Photo Credit: Digital Empowerment Foundation

INSPIRA ADVISORY AND CONSULTING

Outcome Collection | October 2023

South Asia Regional Digital Initiative (SARDI)

USAID FROM THE AMERICAN PEOPLE
DigitalFrontiers SCALING DIGITAL DEVELOPMENT
DAI Shaping a more livable world.

DISCLAIMER This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of DAI and do not necessarily reflect the views of USAID or the United States Government. This publication/report/guide was produced under DAI's Digital Frontiers Project (Cooperative Agreement AID-OAA-A-17-00033) at the request of USA

BUY-IN OVERVIEW

- Client: USAID/India and Indo Pacific Office, Digital Connectivity and Cybersecurity Partnership initiative (DCCP)
- Period of Performance: May 16, 2022 – June 30, 2023
- Budget: $192,343

In 2022, the Bangladeshi government launched Bangladesh Vision 2041, a strategy for the country's digitization, designed to propel Bangladesh towards its goal of becoming a high-income country by 2041. However, the dangers that accompany digitization will present significant barriers to the execution of this vision. In Bangladesh, cybercrime is prevalent and severely affects households and businesses. Cybercrimes and digital harms like malware and ransomware attacks, online scams, cybertheft, cyberbullying, digital property destruction, and the spread of fake news drain resources from the nation's economy and endanger individual citizens.

Micro, small, and medium enterprises (MSMEs) in Bangladesh are particularly exposed to cybersecurity threats. Since the early 2010s, these businesses have gradually adopted IT-enabled services and digital tools. The COVID-19 pandemic further accelerated the digital transformation as traditional MSMEs turned to digital tools and online platforms to sustain their operations. Additionally, many of the country's urban and rural youth are emerging as online entrepreneurs by leveraging social media and e-commerce platforms.

However, despite increases in exposure to cyber threats, entrepreneurs in Bangladesh have limited knowledge about the severity and impacts of these threats, as well as measures that could protect their businesses from them. Many MSME owners have little formal education and low digital literacy levels, and they often fall victim to cyberattacks or cybercrimes. To address this issue, USAID's South Asian Regional Digital Initiative (SARDI) launched the Cybersecurity Awareness Campaign for MSMEs through a grant to the Bangladeshi consulting firm Inspira Consulting to enhance the cybersecurity practices of Bangladeshi MSME owners and improve their personal and business-related digital hygiene.

Three aspects of Inspira's program distinguish it from other Digital Frontiers programming. First, Inspira has used the lessons learned from previous cybersecurity awareness campaigns such as Online Safety in Cambodia and Only Mine in Mongolia to inform its activities, adding a new stratum to Digital Frontiers' layered understanding of awareness-raising across multiple contexts. Second, Inspira's iterative approach to program design is uniquely innovative among Digital Frontiers interventions, charting a path of alternating implementation and evidence gathering that continually increases the project's knowledge base. Finally—and most importantly—Inspira's wide-ranging experiments with awareness-raising strategies that incorporated music, social media, board games, community meet-ups, workshops, and more generated significant learnings about cybersecurity awareness campaigns that can help shape future cybersecurity initiatives.

SUMMARY OF OUTCOMES

1. **Built capacity and awareness of cybersecurity threats and safeguards among MSME owners in 7 key economic districts.** E-commerce businesses are a vital driver of economic growth in Bangladesh: in 2022, there were 70 percent more e-commerce businesses in the country than in the previous year. This makes the entrepreneurial market segment a growing target for cyber criminals. Responding to this threat, Inspira launched an online cybersecurity awareness campaign that reached 3.4 million users; through this campaign, Inspira attracted 846 highly motivated MSME e-business owners to attend 12 in-person workshops. These workshops increased participants' scores on post-activity cybersecurity knowledge assessments by an average of 30 to 40 percentage points.
2. **Developed and deployed processes for innovative, human-centered program design; innovated and rapidly prototyped innovations, adapting them to fit the local context and development needs.** Inspira's proposed interventions navigated the complex social and cultural aspects of Bangladesh's digital landscape with creativity, innovation, and cultural competence. Inspira's initial design proposed engaging popular media personalities and holding *uthan baithak* (courtyard meeting) sessions and *gombhira* (traditional musical theater) performances to complement a phased online campaign that would build users' cybersecurity skills by scaffolding new information on top of already-built knowledge. However, when these strategies showed need for improvement, Inspira used the minimum viable product (MVP) approach to rapidly iterate on them, and in some cases, pivot entirely from the designs initially proposed to DAI. This flexible approach allowed successful interventions to organically emerge.
3. **Drove demand among MSME owners and larger Bangladeshi society for cybersecurity services.** Due to low awareness of cyber threats among Bangladeshis, demand for cybersecurity services is lacking in the country's digital landscape. For example, while one-third of MSME owners report having experienced a cyberattack, 62 percent of them do not think that their business is at any risk from such attacks. To bridge this awareness gap, the Inspira team established deep working partnerships with 14 organizations in the Bangladesh e-commerce space, including public-sector actors, financial institutions, and business organizations. Through these collaborations, Inspira has catalyzed demand for cybersecurity upskilling in the country: a handful of these partners have expressed a willingness to pay for additional tailored cybersecurity training content from Inspira for their members and staff. Meanwhile, to meet individual entrepreneurs' demand for cybersecurity services, Inspira collaborated with the Dhaka-based cybersecurity firm Backdoor Private Ltd. to launch a one-stop service desk (OSD) that accepts cybersecurity-related queries 24/7. Within its first six months of operation, the OSD received 393 queries and 30 cybersecurity incident reports—24 of which were resolved, a resolution rate nearly double that of relevant Bangladeshi regulatory authorities. Further, post-buy-in interviews and anecdotal data suggest that OSD users trust the service more than cyber law enforcement officials.

