



FIRST's Strategic Plan 2025-2028

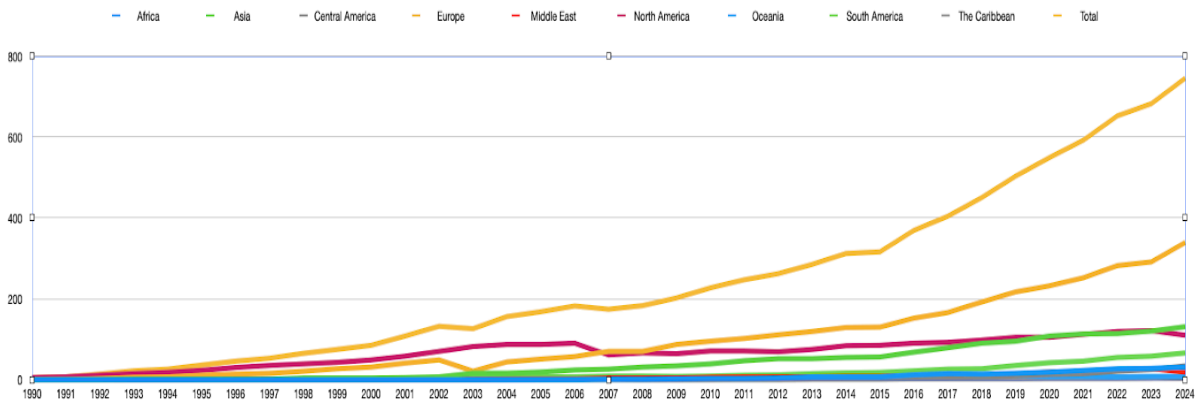
Introduction

FIRST is the Forum of Incident Response and Security Teams. The idea of FIRST goes back until 1989, only one year after the [CERT\(r\) Coordination Center](#) was created after the infamous Morris worm. Back then incidents already were impacting not only one closed user group or organization, but any number of networks interconnected by the Internet.

It was clear from then on that information exchange and cooperation on issues of mutual interest like new vulnerabilities or wide ranging attacks - especially on core systems like the Domain Name System or the Internet as a critical infrastructure itself - were the key issues for security and incident response teams.

Since 1990, when FIRST was founded, its members have resolved an almost continuous stream of security-related attacks and incidents including handling thousands of security vulnerabilities affecting nearly all of the millions of computer systems and networks throughout the world connected by the ever growing Internet. FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

FIRST has grown from five members in one single country (the United States) in 1990, to 165 [liaisons](#) and 762 teams from 111 countries, as of the date this document was written. Today, there are 26 [special interest groups](#) at FIRST, and many initiatives focused on topics like [Diversity and Inclusion](#), [Victim Notification](#), [IR \(Incident Response\) Database](#), [Malware Information Sharing Platform \(MISP\)](#), the [Incident Response Hall of Fame](#), the [Suguru Yamaguchi Fellowship Program](#), among plenty others.



Since its founding, FIRST evolved from a loose association run by volunteers into a structured organization with several staff members and a multi-million-dollar budget. As part of the growth and maturing of the organization, the work on strategic planning that the Board of Directors and the corporate Officers have performed in the past will be enhanced and strengthened. This will allow FIRST to address internal and external challenges that threaten to hinder its ability to effectively achieve its mission and solidify its role as a global leader in cybersecurity and incident response. FIRST operates within a rapidly evolving cybersecurity landscape, facing competition from similar organizations and needing to adapt to emerging trends and technologies.

A three-year Strategic Plan will provide a framework for enhancing member value, expanding global reach and diversity, and ensuring long-term financial sustainability. Through it, FIRST can leverage its strengths, such as its respected brand and global network, to solidify its position as the premier organization for incident response and security.



