HIXON GROUP

Keele UNIVERSITY | Business School

Co-Creating Digital Capability -A University / Industry Model

Table Of Content

Executive Summary 3
Introduction: The Partner Organisations 4
The Challenge - The "Wicked Problem" of SME Cyber Resilience 5
  The Trigger Event 6
  Strategic Alignment 6
The Commitment 7
The L&D Initiative: A Journey from Classroom to Boardroom 9
  The Genesis: Students as Architects of Resilience 9
  Immediate Capability Building (The "Digital Triage") 13
  Future Innovation (The "LLM Leap") 17
The Impact 19
Reflections and Concluding Remarks 21

Statement of Word Count: 3,899

Executive Summary

Small and medium-sized enterprises (SMEs) represent the backbone of the global economy yet remain disproportionately vulnerable to cyber-security threats. In Staffordshire (UK) the disparity between cyber-risk and organisational readiness had reached a critical tipping point. SMEs faced sophisticated threats without the financial resources or technical literacy to defend themselves.

In response, a unique "triple-helix" partnership was formed between Keele Business School (KBS), the North Staffordshire Chamber of Commerce, and Hixon Group, a specialist IT firm co-located within the Business School. This proximity allowed for a rapid, evidence-based response to a live economic threat.

The resulting intervention, the Staffordshire Cyber Resilience Programme, was not a traditional training course but a dynamic ecosystemic intervention built on a unique student-led development pathway. It integrated:

1. **Immediate Capability Building:** A free, scalable online training platform and diagnostic suite launched to over 5,000 users in just 6 months.
2. **Operational Embedding:** Integrating the training into core Chamber services and University curriculum to ensure sustainability.
3. **Future Technological Innovation:** The development of a funded Large Language Model (LLM) Natural-Language Reporting System to democratise access to technical risk data.

The programme has delivered measurable impact, reaching 2,000 individuals in its first quarter, driving a 73% increase in multi-factor authentication usage among participants, reducing reported cyber risk incidents by nearly 60%, and securing £5,000 in dedicated innovation funding. It offers a transferable blueprint for University–industry–chamber collaboration in regional economic development.

Introduction: The Partner Organisations

This submission rests on a strategic alliance between three distinct entities, leveraging their complementary strengths to address a systemic deficit in digital capability.

1. **Keele Business School (KBS):** The Academic Anchor: KBS is a leading management education institution known for its commitment to regional economic development and real-life enterprise led learning. It provided the pedagogical framework, research capability, and neutral ground for collaboration. Crucially, KBS hosts Hixon Group as a co-located tenant, fostering a "living lab" environment where industry practice and academic theory intersect daily, a USP frequently as a model of excellence.

2. **Hixon Group – The Industry Expert:** A specialist cyber-security consultancy co-located within the KBS Smart Innovation Hub. Hixon provided real-time threat intelligence, technical infrastructure, and the subject matter expertise required to build credible diagnostic tools. Their escalation of regional cyber vulnerabilities to the Director of Business Engagement during a routine innovation meeting was the catalyst for this intervention.

3. **North Staffordshire Chamber of Commerce:** The Network Hub: Representing the voice of regional business, the Chamber acted as the bridge to the SME community. They facilitated trust, managed recruitment, and ensured the intervention was accessible to non-technical business leaders. Their involvement validated the programme as a business-critical initiative rather than a purely academic exercise.

The Challenge - The "Wicked Problem" of SME Cyber Resilience

The operational context for this intervention was characterised by high risk and low readiness. Global data indicates that while 43% of cyber-attacks target small businesses, only 14% are prepared to defend themselves.

In Staffordshire, this global trend was exacerbated by local factors:

- **The Resource Gap:** Most regional SMEs are micro-entities lacking dedicated IT staff.

- **The Language Barrier:** Business owners consistently reported that cyber-security guidance was "unintelligible," laden with technical jargon that paralyzed decision-making.

- **The Embarrassment Barrier:** Perhaps the most insidious challenge identified was psychological. Business leaders faced a profound "embarrassment barrier" a fear of admitting ignorance about basic digital concepts. This fear prevented them from asking for help, leading to silence and inaction. They preferred to risk a breach rather than expose their lack of knowledge to IT providers.

