Are You Hitting the Mark with DMARC?

GIAC GCIH Gold Certification

Author: Robert J. Mavretich
Advisor: Christopher Walker, CISSP

Accepted: October 12, 2019

Abstract

As organizations struggle to protect their end-users from email attacks despite pragmatic methods such as phishing and awareness training, there is another tool available to assist in reducing this threat – Domain-based Message Authentication, Reporting, and Conformance (DMARC). Despite the many tangible benefits of DMARC, including monitoring, quarantining, and rejecting potentially harmful emails based on various indicators, many organizations have not moved to implement DMARC to make a positive difference in email protection and delivery worldwide. This paper highlights the benefits and outline steps that security technology departments can take to effectively partner with internal stakeholders (such as Sales and Marketing) to establish a win-win scenario of appropriately protecting the enterprise while furthering business goals.

1. Introduction

The current business environment presents many challenges to success. Connecting with customers through mediums such as social media has taken precedence over electronic mail. Therefore, it is easy to overlook the security of plain old electronic mail in the present day when considering the future. "E-mail is involved in more than 90% of all network attacks, through such exploits such as spearfishing" ("What is DMARC and Why use DMARC for Email?"). As social media continues to be pervasive in society and continues to evolve quickly, electronic mail is seemingly given attention only when used as a vector of compromise into an organization.

Within the constructs of communication technology and how commerce operates continuously (24 hours a day, 7 days a week, 365 days per year), the distant future may only be three to five years away. Due to short business cycles, it may be challenging to start an initiative of securing email communication (planning and monitoring) and re-visit at a later date (reviewing progress and making quarantine decisions) with many competing business priorities and emerging communications platforms. However, suffering at the virtual hands of vast amounts of spam and allowing malicious email to propagate can have wide-reaching negative impacts within the organization. If these negative impacts extend to employees and customers, it may also affect revenue. When viewed through this customer and financial impact lens, securing plain old email communication channels is a problem worth addressing.

Email **must** work to foster communication to support profitability, growth, and excellent customer service. In a digital world, email is always on, always delivering (unless inappropriate configurations or outages prevent that flow) and to a large extent, not given much thought if emails are sent and received – even if there is unwanted junk (spam) delivered with other expected mail. As with any new technology, the *use* and not necessarily the *security* of that technology is the immediate focus, as some vectors of abuse may not even exist until the technology has been in use for a significant duration of time. As email has been in mainstream use for decades (Buxton, 2019), we can no longer consider it a new technology.

It is indicative of how vital plain old email is that the U.S. government is a standard position leader in protecting email delivery. The Binding Operating Directive 18-01 from the Department of Homeland Security mandated that government

organizations implement DMARC to help stem the current email security threats and long term implications of drowning in spam and malicious email. "DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing. The purpose and primary outcome of implementing DMARC are to protect a domain from being used in business email compromise attacks, phishing emails, email scams, and other cyber threat activities" (“What is DMARC”).

It is both instructive and refreshing to see the U.S. government taking pragmatic steps to improve the flow of email communication and secure transmission worldwide. The fact that the Department of Homeland Security is issuing a Binding Directive leaves no doubt about the severity of the problem for those who may still need convincing. If attackers have focused email attacks on the public (government) sector, the private sector may not be far behind.

This directive for the implementation of DMARC starts at a low level (implementing monitor mode initially, reject mode after one year) to ensure a pragmatic path forward that can inform stakeholders of its purpose and value proposition. While some organizations may be hesitant to implement anything that may hurt usability and functionality, the first step the directive takes is to compel organizations to create a plan of action within 30 days to enhance email security. Having a plan is tantamount to ensuring success as it paves a path forward with defined markers along the way to determine progress. As the plan crystallizes, it would be wise to review what is perhaps already in place to help with this initiative from a technology perspective.

A typical technical capability at many organizations may be a Sender Policy Framework (SPF), also known as white-listing. "A study by the FTC Office of Technology Research & Investigation (OTech) of more than 500 businesses with a significant online presence found that the majority of the businesses have implemented SPF, one of the two domain authentication tools" (“Businesses Can Help Stop Phishing”). The fact that many companies are already capable and may already be down the right email security journey can support an implementation of DMARC.

Whether an organization is large or small, the DNS team can also be highly engaged, if not formally responsible, to maintain an authorized Sender Policy Framework

(SPF) list. While this list may seem easy to maintain, it can get quite complicated for **both** large and small organizations alike, as vendors that the organization does business with may use a provider such as Office365 or Google to send their email communications. Attempting to white list Google's massive publicly advertised address space makes this task an exercise in futility from a "known and approved" perspective.

