DIGITAL RESILIENCE OF SWISS FOUNDATIONS

Threat Landscape & Recommendations

CyberPeace Institute

With the support of:

REPUBLIC AND STATE OF GENEVA

POST TENEBRAS LUX

Executive Summary

Swiss foundations play a critical role in advancing philanthropic missions but face rising cybersecurity threats in an increasingly digital world. This report by the CyberPeace Institute, supported by the Republic and State of Geneva, assesses the digital resilience of Swiss foundations and reveals a fragmented cybersecurity landscape. While larger foundations often have dedicated resources, smaller ones operate with limited protections, making them more vulnerable to sophisticated threats.

The report identifies six key challenges: low awareness and training, limited budgets, lack of board-level expertise, inconsistent security practices, fragmented efforts, and restricted access to shared resources. To address these, it recommends targeted training for staff and boards, integrating cybersecurity into governance through dedicated budgets and policies, and mutualizing resources via shared services and expert networks. It also calls for fostering innovation through pilot programs and certifications, encouraging collaboration through peer learning and partnerships, and leveraging external support, including initiatives like CyberPeace Builders.

This report is a call to action: digitale resilience must become a strategic priority for Swiss foundations.

Résumé

Les fondations suisses jouent un rôle essentiel dans la poursuite de missions philanthropiques, mais elles sont confrontées à des menaces croissantes en matière de cybersécurité dans un monde de plus en plus numérique. Ce rapport du CyberPeace Institute, soutenu par la République et Canton de Genève, évalue la résilience numérique des fondations suisses et révèle un paysage fragmenté en matière de cybersécurité. Alors que les grandes fondations disposent souvent de ressources dédiées, les plus petites fonctionnent avec une protection limitée, ce qui les rend plus vulnérables à des menaces sophistiquées.

Le rapport identifie six défis majeurs : un manque de sensibilisation et de formation, des budgets limités, un manque d'expertise au niveau du conseil de fondation, une incohérence des pratiques de sécurité, une fragmentation des efforts et un accès restreint aux ressources partagées. Pour y remédier, il recommande de dispenser des formations ciblées au personnel et aux conseils de fondation, d'intégrer la cybersécurité dans la gouvernance au moyen de budgets et de politiques spécifiques, et de mutualiser les ressources par le biais de services partagés et de réseaux d'experts. Il préconise également de favoriser l'innovation par des programmes pilotes et des certifications, d'encourager la collaboration par le partage de bonnes pratiques et les partenariats, et de tirer parti d'un soutien externe, notamment d'initiatives telles que le programme CyberPeace Builders.

Ce rapport est un appel à l'action : la résilience digitale doit devenir une priorité stratégique pour les fondations suisses.

Foreword

Stéphane Duguin

,

Chief Executive Officer, CyberPeace Institute

The digital age has brought unprecedented opportunities and challenges for organizations worldwide, including Swiss foundations. As the CEO of the CyberPeace Institute, I am acutely aware of the critical importance of cybersecurity in safeguarding the valuable work of our philanthropic community. This report, stemming from our 2023 study of cyber threats affecting the International Geneva, a workshop with Swiss Foundations on March 19, 2024, and a subsequent survey, highlights both the digital vulnerabilities and resilience of Swiss foundations.

The findings reveal indeed a landscape where awareness and preparedness vary significantly across organizations. While some foundations have adopted advanced security measures, many still rely on basic protections, leaving them susceptible to sophisticated cyber threats. The identified challenges – from resource constraints to a lack of expertise and cohesive governance – underline the urgent need for a strategic and collective approach to cybersecurity.

This is a concern not only for Swiss foundations themselves but also for their grantees. New insights from the CyberPeace Tracer platform, launched in 2025, shed light on the cyber threat landscape faced by grantees including those based in Switzerland. They have experienced numerous cyber incidents in the last years, including ransomware attacks, DDoS attacks, and hack-and-leak operations. More than 500 technical vulnerabilities affecting 73 grantees my team monitors, underscore the growing urgency to strengthen their protection —beginning with the donors who support them.

