SETsquared PARTNERSHIP
Universities of Bath, Bristol, Cardiff,
Exeter, Southampton & Surrey

UKRI Innovate UK

CYBER INVESTMENT REPORT 2025

BRISTOL & BATH
CYBER

Foreword from the SETsquared Partnership

Cyber security is a foundational part of the UK's economy and infrastructure. As digital adoption accelerates and threats evolve, the demand for innovative, scalable cyber solutions has never been greater.

The South West is well placed to meet this demand, with a steady pipeline of ambitious founders building companies that address real-world challenges, especially in security-sensitive and high-assurance markets, underpinned by world-class academic research and national security assets.

Yet, that strength does not always translate into consistent investment. When we initially looked at this sector, we uncovered some stark statistics from 2024. Despite the South West cyber sector accounting for 9% of national jobs and ~8% of UK cybersecurity firms, the region received >1% of the UK's investment. However, the evidence in this report points to a conversion challenge rather than a pipeline problem. Companies are building credible technology and raising early-stage capital, but fewer progress to larger rounds.

The Cyber Invest Programme, funded by Innovate UK, was established in response to this dynamic. It was built on SETsquared's track record of delivering investor readiness training, supporting deep tech start-ups in scaling and connecting them with our ever-growing community of 2,000+ investors.

Our focus was twofold: supporting cyber founders in creating investable propositions, and upskilling investors to engage with confidence in a sector that can appear complex and fragmented. By working on both sides of the market, we aim to reduce friction at the point where opportunity and capital should meet.

This report captures the momentum of the South West's cyber ecosystem, while also highlighting the structural gaps and opportunities that must be addressed to unlock further growth. I hope it serves as a useful resource for investors, policymakers and ecosystem partners, and as a prompt for confident engagement with one of the South West's strategic sectors.

Serena Giaminardi,
Head of Programmes and Investment, SETsquared Partnership

About the SETsquared Partnership

SETsquared is an enterprise partnership between the universities of Bath, Bristol, Cardiff, Exeter, Southampton and Surrey. It helps turn commercially promising academic research and early-stage deep tech ventures into scalable, investable companies that drive economic growth and deliver meaningful impact.

Foreword from Bristol & Bath Cyber

The South West has a long-standing relationship with cyber security, shaped by its role in national security, defence, advanced engineering and digital innovation. Over time, this has created an ecosystem with deep technical capability, specialist expertise and a strong culture of collaboration between industry, academia and the public sector.

What is distinctive about the region is not just the presence of cyber activity, but the nature of it. Many South West cyber companies operate in high-assurance, regulated and security-sensitive environments, where trust, technical depth and long-term resilience matter as much as speed of scale. This has produced businesses that are credible, durable and closely aligned to real-world demand, but which do not always fit conventional investment patterns.

As Director of Bristol & Bath Cyber, I work closely with founders, investors and partners across the region. A consistent theme in those conversations is that the South West does not lack ambition or innovation. Instead, it faces a challenge of visibility, confidence and connection – ensuring that strong cyber capability is understood, supported and backed at the point where companies are ready to grow.

This report provides an important evidence base to support that conversation. By combining national data with a detailed picture of the South West's assets, investment activity and ecosystem dynamics, it helps move the discussion beyond anecdotes and towards a shared understanding of where the opportunities and constraints truly sit.

Importantly, the recommendations set out in this report are grounded in the reality of the ecosystem. They focus on enabling better outcomes through confidence-building, clearer pathways to investment and stronger alignment between founders and investors, rather than proposing new structures or duplicating existing support.

I hope this report is useful not only as an analysis of the South West's cyber investment landscape, but as a prompt for continued collaboration. With the right connections and confidence in place, the region is well positioned to translate its cyber strengths into more consistent and sustainable growth.

Ben Shorrock
Director, Bristol and Bath Cyber

About Bristol & Bath Cyber

Bristol & Bath Cyber is a regional cyber security network supporting the growth of cyber companies across Bristol and Bath. It brings together founders, investors, universities and public-sector partners to strengthen the local ecosystem, increase visibility of cyber capability and support pathways to investment and scale.

Executive Summary

Cyber security is now a core component of the UK's digital, economic and national infrastructure. Nationally, the sector comprises over 2,000 companies, employs more than 65,000 people and generates over £13 billion in annual revenue. Investment activity over the past five years reflects a mature and resilient market, with consistent deal flow despite fluctuations in headline investment values driven by the timing of a small number of large transactions.

Within this national context, the South West of England represents a material but under-realised cyber investment opportunity. The region accounts for around 8% of UK cyber security firms and approximately 9% of sector employment, supported by a concentration of nationally significant assets that underpin long-term demand, capability and credibility.

The South West hosts some of the UK's most important anchor institutions in cyber and security. Cheltenham and Gloucestershire are home to GCHQ and closely aligned with the National Cyber Security Centre, shaping a nationally significant cluster focused on high-assurance, defence-aligned and dual-use cyber technologies. The region also benefits from a strong base of defence, infrastructure and regulated-market employers, creating sustained demand for specialist cyber capability.

Academic and research strength is a defining feature of the ecosystem. The Universities of Bristol and Bath deliver internationally recognised cyber research and doctoral training, including an EPSRC-funded Centre for Doctoral Training in Cyber Security, while institutions across the wider South West contribute undergraduate and postgraduate talent aligned to applied cyber, data and security roles. This depth of research and skills capability consistently feeds company formation, spin-outs and specialist SMEs.

Between 2020 and 2024, cyber security companies in the South West raised investment every year, typically representing 3–10% of UK cyber deals by volume. However, the region's share of total investment value has been more volatile, reflecting the timing of a small number of larger growth-stage rounds rather than a lack of underlying activity.

The evidence points to a conversion challenge rather than a pipeline problem. The South West produces technically credible cyber companies operating in regulated, security-sensitive markets, but fewer progress into larger, lead-led growth rounds. This report therefore sets out a series of practical, investor- and policy-facing recommendations aimed at improving conversion, strengthening investor confidence and enabling more consistent cyber investment outcomes over time, building on the region's existing strengths rather than duplicating activity.