Further complicating the issue is the fact that SPF does not give feedback to the domain administrator(s) whose domain it is attempting to communicate with an organization via email if it fails to deliver the message. SPF does not allow any opportunities for course correction, it merely allows or denies, leaving legitimate senders wondering why they cannot deliver to a particular domain.

Within 90 days of starting the program, the DHS requirement pivots to a "combination of SPF and DMARC records, with at minimum a DMARC policy of 'p=none' and at least one address defined as a recipient of aggregate and/or failure reports" (“Binding Operational Directive,” 2017). Setting a DMARC domain policy to "p=none" (which literally means **no** policy; there is now awareness and visibility into what is received through the email gateway and delivered to inboxes) allows an organization to start viewing in a data chart what is received by the corporate email gateway, from which domains, and at what volume; gaining an objective perspective that is guided by existing data is an essential first step in defending the email ecosystem.

Equally important is configuring an address and mail inbox that is capable of receiving these reports that can parse immediately and reviewed after a short period of activity for further details. At this juncture, set some high-level parameters around what senders to reject and what should go to quarantine for further review. Perhaps you have an aggressive spammer who is easily identified by IP address that would represent an easy first option to be on your rejection list. A quarantine example might be multiple communications sent from a cloud-based service provider that needs further validation because the IP space is very large for this particular hosting provider (Google is a great example here).

The DHS directive continues to mandate that within one year, organizations set the DMARC policy to “p=reject” (this will not allow those that have been classified as harmful if not outright known spamming domains and/or actors) for second-level domains and mail-sending hosts. If the organization has used the information gathered

during the monitoring phase appropriately, a number of both malicious and unauthorized domains can be weeded out very quickly on the path to a more secure mail delivery process.

In addition to SPF to aid in the delivery of legitimate email, DomainKeys Identified Mail (DKIM) is also available to assist. DKIM enables validation that the email came from the domain that authorized it – and not from a look-alike, potentially malicious domain. "The sender will configure their email platform to automatically create a hash of the parts of the email they want signed. The hashing process converts readable text into a unique textual string...The problem with DKIM is that because it's more difficult to implement, fewer senders have adopted it. This spotty adoption means that the absence of a DKIM signature does not necessarily indicate the email is fraudulent" (Moorehead, 2016).

The internal process of deciding what parts of the email to encrypt (although the message header is common, as it is always delivered with an email even if other parts may have been stripped away during forwarding), then configuring the corporate email platform to do so, may not be made by a single department within Information Technology, Information Security, or Messaging Services. This may also contribute to the above reference regarding limited adoption.

A DKIM key can be created by choosing a unique value to add to the organization DNS name record(s) in the form of a new text record. This unique value is called a selector. As this will leverage encryption for non-repudiation purposes, a unique public-private RSA encryption key pair needs to be generated internally with a tool such as openSSL in Linux or PuTTY in Windows. The public value can then be shared externally with other domains by publishing that value in the external DNS records of the organization, as shown in the graphic below.

