Applying Market Systems Development to Strengthen Commercial Viability

Case Study: Green Circle and Jordan's Cybersecurity Labor Market System

Prepared by: Lina Khawaja

Executive MBA Participant

Reviewer: Mr. Marshall Bear

Core Trainer and Post-Workshop Coach

Opportunities Unlimited / Mazi

Capacity Building Programme: **Effective Management of Systems Programming**

Date: October 2026

Table of Contents

Applying Market Systems Development to Strengthen Commercial Viability 3
Case Study: Green Circle and Jordan's Cybersecurity Labor Market System 3
Executive Summary 3
Introduction, Methodology and Case Selection Rationale 5
Introduction 5
Methodology 6
Case Selection Rationale: 6
Jordan Cybersecurity and Digital Labour Market Context 7
Market System and Constraint Analysis 10
Market System Analysis 10
Systemic Constraint Analysis 11
Green Circle: Commercial Viability Current Services and Potential Market-System Role .. 18
Current commercial services: 18
Current workforce-development activities. 18
Potential Commercial Role within the Market System: 18
Commercial viability through MSD: 19
Four revenue logics follow: 19
Commercial Value, Revenue Scenarios and Investor Incentives 20
Next Steps 23
Conclusion 23
References 26

List of Tables

Table 1: Constraint/Solution Logic and Indicators of Sustainability 15
Table 2: Commercial Value and Financing Logic 22

List of Figures

Figure 1: Cybersecurity Labour Market System: Function & Players 11

Applying Market Systems Development to Strengthen Commercial Viability

Case Study: Green Circle and Jordan's Cybersecurity Labor Market System

Executive Summary

This case study is written primarily for Jordanian cybersecurity and digital-market stakeholders, including cybersecurity firms, employers, government entities, industry bodies, education and training providers, investors and strategic private-sector partners. It argues that a market systems development (MSD) approach can strengthen Jordan's policy goal of good job-creating economic growth by fostering the commercial viability of service providers in this space. Why? Because a service firm can become more commercially robust when it reduces structural frictions that prevent employers, workers and intermediaries from transacting effectively. The focal issue is the conversion of digitally educated young people into productive, employer-trusted cybersecurity capability.

Jordan provides a fitting setting because national economic, digital-transformation and cybersecurity policy is increasing demand for digital trust, cyber capability and skilled technical services. The relevant context for this case is therefore sector-specific: how policy, regulation, employer demand, skills formation, certification, market information, finance and intermediation interact to shape the supply and commercial use of cybersecurity capability in Jordan. Broader labour-market indicators are used only where they help explain a specific constraint in this cybersecurity/digital labour market.

The case for cybersecurity is especially strong because policy, regulation, and digitization are expanding demand faster than local talent pipelines are adjusting. Jordan's national cybersecurity framework requires public and private entities to build cybersecurity capabilities, and sector strategies[1]. The 2025–2028 energy cyber strategy explicitly identifies workforce and skills shortages, especially in specialized areas such as operational technology security[2]. The digital skills gap analysis commissioned for Jordan similarly found limited hands-on practical training, weak coverage of emerging fields such as cybersecurity and cloud, low absorption of fresh graduates, underuse of women, and costly enterprise-

[1] www.ncsc.jo

[2] www.memr.gov

level skill-upgrading needs. This means that the bottleneck is not a lack of graduates, but it is the conversion of potential talent into productive, billable, employer-trusted capability.[3]

Green Circle provides a useful case through which to examine how a commercial market actor could respond to these constraints contributing to wider market-system change. As a commercial cybersecurity company, it offers managed security operations, penetration testing, incident response, GRC advisory, and AI security.[4] It also runs training and deployability pathways, including grant-supported programmes, internships, a 'Cyber Bridge' training model, and the Zero to Hero platform. Its public materials therefore provide evidence of capabilities spanning cybersecurity services, practical preparation, employer exposure and candidate matching, without making the employment programme itself the organizing frame of the case. [5]

Within this multi-actor system, a commercially feasible **future offer for Green Circle** could be a **Cyber Workforce Readiness and Deployment (CWRD) service**. This proposed service would build on Green Circle's existing cybersecurity delivery and talent-development capabilities but integrate them into a more structured commercial offer combining role-specific assessment, practical preparation, supervised work experience, employer matching, deployment and retention support. Its value proposition would not be training alone, but the reduction of recruitment risk and the conversion of junior talent into productive cybersecurity capacity. Potential revenue streams could include employer-paid recruitment and deployment fees, subscription or managed-service contracts, project-based cybersecurity services delivered through supervised teams, and selected advanced-training or certification fees.

The paper concludes that addressing systemic employment constraints can create commercial value alongside public policy employment outcomes. System-level and public-good functions require a wider distribution of responsibilities. Government entities can coordinate policy, standards, market information and inclusion incentives. Universities and training providers can strengthen foundational and applied learning. Employers can define occupational requirements, co-design training, provide work-based learning and pay for verified capability. Industry associations can support common standards, signaling and demand aggregation. Time-bound development programmes can test innovations and temporarily subsidies public-good or inclusion costs. International investors and private-sector partners can contribute capital, technology, specialist expertise, export connections and access to regional and international demand.

[3] www.modee.gov.jo

[4] https://grcico.com/

[5] https://grcico.com/

In Jordan's cybersecurity market, persistent gaps in workforce readiness, employer confidence, matching mechanisms and pathways into employment represent not only labour-market challenges, but also unmet market needs. For Green Circle and other market actors, responding to these constraints can create viable opportunities to develop services that employers, clients and other stakeholders have an incentive to support or pay for. From an MSD perspective, the central opportunity is therefore not simply to sustain externally funded employment interventions, but to strengthen market functions and incentives so that solutions to youth employment constraints can become commercially relevant and increasingly embedded within the cybersecurity market system.