STUDY OVERVIEW

Overall, this study aims to identify robust outcomes that resulted from the South Asia Regional Digital Initiative (SARDI) buy-in's Cybersecurity Awareness Campaign for MSMEs activity implemented by Inspira Consulting. Through qualitative interviews at the grassroots level, analysis of project reports and documentation, and project-wide surveys, the evaluation team sought to answer three core questions:

1. What were the key achievements from the Inspira activity?
2. How did the activity specifically contribute to the identified outcomes, and what would have happened in the absence of the intervention?
3. What lessons were learned from producing these results?

This study developed outcome stories that incorporated evidence generated from three main sources:

1. **Assessment study**: In September 2022, Inspira staff conducted an assessment study to identify the needs of Bangladesh's unique cybersecurity landscape. Inspira surveyed 500 MSME owners in four different industries across seven target districts and conducted nine focus group discussions and 17 key informant interviews with MSME owners, ecosystem actors, and regulatory and implementation actors in the cybersecurity space.
2. **Interviews with field staff, key stakeholders, and activity part**: In May 2023, DAI staff conducted a four-day field visit in the cities of Dhaka and Narayanganj, Bangladesh. We interviewed seven members of Inspira's project team and organizational leadership, as well as three cybersecurity experts affiliated with the activity. Additionally, we observed a cybersecurity upskilling workshop in Narayanganj held in partnership with the Women and e-Commerce Forum (WE)—a local business organization representing female e-commerce entrepreneurs, most of whom sell goods on Facebook Marketplace. Following this visit, we conducted four small virtual focus groups, focused on beneficiaries in different regions of Bangladesh, with a total of ten focus group participants. These qualitative data are not representative of the program on the whole; rather, they serve as illustrative case studies that augment the narrative outlined by the quantitative data.
3. **Periodic reports**: Inspira's quarterly activity reports include a series of case studies on workshop participants and OSD users, which provided valuable information for this report. The evaluation team also employed a thorough document review of the buy-in's solicitation documents and Inspira's proposals, interim deliverables, and Inspira's final grant report.

Analysis involved systematically interrogating the outcome claims across interviewees and datasets, collecting data using semi-structured, open-ended methodologies, and noting and addressing contradictory perspectives in the rare instances they appeared.

OUTCOMES

OUTCOME #1: CAPACITY AND AWARENESS BUILT AMONG MSME OWNERS

PROBLEM AND APPROACH

In a climate of increasing digitalization—and thus, increased risk of cyberattacks—Bangladeshi MSMEs are insufficiently prepared for safeguarding their online business presences. MSMEs are a main driver of Bangladesh's economy, accounting for a quarter of all domestic employment and 80 percent of export earnings. These businesses are rapidly increasing their online presences: in 2022, there were 70 percent more e-commerce businesses operating in Bangladesh than the previous year. However, Inspira's studies have shown that most MSME owners do not understand what cybersecurity is, let alone how to implement it for their businesses.

According to Inspira's baseline needs assessment, 69 percent of survey respondents knew the term "cybersecurity," but only a minority could identify any specific cybersecurity threats. Among entrepreneurs with low exposure to digital tools, only 57 percent of respondents had heard of the concept of cybersecurity. Moreover, few entrepreneurs said they were concerned that cyber threats could harm them or their businesses. Typically, even "ardent adopters"—business owners who have had significant exposure to digital tools—reported they were not worried about losing business information or money online. Less than a quarter of "ardent" respondents cited these losses as possible risks of operating online.

In response to these survey results, Inspira launched the "Bebshay Digital Shurokkha" (Digital Business Security) campaign, which included a Facebook page for spreading information about cybersecurity practices, a network of local Facebook groups for interacting directly with business owners, a website with a library of resources in the Bangla language and a cybersecurity awareness self-assessment, and a series of in-person workshops for participants to receive hands-on training and ask questions in real time.

Inspira's campaign activities lie on a spectrum between maximizing *reach* (the number of target participants who see the campaign) and *conversion/action potential* (the number of target participants who engage with the campaign and increase their knowledge, change their attitudes, or adopt new practices) based on the cybersecurity-focused messaging. This spectrum can also be conceptualized as a funnel: at the widest point, Inspira maximizes the number of people reached, but compromises on conversion potential; at the narrowest, Inspira reaches relatively few target participants, but does so using methods that maximize action potential.