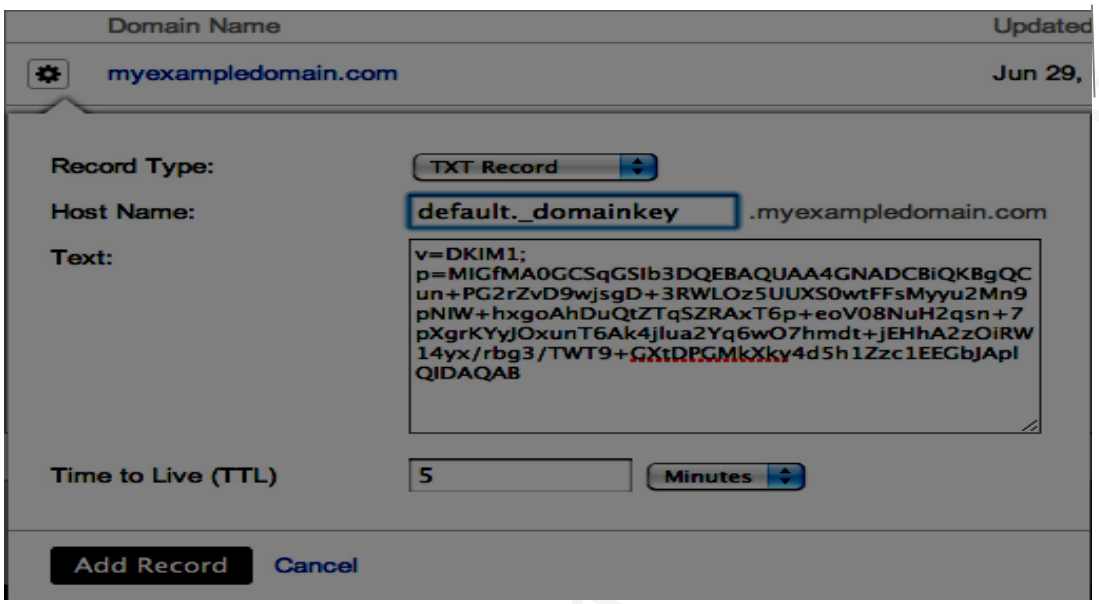

Photo Credit: https://support.rackspace.com/how-to/create-a-dkim-txt-record/

The domain is now ready to communicate in a more secure fashion. “The signing domain, or outbound domain, is inserted as the value of the **d=** field in the header. The verifying domain, or recipient's domain, then use the **d=** field to look up the public key from DNS and authenticate the message. If the message is verified, the DKIM check passes” (“Use DKIM to validate outbound email”).

Another consideration is that of bulk email forwarders such as MailChimp or ConstantContact (for example) that will handle email campaigns and/or communications on an organization's behalf. When working with these mailers, they must be authorized to send on an organization's behalf by having the **bulk mailer public key** published within the authorizing organization's publicly accessible DNS record(s). In this fashion, when any mail system receives email from a bulk mail provider, the domain value in the DKIM-signed header is validated to match the organization that authorized it.

DMARC can help bridge the gap by sitting atop both SPF and DKIM. It will alert organizations what is in use (SPF and/or DKIM), and what the corresponding DMARC policy is (monitor, quarantine, or reject). It also provides information for domain administrators to correct the method of interaction to ensure the delivery/receipt of legitimate email. This is the missing link that DMARC brings to mail administrators and this knowledge can be an effective starting point from which to engage internal business units who will benefit from the use of DMARC.

Marketing and Sales departments will enjoy this detail, as they can authorize campaigns with both large and small senders alike, and weed out the spammers as the information garnered from DMARC telegraphs to other organizations what is a legitimate email and what to reject. Using DMARC also has other positive benefits, such as reducing the amount of time incident handling teams need to devote to investigations. If leveraging SPF, deploying and updating Domain keys with smaller organizations, and building and maintaining authorized sender lists to fully utilize DMARC's potential, the technical support staff can efficiently (perhaps even enthusiastically) and effectively address real incidents.

This type of action plan supports the fact that the use of DMARC is:

1. A valuable tool to combat unwanted email and business email compromise related incidents,

2. Easier to use moving forward from monitoring to rejecting the unwelcome emails,

3. Assist technical staff spend their valuable time on legitimate email incident investigations,

4. A positive influence on email marketing communications campaigns, resulting in higher click-through rates and revenue, defend against brand dilution by nefarious actors, and increase customer's pure brand awareness.

2. Establishing the Program

2.1 Initial DMARC Configuration

For a successful DMARC implementation, it is critical to establish and assign responsibility to a governance team to maintain the process and any associated deviations from that process (risk assessments and sign off). Without a team that is identified to run the program, it is possible that a significant amount of work and data gathering may go to waste. To ensure long term success, "champions" for the initiative should be comprised of stakeholders from a variety of teams such as the DNS team, cybersecurity team, CIRT (Computer Incident Response Team) and other interested parties such as Supply Chain and Legal. However the team is comprised, it is critical that the defined governance team should own the process from initiation to completion, and each group should hold equal influence to determine successful business outcomes and eliminate potential blind spots.

At the onset of the program, after the plan complete, the DNS team may be the best group to decide whether they are going to use an open-source or third-party email vendor to assist with DMARC implementation for the initial monitoring phase (this phase would be 90 days or fewer). Larger organizations may choose to leverage a vendor solution and formalize a relationship (proof of concept) through a short-term contract. "DMARC can prevent the delivery of unauthorized email from your domain, but it can be hard to implement, and gets harder the larger an organization becomes," (“DMARC Implementation,” 2019). Utilizing a third-party, industry vendor allows access to formal training, set up and support, and reporting – all of these can be very useful if the internal DNS team has little experience in implementing DMARC.

If the organization is small, a proof of concept can still be useful, but the cost may eliminate non-open source partners as a go-forward solution. The many options within the DMARC configuration are shown in the graphic below, with the "Policy" tag the first technical step in the process.

