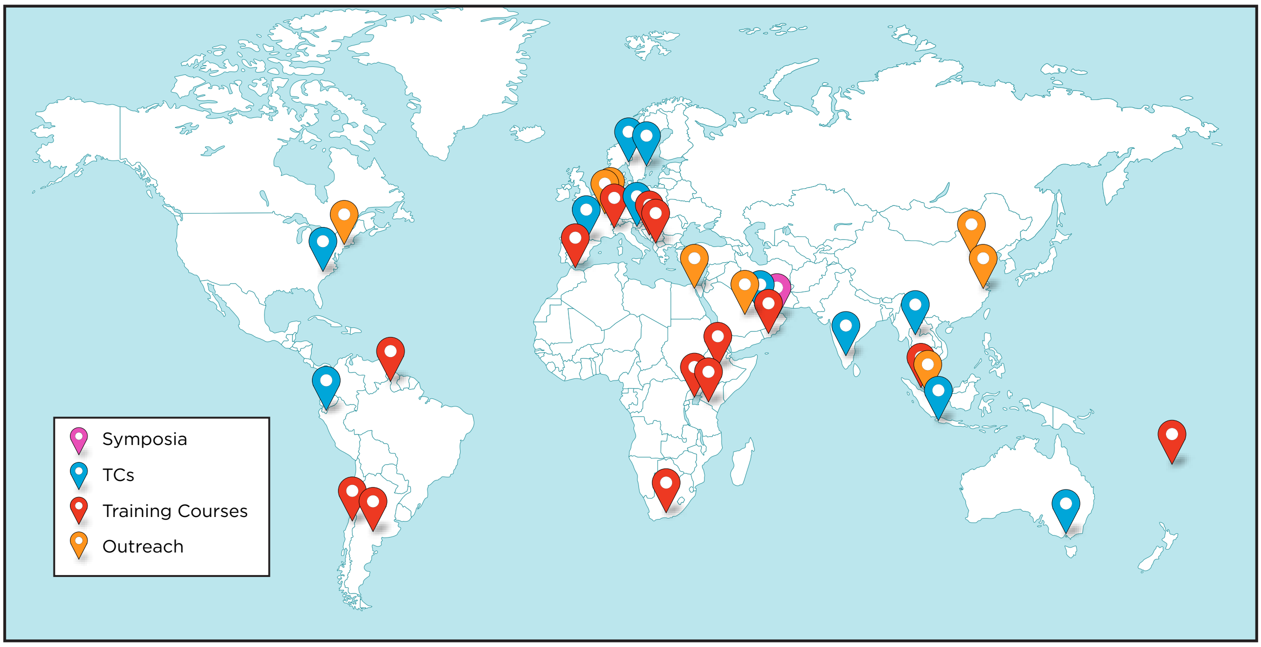
Suguru Yamaguchi Fellowship Program participants and Board Members and friends, Edinburgh Conference 2019

Events

FIRST continues to organize a number of events annually, with the purpose of extending our global reach, building trust among peers and exchanging ideas and knowledge. During 2019-20, we held three Symposia, 11 Technical Colloquia, 15 Workshop and training events and five distinct online events. We also actively participated in 13 outreach events related to Internet Governance and Policy. Note that the Annual Conference was postponed due to COVID-19.

Our events and training sessions would not be possible without our 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**



FIRST activity across the World

Training and Education

Training and Education is one of FIRST's key priorities. We are committed to truly making the incident response community more effective and efficient by providing educational opportunities to our members.

Training and Education Materials

In 2019-2020 FIRST volunteers continued to develop the CSIRT and PSIRT service frameworks. The PSIRT group put much effort into the services framework for Product Security Incident Response, completing an updated version Spring 2020. The CSIRT services framework was also updated and aligned with its PSIRT counterpart - version 2.1 was published in November 2019.

Both service frameworks exceeded our expectations in terms of demand. They are used regularly by several international organizations as the basis for their capacity building programs and have been continuously adopted by our community during the set up or evolution of Security Incident Response teams.

We also released updated and new training courses in the past year - IPv6 Security, Malware Analysis, FIRST Security Bootcamp and Breach Workshops.

Training & Education Sessions

FIRST's training initiatives have become increasingly popular. During last year's Conference in Edinburgh we offered Train the Trainer sessions provided by the original creators of the materials. We have also delivered a number of courses at various locations, attracting ever more students. Our courses not only build capacity but also form a platform to welcome new teams at FIRST. As has been the case historically, FIRST releases all of its training materials under a Creative Commons license, to maximize their usefulness.

In addition, FIRST was happy to deliver exclusive Incident Response training to International Telecommunication Union (ITU) members at their Cyber Drills and collaboration with the Organization of American States (OAS) in their training project under the umbrella of the CSIRT Americas initiative.