At the widest point of the funnel, Inspira conducted mass outreach campaigns through posts on its Facebook page and in partner business associations' Facebook groups. The goal is not to change people's behavior (unless such change occurs incidentally), but rather to increase digital engagement with Inspira and the Bebshay Digital Shurokkha brand. This awareness can be partially quantified by measuring the campaigns' total Facebook post reach: 3.4 million Facebook users by the end of the campaign. This outreach strategy also aims to increase the audience's knowledge of cybersecurity, which is the first step to ultimately affecting their attitudes and practices. When these campaign posts receive comments and shares, this represents interest—signaling to Inspira that the content is relevant and meets the audience's needs.

Social media posts that occupy the funnel's "middle ground" encourage interested individuals to engage directly by messaging with the Inspira team on Facebook, using the OSD, taking the online cybersecurity knowledge self-assessment quiz, or attending an in-person workshop. The extent to which people engage with these options shows their desire to interact more, which leads them further down the funnel.

Inspira's workshops represent the narrowest end of the funnel. While the number of workshop participants—846 as of April 2023—is far smaller than the more than one million target participants reached through social media posts, participants showed a great degree of behavior change and knowledge gain from these workshops.

OUTCOME

Since Inspira began activity implementation, partners' digital literacy and cybersecurity awareness levels increased gradually from a generally low base awareness level. Some participants in Inspira's online and in-person programs are highly digitally literate (these participants reside in Dhaka or are employed in a job in a high-tech industry), while others have a very little digital literacy. Lower-skilled participantstend to come from peripheral, underserved geographies and industries that require less formal education; for example, entrepreneurs who belong to the Bogura Chamber of Commerce or those who run light engineering firms. Most members of such organizations use "button phones"—not smartphones—but they are increasingly using the Internet to access Facebook, often under pressure from their digitally literate children.

When lower-literacy participants enter an in-person workshop, they often express skepticism about the value of cybersecurity knowledge. In one example, a participant claimed that online security was a "cosmetic measure" that was irrelevant for his business. After the workshop ended, the same participant volunteered examples of online risks he faced, signaling that he understood the cyber risks his business faced.

Through DAI's interviews of participating entrepreneurs in diverse geographical areas across Bangladesh, we found that entrepreneurs consistently demonstrated increased cybersecurity awareness post-training. This validates the knowledge gains indicated in the results of the pre- and post-knowledge assessments: the study observed an average 30 to 40 percentage point improvement following workshop completion, with one-third of workshop participants reporting they now used the knowledge learned in the workshops. When asked what specific skills they developed through participating in Inspira's workshops, each of the entrepreneurs DAI interviewed were able to identify one or more. Setting up two-factor authentication and creating strong passwords for accounts were the most frequently mentioned, as well as the practice of opening a business Facebook page not linked to one's personal Facebook account. Another relatively complex social media strategy that many respondents retained and implemented was using their personal Facebook account to create multiple personal pages, which would in turn become the admins of their business Facebook page. Thus, if one page became compromised, the business page could still be recovered using a "backup" personal account.

Since the workshops, several participants noted that they were more interested in taking their businesses online than before. One entrepreneur from Narayanganj reported that she was previously unconvinced that she should create a virtual "storefront" on a personal web domain, but after taking Inspira's workshop, she decided to do so and has started selling her goods online. She also has increased her business aspirations, saying, "Now, I have the potential for worldwide reach, where before I was limited locally by Facebook." Another entrepreneur, who was inspired to create a LinkedIn profile, said, "I wasn't spending time or attention on social media before, but now I'm motivated to do the work to create my profile in earnest." While it is still to early to assess increases to business income, number of customers, or sales, numerous entrepreneurs we interviewed mentioned that they were experimenting with new digital tools.

One major change in program participants' attitudes around cybersecurity is their increased confidence in the face of cyber threats. Several Inspira staff noted that before entrepreneurs' exposure to the online campaign, most of them did not know that there was any recourse to data or financial loss incurred from cyberattacks. Before training, almost none of the participants reported having ever contacted law enforcement or police about cyber crimes they witnessed or fell victim to. When the workshops began, two-thirds of participants said that going to the police was a waste of time, and many of them preferred to visit local "IT experts" who were often fraudulent or unqualified, and either stole participants' money or failed to solve the MSME owners' issues. In contrast, after the workshops, Inspira's cybersecurity expert consultant observed that MSME business owners had set up digital security and contingency plans; participants felt that they knew who would be able to help them in case of cybersecurity or digital emergency and how to reach them

SIGNIFICANCE

With increased cybersecurity awareness, entrepreneurs also reported increased confidence in the future of their businesses. Pre-workshop, several business owners had heard stories of e-commerce entrepreneurs who had lost access to their business page or were infected with malware, and this left them with seemingly no other option than to delete their online presence and start over. The perceived possibility of losing weeks or months of hard work, therefore, made entrepreneurs disinclined to grow their digital presences. However, after learning about and implementing improved cybersecurity practices and safeguards, business owners reported they were more confident digital tools would benefit them in the long run and were more willing to expand their businesses online.