This report provides actionable recommendations to address these challenges. By adopting them, Swiss foundations can significantly bolster their cybersecurity posture. The CyberPeace Institute remains committed to supporting these efforts. I invite all stakeholders to join us in building a safer digital environment for all.

Sincerely,
Stéphane Duguin, CEO, CyberPeace Institute

Call to Action

To address these challenges and leverage the opportunities identified in the report, Swiss foundations must adopt a proactive and collective approach to cybersecurity. The following actions are essential:

1. Enhancing Awareness and Training: Implement targeted training programs and continuous education initiatives to bridge the knowledge gap in cybersecurity. Utilize existing events and platforms to maximize outreach and impact.

2. Mutualizing Resources: Establish platforms and mechanisms for sharing cybersecurity resources, tools, and best practices. Encourage collective procurement and create networks of cybersecurity experts to support foundations and their beneficiaries.

3. Integrating Cybersecurity into Governance: Advocate for dedicated budget allocations for cybersecurity and integrate cybersecurity expertise at the board level. Develop and regularly update comprehensive cybersecurity policies. Update the Swiss Code of Foundations accordingly.

4. Fostering Innovation and Adaptation: Promote cybersecurity certifications, pilot innovative solutions, and implement recognition programs to motivate foundations to enhance their security measures.

5. Encouraging Collaboration and Experience Sharing: Set up forums and networks for experience sharing, document and disseminate best practices, and foster partnerships with cybersecurity organizations and academic institutions.

6. Utilizing External Support: Leverage initiatives like CyberPeace Builders and foster public-private partnerships to access additional resources, expertise, and funding for cybersecurity initiatives.

Purpose of the Report

This report aims to provide a comprehensive overview of the current state of cybersecurity among Swiss foundations, based on insights gathered from a workshop held in March 2024 and a subsequent survey of participants. The primary objectives of this project, supported by the Republic and State of Geneva, were to identify the key challenges these foundations face in terms of cybersecurity, to analyze the effectiveness of current practices, and to propose actionable recommendations for enhancing their security posture and the one of their beneficiaries. By addressing these issues, the report seeks to foster a more resilient and secure environment for Swiss foundations, enabling them to continue their philanthropic missions with greater confidence.

Background

On March 19, 2024, the CyberPeace Institute organized a workshop at the Campus Biotech to discuss the pressing issue of cybersecurity within Swiss foundations. This event brought together representatives from the public sector, members of the philanthropic community, and cybersecurity experts. The primary goal was to facilitate an open dialogue on the challenges these foundations encounter and to explore potential solutions.

In conjunction with the workshop, a survey was conducted among the participants to gather additional insights and feedback. This survey, which received responses from ten participants (five in French and five in English), provided valuable data on the current cybersecurity practices, challenges, and needs of Swiss foundations. The combined findings from the workshop and the survey form the basis of this report.

The report is structured to first present a summary of the meeting, followed by an analysis of the survey results. The largest section of the report focuses on recommendations and next steps, providing a roadmap for Swiss foundations to enhance their cybersecurity measures effectively. By taking a collective and strategic approach, Swiss foundations can significantly improve their resilience against cyber threats, ensuring the sustainability and security of their philanthropic efforts.

1. Workshop Summary

a. Key Challenges Identified

During the workshop, several critical challenges were highlighted:

Financial Risk and Fraud Management

Financial fraud emerged as the primary concern for many foundations. Existing mechanisms for verifying payments and beneficiaries illustrate a partial awareness of these risks, particularly following successful attacks. However, these measures are often isolated and not systematically applied across the foundation ecosystem. Testimonies during the workshop also highlighted the increasing sophistication of attacks, including the use of artificial intelligence, making it imperative to adopt more robust fraud detection and prevention strategies.

Case Studies

Case Study #1: Audio Deepfake CEO Fraud in a Swiss Foundation

Background

A prominent Swiss foundation recently fell victim to a sophisticated cyber-attack involving an audio deepfake. The attackers mimicked the voice and expressions of the Foundation's Director to orchestrate a CEO fraud scheme aimed at the financial team.

