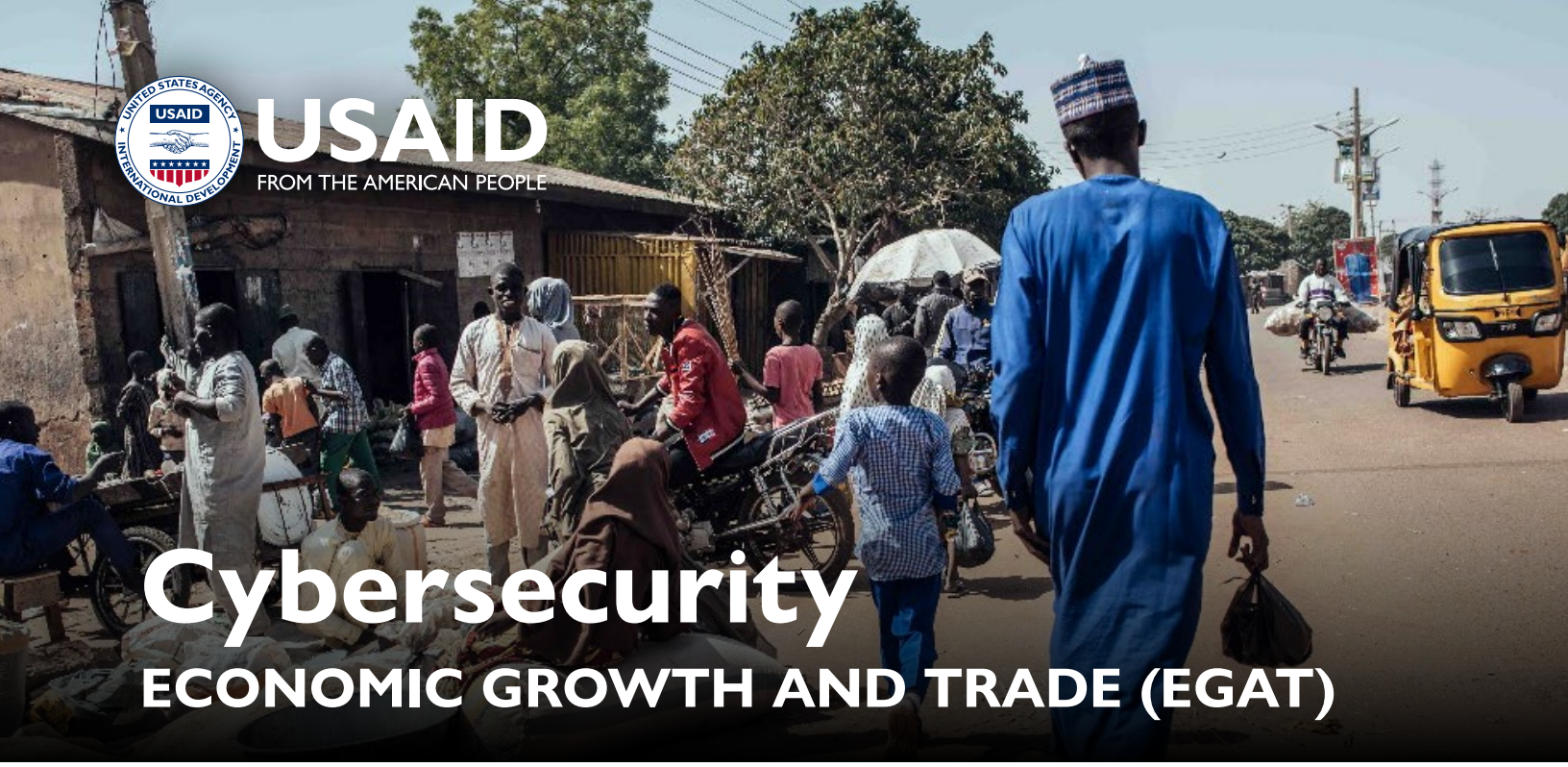

USAID
FROM THE AMERICAN PEOPLE

Cybersecurity

ECONOMIC GROWTH AND TRADE (EGAT)

KC Nwakalor for USAID / Digital Development

Why Does Cybersecurity Matter for EGAT?

Cybersecurity is critical to maintaining economic and financial stability. At a macro level, the significant cost of recovering from a breach or hack of a Central Bank, Ministry of Finance, or any large commercial bank would cause financial harm to stakeholders ranging from national governments to small businesses and individuals. In a 2019 survey, 300 global CEOs cited the lack of cybersecurity as the single greatest threat to the global economy over the ensuing decade. Analysis from cybersecurity industry groups suggests that cyber attacks have a great impact on the global economy. According to one estimate, the global cost of cybercrime is estimated to top $8 trillion in 2023. This figure is larger than the national economies of all but two countries—the United States and the People's Republic of China. And cybercrime is expected to continue to grow unabated over the coming years, with projections as high as $23.84 trillion by 2027.