Learning about cybersecurity also allows more digitally literate business owners to incorporate cybersecurity awareness and services into their interactions with clients. For instance, one interviewee from Dhaka primarily helps his clients produce social media content. However, in one instance, as he helped one of his clients fix a link that had been hijacked by hackers, he was redirected to a malware site instead of the client's product page. The same participant now reminds his clients about cybersecurity best practices by forwarding them Inspira's Facebook posts; when Inspira posts about changing one's password every three months, he changes his password and notifies his clients to do so as well.

Increased cybersecurity awareness provides value that goes beyond Bangladeshi entrepreneurs' businesses and increases safety in their personal lives. For example, one entrepreneur at an Inspira workshop reported that her husband asks her to remember his passwords for him and that her 12-year-old daughter watches pirated anime using Twitter. After the workshop, she identified these as significant cyber risks that could result in data breaches that would affect her family's safety and decided to propose alternative digital habits to her family. A representative of the SME Foundation, one of Inspira's partners owned by the Bangladesh government, also cited the case of a high-profile news story where several girls who ran TikTok accounts had been kidnapped. As cybersecurity awareness increases among business owners in Bangladesh, similar risks and incidents can be avoided, making community members safer as well.

WHAT REMAINS TO BE DONE?

As Inspira's cybersecurity expert consultant explains, the work of increasing cybersecurity awareness has no defined end-goal as the landscape of cybercrime is always evolving. As cyber criminals proliferate and escalate their threats for MSME owners, Inspira must constantly update its strategies for delivering assistance to affected entrepreneurs. For example, in the first half of 2023, Facebook—the largest e-commerce platform in Bangladesh—changed at least 37 settings and policies relating to cybersecurity, all of which affect Inspira's ability to inform their target audience.

Inspira also has additional work to do in engaging with Facebook as a partner institution to combat cyber threats in Bangladesh: many of Inspira's resources are replacements for and supplements to

Facebook's inadequate cybersecurity help pages and support resources regarding cyber threats to Facebook users and business pages.

Finally, small business owners see Inspira's network as a multipurpose platform for them to connect and share information. In addition to increasing their cybersecurity awareness, many entrepreneurs wish to learn about other digital literacy topics like digital marketing, Facebook post boosting and Facebook ads, and topics and skills helpful for business development like branding and photography. Inspira can foster spaces for entrepreneurs to discuss these topics and share best practices as part of its expanded mandate to meet Bangladeshi MSME owners' needs for safe online business expansion.

LESSONS LEARNED:

- **MSME owners need to incorporate a "human touch" into their cybersecurity support.** Sometimes business owners' cybersecurity issues are as psychological as they are material. Inspira's support team is trained equally in cybersecurity and digital technologies and customer service, allowing them to offer help to distressed entrepreneurs who may have limited understanding of a cybersecurity problem and difficulty articulating the specifics of their problem. Inspira's cybersecurity expert consultant emphasized the importance of the "two blue ticks" that signify their message sent to Inspira through Facebook Messenger or WhatsApp has been opened. Simply knowing that a human support staff has seen their query affords entrepreneurs peace of mind and a feeling of connection with Inspira's support staff.
- **Align cybersecurity campaigns' platforms and tactics with the activity's strategic objectives.** Inspira's campaign tactics included diverse activities taking place in different contexts—from Facebook posts to musical theater performances, to lecture-heavy workshops, and even board games. Each of these tactics is ideally aligned with Inspira's overall objective and is planned to occupy a particular position on the spectrum between target participant reach and conversion/action potential. Since Inspira has shown that few, if any, intervention methods can achieve both wide reach and deep action potential, program designers must understand the tradeoff between these two outcomes, and carefully choose the correct interventions based on the intended outcome.

  There is more to learn and quantify regarding the effectiveness tradeoffs between different messages and campaign strategies. For example, the ratio of users reached to users who take action for each step along the spectrum has yet to be measured. Defining this ratio—how much reach must be sacrificed for a marginal conversion, and vice versa—will assist future implementers to select and design the correct tools for desired outcomes.

OUTCOME #2: PROCESS ESTABLISHED FOR INNOVATIVE, HUMAN-CENTERED INTERVENTION DESIGN

DESIGN CHALLENGES

Based on the example of Digital Frontiers' Only Mine cybersecurity campaign in Mongolia—which featured high-profile Mongolian musicians—one of Inspira's proposed interventions at the beginning of the activity harnessed popular Bangladeshi actors' platforms to spread messages of cybersecurity awareness. However, when Inspira piloted this influencer-based intervention design, they found that it encouraged limited uptake, as few members of the target audience—entrepreneurs—were not already knowledgeable about cybersecurity. Thus, this strategy's audience was shown to reach an audience of largely non-target users.

Additionally, Inspira's initial proposal called for the production of 20 *uthan baithak* (courtyard meeting) sessions and six *gombhiras* (traditional musical theater performances). However, Inspira implemented a single *uthan baithak* session before canceling the remainder of the sessions; when convening the pilot *uthan baithak*, the activity team found that local MSME owners were not available to be in their courtyards at the scheduled meeting time, so this approach was unsuccessful in reaching the target audience.