Tag	Description
Version (v)	The v tag is required and represents the protocol version. An example is v=DMARC1
Policy (p)	The required p tag demonstrates the policy for domain (or requested handling policy). It directs the receiver to report, quarantine, or reject emails that fail authentication checks. Policy options are: 1) None 2) Quarantine or 3) Reject.
Percentage (p)	This DMARC tag specifies the percentage of email messages subjected to filtering. For example, pct=25 means a quarter of your company's emails will be filtered by the recipient.
RUA Report Email Address(s) (rua):	This optional tag is designed for reporting URI(s) for aggregate data. An rua example is rua=mailto:CUSTOMER@for.example.com.
RUF Report Email Address(s) (ruf):	Like the rua tag, the ruf designation is an optional tag. It directs addresses to which message-specific forensic information is to be reported (i.e., comma-separated plain-text list of URIs). An ruf example is ruf=mailto:CUSTOMER@for.example.com.
Forensic Reporting Options (fo):	The FO tag pertains to how forensic reports are created and presented to DMARC users.
ASPF Tag (aspf):	The aspf tag represents alignment mode for SPF. An optional tag, aspf=r is a common example of its configuration.
ADKIM Tag (adkim):	Similar to aspf, the optional adkim tag is the alignment mode for the DKIM protocol. A sample tag is adkim=r.
Report Format (rf):	Forensic reporting format(s) is declared by the DMARC rf tag.
Report Interval (ri):	The ri tag corresponds to the aggregate reporting interval and provides DMARC feedback for the outlined criteria.
Subdomain Policy (sp):	This tag represents the requested handling policy for subdomains.

Photo Credit: https://mxtoolbox.com/dmarc/details/what-is-a-dmarc-record

Once DMARC is set to "p=none" (“policy=none” is also known as a “monitor” policy) to gather awareness and details of the organization's email volume and type, dashboard information is typically available through both open source and third-party vendor solutions in a raw format. Strive to capture the appropriate amount of data that would provide a minimum amount of time that can be sufficient to gather both security technology intelligence *and* business intelligence that support business decisions. If the business experiences high email volumes during certain parts of the year, that would represent a good “metrics month” to gather intelligence. If the business is always experiencing high email volumes, there may be enough data with which to make decisions in a shorter duration of the calendar year.

An added benefit is that the raw data can be used to develop a user-friendly dashboard format (or a simple PowerPoint with pivot tables, Tableau, PowerBI, etc.) to present the data. Now the program can be socialized internally through a presentation “road-show” format so that the responsible security/technology parties understand their role in ensuring the success of the initiation and implementation of the program long term. After the internal technical implementation parties understand their roles, it is much more intuitive for them to be advocates of the program. Training opportunities through

internal resources or vendor-provided training will provide opportunities to stay up-to-date with changes.

As the internal technical implementation resources gain a deeper understanding through initial configuration and the results from the monitoring phase, they will accurately and repeatedly evangelize the importance of the program to Sales and Marketing and other interested non-technological divisions, such as top-level executives and Finance. Evangelization is a critical way to present benefits, as Sales and Marketing will likely be the most significant consumers/users of the DMARC program as it will support their email campaigns.

Without this socialization of DMARC's benefits, Sales and Marketing will be blind to the significant efforts of implementation. They will also be expected (through a formalized governance process) to participate in the set-up of their initial email campaigns, migrate existing legacy campaigns, and provide business justification (and related risk assessment/exception details) if they want to use a provider that is outside of vetted and approved email campaign providers. It would be wise to let these groups know in advance about the game-changing benefits that they will receive, and that they are crucial partners in this effort.

The ability of technical employees to assist non-technical employees in navigating a well thought out process will provide those non-technical employees the opportunity to gain confidence as they present technical findings in an executive style format. If the organization applies what it learns through the "monitoring" phase and is successful in moving to a "reject" configuration in their DMARC policy implementation, use that cut-over event to highlight increased click-through execution rates of email campaigns. Sales and Marketing can use this inflection point to track brand awareness and affinity, using metrics to see the further value that DMARC has supported.

Once this switch to "p=reject" occurs, all the domains that previously delivered without question, now need to prove who they are or potentially an encryption key to continue. Most of the questionable and outright malicious domains are less likely to show their true colors (actually, IP addresses in this case!) as they would then blocked with a simple SPF configuration. This policy switch event will result in the elusive "win-win-win" situation; reduced email infrastructure loads as it rejects email that is coming from malicious domains or spam domains, reduced work for technical employees as they focus

only on exceptions and regular audits of existing campaign configurations, and increased click-through rates and customer engagement that Sales and Marketing are striving for. DMARC can help think out the proverbial "haystack" of unrelenting junk mail and allow a sharp focus on what is left.

