SILENT QUADRANT®

SECURING INFLUENCE

RESEARCH REPORT | 2023

Securing Influence

At Silent Quadrant, we are always in search of ways to apply first principles thinking to new and existing challenges that organizations and individuals face when making decisions around security. Our 30-year history has been intrinsically tied to protecting the nation's most influential lobby firms. Based on relationships, respect, and trust, this industry is uniquely human. There are no shortcuts to building these connections, but there are numerous ways to break that trust. As much of critical communication now occurs via email, Silent Quadrant is continuously vetting the most effective solutions to provide assurance and confidence that email traffic can be trusted. To this end, we have conducted a study on the adoption rate of three highly valuable email security protocols among the top-performing federal lobby firms within the United States.

SPF, DKIM, and DMARC are essential email authentication protocols which ensure secure and trustworthy email communication. SPF prevents email forgery and impersonation by verifying the authenticity of the sending server. DKIM adds a digital signature to emails, ensuring their integrity and origin. DMARC combines SPF and DKIM, allowing domain owners to set policies for handling emails that fail authentication checks. Implementing SPF, DKIM, and DMARC enhances email security, reduces the risk of phishing attacks, protects brand reputation, and fosters trust among recipients. These protocols are crucial for individuals and organizations to maintain the integrity of their email communications and protect against email-based threats.

Statistics on Business Email Compromise

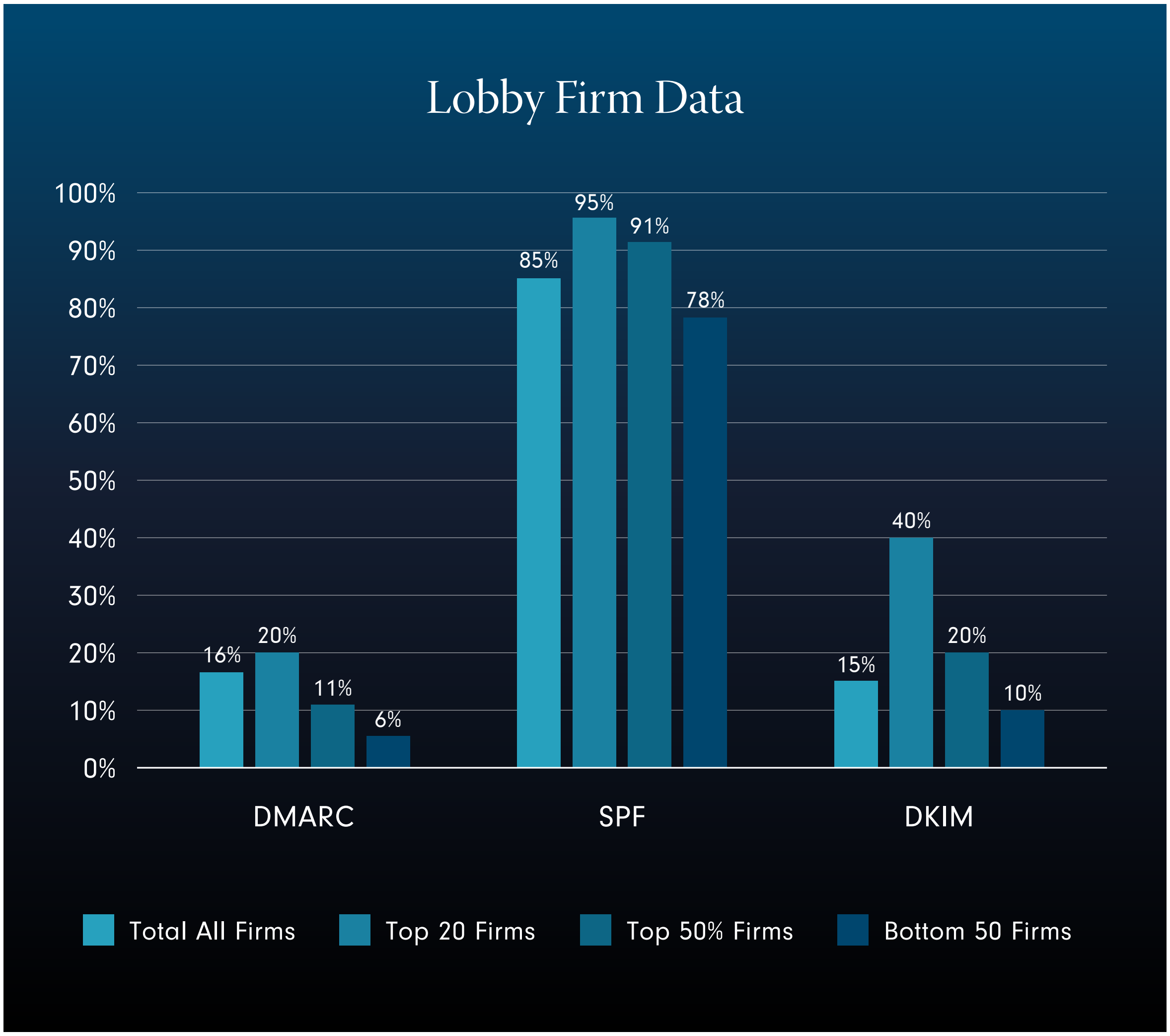
When discussing email security, it is important to contextualize the threat landscape that we all face day in and day out. Business Email Compromise (BEC) has emerged as a highly concerning threat, wreaking havoc on global businesses' financial well-being. The 2022 FBI Internet Crime Complaint Center (IC3) report sheds light on the escalating financial implications of BEC attacks. With reported losses exceeding $5.4 billion in 2022 alone, BEC attacks significantly drain global business finances, highlighting the urgent need for increased vigilance and robust security measures.