Inspira's proposed social media campaign, which followed educational best practices for increasing knowledge and awareness, was designed to gradually scaffold cybersecurity concepts for the target audience. The social media content built in complexity over the course of the campaign, starting with basic cybersecurity knowledge and offering more advanced concepts by campaign's conclusion. However, the implementation team found that participants with minimal digital literacy knowledge who engaged with the campaign months into its implementation—as more advanced cybersecurity concepts were presented—were unable to catch up to participants who had engaged from the campaign's start.

Through confronting these implementation challenges and others, presented below, Inspira showed the advantages of an iterative approach to activity development that adjusts based on the beneficiaries' human experience.

UNIQUE APPROACH

Inspira and its partner organizations stay informed of state-of-the-art international development practices to create effective intervention campaigns. For the cybersecurity awareness campaign in Bangladesh, Inspira employed the minimum viable product (MVP) strategy—a particularly innovative approach in the international development space. Often, development partners use a deductive methodology, collecting and analyzing data to develop a deep understanding of a development context before proposing and executing a strategy that addresses the development challenges identified in initial research. In contrast, by using MVP, Inspira followed an inductive methodology to quickly launch prototype intervention models and test them in the real-world development context.

Rather than using global best practice to assess Bangladeshi SME owners' cybersecurity needs, the Inspira team first used available literature and documentation of previous cybersecurity campaigns in the Global South to start iterating on its Bangladeshi interventions immediately, in the earliest stages of the activity. While Bangladeshi governmental and financial institutions have previously run cybersecurity campaigns, Inspira had no access to high-quality datasets or analyses of those campaigns as it launched its interventions in Bangladesh. Additionally, Inspira's cybersecurity intervention was the first to target MSMEs as the main audience, an approach that encouraged them to adopt a more experimental intervention methodology.

The Inspira team also used personal self-reflection and expertise gained from living in the development context—in other words, local knowledge—to design interventions. The implementation team also used informal interviews—in essence, friendly conversations—with members of their existing networks of microentrepreneurs and personal acquaintances, such as with local *kirana* (convenience or general store) shop owners. As Inspira's networks already included numerous MSME owners from previous projects, the team members found informal polling and "temperature-checking" to be a simple and effective way to collect initial pilot data. Despite this information's limited applicability, unscientific collection, and potential for bias, Inspira used it as a proxy to run "thought experiments" on many of the proposed interventions and receive immediate feedback on their hypothesized theories of change. The informal interviews Inspira conducted during the design phase informed the planning and piloting of proposed interventions—even before the data collection tools for the initial needs assessment were developed—thus jumpstarting the implementation cycle and enabling significant innovation without undergoing an extensive design process.

INNOVATION AND ADAPTATION

Throughout Inspira's use of the MVP approach, they developed multiple prototype interventions that they pursued simultaneously. The activity team contends that the concurrent execution of activities had numerous distinct advantages compared to a hypothetical approach focused on a single data-driven prototype activity. Some elements of Inspira's use of the MVP approach in Bangladesh are detailed below.

> **Targeting cybersecurity messages to MSME owners**—After Inspira's social media strategy using well-known media personalities reached a predominantly non-target audience, the Inspira team modified the approach and used administrators of microentrepreneur Facebook groups as "business influencers" to convey cybersecurity messages in spaces that were tailored to the target audience. This approach was more successful than previous campaign strategies because it directly engaged target participants rather than casting a wide net that ultimately sent messaging to Facebook users who were not part of the campaign's target audience.
>
> **Pivoting from unsuccessful proposals**—Following the limited success of the *uthan baithak* (courtyard meeting) strategy, Inspira's team pivoted from their proposed plan in favor of leveraging their relationship with the Dhaka-based SME Foundation; Inspira's mobile activation unit began visiting SME fairs, seasonal events where microentrepreneurs gather to sell goods and learn business practices from one another.
>
> Inspira also pursued a postering and door-to-door education campaign in industrial and commercial clusters. However, this was shown to be time-inefficient at reaching substantial numbers of entrepreneurs: business owners were unwilling to meet cybersecurity trainers during business hours, and one-on-one training was difficult compared to group training. As a result, the Inspira team explored ways to engage entrepreneurs after hours, when the entrepreneurs would meet to drink coffee and talk shop while playing board games. This catalyzed Inspira to produce a cybersecurity-focused board game, which they distributed to the entrepreneurs and coffee shops where they met.
>
> Moreover, at the first *gombhiras* (musical theater performances) Inspira ran, attendance was shown to be low and have a relatively minor impact on participants' cybersecurity knowledge, attitudes, and practices. As a result, Inspira chose to halve the number of *gombhira* events—eliminating the planned *gombhiras* in more cosmopolitan areas of Bangladesh while retaining performances in rural areas with distinct local cultures and dialects. In these locations, *gombhiras* communicated cybersecurity messaging more effectively than digital resources like Facebook.