I. FIRST's Vision and Mission Statement	4
Strategic Alignment	4
Vision	4
Mission	4
2. Strategic Planning at FIRST	5
3. Strategic Objectives	6
4. Strategic Areas. Goals, Expected Outcomes, and Risks.	7
4.1. Strategic Area #1 - Chairship of the Board of Directors.	7
4.2. Strategic Area #2 - Finance.	8
4.3. Strategic Area #3 - Membership.	9
4.4. Strategic Area #4 - Events.	10
4.5. Strategic Area #5 - Education & Training.	10
4.6. Strategic Area #6 - Community Engagement.	11
4.7. Strategic Area #7 - Governance.	12
4.8. Strategic Area #8 - Policy.	13
4.9. Strategic Area # 9 - Community Capacity Building (CCB).	14
4.10. Strategic Area #10 - Communications and Brand Management.	15
5. Next Steps: From Strategy to Operations	16
3-Year Operating Plan	16

I. FIRST's Vision and Mission Statement

Strategic Alignment

FIRST's Strategic Plan will be aligned with its Vision and Mission Statement. This alignment is crucial for providing a unified direction for the organization, ensuring that all its activities – from member services to governance and policy engagement – directly contribute to achieving its overarching goals. Without this alignment, FIRST risks becoming fragmented in its efforts, pursuing disparate initiatives that may not effectively address the evolving cybersecurity landscape. Aligning the Strategic Plan with FIRST's mission to be a trusted source of information and thought leadership necessitates a concerted effort to enhance its global visibility, engage with policymakers, and produce high-quality research and publications.

By strategically aligning its Plan with its vision and mission, FIRST can leverage its strengths, address its weaknesses, and position itself for long-term success as the globally recognized leader in the field of incident response and cybersecurity.

Vision

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

Effective response is a global task, mirroring the global nature of the internet. Based on a peer to peer network governance model, Computer Security Incident Response Teams (CSIRTs), Product Security Incident Response Teams (PSIRTs) and independent security researchers work together to limit the damage of security incidents. This requires a high level of trust; the fuel our members run on. FIRST fosters trust building among members through a variety of activities. Incidents are not confined to one cultural or political corner of the internet, nor do they respect borders or boundaries. FIRST thus promotes inclusiveness, inviting membership from all geographic and cultural regions.

Mission

Global Coordination - You can always find the team and information you need:

FIRST provides platforms, means and tools for incident responders to always find the right partner and to collaborate efficiently. This implies that FIRST's reach is global. We aspire to have members from every country and culture.

Global Language - Incident responders around the world speak the same language and understand each other's intents and methods: During an incident it is important that people have a common understanding and enough maturity to react in a fast and efficient manner. FIRST supports teams through training opportunities to grow and mature. FIRST also supports initiatives to develop common means of data transfer to enable machine to machine communication.

Policy and Governance - Make sure others understand what we do, and enable us rather than limit us: FIRST members do not work in isolation, but are part of a larger system. FIRST engages with relevant stakeholders, in technical and non-technical communities, to ensure teams can work in an environment that is conducive to their goals.

2. Strategic Planning at FIRST

It is a fundamental part of governance at FIRST and is the first part of a structured planning process, followed by the creation and implementation of a Three-Year Operating Plan, for which an Annual Budget and Operational Plan are defined. The Strategic Plan is updated every three years, while the Three-Year Operating Plan, as well as the Annual Budget and Operating Plan, are updated every year. Each year concludes with an Achievement and Progress report through which the Board of Directors and the Chief Executive Officer and Executive Director communicate performance metrics in support of transparency and accountability.

Strategic Planning at FIRST

	Duration	Updated Every
Strategic Plan	Three years	Three years
Three-Year Operating and Financial	Three years	Year
Budget and Operational Plan	One year	Year
Achievement and Progress Report	One year	Year

As a maturing organization, during the first calendar semester of 2025 the FIRST Board of Directors, along with the Chief Executive Officer and Executive Director, will use this Strategic Plan as the basis to produce the first Three-Year Operating Plan, both of which will in turn be the basis going forward for the Annual Budget and Operational Plan. For clarity, following good finance and accounting practices, FIRST has produced an annual

budget since ____, and it will continue to do so. The only difference is that now it will be based on the Strategic Plan, the Three-Year Operating Plan, and will be part of the yearly operational plan.

