

2021-12-06

# C305 UK Cyber SMEs Survey Support Material



# 01

## Market Opportunity

# Market Opportunity

Country	GDP, USD (million) <sup>1</sup>	GDP per capita, USD <sup>1</sup>	GDP Growth, % <sup>1</sup>	Ease of doing business <sup>2</sup>	Market Size, USD	
					Banking industry asset value, USD (million) <sup>3</sup>	Telecom industry revenue, USD (million) <sup>3</sup>
Brazil	2,053,595	9,881	0.98%	124	1,935	45
Indonesia	1,015,421	3,837	5.07%	73	427	9
Kenya	79,263	1,578	4.87%	56	41	4
Nigeria	375,745	1,969	0.81%	131	91	6
South Africa	348,872	6,120	1.32%	84	247	14

## Sources



1. <https://www.worldometers.info/gdp/gdp-by-country/>
2. <https://www.doingbusiness.org/en/rankings> - Economies are ranked on their ease of doing business, from 1–190. A high ease of doing business ranking means the regulatory environment is more conducive to the starting and operation of a local firm. The rankings are determined by sorting the aggregate scores on 10 topics, each consisting of several indicators, giving equal weight to each topic. The rankings for all economies are benchmarked to May 2019
3. OECD – Banking and Telecoms are two are the key sectors for cyber opportunities. These have been given as an indication as the potential size of the opportunity in each of the target countries.






# 02

## Cyber Awareness

# Cyber awareness by country (1/2)

Country	Rationale
 Brazil	<ul style="list-style-type: none"> <li>There is a significant lack of knowledge and misunderstanding about the maturity of the Brazilian market more generally (a view which is perpetuated by media). The perception is that Brazil is undeveloped and with an unstable economy, which is not the case</li> <li>Brazil has a mature cyber market. Some Brazilian companies are themselves exporting into Europe and the US.</li> <li>The Brazilian government recognised cyber security as a top priority and has a national cyber security strategy.</li> <li>There is awareness of cybersecurity as a business issue, with a significant frequency of news reporting on the subject in Brazilian media. Much coverage focuses on international cybersecurity stories, but major Brazilian business magazine Valor Economico and Brazilian news site G1, report on attacks against Brazilian companies and infrastructure</li> <li>According to a report commissioned by French defence and cybersecurity firm Thales, and carried out by US research consultancy 451 Research, 90% of Brazilian executive are worried about cybersecurity threats. The Thales report found that home working as a result of Covid-19 has increased management concerns over cybersecurity.</li> <li>47% of Brazilian executives do not trust the cybersecurity systems they currently have to protect them from attack.</li> </ul>
 South Africa	<ul style="list-style-type: none"> <li>The South African government has become more alert to the need for cybersecurity following the Transnet attack on Durban Port. They appear to be turning more frequently to UK SMEs for support.</li> <li>Before the Transnet attack, which began July 21, 2021, weeks earlier major businesses across South Africa were hit by a separate wave of cyber attacks, beginning at the end of June and stretching into July.</li> <li>Another major hack against business, the DEBT-IN attack, occurred in late September, with personal data of 1.4 million South Africans stolen.</li> <li>Following the July attack on Port of Durban and other Government owned facilities, in August 2021 the South African Government announced in Parliament that it is building a database of security specialists to ensure greater resilience and recovery against future potential attacks.</li> </ul>

