



2020 - 2021

ANNUAL REPORT

Board Members

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

FIRST Annual Report 2020-2021

Dear Reader,

Welcome to the Forum of Incident Response and Security Teams (FIRST) Annual Report. This is our fifth report and provides a summary of our activities between end of June 2020 until the end of May 2021.

The past year will remain in our memories as most extraordinary.

Covid-19 brought to light the worst and the best in humankind. Incident responders continued working, mostly from home, often struggling with the effects of the pandemic while at the same time fighting an increasing number of criminals that were profiting from the crisis by attacking an already strained resource.

The pandemic has shown us how vital technology is and, in particular, ICT. Without a functioning internet, it would be impossible for anyone to work remotely from home and maintain productivity. This change from on-site to remote in such a short time was a challenge to security people, not to mention the increased risks involved.

These pressures and the general anxiety about Covid have affected us all - a topic we addressed in our new podcast series, among other issues relating to our industry.

The last year has undoubtedly been a big challenge for FIRST. We moved our events online and adapted various services. The board has had to change its normal practice of face-to-face meetings, where the members get to work together for three full days, to achieve the same work through video conferences across multiple time zones. A lot of uncertainty at the beginning of the pandemic made it challenging to plan our regular calendar of activities. As always, our members are our first concern, and we wondered how this would affect them. We also worried about the financial impact on FIRST. We didn't know when we could meet again and if and when we should start preparing for face-to-face meetings or training. These questions remain difficult to answer. Meantime, we have adjusted our services to meet the new conditions and delivered several virtual events and activities to replace our in-person initiatives.

Luckily, with vaccines developed in record times, there is hope. However, as wealthier countries are progressing vaccination programs, emerging economies are expected to struggle for much longer. As a global organization, this affects FIRST, but we will continue to provide services to people who cannot travel. The 2020 virtual conference in November demonstrated that we could reach many people worldwide, even more than at our in-person events, with online events.

Finally, I would like to thank the FIRST staff and all our volunteers who have adapted and worked hard during the past year to keep the organization going in an ever-changing environment.



Serge Droz Chair, Forum of Incident Response and Security Teams

Table of Contents

FIRST Annual Report 2020-2021.....	2
Table of Contents	3
Exisiting Mission.....	4
Organizational Update	5
Membership	5
Fellowship	6
Events	6
Training & Education.....	7
Hall of Fame.....	8
Special Interest Groups (SIG).....	9
Standards	10
Diversity & Inclusion.....	11
Internet Governance & Policy.....	12
Major Announcements & Press.....	14
Financials	15
Infrastructure.....	16

Existing Mission

Many of our FIRST members will recognize our logo's strapline – 'Improving security together.'

Our vision and mission aim to accomplish this.

Our vision states: FIRST aspires to bring together incident response and security teams from every country across the world to ensure a safe internet for all.

We've identified three missions to create a clear direction for our organization to achieve our vision.