Below, this document will present the five Strategic Objectives identified by the Board of Directors, with the reasoning behind them. Later, the document will lay out the ten strategic areas identified by the Board of Directors, with the goals that the organization intends to pursue in each of the areas; and, specific targeted outcomes from each, as well as the risks that may prevent such goals from being achieved.

3. Strategic Objectives

The Board of Directors has identified the following, as the Strategic Objectives that should guide the organization during the next three years, in pursuit of its Vision and Mission Statement:

1. **Global Recognition and Trust:** This objective aims to solidify FIRST's position as the leading advocate for the incident response and security community worldwide by enhancing global visibility and building partnerships with key industry stakeholders and organizations and, most importantly, delivering value beyond its constituencies. This aligns with FIRST's vision to be globally recognized and trusted.
2. **Member Value Creation:** This objective focuses on providing exceptional value to FIRST members, empowering them to excel in their incident response and cybersecurity endeavors by expanding and enhancing member services and benefits as well as strengthening member engagement and support. This aligns with FIRST's mission to support and empower the incident response community.
3. **Development and Education:** This objective aims to establish FIRST as the premier platform for industry newcomers and experienced professionals seeking to enhance their skills and knowledge in incident response and cybersecurity. This can be achieved by, for example, creating comprehensive training programs for new members, developing advanced modules and certification programs, and promoting continuous learning and professional development.
4. **Trusted Venue for Standards and Information Sharing:** This objective aims to position FIRST as the most trusted venue where its members define standards and best practices, as well as share insights and timely information on cybersecurity threats and trends. FIRST plans to achieve this by, for example, seeking enhanced information sharing from its members in its MISP instance, or increased member participation in discussions around standards development.

5. **Effective Governance and Financial Resilience:** This objective focuses on the long term strategy towards strengthening FIRST's governance structure, ensuring financial sustainability, and fostering organizational resilience to navigate evolving challenges effectively. This involves reviewing and updating governance policies, enhancing board and member engagement, diversifying funding sources, and maintaining rigorous financial management practices.

The Board of Directors has identified ten Strategic Areas through which these objectives will be achieved, all of which are below with the detail of the goals to be pursued in each area, along with their respective expected targeted outcomes, and the risks that may prevent their realization.

4. Strategic Areas. Goals, Expected Outcomes, and Risks.

The following sections outline the strategic goals, desired outcomes, and potential risks for each of the ten strategic areas. Each one contributes to achieving the five overarching strategic objectives outlined above.

4.1. Strategic Area #1 - Chairship of the Board of Directors.

Strategic Goals

- Provide overall leadership and direction to the FIRST Board of Directors.
- PEstablish a clear agenda for Board meetings, ensuring focused discussions and productive outcomes.
- PFoster effective communication and collaboration among Board members and between the Board and staff.
- POversee the implementation of the Strategic Plan, monitor progress towards goals, and hold individuals accountable for their responsibilities.

Expected Outcomes

- PBoard members actively engage in strategic discussions and contribute effectively to decision-making, while increasing meeting productivity.
- PA strong and collaborative working relationship exists between the Board and staff, fostering trust and mutual respect.
- PThe Strategic Plan is successfully implemented, and FIRST makes tangible progress towards achieving its objectives.
- PThe Chair effectively represents FIRST in external engagements, advocating for the organization's mission and values.

Risks

- Lack of experience or leadership skills in incoming chairs could hinder effective Board leadership.
- Ineffective communication or collaboration within the Board or between the Board and staff could impede progress.
- Over-reliance on historic approaches versus innovative ways.
- External factors, such as geopolitical tensions or global cybersecurity incidents, could divert attention from strategic priorities.

4.2. Strategic Area #2 - Finance.

Strategic Goals

- Ensure the financial health and stability of FIRST, enabling the organization to pursue its mission effectively.
- Develop and implement a diversified funding strategy to reduce reliance on any single income source.
- Optimize financial efficiency, minimize unnecessary expenses, and ensure responsible and conscious resource allocation.
- Provide transparent and accountable financial management, complying with relevant regulations and best practices.