# Cyber awareness by country (2/2)

Country	Rationale
 Indonesia	<ul style="list-style-type: none"> <li>Indonesia's approach to cyber security is very nascent; they only established BSSN (Indonesia's national cyber security agency) in 2018. They have only recently recognised cyber security as core to their national security and critical national infrastructure.</li> <li>The ASEAN region is currently undergoing a large digital transformation across all markets, which opens the door for conversations about improving their cyber capability and potential partnerships with UK SMEs.</li> <li>Concern over a growing trend of cybercrime has led the Indonesian National Police Force (the central Federal police authority) to form the Directorate of Cyber Crime (Ditipidsiber) within the National CID.</li> <li>Much of the media coverage on cybersecurity in Javanese concerns the need for greater cybersecurity skills and professionals in Indonesia. These include calls by politicians and Government figures, as well as calls by universities for greater enrollment and expansion of courses on cybersecurity.</li> </ul>
 Nigeria	<ul style="list-style-type: none"> <li>Nigeria announced a National Cybersecurity Policy and Strategy in February 2021.</li> <li>According to the strategy, Nigeria faces increasing threats from state and non-state actors, with targeting of elections and destruction of critical infrastructure particular concerns. The actions of terrorist groups in both sabotage and indoctrination are highlighted as a threat.</li> <li>Especially under attack are the country's telecoms infrastructure, financial services, transportation, air traffic control systems, and hydropower grid.</li> <li>Cybersecurity attacks in Nigeria were responsible for losses of 582 million USD (2017 figures), the highest in Africa at the time.</li> <li>There is a belief in Nigeria and Kenya, reflected in a pan-African survey reported Sep. 28, 2021, by Business Insider South Africa, that Nigeria and Kenya have far better cybersecurity than South Africa.</li> </ul>
 Kenya	<ul style="list-style-type: none"> <li>In Kenya, cybersecurity is managed through the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC), a multi-agency framework that coordinates cyber security in Kenya. It began operation in 2017.</li> <li>The Computer Misuse and Cyber Crimes Act of 2018 has strengthened multi-agency collaboration within the KE-CIRT/CC (Kenya's national cybersecurity point of contact).</li> <li>In November 2021, the Kenyan Interior Ministry announced the formation of the National Computer and Cybercrimes Coordination Committee (NCCCC), with a particular focus on preventing abuse or attacks on Kenyan social media aimed at influencing the outcome of elections, with particular concern about the general election to be held in 2022. The new committee will be chaired by the civil service head of the Interior Ministry, Karanja Kibicho.</li> <li>Kenya has the highest internet penetration in Africa, with around 31 million having access, or 65% of the total population.</li> <li>Cybersecurity attacks in Kenya were responsible for losses of 188 million USD (2017 figures).</li> </ul>



# 03

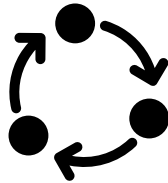
## Barriers to entry

# We have identified seven common themes that each provide opportunities and barriers for entry



## Partnerships

Finding a local partner to support UK SMEs entering new target country markets



## Routes to market

Understanding the best way routes to identify, bid and win new work in target countries.



## Market Intelligence

Information/data on market size, relevant target sectors, potential partner organisation/individuals, and local opportunities in cyber.



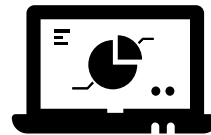
## Local business culture

Understanding local ways of working.



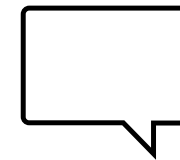
## Legislation

Understanding the local regulations (for both cyber and wider business)



## Perception of UK SMEs

The perceived quality and cost of UK Cyber-SMEs



## Language

Ability and necessity to speak and conduct business in the local language



# 04

## Appendix Detailed findings

# Partnerships

Theme	Insight Type	Description
Partnerships	Context	<ul style="list-style-type: none"> <li>UK SMEs need a in-country presence in order to effectively export and break into a new market. Establishing their own physical presence in-country can be costly and time-consuming.</li> <li>This can also be achieved thorough partnering with multinationals, local cyber-SMEs, a local single representative with industry knowledge/contact or a local 'PR agency'.</li> <li>Partnerships are required to identify opportunities, make introductions, support business development, help understand local regulations, and to aid with marketing, public relations and often translation.</li> </ul>
	Barriers	<ul style="list-style-type: none"> <li>Identifying the right partner organisation can be time consuming and resource intensive.</li> <li>It is difficult for UK SMEs to find a consolidated list of potential partners.</li> <li>Relationships between FCDO/DIT in-country representatives and local contacts can be damaged if introductions are made to UK SMEs who are either slow or do not respond to the opportunity.</li> <li>Larger in-country firms (such as system integrators) can often take a long time to decide which UK SMEs they want to partner with.</li> </ul>
	Enablers / Opportunities	<ul style="list-style-type: none"> <li>Multinationals often have an interest in creating UK SME to local SME partnerships. This might serve a multinational's own purpose within a contract.</li> <li>In-person meetings with potential partners can accelerate this process of deciding whether a partnership is the right fit and getting started on real opportunities</li> <li>The size of the partner is less important than their knowledge of industry contacts, opportunities and knowledge in local ways of working. An effective one-person partner with significant industry/sector expertise is sometimes sufficient.</li> <li>FCDO Brazil are establishing a database of local cyber companies and development hubs to support UK SMEs in partnering.</li> <li>UK SMEs have previously had success in in Singapore by partnering with system integrators (such as NCS, ST Engineering and Ensign). This approach may work in other target countries.</li> <li>In South Africa, having business connections with local firms that both meet and exceed the BBBEE requirements would be a competitive advantage for UK SMEs if they adopted this route.</li> </ul>

