CONNECTWISE

CONNECTWISE EBOOK SERIES

# How to Grow Your VAR Business by Specializing in Cybersecurity

# CONTENTS

# Introduction

As a value-added reseller (VAR) business owner, you're likely hyper-aware of the factors that are shrinking profit margins in today's value-added reselling landscape: an increasingly crowded marketplace, nonstop pricing wars, supply chain challenges, and a significant shortage of tech talent, to name a few.

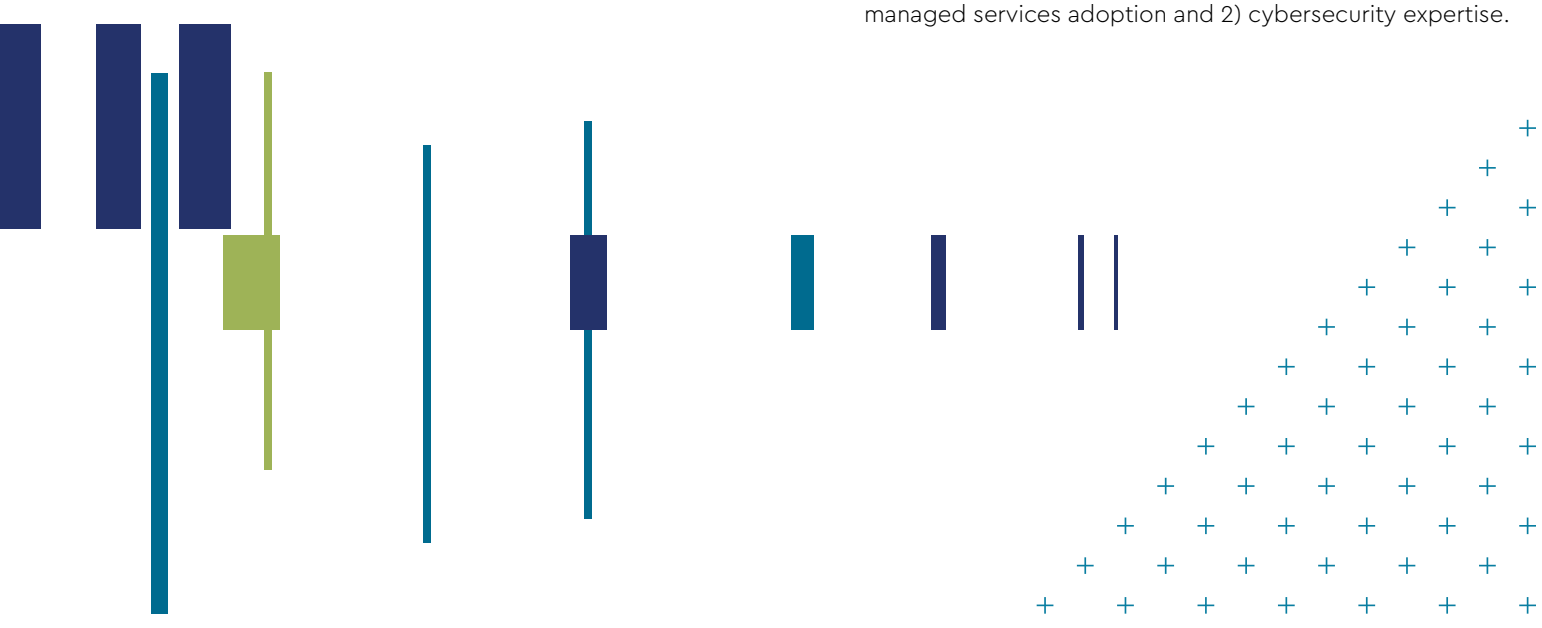
Does this predicament have you searching for a way to build a more stable revenue stream and enable business growth? Enhancing your company's value proposition and business model doesn't happen overnight, and there will always be an element of risk that comes along with adapting to an emerging trend or market.