Expected Outcomes

- FIRST achieves and maintains a balanced budget or budget surplus used to fill the strategic reserve, strengthening its financial position.
- Diversified funding sources provide financial stability and reduce reliance on membership fees or event revenue.
- Improved financial controls and processes enhance efficiency and reduce the risk of financial mismanagement.
- Transparent financial reporting to the Board, members, and stakeholders fosters trust and accountability.
- Prioritizes investments that demonstrate a clear potential for long-term returns on investment (ROI) based on the impact to our mission.
- Ensure financial preparedness for urgent needs or economic slowdowns that may impact membership and require resource allocation.
- Implement a policy to diversify assets across multiple financial institutions, including maintaining relationships with at least two banks in different countries to mitigate risks, address past challenges, and account for geopolitical considerations.

Risks

- Difficulty in securing funding from diverse sources could limit financial flexibility.
- Unforeseen economic downturns or global events could impact FIRST's financial stability.
- The volatility in income streams hinder long term financial planning.
- Lack of qualified individuals with financial management expertise on the Board could hinder effective financial oversight.

4.3. Strategic Area #3 - Membership.

Strategic Goals

- Retain existing FIRST members by providing exceptional value and fostering a strong sense of community.
- Attract new members from diverse regions and sectors, expanding FIRST's global reach and impact.
- Develop a clear and easy-to-follow membership application process that encourages participation.
- Explore new membership categories or tiers to cater to the evolving needs of the incident response and security community.

Expected Outcomes

- Increased membership applications and a steady growth in FIRST's member base.
- Improved member retention rates, indicating high satisfaction with FIRST's services and benefits.
- A more geographically diverse membership, enabling FIRST to address global cybersecurity challenges effectively.
- New membership categories or tiers attract organizations that previously did not meet the membership criteria, broadening FIRST's reach and expertise.

Risks

- Rapid membership growth could strain resources and dilute the sense of community among members.
- Competition from similar organizations, such as regional or sector-specific cybersecurity groups, could limit membership growth.
- Geopolitical tensions or sanctions could restrict membership from certain countries or regions, impacting FIRST's global inclusivity.

4.4. Strategic Area #4 - Events.

Strategic Goals

- Organize events that provide significant value to FIRST members and the wider cybersecurity community, fostering knowledge sharing, networking opportunities, and professional development.
- Expand the geographical diversity of FIRST events, particularly in regions like Latin America, Asia Pacific and Africa.
- Explore new event formats and topics to address emerging trends and challenges in cybersecurity.
- Ensure the financial sustainability of events, balancing ticket prices (particularly to members of FIRST), sponsorship opportunities, and cost management.

Expected Outcomes

- High quality content that drives, among other factors, increased attendance and participation in FIRST events, reflecting their relevance and value to the community.
- Successful execution of regional symposia in underrepresented areas, expanding FIRST's global engagement.
- New event formats and topics attract diverse audiences and address emerging cybersecurity challenges.
- Events generate revenue that supports FIRST's activities while remaining affordable to members.
- High quality content

Risks

- High event costs, especially for international conferences, could make them inaccessible to some members, particularly those from developing countries.
- Competition from other cybersecurity events could limit attendance and sponsorship opportunities.
- Unforeseen circumstances, such as global pandemics or geopolitical events, could lead to event cancellations or reduced participation.

4.5. Strategic Area #5 - Education & Training.

Strategic Goals

- Position FIRST as a leading provider of high-quality education and training programs for incident response and security professionals at all levels.

- Develop and deliver training materials that are current, relevant, and aligned with industry best practices and international standards.
- Expand the pool of qualified FIRST trainers and mentors to provide diverse perspectives and expertise.
- Ensure training programs are accessible to global stakeholders, addressing language barriers and regional needs.

Expected Outcomes

- Increased demand for FIRST training programs, reflecting their quality and relevance to the cybersecurity community.
- Constructive feedback from training attendees, demonstrating the effectiveness of the curriculum and trainers.
- A larger and more diverse pool of FIRST trainers and mentors, offering a wider range of expertise.
- Greater adoption of international cybersecurity standards and best practices by FIRST members and the broader community.