South West Cyber – assets & evidence

National & strategic assets

GCHQ

National Cyber Security Centre

Academic & research strength

EPSRC Centre for Doctoral Training in Cyber Security

University of Bath

University of Bristol

Scale & activity

- ~8% of UK cyber security firms
- ~9% of UK cyber security employment
- 3–10% of UK cyber deals by volume in recent years

Proven companies

immersive

RIPJAR

CLUE

KETS

COHORT PLC
THE INDEPENDENT TECHNOLOGY GROUP

SUREVINE

Context & Why Now

The UK cyber security market at a glance

The UK cyber security sector is now a large, mature and investable market, underpinned by long-term structural demand rather than short-term cycles. The most recent Cyber Security Sectoral Analysis estimates that there are over 2,000 cyber security firms operating across the UK, employing more than 67,000 people and generating in excess of £13 billion in annual revenue. The sector has grown steadily over the past decade and is now embedded across the UK economy.

Investment activity reflects this maturity. Between 2020 and 2024, UK cyber security firms raised capital across hundreds of deals, with deal volumes remaining relatively robust even as total investment value fluctuated year to year. While 2021 represented a peak in aggregate investment value, subsequent years point to a recalibration rather than a retreat, with continued investor appetite for early-stage and growth-stage cyber businesses aligned to clear market needs.

Several long-term structural forces continue to underpin demand. Cyber security now underpins activity across financial services, healthcare, energy, defence, transport and digital infrastructure, and is increasingly intertwined with the deployment of AI and data-driven systems. Regulatory requirements, geopolitical instability, supply-chain risk and the protection of critical national infrastructure have further reinforced cyber security as a long-term priority for both the public and private sectors.

For investors, this context matters because it establishes cyber security not as an emerging or speculative market, but as a core component of the UK's digital and national infrastructure. The question for investors is therefore not whether cyber security is investable, but where differentiated opportunities exist and how regional ecosystems contribute to the national pipeline. This national context provides the baseline against which regional cyber ecosystems should be assessed.

- Over 2,000 cyber security firms nationally
- £13bn+ in annual revenue
- Persistent deal activity despite macroeconomic volatility
- Structural demand driven by AI, regulation, defence and infrastructure

Source: UK Cyber Security Sectoral Analyses 2021–2025

The South West cyber security ecosystem

The South West is a material and established contributor to the UK cyber security ecosystem. National analysis estimates that the region accounts for approximately 8% of UK cyber security firms and around 9% of sector employment, placing it broadly in line with regions such as the North West and Scotland (*UK Cyber Security Sectoral Analysis 2024; 2025*). This reflects a meaningful concentration of cyber capability rather than a nascent or peripheral market.

Cyber activity in the South West is not concentrated in a single location, but distributed across a set of interconnected hubs, each shaped by different assets, institutions and routes to market. Together, these hubs contribute to a region that consistently produces cyber security companies, specialist talent and investable propositions, particularly in regulated and security-sensitive markets.

South West Cyber – at a glance

- ~8% of UK cyber firms
- ~9% of UK cyber employment
- 3–10% of UK cyber deals by volume in recent years
- Strongest in specialist, regulated and defence-aligned markets

Source: UK Cyber Security Sectoral Analyses 2021–2025

Taken together, these indicators point to a region that produces cyber capability at scale, but captures investment unevenly over time. These headline indicators are important, but they only tell part of the story. The nature of the South West's cyber ecosystem helps explain both its strengths and its investment profile.

Anchor assets and clusters

Bristol and Bath form the region's largest concentration of cyber and digital activity and act as its primary hub for software-led and data-driven businesses. The area benefits from a dense employer base spanning start-ups, scale-ups and large technology firms, alongside a strong research and skills pipeline from the University of Bristol, the University of Exeter, and the University of Bath. National analysis repeatedly highlights strengths in computer science, systems engineering, cryptography and AI-related disciplines, which feed directly into cyber company formation and growth.

Companies emerging from this environment tend to focus on security, data protection, identity, privacy-enhancing technologies and cyber-enabled AI. Many serve customers in digital, financial services and other regulated markets, and form a significant proportion of the region's early-stage deal flow .

Cheltenham and Gloucestershire anchor the South West's defence and national security-aligned cyber capability. The presence of GCHQ, combined with a wider ecosystem of defence, intelligence and secure technology employers, has shaped a nationally significant cluster focused on high-assurance cyber, secure communications, cryptography and dual-use technologies. This cluster supports specialist SMEs and spin-outs serving government, defence primes and critical national infrastructure, and represents one of the South West's most distinctive cyber strengths.

Wiltshire and the defence corridor around Corsham add depth in secure networks, operational technology security, critical infrastructure protection and defence digital systems. Firms operating in this part of the ecosystem are often embedded in long-term, contract-led markets where cyber capability is integrated into complex operational environments.

Across the wider South West, including Dorset, Somerset and Cornwall, cyber capability is frequently embedded within broader technology, engineering and infrastructure businesses. In these contexts, cyber security often functions as an enabling technology rather than a standalone product, contributing to areas such as connectivity, resilience, industrial systems and secure-by-design platforms.

Alongside these physical, institutional and employer anchors, the South West's cyber ecosystem is supported by a number of active clusters and networks that play a practical role in convening founders, investors and partners, and in increasing the visibility of cyber capability across the region.

Cyber clusters and networks in the South West

Cyber activity in the South West is supported by a small number of established clusters and networks that connect founders, investors, employers and public-sector organisations. These groups play a practical role in convening the ecosystem, supporting collaboration and increasing visibility of cyber capability across the region.

Bristol and Bath Cyber - https://techspark.co/cyber/
A Bristol and Bath-based cyber community connecting startups, scale-ups, investors and partners through events, programmes and ecosystem activity.

CyNam - https://cynam.org/
A Cheltenham-centred cyber cluster focused on national security, defence-aligned and high-assurance cyber, bringing together founders, investors and public-sector stakeholders.