Introduction, Methodology and Case Selection Rationale

Introduction

This case study is primarily directed to stakeholders shaping Jordan's cybersecurity and digital market system: cybersecurity firms, employers, government entities, industry bodies, education and training providers, investors and strategic partners. It uses an MSD lens to examine a practical commercial question: can addressing systemic employment constraints generate commercially valuable opportunities for cybersecurity firms, their customers and other market actors? MSD is relevant because it focuses on how core transactions, supporting functions, rules and actor incentives shape market performance. The paper therefore treats youth employment as part of the cybersecurity market system rather than as a stand-alone social programme. [6]

The paper's contribution is managerial and market-facing. Where labour-market failures increase recruitment costs, delay staff deployment and constrain business growth, addressing those failures can create value for which employers and other market actors may be willing to pay. In cybersecurity, the weak conversion of digitally educated young people into employer-trusted professionals therefore represents a potential commercial opportunity involving practical preparation, assessment, matching, supervised deployment and service delivery. The analysis is intentionally focused on this commercial and system-level proposition rather than on broader organizational-change frameworks.

The opportunity is not limited to Green Circle and cannot be realized by one company alone. Cybersecurity firms, employers, universities, training providers, government entities, industry associations, development programmes, investors and strategic private-sector partners perform different but complementary functions. The central question is therefore whether a better-functioning cybersecurity employment market can strengthen the

[6] https://www.springfieldcentre.com

commercial viability of service providers while advancing Jordan's cybersecurity capability and employment objectives.

Methodology

This paper uses a qualitative, theory-informed single-case study based on secondary public sources. The method is interpretive rather than econometric and triangulates Jordanian policy documents, cybersecurity and digital-labour evidence, MSD guidance, programme literature and Green Circle's public materials. The analysis uses three directly relevant lenses: (1)M4P/MSD concepts of core transactions, supporting functions, rules, incentives and systemic change; (2) youth-employment market-system analysis to distinguish symptoms from root causes across labour demand, skills development and matching; and (3) commercial-value analysis to examine who benefits, who pays, potential revenue streams and the conditions under which recurring functions can become financially sustainable. [7]

Because the evidence base is secondary, the paper does not claim to reconstruct commercial market actors internal financials or confidential strategy. Instead, it uses publicly stated offerings, partnerships, and programme design as evidence of organizational positioning. Where the paper infers management implications, for example, about likely business-model tensions or the maturity of commercial actor internal systems, those inferences are identified as interpretations grounded in documented offerings rather than as verified internal facts. **Likewise, the proposed revenue options are presented as scenarios requiring validation, rather than as confirmed sources of income. These include employer-paid recruitment and deployment services, managed-service contracts, supervised project delivery and selected advanced training fees.**

This approach is consistent with MSD practice because it combines market-system diagnosis, causal reasoning and analysis of actor incentives with a practical test of commercial value. The paper asks not only what functions are weak, but also which actors have the incentive and capacity to perform them, who captures the resulting value, and which functions could plausibly be financed through recurring market revenue. [8]

Case Selection Rationale:

Green Circle is a strong case for four reasons. First, it is highly relevant to the substantive problem: Jordan is actively promoting digital transformation and cybersecurity, while the labour market continues to struggle to translate education into high-quality work, especially for youth and women. Second, Green Circle occupies an analytically rich position at the

[7] https://www.ilo.org

[8] https://www.ilo.org/publications/market-systems-analysis-decent-work-user-friendly-guide

intersection of three systems: the cybersecurity services market, the digital-skills system, and the youth-employment system. Third, it is a rare example of a firm publicly presenting itself as an integrated cybersecurity ecosystem, combining managed services, training, community pathways, and employment support. Fourth, it has been selected and co-funded by CFYE, which indicates that external actors also viewed it as a potentially scalable employment model, not merely as a conventional training provider.[9]

Green Circle is treated as one commercial provider within a broader cybersecurity ecosystem. Its relevance lies in the combination of cybersecurity service delivery and workforce-development activities, which makes it possible to examine whether employment-system constraints can be converted into commercially valuable services. The case does not assume that Green Circle should coordinate the whole market. Rather, it distinguishes functions that can generate firm-level revenue from functions, such as common standards, neutral market information and enabling policy, that are more appropriately led by government, industry bodies or collective mechanisms.

This makes Green Circle neither a purely "typical" case nor a purely "exceptional" one. It is better understood as a **strategic case**: a case through which one can test whether treating skill formation, matching, and employability as a market-system problem can help a commercial actor improve its own viability. The case is also timely. Green Circle's public materials show active grant-linked programming, ongoing training pathways, and a current ecosystem narrative that explicitly connects cybersecurity services with workforce development and community impact.[10] Those features make it suitable for an MBA paper concerned with the relationship between strategy, system change, and commercially feasible offers.

Jordan Cybersecurity and Digital Labour Market Context

Jordan's cybersecurity and digital labour-market context is best understood as a system rather than as a description of the national labour market statistics. Diagram 1: Cybersecurity Labour Market System offers a picture of the key players and the functions they perform in matching demand and supply. At its core is demand from organisations for trusted cybersecurity and digital capability and the supply of people who can perform those roles productively. The system is enabled by supporting functions including applied skills development, work-based learning, recruitment and matching, assessment and certification, labour-market information, technology infrastructure, finance, and

[9] https://www.linkedin.com/posts/challenge-fund-for-youth-employment_jordan-activity-7392104765536776192-XCdB

[10] https://z2h.me/elearning/index.xhtml

business/market linkages. Its principal players include government and regulators, cybersecurity and digital firms, employers across sectors, universities and training providers, workforce intermediaries, industry associations, technology providers, investors and development partners, and regional/international clients. Formal and informal rules, including cybersecurity regulation, data protection, procurement, employment practices and employer preferences, standards and certification requirements, shape how these functions perform.

Labour-market evidence is therefore used selectively in this paper. Youth employment and women's participation remain relevant where they reveal a specific market-system constraint, for example weak conversion of graduate supply into job-ready capability or under-use of available technical talent, but they are not treated as the organizing frame for the case study.