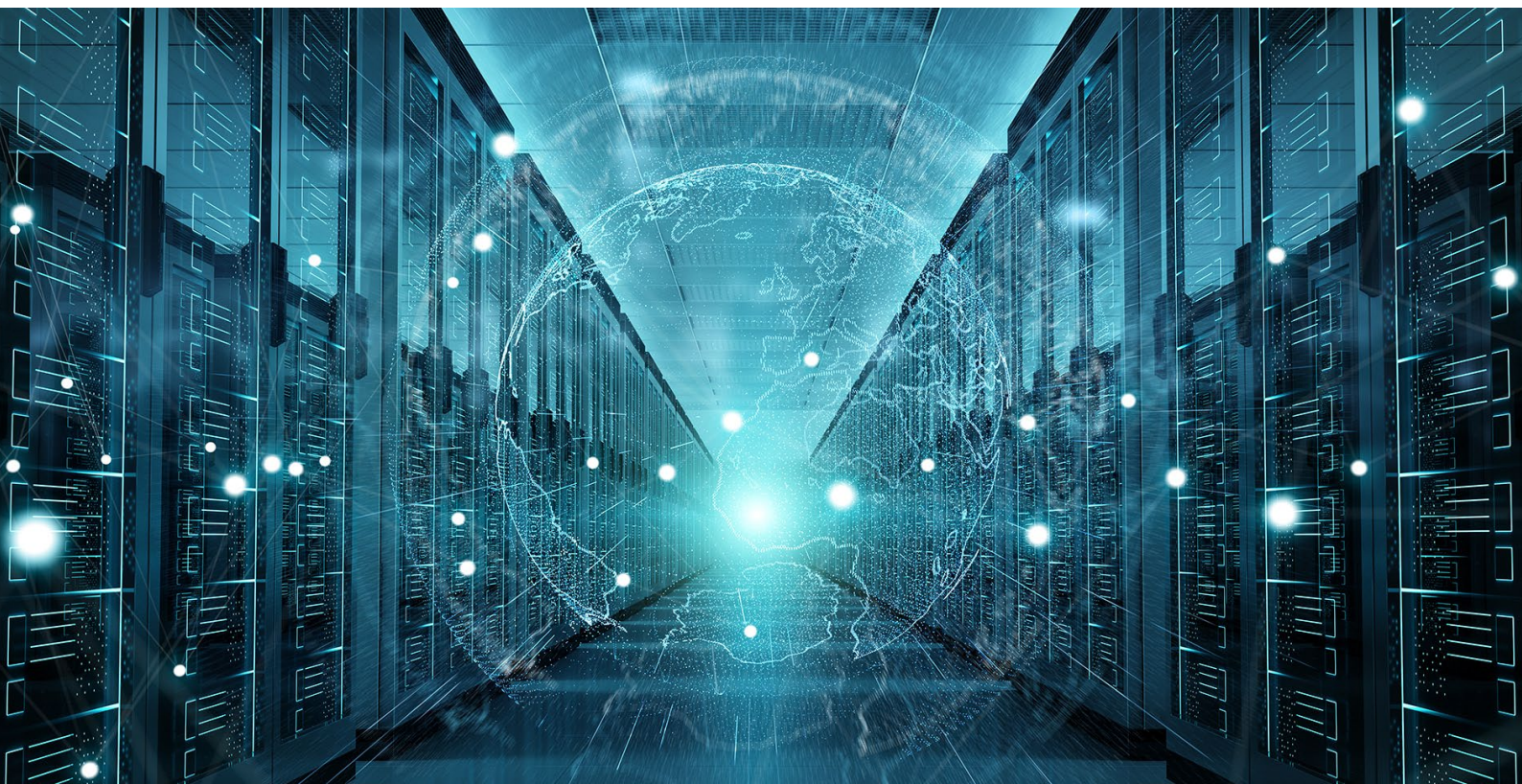
The first mission is to get at least one member in every country to become a FIRST member. With 97 countries represented, we still have a long way to go.

Secondly, we promote working together. A key ingredient in seamless collaboration is a common understanding of issues. Challenges happen when two teams interpret the same problem differently. So we aim to establish a global language through aiding collaborations, operating training courses, releasing standards, facilitating SIGS, and so on.

Lastly, our work is increasingly affected by global politics, laws, rules, and so on. FIRST engages with policymakers so that regulations help rather than hinder the valuable work that we do.

This clear vision and mission provide a focus for us to strategize and deliver a concise business plan.

[Read more on our website.](#)

