# Scaling a Solo Cybersecurity Consulting Practice - Business Plan Research

*by Dinis Cruz and ChatGPT Deep Research, 2024/04/07*

## Market Demand for Cybersecurity Consulting and Training

**Rapid Growth in Cybersecurity Spending:** Organizations worldwide are significantly increasing their cybersecurity investments. Global cybersecurity spending is projected to reach **$458.9 billion by 2025** (Boost Recurring Revenue with Profitable Cybersecurity Offerings | ConnectWise). In one survey, **78% of organizations planned to boost cybersecurity spending in the next year**, reflecting a broad recognition of escalating cyber threats. This surge in spending is not limited to tools and software – many companies are allocating budgets for expertise and services to bolster their defenses.

**Skills Shortage and Internal Capability Gaps:** A well-documented **cybersecurity talent shortage** is driving demand for external consultants and training services. Companies struggle to fill roles – with an estimated **2.8 million cybersecurity jobs unfilled globally** (Closing the Gap in the Cybersecurity Talent Shortage | BCG) and an average 28% vacancy rate that **impedes their ability to address threats**. New technologies (like AI) introduce fresh vulnerabilities, making it even more urgent for organizations to have workers with up-to-date skills . Many firms now realize they **"lack candidates with the desired skills"** internally, which boosts demand for consulting expertise and staff training to fill those gaps.

**Emphasis on Upskilling and Continuous Learning:** In response to the talent gap, companies are heavily prioritizing internal team development. Industry research recommends that organizations *"offer the current workforce opportunities for upskilling and continuous learning, including sponsoring certifications and providing internal and external training."*. Put simply, investing in employees' security skills is now seen as *"fundamental, critical"* to building resilient teams (2024 ISC2 Cybersecurity Workforce Study). Even during tight budgets, forward-looking organizations continue funding training, conference attendance, and coaching for their cybersecurity staff This environment creates strong market demand for services like in-house workshops, mentoring programs, and tailored training curricula delivered by external experts.

**Threat Intelligence and Specialized Services:** The consultant's niche of **cyber threat intelligence** is also in high demand. The global threat intelligence market is growing at over **12% CAGR**, expanding from ~$13.5 billion in 2023 to an estimated **$43.3 billion by 2033** (Threat Intelligence Market to Reach $43.3 Billion,) . This growth is driven by the rise of sophisticated attacks and the need to protect critical infrastructure. However, a **lack of skilled professionals to implement threat intel solutions** is cited as a barrier for organizations. Companies often need guidance to build out threat intelligence functions, interpret threat data, and train their teams on using intel – a clear opening for consultants who can develop internal capability.

**Regulatory Pressures Increasing Demand:** Compliance requirements are another factor fueling market demand for training and internal security improvements. Regulations like GDPR and HIPAA **mandate that companies implement adequate cybersecurity training** for staff to protect sensitive data (Worldwide Cyber Security Training Market Research Report 2025, Forecast to 2031 – PW Consulting). Non-compliance can lead to hefty fines, which *incentivizes organizations to adopt robust training programs* . Many firms are not only training to "check the box" for compliance, but also to **foster a culture of security awareness at every level**. This trend benefits consultants offering security education, as even resource-constrained organizations must find ways to educate their teams. One industry expert observed the *"huge skills gap in security"* and noted that companies had tried to fill it with technology, but *"training can help fill that gap better than anything else."* (Pay What You Can Training from John Strand - Black Hills Information Security | CompTIA Instructors Network) This recognition is driving businesses to seek external training and mentoring expertise to truly improve their security posture.

In summary, **current market conditions strongly favor cybersecurity consulting and training services**. A confluence of factors – relentless cyberattacks, a shortage of experienced talent, new tech risks, and compliance mandates – is pushing organizations to invest in both external advisors and the development of their internal teams. A solo consultant who can help companies build internal capabilities (through threat intelligence expertise, staff upskilling, and mentorship) is positioned in a growing niche with ample demand.