Incident Overview

The fraud attempt unfolded when the foundation's financial team received a phone call that sounded unmistakably like their Director. The voice deepfake was so convincing that it successfully deceived two out of three team members. The caller, impersonating the Director, provided instructions to authorize a substantial disbursement.

What saved the foundation from financial loss was the vigilance of the third team member. Sensing something was off, this individual decided to use a secondary communication channel to verify the request directly with the Director. This step confirmed the fraud and thwarted the attack.

Attack Tactics

Several factors highlighted the sophistication and preparation behind this attack:

- Voice Mimicry: The deepfake technology convincingly replicated the Director's voice, including specific expressions and nuances.
- Targeted Personnel: The attackers accurately identified and contacted key individuals within the financial team, demonstrating an in-depth understanding of the foundation's internal processes.
- Pre-Attack Research: The attackers had evidently conducted thorough research, gathering contact details and understanding the foundation's disbursement procedures. This level of preparation suggested the involvement of well-prepared, determined cybercriminals, rather than typical scammers.

Implications for Cybersecurity

This case underscores the growing threat of deepfake technology in cyber fraud. As generative AI and video deepfakes become more advanced, these types of attacks will likely become more prevalent and harder to detect. Foundations and similar organizations, which may not consider themselves prime targets, need to be particularly vigilant.

Lessons Learned and Recommendations

- Secondary Verification Channels: Always use secondary channels to confirm sensitive requests, especially those involving financial transactions.
- Awareness Training: Regular training for all employees on recognizing deepfake threats and understanding the importance of verification procedures.
- Monitoring and Controls: Implement robust monitoring systems and internal controls such as role based permissions or dual approval systems to detect and prevent unauthorized transactions.
- Increase Awareness of Online Exposure: Limit the availability of executive videos and audio clips online to reduce the risk of deepfake creation.
- Collaboration with Experts: Partner with cybersecurity experts to stay informed about emerging threats and to implement advanced protective measures.

Conclusion

The attempted CEO fraud on this Swiss foundation serves as a critical reminder of the evolving nature of cyber threats. Deepfakes powered by generative AI present new challenges in the realm of cybersecurity. By staying informed and proactive, organizations can protect themselves against these sophisticated attacks and ensure the security of their operations.

Case Studies

Case Study 2: Impersonation Scams Targeting a Swiss Foundation

Background

A prominent foundation was recently targeted by cybercriminals employing a sophisticated impersonation scam. This case underscores the growing threat of social media and email scams designed to exploit the reputation and trust associated with philanthropic organizations.

Incident Overview

The scam began with the creation of fake social media profiles and email addresses impersonating a well-known philanthropist associated with the foundation. These fraudulent profiles engaged with potential victims on platforms like Instagram, building rapport through seemingly genuine interactions.

One such target was approached by an individual claiming to be the philanthropist. After initial friendly exchanges, the scammer shifted the communication to email, using an address closely mimicking the philanthropist's name. They promised a substantial donation of $800,000, contingent upon the target using the funds for business ventures and charitable causes. To proceed with the disbursement, they requested personal information, including full name, home address, and telephone number. Such information can then be used for identity theft, or in preparation of the next steps of the scam, which involve luring the target into transferring some funds to the scammer, the latter arguing this is required to obtain the substantial donation.

The scammer's approach included specific details about the foundation's operations and disbursement processes, indicating a high level of preparation and understanding. Fortunately, the target contacted the foundation via other channels, which prevented any financial loss. The foundation had advised potential beneficiaries to confirm any offers directly through official channels, a practice that the target followed, ultimately exposing the scam.

Attack Tactics

Several key tactics were employed by the scammers:

- Impersonation: Using the name and likeness of a prominent philanthropist to gain the trust of potential victims.
- Social Media Engagement: Initial contact and rapport-building through fake social media profiles.
- Email Fraud: Transitioning to email communications using addresses that closely resemble those of legitimate figures.
- Detailed Pretext: Providing convincing details about donations and disbursement requirements to lend authenticity to their claims.
- Information Gathering: Requesting sensitive personal information under the guise of processing the donation.