In order to ensure that the process continues to be an effective tool for both the business and technology departments alike, it is also important to offer a service request within an automated IT service catalog system to leverage templates and common (already approved “sending on behalf of” vendors, for example) email campaign platform choices. Whether choosing to implement a vendor product such as ServiceNow or an open-source product, end-users should have an intuitive interface and clear selections to reach the needed forms for their requests.

An example flow within a service management tool would be as follows;

1. Email → 2. Email Campaigns, → 2. Set Up New Email Campaign Vendor(s), 3. Change Existing Email Campaign Vendor configuration(s), 4. Delete Existing Email Vendor(s).

Under “Email Campaigns," there could be a sub-choice (2a in this example) for an exception that would allow for a new vendor that is not on the existing approved list by linking it to a Governance, Risk, and Compliance tool set (GRC) and exception process. In this way, end-users are encouraged to use a well-known provider that the organization already does business with (such as Adobe, Constant Contact, MailChimp) daily. With the appropriate justification provided through a defined exception process, it would also permit faster set up and service while still allowing for situations where a smaller provider is leveraged.

2.2 Domain and Sub-domain Strategies

When determining how to implement a domain strategy, it is wise to carefully craft a domain strategy that allows the organization to grow both organically as a stand-alone company and through potential mergers and acquisitions. As previously indicated, when starting down a strategic project path, it may be hard - if not outright business disrupting - to undertake a massive shift in strategy when failing to account for business realities. For the initial domain creation, leverage the DNS team armed with the knowledge to take the lead in configuration tasks. It is highly likely that this domain name is a derivative of the organization name or defining product, such as sales.software.com or sales.planes.com, for example. It is the sub-domain where DMARC can start to ingrain itself as an ally of the business, and become a hero for the mail administrators.

There is quite a bit of foresight required when creating sub-domains – the more domains that exist, the more DMARC can be used to get specific results and establish a good sending reputation in the worldwide email ecosystem. “One aspect of email reputation that doesn’t get enough attention? Figuring out which domain you’re going to use to send your email. It’s an industry best practice to send from a subdomain, rather than your parent domain…,” (Buxton, 2019). Opportunities to create sub-domains such as sales.company.com and marketing.company.com should be considered, even if Sales and Marketing may be one department and/or have common pursuits, goals, and perhaps even processes. The great benefit of this strategy is helping to ensure that a positive domain reputation can be managed and perhaps mitigated; if one of the sub-domains ends up compromised by an attacker and starts sending spam, the other domain(s) may save the day and temporarily take over the campaigns of the compromised domain(s) until a good reputation can be re-established.

Proprietary "reputation" scores developed by third-party vendors do have the ability to recover relatively quickly from an unfortunate situation(s) such as the one described above. "The higher your score, the better your reputation, and the higher your email deliverability rate. Numbers are calculated on a rolling 30-day average and illustrate where your IP address ranks against other IP addresses," (Boyd, 2018). In other words, there may be a penalty for sending spam in the short term (a compromised computer or email account, perhaps), however, if that device/account stops sending spam,

scores can dynamically drop to a lesser threat score as time marches on. However, online business revenue may suffer impacts in the interim such as a product launch, or a holiday surge in web and corresponding mail blast/offer traffic. A sub-domain strategy can assist in sidestepping potential situations like these. When viewed through this lens, Sales and Marketing **want** to be a part of the conversation, further ingraining the DMARC program within the enterprise.

Using "placeholder" sub-domains, such as acquistion1.company.com, acquisition2.company.com would be forward-thinking on the part of internal technology staff and pave the way to growth by having a domain and sub-domain framework already in place to be easily and quickly leveraged as the company grows. In this example, "acquisition1" can be renamed to a different name. Because of its prior existence in a company's domain schema, having a DMARC policy already set to "p-none" ensures that monitor mode is already set – effectively making it a template that can be leveraged to ensure there are no actionable intelligence gaps when the domain goes into production. Ready to use templates effectively shorten the time to move from "p=none" to "p=reject" as the suggested minimum 30 days of mail traffic can start immediately after a rename to reflect the acquired/new domain and corresponding review of its mail traffic. A preset SPF configuration can also already be in place, to ensure a baseline of communication is possible right from the start.