**While it can be difficult to pick an area to double down and expand on to grow your VAR business, there is one emerging niche that a growing number of VARs are finding success specializing in (and capitalizing on): cybersecurity.**

In recent years cybersecurity has become a very high priority for businesses of all sizes and across all industries. The cause? A rapidly growing global network of sophisticated cybercriminals. According to a recent report from Cybersecurity Ventures, cybercrime is expected to cause $10.5 trillion in annual associated costs by 2025 (up from $3 trillion in 2015).

Cybersecurity is probably top-of-mind for some of your clients, too: The State of SMB Cybersecurity in 2021 survey conducted by Vanson Bourne and commissioned by ConnectWise found that 92% of organizations would consider using or moving to a new IT provider if they offered the "right" security solution. Not only that, these companies say they are willing to pay 34% more for a service provider that can provide that peace of mind.

To launch a lucrative security-as-a-service offering, there are two areas that your VAR business must successfully mature: 1) managed services adoption and 2) cybersecurity expertise.





CONNECTWISE
ManagedServices@dandh.com

# Chapter 1: Embracing the Benefits of Managed Services

Launching a security-as-a-service offering doesn't mean you have to overhaul or dramatically restructure your existing VAR business model. After all, you may not be ready or willing to make the transition into becoming a full-fledged managed service provider (MSP).

However, relying largely on upfront sales to keep your cash flow running can be risky, and margins on hardware are continuing to shrink. Perhaps you're a reseller that currently offers a mix of 90% hardware and 10% services, or 75% hardware and 25% services. In either case, it's likely that the services component of your business is heavily oriented toward front-line support for vendor technologies.

**To prepare to launch security-as-a-service, you must evolve to become a technology and a service organization that is both proactive and rapidly reactive in protecting your customers against cyber threats.** Naturally, this means increasing the amount of recurring revenue involved in your business model as you adapt to serve your customers' changing needs. From increased profit margins to enhanced customer satisfaction, there are a number of benefits that accompany the decision to add on additional managed services (see: Six Reasons Why a VAR Should Add Managed Services).

As you plan to expand the managed services aspect of your business, consider how you will keep track of many moving parts across your operations and client relations.

A robust professional services automation (PSA) tool can help you maintain full visibility into all aspects of your business while reducing redundant manual tasks and boosting efficiency. PSA software making launching managed services easier by allowing you to:

- Oversee all hardware and service costs involved related to customer agreements
- Integrate with hundreds of other tools to capture data across various sources
- Maintain employee trust and accountability by serving as a single source of truth
- Carry out frictionless billing to provide clarity to customers and improve cash flow

Another area to consider is how to have the conversation with existing customers about making the transition to managed services. You've already gained the trust of these business owners and leaders as an expert provider of technology solutions. To prove that managed services are a worthwhile investment, use this as an opportunity to discuss where your customers currently stand on their cybersecurity maturity journey and to emphasize the importance of strengthening their cybersecurity posture.

# Chapter 2: Acquiring the Tech and Talent Needed to Offer Cybersecurity Services

When assessing the current state of your VAR business's offerings, it's possible that you have experience selling and installing point products such as antivirus, firewall, and email security solutions. **To provide truly robust security-as-a-service, you must acquire the right cybersecurity expertise and technologies so that you can confidently propose ways for customers to optimize their protection.** That means recommending systems and methods that *your own business* uses.

One of the best ways to accelerate your understanding and proficiency of essential security concepts is to leverage an established, time-tested cybersecurity framework. A framework serves as a system of standards, guidelines, and best practices to manage risks that arise in today's digital business world. By learning and implementing a flexible and repeatable approach to enhancing the protection and resilience of your business, you will be able to use this hands-on knowledge to better serve your customers, as well.