The IC3 report reveals a rapid proliferation of BEC incidents, with a 15% increase in reported cases compared to the previous year. This surge underscores the growing effectiveness and sophistication of BEC techniques. Cybercriminals continuously refine their tactics, employing payroll diversion schemes, invoice fraud, and executive or vendor impersonation to infiltrate organizations and manipulate employees into transferring funds or sensitive information.

BEC attacks target all industries, with particular vulnerability observed in the financial, healthcare, and technology sectors. The potential for lucrative outcomes in these industries attracts threat actors who capitalize on the success of these attacks. Moreover, the global reach of BEC attacks is evident, with the United States alone experiencing a staggering 14,442 reported incidents in 2022. Other countries like the United Kingdom, Australia, and Canada also suffered substantial losses, emphasizing the widespread nature of this pervasive threat. These statistics underscore the pressing need for cross-sector collaboration, information sharing, and proactive security measures to combat the escalating financial implications of BEC attacks.

Our Findings

To conduct this study, we queried the publicly available domain-related information for the 350 top-performing federal lobby firms by revenue. With this information, we analyzed the statistics around which firms within specific dimensions of each studied group are implementing SPF, DKIM, and DMARC and found the following results.



SPF had an 85.13% implementation rate, DKIM at 15.16%, and DMARC at 16.00%. While SPF was quite widely adopted, DKIM and DMARC are surprisingly underrepresented. As revenue drops, so too does implementation, with the bottom 50 performers having an adoption rate of 78.00% for SPF, 10.00% for DKIM, and 6.00% for DMARC. A trend observed as the scope of the study was broadened: the implementation drops significantly within the lower revenue tiers.

We decided to take this further and expand our investigation beyond the government affairs sector. In doing so, we unearthed a study by Redhunt Lab's Internet-Wide Study: State of SPF, DKIM, and DMARC. Redhunt Lab performed its study on over 2.2 billion domains across various industries. Of the 2.2 billion queried, they received a response from 1.5 billion domains. The overall percentage of the responsive domains with these controls in place was 32% for SPF, 0.04% for DKIM, and 0.036% for DMARC. Even though these numbers are significantly lower, they follow the same pattern demonstrated in our industry-specific study; SPF is implemented at a much greater scale than the other two controls.

Our results – and those of the Redhunt Lab's team - clearly demonstrate a trend in which top performers are much more likely to implement email security controls than a cross-section of all domains. While it is encouraging that SPF is comparably implemented at a much higher rate, the other two controls which go hand in hand with it are rarely seen. According to statistics from dmarc.org, fewer than 6 million total active DMARC records worldwide exist. Implementing SPF is a good start, but distinguishing between real and fraudulent emails becomes problematic without the addition of properly configured DMARC and DKIM.

Example of Improved Defense

To illustrate the real-world implications of these findings and what it means for the businesses properly leveraging these protocols, let's examine two hypothetical organizations—one relying solely on SPF and another fully utilizing the combined strengths of SPF, DMARC, and DKIM.