2.3 Email Senders

An essential part of any program is the maintenance required to keep it functioning at a high level and continuing to show benefits, even if incrementally. Once the DNS team has configured DMARC records, moved through monitoring, and onto rejecting the malicious and suspicious email, an organization may feel the job is complete – but it is not. Through this vital exercise, an organization has learned quite a bit about its intended and unintended actions and possible perceptions on the public internet. Armed with this knowledge, business divisions that may have had a less than ideal relationship with IT have now come to realize that without a partnership and alignment to business goals, technology cannot be efficient and effective in furthering the organizational business goals.

The organization should have learned that there are several large senders in use corporate-wide, and IT should market these as "Preferred Senders" that should be given priority and campaigns standardized on as the larger email providers such as Microsoft, AT&T, AOL who are a few examples of DMARC capable receivers. There should also be several "second-tier" options that vary in number from organization to organization. It is within these second-tier options that IT again has an opportunity to shine within the overall organization and show business value. The second-tier options may not be as big as the larger providers, but may also represent a "shadow IT" function. Due to the multitude of marketing campaign providers, individuals may be able to purchase a turnkey campaign platform directly with a corporate credit card - without going through a formal approval process that considers the organization's overarching email ecosystem.

Regular viewing through the lens of a tool set such as Agari or an open-source tool similar to DMARCIAN (www.dmarcian.org), can help identify and direct these "shadow IT" vendors into an established email campaign process. Without the knowledge of an *ad hoc* vendor communication campaign through a determined process, blocking these type of shadow campaigns as an unknown sender, increases. Another way to highlight the value of the DMARC program is to include Accounts Payable and Vendor Management into a regular email provider audit and assessment conversation.

Identifying a budget level that does not exceed a certain threshold requiring senior-level approval (perhaps $5,000 - $10,000 maximum), represents an opportunity to introduce the formalized process to those who would try to go it alone. While these individuals may have the best of intentions, it can unnecessarily complicate the overall efforts to secure the email communication channel by creating the opening for shadow IT in the form of turnkey email marketing campaign vendors.

As a further offering, socialize the continued gains from the DMARC process through quarterly newsletters, company-wide annual Information Security awareness training, and short videos from senior-level executive extolling the virtues and benefits of the email security initiative. For senior-level executives, provide timely news items that show the concepts of email "whaling" to convey that top executives (whales) are directly threatened by malicious actors every day for their considerable proprietary knowledge and company financial access. "...CEO fraud, or whaling—have been around since at least 2013. Between October 2013 and May 2018, more than $12 billion in domestic and

international losses were attributed by the FBI to BEC scams," ("BEC Scams Remain a Billion-Dollar Enterprise", 2019). DMARC will help protect these senior executives.

Define, collect, and report metrics that make sense from an organizational standpoint (number of quarantined messages from certain providers, for example). Update continuously and leverage those metrics to help inform broadly and build support and trust among internal consumers. Showing the success of implementing DMARC to aid in rejecting malicious mail, alongside the published perils of organizations that do less to protect their organization, will be a powerful differentiation point when requesting funding/budget for the initiative.

While the exact numbers may be hard to establish until you start down the path of DMARC at an organization, the Global Cyber Alliance "estimates that deploying DMARC at enforcement will deliver BEC loss reduction for enterprises of 302K/year as a conservative estimate if business email compromise (BEC) leads to user action 1% of the time. The savings are estimated at 1.3M if the BEC action rate grows to 5%," ("The Real Value of DMARC"). Socialize these preliminary figures to aid in the budgetary process. If this initiative is a small percentage of overall company revenue, it stands a good chance of being approved and funded to defend the company.

3. Conclusion

Despite the technical steps that need to be taken to ensure any organization can realize the benefits of DMARC, the email ecosystem relies on a reliable process carried out by committed people within the organization. Configuring DMARC and setting it to monitor mode is the first technical step. Taking the data and making choices with it increases the likelihood the organization moves confidently in the direction of reject mode, where benefits materialize as the junk mail in the email communication line decreases.

As noted in Harold Leavitt's "Applied Organizational Change in Industry" paper, there are three components of every successful change program: 1) People, 2) Process, and 3) Technology. It is instructive to note that the "technology" portion comes last in that list, and the specific order aligns with the earlier referenced metric of 90% of network attacks stem from people clicking on unknown links. Any program that is designed to increase the security posture of an organization starts with the people who are consumers of the technology/platform. Processes and technology provide a path and tools to plot the course, but business provides the number of lanes, exit signs, and traffic lights that are necessary components to guide any organization (large or small, public or privately held) on its secure email delivery journey.