Implications for Cybersecurity

This case highlights the increasing prevalence and sophistication of impersonation scams targeting foundations. As scammers continue to refine their tactics, including detailed pretexts and realistic communications, foundations must adopt robust measures to protect themselves and their beneficiaries.

Lessons Learned and Recommendations

- Verification Protocols: Implement and enforce strict verification protocols for any financial transactions or offers. Encourage beneficiaries to confirm the legitimacy of offers through official channels.
- Awareness Training: Conduct regular training sessions for staff and beneficiaries on recognizing and responding to impersonation scams.
- Proactive Monitoring: Regularly monitor social media platforms and online presence for fake profiles and fraudulent activities involving key figures associated with the foundation.
- Clear Communication: Maintain transparency about grant processes and known scams on the foundation's website. Include a dedicated section to educate the community about potential threats.
- Reporting Mechanisms: Establish and promote easy-to-use mechanisms for reporting suspected scams. Collaborate with social media platforms and law enforcement to take down fraudulent accounts swiftly.

Conclusion

The impersonation scam targeting this foundation serves as a critical reminder of the evolving nature of cyber threats. By adopting proactive and comprehensive cybersecurity measures, foundations can safeguard their operations and protect their community from sophisticated scams. The lessons learned from this incident underscore the importance of vigilance, education, and robust verification processes in maintaining the integrity and trust of philanthropic organizations.

Awareness and Training

A significant issue identified was the lack of cybersecurity awareness and knowledge among foundation staff, particularly in smaller entities and among board members. Many foundations, especially those with limited digital transformation, mistakenly believe they are immune to cyber-attacks. While some training initiatives exist, they are often insufficient, underlining the need for continuous and tailored awareness programs at all organizational levels.

Budgetary and Organizational Challenges

One of the central issues discussed was the lack of specific budget allocations for cybersecurity. Many foundations underestimate the risks, leading to inadequate funding for necessary security measures for their own needs. Consequently, there is also a lack of demand for cybersecurity funding from the beneficiaries they support, perpetuating a cycle of underinvestment.

Our previous research on the threats facing the International Geneva highlighted a similar challenge for foundations' beneficiaries. The lack of awareness among board members results in cybersecurity not being prioritized during budget planning. As a consequence, NGOs do not actively seek cybersecurity resources, and foundations fail to provide them.

Disparities and Lack of Cohesion

The workshop revealed significant disparities within the ecosystem of Swiss foundations. Large organizations tend to be better equipped with resources and cybersecurity measures, whereas small and medium-sized entities are more vulnerable. This disparity is further exacerbated by a lack of resource and knowledge sharing. A cohesive approach to cybersecurity, including mutualization of resources and collaborative efforts, is essential to address these gaps.

2. Survey Analysis

a. Methodology

The survey conducted among the participants of the March 19, 2024, workshop aimed to gather additional insights into the cybersecurity practices, challenges, and needs of Swiss foundations. The workshop brought together approximately 40 foundations from both the French-speaking region and other parts of Switzerland. To maintain confidentiality, the foundations' names will not be disclosed. About 25% of participants completed the survey—5 responses in English and 5 in French—and the report, along with the subsequent recommendations, is based on these responses. The survey questions were designed to capture data on participants' awareness of cybersecurity issues, current practices, specific challenges they face, and their feedback on the workshop's effectiveness. The full survey results are available in the next part of the report.

b. Key Findings

The survey results provided valuable information on the state of cybersecurity within the foundations, highlighting both strengths and areas for improvement.

Awareness Levels

The survey revealed varying levels of awareness and knowledge of cybersecurity among the respondents. While some participants demonstrated a good understanding of cybersecurity principles and practices, others showed significant gaps yet an interest. This disparity underscores the need for targeted awareness programs to bridge the knowledge gap, particularly among smaller foundations and board members with limited understanding of cybersecurity requirements and necessities.

Key Statistics:

- High Awareness: 40% of respondents rated their cybersecurity awareness as high.
- Moderate Awareness: 30% of respondents rated their cybersecurity awareness as moderate.
- Low Awareness: 30% of respondents rated their cybersecurity awareness as low.

