EASYDMARC

Sales Process and Pricing Models for MSPs

Table of **Contents**

Sales Process Workbook for MSPs

Without Email Authentication, your clients are not cyber secure. Fortunately, you can help them. This workbook aims to provide you with a comprehensive and step-by-step guide to selling DMARC.

This workbook will walk you through the entire sales process, from understanding client needs to close the deal and pricing strategies you can adopt to monetize the process.

What will you learn?

- How to position yourself as a trusted cybersecurity partner and improve your brand reputation.
- How to begin the DMARC enforcement conversation that is affecting the customers' deliverability. This puts you in 'The Trusted Advisor' Seat.
- How to get new clients to buy DMARC.
- How to get the results you want.

Step 1: Conducting a Client Assessment

First Appointment

A. Run a domain health check using EasyDMARC's Domain Scanner tool to detect a client's current domain infrastructure vulnerabilities.

B. Export the pdf of the domain check and send it to the client with a warning message about the vulnerabilities and how you can help.

C. Schedule a call with the client to start.

Discovery Call

A. Discuss the impact of email attacks on their business (e.g., data breaches, brand reputation damage).

B. Make the case for how DMARC can improve their email security, protect their brand and increase their email deliverability.

C. Determine any regulatory compliance requirements related to email security (e.g., DMARC is a must when applying for cyber insurance).

D. Evaluate the client's budget and resource constraints.

Discovery Call Questions

- What email security challenges or incidents have you experienced in the past?
- Are you aware of the risks associated with email spoofing, phishing, or domain abuse?
- Are there any regulatory compliance requirements or industry standards that you need to adhere to regarding email security?
- Do you have a clear understanding of the potential impact and costs of a successful email-based attack on your business?
- Do you use email marketing for your business goals? If yes, what is the percentage of your opens, clicks, and deliverability? Have you noticed any recent changes?
- What resources, budget, and technical expertise are you willing to allocate to enhance your email security?
- Are you interested in proactive monitoring and reporting to identify unauthorized email senders or abuse of your domain?
- How would you like to handle unauthenticated or fraudulent emails received by your recipients?
- Are there any other email security solutions or services you are considering or have implemented alongside DMARC? What do you know about BIMI?
- How would you measure the success of implementing DMARC in your organization?

Step 2: Showing the Value

Explain the basics of DMARC:

A. Define DMARC and its role in simple terms.

B. Explain that leading ISPs like Google and Yahoo are making DMARC mandatory.

C. Export the pdf of the domain check and send it to the client with a warning message about their vulnerabilities.

D. Avoid using technical jargon (e.g., use “phishing protection” instead of “domain-level security” or “focus on your business goals with peace of mind” instead of “invest in a strong cybersecurity solution by implementing DMARC”).

E. Highlight the benefits of DMARC implementation, such as reduced phishing attacks and domain abuse, full visibility of email traffic, or explain the benefits of DMARC on email deliverability.

Speak more about the deliverability:

A. Explain how DMARC improves the deliverability issues and increases marketing ROI (they are all discovering their deliverability declining, and they are hearing it is due to DMARC compliance).

B. Explain the importance of messages landing in customers’ inboxes and that spam counts can negatively impact a domain's reputation and future sending capabilities.

Provide case studies and statistics:

A. Share success stories and testimonials from previous clients who have implementedDMARC.

B. Present industry data and statistics showcasing the effectiveness of DMARC in preventing email-based attacks.

Offer proof of expertise:

A. Highlight your experience and certifications in email security and DMARC implementation.

B. Showcase partnerships or affiliations with reputable cybersecurity organizations.

On becoming an EasyDMARC MSP Partner, we will share with you access to ready to use marketing materials, training sessions and our DMARC certification program. You can personalize content to communicate to your clients' to help cover these steps.

Step 3: Monetizing DMARC

Emphasize the return on investment (ROI):

A. Quantify the potential cost savings and risk reduction associated with DMARC implementation.

B. Provide concrete figures and examples of how DMARC can save the client money by preventing email fraud and phishing attacks. (Use the "Non-Compliant" tab of the Aggregate Report section in your EasyDMARC MSP account to show the spam email rate and phishing attempts on the client's domain).