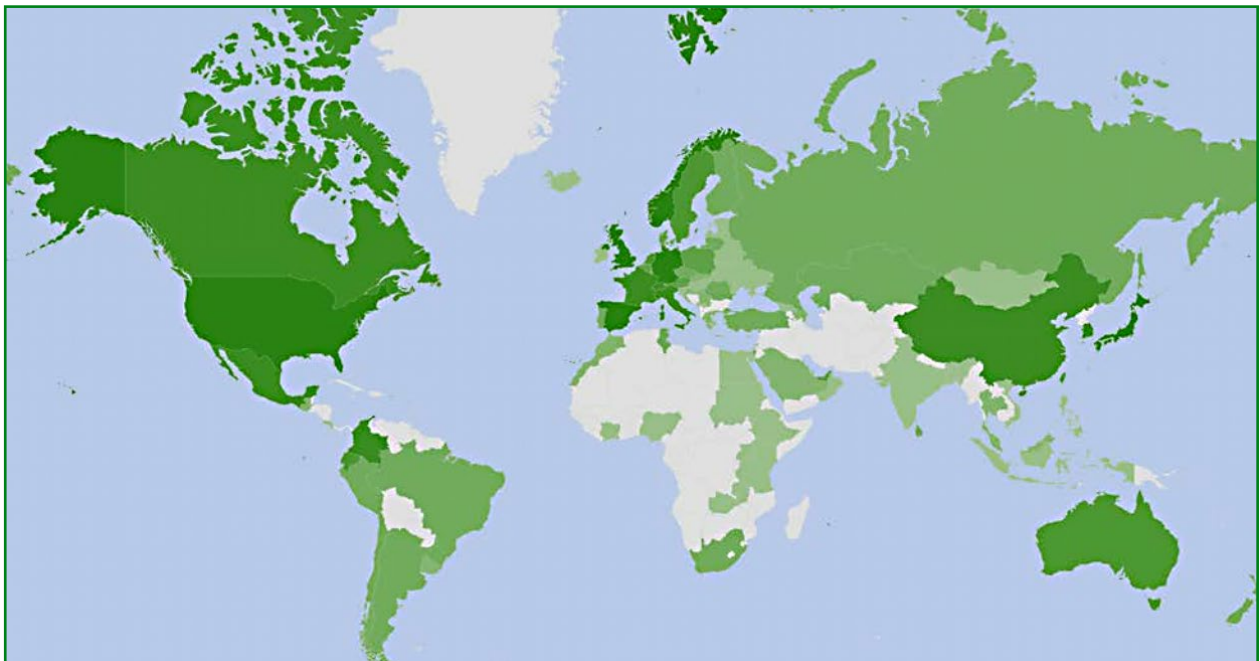
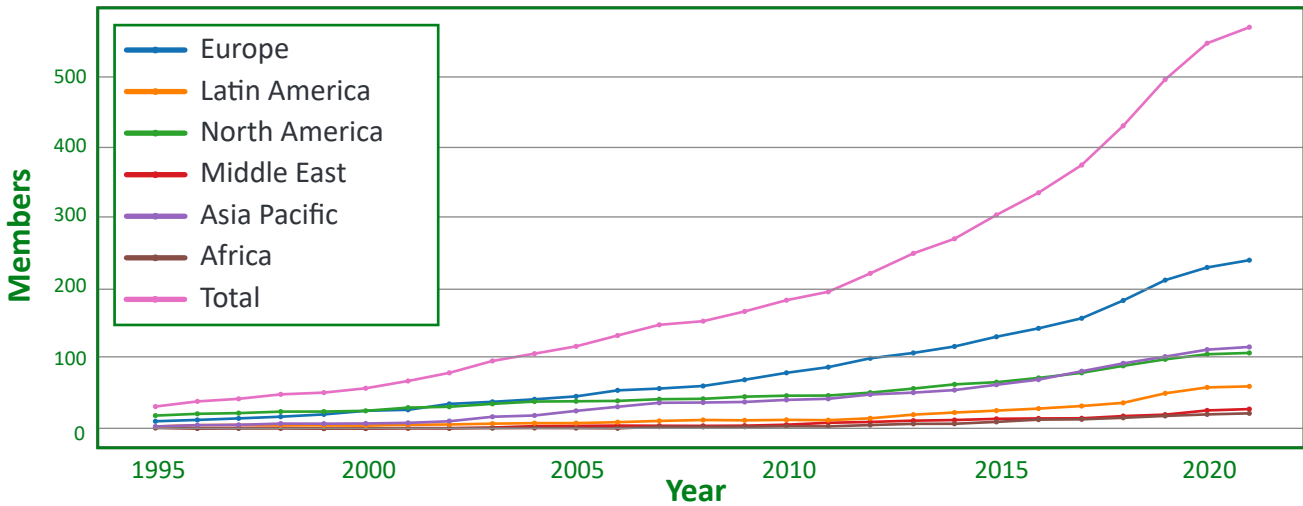


Organizational Update

The past year has undoubtedly been exceptional in many respects, and clearly, the pandemic has had a visible impact on FIRST. Many of our programs, in particular face-to-face meetings, had to be canceled. It took some time to adjust, but we soon found a practical compromise for events thanks to our staff and events team. The initial fear of a decline in membership has not materialized. The following summarizes the key figures.