Current Practices

The survey responses highlighted the diverse range of cybersecurity measures currently in place within the foundations. Larger organizations generally have more comprehensive practices, including regular audits, advanced threat detection systems, and dedicated IT security staff. In contrast, smaller foundations often rely on basic measures such as antivirus software and password protection, with limited access to advanced cybersecurity resources.

Key Practices Identified:

- Regular Security Audits: 50% of respondents conduct regular security audits.
- Advanced Threat Detection: 30% of respondents use advanced threat detection systems.
- Basic Security Measures: 70% of respondents rely on basic security measures like antivirus software and password protection.

Challenges and Needs

Respondents identified several challenges that hinder their ability to effectively manage cybersecurity:

- Resource Constraints: Limited financial and human resources dedicated to cybersecurity.
- Lack of Expertise: Difficulty in accessing skilled cybersecurity professionals.
- Awareness Gaps: Insufficient awareness and training for staff and board members.
- Fragmented Efforts: Lack of coordinated efforts and knowledge sharing among foundations.

In terms of support and resources needed, participants expressed a strong desire for more accessible training programs, shared resources, and expert guidance to help them navigate the complexities of cybersecurity.

Top Needs Identified:

- Training Programs: 80% of respondents indicated a need for more training programs.
- Expert Guidance: 70% of respondents expressed a need for expert advice and support.
- Shared Resources: 60% of respondents highlighted the importance of access to shared cybersecurity resources.

c. Conclusion

The survey revealed varying levels of awareness and knowledge of cybersecurity among the respondents. While some participants demonstrated a good understanding of cybersecurity principles and practices, others showed significant gaps yet an interest. This disparity underscores the need for targeted awareness programs to bridge the knowledge gap, particularly among smaller foundations and board members with limited understanding of cybersecurity requirements and necessities.

3. Recommendations

Based on the insights from the workshop and the survey results, the following recommendations and next steps are proposed to enhance cybersecurity among Swiss foundations. These recommendations aim to address the key challenges identified and leverage existing strengths within the foundation community.

a. Enhancing Awareness and Training

A significant gap in cybersecurity awareness and knowledge was identified among foundation staff and board members, particularly in smaller entities. To address this, the following strategies are recommended:

- Targeted Training Programs: Develop and implement comprehensive training programs tailored to the specific needs of foundation staff and board members. These programs should cover fundamental cybersecurity principles, risk management, and best practices for protecting digital assets.
- Use of Existing Platforms: Leverage established events and platforms, such as the Swiss Foundation Day, to deliver cybersecurity awareness sessions and training workshops. This approach can help reach a broader audience and integrate cybersecurity into the broader conversation about foundation management.
- Continuous Education: Establish a culture of continuous learning by offering regular updates and refresher courses on emerging cybersecurity threats and solutions. Online courses, webinars, and interactive workshops can be utilized to keep foundation staff and board members informed and prepared.

b. Resource Mutualization

Resource constraints, particularly among smaller foundations, pose a significant challenge to implementing robust cybersecurity measures. To address this, the following actions are recommended:

- Shared Services Platform: Create a platform for sharing cybersecurity resources, tools, and best practices among foundations. This platform can include access to threat intelligence, security templates, and incident response playbooks.
- Collective Procurement: Encourage collective procurement of cybersecurity solutions and services. By pooling resources, foundations can benefit from economies of scale, reducing costs and gaining access to higher-quality services.
- Expert Networks: Develop networks of cybersecurity experts who can provide pro bono or subsidized consulting services to foundations. Initiatives like CyberPeace Builders can be expanded to offer more comprehensive support to a larger number of foundations.

c. Integrating Cybersecurity into Governance

To ensure sustained attention and resources for cybersecurity, it is crucial to integrate it into the governance frameworks of foundations, such as the Swiss Code for Foundations. The following recommendations can help achieve this:

- Budget Allocation: Advocate for dedicated budget allocations for cybersecurity within foundation budgets and grants. This can be achieved through awareness campaigns targeting foundation leadership, emphasizing the importance of cybersecurity as a strategic priority.
- Board-Level Expertise: Include cybersecurity expertise at the board level by appointing members with relevant backgrounds or providing cybersecurity training for existing board members. This integration ensures that cybersecurity is considered in decision-making processes and governance practices.
- Policy Development: Develop and implement comprehensive cybersecurity policies and procedures that align with best practices and regulatory requirements. These policies should be regularly reviewed and updated to address evolving threats and vulnerabilities.