South West Cyber Security Cluster (SWCSC) - https://southwestcsc.org/
A regional membership network supporting cyber security organisations across the South West through collaboration, knowledge sharing and industry engagement.

Swindon and Wiltshire Cyber Cluster - https://swcybercluster.co.uk/
A growing network aiming to raise the profile of cyber capability across Swindon and Wilthisre and support connections between businesses, academia and public bodies.

Academic and research pipeline

The South West's academic base plays a central role in sustaining the region's cyber security pipeline, providing depth of capability across undergraduate education, postgraduate training and doctoral-level research. Universities in Bristol, Bath and across the wider South West contribute skilled graduates, applied research and spin-out activity, particularly in cryptography, systems engineering, AI and data security.

UKC3 analysis highlights the importance of advanced research capability and doctoral training as foundational inputs to the UK cyber ecosystem, particularly in specialist and high-assurance markets. Institutions in the South West participate in nationally recognised research and doctoral training networks, including EPSRC-funded Centres for Doctoral Training, contributing PhD-level expertise that feeds into defence-aligned SMEs, deep-tech ventures and security-sensitive markets.

Alongside this, the region benefits from a broad education and skills pipeline, spanning early-stage engagement through to postgraduate and professional training. Nationally recognised cyber education provision, further-education pathways and regional coordination help ensure a steady flow of talent into South West cyber companies and employers.

A summary of the South West's cyber education, research and talent pipeline is provided in the accompanying pop-out box.

This combination of depth and breadth underpins the region's ability to generate technically credible cyber companies, often with early validation in regulated or security-sensitive markets, but with longer pathways to commercial scale.

Cyber education, research and talent pipeline in the South West

The South West's cyber ecosystem is strengthened by a joined-up talent and research pipeline, spanning early engagement, further and higher education, postgraduate study and doctoral-level research.

Early-stage pipeline

CyberFirst

The South West participates in the national CyberFirst programme, supporting early engagement in cyber security through schools, bursaries, competitions and outreach. CyberFirst plays a key role in building awareness of cyber careers and developing early technical interest, particularly in areas aligned to defence and national security.

Gloucestershire College

Gloucestershire College delivers cyber and digital provision at further-education level, supporting progression into higher education, apprenticeships and employment. This provision aligns closely with employer demand within the Cheltenham and Gloucestershire cyber and security cluster.

Advanced research and doctoral training

EPSRC Centre for Doctoral Training in Cyber Security (Universities of Bristol and Bath)

The South West hosts an EPSRC-recognised Centre for Doctoral Training in Cyber Security, jointly delivered by the Universities of Bristol and Bath. The CDT provides interdisciplinary PhD-level training across secure systems, cryptography, trust, identity and socio-technical security, with strong links to industry and the public sector.

University of Bristol – Academic Centre of Excellence in Cyber Security Research

The University of Bristol is recognised under the NCSC/EPSRC Academic Centres of Excellence scheme, reflecting nationally significant cyber research capability that underpins doctoral training and specialist spin-outs.

Higher education & postgraduate capability

Bath Spa University delivers undergraduate and postgraduate cyber security programmes, including a hands-on BSc (Hons) Cyber Security and an MSc Cyber Security that equip students with practical defensive and analytical skills to identify and mitigate cyber threats in organisational and infrastructure contexts.

The University of Bath provides postgraduate cyber education through taught MSc programmes alongside interdisciplinary research and training via its Institute for Digital Security and Behaviour, developing advanced skills in digital security, socio-technical risk and cyber-relevant analysis for industry and research contexts.

The University of Bristol offers specialist postgraduate cyber teaching, including MSc degrees in Cyber Security (Infrastructures Security) and Cyber Security (Software Security) informed by world-leading research and applied learning, contributing highly skilled graduates into technical and research-led cyber roles.

The University of Exeter delivers postgraduate cyber education through its MSc Cyber Security Analytics, a multidisciplinary programme combining cyber security, data analytics, law and industry engagement to develop skills in recognising, managing and defending against digital threats and analysing security risks.

The University of Gloucestershire delivers dedicated BSc and MSc Cyber Security programmes, contributing graduate and postgraduate talent aligned to security, risk and applied cyber roles.

The University of Plymouth offers a specialist MSc Cyber Security, supporting postgraduate skills development and applied research capability across the wider South West.

UWE Bristol is recognised by the UK National Cyber Security Centre as a Gold Academic Centre of Excellence in Cyber Security Education, the only institution in the South West to hold this designation. This reflects nationally recognised strength in cyber teaching, industry engagement and skills development across undergraduate and postgraduate programmes.

Research Institutes

RISCS – Research Institute for Sociotechnical Cyber Security

The Research Institute for Sociotechnical Cyber Security (RISCS) is the UK's first academic research institute to focus on understanding the overall security of organisations, including their constituent technology, people, and processes.

Together, these pathways support a full-stack cyber talent pipeline, reinforcing the South West's ability to sustain specialist cyber companies and long-term growth.

Employer base and demand signals

Cyber activity in the South West is underpinned by a diverse and substantial employer base. Nationally, the UK cyber security sector employs around 65,000–67,000 people, reflecting its role as a core component of the UK economy rather than a niche technology segment.

The South West accounts for approximately 9% of UK cyber security employment, indicating a material concentration of organisations that both develop and consume cyber capability. This employer landscape spans start-ups, scale-ups, defence primes, public-sector organisations and large digital firms, creating sustained demand across a range of markets characterised by regulation, security requirements and long-term contracts.

The presence of defence, public-sector and regulated commercial customers is especially significant. While these markets can introduce longer sales cycles and higher compliance requirements, they also support durable demand and defensible market positions for cyber companies operating within them, shaping the investment and growth dynamics explored in later sections.

What kind of companies emerge here

Companies emerging from the South West often combine deep technical capability with early traction in regulated or security-sensitive markets. These businesses can be highly investable, but may require more active investor engagement to navigate complex routes to market and progress into larger growth-stage rounds.

immersive

https://www.immersivelabs.com

A Bristol-founded cyber security skills and resilience platform used by enterprises and government organisations to assess and develop cyber capability.