## Scalable Revenue Models for a Hybrid Service-Product Business

For a one-person consulting practice aspiring to scale, choosing the right revenue model is crucial. A **hybrid service-product approach** can generate more stable income and support growth beyond the consultant's personal billable hours. Below is a comparison of several viable revenue models, with an emphasis on recurring revenue, on-demand services, and low overhead:

| Revenue Model | Description | Recurring? | Pros | Cons |
|---|---|---|---|---|
| **Project-Based Consulting** | One-off projects or hourly consulting engagements for clients (e.g. security assessments, audits). | No (one-time) | Simple to start; immediate cash for work delivered. | Income is unpredictable; hard to scale beyond the solo consultant's hours. |
| **Retainer / Subscription Services** | Clients pay a flat monthly or quarterly fee for ongoing services. For example, a *Virtual CISO (vCISO)* service providing on-demand security leadership and guidance. | Yes (recurring) | Predictable cash flow and long-term client relationships (Moving to a professional services subscription model) smoother revenue stream improves stability. Clients get continuous access to expertise without negotiating new contracts each time | Requires delivering continuous value; risk of under-scoping (if client needs exceed expectations). Must carefully manage time across subscribers. |
| **Productized Training & Workshops** | Developing repeatable training offerings – e.g. a standardized workshop or an online course – and selling them to multiple customers. Could be sold per seat or via a subscription for ongoing training access. | Partial (one-off per training; or recurring if subscription-based) | Scales expertise beyond one-to-one consulting; can train many people at once. Online courses or recurring workshop series create assets that generate income repeatedly. Low marginal cost for additional participants. | High upfront effort to create quality content. Competitive market (many training providers). To make recurring, may need continual content updates or a subscription model for new modules. |

| Revenue Model | Description | Recurring? | Pros | Cons |
|---|---|---|---|---|
| **Managed Services (Lightweight)** | Providing security services on an ongoing basis, possibly with automation or subcontractor help – e.g. managed threat intelligence reports, continuous monitoring (MDR) for SMEs, or a “security coach” service. Often structured as monthly plans. | Yes (recurring) | High client stickiness and monthly revenue. Leverages tools to deliver value at scale (e.g. automated threat intel feeds, regular risk reports). Can grow by onboarding more clients on the same service model. | Requires some infrastructure or tooling (though this can be cloud-based to stay lean). Service quality must be maintained 24/7 in some cases. If over-reliant on the solo consultant, can be a strain – may need to bring in partners or software for scalability. |
| **On-Demand Advisory** | Offering consulting in bite-sized increments or as-needed. For instance, a client purchases a block of hours or can request emergency consulting at a premium rate. | Maybe (if clients repeatedly buy hours) | Flexible for clients with sporadic needs; can charge premium for urgent or ad-hoc requests. Minimal ongoing commitment required from either side. | Unpredictable usage – hard to forecast revenue. The consultant must remain available on short notice. Not truly recurring unless formalized into a retainer. |
| **Membership or Content Subscription** | Creating a productized information service, such as a **threat intelligence newsletter**, a private community, or a library of resources for paying members. Clients (or individuals) subscribe for continuous updates, reports, or mentorship forums. | Yes (recurring) | Leverages the consultant’s expertise into a product that can reach many subscribers at once. Low overhead if delivered digitally (e.g. email newsletter or community platform). Recurring revenue without constant one-on-one work. | Growth depends on offering unique value (content must be high quality and regularly updated). Also requires marketing to grow subscriber base. Engagement needs to be maintained to prevent churn. |

In practice, a **combination of these models often works best** for a hybrid business. For example, the consultant might maintain a few **subscription retainer clients** (for steady income), while also **productizing** some knowledge into a training course or subscription resource (to scale reach). This hybrid approach allows earning recurring revenue while still taking on high-value projects. Crucially, it decouples growth from strictly working more hours – which is essential for scaling beyond a solo operation.

**Emphasizing Recurring Revenue:** Shifting from purely hourly billing to a recurring **“as-a-Service” model** is a proven strategy for scalability. In the professional services sector, subscription models are becoming popular because they offer more predictable revenue and stronger client loyalty (Moving to a professional services subscription model). Clients appreciate having ongoing support available and often prefer a flat fee they can budget for, rather than surprise bills. For the consultant, this means steadier cash flow and the ability to plan and invest in the business with less uncertainty. As an example, some cybersecurity consultancies now offer **vCISO services on a subscription basis** – essentially acting as a part-time Chief Information Security Officer for multiple clients. This was the case with Eden Data, a startup which *“outsources cybersecurity and compliance needs for a flat monthly price, rather than charging by the hour”* (Starter Story: Learn How People Are Starting Successful Businesses). That recurring revenue approach enabled Eden Data to rapidly reach **$45K in monthly recurring revenue (MRR)** with a small team. This illustrates the power of subscription models in turning a one-person service into a scalable business.