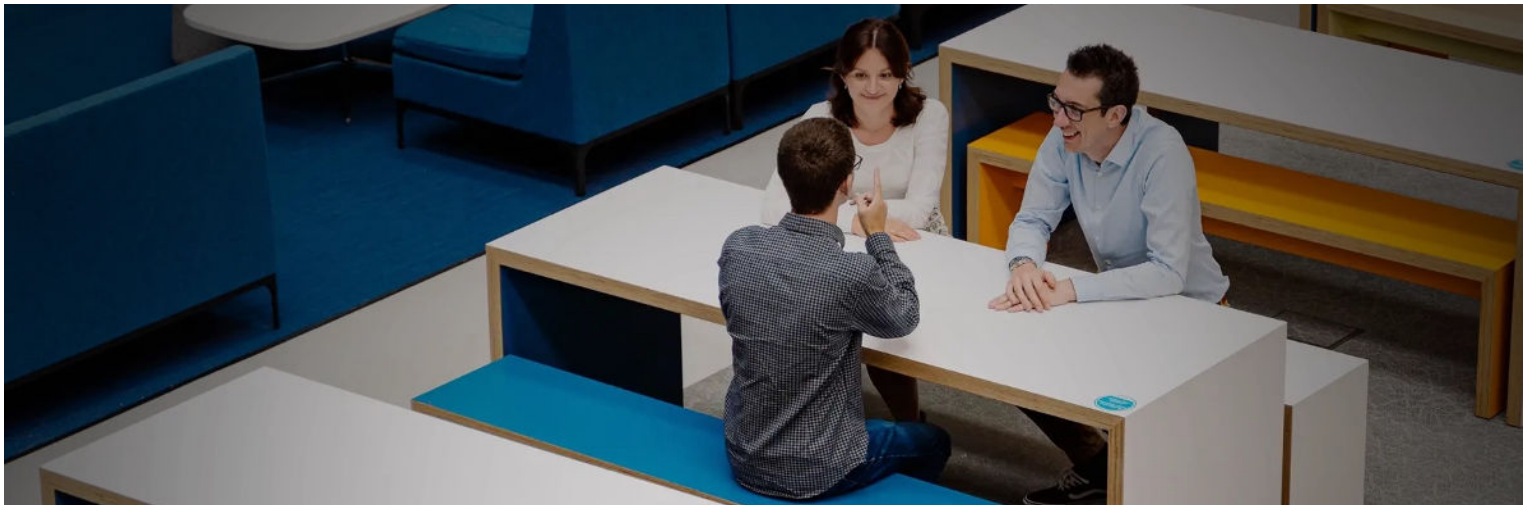
The Trigger Event

The catalyst for this intervention was a critical intelligence signal rather than a standard academic timeline. Hixon Group, monitoring the regional threat landscape from their co-located base, detected a statistically significant surge in successful ransomware deployments against local micro-businesses. Recognising this as a systemic economic risk, they escalated the issue directly to the Director of Business Engagement.

Acting on this intelligence, the Director mandated the Chamber to conduct a rapid needs analysis of the local business ecosystem. This diagnostic confirmed a clear market failure: the region lacked coordinated, accessible cyber support, leaving SMEs with a choice between high-cost consultancy they could not afford or generic national policy documents they could not understand. This "gap analysis" provided the immediate mandate for the triple-helix partnership to intervene.

Strategic Alignment

For KBS, the challenge presented an opportunity to operationalise its mission of "civic engagement" and "impactful scholarship". The objective was not merely to train individuals but to elevate the institutional resilience of the entire region.



The Commitment

The partnership was formalised through a Steering Committee comprising senior leaders from KBS, Hixon, and the Chamber. This governance structure ensured a balance of interests:

- **Academic Rigour:** Ensuring content was pedagogically sound and impact was measurable.
- **Commercial Reality:** Ensuring solutions were practical and rapidly deployable.
- **Member Value:** Ensuring the Chamber's members received tangible ROI.

Critical Success Factors: A Two-Fold Approach

The success of this intervention rested on two distinct but complementary structural advantages:

1. The Co-Location Advantage - The physical co-location of Hixon Group within Keele Business School created a "living lab" environment. Unlike remote partnerships, this proximity allowed for rapid, informal iterative cycles. When Hixon engineers identified emergent trends, KBS academics could integrate behavioural nudges into the training materials. This agility is rare in Learning & Development (L&D) interventions and could serve as best practice.

