ESG BRIEF

Third-party Security Controls Needed to Close Gaps in Native Email Security

Date: February 2020 **Author:** Dave Gruber, Senior ESG Analyst

ABSTRACT: Email security is considered a top-five priority for most. With the move to cloud-delivered email solutions and an expanding email threat landscape, organizations believe that email security is in a state of transformation and are therefore reconsidering their current email security controls. Most are using or planning on using third-party security controls to fill gaps in the native security controls available from their email service providers.

Overview

ESG recently surveyed 403 IT and security professionals responsible for evaluating, purchasing, and managing email security technology products and services. With the move to cloud-delivered email solutions and the expanding email threat landscape, organizations are facing new email security challenges that are causing them to reconsider email security controls.

While most have migrated to cloud-delivered email solutions, two-thirds still depend on on-prem email solutions for some part of their email infrastructure. Of those utilizing Office 365, 42% are not leveraging the more advanced security controls offered by Microsoft. While most believe there are gaps in native security controls, most also believe that these gaps will eventully be addressed over time. In the interim, third-party email security tools will be utilized to close these gaps. For those already employing third-party controls, half added these controls post-migration to a cloud-delivered email solution.

Phishing continues to be the top threat concern for most, with ransomware and malware a close second. Sensitive data loss is considered the biggest risk, with most depending only on native security controls for sensitive data loss protection.

Budgets plans are up for most, with plans to increase their budgets in the coming 12 months. Top-five priorities for spending include phishing controls, end-user security training, sensitive data protection, ransomware protection, and malware protection.

Research Highlights

1. **Email is a top-five security priority** for more than half of organizations.
2. **More than half believe that email security is in a state of transformation** and will therefore reevaluate all available security controls.
3. **A majority run cloud-delivered email, but report gaps in the native email security controls provided**.
4. **Most plan to use third-party controls** to supplement gaps in native controls.

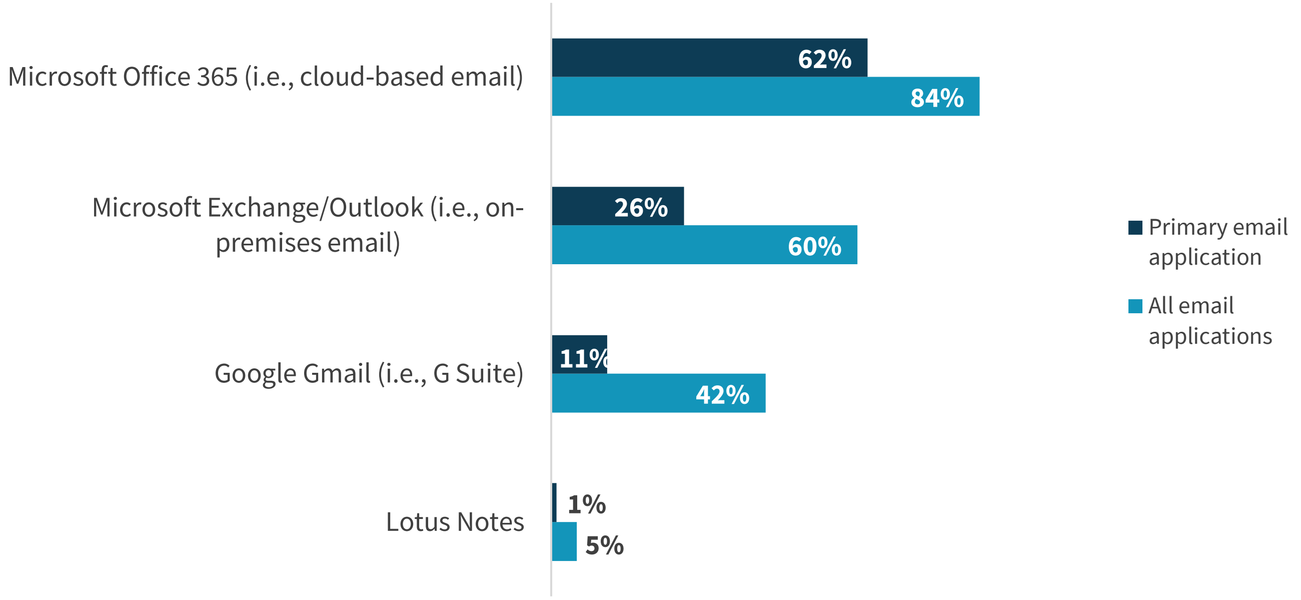
5. Stopping phishing is today’s top email security concern. While ransomware and malware are also top-of-mind, phishing is plaguing most and considered the top risk.
6. Protecting sensitive data is a top-five concern, but few have invested in specialized controls to protect it.
7. Specific business email compromise controls are desired by most.