C. Highlight the potential financial losses that could result from a security breach and emphasize how DMARC can mitigate those risks.

D. Emphasize how DMARC applies to the successful delivery of all emails, including transactional (e.g. Purchase Orders, Invoices. Payment notifications etc).

E. Demonstrate the ROI of DMARC investment: Show how the investment in DMARC will lead to enhanced email security, brand protection, and improved email marketing success.

F. Explain how DMARC can improve deliverability rates, ensure legitimate emails reach recipients' inboxes, and protect the brand's reputation.

G. Use case studies or success stories from other clients to illustrate the positive impact of DMARC implementation.

Offer a pilot program:

A. Propose a smaller-scale implementation of DMARC to showcase its effectiveness. This will allow the client to experience the benefits firsthand without committing to a full-scale deployment.

B. Offer a limited-time offer or discounted pricing for the pilot program to incentivize their participation and reduce their perceived risk.

Address any remaining concerns:

A. Revisit any objections or concerns raised earlier in the sales process and provide further clarification or evidence to alleviate them.

B. Be prepared to answer technical questions and provide additional guarantees or assurances to address any doubts.

C. Offer different service packages based on the client's budget and requirements, providing flexibility and options.

D. Highlight the additional services you can provide alongside DMARC implementation. These may include regular reporting on email authentication status, proactive monitoring for potential issues, and incident response services to quickly address any email security incidents.

E. Emphasize the ongoing support and added value you bring to the table.

Close the deal:

A. Request a commitment from the client, such as a signed contract or statement of work, to solidify the agreement.

B. Agree on a start date for the DMARC implementation project to ensure clear expectations and timelines.

C. Discuss the pricing structure, including the cost of the consulting services to fix any identified issues and the ongoing monitoring fees that will be added to the monthly cost.

D. Provide a clear breakdown of the costs and services to avoid any confusion.

Step 4: Upselling and Expansion

Assess additional email security needs:

A. Identify opportunities to upsell complementary email security solutions (e.g., security awareness training, BIMI implementation, MTA-STS reporting, etc.).

B. Evaluate the client's evolving requirements and suggest upgrades to existing DMARC policies.

Foster long-term relationships:

A. Provide exceptional customer support and respond promptly to inquiries.

B. Offer ongoing education and awareness programs to keep clients

Remember to adapt the process to each client's unique needs and maintain open communication throughout the implementation and management stages.

With DMARC, you can establish yourself as trusted partner in the fight against email-based threats and provide long-lasting value to your clients.

Learn how we can help you become a trusted DMARC provider for your clients. You'll be in excellent company.

Become an MSP

If you’re an EasyDMARC MSP Partner, we will provide you with valuable security awareness training materials so that you can share them with your clients and minimize human-error risk.

Every outsourcing owner grapples with pricing at some point. Out of fear of losing customers, many end up under pricing their services.

Take the time to understand the scope of a given project. Potentially break it down to an hourly rate to arrive at a realistic price that covers your costs and desired profit margin.

Being the cheaper option might get you jobs, but you'll be straight-jacketed at that price.

The next section outlines pricing strategies you may want to consider.

Revenue Options for DMARC Services

We recognize that no two clients are the same. But no matter the size or business focus, the need for effective cybersecurity and email deliverability improvements is universal.

Whether you provide specific products or specialize in Cybersecurity as a Service (CSsaS), we'd like to ensure that your clients' Email Domains are DMARC protected.

What we outline here are some best practices in flexible pricing options that may offer a more effective way to protect your clients' businesses and drive additional revenue.

Flexible Pricing Options

Option 1 - Charge an Hourly Rate

Working out an hourly rate involves taking into account all of your fixed costs (Rent, utilities, staffing costs if applicable, paid time off, capital expenditure etc) and then working out your total billable hours per year.