Technical contributors should be encouraged to do the research and present their findings to the business, so the information is part of a strategic decision-making process. The ability to have a comprehensive viewpoint regarding an organizational email ecosystem makes IT departments a more authentic partner in the eyes of the business, and their reliable "source of truth" to drive positive results. When the technology is supported by a robust and repeatable process, the more people will recognize the role they have to play to defend this critical communication and revenue-driving program.

To ensure long term success of the DMARC program implementation, always consider the following guidelines:

1. Communicate to the organization through web sites, newsletters, and senior-level executive briefings that a new enhancement to email is coming soon.
2. Engage the DNS team to start monitoring the state of email delivery by using an agreed-upon tool set (either open-source or industry-supported) to gather data by configuring the DMARC policy setting to "p=none."
3. Once the DNS team has at least a business driven set of monitoring data, use this to show preliminary findings such as top domains that are engaging the organization, any potentially harmful reputation data available, and any whitelist/blacklist definitions already in use.
4. Partner with Sales and Marketing to identify authorized partners and vendors who send on behalf of the organization, and configure these vendors in the established tool set as "allowable" vendors. Define domain names, IP space, and as many attributes as practical to ensure that the allowed vendors are not blocked when moving a DMARC policy to reject.
5. Communicate again to the organization through web sites, newsletters, and senior-level executive briefings that the new enhancement to email has produced actionable results.
6. Edit the DMARC configuration to p=reject, and ensure there is a "war room" set up to immediately respond to any significant events (unintentionally blocking a preferred partner, for example).
7. Enjoy a decrease in malicious email traffic from known malicious domains, especially those that refuse to participate in the use of DMARC.
8. Deploy regular reporting (at least quarterly to show initial success and progress) to the business, such as Sales and Marketing, as well as IT Risk Management. These reports will show the efficacy/efficiency of authorized senders and (hopefully), a measurable decrease in business email compromise events.

4. References

BEC Scams Remain a Billion-Dollar Enterprise, Targeting 6K Businesses Monthly. (2019, July 23). Retrieved November 11, 2019, from https://www.symantec.com/blogs/threat-intelligence/bec-scams-trends-and-themes-2019

Binding Operational Directive 18-01. (2017, October 16). Retrieved May 30, 2019, from https://cyber.dhs.gov/bod/18-01/

Boyd, W. (2018, Nov 22). 5 Ways to Check Your Sending Reputation. Retrieved June 19th, 2019 from https://sendgrid.com/blog/5-ways-check-sending-reputation/

Businesses Can Help Stop Phishing to Protect Their Brands Using Email Authentication. (2017, March). Retrieved May 30, 2019, from https://www.ftc.gov/system/files/documents/reports/businesses-can-help-stop-phishing-protect-their-brands-using-email-authentication-ftc-staff/email_authentication_staff_perspective.pdf

Buxton, L. (2019, June 19). https://www.braze.com/blog/email-subdomains/

Create a DKIM TXT Record. (2019, Oct 18). Retrieved January 8th, 2020, from https://support.rackspace.com/how-to/create-a-dkim-txt-record/

DomainKeys Identified Mail. (n.d.). Retrieved September 11th, 2019 from https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail#Short_key_vulnerability

DMARC Implementation: Automated Email Authentication. (n.d.). Retrieved July 18, 2019, from https://www.agari.com/solutions/dmarc-email-authentication/

Moorehead, M. (2016, July 16). How to Explain DKIM in Plain English. Retrieved from https://www.validity.com/blog/how-to-explain-dkim-in-plain-english/

Seals, T. (2018, Jan 2). DMARC Adoption Surges. Retrieved November 13, 2019, from https://www.infosecurity-magazine.com/news/dmarc-adoption-surges-ahead-mandate/

The Real Value of DMARC. (n.d.). Retrieved November 13, 2019, from https://www.valimail.com/resources/the-real-value-of-dmarc/

Use DKIM for email in your custom domain in Office 365, 2048-bit, 1024-bit, steps, How it works, SPF, DMARC - Office 365. (n.d.). Retrieved January 8, 2020, from https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email#SetUp3rdPartyspoof

What is DMARC. (n.d.). Retrieved December 1st, 2019 from https://en.wikipedia.org/wiki/DMARC

What is DMARC and Why use DMARC for Email? (n.d.). Retrieved November 18, 2019, from https://dmarcian.com/why-dmarc/