The digital sector itself has stronger fundamentals than the wider labour market, but those fundamentals coexist with a skills-conversion problem. GIZ's sector analysis described ICT as a growth and employment sector in Jordan and identified opportunities in regional markets such as infrastructure, core skills, and localization for Arab markets. Yet it also identified recurring constraints: a limited domestic market, weak business linkages, weak management capacity in MSMEs, gaps between education providers and industry, and a weak business-enabling environment. The same report argued that Jordan can only really achieve scale through exports[11]. In more recent investment promotion materials, Jordan presents itself as a regional digital hub with strong infrastructure, cost-efficient talent, export tax incentives, and government support programmes for firm expansion, talent development, internships, and market access. Those sources point to a hybrid reality: the opportunity is real, but firms still need mechanisms that translate digital potential into reliable contracts, talent, and productivity. [12]

The digital skills gap analysis for Jordan makes the conversion problem clearer. The MoDDE report argues that Jordan needs a two-pronged strategy: attract global IT/BPO outsourcing firms while also supporting existing local companies to meet demand. It found that more than 80 per cent of surveyed domestic firms planned to expand by at least 10 per cent over one to two years and would need at least 3,000 trained resources in the near term. Yet it also found a chronic employability gap, with only about 42 per cent of ICT graduates being absorbed into the sector, widespread shortages of practical and internship-based training, limited curricular coverage of emerging fields such as cybersecurity and cloud, and significant enterprise-level costs because companies must spend time and resources

[11] https://www.giz.de/sites

[12] https://invest.jo

training selected candidates before deploying them. This is precisely the kind of structural mismatch that creates space for a private intermediary that can reduce the cost of translation between education and work. [13]

Age and gender evidence is retained only as diagnostic evidence where it affects the cybersecurity talent pipeline. The analytical emphasis remains on the market functions and incentives that determine whether available talent is converted into productive cybersecurity capability.

Cybersecurity adds a further demand pull. Jordan's National Cybersecurity Framework states that both public and private entities are required to build and develop capabilities that improve cyber maturity and support digital transformation. The regulatory framework drafted around the Jordan National Cyber Security Framework aims to position Jordan as a leading country in cybersecurity while enhancing institutional and human capacity[14]. Sector strategies make the workforce issue still more concrete. The Jordan energy sector cybersecurity strategy for 2025–2028 explicitly names workforce and skills shortages as critical concerns, calls for expanded skilled workforce capacity, and notes that practical experience remains insufficient even as cyber risk rises with digital transformation, smart systems, and IT/OT convergence. That combination, expanding mandates plus thin practical supply is highly favorable for a company that can productize cyber capability development[15].

A final contextual point is that Jordan's digital economy is increasingly oriented outward. Investment promotion material stresses zero per cent income tax on exported services, zero per cent sales tax on IT services, support for BPO/ITO hubs, and opportunities in cloud, SaaS, and cybersecurity[16]. GIZ similarly stresses that Jordan must seek scale through export markets. For Green Circle, this matters because commercial viability need not depend only on Jordanian employers. A Jordan-based cybersecurity employment market system can, in principle, monetize regional demand, remote delivery, outsourced projects, and exportable managed services. The local labour-market challenge is therefore inseparable from an export-oriented business opportunity.

---

[13] https://digiskills.jo/Default/En

[14] https://ncsc.jo/Ar/List/Policies_and_Strategies_AR

[15] https://memr.gov.jo/EBV4.0/Root_Storage/AR/EB_Info_Page/Cyber_Security_Strategy_2025.pdfpe

