So You Want to Run a Cybersecurity Startup

Cait von Schnetlage, MBA
CEO
Full Suite Solutions

The potential for entrepreneurship in information security has piqued the interest of many techies who haven't yet had the opportunity to strike out on their own. The reasons for not starting a company vary almost as much as the reasons to do so. With 90% of tech startups failing, it is easy to see why entrepreneurship isn't for the faint of heart.[1]

Demand for cybersecurity has increased dramatically due to the global surge in cyber-attacks. Supply has followed suit, and 2015 has become the year of the cybersecurity startup. While many can play, few will win, and even those that seem like a sure bet can fail. Take for example the publicly traded cybersecurity company ISC8, which held over 200 patents and $160M in federal government contracts – and filed for bankruptcy in 2014. The risks are big, but with Gartner's forecasts estimating that total spending for information security in 2015 will exceed $76.9 billion, so are the potential rewards.[2]

Bright-eyed cybersecurity experts have two choices: remain utterly nonplussed when contemplating diving into the shark tank; or develop a well-thought-out strategy for success and cross entrepreneurship off their bucket list. With the right strategies, a cybersecurity guru can become a business guru.

Write a Strong Business Plan

A business plan is the paper incarnate of the company it describes. If anything seems odd in a plan, chances are there is something odd in the business, and "odd" can be very expensive. The first step is to develop a strengths, weaknesses, opportunities, and threats (SWOT) analysis to isolate the factors that may impact your company's success. In this case, strengths and weaknesses are internal attributes within the organization and its management, and opportunities and threats are external factors that can open or close doors for your business.

The business plan should be a combination of research and business processes (a series of actionable items that is developed to achieve an organizational goal, such as sales, support, or marketing). Many of these processes have overlapping tasks which can result in redundancies in the business. If there are redundancies described in the business plan, management is more than likely doubling their resources and efforts on processes that should be simplified and consolidated. Customer Relationship Management (CRM) software can save companies many labor hours by eliminating redundancies.

When writing the plan, avoid writing it like an academic paper. Instead, write it in a magazine format with attention to graphics and the key points you wish to make. Successful entrepreneurs understand that time is money; write succinctly and with purpose, and make your key arguments stand out.

Business Plans as Diagnostic Tools

A business plan isn't just for sending out to venture capitalists – it's also an effective diagnostic tool. If business processes can't easily be mapped out in accordance with the plan, the various back end and front end departments are ineffectively integrated, often resulting in a lack of communication between different departments in the company. In the cybersecurity field, it can also result in severe vulnerabilities in networks, hardware, and software, which can lead to the loss of confidential data. Changing business plans too often indicates a lack of focus, as the company may not have tried an approach long enough to determine whether or not it is actually successful. If a business plan is too long, it can indicate unnecessary complications or a lack of specialization. If it is too short, the company typically lacks attention to risk mitigation and a long-term vision of its direction.

Specialization Is the Key to Success

Well before cybersecurity was even an industry, Adam Smith published *The Wealth of Nations* in 1776. Smith asserts that specialization and the division of labor is the key to economic success. As the cybersecurity industry

experiences significant growth, the need for further specialization becomes more pressing. Unlike Benjamin Franklin, who was experimenting with electricity around the same time Smith was working on *The Wealth of Nations*, most of us are not outstanding polymaths who can stay on top of rapidly changing technologies and processes in addition to making sales and running a company.

The concept of specialization in the field of cybersecurity is critical for several different reasons. First and foremost, applications and devices obsolesce rapidly. Moore's Law states that the computing power of chips will double approximately every two years. It is no longer just a statement so much as a self-fulfilling prophecy as industry leaders strive to meet this benchmark. Increased processing power expands the performance of modern technology, so companies who fail to keep with the latest hardware and software applications are left in the dust.

Demand for cybersecurity has increased dramatically due to the global surge in cyber-attacks. Supply has followed suit, and 2015 has become the year of the cybersecurity startup.

Market Segmentation

Another reason for specialization is to successfully carve out a niche and capture market share. Though seemingly counterintuitive, trying to appeal to everyone actually appeals to no one. Customers need to be able to identify with the companies they buy from, and failing to deliver a strong value proposition promptly loses the attention of target audiences. Though cybersecurity is still an emerging industry where supply has not yet met demand, certain markets in the field will quickly become saturated, and firms without a strong customer base and a competitive advantage will surely fail.