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

Symposium for Pacific Island Nations, Fiji 2019

Special Interest Groups (SIG)

Special Interest Groups exist to provide a forum where FIRST Members can discuss topics of interest common to the incident response community. FIRST facilitates these groups by providing support such as website infrastructure, a conference bridge, a Program Manager, and a meeting space at our events.

FIRST members established four new SIGs during 2019-2020:

CSIRT Framework Development SIG
DNS Abuse SIG
PSIRT SIG
Exploit Prediction Scoring System (EPSS)

Of note, a group was established to develop the Exploit Prediction Scoring System (EPSS), an open, data-driven standard for predicting when software vulnerabilities could be exploited.

Existing SIGs were very active during the year, and released the following materials:

New CSIRT Service Framework 2.1
New PSIRT Service Framework 1.1
New CVSS v3.1
IEP 2.0 approved
EthicsFIRST draft was released
CTI Curriculum
Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure v1.1
Two webinars Metrics SIG with average 40 attendees out of FIRST members
Six webinars on Cyber Insurance
Anti-Trust Statement for Cyber Insurance SIG
Working Group on Cyber Insurance Coverage Mapping
Big Data Framework for Incident Detection and Response
DNS Abuse SIG

The following other SIGs are currently active within FIRST:

1. **Academic Security**
2. **Big Data**
3. **CSIRT Framework**
4. **CTI**
5. **CVSS**
6. **Cyber Insurance**
7. **Ethics**
8. **IEP**
9. **Malware Analysis**
10. **Metrics**
11. **PSIRT**
12. **Red Team**
13. **Security Lounge**

Members can find out more about the SIGs, or join one or more, via the FIRST Portal **https://portal.first.org/**. New SIGs can be commenced, and funded by FIRST, with sufficient membership interest. We invite any member to reach out with any new initiatives they would like to organize within FIRST.

Standards

Standards help define a common vocabulary across our industry and help us to prevent misunderstandings. With this in mind, FIRST supported the development and maintenance of several cybersecurity standards during 2019-20:

- **ISO/IEC 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/IEC 30111 'Vulnerability Handling Process':**the second revision of this standard was finalized and published in 2019.
- **ISO/IEC 27035 'Information Security Incident Management':** The third part of this standard is due to be published at the end of 2020.
- **Common Vulnerability Scoring System (CVSS):** FIRST offers an on-line learning platform training on CVSSv3.
- **Traffic Light Protocol (TLP):** It is a set of designations used to ensure a common expectation in the 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 and FIRST continued to update this version in 2019-20. TLP was also translated by members into Dutch and Japanese this year.
- **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.
- **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 has recently been updated by the FIRST community.

The following new standards and ISO are currently being proposed and FIRST will contribute to their development if they are signed off:

- **ISO/IEC PWI 5189 'Information security incident response coordination'**
- **ISO/IEC NP 4983 'Remedial Systems Updating'**
- **ISO/IEC PWI 5192 'Guidelines on Security Operations Center'**
- **Study Period, Multi-Party Coordinated Vulnerability Disclosure and Handling**

FIRST continues to be a sector member in the International Telecommunication Union as a standards body and is a Category C liaison to ISO. We also continue to maintain an Memorandum of Understanding with standards organization OASIS to permit closer cooperation on threat intelligence specifications such as Structured Threat Information Expression and Trusted Automated eXchange of Indicator Information.

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 builds mutually beneficial relationships with policymakers and Internet governance bodies by providing technical expertise where appropriate. We contribute to technical discussions adding to the wider Internet governance debate by educating policymakers and other stakeholder communities about the challenges facing the Incident Response community.

Our activities for 2019-20 are listed below:

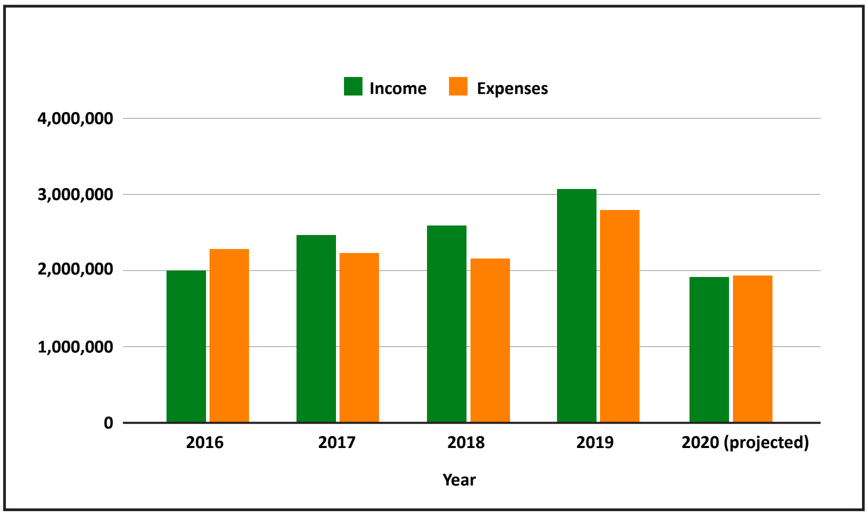
- Executive Director Chris Gibson gave a keynote at the Beijing Cyber Security Conference, China.
- Board member Serge Droz actively participated in the Meridian annual conference in Geneva.
- Board member Serge Droz gave a keynote at the 2019 Wuzhen World Internet Conference, China.
- Executive Director Chris Gibson participated in the Interpol/Europol Cybercrime Conference in The Hague
- Board members Maarten Van Horenbeeck and Serge Droz participated in the IGF 2019 in Berlin.
- Executive Director Chris Gibson actively participated in the WEF Center for Cybersecurity's annual conference.
- Michael Bem continues to participate in WEF Cybersecurity activities.
- Board member Maarten Van Horenbeeck represented FIRST at the Informal intersessional consultative meeting of the OEWG in New York.
- Board member Serge Droz represented FIRST at the UNIDIR multi stakeholder dialogue on responsible vulnerability disclosure in Geneva.
- Board members Maarten Van Horenbeeck and Serge Droz participated in the Yale Workshop on norms in cyberspace as subject matter experts.
- Executive Director Chris Gibson gave a keynote at the 1st National Cybersecurity Summit, Cairo, Egypt.
- Executive Director Chris Gibson was involved in a panel discussion at the G20 Cybersecurity Dialogue in Riyadh, Saudi Arabia.

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

Financials

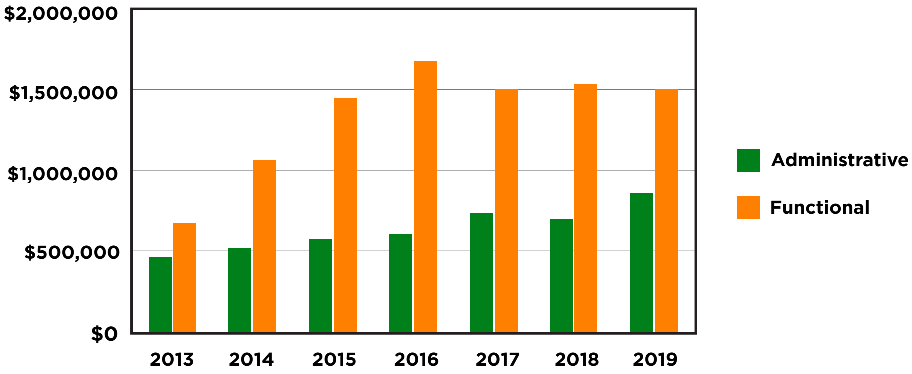
In 2019 FIRST achieved a surplus of around US$270,000. This was aligned with our budget forecast. As the organization grows and matures, our expenses grow too but so does our income, as shown in the graph below. Please note that the figures for 2020 are projections only. The Board adjusted the budget to reflect the changes in FIRST's operations due to the COVID-19 pandemic.

Income vs. Expenses



Administrative vs. Functional Expenses

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



2019 was a year of changes with some having a direct impact on finances. While the introduction of Associate Management System (AMS) was aborted in 2018, we maintained US$40,000 in reserves in case of a dispute with the AMS vendor. These reserves will have to be in place until 2021. 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

Portal & SSO

FIRST invested, and was heavily focused, on the identity project in the infrastructure domain during 2019-20 to make it easier for all members to engage and access our materials safely.

In April 2020 we released a new Portal and Single Sign-On (SSO) platform for FIRST team representatives, members, liaisons, collaborators and event attendees. Members are now able to manage their profiles and access key FIRST resources including the directory, MISP, Wiki, and more from Portal.

This work ultimately proved timely in facilitating rapid adaptation in response to the global pandemic and we are now at nearly 1000 users. The success of this effort has improved the organization's security posture, reduced support overhead, and simplified access while eliminating challenges previously posed by X.509. Representatives are also able to manage their team profiles and rosters, perform AGM related tasks via SSO-enabled eVoting, access online events and view and pay their dues invoices.

At the same time, we have expanded the use of administrative groups to control access across FIRST services, such as mailing lists, wiki spaces, Slack channels, and more.

Slack

This year we also made a Slack workspace available to members. This is an SSO-enabled service with channels in place for SIGs and committee members to discuss events and specific interests. Access to Slack is available through Portal.

We look forward to providing you with a new update in 2021, and to all we'll achieve, together.

FIRST™

Improving Security Together

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

Forum of Incident Response and Security Teams
2500 Regency Parkway, Cary, North Carolina, 27518
United States of America