[16] https://invest.jo/index.php/en/investment-sectors/ictbpo

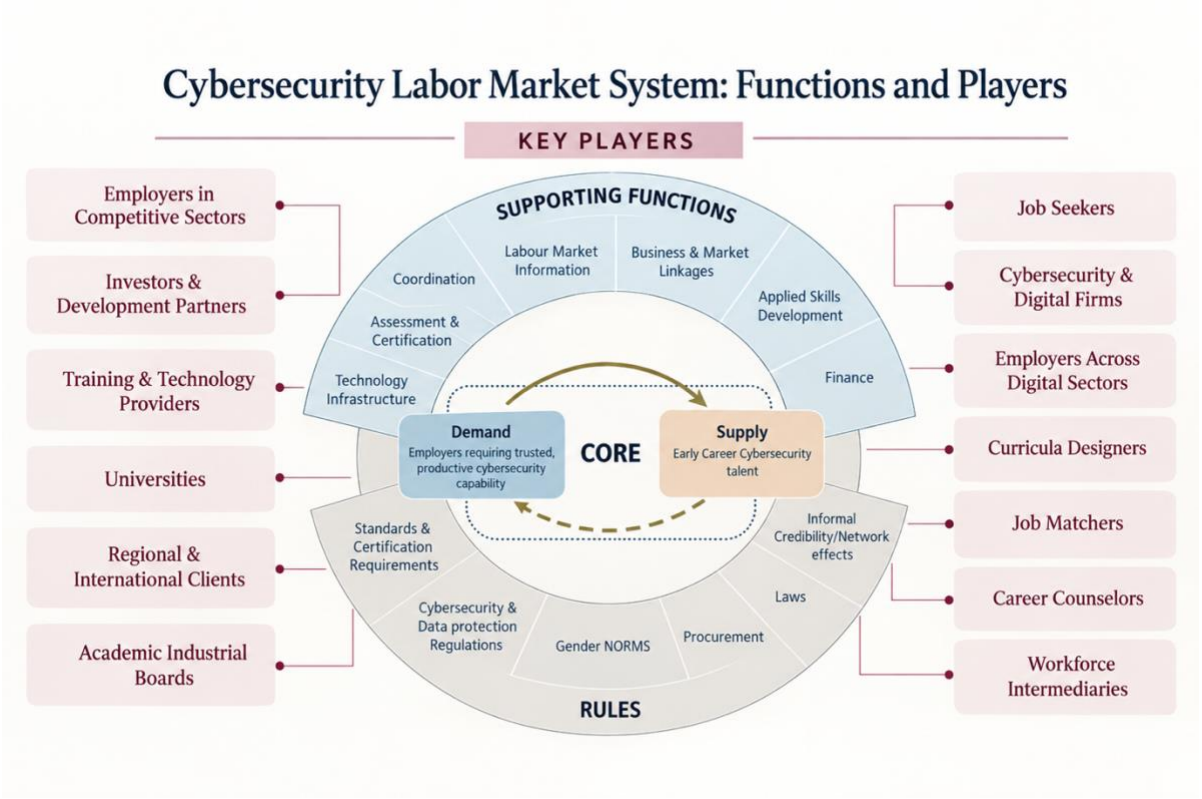


Figure 1: Cybersecurity Labour Market System: Functions & Players

Market System and Constraint Analysis

Market System Analysis

The focal "market system" in this paper is the demand/supply **for entry-level to early-career talent in Jordan's cybersecurity segment of the broader ICT sector**, as illustrated by Figure 1: Cybersecurity Labour Market System: Functions & Players, Its core exchange is between employers that need trusted cybersecurity capability and workers who need access to decent cyber work. Cybersecurity companies, workforce intermediaries and other service providers help convert potential talent into verified capability that employers can confidently recruit or deploy. However, this exchange depends on a wider group of market actors rather than on any single company. Supporting functions include university provision, academy-based training, internships, certification pathways, assessment, signaling, matching, mentoring, employer outreach, financing, and digital platforms. **Government entities contribute policy direction, coordination, standards and market information; employers define demand and provide work-based learning; universities and training providers develop skills; industry associations support signaling and demand aggregation; and private-sector partners and international investors can provide technology, capital, specialist expertise and access to regional markets**

Rules include formal regulations, cyber standards, procurement norms, employer preferences for experience, gender norms, wage expectations, and the informal credibility cues through which firms decide whether a junior candidate is "safe" to hire. This way of framing the case matters because MSD warns against confusing symptoms with root causes and argues that effective intervention should leverage the behavior of system actors rather than substitute for them. **It also requires attention to who currently performs and finances each function, and who would have the incentive and capacity to do so in a competitive, inclusive and sustainable future system.** [17]

The Rough Guide to MSD for youth employment is especially useful here because it conceptualizes youth employment systems as a labour market with three important supporting systems: knowledge/information on labour demand, skills development, and job matching. It also stresses that an effective strategy must be rooted in a conceptual model that reflects local reality, scanning both sector dynamics and labour-market issues and avoiding preconceived service solutions. **Jordan's cybersecurity labour market reflects this problem clearly.** Cybersecurity employment in Jordan is not underperforming because there are no training courses; it is underperforming because the three supporting systems do not connect smoothly enough. Skills development is still too theoretical. Labour demand exists but is cautious and risk sensitive. Matching remains fragmented. **Coordination between employers, education providers and public institutions is also insufficient, while links to private partners, investors and regional demand remain underserved. Together, these weaknesses create commercially valuable opportunities for assessment, practical preparation, matching, supervised deployment and cybersecurity service delivery.**[18]

Systemic Constraint Analysis

The first systemic constraint is the **employability conversion gap** between education and work. The digital skills gap analysis states that most university programmes cover core IT subjects theoretically but with limited practical training; it identifies lack of hands-on experience and weak internship integration as key reasons for low employability. It also highlights its limited curricular coverage of cybersecurity, cloud, and other emerging technologies. This means that the market is producing credentials faster than it is producing deployable workers. For employers, the result is hiring risk. For students, the result is delayed entry. **For cybersecurity firms and workforce intermediaries, the gap creates a potential commercial opportunity to provide assessment, applied preparation, supervised experience and deployment support. Universities, employers and training**

[17] https://www.springfieldcentre.com/

[18] https://beamexchange.org/resources/tools/1752/

providers must nevertheless share responsibility for correcting the underlying skills-development failure. [19]

The second constraint is a **thin mid-level talent pipeline paired with enterprise aversion to junior hiring**. The gap analysis notes that Jordanian companies often need to spend significant time and resources training new hires before they are project-ready, and that shortages of mid-level resources have pushed up salaries and distorted project economics. The age-composition data reinforce the point: firms are not hiring as many 20–24-year-olds as the graduate pipeline would imply. In systems terms, the problem is not just insufficient talent; it is insufficient risk-bearing and insufficient intermediation around the early-career transition.[20] **Employers may be more willing to recruit junior talent when practical capability has been independently verified, initial deployment is supervised, and part of the performance risk is carried by a specialized provider. The commercial value therefore lies in reducing time-to-productivity and recruitment risk, rather than in selling training alone**

The third constraint is the **limited scale of the domestic market and weak business linkages**. GIZ identifies Jordan's limited domestic market, poor linkage to customers, weak promotion in export markets, and access-to-finance frictions as key obstacles to ICT MSME growth. This matters for cyber employment because small firms will be reluctant to invest in junior talent if sales pipelines and payment cycles are uncertain. It also matters because skills providers need enough predictable employer demand to sustain training and deployment pathways. Without stronger linkage to regional buyers or to larger domestic clients, firms may fall back on ad hoc hiring and short-term contracting[21]. **Government entities and industry associations can help aggregate demand and improve market information, while international investors and private-sector partners can provide growth capital, technology partnerships, export connections and access to larger markets. These actors do not replace commercial firms; they improve the conditions under which firms can expand services and sustain employment.**

The fourth constraint is **fragmented demand-side intermediation**. MSD youth-employment guidance warns that interventions can over-focus on upskilling while neglecting the commercial motivations and constraints of employers. Jordan's digital-skills and ICT evidence reflects this problem. Firms need candidates who can work with practical tools, communicate professionally, and become productive quickly, yet the system does not consistently generate or signal those attributes. In the absence of trusted standards, employers use proxies such as prior experience, brand-name certification, or personal networks, raising entry costs for young people and especially those outside established

[19] https://digiskills.jo/Default/En

[20] https://digiskills.jo/Default/En

[21] https://www.giz.de/sites

networks[22]. The required response is a stronger intermediation function connecting verified skills, employer requirements, work-based learning and deployment. This function can be delivered competitively by commercial providers, supported by common signals and standards coordinated by government entities or industry bodies.