# Routes to market

Theme	Insight Type	Description
Routes to market	Context	<ul style="list-style-type: none"> <li>It is important for UK SMEs to understand the different ways in which they can identify opportunities, respond to opportunities and the understand the help that is available to them.</li> <li>UK SMEs need to define a strategy for how they will enter the foreign market, including their target sectors, whether they will take a bilateral or regional approach and define their partnering approach.</li> <li>For cybersecurity, it is likely to be more beneficial to focus on individual countries (bilateral agreements) rather than taking a regional approach as the differences between the markets, cyber strategy and local business cultures are so different.</li> </ul>
	Barriers	<ul style="list-style-type: none"> <li>Many businesses trying to enter the wider APAC region first establish themselves in Singapore where doing businesses is more familiar. However, this approach will not necessarily make it much easier to enter the Indonesian cyber market (as the market is specific to each country) but may provide a slight advantage in earlier identification of opportunities.</li> <li>Entering the market with a multinational can open significant opportunities for UK SMEs but establishing a new relationship can be risky and high-cost.</li> <li>Government tenders in target countries are sometimes written to favour larger or existing suppliers.</li> </ul>
	Enablers / Opportunities	<ul style="list-style-type: none"> <li>The UK has a memorandum of understanding (MOU) with Indonesia which provides a channel for UK SMEs to influence cyber development.</li> <li>Tradeshows and webinars are a great opportunity for UK SMEs to learn more about opportunities and approaches to cyber. In Q1 2022, tradeshows are being planned for UK cyber-SMEs in Brazil and the APAC region.</li> <li>Brazil have commenced working on improving the marketing for cyber in the LATAC region, with a focus on attracting UK cyber-SMEs to Brazil.</li> <li>Brazil and Singapore have e-procurement portals where foreign companies can register and bid for government cyber contracts.</li> <li>Whilst many UK companies assume markets such as the US will be easier to enter, SMEs often find they are too small and do not have sufficient credibility. Targeting countries with a culture open to taking increased risk (such as the LATAC region) may be more beneficial.</li> </ul>



# Market intelligence

Theme	Insight Type	Description
Market intelligence	Context	<ul style="list-style-type: none"> <li>In this context, the term market intelligence encompasses information/data on market size, relevant target sectors, potential partner organisation/individuals, and local opportunities in cyber covering both the public and private sector.</li> <li>This information is key for UK SMEs to understand the cost-benefit analysis of entering a new market.</li> </ul>
	Barriers	<ul style="list-style-type: none"> <li>It is very difficult for UK SMEs to get consolidated market intelligence. Often, their only option is to contact the British Embassy in the target country to request any information that is readily available.</li> <li>In APAC, lots of individual reports have been commissioned covering parts of the market intelligence array, suggesting there is currently no consolidated view.</li> <li>It is challenging to get accurate target-country market information on cyber specifically; often cyber is grouped under several other sectors (such as software, technology, IT, professional services etc.).</li> <li>Due to the COVID-19 pandemic, the Malaysian government has been taking back budget to fund their response which has reduced the number of tenders and expenditure on cyber.</li> <li>It is difficult for UK SMEs to identify opportunities in private companies in the target countries. Some advertise opportunities on their own website, but it is unlikely UK SMEs would know where to look for this information.</li> </ul>
	Enablers / Opportunities	<ul style="list-style-type: none"> <li>Recently in Thailand, there have been several high-profile data leaks which may provide an opportunity for UK SMEs to provide support across response, resilience and cyber infrastructure.</li> <li>DIT/FCDO often run webinars in the target countries (either wholly or partly focussed on cyber) for UK SMEs to provide market intelligence.</li> <li>Brazil have recently committed resources to improve their understanding of the local cyber market.</li> <li>Cyber is a growing market in Brazil. Their demand for cybersecurity products (across private and public sector) increased during the COVID-19 pandemic due to increased in remote working.</li> <li>Both Brazil and Singapore have an e-procurement portal that foreign companies can access to see and respond to government tenders.</li> </ul>

