Cybersecurity Entrepreneurship Ideas

Danielle Caplinger

Old Dominion University

CYSE 494

Professor Batchelder

October 19, 2025

Individual Ideas Assessment 1

1. **Overview and Need:**

   My first idea would be an accelerator platform for cybersecurity compliance and risk assessments. This platform would be customizable based on the compliance or regulatory standards a given business must comply with, and would then provide step-by-step guides, risk scoring, identification of necessary vulnerability scans, and cyber insurance recommendations. There would also be a people-first consulting side to this where I would be able to explain some of these standards and act as coordinator between MSPs, SOCs, or ethical hacking teams that need to be involved to meet such requirements. Many small-to-medium businesses or startups are required to comply with certain regulations or standards, but don't have the resources or expertise to understand, implement, or document them. Without following these guidelines, though, businesses are exposed to liability issues or penalties from federal and state law enforcement. Right now, there is not an integrated platform that addresses cyber compliance and insurance issues at the same time or one that includes the human consulting perspective.

2. **Evaluation of Potential:**

   There is an increasing market demand for this kind of platform as tech startups and small businesses seek higher cybersecurity practices for their own liability or for legal requirements. A platform-based product is very scalable, especially since it can be cloud based. The human consultancy aspect is not as scalable. However, the more expertise given that can be integrated into the platform through some form of chatbot or FAQs would make it more scalable in the long term. The biggest challenge would be that legal and regulatory content changes can be very different based on the industry or regulation

version. Keeping such quantities of information up-to-date will be difficult to ensure no liability issues.

3. **Discovery Process:**

   I discovered this opportunity based on the last few IT companies I have worked for, and being able to see clients struggle with similar issues. One company in particular was a Managed IT Services Provider (MSP) and many of our clients were from various industries and subject to different regulations when it came to cyber compliance. Having a singular platform that an MSP can provide or the business themselves can buy would have made it much easier for them to handle these kinds of issues. Even at that company, we would have to outsource various individuals or organizations to handle all of these details that aren't part of a standard IT or cybersecurity package.

Individual Ideas Assessment 2

1. **Overview and Need:**

   This idea would be a digital-forensics-on-demand service where small businesses that experience a data breach or cyber incident can immediately request forensic analysis and triage. This can address the gap where businesses don't always have digital forensics tools available because they don't expect to need them. However, once they do, cybersecurity teams, cyber insurance claims analysts, and legal entities often require specialized information that only digital forensics professionals can provide. This service would automate the triage process, enable backups and snapshots, and curate the reports necessary for any legal proceedings or insurance claims.

2. **Evaluation of Potential:**

This product has a high market demand because small-to-medium sized businesses are increasingly being targeted for cyber crimes but don't necessarily have the resources for an in-house forensic team or the capability to hire an external one indefinitely. Profitability would be dependent on the retainer model for how assistance can be requested. An incident-fee would cover the bulk of the costs and then an ongoing subscription for monitoring after the incident would allow for the most coverage for consumers while also ensuring profitability for the business. There will be some challenges in the form of how to differentiate from Managed Services Providers, but I think this also presents an opportunity to partner with them to have a higher client base that can utilize our specialist services.

3. **Discovery Process:**

   I first thought about this idea at my old company when a client experienced a cyber incident and did not have any digital forensics tools in place. Because of their industry, though, they were required to have certain verifications of digital forensics analysis. We, as the managed IT provider were then responsible for either learning the necessary tools, which was a steep learning curve, or outsourcing once again to a forensics team. Hiring a professional forensics team that is used to having ongoing protection was extremely expensive, making me wonder about the feasibility of having a pricing model that only uses on-demand services.

Comparative Analysis

Both of these ideas would be feasible from a marketing perspective because there is high demand for these services, especially with the increasing amounts of cyber attacks and regulations on how to handle cybersecurity as an organization. They also focus on a market of

small-to-medium sized businesses that struggle with this specialized expertise and would need to outsource it with either a product or a different consulting firm. For the compliance monitoring idea, there is not a simple automated tool that would be able to replace legal cybersecurity expertise, which is already a niche professional group. For the digital forensics idea, there is not an immediately remote response forensic service on the market for small businesses.

The revenue models for both businesses are different with one being a long-term subscription model and the other as an as-needed retainer fee and potential short-to-medium-term subscription. This makes the digital forensics process harder to gain revenue in the beginning, but I believe this is made up for in its ability to scale. The digital forensics idea can have more aspects automated as digital forensics tools can be automated more easily than the legal and regulatory information for an ever-increasing number of industries, requirements, and revision standards. From a competition standpoint, the digital forensics platform competes against high-cost long-term forensic firms which small businesses usually can't afford or using public labs that take months, if not years, to get results from. The compliancy platform competes with governance and compliancy platforms that are already built into existing tools like Azure and Sophos. Finally, the skills and resources are vastly different for these two ideas. The compliancy one would require legal expertise beyond my current understanding and a continuous learning cycle to remain up-to-date. The digital forensics one, on the other hand, does require some human understanding but more so relies on using automated tools that are increasingly open-source. This also eliminates the costs necessary for starting the platform.

Most Plausible Idea

Overall, I think the digital forensics on-demand service has the most potential. Based on my analysis, it has a good focus, market outlook, competitive advantage, profitability, and aligns

to my current skills and resources the most. Although I find the compliancy platform very interesting, I am not sure on its feasibility right now as my business.