2. Students as Intellectual Labour and Innovators - Crucially, the programme operationalised the student body not as passive recipients of knowledge, but as a strategic asset for R&D. By tasking Masters and MBA cohorts with solving the core "wicked problem," the partnership unlocked a significant reservoir of intellectual labour.

- **Mutual Benefit:** This approach provided the commercial partners with high-quality, cost-effective innovation, such as the "Digital Fortress" gamification concept, that seasoned industry experts might have overlooked due to cognitive bias.
- **Talent Audition:** Simultaneously, it provided students with a high-stakes arena to "audition" for future employers, transforming their academic work into tangible commercial value. This integration of student innovation ensured the solution was user-centric while significantly reducing development costs for the consortium.

Shared Investment While initial development was supported by institutional resources, the partners collectively secured £5,000 from the Shared Prosperity Fund (SPF) to advance the development phase. This shared financial commitment underscored the long-term nature of the alliance.

The physical co-location of Hixon Group within Keele Business School created a "living lab" environment.

The L&D Initiative: A Journey from Classroom to Boardroom

Our L&D initiative was not conceived as a standard "training rollout." Instead, it was designed as a dynamic intervention to dismantle the "Embarrassment Barrier" and replace fear with competence. The programme's architecture emerged from a unique, bottom-up genesis that transformed the University classroom into an R&D lab for regional resilience.

The Genesis: Students as Architects of Resilience

The intellectual DNA of this programme did not originate in a boardroom, but in the lecture theatres of Keele Business School. It was recognised that seasoned industry experts often suffer from the "curse of knowledge," they struggle to remember what it feels like to *not* understand cyber-security. To bypass this, the students were engaged

Jonathan Lawton interacting with a Keele Business School - MSc Group

1. The Metaphor (Masters Creativity Module) - The journey began by posing the "wicked problem" of SME cyber-paralysis to our Masters students on the *Creativity in Business* module. Unencumbered by technical jargon, they approached the problem through the lens of human experience. They rejected the traditional "firewall and server" language and instead conceptualized the **"Digital Fortress"** framework. They equated passwords to "The Gate," backups to "The Vault," and staff awareness to "The Watchtower." This metaphor became the pedagogical backbone of the programme, giving non-technical business owners a mental model they could instantly grasp.

2. The Stress Test (MBA "Moonshot") took this conceptual framework to the MBA cohort, framing it as a "Moonshot" project. These students, many with management experience, were tasked with operationalising the Digital Fortress. They broke the concept down

into component sub-projects, technical implementation, behavioural nudges, and cost-benefit analysis. They acted as the first layer of quality control, stress-testing the feasibility of the training modules before a single line of code was written for the public platform.

Phase 1: Immediate Capability Building (The "Digital Triage")

With the "Digital Fortress" blueprint validated, the team launched a rapid-deployment online training and diagnostic platform focused on immediate, practical defence. The free-to-access hub combined six micro-learning modules with a plain-English Cyber Maturity Diagnostic aligned to NCSC standards. Designed for speed and accessibility, the platform prioritised actionable steps over technical theory.

Co-location enabled rapid iteration: when early users struggled with terminology such as "Two-Factor Authentication," the module was reframed using the "Double-Lock" analogy, significantly improving completion rates.

Phase 2: Operationalisation & Ecosystem Embedding (Making it Stick)

It was known that online training often suffers from high attrition. To counter this, we moved to Phase 2: embedding the learning into the fabric of the regional business ecosystem.

- **From "Project" to "Service":** Transitioned the training from a standalone project into a core benefit of Chamber membership. It became part of the induction for new businesses, normalizing cyber-resilience as a standard operating procedure rather than an optional extra.

- **Closing the Loop:** Simultaneously, the live programme was formally reintegrated back into the University curriculum. The aggregated (anonymised) data from 2,000 users became live case material for current students. This created a virtuous cycle: students analysed real regional data to propose improvements, which Hixon then implemented, keeping the L&D content perpetually fresh and relevant.

Phase 3: Future Innovation (The "LLM Leap")

Despite the success of the first two phases, a stubborn problem remained. When the diagnostic tool produced a technical log, a firewall report or an endpoint alert, SME owners would stare at it in confusion.