Membership

Membership grew by over 10% to more than 570 teams across 97 countries. This substantial achievement still falls short of our goal of having a member in every country on the planet.



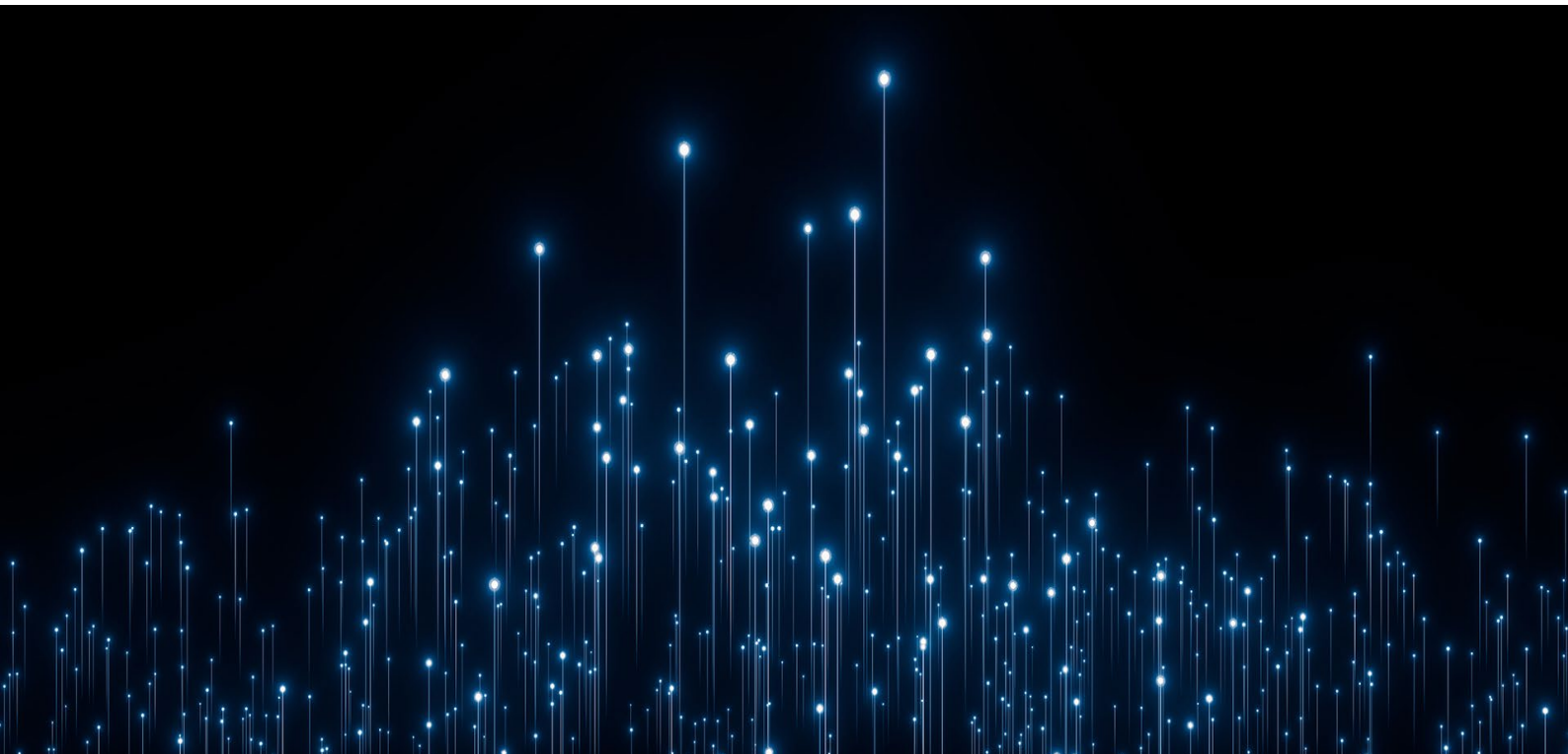
Fellowship

The Fellowship program, up until now, was primarily based on working with participants at the annual conference. As we have been unable to meet in person due to the Covid-19 pandemic, we organized two breach workshops geared explicitly to members of the Fellowship program. The Board and Membership Committee has also started to expand fellowship-related activities outside of the conference to engage more often throughout the year with the program participants, focusing on CSIRT community building.