**On-Demand and Low Overhead Services:** In crafting revenue streams, it's wise to play to a solo consultant’s agility and low overhead. **On-demand offerings** (like emergency incident response or ad-hoc coaching sessions) can command premium prices and leverage the consultant’s flexibility. Additionally, any **digital products or services** (reports, toolkits, e-learning content) can be delivered with virtually no physical overhead – aligning with a lean, serverless business model. The goal is to avoid revenue models that require heavy fixed costs (e.g. owning data centers or expensive software development upfront) and instead utilize cloud services or existing platforms. For instance, if offering a managed threat intelligence feed, one could use cloud functions (serverless architecture) to aggregate and email out threat reports to clients, incurring costs only per use rather than maintaining servers. This keeps the business **“asset-light”** and scalable without large capital investments.

In sum, **viable revenue models for a solo cybersecurity business include**: retainer-based consulting (e.g. vCISO), productized training services, subscription content or tool access, and value-added on-demand services. The common thread is to **maximize recurring income and scalability** while minimizing one-off transactional work. This mix provides a foundation to hire subcontractors or staff as needed, since recurring revenue can fund their involvement and the productized elements can be sold beyond just the principal consultant’s time.

## Case Studies and Competitors in Solo Cybersecurity Ventures

Examining how others have grown solo or micro cybersecurity businesses offers valuable insights. Below are a few **case studies and examples** of individuals or small teams who scaled consulting and training ventures, highlighting their service structure, market positioning, and growth path:

- **Eden Data (Virtual CISO for Startups):** Founded by Taylor Hersom in 2020, Eden Data began as a one-person cybersecurity consultancy targeting tech startups. Hersom noticed many startups couldn't afford a full-time CISO, so he offered a **fractional CISO service on a subscription model** (Starter Story: Learn How People Are Starting Successful Businesses). Clients pay a flat monthly fee for outsourced security and compliance leadership. By packaging strategic consulting as an ongoing service, Eden Data achieved rapid growth – reaching **$45,000 in monthly recurring revenue** with just 4 team members in under two years. The business scaled entirely remotely with minimal startup costs. This case demonstrates how a **single-consultant practice can scale by focusing on a niche (startups) and a recurring-value offering**. The flat-rate vCISO model differentiates them from hourly consultants and creates a steady income that supported expansion to a 20-person team by 2023.
- **Fractional CISO (Rob Black's Consultancy):** Rob Black launched *Fractional CISO* in 2017 as a one-man operation providing vCISO services and security workshops. Over **5+ years, he grew the company from 1 person to 18 employees** (66 months in - what I've learned starting a cybersecurity company.). A key to his model was treating the business as a **"CISO-as-a-Service"** firm – essentially a *lean consulting startup focused on recurring vCISO engagements*. Black emphasizes content marketing (he runs a cybersecurity newsletter and blog) and developed packaged offerings like a **Cybersecurity Workshop Series** to train client teams. By having multiple service lines (fractional leadership, compliance consulting, training) all delivered with low overhead, Fractional CISO managed to scale staff while remaining profitable. This case study underlines the importance of **service packaging, marketing, and gradually adding subcontractors or employees** once revenue streams are steady.
- **Competitors and Niche Peers:** The solo consultant will likely encounter both individual competitors and larger firms in the cybersecurity training and mentoring space. Large providers (like SANS Institute, which offers security training courses) are well-established, but they operate with high fees and big overhead. This leaves room for **leaner, more personalized offerings**. For example, **Black Hills Information Security (BHIS)** started as a small consultancy and built a strong community presence by offering free or "pay-what-you-can" training (through their Antisyphon training arm). BHIS's founder John Strand noted that traditional training was too expensive for many, and by lowering barriers he could both **help fill the skills gap** and create goodwill that attracts business (Pay What You Can Training from John Strand - Black Hills Information Security | CompTIA Instructors Network). BHIS grew a global following via webinars and affordable courses, which in turn funneled demand for their consulting services. This

demonstrates an innovative model where **training isn’t just a revenue stream, but also a marketing and talent pipeline** – a strategy a solo consultant can emulate on a smaller scale (e.g. hosting workshops or webinars to build credibility and a client base).

- **Mentorship-Focused Micro-Businesses:** A few professionals have carved out a niche specifically in career development and team mentoring for cybersecurity. These often start as a personal brand – for instance, an expert offers coaching to junior security teams or runs a subscription community for security professionals. While not always publicly documented, success stories exist where a solo mentor becomes a go-to resource for multiple companies’ staff training. They productize their mentorship via scheduled coaching sessions, curated learning paths, and perhaps an online forum or Slack channel for members. Over time, such a business can scale by **hiring additional mentors on a contract basis** to serve more clients. This is somewhat analogous to executive coaching businesses, but in the cybersecurity domain. The competitive advantage here is the deep personalization and real-world experience a seasoned practitioner brings, compared to generic training vendors.