ORGANIZATION A:
SPF-ONLY IMPLEMENTATION

Organization A recognizes the importance of email authentication and deploys SPF to validate domains sending email on behalf of its own. SPF helps verify the source IP addresses of messages being sent against the authorized IP addresses listed in the organization's DNS records. While this step helps reduce some email spoofing attempts, it falls short in addressing more sophisticated BEC attacks.

In a BEC scenario, a cybercriminal impersonating a high-ranking executive sends an email to an unsuspecting employee, persuading them to initiate a wire transfer to a fraudulent account. Unfortunately, SPF alone cannot prevent this attack because the attacker's email passes SPF validation, as the authorized IP address belongs to a legitimate email server used in the scheme.

ORGANIZATION B:
FULL IMPLEMENTATION OF SPF, DMARC, AND DKIM

Organization B takes a proactive approach against BEC attacks by implementing DMARC correctly. DMARC builds upon SPF by introducing an additional layer of email authentication and policy enforcement.

With DMARC, the organization publishes a DNS record specifying alignment criteria between the "From" address domain and the DKIM (Domain Keys Identified Mail) or SPF authentication results. In addition, DMARC instructs email receivers on handling emails failing authentication, either by quarantining or rejecting them.

When the cybercriminal impersonates the high-ranking executive in our BEC scenario, Organization B's DMARC record detects a misalignment between the "From" address domain and the DKIM/SPF results. As a result, the email fails DMARC authentication. The organization's email receiver can then enforce DMARC policies, such as quarantining or rejecting suspicious emails, mitigating the risk of falling victim to the fraudulent scheme.

Challenges to Implementing DMARC

Modern-day organizations use emails to communicate with clients, stakeholders, and internal team members. Like other technologies, emails are vulnerable to cyber threats, prompting the development of protective measures such as SPF, DKIM, and DMARC. These protocols are designed to detect and prevent email spoofing, ensuring email authenticity and integrity.

However, many organizations bypass these vital security steps for various reasons.

LACK OF AWARENESS

Lack of awareness is why many organizations do not implement SPF, DKIM, and DMARC. According to the Global Cyber Alliance (GCA), only a small percentage of organizations use DMARC, indicating widespread unawareness. Many small to medium-sized enterprises may not have dedicated IT or cybersecurity teams, making them more susceptible to overlooking such measures.

PERCEIVED COMPLEXITY

In addition, the technicalities behind SPF, DKIM, and DMARC might appear daunting. These protocols involve DNS configurations, cryptographic signatures, and regular monitoring. A 2018 study by Agari found that many companies hesitate to implement DMARC due to fears of blocking legitimate emails. Such misconceptions might stem from inadequate technical documentation or guidance.

RESOURCE CONSTRAINTS

Implementing and managing SPF, DKIM, and DMARC require dedicated resources and monitoring. Some organizations may find it challenging to allocate the budget or personnel for these initiatives, especially when they are already stretched thin managing other cybersecurity measures.

OVERCONFIDENCE IN EXISTING SECURITY MEASURES

Many enterprises trust their existing cybersecurity measures enough to believe they don’t need additional protocols. The thinking goes: “We’ve not been a victim so far; our current tools must be sufficient.” This mindset is dangerous because cyber threats are continually evolving. It has proven that not having these email authentication methods leaves an organization exposed and vulnerable.

FEAR OF DISRUPTING BUSINESS OPERATIONS

Implementing security protocols can sometimes come with unintended consequences, particularly in the initial stages. Businesses may also fear that introducing SPF, DKIM, and DMARC might disrupt their email services, causing missed communications and potential loss of business. While the concern is valid, disruptions can be minimized with proper planning and implementation.

VENDOR MISCOMMUNICATION

Some organizations believe that their email service providers have these protective measures in place as default features. However, not all vendors offer them out-of-the-box, leading to a gap in email security. It's always advisable to cross-check with service providers regarding the built-in security features they provide.

In today’s cyber landscape, businesses should not overlook SPF, DKIM, and DMARC. While the reasons for bypassing these protocols can vary, the risks of ignoring them remains consistently high. It’s best to evaluate the pros and cons and make informed decisions for your organization’s cyber-safety.

Risks of Bypassing DMARC

As our digital communication tools evolve, so too do vulnerabilities and. One such area is email communication, which remains a top target for cyber-attacks. That fact prompted the rise of protocols such as SPF, DKIM, and DMARC; designed to minimize the risks associated with email spoofing and phishing.