Events

FIRST continued to organize several virtual events during the pandemic to extend our global reach, build trust among peers, and exchange ideas and knowledge. During 2020-21, we held three symposia, 12 webinars, seven workshops, and training events. The virtual events were exceptionally well attended by members and non-members. The highlight was the largest ever annual conference with over 2,500 online participants, doubling our 2019 Edinburgh in-person attendance. The event was offered to attendees without a registration fee and would not have been possible without the help of generous sponsors and members. This success shows that moving events, at least partially online, increases accessibility and our reach.

[Read more about our events on our website.](#)



Training & Education

Training and Education are part of our mission to encourage incident response and security teams to work together and use the same language. Consequently, we are committed to promoting efficiency and effectiveness among the community by providing educational opportunities as follows:

Throughout 2020-2021 FIRST volunteers continued their work to improve the CSIRT and PSIRT service frameworks. The latest versions (2.1 for CSIRT and 1.1 for PSIRT) are available on the FIRST web page under Standards - Service Frameworks. Both frameworks exceeded our expectations in terms of demand. Used regularly by several international organizations in their capacity-building programs, our community has continuously adopted them during the setup or evolution of Security Incident Response Teams.

We also released updated versions of the Malware Analysis and DDoS Mitigations Fundamentals training courses in the past year.

There was at least one training day with operational or technical topics during all FIRST virtual events, covering different regions and time zones.

In addition, FIRST was happy to deliver exclusive Incident Response training to the Organization of American States (OAS) members 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/>



Hall of Fame

In 2020 FIRST introduced two outstanding individuals to the Incident Response Hall of Fame: Ian Cook and Don Stikvoort. Both have been and still contribute to the global Incident Response Community.

Ian Cook is a cybersecurity veteran with 43 years of experience, including six years on the FIRST Board. He has held senior technical and management positions at the UK NHS, Tricentrol Oil Corporation, Saudi American Bank, Citigroup, Merrill Lynch, Pentest Ltd, Barclays Bank, and Team Cymru. Ian has been an active member of FIRST since 1997 and has sponsored many companies to join too. As well as co-chairing the 19th Annual FIRST Conference and leading many other initiatives, Ian was one of the key drivers who transformed FIRST into a professional and influential global organization. More recently, Ian was instrumental in forming the FIRST Cyber Threat Intelligence SIG and facilitated the 2019 FIRST CTI Symposium in London.

In 1988 Don joined the Dutch national research network SURFnet. Don was among the pioneers who created the European Internet in 1989. He recognized "security" as a concern in 1991, chaired SURFcert between 1992-8, and was the founding father of NCSC-NL, the Dutch national team. Don became a member of FIRST in 1992 and has been incredibly active during his membership, from chairing the FIRST conference in Australia, co-chair of the Traffic Light Protocol working group, and participating in CSIRT, Metrics, and Ethics working groups. In 1998 he co-wrote the 'Handbook for Computer Security Incident Response Teams (CSIRTs)'. Don continues to support the global cybersecurity community through S-CURE, the company he founded in 1998.

[Read more about our Incident Response Hall of Fame on our website](#)



Special Interest Groups (SIG) exist to provide a forum where FIRST Members can discuss topics of interest common to the incident response community and work together to create new standards, tools, training, and other collateral to improve security for everyone. FIRST facilitates these groups by providing website infrastructure, a conference bridge, a Program Manager, and meeting space at our events. We also initiate quarterly meetings for SIG chairs to gather feedback on support needs, discuss best practices, and identify potential synergies across groups.