For organizations that don't already have a high level of cybersecurity maturity, we often recommend they utilize the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The five pillars included in the NIST CSF cover all the core elements of cybersecurity, making it a complete, risk-based approach to securing almost any organization. Those five areas are:

- **Identify –** Pinpoint the organization's critical functions and the cybersecurity risks that could disrupt them.
- **Protect –** Determine the potential impact of a cybersecurity breach and develop a plan to minimize the damage done.
- **Detect –** Enable timely discovery of cybersecurity incidents and how to determine that a breach has occurred.
- **Respond –** Prepare for rapid response to any cybersecurity incidents in order to keep them from spreading.
- **Recover –** Restore any data or capabilities that were affected by a cybersecurity incident so that the organization can return to business as usual.

Keep in mind that, while this process may take months and could end up being a significant endeavor depending on where you are in your cybersecurity maturity journey, it will be well worth it in the long run. Not only will you fortify your own defenses, learning to align controls across local, offline, and cloud backups will ultimately help you grow your business by selling your expertise to clients.

As you can see above, a foundational step in this process is to assess your VAR business's current risk levels so you can develop plans and priorities for remediation. To help with both the risk assessment itself and remediation recommendations, consider employing risk assessment software. Comprehensive risk software evaluates risk not just for your network, but across the entire business.

Additionally, this technology can (and should) be used as a launching point to have meaningful risk-based security conversations with your clients. For example, it can be used to generate digestible, custom-branded risk reports that show your clients' decision makers what needs to be done and why. By using risk assessment software to outline actionable next steps to improve their cybersecurity posture, you showcase the value of your other security-as-a-service offerings.

After you've used your cybersecurity framework and risk assessment to establish the necessary policies, procedures, guidelines, and standards, it's important to educate your employees on what these things mean for them. **We frequently advise VARs to put a cybersecurity awareness and training program in place to increase visibility and keep everyone up to date on the latest security requirements.** There are also free online resources that can be used to train your technical staff and sales people on cybersecurity best practices specifically as they relate to the SMB sector.

While kicking off cybersecurity awareness training and training for your VAR business, you may also reach the conclusion that you don't have sufficient personnel on board to help guide the journey and provide the services you desire. This is a tough realization to have, as top security talent is hard to find and hiring several cybersecurity experts, or even just one, can become prohibitively expensive. Fortunately, this is an issue that can be overcome by selecting a vendor with the right technology and outsourced expertise for the as-a-service model.

Having successfully proven the importance of cybersecurity to your clients, you can begin to sell them on specific services that are the best fit for their unique business needs. In addition to routine risk assessments, here are a few examples of as-a-service offerings that VARs often have the most success and profitability providing to customers:

- Dark web scanning
- Threat detection and response
- Security information and event management (SIEM)
- Security operations center (SOC)
- Backup and disaster recovery (BDR)

A partner such as ConnectWise can help accelerate your journey to becoming a cybersecurity solutions provider through in-depth expertise in the SMB market, a state-of-the-art research unit to keep you in the loop about emerging threats, and, perhaps most importantly, a streamlined technology stack that puts you on the right path to increased profitability.

# Chapter 3: Facilitating Profitability Through Process Improvements and Automation

Once you have elevated your cybersecurity expertise to a place where you're comfortable having the cybersecurity conversation with your customers, you'll need to start thinking about how you will increase the *profitability* of your security-as-a-service offering. It's possible that your processes for managing and optimizing recurring revenue services are not fully developed. After all, many of the principles you've used to develop a successful product-centric business don't necessarily apply here.

With security-as-a-service, the time you spend providing these services will typically have the biggest impact on your profit margins. **That's why it is essential to install repeatable systems that allow you to do more with less so you and your staff can focus solely on areas where they provide maximum value.** Remote monitoring and management (RMM) software is a powerful technology that can be used to outsource and/or automate repetitive tasks, such as patching, network scans, agent deployment, and more. Programmatically offloading routine workloads will help reduce associated costs and cut time for your busy staff.