Iterating to take advantage of complementarities—Inspira initially encountered representatives from Bangladesh's SME Foundation while performing outreach to Bangladeshi entrepreneurs at SME fairs, where they would be able to access many members of the target group at the same time. The relationship with the SME Foundation resulted in the two entities collaborating to run the in-person cybersecurity workshops, with the SME Foundation serving as an outreach liaison with local business organizations across Bangladesh to recruit participants. The SME Foundation's ability to reach many entrepreneur contacts within trusted organizations in key strategic geographies and industries then allowed Inspira to access new groups of entrepreneurs without sacrificing the depth of their engagement.

Pursuing contextual solutions over global best practices—As users with various digital literacy levels engaged with Inspira at different phases of its social media campaign, the organization chose to adjust its cybersecurity-related posting strategy from one that followed a progressive increase in informational complexity to one that made cybersecurity information clearly accessible to Facebook users of all digital literacy levels. Under the new strategy, Inspira only introduced new cybersecurity information in Facebook posts once per week and re-posted older content on the remainder of the days. This allowed participants with more basic knowledge to begin engagement at any point of the campaign, while still maintaining the attention of the more knowledgeable audience.

LESSONS LEARNED

- **The MVP approach requires staff to code-switch**. Due to the deep knowledge of the local context needed to design interventions tailored to beneficiaries' personal experiences and needs, the success of the MVP strategy for cybersecurity awareness hinges on team members who are grounded, empathetic, good communicators, and adept code-switchers, equally comfortable in all dialects and social registers. Since the project staff engaged stakeholders from across the social spectrum, from Bangladeshi government officials, to USAID Mission staff, to microentrepreneurs in diverse cultural and linguistic regions of Bangladesh, the project's success depended on implementers to be culturally competent in numerous contexts.
- **Including diverse subject-area experts is crucial to developing innovative programming**. During implementation, Inspira staff employed multidisciplinary approaches informed by their backgrounds in various disciplines. One of the project's principal trainers and cybersecurity experts, for example, has professional credentials in cybersecurity, communications and marketing, and psychology. Owing to the team's diverse backgrounds and experience in wide-ranging subjects, Inspira's ideation sessions were influenced by methodologies not commonly incorporated in international development strategy. Inspira's successive iterative planning sessions guided by expert staff ultimately yielded unique and high-impact interventions.
- **The MVP approach requires trusting partnerships**. The funder-grantee relationship between DAI and Inspira was built on trust and flexibility, and allowed the Inspira team to achieve unique successes as they pursued the MVP approach to activity iteration. The MVP strategy is largely ineffective when operating entities are constrained by rigid contracts; this was the case with a previous client, when Inspira was limited by contractual terms that limited Inspira's mobility and left them unable to adapt to the specific development context. As a result, the performance of that intervention suffered.

OUTCOME #3: DROVE DEMAND FOR CYBERSECURITY SERVICES

PROBLEM AND APPROACH

Despite Bangladesh's accelerating digitization—and its concomitant need for increased awareness of cyber threats—demand for cybersecurity services is not proportional to the actual level of need for these services; many more MSMEs require cybersecurity services than are aware or take advantage of them. Before Inspira began its intervention, there were no comprehensive cybersecurity or digital hygiene trainings, courses, or workshops available for Bangladeshi MSMEs. Moreover, Inspira found in their digital landscape assessment in Bangladesh that while one-third of MSME owners had experienced a cyberattack, 62 percent of MSME owners did not think that their business was at risk from cyber threats.

Predictably, there is little recourse for cyberattack victims after these incidents, especially among entrepreneurs with lower digital literacy levels, almost half of whom decline to report their incidents to law enforcement. Although there are no standard terms in the Bangla language to describe various cyberattack methods, several interviewed entrepreneurs described their experiences of falling victim to cybercrime as *loss khawa*—literally, absorbing or "eating" the data and financial losses, demonstrating the feeling of futility in the face of online risks.

In response to these issues, Inspira has employed three main approaches: first, they catalyzed partnerships with business organizations, financial institutions, and government entities to build institutional support for mainstreaming cybersecurity services in Bangladesh; second, they integrated marketing and consumer psychology into their in-person and online training content (including the first-ever digital public library of cybersecurity resources in the Bangla language); and third, they set up the one-stop service desk (OSD) to continue to engage social media users and workshop participants after they first interact with Inspira, providing them a channel to receive real-time assistance for their cybersecurity inquiries.

OUTCOME

Inspira has significantly magnified demand for cybersecurity and digital literacy services in Bangladesh through their partnerships in three organizational spheres—business organizations, government entities, and financial institutions—as well as through the OSD. The OSD is accessible through a portal on Inspira's website, a Facebook messaging service, and a WhatsApp number. OSD users can converse with cybersecurity professionals and receive answers and resolutions to their cybersecurity and digital hygiene queries; Inspira has contracted with Backdoor Private Ltd., a firm working in the Bangladeshi cybersecurity space, to staff the help desk 24/7.

