Transforming your Cyber Security Sales Strategy

Expressing the value of security solutions
to clients and prospects.

The Evolution of the Security Landscape

In recent years, the security threat landscape has evolved rapidly, posing new challenges for businesses across the globe.

In our last eBook, The Changing Cyber Security Landscape, we discussed the advancements of cyber crime following the COVID-19 pandemic, and how MSPs can enhance and improve their cyber security offerings for the threats of 2022.

As the world has become more reliant on technology to facilitate a hybrid model of working, cyber criminals have been able to capitalise on the vulnerabilities of businesses all over the world. Threats such as phishing and ransomware have mutated and become more pervasive, and new forms of attack such as cryptojacking and exploitation of the Internet of Things have begun to emerge.

As highlighted by the fact that cyber crime has increased by 600% since the beginning of the pandemic, the cyber security environment is now completely different. As such, cyber security services need to be treated with a new outlook, both by MSPs and your end users.

Managed Services:
A Necessary Shift in Expectations

When Managed Services first became popular amongst smaller businesses, the main attraction was the promise of uptime that consistent IT support could guarantee.

Therefore, a lot of customers invested in proactive SLA contracts with their chosen MSP to minimise disruption to their systems. Businesses are still investing in these packages with the same hope of uptime, despite the fact that the technology space has developed almost beyond recognition.

When these contracts were originally signed, cyber security posed far less of a threat to a business' uptime, as the threats were far less advanced and widespread. In the current security landscape, however, a cyber attack or data breach could negatively affect operations, productivity and revenue for a significant period of time.

There is a common yet unfortunate misconception among clients that cyber security cover is included as part of traditional IT support packages. Given the advancements in cyber security, this is, of course, no longer the case. Therefore, in order to be protected from cyber threats, end users need to invest in additional cyber security services from their MSP.

As end users can be reluctant to pay more for services they do not fully understand the need for, the challenge for MSPs is demonstrating the value and necessity of these additional cyber security solutions. This will not only aid the end user, as their business will have greater protection from dangerous cyber threats, but it will have the added benefit of being more profitable for your MSP.

In this eBook, we explore how to demonstrate the value of cyber security in the modern IT landscape, and the various methods by which to sell protective solutions to end users. We will teach you how best to express the very real advantages of managed cyber security services to your customers and thereby transform your MSP's sales pitch.

How to Demonstrate the Importance of Cyber Security

Your MSP’s client base is likely to be made up of small and medium-sized businesses. In the current security landscape, this business demographic is most at risk of experiencing a cyber attack. An effective way to demonstrate the value of your cyber security services is to highlight the very real threat your customers are facing, using reliable statistics.

43% of cyber attacks are aimed at small businesses

Source: Ponemon Institute

66% of small businesses have experienced a cyber attack in the past 12 months

69% of small businesses say that cyber attacks are becoming more targeted

The value of your MSP’s cyber security services is primarily in what they can prevent, rather than what they can add. By expressing the potential severity of the consequences your customers could face if they do not invest in cyber security, you can highlight the need for your solutions.

40% of small businesses that face a severe cyber attack experience at least eight hours of downtime

Source: Cyber Security Magazine

83% of small and medium sized businesses are not financially prepared to recover from a cyber attack

Source: Cyber Security Magazine

33% of UK organisations say they lost customers after a data breach

Source: CSO

How to Sell
Cyber Security Services

When it comes to selling cyber security services, there are two different approaches you can take.

Firstly, you can target your existing customers, and sell them a new cyber security package on top of the services they are already receiving from you. For instance, if you are already providing IT support services to a client, you can recommend that they invest in managed cyber security solutions too.

Alternatively, you can take the opposite approach. Given the prevalence of cyber threats in the current technology space, many businesses are becoming more concerned about their cyber security. With more companies in the market for cyber security services, you could make these solutions your initial sell, and then transition to offering more generic Managed Services at a later date.

We will now explore both methods and explain their benefits, so that you can clearly decide which approach to take when selling cyber security.

Method One:
Upsell Existing Clients

When selling cyber security services to your existing customers, you can build upon the foundation of trust you have already established with them.

A major advantage of selling cyber security this way is that your pre-existing customers already believe in the value of your services, as they are already working with you in some capacity. Therefore, having already established your reliability as a service provider, you can highlight the need for additional cyber security solutions more easily.

There are two ways that you can approach existing customers when it comes to cyber security sales: you can upsell or you can cross-sell. Before we explain how to identify opportunities for each, let's establish a clear definition of both sales strategies and provide some examples of how this could be applied when selling cyber security solutions.

Upsell: a sales strategy that encourages customers to purchase a premium version of a product or service that they were intending to buy.

E.g. Your MSP is already providing some cyber security solutions to an existing client (in this instance, let's imagine that you are delivering email security services). You could then upsell a related service, (such as phishing simulation software) for an additional profit.

Cross-sell: a sales technique that involves selling additional complementary products or services to existing customers.

E.g. You are currently providing IT support for a customer and you sell them managed security services on top.

How to Identify a Selling Opportunity

When selling cyber security services to existing customers, you should not take a blanket, one-size-fits-all approach.