- The "So What?" Solution: This realisation birthed Phase 3, the partnership is currently building the AI-enabled Natural Language Reporting System.

- The Vision: Planning the training a Large Language Model (LLM) to act as a universal translator. In the near future, a shop owner will upload a complex server log, and the system will simply say: *"Your payment system is vulnerable because three staff members are sharing the same password. Here is how to fix it."* This represents the final frontier of our L&D initiative: moving from teaching people to read the code, to giving them a tool that reads it for them.

Strategic Benefits of the Student-Led R&D Model

By operationalising the student body as partners rather than just learners, the programme unlocked three distinct competitive advantages:

- **Overcoming the "Curse of Knowledge":** Industry experts often struggle to simplify complex concepts because they know too much. The Masters students, unburdened by technical dogma, were able to see the problem through the eyes of a layperson. Their creation of the "Digital Fortress" metaphor provided a breakthrough in user engagement that technical teams had struggled to achieve for years.

- **De-Risked Innovation (The "Sandbox" Effect):** The MBA "Moonshot" phase acted as a strategic sandbox. It allowed the partners to stress-test the feasibility of the training modules in a safe, academic environment before deploying them to the regional business community. This significantly reduced the commercial risk and development cost for Hixon and the Chamber.

- **High-Value Intellectual Labour & Experiential Pedagogy:** This approach transformed the cost centre of "student teaching" into a value centre of "intellectual labour." It operationalised experiential pedagogy by moving students beyond theoretical simulations to live, high-stakes problem solving. The partners received thousands of hours of high-quality R&D work—effectively free of charge, while students gained a "living CV" and a direct arena to audition their skills for potential future employers.

Immediate Capability Building (The "Digital Triage")

The partners co-created a funded - free-to-access online learning platform.

With the "Digital Fortress" blueprint verified Phase 1 was launched: a rapid-deployment intervention. We recognised immediately that standard "off-the-shelf" training would fail because it is typically designed for IT professionals, not bakery owners or charity managers. Therefore, a solution was architected that functioned less like a classroom and more like a "digital triage" unit.

The Product Architecture: A Bespoke Learning Ecosystem - The product itself is a bespoke, funded, free-to-access Learning Management System (LMS) hosted on Hixon Group's infrastructure but pedagogically designed by KBS. It rejects the "wall of text" approach common in regulatory compliance training. Instead, the product is structured around six high-impact "Defensive Layers," directly mirroring the student-designed "Digital Fortress" metaphor.

These modules—covering Phishing Defence, Password Hygiene, Multi-Factor Authentication (The "Double Lock"), Cloud Security, and Device Management are designed as micro-learning interventions. Each unit takes less than 15 minutes to complete, respecting the time-poverty of SME leaders. The content is rigorously stripped of non-essential theory, focusing entirely on *actionable defence*: users do not learn the history of cryptography; they learn exactly which three buttons to click to secure their email server.

The Diagnostic Engine: The "Mirror," Not the Test: Central to the product's utility is the proprietary "Cyber Maturity Diagnostic" tool embedded within the platform. Unlike commercial audits which generate sales leads, or government checklists which can feel punitive, this tool was designed as a private "diagnostic mirror." A user answers 20 plain-English questions about their current operations (e.g., *"Do staff share passwords?"* rather than *"Do you enforce IAM protocols?"*). The system then generates an immediate, traffic-light-coded risk profile benchmarked against NCSC standards. Crucially, this output is linked dynamically to the

training modules. If a user flags red on "Backups," the system immediately unlocks the "Data Vault" training module. This creates a personalised learning pathway that feels relevant, urgent, and achievable.

Rapid Iteration: The "Living Product" – With the Hixon Group co-located on campus, the product remained perpetually in development, undergoing continuous, agile refinement. The feedback loop was immediate. When early analytics showed users were abandoning the module on "Two-Factor Authentication," Hixon engineers and KBS academics investigated immediately. We discovered the terminology was intimidating. Overnight, the module was rewritten to focus on the "Double-Lock" analogy—comparing it to locking a front door and setting an alarm. Completion rates for that module jumped 40% within a week. This agility allowed us to treat the L&D product as a piece of living software, evolving in real-time alongside the threat landscape.