Micro, small, and medium enterprises (MSMEs) are not immune to these attacks. One study found that companies with fewer than 100 employees are three times more likely to be targeted by cybercriminals than larger companies. Cyber attacks or cyber crimes perpetrated against micro, small, and medium enterprises (MSMEs) can ruin the livelihoods of individual business owners and their employees. As many as 60% of MSMEs go out of business within 6 months of facing a cyber attack. The dire threat that cyber attacks pose to MSMEs underscores the importance of incorporating cybersecurity protections into USAID's EGAT programming.

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.

"USAID's Trade and Competitiveness Activity's (TCA) Guide to Cybersecurity for Micro, Small and Medium Businesses"

Many MSMEs are highly vulnerable to cyber attacks because of budget constraints and a lack of cybersecurity awareness among staff. USAID's TCA released a practical guide to cybersecurity for MSMEs in USAID partner countries in September 2022 to make basic cybersecurity knowledge more accessible. The guide describes basic cybersecurity concepts and suggests several simple and cost-effective measures that MSMEs can deploy to improve their cybersecurity posture.

Cybersecurity Trends in EGAT

Ransomware is an acute cyber risk for businesses. According to the Stop, Think, Connect campaign, ransomware is "a type of malware that accesses a victim's files, locks and encrypts them, and then demands the victim pay a ransom to get them back." The number of ransomware attacks nearly doubled in 2021, increasing almost 93 percent year-to-year. Business owners are taking notice. In a 2022 survey of 650 cyber risk professionals at organizations in 56 countries, more than one-third of respondents said that ransomware was the number one cyber threat facing their organization. Ransomware is also a key component of the malware-as-a-service market. Off-the-shelf ransomware packages can be purchased for as low as $10 and customized ransomware is available for around $3,000. The low cost and increasing availability of ransomware kits has made this highly lucrative form of cybercrime easily accessible to criminals with little digital savvy or knowhow.

MSMEs and financial services providers are especially at risk. MSMEs in many USAID partner countries generate a significant portion of GDP. MSMEs are often not prepared for this threat. According to a study carried out by the National Cyber Security Alliance, some 25 percent of MSMEs surveyed do not have a cybersecurity plan, despite the evidence that cyber attacks can have devastating financial consequences. Financial institutions are also a high-risk target. Banks may spend three times as much on cybersecurity as companies in other sectors, but banks in USAID partner countries typically have a lower cyber maturity level than financial institutions in other countries. This creates financial stability risks at the global level, given the interconnectedness of the international financial system.

Trade-specific cyber vulnerabilities, including supply chain intrusions, can have global impact. The modern trade system is highly globalized, so supply chain cyber vulnerabilities are a major concern for companies. Working with multiple suppliers and vendors—especially smaller ones who may not adequately invest in cybersecurity—increases the ways that global companies can be hacked. In addition to supply chain-related vulnerabilities, national security and geopolitical concerns related to cybersecurity also affect global trade. Such cyber threats can have far-reaching unintended consequences that have a negative impact on trade. The 2017 NotPetya attack against Ukraine unintentionally spread to the networks of international shipping giant Maersk, crippling 17 major port terminals from Los Angeles to Mumbai for days and costing the company $300 million. This amount does not capture the cost incurred by businesses and individuals who rely on global supply chains for their livelihoods. More recently, a cyber attack against shipping firm Expeditors International of Washington halted all operations for three weeks, leading to more than $40 million in losses for the company along with legal headaches. As global trade becomes increasingly digitized in the wake of the COVID-19 pandemic, cyber threats to the sector are likely to grow.

Foreign companies may be using their digital infrastructure to conduct surveillance in USAID partner countries. Some governments are growing increasingly concerned about foreign companies using their local footprints to surveil citizens or compromise national security, particularly within the critical infrastructure sector. Fears that 5G infrastructure made by telecommunications company Huawei would allow the People's Republic of China (PRC) to monitor local communications have prompted several countries to ban or restrict Huawei equipment from their countries.

USAID and other donors are increasingly working with businesses to build their cyber resilience. USAID is working with MSMEs in its partner countries to build their cybersecurity knowledge and skills, often bundling cybersecurity skills-building with other digital skills. The Digital Asia Accelerator buy-in under Digital Frontiers awarded a grant to Impact Hub Phnom Penh to design an e-learning course for SMEs and start-ups called "Building Your Business's Online Presence," which covered topics including cybersecurity as well as digital storytelling and marketing. Several donors, including USAID, have invested in cybersecurity toolkits for SMEs: similar to USAID TCA's Guide to Cybersecurity for Micro, Small and Medium Businesses detailed above, FCDO launched a Cybersecurity Toolkit for Small and Medium Enterprises (SMEs) under its Digital Access Programme in 2022. Donors are also addressing sector-specific cybersecurity concerns for businesses. The African Development Bank-funded Africa Cybersecurity Resource Center works directly with financial institutions to address challenges specific to the financial services sector as a way to improve their cybersecurity capacity.

Key Considerations for Cybersecurity in EGAT

- 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.
- Coordinate with other donors to identify areas of alignment in cybersecurity.
- Identify areas of alignment with existing USAID or USG strategies, partnerships, and initiatives.
- Embed cybersecurity considerations, resources, responsibilities, and management tools into every EGAT project or activity.
- Build or strengthen a robust pipeline of cybersecurity and technology professionals in the partner country by working closely with appropriate institutions or with other donors.

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