When analyzing competitors, it’s clear that **differentiation and specialization** are key. The solo consultant’s edge can be a highly specialized skill (like threat intelligence) combined with a personalized, high-touch service (like building an internal intel program alongside the client team, then mentoring their analysts). Many boutique security firms that succeeded started with a niche focus and grew by word of mouth and community engagement rather than big advertising budgets. The case studies above reinforce a few points: **recurring service models (vCISO, etc.) provide stability**, **content marketing and thought leadership build credibility**, and **scaling often involves hiring carefully or partnering** (to extend capacity while keeping overhead low). A new entrant should map out the landscape of similar offerings, but these examples show there is room for a small, passion-driven business that provides quality over quantity.

## Best Practices for Launching a Lean, Low-Overhead Cyber Consulting Startup

Building a scalable business from a one-person consultancy requires a **lean startup mindset** – maximizing impact while minimizing costs. Below are best practices and practical tips for a solo cybersecurity consultant aiming to grow a **serverless, low-overhead operation** with modern tools, subcontracting, and AI integration:

**1. Adopt a Cloud-First, Serverless Infrastructure:** Keep the technology stack lightweight by leveraging cloud services and serverless platforms. There’s no need to invest in physical servers or complex data centers. Instead, use solutions like **Software-as-a-Service (SaaS)** tools for everyday operations (email, CRM, project management) and **serverless computing** for any custom applications. For example, if you develop a small tool to support client work (such as a script to analyze threat feeds), deploy it on AWS Lambda or similar services so it scales automatically and only incurs cost per use. This approach ensures **low overhead** – you're not paying for idle infrastructure. It also improves reliability and scalability from day one. A lean consulting startup can run its entire business on cloud-based tools: consider using platforms like Microsoft 365 or Google Workspace for collaboration, a cloud-based password manager and vault for managing client credentials, and virtual lab environments (cloud VMs or containers) for any hands-on security testing. By **outsourcing IT infrastructure to cloud providers**, the consultant can focus on delivering value without the burden of maintaining hardware.

**2. Utilize a Modern Tool Stack for Efficiency:** Embracing the right tools can dramatically reduce the workload on a small team. Some categories and examples include:

- **Project & Knowledge Management:** Tools like Notion or Confluence for maintaining playbooks, client documentation, and training materials in an organized, shareable way. This avoids cumbersome paperwork and helps when bringing in subcontractors (they can quickly get up to speed via shared docs).
- **Automation and Scripting:** Wherever possible, automate repetitive tasks. This could mean using simple Python scripts for data collection and report generation, or integrating services with APIs (for instance, auto-pulling threat intel data into a report template). Automation saves time and ensures consistency in deliverables.
- **Client Communication and Delivery:** Rely on virtual meeting platforms and learning management systems. For example, deliver training workshops via webinars (Zoom/Teams) to save travel costs, and record them for reuse. If mentoring, schedule regular calls or use Slack/Discord communities for continuous engagement without physical presence.
- **Professional Services Automation (PSA):** As the business grows, a lightweight PSA tool (or even just a combination of calendaring, time-tracking, and invoicing software) will help manage multiple clients efficiently. There are **"no-code" and inexpensive tools** that can integrate scheduling, billing, and CRM, ensuring that even as you scale to multiple clients or subcontractors, coordination remains smooth.

By investing in such a tool stack, the solo consultant can **punch above their weight**, delivering work with the efficiency of a larger firm. Importantly, many of these tools are affordable or have free tiers, aligning with the low-overhead philosophy.

**3. Implement a Subcontractor / Gig Model for Scaling Expertise:** When the workload grows or a project demands skills outside your core strengths, consider leveraging subcontractors or a network of freelance experts. Many successful small consultancies operate with a **"flexible workforce"** – the core solo consultant plus a circle of trusted independents they can bring in for specific engagements. For instance, if a client needs cloud security architecture review and that's not your specialty, you can subcontract a cloud security architect for that part of the project. This model means you **only incur labor costs when you have revenue to support it**, avoiding the fixed expense of full-time hires. It's important to set clear agreements (NDAs, contractor rates, and quality standards) and possibly use contract management platforms for ease. By cultivating a reputation as a fair and reliable partner, you can also become part of others' networks – sharing work opportunities in both directions. This aligns with the *"gig economy"* trend in consulting, where niche experts collaborate on an as-needed basis. The benefit is two-fold: you can take on larger or more complex contracts by augmenting your capacity, and you maintain a **lean core team** without permanent salaries and benefits overhead. Just as tech startups scale using outsourced components until they're ready to justify in-house staff, a consulting startup should **scale through partnerships** first. Over time, if the business achieves steady recurring revenue, you might convert some contractors to employees or continue operating with the agile contractor model.