Several of Inspira's business organization partners in business organizations have not only provided venues and recruited participants for the activity's cybersecurity workshops, but because of the enthusiasm and interest of their members, have repeatedly expanded the scope of their engagement with Inspira by holding additional workshops and sustaining engagement on Facebook groups, such as hosting conversations on cybersecurity and publicly polling their members how they implement digital hygiene in their businesses.

Two of Inspira's most-engaged partners, the e-Commerce Association of Bangladesh (e-CAB) and the Women and e-Commerce Forum (WE), have signaled interest in paying for workshops outside the initial scope of the activity. Inspira accounts for the mental health aspects of digital safety in their cybersecurity workshops, which led to WE requesting additional workshops to allow 300 of their members to receive training that explored the psychological ramifications of social media use. Inspira has also drawn similar interest from primary schools in two Bangladeshi cities that hope to offer such cybersecurity trainings.

Inspira's nascent partnerships with two government-owned institutions, Aspire to Innovate (a2i) and the SME Foundation, have also bolstered citizen participation in cybersecurity upskilling. When Inspira inaugurated its partnership with the SME Foundation, the government entity acted as a broker to connect Inspira with numerous business organizations across Bangladesh, catalyzing Inspira's widespread provision of cybersecurity services like workshops and direct incident-based assistance. Meanwhile, a2i, among other public-sector actors, is currently working with Inspira to create a national school-age curriculum so that Bangladeshi minors can receive reliable information on the risks and threats they may encounter online. A2i is also leveraging Inspira's cybersecurity and awareness-raising expertise to produce online cybersecurity video campaigns.

Inspira's financial institution partners, the Bangladesh Rural Advancement Committee (BRAC) Bank and Bank Asia, have repeatedly used Inspira's services for training their staff on cybersecurity awareness and teaching them how to spread messages of cybersecurity awareness to MSMEs—who are critically underserved as a target audience for financial cybersecurity education. In October 2022, Bank Asia ran an awareness campaign among its members for Cybersecurity Awareness Month, but the messaging was targeted towards consumers—not entrepreneurs. However, in 2023, Inspira influenced Bank Asia to include Bangladeshi small businesses as a distinct campaign target audience.

Even other banks, such as Mutual Trust Bank (MTB) and Standard Chartered, are now sending their customers cybersecurity campaign messages by SMS year-round—not only during Cybersecurity Awareness Month in October—although the attributability of this outcome to Inspira's efforts cannot be verified. Nevertheless, these messaging trends are reflective of the growing understanding among Inspira's financial partners that cybercrime is a profound business financial risk, but they can mitigate the risk to businesses' balance sheets by ensuring cybersecurity awareness.

Finally, the OSD shows the magnitude of demand for Inspira's provision of cybersecurity services. In its first six months of operation, the OSD received 393 queries and 30 incident reports, 24 of which were resolved. This resolution rate of 80 percent is almost double the resolution rate of Bangladeshi regulatory authorities—which is approximately 42 percent. Several queriers' incident reports were dependent on help from Facebook for resolution, such as when several entrepreneurs' Facebook pages were arbitrarily taken down or their posts were flagged and removedInspira went through Facebook's official help desk on the entrepreneurs' behalf to resolve these incidents.

Numerous individuals contacting the OSD have requested assistance not directly related to cybersecurity risks or that are outside of the scope of Inspira's expertise, such as performing online detective work to search for missing persons or to pursue suspicions of marital infidelity. Some queriers have also contacted OSD to report a crime that they felt uncomfortable approaching law enforcement with. Thus, of the 24 resolved incident reports, half were resolved by filing a police report (known in the Bangladesh justice system as a General Diary, or GD). Three more reports were resolved by directly contacting cybercrime enforcement officers in the Bangladesh's national police, Dhaka Metropolitan Police, or the Bangladesh Directorate of Consumer Rights Protection. Through these resolutions, Inspira's OSD became an important conduit that allows members of the public to seek resolutions for cybercrimes from local and national law enforcement entities.

On one hand, these examples are positive outcomes that showcase Inspira's influential reach and the popularity of the OSD—one of their highest-profile tools. However, the OSD's implementation remains in progress and Inspira is still iterating the tool's operational strategy; as strategies change, it may take more time to see increased requests for support and positive outcomes from the OSD.

SIGNIFICANCE

The central challenge for an organization like Inspira working in the Bangladesh cybersecurity space is to drive demand for cybersecurity knowledge and skills: in essence, the organization endeavors to build knowledge and awareness of cybersecurity risks among progressively larger audiences. Inspira, in no small part due to its creation of an accessible and prolific online library of Bangla-language cybersecurity knowledge, has driven domestic MSMEs' demand for cybersecurity services to unprecedented levels, opening opportunities for new businesses while also meeting increased demand for cybersecurity and digital hygiene knowledge.

Inspira's cybersecurity learning resources were not the first in Bangladesh, but they are among the most successful and popular. Both the Bangladeshi government and Meta (the parent company of Facebook, WhatsApp, and Instagram) have made resources available in Bangla, including materials on digital safety and security, but the Facebook articles are highly rudimentary and poorly translated from English into Bangla, using transliterations for most technical words that are incomprehensible to non-English speakers. Inspira wrote their materials in Bangla first, occasionally coining new technical words that are intuitive to Bangla speakers.

