

From the Mouth of a Venture Capitalist: B2B, Cybersecurity, and the Relative Unimportance of Business Valuation

7 min read

**HONING YOUR
PROFIT
SUPERPOWERS**

*Path to
PROFIT
PODCAST*

Stephen King
Podcast Host, CEO, Growthforce

Guest:
Sid Trivedi
Partner at Foundation Capital

GrowthForce

Key Takeaways

- **B2B and What You Should Learn From Your First 10 Sales** These sales are opportunities to identify sales patterns immediately.
- **Why Cybersecurity Should Keep Your SMB up at Night:** On average, a cybersecurity incident costs SMBs \$7.5 million- meaning your business could suffer significantly greater losses.
- **The Relative Unimportance of Business Valuation:** Startups should focus on THIS instead...

To achieve long-term success as a venture capitalist, you have to know business – and not just a few aspects of business management – but the ins and outs of startup strategy and operations, people, and relationships.

And, according to [Sid Trivedi](#), a Partner at [Foundation Capital](#), it doesn't hurt to have a superpower or two to bring to the table.

As an investor and partner, Trivedi's superpowers that he offers startups are his immense list of valuable B2B contacts and a strong background in cybersecurity.

In this episode of Path To Profit, host Stephen King sat down with Trivedi to discuss how he uses his superpower to help B2B businesses navigate their own path to profits.

With these talents in mind, King asked Trivedi, as a thought leader in the venture capital industry, to offer some advice on what established business owners and individuals who are just getting into the startup game can do to strengthen their businesses and make the right choices for fostering success and growth.

[Subscribe \(Don't miss an episode!\) & find the full conversation here!](#)

B2B and What You Should Learn From Your First 10 Sales

As a venture capitalist, you get to watch and be involved in the early growth stages of countless businesses. Along the way, investors become experts in the steps and strategies that foster the greatest success during the crucial early days.

In particular, Trivedi emphasizes the importance of a startup's first 10 sales. Not only are these clients the ones who will be responsible for initially transforming your business from an unknown entity to a known company, but these sales are also opportunities to identify sales patterns immediately.

Trivedi recommends listening carefully to the voice of the customer, paying attention to their sales journey, their pain points, and their feedback on your pricing structure, your product, its delivery, and every other aspect of their interactions with your business.

Ultimately, these first 10 clients represent your opportunity to tweak your processes, adjust your price points or structure, and start learning your sales process to get your business in the best possible shape before your first growth stage and the crucial onboarding of your next generation of sales representatives.

Why Cybersecurity Should Keep Your SMB up at Night

In small and medium-sized businesses, defined as businesses with fewer than 500 employees, there is a major failure in the C-suite – and that lies with cybersecurity, taking it seriously as a threat, and implementing (and following) sound IT security policies and procedures.

Read More: [Major Failure in the C-Suite: CEOs Need to Take More Caution In Cybersecurity](#)

Quick Cybersecurity Facts

- 84% of C-level executives have been the target of at least one cybersecurity attack.
- 54% of those attacks are categorized as phishing.
- 78% of IT professionals believe C-suite executives are the most likely targets of phishing attacks ^[1].
- 76% of C-level executives admit to bypassing cybersecurity procedures.
- 40% of IT professionals name their organization's CEOs as the weakest cybersecurity links ^[2].
- Cybercrime has cost the global economy an estimated \$375 to \$575 billion ^[3].

Despite these frightening statistics, most SMB leaders don't give cybersecurity a second thought, simply assuming that they're too small to matter, that hackers only target big businesses, that they would never waste the time targeting a smaller organization.

This assumption, however, is wrong.

If You Aren't Worried About Cybersecurity, You Should Be

Citing statistics reported from a 2019 Verizon study on data breaches, Trivedi said that on average, a cybersecurity incident costs SMBs \$7.5 million, emphasizing the words "on average," meaning your business could suffer significantly greater losses.

Additionally, the study also found that of the SMB leaders polled, over 60% had, in fact, reported a data breach at some point during the previous year. Of the same group of business leaders, only about 40% reported having any type of cyber defense in place. No endpoint solution, no firewall, no email security.

As Trivedi put it, "The truth is that you will get breached...the goal is really to protect your assets."