**4. Leverage Content Marketing and Thought Leadership (Low-Cost Marketing):** Marketing a consulting business doesn't have to mean expensive ads or trade shows. A proven strategy for lean consulting startups is **content marketing** – sharing valuable insights to build credibility and attract clients organically. This could involve starting a technical blog, releasing short research reports, hosting free webinars, or active participation in cybersecurity forums and social media (LinkedIn posts, Twitter threads, etc. discussing threat trends or career tips). For example, posting a well-researched article on improving threat intelligence processes internally can showcase your expertise to potential clients. Many industry figures have successfully grown their client base by giving away knowledge; it establishes trust and often leads to referrals. Additionally, offering a **free monthly newsletter** with curated threat intel or security team leadership tips can keep you on the radar of prospective clients. The only cost is your time, and it doubles as continuous learning since you'll stay up-to-date while writing content. Over time, this thought leadership can create inbound demand, reducing the need for a large salesforce. It's essentially a low-overhead marketing funnel – one that also aligns with the passion for education and helping others (which the prompt indicates is a driver for this consultant).

**5. Integrate LLMs and AI to Amplify Productivity:** Modern AI, especially large language models (LLMs) like GPT-4, can be a force multiplier for a solo or small team. Embracing **AI assistance** can streamline both service delivery and operations. Some practical uses include:

- *Report Generation and Editing:* Drafting security assessment reports or threat briefs can be time-consuming. An AI like ChatGPT can help generate initial drafts of findings, summarize technical data, or polish language. The consultant still provides the expertise and verification, but AI can cut writing time significantly. In fact, **45% of cybersecurity teams have already implemented GenAI tools to augment tasks like report writing and**

**incident analysis** (2024 ISC2 Cybersecurity Workforce Study). This shows that AI is becoming a mainstream aid in the field, expected to *"bridge skills gaps [and] improve threat detection"*. A lean consultancy should capitalize on these tools to deliver faster without needing more staff.

- *Internal Research and Knowledge*: When preparing a training or tackling an unfamiliar issue, an LLM can quickly summarize relevant information (with the necessary caution for accuracy). It's like having a research assistant on call. For example, you might prompt an AI for the latest tactics of a certain threat group when building a threat intel briefing, then verify and enrich that info with your own analysis. This saves hours scanning dozens of sources.
- *Client-Facing Tools:* Some consultants even integrate AI into their service offerings. One idea is providing clients with an AI-powered chatbot trained on the company's policies or past security questions – so client employees can ask the chatbot basic security questions (like "how do I report a phishing email?") and get instant answers. This kind of lightweight product can add value to a consulting engagement without heavy development work (since APIs for LLMs are readily available). It demonstrates innovation and can be a differentiator.
- *Business Automation:* AI can assist in drafting proposals, generating marketing content, or analyzing survey results from clients. For instance, if you run a security awareness survey internally for a client, an LLM could help parse open-ended responses and highlight common themes, giving you quick talking points for your recommendations.

When using AI, of course, **guardrails and quality control** are vital – especially in cybersecurity where accuracy is paramount. Data privacy must be considered (avoiding feeding sensitive client data into public AI services). However, when used wisely, LLMs let a tiny team produce outputs comparable to a much larger team. As evidence of the trend, even big vendors like Microsoft are launching tools such as *Security Copilot* (an AI assistant for security analysts) to speed up tasks like threat hunting and incident reporting (2024 ISC2 Cybersecurity Workforce Study). A nimble consultancy can ride this wave by integrating AI at every suitable opportunity to maintain a competitive edge with minimal cost.

**6. Financial Discipline and Lean Operations:** Running a low-overhead business also means keeping fixed expenses to a minimum and being strategic with investments. Operate initially from a home office or co-working space rather than renting an office. Use **open-source tools** where possible (there are plenty of open-source cybersecurity tools for things like threat intel, monitoring, etc.) to avoid costly licenses. Keep travel minimal by doing work remotely; if in-person meetings or training are necessary, plan them efficiently or bill them to the client. Essentially, follow lean startup principles: validate offerings on a small scale before spending more. For example, pilot a new training workshop with one client (or even free for a friendly organization) to get feedback, *before* pouring resources into polishing a full-fledged product that might miss the mark. This iterative approach prevents wasted overhead on services or products that don't resonate.