This total is the bottom line cost that must be covered by your hourly rate. What you charge in addition can be influenced by any number of variables (size of client, further business potential, pricing vs the competition etc).Ultimately, it's about your profit margin.

Calculating an hourly rate

Annual Billable Hours	X
+ Annual Fixed Costs	$X
+ Desired Margin	X%
= Total Hourly Rate	$X

Once you've arrived at your hourly rate, take the number of Domains within a project as a starting point and factoring in your personal project management experience, price the project based on an hourly rate for the implementation and configuration stage of a project.

This will ensure that your costs and some profit are covered. Provide a scope of work to your client including the caveat that additional hours may need to be charged should any unforeseen eventualities occur outside of your original scope.

Once a client's domain has reached the full 'Reject' phase, there's the potential to recognize additional revenue with Monthly Domain checks, again scoped on an hourly rate.

The Advantages to You

A. Maintains regular, monthly contact with your client with the potential for securing additional business.

B. Promotes effective time management when dealing with multiple clients.

The Advantages to Your Client

A. Transparent and cost effective - paying only for the services provided - Ideal for SMBs.

B. Peace of mind with regular, scheduled contact with their cybersecurity expert.

Option 2 - All Inclusive, Fixed Annual Contract

For convenience or budgeting purposes, medium to larger clients may prefer the option of a fixed, annual price for all of the services you provide around DMARC implementation.

Including:

- Configuration
- Maintenance
- Additional Domains
- Monthly Domain Checks

This model fits well with MSPs providing total 'Cybersecurity as a Service' options, with DMARC becoming an additional invoice line item.

For MSPs concentrating on providing a service based around DMARC, receiving the annual figure upfront may be advantageous but pricing will need to reflect all potential risks associated with the project.

It's also important to build in the Monthly Domain checks to maintain a regular checkpoint with the client once DMARC nears its full implementation. This is to identify any potential red flags and to recognize potential opportunities.

The Advantages to You

A. Cash flow - Full payment for services in advance of delivery.

B. The opportunity to maintain contact on a monthly basis.

C. An incumbent provider of cybersecurity. In a primary position at the point of services Renewal.

The Advantages to Your Client

A. Single PO/Invoice to manage all annual service provision.

B. One supplier for all related services.

Option 3 – 'Cybersecurity as a Service'

This is more for the MSP who's looking to build their practice around providing cyber security services, rather than being an all round IT services provider.

It provides the opportunity to specialize, developing a deep knowledge of the current landscape and the ability to anticipate change.

In this instance, DMARC can be added as an element of the overall services provided in thei cybersecurity stack.

The Advantages to You

A. An area of specialization and expertise. Concentrate on this aspect of service deliverability, with the potential to charge a premium.

B. Opportunity to work both your own customer-base and collaborate with other MSPs to deliver cybersecurity services on behalf of their clients.

The Advantages to Your Client

A. Single point of contact for all cybersecurity provisions.

B. The knowledge that you're aware of both current potential threats and ready to provide a rapid response.

Option 1 | Additional Revenue Model

SMB

Number of Domains (Per Customer)	Per Domain	Configuration and Maintenance (Hourly Rate)	Monthly Domain Checks (Hourly Rate)	Monthly Recurring Revenue	Annual Recurring Revenue
X	$X	$X	$X	$X	$X

Option 2 | Additional Revenue Model

Medium/Enterprise

Number of Domains (Per Customer)	Annual, Fixed Cost Per Domain	Annual Revenue
	Fee Includes: • Configuration • Maintenance • Monthly Domain Checks	
X	From $x/Per Domain	$X

Option 3 | Additional Revenue Model

Cybersecurity as a Service | CSaas

DMARC a line item in an overall IT project scope covering:	Annual Revenue
• Provision of infrastructure • Configuration • Implementation • Maintenance • Monthly Check in	
	$X

Conclusion

A flexible approach and adjusting your pricing strategy to meet client needs is a key component in providing a higher level of customer service and competitive edge.

Want to find out more? Contact: partners@easydmarc.us