Attempting to sell without discrimination is unlikely to get you very far. The best way to upsell or cross-sell cyber security is to identify customer needs and customer pain points and pitch a service that facilitates a solution.

For instance, if a customer works in an industry which requires them to adhere to strict compliance regulations, such as the legal or financial sectors, this could be an excellent opportunity to upsell a more stringent data protection solution.

Another potential opportunity to upsell or cross-sell cyber security solutions is when a customer's business undergoes growth. As they are entering a period of transition and potential uncertainty, they will need their security to be robust and comprehensive.

In order to identify opportunities to sell, **you need to have a clear and consistent idea of your customers' business trajectory and evolving requirements**. This allows you to evaluate when they might need additional security services most accurately. It might be sensible to establish monthly or quarterly reviews with your clients so that you can discuss their current needs and future goals, and sell security products or services that will support their growth journey.

Method Two: Target New Prospects

Alternatively or additionally, you could implement the second approach to selling cyber security services: targeting new prospects.

In order to convince new clients of the value of your cyber security services, you need to open up a dialogue that will highlight the need for these solutions. An effective way to do this is to ask questions that will reveal the current gaps in their cyber security posture and the potentially damaging consequences of not filling them.

So, what should that conversation look like? We have suggested nine potential questions you can ask to begin selling cyber security to new clients.

Question One:
What does your current cyber security infrastructure look like?

This question is a good way to begin the conversation about cyber security. It allows you to assess what systems the customer currently has in place, and what they still need to implement.

Question Two:
Does your business need to adhere to any specific regulations?

Asking this question allows you to explain how investing in data protection and security solutions can make adhering to legal regulations easier. If you are targeting a business that operates in a sector that is required to meet compliance standards, then this is a particularly clear selling point. However, all businesses can benefit from meeting security best practices.

Question Three:
How do you currently protect your sensitive data?

Your prospect may not yet have considered the amount of confidential data they are housing on their systems. Asking this question provides you with an excellent opportunity to highlight any exploitable vulnerabilities they may have. You can also recommend solutions like data identification and encryption that can help secure client data.

Question Four:
Does your business need to adhere to any specific regulations?

This question allows you to judge how much your prospect knows about their own cyber security. They may not know which of their systems need the most protection, or even what the term 'high-risk' means. This provides you with an opportunity to educate them and establish your MSP as a reliable and knowledgeable source.

Question Five:
Do you carry out regular cyber security awareness training with your staff?

Despite the prevalence of cyber threats, a recent report from Software Advice has found that nearly half of all SMEs do not provide regular cyber security training for their staff. Therefore, this question allows you to educate prospects about the dangers of not strengthening their human firewall. As some of the worst breaches can occur as a result of human error, you can express that investing in regular security training is essential and present your MSP as a source that can assist with this.

Question Six:
Are you regularly scanning your network data for malware?

This question allows you to draw attention to both the necessity of regularly checking for malware, and the importance of protecting all data on a network, including backup data and that stored in archives.

Question Seven:
Have you developed a clear incident response and disaster recovery strategy?

In the current security climate, there is an extremely high likelihood of a business suffering from some form of cyber attack. Without a clear incident response plan in place, there could be extremely significant negative financial, operational and reputational consequences for an organisation.

If a prospect doesn’t have a clear incident response plan, you have a ready-made service to pitch them. As the potential consequences are so damaging, the majority of businesses will be keen to implement an incident response or disaster recovery strategy.

Question Eight:
How would a cyber attack or security breach impact your business?

Your prospect might have already considered the operational and financial impacts of suffering from a cyber attack: namely downtime. However, your job is to demonstrate the consequences that they may not have thought of. For instance, how would a security incident affect company morale?

How would a data breach affect their client relationships? Would there be any legal implications for their business? Once a prospect has explored the potential pain points a cyber attack could cause, they may be more likely to want to implement cyber security procedures.

Question Nine:

Are you currently using an MSP to improve your security posture? If so, are you satisfied with the results?

This question allows you to demonstrate the need for your services. If a business is not currently working with an MSP, then you can highlight the advantages that working with a team of technical experts and security specialists can bring.

If your prospect is currently working with an IT provider, you can identify any gaps in the services they are providing and take the opportunity to promote your unique selling points, or any distinctive qualities that make your security services stand out.

The Sales Pitch

Your prospect's answers to these questions should reveal gaps or vulnerabilities in their security posture, which you can use to sell services to them.

After you have convinced them of the value of your security solutions and onboarded them as a new client, you can eventually transition to selling them wider Managed Services such as IT support.

Essentially, your security sales pitch should show them the value of your wider services, by highlighting your reliability and credibility as an MSP.

Revolutionise Your Sales Strategy with Trend Micro

The cyber security landscape is always evolving and so the services your MSP provides need to continually adapt alongside it. As such, you should always be offering more value to clients via innovative new solutions.

As global security leaders, with decades of experience providing security expertise, carrying out global threat research and delivering continuous innovation, Trend Micro are the ideal partner to help guide you through selling and marketing your cyber security services. Whether you are upselling to existing clients or transitioning new prospects to your services, we can guide you through the sales process and help you to optimise your value propositions.

For expert support with selling cyber security, get in touch with a representative at Trend Micro.

Get in touch