CLUE

https://www.cluesoftware.com

A Bristol-based company providing secure data and intelligence software for law enforcement, defence and national security users.

GEMBA ADVANTAGE

https://www.gembaadvantage.com

An Exeter-based company working in operational resilience and security for industrial infrastructure environments, with strong relevance to OT and critical systems.

COHORT PLC THE INDEPENDENT TECHNOLOGY GROUP

https://www.cohortplc.com

A Cheltenham-headquartered defence and technology group with cyber and secure systems businesses serving defence, national security and regulated markets.

RIPJAR

https://www.ripjar.com

A Cheltenham-based data intelligence and analytics company with strong roots in national security and applications across cyber, defence and financial crime.

SUREVINE

https://www.surevine.com

A Gloucestershire-based cyber security company specialising in secure collaboration and information sharing for defence and security-sensitive environments.

modux

https://www.modux.co.uk

A Bristol-based company developing secure hardware and embedded systems at the intersection of cyber security, connectivity and infrastructure.

Examples shown for context only and do not imply endorsement.

This profile reflects the ecosystem assets described above and provides important context for the investment patterns explored later

Source: Cyber pullout; CyNam Angel Investment Report; UK Cyber Security Sectoral Analyses

Why this context matters

Taken together, the South West's cyber ecosystem combines material scale, nationally significant assets and consistent early-stage activity. Its strengths lie not in volume-driven, consumer-facing cyber markets, but in specialist, regulated and defence-aligned segments where technical credibility and trust are critical.

This context is essential for interpreting the investment data in Section C, understanding the investor-readiness dynamics set out in Section D, and identifying the priority opportunity areas described in Section E.

The South West Cyber Investment Picture

This section looks at how cyber security investment into the South West has played out over recent years. It focuses on deal activity, investment value and where capital comes from, drawing on the UK Cyber Security Sectoral Analyses and supporting regional investment snapshots.

The aim is not to present the South West as an outlier, but to understand how investment patterns reflect the kind of cyber ecosystem described earlier, and what that means for investors assessing opportunity and risk.

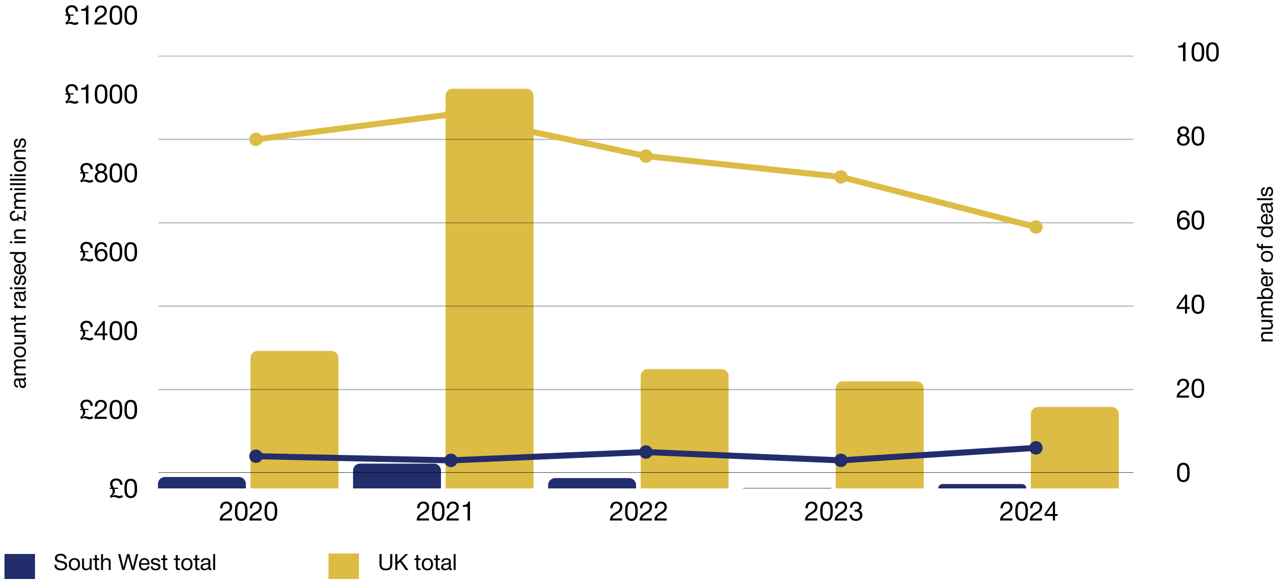
Investment into South West cyber security firms (2020–2024)

Headline data shows a consistent level of cyber investment activity in the South West over time. Deals continue to take place year after year, even as total investment value rises and falls.

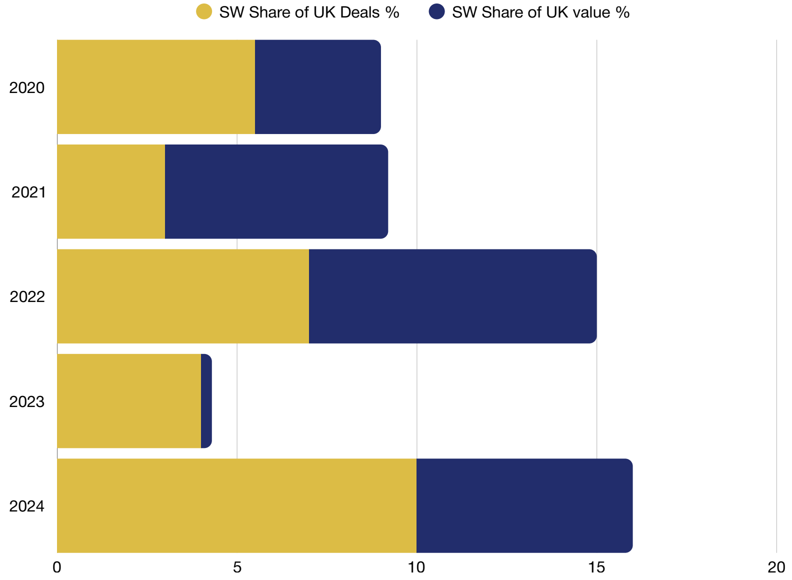
Across the period shown, the South West accounts for a meaningful share of UK cyber deal activity. In most years, its share of deals broadly tracks its share of UK cyber firms and employment. This indicates that the region continues to generate investable companies at the early stages.