Risks

- Rapid technological advancements and evolving cyber threats could lead to outdated training content if not regularly updated.
- Lack of qualified trainers, especially in specific regions or languages, could limit training accessibility.
- Limited financial resources could hinder the development of new training materials and programs.

4.6. Strategic Area #6 - Community Engagement.

Strategic Goals

- Cultivate a vibrant and active FIRST community where members and volunteers feel valued, supported, and empowered to contribute.
- Provide clear and rewarding opportunities for members to volunteer their time and expertise, contributing to FIRST's mission.
- Recognize and appreciate the contributions of volunteers, fostering a culture of appreciation and belonging.
- Promote diversity and inclusion within the FIRST community, ensuring representation from various backgrounds, regions, and sectors.

Expected Outcomes

- Increased volunteer engagement in FIRST activities, demonstrating a strong sense of community and shared purpose.
- Positive feedback from volunteers, indicating they feel valued and their contributions are appreciated.
- A more diverse and inclusive FIRST community, reflecting the global nature of cybersecurity challenges.
- Improved collaboration and knowledge sharing among FIRST members through volunteer-led initiatives.

Risks

- Lack of clear communication or processes for volunteer engagement could lead to frustration or disengagement.
- Insufficient resources or support for volunteer-led initiatives could limit their effectiveness.
- Unintentional exclusion of certain groups or perspectives could hinder diversity and inclusion efforts.
- SIGs becoming too independent or inactive, potentially diverging from FIRST's overall strategic direction.

4.7. Strategic Area #7 - Governance.

Strategic Goals

- Ensure that FIRST's governance structure is robust, transparent, and accountable, enabling effective decision-making and organizational agility.
- Develop and implement clear policies and procedures that guide FIRST's operations and ensure compliance with relevant regulations.
- Identify and define criteria to recruit and retain qualified and diverse Board members who bring valuable skills, experience, and perspectives to the organization.
- Facilitate a smooth and efficient transition process for new Board members, ensuring continuity and effective knowledge transfer.

Expected Outcomes

- A well-defined and documented governance framework that outlines areas, responsibilities, and decision-making processes.
- A diverse and experienced Board of Directors that effectively represents the interests of FIRST members and stakeholders.

- Transparent and accountable decision-making processes that foster trust and confidence in FIRST's leadership.
- A seamless transition process for new Board members, ensuring they can effectively contribute to FIRST's mission.

Risks

- Resistance to change or a lack of consensus among Board members could hinder the implementation of governance improvements.
- Difficulty attracting and retaining qualified and diverse Board members could limit the effectiveness of governance oversight.
- Lack of resources or support for governance-related activities could hamper progress and create inefficiencies.
- Ensuring that the governance structure and the base of operations for the organization holds the most competitive advantage to accomplish the Mission and the Strategic Objectives.

4.8. Strategic Area #8 - Policy.

Strategic Goals

- Position FIRST as a trusted and influential voice in global cybersecurity policy discussions, advocating for the needs of incident responders and security practitioners, while bringing recognition to the value they generate.
- Engage with international organizations, governments, and other stakeholders at the policy level to help educate them when needed, so they can shape effective cybersecurity policies that promote a safer and more secure online environment.
- Develop clear and well-informed positions on key cybersecurity policy issues, representing the collective expertise of FIRST members.
- Educate policymakers and the public on the importance of incident response and the role of FIRST in strengthening global cybersecurity.

Expected Outcomes

- Increased recognition of FIRST as a neutral thought leader and influencer in global cybersecurity policy circles.
- Establishment of strategic partnerships with key international organizations and governmental bodies involved in cybersecurity policy development.
- FIRST's positions on cybersecurity policy issues help create better international frameworks and agreements.

- Greater awareness among policymakers and the public of the importance of incident response and FIRST's contributions to a safer online environment.

Risks

- Lack of access or limited influence within international policymaking bodies could hinder FIRST's ability to effectively advocate for its positions.
- Geopolitical tensions and a lack of trust between nations could make it challenging to achieve consensus on critical cybersecurity policy issues.
- Limited resources or internal disagreements within the FIRST community could affect the organization's ability to engage effectively in policy discussions.
- International organizations potentially co-opting FIRST's work or implementing similar initiatives could diminish the impact of FIRST's efforts.
- Incident response becomes politicized, threatening FIRST's ability to act as a neutral body.