The fifth constraint is the **underutilization of women**. The World Bank highlights very low female participation nationally, while Jordan's digital-skills evidence shows that women are heavily represented in ICT education but much less represented in ICT employment[23]. The gap analysis explicitly says that targeted training could deploy trainable female resources more effectively. From an MSD perspective, this is not only an equity issue but a market-efficiency issue. When half the potential pool is only partially converted into the workforce, employers face artificial scarcity and the system loses resilience. For cybersecurity firms, improving women's entry and retention can widen the available talent pool and support business growth. However, commercially viable participation may still require complementary action from employers and government entities to address workplace practices, transport or care constraints, and other inclusion costs that an individual provider cannot recover through its normal revenues. Time-bound development financing may help test solutions, but sustainable functions should ultimately be financed by the actors that benefit from them or justified as public goods.

The sixth constraint is **the mismatch between who pays and who benefits**. Youth often bear the cost of training, but many of the immediate benefits of employability conversion accrue to employers: lower search costs, quicker onboarding, less failed hiring, and reduced internal training expenditure. This payment-benefit mismatch is a classic market-system issue because it leads to underinvestment in practical readiness. MSD would predict that commercial viability improves when an intermediary designs a business model that captures part of that employer-side value. Cybersecurity firms and specialized intermediaries therefore have stronger prospects when employers pay for verified capability, deployment support or productive cybersecurity services, rather than when the model depends primarily on learner fees or continuing grants. Learner payments may remain appropriate for optional, portable certifications, while public or development finance should be limited to public-good, inclusion or early experimentation costs that cannot reasonably be captured by one firm. [24]

A seventh constraint is the weak coordination of functions and financing across the market system. Government entities, employers, education providers, industry associations,

[22] https://www.ilo.org/publications/market-systems-approach-skills-development

[23] www.worldbank.org

[24] https://www.springfieldcentre.com

TABLE (1)[25]: CONSTRAINT/SOLUTION LOGIC AND INDICATORS OF SUSTAINABILITY			
CONSTRAINTS	**SYSTEM RESPONSE**	FINANCING **LOGIC**	INDICATORS
Employer risk and weak trust in junior talent	***Function: Assessment/Certification*** • Verified practical assessment + supervised deployment ***System Players:*** • Service providers deliver; • Employers co-design roles and provide work-based learning; Education providers strengthen foundations. • Government/industry bodies enable standards	***Private:*** • Employers pay when avoided recruitment/training cost and productive value are demonstrated. • Learners may pay for optional portable certifications ***Public:*** • Justified experimentation, accelerate inclusion	Conversion to billable work; repeat purchase; failed-hire reduction; gross margin.
Fragmented skills, demand and matching	**Function:** Labour-market information, skills development and job matching Employer-led role profiles + integrated readiness and matching. **System Players:** • Employers define requirements and co-design preparation; • Universities/training providers align practical curricula; • Cybersecurity providers/intermediaries	**Private:** • Employer pipeline/service fees finance readiness and matching; employer contracts may finance specialized training. **Public:** • Shared standards and neutral market information.	Employer conversion; time-to-hire; retention; provider adoption.

[25] https://springfieldcentre.com

TABLE (1)[25]: CONSTRAINT/SOLUTION LOGIC AND INDICATORS OF SUSTAINABILITY			
CONSTRAINTS	**SYSTEM RESPONSE**	FINANCING **LOGIC**	INDICATORS
	assess, prepare and match candidates; • Government/industry bodies coordinate neutral information and standards.		
Experience barrier	**Function:** Work-based learning, mentoring and supervised deployment Structured work-based learning with expert risk-sharing. **System Players:** • Employers provide practical opportunities and supervision; • Cybersecurity providers organize supervised projects and deployment; • Universities/training providers integrate internships; • Development facilitators support initial testing.	**Private:** • Employer contribution rises as productivity is proven; service contracts recover deployment costs. **Public/development:** • Temporary pilot subsidy declines.	Time-to-productivity; supervisor cost; placement/contract conversion.
Underutilization of women	**Function:** Inclusive recruitment, workforce participation and retention Flexible role design, inclusive recruitment and retention measures. **System Players:** • Employers implement inclusive workplace practices; • Cybersecurity providers/intermediaries support entry and	**Private**: • Employers fund measures with business value. **Public/development:** • Finance justified additional public-good and inclusion costs.	Women's completion, placement and retention; employer willingness to continue financing.

TABLE (1)[25]: CONSTRAINT/SOLUTION LOGIC AND INDICATORS OF SUSTAINABILITY			
CONSTRAINTS	**SYSTEM RESPONSE**	FINANCING **LOGIC**	INDICATORS
	deployment; • Universities/training providers strengthen practical access; •Government/development actors address wider inclusion barriers.		
Limited domestic scale and weak market access	**Function:** Business/market linkages, technology infrastructure and access to finance Technology partnerships, investment and regional customer linkages. **System Players:** • Cybersecurity firms develop market-facing services; • Government/industry associations support demand aggregation and connections; • Investors provide growth capital; • Strategic/technology partners provide tools, expertise and market access; • Domestic/international clients purchase services.	**Private:** • Investment finances scalable assets and expansion; partners contribute where returns are credible. • Customer contracts not investment cover recurring operations. **Public**: • Shared market information and enabling linkages.	Regional contracts; customer concentration; revenue growth; unit economics.
Coordination	**Function**: Market coordination, common standards, labour-market information and financing alignment Coordinate demand, practical skills, assessment, work-based	**Private:** • Employer fees and cybersecurity-service revenues fund recurring commercial functions; investors/partners finance viable expansion.	Continued market-actor participation; repeat transactions; common standards adoption; reduced subsidy dependence;

TABLE (1)[25]: CONSTRAINT/SOLUTION LOGIC AND INDICATORS OF SUSTAINABILITY			
CONSTRAINTS	**SYSTEM RESPONSE**	FINANCING **LOGIC**	INDICATORS
	learning and matching; clarify who performs and finances each function. **System Players:** • Government/industry bodies coordinate neutral functions and standards; • Employers articulate demand and purchase services; • Universities/training providers and cybersecurity firms deliver complementary services; • Investors/strategic partners support expansion; • Development facilitators catalyze early cooperation.	**Public/collective:** • Government/industry bodies support neutral coordination, standards and information; time-bound development finance supports experimentation and public goods.	sustained coordination.

development programmes, commercial firms, private-sector partners and investors may each support parts of the talent pathway, but their activities are often fragmented or temporary. The current system therefore lacks a clear allocation of who performs and who finances assessment, practical preparation, work-based learning, matching, inclusion support, deployment and market coordination. A sustainable future system requires recurring commercial functions to be funded increasingly through employer demand and cybersecurity-service revenue, while neutral coordination, standards and other justified public goods are financed or coordinated by appropriate public or collective institutions.