What changes from year to year is not whether deals happen, but how much capital is deployed. In some years the region captures a mid-single-digit share of UK cyber investment value. In others, that share drops sharply. This volatility reflects the small number of larger transactions that typically drive annual totals, rather than a collapse in underlying activity.

> **“The South West is a real innovation engine, with a strong pipeline of cyber technology coming out of our universities. That strength hasn’t always translated into consistent national investment outcomes, even though the region produces a significant share of UK cyber activity.”**
>
> *Chris Hill, Investment Programme Manager, SETsquared*



Source: UK Cyber Security Sectoral Analyses 2021–2025



Deal volume versus deal value

Looking more closely at the data, a clear and consistent pattern emerges. The South West’s share of UK cyber deals is typically higher than its share of total investment value. In simple terms, companies are raising capital, but average ticket sizes tend to be smaller and large, lead-led rounds occur less often.

This gap between volume and value is not unusual in cyber. Nationally, headline investment totals are often driven by the timing of a small number of growth-stage raises in any given year. When one of those rounds happens in the South West, the region’s share of investment value rises sharply. When it does not, total value can fall away even where deal activity remains steady.

The implication is important. Year-to-year swings in total investment value often say more about the timing of a few large rounds than about the underlying health of the regional pipeline.

Why deal value can be misleading year to year

Headline investment figures illustrate how a small number of transactions can materially skew annual investment totals, even when underlying deal activity remains steady.

In 2022, cyber security companies in the South West (and South Wales) raised approximately:

- £64.1m total investment
- Across 7 deals
- Largest single raise: £59.9m

In practice, one growth-stage round accounted for the vast majority of total investment value, while the remaining deals were significantly smaller. As a result, aggregate investment figures for the year appear strong, despite only modest changes in deal volume.

This pattern helps explain why the South West's share of UK cyber investment value can fluctuate sharply year to year, even where deal flow remains relatively consistent.

Returning to the broader picture, this distinction matters for investors. Fluctuations in headline investment totals should not be read as a proxy for pipeline strength or weakness.

Alongside occasional larger growth-stage rounds, the South West has developed a growing cohort of cyber companies that have raised meaningful early capital. These businesses operate across defence, digital, infrastructure and deep-tech cyber markets, and demonstrate that investable opportunities exist at scale, even if progression into larger rounds is uneven.

South West Cyber Companies (≥ £500k raised)

BLUESKYTEC
CLUE
COHORT PLC
THE INDEPENDENT TECHNOLOGY GROUP
continual
GEMBA
ADVANTAGE
immersive
KETS
MISSION DECISIONS
modux
Pennant
RIPJAR
SUREVINE

How this compares nationally

At a UK level, cyber investment over the past five years has followed a similar pattern: relatively robust deal volumes alongside volatile aggregate value. Peaks in investment value tend to reflect periods when a small number of companies raise very large rounds, rather than broad-based shifts in activity.

The South West broadly mirrors this national picture, but with greater sensitivity to individual transactions because the absolute number of deals is smaller. As a result, the presence or absence of one or two growth-stage rounds can materially change how the region appears in any single year.

This context is important when interpreting regional investment data. Volatility in annual figures does not imply a lack of opportunity.

Where investment comes from

A significant proportion of the capital flowing into South West cyber companies comes from outside the region, particularly from London and the South East. This is most visible at later stages, where investors tend to look for larger, more de-risked opportunities.

Local angels and early-stage investors play a crucial role in the early life of many companies, providing first capital, validation and support. However, they are less often positioned to lead larger follow-on rounds in specialist cyber markets, particularly where capital requirements and diligence complexity increase.

This can introduce friction into the fundraising process. Rounds may take longer to assemble, syndicates can be fragmented, and founders often need to engage with non-local investors earlier than expected.

This pattern is common across UK regions outside London, but can be more pronounced in cyber due to the specialist knowledge needed to assess technical, regulatory and market risk.

What the data suggests

Taken together, the investment evidence points to a consistent set of conclusions:

- the South West continues to generate investable cyber companies
- deal activity remains present year after year
- investment value is highly sensitive to a small number of larger rounds
- the main gap is at the point where companies seek lead investors and scale

This suggests a conversion challenge rather than a pipeline problem.

Implications for investors

For investors, the South West cyber investment picture points to untapped opportunity rather than elevated risk. The region combines technical depth, specialist markets and steady early-stage activity, but lacks the concentration of repeat lead investors that smooths outcomes over time.

Investors willing to engage earlier, build sector familiarity and play a more active role in leading or anchoring rounds are well placed to shape outcomes in a market that is differentiated, active and not yet crowded.

Early-stage cyber investors and angel networks active in the South West

Early-stage cyber companies in the South West are supported by a number of angel networks and investor groups that provide pre-seed and seed capital, early validation and founder support. These investors typically play a critical role prior to the involvement of larger institutional funds.

Halceon
A cyber-focused angel investment community rooted in Cheltenham, bringing together experienced cyber founders, operators and investors to back early-stage cyber and deep-tech companies.

MAINStream Investor Network
A Cheltenham-based angel investor network established in 2019, supported by Michelmores and Hazlewoods. The network brings together approximately 90 members and focuses on accelerating the growth of angel investment across the South West through regular pitch events and connectivity.

Minerva Business Angel Network
A South West-based angel network supporting early-stage technology businesses, including cyber and security-adjacent companies, through structured syndication and follow-on investment.

Oxford Innovation Finance
An early-stage investor connected to Oxford Innovation's incubation and accelerator network, with experience supporting deep-tech and university-linked spin-outs across the South West and wider UK.

