USAID
FROM THE AMERICAN PEOPLE

Cybersecurity
EDUCATION

Photo credit: ACCESS Development Services

Why Does Cybersecurity Matter for Education?

There is a direct link between increased global connectivity and access to education. In order to reach a wider audience, both formal and informal education institutions are using digital tools to put educational materials online, track student progress, share research, and manage their operations. Educational institutions host a wealth of data online, making them increasingly attractive cyber attack targets. Robust cybersecurity protections are critical to protecting learners in an increasingly connected world. Educational institutions can train students to improve their cybersecurity awareness and to build a cadre of cybersecurity specialists, addressing a global shortage of cybersecurity professionals.

What is cybersecurity, and why does it matter for international development?

As noted in USAID's Cybersecurity Primer, USAID defines cybersecurity as "*the activity or process, ability or capability, or state whereby information and communications systems that support or affect development outcomes, and the information contained therein, are protected from and/or defended against damage, unauthorized use or modification, or exploitation.*" As USAID partner countries further their digital transformation and continue to adopt new digital tools and systems, cyber risks and vulnerabilities proliferate. Cybersecurity failures pose material threats to USAID partner countries and undermine partner country government legitimacy. USAID must protect its digital investments by ensuring that its digital programming addresses cyber harms and includes cybersecurity mitigation measures.

"Cyber Champ in Bangladesh" project

Bangladeshi social enterprise Dnet collaborated with the Government of Bangladesh's ICT Division in 2019 to launch a digital safety e-awareness Olympiad with USAID funds. Each week, Grade 9 through 12 students log into the Cyber Champs website to take a quiz about cybersecurity. The top 200 students are eligible to compete in the Olympiad. Dnet complemented this event by training teachers and students from 100 schools in Dhaka, Chittagong, and Rajshahi on safer internet practices.

Cybersecurity Trends in Education

Educational institutions are especially vulnerable to cyber attacks. Cyber attacks can have dire financial impacts on schools and educational institutions, diverting scarce resources from learning materials. The education sector is a high priority target for cyber attacks, especially cyber crime. School districts and educational institutions often lack the funding to invest in robust cybersecurity protections – including top-tier equipment and cybersecurity personnel which means that often they do not follow cybersecurity best practices. Educational institutions may think that they do not possess anything of value for cyber attackers or cyber criminals to steal, a dangerous miscalculation given the amount of student data these institutions gather and store. Students, faculty, and visitors often use their personal devices on educational institution-provided Wi-Fi networks, which further complicates the issue by increasing the potential entry points for malign actors.