What makes these constraints **systemic** is that they appear across multiple functions, are reinforced by both formal and informal rules, and cannot be resolved by one-off direct delivery alone. Training more people will not solve the problem without changing employer risk/reward calculation, signaling, matching, and deployment. Nor will subsidies alone if companies still perceive junior talent as slow or costly to absorb. MSD's value here is that it shifts the analysis from "how many youths can be trained?" to "what changes in system

player incentives and behaviors are required to make the market clear this talent commercially?" [26]

Green Circle: Commercial Viability Current Services and Potential Market-System Role

Current commercial services:

Green Circle is first and foremost a commercial cybersecurity company. Its public portfolio includes managed security operations, SOC and threat hunting, incident response, penetration testing, GRC advisory, vulnerability management, threat intelligence and AI/LLM security. These are existing market-facing services sold around cybersecurity capability and risk reduction[27]. This commercial base matters because it anchors the case in an operating business rather than in a stand-alone employment programme.

Current workforce-development activities.

Alongside its commercial cybersecurity services, Green Circle publicly describes hands-on training, expert mentoring, career readiness, market exposure, employer-facing events and supported pathways such as Zero to Hero and Cyber Bridge. These activities show existing capability in practical preparation and employment linkage, but they should be distinguished from Green Circle's established cybersecurity service revenues. The case therefore treats them as evidence of capabilities that could be developed into a clearer commercial workforce offer, subject to validation of employer willingness to pay.[28]

Potential Commercial Role within the Market System:

Building on its existing commercial capabilities and workforce-development experience, Green Circle could productize additional functions that address identified weaknesses in the wider cybersecurity market system while generating sustainable revenue streams. These could include practical workforce readiness, employer-linked assessment, supervised deployment, matching and retention support. The commercial rationale would be strongest where these functions reduce identifiable costs or risks for employers and other buyers and therefore create a clear willingness to pay.

Green Circle has a credible basis for such an offer because its cybersecurity service operations expose it to real tools, workflows, documentation standards and client pain

[26] https://www.springfieldcentre.com/wp-content/uploads/2014/09/2014-09-M4P-Operational-Guide-with-watermark1.pdf

[27] https://www.grcico.com/

[28] https://www.grcico.com/academy.html

points. This can shorten the distance between training and productive work and allow workforce preparation to be designed around actual service requirements. The commercial proposition is therefore stronger when workforce readiness is linked to measurable employer outcomes: lower recruitment risk, faster time-to-productivity and access to deployable cyber capability rather than sold as training alone.

The boundary of the commercial role is equally important. Functions for which a paying customer and recoverable value can be identified may be commercially delivered by Green Circle or peer providers. Functions that depend on neutrality, collective legitimacy or public-good financing should sit elsewhere in the system. This distinction protects the commercial logic of the offer while avoiding dependence on a single provider.

Commercial viability through MSD:

The commercial case rests on willingness to pay. Employers bear identifiable costs when the system fails: long recruitment cycles, expensive internal training, uncertainty about junior capability, delayed deployment and difficulty sourcing specialized talent. The **MSD** approach helps identify which of these frictions can be converted into services with a paying customer.

Green Circle's opportunity is therefore to capture part of the value created when those costs and risks are reduced.

Four revenue logics follow:

- **First:** managed services and supervised deployment can generate revenue where an expanded pool of junior talent (both women and men) contributes under expert oversight to SOC, GRC, documentation, awareness or testing workflows.
- **Second:** employers may pay for pipeline services such as verified assessment, role-based shortlisting and demand-tailored preparation.
- **Third:** retainer or subscription arrangements can provide recurring access to talent pipelines or selected cybersecurity capability.
- **Fourth:** advanced training or portable certification may generate learner or employer fees where the credential has clear market value.

These four scenarios are to be commercially validated and not assumed income streams; however, the implication is that systemic constraint resolution can create commercial value when it improves a transaction that buyers already care about. Practical preparation can reduce onboarding cost; trusted assessment can lower hiring risk; supervised deployment can convert experience from an entry barrier into productive service delivery; and stronger inclusion of women can widen the available talent pool. The commercial test is whether these benefits are sufficiently valuable for employers or other buyers to pay repeatedly.

Framing a Context-Specific Feasible Offer. A feasible offer for Green Circle should therefore be framed around **business pain**, not around beneficiary status. The most promising proposition is a "**Cyber Workforce Readiness and Deployment Service**" targeted at SMEs, regulated sectors, and regional digital-service firms that need cyber capability but cannot efficiently build it alone. The offer would combine candidate sourcing from an expanded talent pool (women and men), practical skilling, supervised project-based apprenticeship, employer matching, retained technical oversight, and quality assurance. Green Circle could test flexible scheduling and remote-compatible cyber functions, while employer and public actors address inclusion constraints that cannot be recovered through the service model [29]. Employers would buy a lower-risk route to acquiring cyber capability. Participants would gain a credible pathway into work. Green Circle would earn from contracts that blend talent intermediation with live service delivery.

Government entities or development programmes could temporarily finance justified public-good and inclusion components, while international investors and private-sector partners could finance scalable digital infrastructure, technology integration and entry into regional markets. Their participation would therefore support scale and market access, but the offer's recurring costs should ultimately be covered by employer fees, managed-service contracts and cybersecurity-service revenue This is context-specific because it fits Jordan's SME-heavy market, thin mid-level pipeline, export orientation, and policy emphasis on digital jobs and practical skilling. [30]

Gender design remains commercially relevant where it expands the usable talent pool.