Photo Credit: https://support.rackspace.com/how-to/create-a-dkim-txt-record/

Last Updated: August 5th, 2020

Upcoming SANS Penetration Testing

Instructor-Led Training | Aug 10 ET	**, VA**	**Aug 10, 2020 - Aug 15, 2020**	**CyberCon**
SANS Reboot - NOVA 2020 - Live Online	**Arlington, VA**	**Aug 10, 2020 - Aug 15, 2020**	**CyberCon**
SANS Reboot - NOVA 2020	**Arlington, VA**	**Aug 10, 2020 - Aug 15, 2020**	**Live Event**
Live Online - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	**, United Arab Emirates**	**Aug 11, 2020 - Aug 29, 2020**	**vLive**
Cyber Defence APAC Live Online 2020	**, Singapore**	**Aug 17, 2020 - Aug 22, 2020**	**CyberCon**
SANS Essentials Live Online 2020	**, Australia**	**Aug 17, 2020 - Aug 22, 2020**	**CyberCon**
Instructor-Led Training | Aug 17 ET	**, DC**	**Aug 17, 2020 - Aug 22, 2020**	**CyberCon**
Instructor-Led Training | Aug 17 MT	**, IL**	**Aug 17, 2020 - Aug 22, 2020**	**CyberCon**
SANS Summer Hack Europe 2020	**, United Arab Emirates**	**Aug 17, 2020 - Aug 28, 2020**	**CyberCon**
SANS Japan Bilingual Live Online	**, Japan**	**Aug 31, 2020 - Sep 05, 2020**	**CyberCon**
SANS London September 2020	**London, United Kingdom**	**Sep 07, 2020 - Sep 12, 2020**	**Live Event**
SANS London September 2020 - Live Online	**London, United Kingdom**	**Sep 07, 2020 - Sep 12, 2020**	**CyberCon**
SANS Philippines 2020	**Manila, Philippines**	**Sep 07, 2020 - Sep 19, 2020**	**Live Event**
SANS Baltimore Fall 2020 - Live Online	**Baltimore, MD**	**Sep 08, 2020 - Sep 13, 2020**	**CyberCon**
SANS Baltimore Fall 2020	**Baltimore, MD**	**Sep 08, 2020 - Sep 13, 2020**	**Live Event**
SANS Munich September 2020	**Munich, Germany**	**Sep 14, 2020 - Sep 19, 2020**	**Live Event**
SANS Munich September 2020 - Live Online	**Munich, Germany**	**Sep 14, 2020 - Sep 19, 2020**	**CyberCon**
SANS Network Security 2020 - Live Online	**Las Vegas, NV**	**Sep 20, 2020 - Sep 25, 2020**	**CyberCon**
SANS Network Security 2020	**Las Vegas, NV**	**Sep 20, 2020 - Sep 25, 2020**	**Live Event**
SANS Australia Spring 2020	**, Australia**	**Sep 21, 2020 - Oct 03, 2020**	**Live Event**
SANS Australia Spring 2020 - Live Online	**, Australia**	**Sep 21, 2020 - Oct 03, 2020**	**CyberCon**
SANS San Antonio Fall 2020 - Live Online	**San Antonio, TX**	**Sep 28, 2020 - Oct 03, 2020**	**CyberCon**
SANS Northern VA - Reston Fall 2020	**Reston, VA**	**Sep 28, 2020 - Oct 03, 2020**	**Live Event**
SANS San Antonio Fall 2020	**San Antonio, TX**	**Sep 28, 2020 - Oct 03, 2020**	**Live Event**
SANS Northern VA - Reston Fall 2020 - Live Online	**Reston, VA**	**Sep 28, 2020 - Oct 03, 2020**	**CyberCon**
Oil & Gas Cybersecurity Summit & Training 2020	**Virtual - US Central,**	**Oct 02, 2020 - Oct 10, 2020**	**CyberCon**
SANS Amsterdam October 2020	**Amsterdam, Netherlands**	**Oct 05, 2020 - Oct 10, 2020**	**Live Event**
SANS Tokyo Autumn 2020	**Tokyo, Japan**	**Oct 05, 2020 - Oct 17, 2020**	**CyberCon**
SANS Amsterdam October 2020 - Live Online	**Amsterdam, Netherlands**	**Oct 05, 2020 - Oct 10, 2020**	**CyberCon**
SANS London October 2020 - Live Online	**London, United Kingdom**	**Oct 12, 2020 - Oct 17, 2020**	**CyberCon**
SANS Prague October 2020 - Live Online	**Prague, Czech Republic**	**Oct 12, 2020 - Oct 17, 2020**	**CyberCon**