To better understand the importance of DMARC, let's illustrate the risks your organization might face when they do not implement these protocols.

INCREASED VULNERABILITY TO PHISHING ATTACKS

Without SPF, DKIM, and DMARC, organizations can become prime targets for phishing attacks. Cybercriminals can easily impersonate the company's email domain to deceive employees, clients, and stakeholders into taking malicious actions, such as downloading malware or sharing sensitive information.

DAMAGE TO BRAND REPUTATION

Emails coming from a spoofed domain might not always carry malicious intent. Sometimes, the goal is to tarnish the brand's reputation. For instance, scam emails appearing to originate from a company's official domain can cause mistrust among clients and stakeholders.

FINANCIAL LOSSES

Phishing campaigns are not just about stealing information. They can also lead to direct financial losses. As noted earlier, an attacker might impersonate a company executive and request a wire transfer. Without email verification mechanisms like DMARC, these requests might seem legitimate to unsuspecting employees.

LOSS OF SENSITIVE DATA

With successful phishing, cybercriminals can gain unauthorized access to sensitive company information, including intellectual property, client data, and employee records. This can lead to severe consequences, especially for companies in regulated industries where data breaches can lead to hefty fines.

LEGAL IMPLICATIONS

If an attacker uses a company's email domain for phishing attacks resulting in financial or data losses for others, they might face legal consequences. Even if the company wasn't directly involved in the scam, the fact that an unauthorized person used their email system could lead to legal repercussions.

INCREASED IT COSTS

Ignoring the adoption of SPF, DKIM, and DMARC can lead to higher operational costs in the long run. The aftermath of a successful phishing campaign includes an extensive investigation, system hardening, and a system overhaul. These costs can heavily outweigh the initial investment required to set up proper email security.

Email security through protocols like SPF, DKIM, and DMARC is a matter of fundamental technical compliance with safeguarding the company's reputation, finances, and data. Regardless of size, organizations should prioritize the implementation of these protocols to ensure the integrity and authenticity of their email communications.

Conclusion

Given the level of concern for and discussion of email security, we were surprised to find the level of adoption and full implementation of these three protocols so low. Especially when factoring in the amount of time these tools have been available and the fact that there is no cost barrier to implementing them. However, this should not be an indictment of email security in general, but a call to arms for organizations to get back to their internal IT teams or managed service providers and ask some questions. What if any of these protocols do we have in place? And what, if any, value could we add to our security posture by working to get these configured?

Email security always comes down to someone sitting at a computer making sound decisions while juggling crucial tasks. Implementing basic tools like DMARC, DKIM, and SPF will provide effective screening and information that can help empower the individuals on our teams to make the best decisions.

In the realm of influence, trust is paramount. For over three decades, Silent Quadrant has been the guardian of that trust for the nation's leading lobby firms. Our study underscores a pressing need in a digital world: the fortification of our electronic communications. The data speaks clearly, but beyond the numbers lies the essence of our mission - to secure influence, to protect purpose. As we navigate this ever-evolving landscape, let us remember the words of our Founder & Chairman, Kenneth Holley: "Influence is built on trust, and trust is built on security. In our commitment to safeguarding that trust, we not only protect our clients but also the very fabric of the relationships they've nurtured over the years." Let this be a clarion call to all organizations: prioritize, implement, and fortify. For in the balance hangs not just data, but the very credibility upon which influence thrives.

Contributors

Jake Van Slyke
Primary Researcher and Author, Silent Quadrant Fellow, 2022-2023

Christopher Ellerson
Co-researcher and Author, Silent Quadrant Director, Client Experience

Kenneth Holley
Technical Subject Matter Expert, Silent Quadrant Founder & Chairman

Adam Brewer
Co-technical Subject Matter Expert, Silent Quadrant Chief Executive Officer

About Silent Quadrant

For over three decades, Silent Quadrant has been the cornerstone of security for the nation's premier government relations firms. Our enduring legacy is built on rigorous research, innovative solutions, and a profound understanding of the dynamic digital landscape. "Securing Influence" is more than a motto; it's our unwavering commitment to upholding the trust and reputation our clients have meticulously cultivated. In an industry where every digital exchange is pivotal, we ensure that influence remains intact, and communications are safeguarded. As the digital landscape shifts, Silent Quadrant remains resolute, crafting tailored solutions that empower our clients to navigate with unmatched confidence.