When deciding on your primary market segment, it is important to clearly define the mission of your company. Just as an infosec engineer may choose to specialize in penetration testing and the exploitation of vulnerabilities, an entrepreneur will need to decide whether to focus on federal or commercial contracts, as the two cultures are vastly different. This is not to say one can't eventually straddle both worlds, but in the beginning, specialization is key.

The cybersecurity firm ISC8 held a strong market share up until the company's rebranding in 2011. The firm filed for bankruptcy in 2014, not long after they attempted to shift from government contracting to high-profit margin commercial spaces. ISC8's bankruptcy could arguably be attributed largely to the firm's acquisition of Bivio Networks, which included not just the technologies the company owned, but also sales, engineering, managerial, and operational resources. Many companies who are new to the acquisition process overvalue the opportunity and underestimate the amount of resources necessary for successful integration. Bivio Networks was in financial trouble at the time of the acquisition, and ISC8 made the risky decision of hitching their wagon to a dead horse by entering the commercial side of the cybersecurity industry through a failing company.

A strong and consistent corporate culture is critical for companies wishing to grow and expand. One of ISC8's biggest mistakes was to shift their focus from government contracts to the wild west of commercial cybersecurity without clear segmentation of their federal and commercial markets. Both public and private sectors hold a massive potential for strong revenue, but commercial sector work is often high risk and high reward, which requires much different risk mitigation strategies than public sector work.

Price for Scalability

Pricing service offerings can be quite difficult for even the most seasoned entrepreneur, let alone cybersecurity professionals new to the role. There are several different strategies to incorporate into pricing to ensure that services are delivered on time and within budget. When determining the level of effort necessary to complete a job, many new business owners fail at accurately estimating costs and labor. It is prudent to include the hours it takes to land the contract, as well as to establish pricing with an eye on the company's future development.

A contractor may be happy that they are billing $100 per hour for a 40-hour job, but if it took 30 hours to land the contract, the contractor is making $57.14 per hour. $57.14 per hour is not enough money to build a scalable company or put aside money to reinvest back into business development. Looking at these numbers, sales carves out a huge chunk of time that could be spent billing clients. A smarter alternative would be to raise the billable hourly

rate to $125 per hour and hire salespeople to work on commission for 10% of the final contracted amount.

Those Without Sales Fail

One of the biggest reasons small companies fail is a lack of sales. Regardless of how brilliant a cybersecurity professional is, a business that lacks cash flow will not stay afloat. Factoring commission for excellent salespeople into pricing models is crucial for entrepreneurs without sales experience or high social capital. A good salesperson will think of how to make money, which allows the cybersecurity professional to focus on their craft and spend more of their time billing customers. This allows the entrepreneur to have stronger profit margins, so they can reinvest back into the company and bring in more talented professionals.

Confidence and Communication

Many opponents of the Myers Briggs Type Indicator (MBTI) psychometric personality test argue that lumping people into mutually exclusive categories such as extroverts and introverts is unrealistic, as most people fall somewhere in the middle. The fact remains, however, that magnetic personalities have a significant advantage in terms of enlisting people in their vision. Across the United States, improv comedy is becoming an immensely popular tool to teach business and engineering professionals how to quickly adapt to various situations in order to communicate effectively. The arts of conversation and face-to-face negotiation have become less common, but no less important when dealing with customer needs and requirements, conflict resolution within teams, and employee satisfaction.

Though not as obvious as the cost of healthcare benefits, high employee turnover can destroy an otherwise successful company's profit margins. In indefinite delivery, indefinite quantity (IDIQ) contracts with significant competition for highly technical cybersecurity engineers, business owners can suffer significant cuts in revenue when excellent talent moves to another company. It is critical for business owners to understand that it is much cheaper to keep employees happy than it is to find new ones, as searching for good talent is like finding a needle in a haystack.

Sources

1. Griffith, Erin. "Why Startups Fail, According to Their Founders." Fortune.com. September 25, 2014. http://fortune.com/2014/09/25/why-startups-fail-according-to-their-founders/.
2. Gartner, Inc. Gartner Research. "Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware." News release, August 22, 2014. Gartner.com. http://www.gartner.com/newsroom/id/2828722.

About the Author:

Cait von Schnetlage *is CEO of Full Suite Solutions, a WOSB which provides cyber security and software development services for data warehousing and geospatial information systems throughout the Washington D.C. area to public and private sector clients. She also teaches Design, Prototyping, and Testing to graduate students in University of Maryland's Master of Technology Entrepreneurship program. Cait is passionate about improving antiquated business processes and has over 5 years of experience providing entrepreneurs and executives with entrepreneurship consulting.*

FULL SUITE SOLUTIONS