4.9. Strategic Area # 9 - Community Capacity Building (CCB).

Strategic Goals

- Strengthen global cybersecurity resilience by supporting the development of incident response capabilities in underrepresented regions and communities.
- Expand access to FIRST's expertise, resources, and training programs to empower a diverse range of individuals and organizations to combat cyber threats.
- Foster collaboration and knowledge sharing between established and emerging incident response teams, promoting a global culture of cybersecurity awareness and preparedness.
- Secure sustainable funding for CCB initiatives to ensure long-term impact and reach.

Expected Outcomes

- New incident response teams and communities established or strengthened in underrepresented regions, particularly in developing countries.
- Increased participation of individuals from underrepresented groups in FIRST activities and the broader cybersecurity community.
- Improved communication and collaboration between incident response teams globally, facilitating knowledge exchange and joint efforts to address cyber threats.

- Sustainable funding mechanisms in place to support the continued growth and impact of CCB initiatives.

Risks

- Difficulty in securing sustainable funding for CCB programs could limit their scope and longevity.
- Lack of local support or infrastructure in some regions could hinder the effectiveness of capacity-building efforts.
- Difficulties in retaining skilled cybersecurity professionals in developing countries could undermine the long-term impact of capacity building.
- The potential need for prioritization due to limited resources could create challenges in addressing all areas in need.

4.10. Strategic Area #10 - Communications and Brand Management.

Strategic Goals

- Enhance FIRST's brand awareness and reputation globally, positioning the organization as the trusted authority on incident response and security.
- Develop and implement a comprehensive communications strategy that effectively reaches target audiences, including members, potential members, policymakers, and the public.
- Promote FIRST's activities, achievements, and contributions to cybersecurity through various channels, such as media outreach, social media, and online platforms.

Expected Outcomes

- Increased media coverage and positive portrayal of FIRST in relevant publications and online platforms.
- Growth in FIRST's social media presence and engagement, reflecting broader awareness and interest in the organization's activities.
- Increased engagement from FIRST members and the public with FIRST's communications, demonstrating the effectiveness of messaging and outreach efforts.

Risks

- Lack of resources or expertise in communications could limit the effectiveness of outreach and brand-building efforts.
- Inconsistent messaging or a failure to tailor communications to specific target audiences could dilute the impact.
- Negative publicity or reputational damage from external sources could harm FIRST's brand image.
- Over-reliance on a single communications channel or approach could limit reach and impact.

5. Next Steps: From Strategy to Operations

3-Year Operating Plan

Defining the Strategic Plan is a crucial first step. The next stage involves developing a three-year Operating Plan to translate the strategic objectives and goals into actionable steps, so that the expected outcomes can be achieved while the corresponding risks are mitigated. This Operating Plan outlines:

- **Specific activities:** Always aiming at achieving the Vision and Mission Statement as well as the five Strategic Objectives outlined above in Section III. This is the breakdown of each strategic objective into smaller, manageable tasks.
- **Timeline:** A clearly defined timeframe for each activity, including start and end dates.
- **Responsibilities:** Assigned ownership of each activity to specific individuals or teams within FIRST.
- **Resources:** Resources needed for each activity, like budget, personnel, or technology.
- **Metrics:** Key performance indicators (KPIs) to measure progress and success for each activity and objective. Conclusions

This three-year Strategic Plan provides a framework for FIRST to strengthen its position as the global leader in security and incident response. By focusing on global recognition and trust, member value creation, development and education, becoming a source of expertise and information, and ensuring effective governance and financial resilience, FIRST can continue to advance its mission and support the evolving needs of the cybersecurity community.



The success of this plan depends on the commitment and collaboration of FIRST's Board of Directors, staff, members, and partners. By working together, FIRST can navigate the complex and ever-changing cybersecurity landscape and contribute to a safer and more secure online environment for all.