# Local business culture

Theme	Insight Type	Description
Local business culture	Context	<ul style="list-style-type: none"> <li>Business culture refers to the ways in which different countries, regions and communities tend to conduct business.</li> <li>This encompasses communication style, approach to networking, sharing and identifying opportunities, the importance of personal relationships and the best ways to cultivate and develop new working relationships.</li> <li>Each country has distinct business cultures which UK SMEs must understand to be successful in these markets.</li> </ul>
	Barriers	<ul style="list-style-type: none"> <li>It is very important to build up strong personal and business relationships with potential partners and customers, but this can be time consuming.</li> <li>There are big differences in the approach to cyber security between countries within the APAC region. Each country must therefore be treated independently, and a regional approach is unlikely to prove fruitful.</li> <li>UK SMEs often do not fully understand or appreciate the different business cultures and ways of working before trying to enter new markets (e.g., even within Europe, there are big differences between entering France vs. Germany).</li> <li>Issues of trust in South African society are very important in how industry works, and business is done. Notwithstanding legislation, companies will not do work with firms unless they can place the firm within their business network, and the firm and its personnel are known and trusted.</li> <li>An on-going in-country presence is required. It is extremely challenging to do business without face-to-face meetings. This can be done either through a direct presence or through a local partner.</li> <li>South African business still operates by a word-of-mouth approach, and they are unlikely to place new firms in their business network without a persona and trusted relationship.</li> </ul>
	Enablers / Opportunities	<ul style="list-style-type: none"> <li>The UK is a very trusted brand in Brazil.</li> <li>In-country, face-to-face meetings can significantly accelerate the process of building relationships in the target countries.</li> <li>If UK SMEs can take a longer-term, strategic view (3-5 years) to establish themselves and build up relationships, there could be significant opportunity in these new markets.</li> </ul>

# Legislation

Theme	Insight Type	Description
Legislation	Context	<ul style="list-style-type: none"> <li>Foreign markets each operate under a unique legal system that impact both cyber itself but also the way that native or foreign companies can establish and operate.</li> <li>Whilst some markets may be more like the UK than others, each has their own regulations which must be understood to be able to operate in that country.</li> </ul>
	Barriers	<ul style="list-style-type: none"> <li>It can be challenging to form partnerships relating to the software/product sub-sector of cyber due to IP issues.</li> <li>Exporting hardware to Brazil is challenging. There is a lot of regulation and need to translate technical documentation in Portuguese.</li> <li>According to a recent DIT report, Indonesia is seen as a complex market with a challenging regulatory landscape. Regulation can sometime change overnight.</li> <li>The cyber industry is part of the Technology industry, which is a classified industry under Broad-Based Black Economic Empowerment Act (BBBEE) and has a specific scorecard drawn up to regulate it. This affects UK cyber-SMEs bidding for any government contracts.</li> </ul>
	Enablers / Opportunities	<ul style="list-style-type: none"> <li>In February 2021, Brazil brought in new legislation that meant for certain projects with sensitive material/technologies, companies do not have to go through the standard procurement processes. There is an expedited version and avoids needing to share sensitive material.</li> <li>Last year, Brazil passed their equivalent of GDPR legislation. Whilst this is not directly related to cyber, people see the intrinsic link between GDPR and cyber which caused a boom in the UK. David thinks the same is likely to happen in Brazil.</li> <li>In 2020, the International Maritime Organisation passed a new law stating that all maritime organisations must meet a minimum standard of cyber security. This could provide UK SMEs with the opportunity to support these organisations internationally to meet these standards.</li> </ul>



# Perception of UK SMEs & Language

Theme	Insight Type	Description
Perception of UK SMEs	Context	<ul style="list-style-type: none"> <li>This theme covers the way in which UK SMEs are perceived by the chosen target markets.</li> <li>This covers both the perceived quality and price of UK SMEs.</li> </ul>
	Barriers	<ul style="list-style-type: none"> <li>UK SMEs are generally seen as being more expensive than many other international competitors. This is also true when comparing to the internal cost of the target countries.</li> </ul>
	Enablers / Opportunities	<ul style="list-style-type: none"> <li>Generally, UK Cyber-SMEs are seen as highly proficient and skilled and have a strong reputation when compared to other international competitors.</li> <li>The UK is helping South Africa to build up government and police capability to deal with cyber attacks. There seems to be an inclination to use UK companies which is the first time this has happened (following Transnet attack).</li> </ul>

Theme	Insight Type	Description
Language	Context	<ul style="list-style-type: none"> <li>Language is a common barrier when entering many foreign markets.</li> <li>Whilst many countries may speak English, not all people will feel comfortable to conduct business fully in English.</li> <li>Speaking the local language is not only about understanding, but also about building trust in new relationships.</li> </ul>
	Barriers	<ul style="list-style-type: none"> <li>In both Brazil and Indonesia, it is important that UK SMEs have support in the local language. This is not just about translating material, but understanding the way that people communicate with one another.</li> <li>In Brazil, whilst lots of people speak English, many would not feel comfortable to conduct business fully in English.</li> <li>Even in countries where English is widely spoken, having a partner that speaks the local language is very helpful in building up trust with potential clients in that country.</li> </ul>
	Enablers / Opportunities	<ul style="list-style-type: none"> <li>English is the primary language used to conduct most business and government work in South Africa.</li> </ul>