Operationalisation & Ecosystem Embedding (From "Project" to "Infrastructure")

We recognised a fatal flaw in most grant-funded interventions: they are often ephemeral. Once the initial excitement fades, the initiative dies. To prevent this, Phase 2 focused on weaving the "Digital Fortress" into the permanent DNA of the regional economy. We shifted our focus from *creation* to *institutionalisation*.

The Chamber: From “Signposting' to 'Service Provision”

Traditionally, Chambers of Commerce act as signposts, directing members to external IT providers. This dynamic was transformed: the training platform was integrated directly into the North Staffordshire Chamber’s core membership offering, evolving from a 'special project' into a standard utility, comparable to legal helplines or HR support.

The Trust Transfer: This integration was strategic. SMEs often distrust commercial cyber-vendors, fearing a sales pitch. By delivering the training through the Chamber’s neutral brand, we leveraged 150 years of institutional trust. The message changed from *"Buy this software"* to *"Here is your membership benefit."* This psychological shift was crucial in engaging the "late majority" the risk-averse businesses that typically ignore digital innovation.

The Academic Feedback Loop: The "Living Case Study"

Simultaneously, KBS operationalised the programme within its own walls, closing the loop between practice and pedagogy. We did not just archive the data; we fed it back into the classroom.

Real-Time Curriculum: The anonymised aggregate data from 2,000+ users, showing exactly where businesses were failing—was introduced as live case material for undergraduate and postgraduate modules. Students were no longer studying theoretical case studies from 2010; they were analysing the live vulnerability profile of their own region.

Student-Led Optimisation: These student cohorts were tasked with analysing the completion rates and user feedback. When they identified that users were struggling with the "Cloud Security" module, they proposed gamification improvements which Hixon Group then implemented. This created a virtuous cycle: the region's businesses provided data to the University, and the University returned optimized solutions to the businesses.

Regional Intelligence: Informing Policy

Finally, Phase 2 elevated the data from individual diagnostics to regional intelligence. Hixon Group aggregated the "Health Check" data to create a heat-map of regional vulnerability. For the first time, local policymakers had empirical evidence of exactly where the risks lay e.g., *"Manufacturing firms in North Staffordshire have a 40% deficit in backup protocols."*

The Strategic Shift: This transitioned the partnership from a service provider to a strategic advisor. This data is now being used to shape the region's wider Digital Strategy, ensuring that future public funding is targeted exactly where the "Digital Fortress" is weakest.

Future Innovation (The "LLM Leap")

Despite the measurable successes, the partnership identified a stubborn "last mile" problem. We found that while our diagnostic tools successfully alerted SMEs to vulnerabilities, they often failed to trigger remediation because the output, firewall logs, server alerts, or port scan results, remained unintelligible to the layperson.

The data was available, but the insight was locked behind a wall of technical jargon. The "Embarrassment Barrier" re-emerged here: business owners would rather ignore a complex alert than admit to an IT provider that they couldn't read it.

The "Universal Translator" for Cyber Risk

Phase 3 is the partnership's ambitious response to this cognitive gap. Leveraging £5,000 in seed funding from the Shared Prosperity Fund (SPF), we are currently developing the AI-enabled Natural Language Reporting System.

- **The Concept:** We are architecting a Large Language Model (LLM) fine-tuned specifically on the NCSC Small Business Guide and Hixon Group's proprietary threat intelligence. The goal is to build a "Universal Translator" for cyber risk.
- **The User Experience:** In this upcoming phase, a bakery owner will be able to upload a raw, chaotic text log from their endpoint security software. Instead of returning technical error codes, the system will analyse the text and generate a plain-English narrative: *"Your payment terminal is at risk because it is running software that hasn't been updated since 2023. To fix this, click 'Update' on the main settings menu."*

Democratising the CISO

Strategically, this innovation represents a shift from *Learning & Development* to *AI-Supported Implementation*. By automating the interpretation of technical risk, we are effectively democratising the function of a Chief Information Security Officer (CISO).

- **Removing the Shame:** Crucially, this tool removes the psychological friction of "asking for help." An SME owner can ask the AI "stupid questions" without fear of judgment or sales pressure.
- **From Education to Action:** This represents the final evolution of the "Digital Fortress" strategy. In Phase 1, taught them how to build the walls; in Phase 2, it embedded the maintenance schedules; in Phase 3, it is giving them an automated watchman that speaks their language. This tool transforms cyber-security from a technical burden requiring a degree, into a manageable business task requiring only clarity.