We want to welcome the following SIGs that joined FIRST during 2020-2021:

Retail and Consumer Packaged Goods (CPG) - NEW SIG
Threat Intel Coalition (TIC) SIG

Existing SIGs continued to meet virtually and released the following materials:

EthicsFIRST released ethics guidelines and a new website

Currently, active SIGs include:

-
- | | |
|--|--|
| 1. Academic Security | 10. Malware Analysis |
| 2. CSIRT Framework | 11. Metrics |
| 3. Cyber Threat Intelligence (CTI) | 12. Passive DNS Exchange |
| 4. Common Vulnerability Scoring System SIG (CVSS) | 13. PSIRT (Education, Tools, Framework, |
| 5. Cyber Insurance | 14. Red Team |
| 6. Domain Name System (DNS) Abuse | 15. Retail and Consumer Packaged Goods |
| 7. Ethics | 16. Traffic Light Protocol |
| 8. Exploit Prediction Scoring System (EPSS) | 17. Women of FIRST (Birds of a Feather) |
| 9. IEP | 18. Security Lounge |
-

To see the latest updates of ongoing SIG work, please check out FIRST's YouTube channel https://www.youtube.com/channel/UCK3_z6YyWvfqrOuCmrfxsTw.

Members can find out more about the SIGs, or join one or more, via the FIRST Portal <https://portal.first.org/>.

New SIGs with sufficient interest from members can be commenced and funded by FIRST. If you are interested in starting a SIG, please see <https://www.first.org/global/sigs/>.

Standards

Standards help our industry to adopt a common language and prevent misunderstandings. With this in mind, FIRST supported the development and maintenance of several cybersecurity standards in 2020-21:

- **ISO/IEC 29147 'Vulnerability Disclosure'**
- **ISO/IEC 30111 'Vulnerability Handling Process'**
- **ISO/IEC 27035 'Information Security Incident Management'**
- **Common Vulnerability Scoring System (CVSS):** FIRST has updated the online learning platform training for CVSS v3.1.
- **Traffic Light Protocol (TLP):** A set of designations 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 2020-21.
- **Information Exchange Policy (IEP):** a framework for defining information exchange policy and a set of standard 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 standard output format for Passive DNS servers. This standard was released in 2015 as part of an IETF RFC, and updated in the past year.

[Read more on our website.](#)



Diversity & Inclusion

The cybersecurity community continues to look for ways to increase diversity within its workforce and create inclusive environments so that all feel welcome to participate. The FIRST Board is also committed to this goal and has produced several initiatives towards achieving this:

1. FIRST's Chair Serge Droz was invited by UNIDIR to contribute a blog about 'Diversity and Cyber Resilience: Views of an Incident Responder'
<https://www.unidir.org/commentary/diversity-and-cyber-resilience-views-incident-responder>
2. The Women of FIRST, Birds of a Feather (WoF BoF), continues to grow and expand its charter.
3. This past year saw one of the most diverse groups of candidates for the Board in FIRST's history.
4. In 2021 FIRST joined forces with International Telecommunication Union (ITU) and EQUALS to create the Women in Cyber Mentorship Program for empowering women in cybersecurity. The pilot program targeted women in the Middle East and African regions interested in cybersecurity or trying to get to the next level in their careers. This program consists of:
 - FIRST Board member Shawn Richardson gave the Opening Remarks at the start of ITU's Women in Cyber Program.
 - Keynote speakers – four well-known women, talking about their careers and how they got there.
 - Technical and soft skills training by delivering six courses on professional and personal development.
 - Six months of mentoring hosted by experienced cybersecurity professionals.

Please see more information on ITU's [website](#). If you are interested in participating as a trainer or a mentor in the next session (tentatively late CY2021, Q4), please contact Shawn@FIRST.org. And thank you to Traci Wei for coordinating details with ITU.

Internet Governance & Policy

Despite COVID-19 and its impact on the world's ability to travel to meet and discuss policy issues, cybersecurity policy work continued at an even higher pace. Major incidents related to ransomware and the supply chain increased the urgency with which policymakers took an interest in cybersecurity and incident response.