Additionally, in-person family and social networks are changing cybersecurity practices faster and more effectively than online social media campaigns can. An interview respondent in Dhaka reported that he recommended four family members attend an Inspira workshop, as well as several clients he creates online content for. He also mentioned that when he received inaccurate information from a representative of his mobile phone provider, he suggested the representative use Inspira's online library to improve the knowledge they provide to customers.

Desire for personalized cybersecurity assistance has driven demand for Inspira's workshops. Often, a participant will attend a workshop to receive an answer for a specific question, such as how to recover their account information after their phone was stolen. Since Inspira's workshop facilitators do not not conclude a session until all participant questions have been answered, these questions are usually addressed during the workshops. However, in cases where workshop participants do not have the opportunity to ask their specific question, they sometimes leave the session unsatisfied, and report back to Inspira that they would like to attend additional workshops. Since this feedback is seldom given with the reason—that the participant felt neglected at the first workshop they attended—the perceived demand for workshop sessions could be overstated. Participants' interest in additional workshops for personal reasons is not, overall, a strong indicator of widespread demand for cybersecurity services. Inspira has more digital follow-up strategies, such as the OSD, in place to assist participants with such queries and has others, like a full online training course, in development.

Overall, the SARDI cybersecurity awareness campaign has profoundly shaped the direction of Inspira's institutional evolution. Several high-level managers reported in interviews that a cybersecurity focus will likely be a permanent fixture of Inspira's work, despite imminent end of USAID activity funding. Cybersecurity topics have now also been woven into other aspects of Inspira's work; for example, Inspira integrated cybersecurity information and resources into a recent business development project funded by a non-USAID donor; since many participants are operating their businesses online, Inspira integrated cybersecurity information into the business development programming. On a more strategic level, this business development project also uses and benefits from the partnership model that Inspira developed for the SARDI intervention.

WHAT REMAINS TO BE DONE?

The OSD is currently in its later stages of development; the OSD team is still accepting queries and incident reports that shape new iterations of the service, and more improvements are possible. For example, the OSD system currently cannot collect data on the themes and subjects of queries, nor can it track queriers' locations. This severely limits the insights the OSD can generate about demand for particular types of cybersecurity services in particular geographic areas. The OSD also lacks staff capacity: with a staff of three, it is not able to provide the highest level of support to a high volume of queries, as each query requires a thoughtful human response.

Nonetheless, OSD query response time and resolution quality can be improved by leveraging additional online resources. In partnership with a2i, Inspira plans to develop and release a comprehensive online training curriculum that will provide answers to a much broader range of cybersecurity-related questions than their current online content, as well as absorb excess demand for in-person workshops, which are costly and time-consuming to produce. Inspira also plans to collaborate with a2i to roll out an additional online training module on misinformation and disinformation.

Finally, Inspira plans to assist their financial institution partners to conduct cybersecurity outreach campaigns through their agent banking personnel. In rural Bangladesh, financial institutions typically form customer relationships with MSMEs through agent bankers, who provide financial services as well as business advice and access to peer networks. Inspira will engage and train these agent bankers to spread cybersecurity messaging to their entrepreneur customers.

LESSONS LEARNED:

- **Validate business associations that could become partner organizations.** Legitimate business associations can exert powerful influence on MSME owners to engage with cybersecurity campaigns. However, some organizations project a superficial presence that masks a lack of resources and organizational capacity to support a meaningful partnership with Inspira. For instance, some organizations may have minimal staff or volunteer capacity and would not be able to help co-organize an in-person workshop. Others may not have a large or engaged membership that could be mobilized to attend such workshops. Organizations should be vetted to gauge their actual influence in their entrepreneurial community, since Inspira would rely on them to generate substantial engagement.
- To validate an organization, Inspira follows these steps: First, the Inspira team researches the organization's activities by auditing their entire online presence and communicating with local contacts acquired via SME Foundation. Second, the team studies the organization's history of events; typically, the longer the event history the more reputable and influential the organization

is. Third, Inspira meets with the organization leadership directly to assess their willingness and ability to support a cybersecurity campaign targeted at their members.

- **With larger organizations and corporations, begin partnership work before paperwork is completed.** Inspira found that larger government entities and financial institutions were unable to initiate and complete memoranda of understanding by the time their collaboration was needed on the project. Inspira found that proactivity was crucial to activity success; there was no associated legal risk in, for example, co-designing educational materials with a2i or providing advice on Bank Asia's cybersecurity awareness campaign, and partnership work would have been delayed unless Inspira took initiative to begin these collaborations before the memoranda with these entities were formally executed. Inspira therefore began operationalizing partnership work after USAID Mission approval, but before the memoranda and formal partnership governing documents were fully approved. This made it possible to leverage the influence of high-level partners while still able to operate on the comparatively expeditious timeline of an international development project.