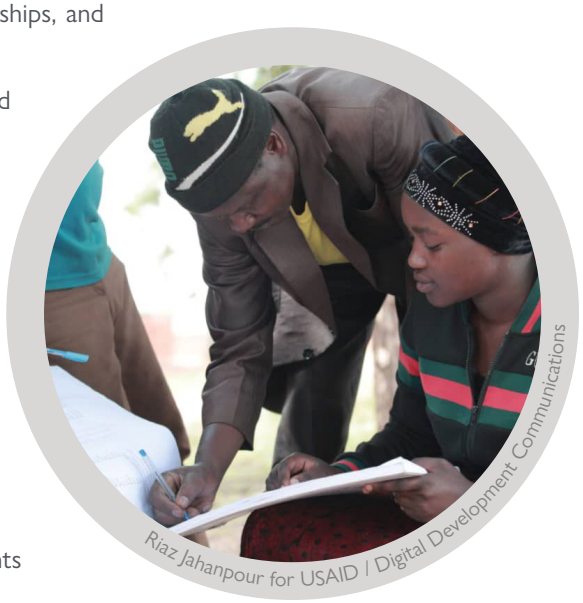

Photo Credit: ACCESS Development Services

Incidents of ransomware and data theft are increasing in the education sector. In a ransomware attack, cyber criminals block victims' access to their own data and will release the block only if the victim pays a ransom. The criminals often threaten to release the data publicly if the ransom is not paid. According to Sophos's *State of Ransomware in Education 2022* report, over half of surveyed IT professionals in the education sector across 31 countries reported that their educational institutions were hit by ransomware in 2021, compared to 44 percent in the previous year's survey. Higher education and lower education had the highest data encryption rates across all professional sectors in the Sophos research, at 74 percent and 72 percent respectively. Information about data breaches of educational institutions from low and middle income countries (LMICs) is not widely available, but data from the U.S. shows more than 1,850 data breaches against U.S.-based primary, secondary, and higher education institutions since 2005, affecting more than 28 million individual records. Widely publicized cases in LMICs, such as the University of Limpopo's 2016 breach that exposed the personally identifiable information of thousands of students and alumni in South Africa, help illustrate the scope of the problem.

Cybercriminals and nation-states each conduct cyberattacks on educational institutions. While potential financial gain typically motivates cybercriminals to attack educational institutions, nation-states have their own motivations. State-sponsored actors might attack education sector institutions—typically those in higher education—because they seek sensitive research or intellectual property, they want to stop research that might be politically embarrassing, or they seek to influence institutions to adopt more favorable policies. Given its high strategic value, cutting-edge national security; military; and Science, Technology, Engineering, and Math-related (STEM) information at universities is among the most valuable for nation-state or nation-state affiliated actors. Iran and the People's Republic of China are perpetrators. Universities in North America and Western Europe have historically been the targets of known nation-state cyber attacks, but universities and other educational institutions in LMICs are not immune to this threat.

Recognizing this growing cybersecurity threat, USAID promotes cybersecurity and digital hygiene education at multiple levels of the educational system. At the K-12 level, the Uzbekistan Excellence for Education activity is testing the skills of Grade 9 students in cybersecurity, data security hacking, and privacy as part of its ICT End-of-Grade Assessments. In higher education, the USAID/Philippines STRIDE activity worked with Holy Angel University to develop and refine its Professional Services Masters in Cybersecurity together with Cloudstaff Inc., a Philippine IT company. In terms of technical and vocational education, the USAID/Kosovo Partnering for Impact – Workforce Partnership in ICT program which works with out-of-school youth hosted several cybersecurity study visits and panels. Students visited one of Kosovo's only cybersecurity companies during Global Entrepreneurship Week, speaking with and asking the company's founders about their work. A panel discussion with cybersecurity professionals from major companies and educational institutions in Kosovo covered such topics as cybersecurity risks, the cybersecurity regulatory environment for companies, and local career paths in cybersecurity.

Key Considerations for Cybersecurity Activities in Education



- Identify areas of alignment with existing USAID or USG strategies, partnerships, and initiatives on education and technology.
- Understand partner country policies, strategies, and regulations around cybersecurity, data privacy, communications infrastructure, and digitalization.
    - USAID Missions and Bureaus must understand the cybersecurity ecosystems they are operating in *before* designing and implementing new activities. Digital Ecosystem Country Assessments (DECAs) are one mechanism for better understanding these dynamics. If your Mission does not have a DECA, consider commissioning one.
- Research project- and activity-specific cyber vulnerabilities within education sector programming.
- Embed cybersecurity considerations, resources, responsibilities, and management tools into every education sector project and activity.
- Develop standalone cybersecurity elements with significant digital components within education sector projects and activities.
- Encourage digital literacy and cyber hygiene training across all education sector programming.
- Support training on the critical use of information in general education programs.
- Build the capacity of USAID Mission staff to understand why cybersecurity and its societal implications are relevant for education sector programs.
- Encourage education sector partners to adopt risk-based approaches to cybersecurity, including clear processes to identify, protect, detect, respond to, and recover from cyber attacks.

TO LEARN MORE about cybersecurity and USAID programming, please reach out to USAID's Cybersecurity Team at cybersecurity.itr@usaid.gov.