The Swiss Code of Foundations:
https://www.swissfoundations.ch/wp-content/uploads/2022/02/SFC_2021_FR.pdf

d. Fostering Innovation and Adaptation

Encouraging innovation and adaptation in cybersecurity practices can help foundations stay ahead of emerging threats. The following strategies are recommended:

- Cybersecurity Certifications: Develop and promote cybersecurity certifications or labels for foundations that meet specific security standards. These certifications can serve as benchmarks for best practices and motivate foundations to enhance their cybersecurity measures.
- Pilot Programs: Launch pilot programs to test and evaluate innovative cybersecurity solutions, such as advanced threat detection systems, blockchain for secure transactions, and artificial intelligence for threat analysis. Successful pilots can be scaled and shared with the broader foundation community.
- Recognition and Incentives: Implement recognition programs and incentives for foundations that demonstrate exemplary cybersecurity practices. Awards, public acknowledgments, and grants for cybersecurity initiatives can motivate foundations to prioritize and improve their security measures.

e. Encouraging Collaboration and Experience Sharing

Collaboration and experience sharing among foundations can significantly enhance collective cybersecurity resilience. The following actions are recommended:

- Forums and Networks: Establish forums and networks for foundations to share experiences, challenges, and solutions related to cybersecurity. Regular meetings, conferences, and online discussion groups can facilitate knowledge exchange and foster a collaborative approach to cybersecurity.
- Case Studies and Best Practices: Document and share case studies and best practices from foundations that have successfully implemented cybersecurity measures. These resources can serve as practical guides and inspiration for other foundations looking to enhance their security posture.
- Partnerships: Encourage partnerships between foundations, cybersecurity organizations, and academic institutions. These collaborations can provide access to cutting-edge research, expert advice, and additional resources for cybersecurity initiatives.

Case studies from International Civil Society Organizations can be found here: https://solidarityaction.network/key-activities/strengthening-cybersecurity/

f. Utilizing External Support

External support can play a critical role in helping foundations improve their cybersecurity measures. The following recommendations can help foundations leverage available support effectively:

- CyberPeace Builders Initiative: Expand the CyberPeace Builders initiative to provide more comprehensive support to a larger number of foundations. This support can range from awareness training to incident response and ongoing cybersecurity consulting.

More information about the CyberPeace Builders program in Geneva can be found here: https://cyberpeaceinstitute.org/cybersecure-geneva/

- Public-Private Partnerships: Foster public-private partnerships to access additional resources, expertise, and funding for cybersecurity initiatives. Government agencies, private sector companies, and philanthropic organizations can collaborate to support the cybersecurity needs of foundations.
- Grant Programs: Develop grant programs specifically targeted at enhancing cybersecurity within foundations. These grants can fund training programs, technology upgrades, and other initiatives aimed at improving cybersecurity resilience.

g. Conlusion

Implementing these recommendations requires a concerted effort from all stakeholders within the foundation community. By enhancing awareness and training, mutualizing resources, integrating cybersecurity into governance, fostering innovation, encouraging collaboration, and utilizing external support, Swiss foundations can significantly improve their cybersecurity posture. These measures will not only protect the foundations themselves but also ensure the security and sustainability of their philanthropic missions. As cyber threats continue to evolve, a proactive and collective approach to cybersecurity is essential for safeguarding the valuable work of Swiss foundations.

4. Conclusions

The urgency of addressing cybersecurity within the Swiss foundation ecosystem cannot be overstated. As cyber threats continue to evolve, foundations must recognize that cybersecurity is not merely a technical issue but a critical component of good governance and organizational resilience. By taking collective and strategic actions, foundations can protect their operations, secure their digital assets, and ensure the sustainability of their philanthropic missions.