**7. Cultivate Partnerships and Ecosystem Connections:** Lastly, leverage partnerships as a growth and cost-saving strategy. Partner with complementary service providers – for instance, an IT managed service provider (MSP) who lacks in-house security expertise might white-label your services to their clients, providing you a pipeline of business without marketing spend (in return, they broaden their portfolio). Or partner with security product companies as an official consultant who can implement their solution; they might refer clients to you in exchange for you recommending their tool where appropriate. Being part of an ecosystem can greatly amplify a solo business's reach. It's effectively using **others' channels** at low cost. Just as subcontractors extend delivery capacity, partnerships extend sales capacity.

In conclusion, the **best practices for a lean consulting startup** revolve around making smart use of technology, maintaining flexibility, and avoiding heavy investments until truly needed. By **running "serverless" (both technically and organizationally)** – i.e., using cloud tech and a fluid talent model – the business can scale up or down painlessly. This provides resilience; the cost base remains low during slow periods, but the operation can expand to seize opportunities during high demand. Combining that with modern tools and AI means a solo cybersecurity consultant can realistically compete with far larger firms in terms of output and innovation, all while staying true to a passion for helping companies and individuals grow in cybersecurity capabilities.

**Sources:**

1. BCG / Global Cybersecurity Forum – *"2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap."* (Oct 2024). Highlights the worldwide talent shortage and the need for upskilling internal teams (Closing the Gap in the Cybersecurity Talent Shortage | BCG) .
2. ConnectWise (MSP Resources) – *"Market demand for cybersecurity services"* (2023). Notes that **78% of organizations plan to increase cybersecurity investment** in the coming year (Boost Recurring Revenue with Profitable Cybersecurity Offerings | ConnectWise), reflecting surging demand for security expertise.
3. Allied Market Research – *Threat Intelligence Market Forecast 2023–2033* (Feb 2025). Reports the threat intelligence market's growth from **$13.5B in 2023 to $43.3B by 2033 (12.4% CAGR)** and points out the **lack of skilled professionals** as a growth barrier (Threat Intelligence Market to Reach $43.3 Billion,).
4. Training Industry / PW Consulting – *Cybersecurity Training Market Trends* (2024). Discusses how regulations like **GDPR mandate employee cybersecurity training**, pushing organizations to invest in robust training programs (Worldwide Cyber Security Training Market Research Report 2025, Forecast to 2031 – PW Consulting). Also emphasizes the shift to a culture of continuous security learning.

5. Starter Story – *“How I Started a $45K/Month Cybersecurity Consulting Firm”* (Eden Data case study, 2023). Describes how Eden Data scaled to ~$2.76M/year with a **flat-fee virtual CISO subscription model**, fully remote and low-overhead (Starter Story: Learn How People Are Starting Successful Businesses).

6. Fractional CISO Blog – *“66 Months In: Lessons from Starting a Cybersecurity Company”* by Rob Black (Jan 2023). Shares insights from growing a one-man vCISO consultancy to 18 employees, underlining the value of reading, service packaging, and treating it as a “CISO-as-a-Service” business (66 months in - what I've learned starting a cybersecurity company.).

7. Rocketlane – *“Transitioning Your Professional Services Business to a Subscription Model”* (Feb 2024). Explains benefits of recurring subscription models for consulting, noting they provide **consistent cash flow and value delivery** for clients and providers (Moving to a professional services subscription model).

8. ISC^2^ Cybersecurity Workforce Study (2024). Emphasizes that after years of budget cuts, **investment in skills development is more crucial than ever** to address security risks (2024 ISC2 Cybersecurity Workforce Study). Also finds **45% of cyber teams use GenAI tools** already, expecting big benefits in efficiency.

9. John Strand (Black Hills InfoSec) via CompTIA Network (2021) – Discussing *“Pay What You Can”* training. Highlights the **huge cybersecurity skills gap** and asserts *“training can help fill that gap better than anything else”* (Pay What You Can Training from John Strand - Black Hills Information Security | CompTIA Instructors Network), leading to innovative training approaches to upskill more people. This exemplifies aligning a business model with industry needs and social good, which in turn built BHIS’s brand.