As a result, FIRST contributed to many different forums throughout the year to make the incident response community's voice heard. Some of our work included:

- FIRST representatives Yukako Uchida and Koichiro Komiyama participated in an ITU initiative to develop guidance on national cybersecurity strategies.
- FIRST co-edited and signed onto [civil society feedback](#) on the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security.
- FIRST Board member Maarten Van Horenbeeck served as a lead expert to another iteration of the [IGF Best Practices Forum on Cybersecurity](#), which looked at lessons learned from norms building in non-cyber norms processes. This work will continue throughout 2021.
- FIRST continues to participate in the Global Forum on Cyber Expertise (GFCE) Working Group B, leading the task force on Cyber Incident Management.
- FIRST participated in the panel "International security and emergency response cooperation" at the EU Cyber Forum 2020, sharing perspective on emergency cybersecurity cooperation.
- FIRST's Chair Serge Droz continued the engagement with the OECD in activities to clarify the tech community's role in implementing norms and CBMs.
- FIRST's Chair Serge Droz represented FIRST as an observer in the [Geneva Dialogue](#).
- FIRST was engaged through the reporting period in DCAF's activity to improve [Cybersecurity Governance in the Western Balkan Region](#).

Continued on Page 13

Internet Governance & Policy (continued)

In all of these engagements, FIRST advocates for positions in the development of new international cybersecurity policies:

- We request that all stakeholders adopt practical measures to indicate their respective communities' roles and responsibilities and increase trust and capacity. For example, FIRST published a Code of Ethics, ethicsFIRST, which describes the duties of computer security incident responders, including a duty of confidentiality, a commitment to respect human rights, evidence-based reasoning, and increased trust and transparency.
- We appeal for states to consider how policies may negatively affect the work of incident responders and security teams. For instance, we advocate against the criminalization of security expertise. Security teams learn and build expertise from exchanging information on security incidents, defensive and offensive techniques. Any activities to limit this sharing are unhelpful.
- We request for countries and regions to build exemptions for domestic and international sanctions. The internet knows no borders, and a vulnerability exploited in one state today can be used in another tomorrow. We need to ensure the free flow of both requests for assistance, and information on new incidents and techniques, between all incident responders, regardless of where they live.
- We encourage states to review norms developed in multi-stakeholder communities, such as the Global Commission on the Stability of Cyberspace. In particular, we believe the norm to "protect the public core of the internet" has a significant value in potentially reducing the impact of security incidents.

FIRST was encouraged by the publication of the OEWG report in early 2021 and will continue to take advantage of the opportunity to provide input into UN processes.



Major Announcements & Press

To increase our global reach and awareness of FIRST among incident responders worldwide FIRST delivers an integrated communications strategy. This strategy involves building relationships with journalists, keeping our members informed, and providing members and non-members with regular updates across our social media channels.

During the last year, FIRST issued five press releases:

- **FIRST releases its 2019-20 Annual Report.**
- **FIRST jointly honors Ian Cook and Don Stikvoort in The Incident Response Hall of Fame awards.**
- **FIRST launches new code of ethics for incident response and security teams on Global Ethics Day.**
- **FIRST sees over 1600 cybersecurity professionals from 97 countries sign up for the 32nd Annual Conference.**
- **FIRST 33rd Annual Conference to be streamed live June 7-9, 2021.**

FIRST appeared in Computable, Cybersecurity News, Daily Swig, Dark Reading, InfoSecurity Magazine, Internet Watch, Portswigger, Revista Sic, Security Magazine, and Start-Up Digital. Readership covered Indonesia to the Netherlands. FIRST was also mentioned by Back End News, Cyberguerre, Finance Colombia, Help Net Security, Manila Standard, Mobile World Live, Security Intelligence, Tripwire, Wired, Zdnet Japan.

Our quarterly newsletter emailed directly to our members has sustained a readership of over 350 per issue and is well-read across the US, Europe, Middle East, and the Asia Pacific.