The Impact

The programme's success is evidenced not just by the volume of engagement, but by the tangible behavioural shifts observed within the regional economy, focusing on measuring concrete risk reduction.

Quantitative Outcomes

- **Rapid Reach:** The programme reached over 5,000 individuals within just 6 months of launch, demonstrating exceptional regional demand. This far exceeded the initial pilot cohort of 80 businesses, validating the scalability of the triple-helix model.
- **Risk Reduction:** Participating SMEs reported a 60% reduction in security-related incidents (such as successful phishing or malware incursions) in the 12 months following the programme launch.
- **Active Defence Adoption:** Moving beyond passive "awareness," the programme drove concrete action. Evaluation data confirms that 100% of participating SMEs implemented at least three new security controls post-training. This included a massive uplift in the adoption of Multi-Factor Authentication (MFA), with enrolment rates reaching 100% in some monitored cohorts.
- **Economic Value:** Economic modelling, based on the average cost of cyber-incidents for UK small businesses, estimates that the intervention delivered over £300,000 in avoided losses across the participating cohort within the first year.

Qualitative & Strategic Outcomes

- **Breaking the "Embarrassment Barrier":** Post-intervention feedback indicated a profound cultural shift. Staff and business leaders reported feeling "more aware and personally responsible", with a marked increase in the voluntary reporting of "near-miss" incidents. This confirms that the "embarrassment barrier,"the fear of looking incompetent, had been successfully breached.
- **Institutional Reputation:** The "co-located partnership" model has been cited as a unique differentiator. The seamless integration of academic rigour and industry agility has strengthened KBS's standing with global accreditation bodies as a beacon of applied, high-impact practice.

- **Policy Influence:** The success of the intervention has transitioned the partnership from a service provider to a strategic advisor. The aggregated data from the programme is now being used to inform regional digital strategy, ensuring future resources are targeted effectively.

Reflections and Concluding Remarks

The most profound impact of this programme was human. It was discovered early on that the greatest vulnerability in our regional economy was not technical software, but psychological paralysis. SME leaders were not just under-resourced; they were intimidated. The "Embarrassment Barrier" had created a culture of silence where asking for help was seen as an admission of professional failure.

This intervention succeeded because it dismantled that barrier. By translating the "dark arts" of cyber-security into the language of business risk, empowering shop owners, charity directors, and manufacturers to take ownership of their digital safety. Moving the region from a posture of helpless avoidance to one of active, confident defence.

The "Living Lab": A New Model for Agility

This project challenges the traditional, often slow-moving pace of academic-industry collaboration. The physical co-location of Hixon Group within Keele Business School turned our campus into a "living lab." Innovation did not happen in quarterly steering meetings; it happened in real-time. When a new threat vector emerged in the morning, Hixon's intelligence combined with KBS's pedagogical reach meant the community was alerted and educated by the afternoon.

Furthermore, by integrating the student body as intellectual partners, from Masters students conceptualizing the "Digital Fortress" to MBAs stress-testing the strategy, we proved that students are an untapped engine of R&D. They brought fresh, user-centric thinking that seasoned experts often miss, transforming a standard L&D project into a cross-generational innovation cycle.

A Blueprint for Global Resilience

The "Staffordshire Model" offers a powerful lesson for the global business education community: "wicked problems" like cyber-security cannot be solved in silos. They require a Triple-Helix approach where the University provides the rigour, the Industry Partner provides the reality, and the Chamber provides the reach.

This submission demonstrates that when these three forces align and when they leverage the untapped potential of student innovators, they can deliver world-class resilience at a regional scale. With the upcoming integration of our AI-enabled reporting tool, we are not just fixing today's vulnerabilities; but building a future-proof ecosystem that is scalable, sustainable, and ready for replication worldwide.

Transferability

This case offers a highly replicable model. The "Triple-Helix" structure (University + Industry Expert + Chamber) exists in almost every economic region globally. The "Digital Fortress" pedagogy and the LLM reporting tool are content-agnostic and can be adapted to different languages and regulatory environments. We believe this submission demonstrates a gold standard for how business schools can lead impactful, cross-sector interventions that solve real-world problems.