Green Circle could test flexible scheduling and remote-compatible cyber functions, while employer and public actors address inclusion constraints that cannot be recovered through the service model.

Commercial Value, Revenue Scenarios and Investor Incentives

Commercial sustainability requires more than identifying potential revenue streams for Green Circle. It requires a credible allocation of value, payment and return across the wider market system. The central commercial proposition is that resolving workforce constraints can create measurable private value for employers, cybersecurity providers, investors and

[29] https://invest.jo

[30] https://fundforyouthemployment.nl/

strategic private-sector partners, while selected system-level functions continue to generate public or collective value. A sustainable model therefore depends on matching each function to the actor with both an incentive and a capacity to finance it.

Table 2: Illustrative commercial value and financing logic (below) shows the mutually reinforcing incentives available to all market system stakeholders when a market system development approach is taken in cybersecurity/digital service market.

Table (2): Illustrative commercial value and financing logic				
Actor	**Value / incentive**	**Potential return or revenue**	**Commercial test**	**Appropriate financing**
Cybersecurity providers	More deployable talent; lower delivery constraints; new client offers	MSSP/SOC or project revenue; deployment fees; retainers; subscriptions	Repeat purchase and acceptable margin	Commercial revenue
Employers / buyers	Lower hiring risk; faster productivity; reduced cyber and compliance risk	Cost savings and productivity rather than direct revenue	Purchased service costs less than internal recruitment/training risk	Employer budgets
Investors	Removal of talent constraints on scalable firms and service expansion	Equity appreciation; returns on growth capital	Growth and return remain credible without permanent subsidy	Equity / growth capital
Strategic & technology partners	Technology adoption; market access; larger customer/user base	Licensing, partnerships, service sales, customer acquisition	Participation advances a commercial objective	Cash, in-kind or commercial partnership
Universities / training providers	Employer relevance; stronger placement; specialized demand	Programme fees and delivery contracts	Employer demand and outcomes sustain provision	Education budgets / employer contracts
Government / industry / facilitators	Public goods, standards, inclusion, coordination and learning[31]	Economic/development return rather than firm-level profit	Function persists or transfers after catalytic support	Time-bound public / development finance

[31] https://www.worldbank.org

For Green Circle and peer cybersecurity providers, the most direct revenue scenario is employer-funded workforce and cybersecurity service delivery. Employers may pay for verified assessment, recruitment-risk reduction, role-specific preparation, supervised deployment, managed cybersecurity services, project delivery or retained technical support. The commercial offer is therefore not training for its own sake; it is a lower-risk route to productive cybersecurity capability. Revenue becomes more sustainable where the same talent-development infrastructure supports billable client work, repeat contracts, subscriptions or managed-service relationships rather than depending on one-off learner fees or continuing grants.

A second layer of value accrues to employers and other buyers. Their incentive to participate is the prospect of shorter recruitment cycles, lower failed-hire and onboarding costs, faster time-to-productivity, access to scarce cybersecurity capability and reduced operational or compliance risk. Employer willingness to pay should therefore be tested against these business outcomes. If the cost of purchasing verified readiness or supervised deployment is lower than the cost and risk of building the capability internally, the model has a credible commercial basis.

Investors and strategic private-sector partners have a different but complementary incentive. They do not need to finance employment outcomes as a charitable objective; their rationale is that stronger workforce capability can remove a constraint on business growth. A reliable pipeline of deployable cybersecurity talent can increase the capacity of investee firms to win contracts, launch new service lines, serve regional clients and scale without talent shortages becoming a binding constraint. Investors may capture value through equity appreciation or returns on growth capital, while strategic partners may benefit through commercial partnerships, technology adoption, licensing, market access, customer acquisition or expansion of complementary services. Their participation is therefore most credible where the workforce intervention is linked to an investable growth proposition rather than presented as a stand-alone social programme.

Technology companies and other private-sector partners can also benefit from an expanded user and client base. Providers of platforms, cybersecurity tools, cloud infrastructure, certification or specialist technology may contribute expertise, discounted access, in-kind resources or co-investment where participation supports product adoption, licensing revenue, market entry or access to a larger pool of trained users and enterprise customers. Universities and training providers can similarly benefit through employer-funded programmes, specialized delivery contracts and stronger placement outcomes when curricula and practical preparation respond to demonstrated market demand.[32]

This creates a blended but disciplined financing model. Commercial actors should increasingly finance functions from which they capture direct private value: employers pay for recruitment-risk reduction and productive capability; cybersecurity providers earn from

[32] https://www.ilo.org

service and deployment contracts; investors finance scalable business growth where a return is plausible; and strategic partners invest where participation expands their own commercial opportunities. Government entities, industry bodies and development facilitators should concentrate on functions whose benefits are diffuse or difficult for one firm to appropriate, such as neutral coordination, common standards, market information, inclusion measures and early-stage experimentation. Public or development finance should therefore be catalytic and time-bound rather than a permanent substitute for market revenue.[33]

The commercial test is consequently broader than whether Green Circle can generate income from its workforce readiness/deployment activities. A sustainable market-system outcome would show that Green Circle and other providers can earn acceptable margins from functions customers repeatedly purchase; employers continue paying because the services reduce real business costs or risks; investors and strategic partners commit resources because stronger workforce capability supports growth and return; and other providers can enter, imitate or adapt successful models. Green Circle may monetize its differentiated commercial services, while neutral coordination and public-good functions should remain with appropriate independent, public or collective actors so that the market can strengthen beyond any single firm.

Next Steps

The proposed Cyber Workforce Readiness and Deployment Service, revenue scenarios and division of responsibilities between government entities, commercial providers, employers, investors and development facilitators are therefore analytical propositions requiring validation. A final assessment would be strengthened by interviews and commercial data from Green Circle and peer providers, employer willingness-to-pay research, provider-level cost and margin analysis, investor perspectives and evidence concerning which actors are willing to finance each function after external support ends.