Angel Investors Bristol
Supports and invests in founders across Bristol, the South West and Wales, operating as a network of angels seeking opportunities in innovative start-ups and early growth businesses. Typical investments range from £150k–£500k, utilising SEIS and EIS structures.

SETsquared Investor Network
An investor network linked to the SETsquared university partnership, supporting spin-outs and early-stage technology companies emerging from Bristol, Bath and the wider South West.

Investment Group Bath
Investment Group Bath (IGB), founded in 2024, offers members access to technology sector investment, focusing on fostering innovation and supporting UK ventures. The four co-founders bring decades of combined experience in business leadership and technology investment.

The pipeline and the investor-readiness gap

What the South West cyber pipeline looks like in practice

The South West consistently produces new cyber security companies. They emerge from universities, defence-aligned environments and specialist employers, creating a pipeline that is broad at the early stages. Pre-seed and seed activity shows up year after year across digital, defence, infrastructure and deep-tech cyber markets.

That steady flow is reflected in the investment data. Deals continue to happen, even when the total amount of capital invested moves up and down. In simple terms, companies are forming and raising early money, but fewer are making the jump into larger, growth-stage rounds.

This is closely linked to the kinds of markets many South West cyber companies operate in. Rather than fast-scaling, horizontal SaaS models, many are selling into regulated, security-sensitive or infrastructure-linked environments. These markets tend to validate more slowly and follow less predictable paths to scale, even when the underlying technology is strong.

Founder-side constraints: turning technical depth into investability

Many of the challenges founders face are closely tied to the region's strengths. A large proportion of South West cyber companies are built by deeply technical teams with strong domain expertise, often coming from academic or defence-adjacent backgrounds. This creates high-quality propositions, but it can also make them harder to explain and position for investors.

"Sometimes when you're very, very technical in something, you assume your audience is aware of the knowledge. In deep tech you're often educating and selling at the same time."

Joyann Boyce, Deep Tech Community Manager, techSPARK

This gap shows up most clearly when founders try to communicate opportunity, traction and risk to investors who don't live and breathe cyber. It's compounded for companies selling into defence, public-sector or regulated markets, where sales cycles are longer, procurement is complex and accreditation matters.

Face-to-face engagement often helps surface where the problem lies:

"Getting in front of customers and investors face to face helps you see where that gap is – what needs simplifying, reframing or explaining differently."

Joyann Boyce, Deep Tech Community Manager, techSPARK

These issues don't reflect a lack of quality. They point to a mismatch between technical depth and investor-facing readiness, particularly at the point where companies are trying to raise larger rounds.

Early-stage cyber investors and angel networks active in the South West

Cyber Invest is an early-stage programme delivered by the SETsquared Partnership, supporting cyber security founders as they prepare for engagement with investors. The programme focuses on clarifying propositions, understanding investor expectations and navigating early fundraising conversations in a specialist and highly regulated sector. Once on the programme and when deemed ready, companies are eligible to join the SETsquared Investment Programme which then gives them access to further support and national showcasing opportunities.

The programme provides a practical view of the challenges faced by cyber SMEs as they move from technical validation to investor readiness.

Companies that have completed the Cyber Invest programme include:

CyBOK
HACKTONICS
goodbot
HIGOE
COOL WATERS CYBER SECURITY
Qemplate
SECUR!OUS cyber security confidence

These businesses span a range of cyber and cyber-adjacent applications, from secure systems and assurance to applied security tooling and specialist consultancy.

While programmes like Cyber Invest play an important role at the early stages, the investment evidence in this section shows that the key challenge lies in supporting progression into larger, lead-led growth rounds.

Source: SETsquared – Cyber Invest programme

Investor-side constraints: familiarity, confidence and perceived risk

From the investor side, the challenges are different but closely related. Cyber security, especially in defence-aligned, operational technology or deep-tech contexts, can feel complex and fragmented. Assessing technical risk, regulatory exposure and routes to market often requires deeper diligence than in more familiar software models.

Investors involved in the programme consistently pointed to the importance of founders demonstrating not just technical excellence, but real empathy with the customer problem:

“The strongest signal for us is empathy for the problem owner. Founders who have sat in the customer’s shoes, understand the problem deeply, and can speak the customer’s language.”
Paul Wilkes, Partner, Osney Capital

For generalist investors, limited exposure to specialist cyber markets can translate into higher perceived risk. That often leads to a preference for co-investing rather than leading rounds, which in turn helps explain smaller average ticket sizes and a reliance on non-local lead investors.

Syndication, leadership and the step up to scale

One of the most consistent features of the South West cyber investment landscape is the shortage of investors willing to anchor rounds, particularly at the step from seed to Series A. Local angels and early-stage investors play a vital role early on, but are less often positioned to lead larger raises in specialist cyber markets.

In practice, this leads to a familiar set of outcomes:

- rounds are built through fragmented syndicates
- fundraising takes longer than founders expect
- companies look beyond the region to secure a lead investor

Together, these dynamics contribute to the year-to-year volatility seen in investment totals, even when deal flow itself remains steady.

Founder reality: resilience and longer time horizons

For founders working in specialist cyber markets, progress is rarely smooth or linear. Several highlighted the importance of resilience and realism, particularly in deep-tech and infrastructure-linked areas.

“Scaling is not a hockey stick. It’s a rollercoaster. You’re humbled along the way by what you don’t know, by what customers won’t buy, and by how long funding really has to last.”
Robert Starkwood, Head of Performance, KETS Quantum Security

This is especially relevant in emerging areas such as quantum security, where market education often has to happen alongside product development.

“Surviving long enough means building deep expertise. That gives you the confidence to go out and educate the market, because there’s often no one else people can learn this from.”
Robert Starkwood, Head of Performance, KETS Quantum Security

For investors, this reinforces the need to align expectations around pace, capital efficiency and time horizons when engaging with South West cyber companies.

What this means for conversion

Taken together, the evidence points to a conversion challenge rather than a supply problem. Early-stage activity is strong and consistent. Technical depth and specialist markets are clear strengths. The friction appears when companies try to scale and raise larger rounds.