The recommendations and next steps outlined in this report provide a roadmap for Swiss foundations to enhance their cybersecurity posture effectively. By working together and committing to continuous improvement, Swiss foundations can build a more secure and resilient future for their organizations and the communities they serve.

The key points highlighted in this report are:

1. Awareness and Training Deficiencies: There is a notable lack of cybersecurity awareness and training, particularly among smaller foundations and older board members. This gap poses a significant risk as cyber threats become increasingly sophisticated.

2. Resource Constraints: Many foundations, especially smaller ones, face financial and human resource constraints that hinder their ability to implement robust cybersecurity measures. This includes insufficient budget allocations and a lack of skilled cybersecurity professionals.

3. Governance and Policy Gaps: Cybersecurity is often not integrated into the governance frameworks of foundations such as the Swiss Code of Foundations, resulting in inadequate strategic focus and resource allocation. This issue is compounded by the absence of cybersecurity expertise at the board level.

4. Disparities in Cybersecurity Practices: There is a significant disparity in the cybersecurity practices of large versus small foundations. While larger foundations may have comprehensive security measures, smaller entities often rely on basic protections, leaving them vulnerable to attacks.

5. Need for Collaboration and Resource Sharing: The fragmented efforts and lack of coordinated action among foundations underline the necessity for collaboration and mutualization of resources to enhance collective cybersecurity resilience.

6. Positive Workshop Feedback: The feedback from the workshop participants was overwhelmingly positive, highlighting the value of such events in fostering knowledge exchange and collaboration. There is a clear demand for more interactive and practical sessions in future workshops.

About Us

CyberPeace Institute Offering

The Institute has created an extensive set of tools and services that can assist Swiss foundations in overcoming the challenges outlined in the report. These resources aim to bolster the missions of foundations by addressing key cybersecurity concerns.

1. Assessment: Foundations and their grantees can complete a General Cybersecurity Assessment (GCSA) to identify vulnerabilities and receive recommendations aligned with frameworks like NIST and Cyber Essentials. The assessment will focus on the following key cybersecurity areas:
    - Assets and user management
    - Endpoint and network security
    - Remote access and cloud services
    - Backup
    - Public-facing digital perimeter security
    - Multi-Factor Authentication (MFA) and password management
    - Cybersecurity awareness
    - Dark web and active logs monitoring
    - Governance (policies)

An example GCSA report is provided with this proposal. More details about our GCSA can be found here.

2. Alerts and Individual reports: Foundations and their grantees can access detailed threat intelligence we collect on them aggregating commercial data, and receive alerts about immediate threats, alongside specific action plans. These plans will prioritize resource-efficient solutions and guide Foundations and their grantees through a roadmap for continuous improvement.

More information about our threat intelligence services can be found here.

3. Volunteer Support: to address the vulnerabilities identified by our in-house threat analysts and bridge the gaps surfaced by the GCSA, NGOs will have access to the CyberPeace Builders volunteers, a network of over 1,30 corporate cybersecurity volunteers for targeted missions, including cybersecurity awareness training, phishing simulations, vulnerability assessments, cybersecurity policy development, and more. Attached to this proposal you will find a detailed list of our current volunteer-led missions, bearing in mind NGOs can also request custom support. Our volunteers have already provided over 2500 hours of support in over 1000 different missions, for more than 500 different Foundations and grantees across the globe.

More information about our CyberPeace Builders programme can be found here.

4. Training: We provide training, AI-driven insights, and tabletop exercises to help nonprofits and foundations strengthen their cybersecurity. Our programs build skills, improve threat detection, and enhance response strategies, ensuring Foundations and their grantees can protect their mission and the communities they serve.

More information about the CyberPeace Academy can be found here.

5. Tools: Access to free cybersecurity tools and guides negotiated with partners, including solutions for phishing protection, threat detection, vulnerability scanning, and more. As a founding member of Nonprofit Cyber we know of, and can recommend many cybersecurity tools that others provide for free.

More information about these tools can be found here.

6. Community Building: Foundations and their grantees will be part of a growing nonprofit cybersecurity community, enabling peer learning, best practice sharing, joint advocacy and community alerts.

More information about our cybersecurity community and campaigning activities can be found here.