Conclusion

A better-functioning future system would connect cybersecurity demand, practical skills formation, trusted assessment, work-based learning, matching and financing more coherently. Employers would articulate demand earlier and pay for services that demonstrably reduce recruitment or capability risk; cybersecurity providers would compete on differentiated readiness, deployment and service offers; universities and training providers would strengthen applied learning; government and industry bodies would

[33] https://springfieldcentre.com/

coordinate standards, market information and enabling policy; and investors and strategic partners would finance scalable technology, market access and business growth. Development finance would be time-bound and catalytic, supporting experimentation or justified public-good and inclusion costs rather than permanently subsidising routine commercial delivery. The result would be a more competitive cybersecurity market that creates value for Jordan while generating sustainable revenue opportunities for multiple commercial firms, including Green Circle.

This case supports the thesis that addressing systemic employment constraints can generate commercially valuable opportunities for cybersecurity firms, their customers and other market actors, including government. In Jordan, the strategic issue is not simply whether more people can be trained for cybersecurity roles. It is whether the wider cybersecurity and digital labour market can perform the functions required to convert available talent into trusted, productive capability that employers and clients value. The seven constraints identified in this case beginning with the employability conversion gap and extending through employer risk, weak work-based learning and matching, limited absorption of available talent, constrained domestic scale, and weak system coordination represent frictions that carry economic costs for firms as well as policy costs for Jordan.

Green Circle illustrates the commercial opportunity embedded in those frictions. Its existing cybersecurity services should remain analytically distinct from the additional workforce-readiness, deployment and intermediation functions it could potentially offer. The commercial case for expanding into such functions does not rest on an employment objective alone. It rests on whether Green Circle, or other market actors, can solve problems for which customers are willing to pay reducing recruitment and deployment risk, shortening time-to-productivity, improving access to verified skills, supplying supervised project capacity, and connecting Jordanian capability to domestic and international demand. The relevant revenue scenarios therefore include employer-paid assessment and placement, deployment and project fees, managed-service contracts, subscription or retainer arrangements, and investor- or partner-backed expansion where a credible path to recurring commercial revenue exists.

For government and development partners, the implication is to use a Market Systems Development approach to accelerate Jordan's cybersecurity and digital policy goals by improving how the market performs rather than by substituting for market actors. Public and development resources can help address coordination failures, strengthen standards and trusted assessment, improve labour-market information, support stronger links between education providers and employers, de-risk early experimentation, and stimulate work-based learning and matching functions. The purpose of such support should be catalytic: to demonstrate value, align incentives and crowd in firms, investors, training providers and intermediaries that can continue to perform and finance valuable functions after temporary support ends.

This changes the role of development support. Instead of repeatedly financing stand-alone training cohorts or firm-specific activities, an MSD approach asks which underlying function

is failing, why existing actors are not performing it, what incentives or capacities prevent them from doing so, and what limited intervention could enable a durable market response. Government can use policy, standards, procurement, coordination and market information to improve the enabling environment, while development partners can absorb some of the early learning and coordination costs associated with testing new commercial models. Neither should become the permanent provider of functions that firms, employers, investors or other market actors have an incentive to sustain.[34]

The future vision is therefore a better-functioning Jordanian cybersecurity market in which employers communicate demand more clearly; education and training providers respond to changing technical requirements; assessment and certification provide credible signals of capability; intermediaries reduce search and hiring costs; firms develop commercially viable services around talent readiness and deployment; investors can identify scalable business opportunities; and government provides an enabling policy and regulatory environment. In such a system, employment outcomes and commercial growth reinforce one another rather than operating as separate development and business objectives.

The central argument is not that Green Circle alone should solve Jordan's cybersecurity labour-market constraints. Rather, the case demonstrates how an MSD lens can reveal commercially valuable opportunities within those constraints and help government and development partners accelerate policy objectives by enabling multiple market actors to respond. Success would therefore be evidenced not by the continuation of a donor-supported programme, but by repeated transactions, sustained private and public investment where appropriate, adoption or replication by other actors, stronger market functions and commercially viable revenue streams that persist beyond external support. In this sense, MSD offers Jordan a practical route for connecting cybersecurity policy, market development and commercial value while strengthening the country's capacity to supply trusted cybersecurity capability at scale.

[34] https://www.ilo.org/publications/market-systems-analysis-decent-work-user-friendly-guide

References

1. www.ncsc.jo

2. www.memr.gov

3. www.modee.gov.jo

4. www.grcico.com

5. www.grcico.com

6. https://www.springfieldcentre.com

7. https://www.ilo.org

8. https://www.ilo.org/publications/market-systems-analysis-decent-work-user-friendly-guide

9. https://www.linkedin.com/posts/challenge-fund-for-youth-employment_jordan-activity-7392104765536776192-XCdB

10. https://z2h.me/elearning/index.xhtml

11. https://www.giz.de/sites

12. https://invest.jo

13. https://digiskills.jo/Default/En

14. https://ncsc.jo/Ar/List/Policies_and_Strategies_AR

15. https://memr.gov.jo/EBV4.0/Root_Storage/AR/EB_Info_Page/Cyber_Security_Strategy_2025.pdfpe

16. https://invest.jo/index.php/en/investment-sectors/ictbpo

17. https://www.springfieldcentre.com/

18. https://beamexchange.org/resources/tools/1752/

19. https://digiskills.jo/Default/En

20. https://digiskills.jo/Default/En

21. https://www.giz.de/sites

22. https://www.ilo.org/publications/market-systems-approach-skills-development

23. www.worldbank.org

24. https://www.springfieldcentre.com

25. https://www.springfieldcentre.com/wp-content/uploads/2014/09/2014-09-M4P-Operational-Guide-with-watermark1.pdf

26. https://springfieldcentre.com

27. https://www.grcico.com/

28. https://www.grcico.com/academy.html

29. https://invest.jo

30. https://fundforyouthemployment.nl/

31. https://www.worldbank.org

32. https://www.ilo.org

33. https://springfieldcentre.com/

34. https://www.ilo.org/publications/market-systems-analysis-decent-work-user-friendly-guide