Investor confidence, familiarity with the sector and a willingness to lead all play a decisive role. Importantly, this gap is structural and addressable, not a sign of weak demand or limited opportunity.

What this means for investors

For investors, the South West offers access to cyber companies with deep technical credibility, differentiated positions and exposure to long-term structural demand. Unlocking that opportunity often means engaging earlier, building sector understanding, being willing to lead or anchor rounds, and accepting growth paths that are longer and less linear.

These characteristics set up the opportunity areas explored next, where the South West’s strengths are most likely to translate into sustained investment outcomes.

Priority opportunity areas

TThe South West's cyber opportunity is not evenly spread across the sector. Its strengths are most evident in a set of specialist, often security-sensitive areas where technical depth, trust and long-term demand matter more than rapid, consumer-led scale.

These areas reflect the region's research base, employer landscape and market access, and help explain why the South West consistently produces high-quality cyber companies, even if growth trajectories are less linear.

What follows are not predictions or bets, but areas where the South West already shows credible momentum and where investor engagement is most likely to translate into outcomes.

Cyber and defence-aligned security

Cyber companies operating at the intersection of defence, national security and government remain one of the South West's most distinctive strengths. This reflects the long-standing presence of defence, intelligence and secure systems employers, particularly in Cheltenham, Gloucestershire and along the wider defence corridor.

Companies in this space typically focus on high-assurance cyber, secure communications, data protection and systems integration. Routes to market are often complex, with longer sales cycles and higher compliance requirements, but demand is durable and closely tied to national priorities.

These characteristics can make defence-aligned cyber less attractive to purely growth-driven capital, but highly relevant to investors with longer time horizons and experience in regulated markets.

South West companies

Cohort plc - A Cheltenham-headquartered defence and technology group with cyber and secure systems businesses serving defence and national security markets.

Surevine - A Gloucestershire-based cyber company specialising in secure collaboration and information sharing for sensitive environments.

Identity, access and trust-based technologies

Identity, authentication and trust-based cyber technologies represent another area of relative strength. These businesses often sit beneath critical digital infrastructure, supporting secure access, data integrity and risk management across regulated sectors.

The South West's capability here draws on strong foundations in cryptography, systems engineering and applied security research, alongside early adoption by public-sector and regulated commercial customers.

Growth in this area is driven less by consumer trends and more by regulatory change, digital transformation and the need for secure, interoperable systems.

South West companies

Ripjar - A Cheltenham-based data intelligence company with roots in national security and applications across cyber, financial crime and risk.

Clue - A Bristol-based provider of secure data and intelligence software used by law enforcement and security-sensitive organisations.

Cyber and operational technology (OT) / critical infrastructure

Cyber security for operational technology and critical infrastructure is an area where demand is growing steadily, but solutions remain technically complex and highly context-specific. The South West's mix of infrastructure, defence and engineering capability makes it well placed to develop companies in this space.

Businesses here often work closely with customers to secure industrial systems, networks and physical infrastructure, and may operate in sectors such as energy, transport, defence or utilities. Sales cycles are long, but customer relationships tend to be sticky once established.

For investors, OT cyber offers exposure to long-term structural demand, but requires comfort with slower scaling and more bespoke delivery models.

South West companies

Gemba Advantage - Based in Exeter, working on operational resilience and security in industrial and infrastructure environments.

Modux - A Bristol-based company developing secure hardware and embedded systems relevant to infrastructure and connectivity.

Secure-by-design and cyber-enabled deep tech

further opportunity lies in companies where cyber security is embedded by design rather than bolted on. This includes businesses working at the intersection of cyber, hardware, data, AI and advanced engineering.

These companies often emerge from research-intensive environments and address problems where security is a prerequisite rather than a feature. While markets may take longer to mature, these businesses can establish strong technical moats and defensible positions.

This profile aligns with the South West's academic strengths and its track record of producing technically credible spin-outs.

South West companies

KETS Quantum Security - Headquartered in Bristol, developing quantum-safe cryptography for future-proof security.

Methodical Minds - A Cheltenham-based cyber and digital engineering consultancy delivering secure-by-design solutions in regulated environments.

Proven Team. Proven Idea.
Team Background
AIRBUS
dyson
Evolito
We started working on this idea in 2018.
We proved the feasibility of eVTOL 'buses' at GKN over 5 years of studies co-funded by the UK government.
11 engineers
~150 years combined experience
Industry renowned founders
SORA
TLT

What these opportunities have in common

Across these opportunity areas, several shared characteristics stand out:

- strong technical depth and domain expertise
- early validation in regulated or security-sensitive markets
- longer and less predictable routes to scale
- demand driven by structural and regulatory forces rather than consumer trends

These traits help explain why South West cyber companies may not always fit standard venture growth patterns, but can offer attractive risk-adjusted opportunities for investors aligned to the sector.

Why the South West is well placed

The South West's advantage in these areas is not accidental. It reflects:

- a strong academic and research base
- long-standing defence and public-sector demand
- a steady flow of technically capable founders
- an ecosystem used to operating in complex, high-assurance environments

Taken together, this creates a pipeline of cyber opportunities that are differentiated at a national level, even if they require a different investment lens.

These opportunity areas provide the context for the practical recommendations that follow, focused on improving how capital engages with the pipeline rather than reshaping the pipeline itself.

What should change: enabling more effective cyber investment

The evidence in this report points to a clear conclusion. The South West does not lack cyber capability, early-stage activity or technical depth. The challenge sits in how that capability converts into consistent, scalable investment outcomes.

The aim of this section is not to propose a new delivery body or a fixed programme of interventions. Instead, it sets out a small number of practical shifts that could improve how investors and founders engage with the cyber pipeline, building on existing activity rather than duplicating it.

Build investor confidence through targeted cyber education

One of the most persistent themes to emerge is investor confidence. For many generalist investors, cyber security remains difficult to assess, particularly in defence-aligned, infrastructure or deep-tech contexts. This can limit appetite to lead rounds, even where opportunity exists.