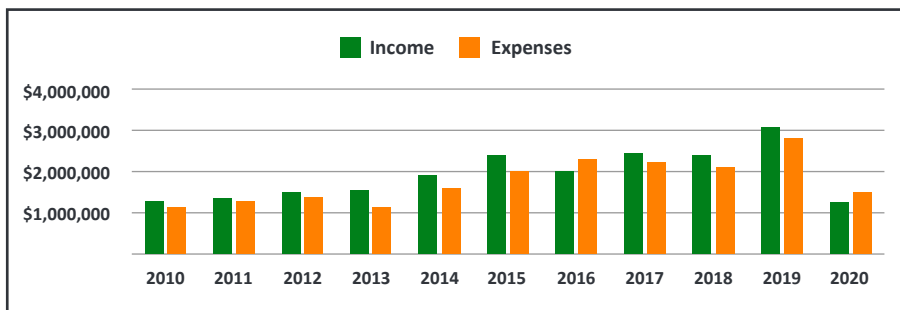
Social media reach continues to increase. We saw a 20% increase in followers across our social media channels in the past 12 months. The total number of followers is now at 14,545, with all channels, Facebook, Twitter, and LinkedIn, increasing.

Financials

2020 was a financially challenging year for FIRST. The global pandemic made in-person events too risky and impacted registration fees and sponsorship agreements, both being our main income streams. But when we reviewed planned spending for the rest of the year, the financial impact was much smaller than expected.

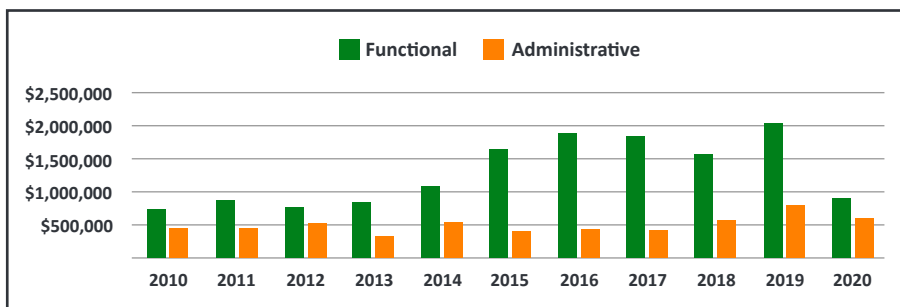
One of the lessons of the past year was to create a reserve policy tool to calculate reserves and guide us on how and when to use them. The Board formally approved this in early 2021. Under the Reserves Policy, we have set a target amount equal to six months of average operating costs. This amount is then designated such that specific Board approval is required before we can access and spend this money.

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:



The significant change in Admin vs Functional expense is, again, primarily due to the pandemic. We were unable to hold in-person events for much of 2020 – which is where much of our functional expense comes from. We were also limited in the amount of revenue raised – further restricting our ability to deliver events. Before this, we ran at a very healthy ratio of functional expense to total expense – approximately 78% over the last five years. In 2020 this ratio was 61%. Our ambition is to return to the former ratio as soon as possible.

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 provided upon request to interested parties such as grantors and sponsors. [Read more on our website.](#)

Infrastructure

Over the past year, the infrastructure team has focused on streamlining, securing, and optimizing FIRST's services and operations. Some highlights from these efforts include:

- We upgraded the FIRST Portal, including a revamped logon screen, security codes (supporting password and MFA recovery), and the addition of FIRST usernames, which will help the future use of third-party services.
- The 2021 Membership dues moved to QuickBooks Payments. This reduced payment processing fees and tightly integrates with the existing accounting platform.
- We launched the ethicsfirst.org site, and first.org registrar services were migrated to MarkMonitor, providing improved protection.
- We designed a new FIRST Groups service to support committees, working groups, SIGs, and informal groups. The full version of this service will be released soon. It will provide group leaders with improved control to manage their members and available services and allow users to join a group more easily.
- We integrated a Single Sign-On application on the FIRST learning platform and an updated course for CVSS 3.1.
- We re-worked our events mechanism to support new events, such as the 'Virtual Lightning Talks in a Box' and SIG updates. Many events are now live-streamed through the FIRST Youtube account: <https://www.youtube.com/firstdotorg>.

Several exciting efforts and projects are planned and already underway for the coming year that will continue to improve and optimize the services that FIRST provides to its members.

We look forward to providing you with a new update in 2022 and to all we'll achieve 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