Why the Problem Is Getting Worse

Trivedi believes the market for cyber attacks is ballooning as a direct result of people's assets and valuable personal information being transferred from being stored in the physical world to the digital world.

Our valuables used to be stored in cash at the bank. Now, they're in our online accounts. We used to keep hard copies of our resumes. Now, we have them saved to our hard drives or published for everyone to see on our LinkedIn pages.

The criminals are simply following the migration of our assets out of the physical world and into the digital one. As a result, everyone, every business, and every person in your business (especially high-level executives) are potential targets.

Simple Steps to Take Action and Protect Your Business

#1 The first step is to realize you're at risk. Once you've done that, Trivedi recommends implementing an endpoint solution on all of your hardware. This means installing some form of IT security software (McAfee, Symantec, etc.) on your desktop, laptop, mobile phone, and servers.

#2 Next, your business needs to be protected by a firewall (*Fortinet, Checkpoint, Palo Alto, etc.*).

#3 Also, implement an email security tool (*Barracuda, Proofpoint, Mimecast, etc.*) to help mitigate phishing threats.

#4 In addition to these steps, Trivedi also emphasizes why it's so important to back up your own data with a system that's likely stored on physical servers to a secure system in the cloud that's stored on someone else's secure servers. This step shields your company from data breaches, data loss, and the ever-looming threat of ransomware.

The Relative Unimportance of Business Valuation: Startups Should Focus on This Instead

To round out their conversation, King asked why the market seems to be flooded with available investment dollars, as if there is currently more money to be invested than places to invest it, and how someone looking for funding can be smart about choosing investors.

Trivedi explained that he attributes the abundant availability of potential investors to the overall economy. Having not had a serious economic crisis since the 2008 crash and operating in a climate where governments are keeping interest rates intentionally low, he believes there is simply a greater amount of cash sitting in the bank that potential investors are looking to get greater returns from – and in a low-interest-rate climate, one of the ways to do that is to invest in startups.

Additionally, remote work culture, virtual meetings spaces, and the pandemic's contribution to society's acceptance of these platforms for business have also changed the venture capitalism landscape. With the ability to meet "face-to-face" with anyone, anywhere, at any time, investors are no longer so regionally bound as they once were to investing in local startups.

Despite the abundance of cash, Trivedi cautions entrepreneurs to be smart about the investors they choose. He says that rather than going after the investor that gives you the

greatest valuation or the largest sum of cash, a savvy entrepreneur will, instead, look for value in the partnership itself.

It's all about recognizing the difference between smart money and dumb money. Trivedi advises entrepreneurs to choose investors who not only bring cash to the table but who can also bring their own, individual superpower to your business.

Choose an investor who can add value to your board meetings, act as an advisor, and who can contribute more than dollars to your company's success.

Embracing the Chaos: What It's Like to Be An Entrepreneur

Trivedi described his experience in startups, saying, "The amazing thing about being in startups and being in early-stage companies is when you're at a startup, there's a fire burning every single day. There's something going on, and there are usually moments of extreme highs followed immediately thereafter with the moments of extreme lows."

He continued, "It's one of those situations where if you feel like this is the best day in the world or the worst day in the world, you just need to wait a little bit, and very quickly things will change. It's not a normal day of going into the office."

The takeaway? If you're involved in a startup, one of the main things you can do to prepare yourself is to be ready to ride a veritable rollercoaster.

However, following Trivedi's advice with respect to focusing on your customers and sales patterns, shoring up your business against cybersecurity threats, and staying focused on partnering with investors who bring more than their cash to the table can help you create a smoother ride.

Be Prepared With A Smart Back Office

Being proactive vs. reactive is the first step in getting ahead. Be prepared with a robust, smart back office. If you're still relying on manual accounting processes, the first thing you need to do is to streamline, automate, and update.

A robust back office will provide you with the financial data you need for pulling management reports that can give you invaluable insights into your business's operation, strategy, and each of the decisions you make.

With a powerful back office, you can make data-driven decisions to improve profits while also strengthening the financial health and future of your company.

[1]

<https://www.forbes.com/sites/louiscolombus/2020/05/29/cybersecuritys-greatest-insider-threat-is-in-the-c-suite/?sh=5b70d257626f>

[2] <https://www.theceomagazine.com/business/innovation-technology/cybersecurity/>

[3] <https://www.ibm.com/downloads/cas/M94RB4WR>