To measure the financial impact task automation and process refinement have on your VAR business, you need to make sure you're tracking the right key performance indicators (KPIs). There are dozens, if not hundreds, of custom metrics that you could formulate to gauge profitability. Here are a few commonly used KPIs that we recommend using along with the formulas for calculating them:

- **Margin by Product Offering:** *( [Revenue – Cost of product] / Revenue) x 100 = Product Margin %*
- **Margin by Service Offering:** *( [Revenue – Cost of Service] / Revenue ) x 100 = Service Margin %*
- **Customer Lifetime Value (LTV):** *(Average revenue per customer x Average length of contract) = Customer lifetime value or (Average revenue per customer / Customer churn rate) = Customer LTV*
- **Effective Rate by Customer:** *(Total Customer's Services Revenue / Total Hours Dedicated) = Customer Effective Rate*

When launching your security-as-a-service offering, you may feel an urge to try and accumulate as much business as you possibly can. However, keep in mind that quality is almost always more valuable than quantity. In other words, it's better to have a small number of highly profitable clients than it is to have many clients with a low profit margin.

Another area that must be closely examined before, during, and after you begin offering cybersecurity services is pricing. Some VARs that are new to the world of managed services start out by setting their prices so low they can hardly cover labor costs; however, if you price too aggressively it will make it difficult to sell customers on security-as-a-service. To help you think more critically about your operating costs and current competitive landscape, peer industry groups and partner programs can be invaluable resources for finding success with cybersecurity service pricing.

# Chapter 4: Maximizing Cybersecurity Revenue With Sales and Marketing Alignment

As a VAR, it's likely that you have a carefully tuned sales machine that has grown accustomed to your current business model. **Launching a security-as-a-service offering will require some retraining and conversations about selling managed cybersecurity.** You can't simply tell your sales team to start focusing on services over products.

To earn buy-in from your salespeople, you may have to adjust your compensation structure accordingly. Creating appropriate incentives will ensure that they're on the same page as you and the rest of the leadership team. A few possible methods for this include:

- Providing more quota relief for services
- Paying higher commissions on services than products
- Offering commissions on products only after a rep's services quota is met

It's also important to empower your sales team with time-saving, automation-based technology just as you are doing across other parts of your business. For example, automated quote and proposal software can help with seamless customer relationship management (CRM) system updates, automatic upselling suggestions based on client needs, templates that can save hours per quote, and more.

Similarly, your marketing department can help generate more leads and drive more sales with cutting-edge technology that streamlines many of their daily tasks. This can include generating custom campaigns that are delivered at just the right time, measuring vital KPIs to identify your most effective marketing channels, and scheduling cross-platform social media posts to reach your prospects and clients wherever they are online.

For both of these departments, a cybersecurity partner program can once again prove hugely beneficial by giving your business access to world-class sales playbooks, ready-to-use marketing assets, market development funds, and more.

# Security-as-a-Service: Better Together with ConnectWise

In today's rapidly changing cyber threat landscape, it can be difficult to build out a robust security program all by yourself. Consider leveraging ConnectWise, the number one strategic partner for VARs looking to launch security-as-a-service, to help you build, grow, and sustain a profitable services practice. By partnering with ConnectWise, you will have access to:

- Industry-leading security practices and playbooks
- Best-in-class cybersecurity technology and services
- Educational resources, in-depth training, and community events
- Guidance on how to introduce new value-added services to your clients
- And more

Your customer relationships and sales prowess combined with the experience and operational maturity of our security expertise, products, and service make for a powerful force that can help your clients stay as protected as possible.



CONNECTWISE
ManagedServices@dandh.com

# Conclusion

As you can see, launching a profitable security-as-a-service offering for your VAR business is not an insurmountable endeavor. There's no denying that it will take a lot of work, but with the right people, processes, and technology in place, you will be on a steady path to becoming your clients' trusted IT cybersecurity partner.

Cybersecurity has never been more of a priority for your prospects and clients than it is right now. Looking for expert guidance on how to launch your security-as-a-service offering? Reach out to our team today to find out how we can help put your VAR business on the fast track to providing lucrative cybersecurity services.