"The challenge isn't a lack of opportunity – it's that cyber can feel difficult to assess if you haven't seen enough of it".

Chris Hill, Investment Programme Manager, SETsquared

What would help is not broad evangelism, but focused, investor-facing insight that demystifies cyber business models and routes to market.

This could include short, practical briefings on how cyber companies make money, how sales cycles work in regulated markets, and what credible early traction looks like at pre-seed and seed. The aim would be familiarity rather than persuasion, helping investors build confidence through repeated exposure.

Improve visibility of the cyber investment pipeline

The South West produces a steady flow of cyber companies, but visibility of that pipeline is often fragmented. Investors may encounter opportunities sporadically, making it harder to build conviction or track progress over time.

Rather than creating new platforms, a lighter-touch approach focused on curation would be more effective. Regular snapshots of investor-ready companies, using consistent profiles and shared at predictable points in the year, would allow investors to see momentum building rather than making one-off decisions.

Over time, this kind of visibility supports earlier engagement and increases the likelihood of lead investment when companies reach the right stage.

Strengthen peer learning among cyber investors

Confidence in specialist sectors often grows fastest through peer interaction. While there are active angel networks in the South West, opportunities for cyber-specific investor learning and deal discussion remain limited.

Several investors highlighted the value of learning how others think about cyber opportunities.

"Confidence often comes from seeing how other investors think about a deal, not just analysing it alone."

Paul Wilkes, Partner, Osney Capital

Small, invite-only sessions focused on shared learning rather than pitching could help build collective confidence, support co-investment and reduce the perceived risk of leading rounds. Importantly, this would complement existing networks rather than compete with them.

Support founders at the point of conversion

As set out earlier, many South West cyber founders are technically strong but face challenges articulating opportunity, traction and growth in investor terms, particularly when operating in complex or regulated markets.

Targeted, time-limited support at the point where companies begin to fundraise could make a meaningful difference. This might focus on refining investor narratives, explaining sales cycles and procurement clearly, and aligning fundraising plans with the expectations of different investor types.

The emphasis here is on conversion, not capability building for its own sake.

Align cyber activity with wider access-to-finance work

Cyber investment does not sit in isolation. Many of the issues identified in this report also apply to adjacent areas such as AI, defence and deep tech.

Ensuring cyber-specific activity is embedded within wider access-to-finance and innovation initiatives would help avoid duplication and maximise impact. This includes aligning investor engagement, sharing learning across sectors, and using existing convening moments rather than creating parallel structures.

What success would look like

Success should not be judged solely on headline investment totals in any single year. A more meaningful measure would be greater consistency and predictability over time, reflecting improved conversion rather than one-off spikes.

“Success isn’t just bigger numbers in one year – it’s seeing companies progress more predictably over time.”

Chris Hill, Investment Programme Manager, SETsquared

In practice, this would mean more lead-led rounds, smoother progression from seed to growth stages, and stronger alignment between the South West’s technical strengths and investor behaviour.

SETsquared PARTNERSHIP
Universities of Bath, Bristol, Cardiff,
Exeter, Southampton & Surrey

About the SETsquared Partnership

SETsquared is an enterprise partnership between the universities of Bath, Bristol, Cardiff, Exeter, Southampton and Surrey. It helps turn commercially promising academic research and early-stage deep tech ventures into scalable, investable companies that drive economic growth and deliver meaningful impact.

https://www.setsquared.co.uk/

BRISTOL & BATH
CYBER

About Bristol & Bath Cyber

Bristol & Bath Cyber is a regional cyber security network supporting the growth of cyber companies across Bristol and Bath. It brings together founders, investors, universities and public-sector partners to strengthen the local ecosystem, increase visibility of cyber capability and support pathways to investment and scale.

https://techspark.co/cyber/

Sources

A UK Cyber Growth Action Plan – UK Government
https://www.gov.uk/government/publications/a-uk-cyber-growth-action-plan

Beauhurst – Defence, Cyber and Deep Tech Investment Reports – Beauhurst
https://www.beauhurst.com/research/

CyberFirst Programme – UK National Cyber Security Centre
https://www.ncsc.gov.uk/cyberfirst

CyNam – Unlocking Angel Investment Potential in Cyber (Redacted) – CyNam / Cheltenham Chamber of Commerce
https://cheltenhamchamber.org.uk/wp-content/uploads/2025/07/Cynam-Report-_-Unlocking-Angel-Investment-Potential-in-Cyber-Redacted.pdf

EPSRC – Centres for Doctoral Training in Cyber Security – UK Research and Innovation
https://www.ukri.org/councils/epsrc/

RISCS – Regional Institute for Cyber and Security Skills
https://riscs.org.uk

UK Cyber Security Sectoral Analysis 2020 – UK Government
https://www.gov.uk/government/publications/uk-cyber-security-sectoral-analysis-2020

UK Cyber Security Sectoral Analysis 2021 – UK Government
https://www.gov.uk/government/publications/uk-cyber-security-sectoral-analysis-2021

UK Cyber Security Sectoral Analysis 2022 – UK Government
https://www.gov.uk/government/publications/uk-cyber-security-sectoral-analysis-2022

UK Cyber Security Sectoral Analysis 2023 – UK Government
https://www.gov.uk/government/publications/uk-cyber-security-sectoral-analysis-2023

UK Cyber Security Sectoral Analysis 2024 – UK Government (DSIT)
https://www.gov.uk/government/publications/uk-cyber-security-sectoral-analysis-2024

UK Cyber Security Sectoral Analysis 2025 – UK Government (DSIT)
https://www.gov.uk/government/publications/uk-cyber-security-sectoral-analysis-2025

University of Bath https://www.bath.ac.uk

University of Bristol https://www.bristol.ac.uk

University of Gloucestershire https://www.glos.ac.uk

University of Plymouth https://www.plymouth.ac.uk

University of the West of England (UWE Bristol) https://www.uwe.ac.uk

Western Gateway Cyber Gateway Report – Western Gateway Partnership
https://www.western-gateway.co.uk/publication/cyber-gateway-report