Analysis

While nine out of ten organizations are now using cloud-delivered email solutions in some capacity, 60% still depend on Miscrosoft Exchange on-premises to operate some portion of their email infrastructure (see Figure 1). According to Figure 2, for those who consider Microsoft Office 365 to be their primary email platform, 42% are doing so using the E1 or E3 license, which omits the more advanced email security controls offered with ATP. Put together, these statistics reflect the need for third-party solutions that can cut across multiple email providers to provide those additional security controls.

Figure 1. Majority Now Use Cloud-delivered Email

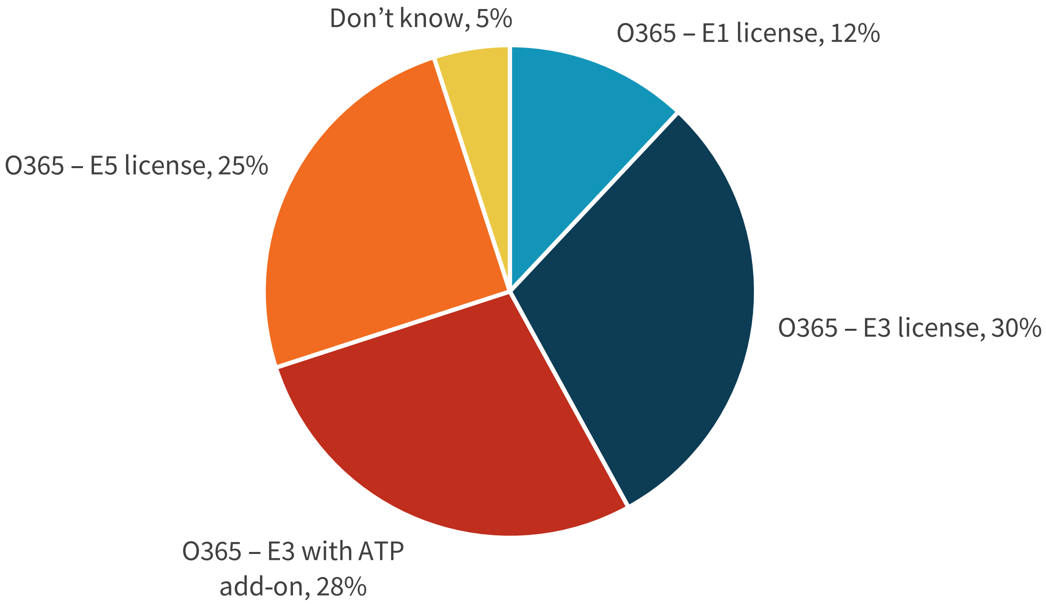
Which of the following email application solutions does your organization currently use? What would you consider to be your organization’s primary (i.e., most widely deployed) email application solution?(Percent of respondents, N=403)



Source: Enterprise Strategy Group

Figure 2. Microsoft Office 365 License Version Breakdown

You indicated that Microsoft O365 is your organization's primary email application. Which version does your organization currently use? (Percent of respondents, N=249)



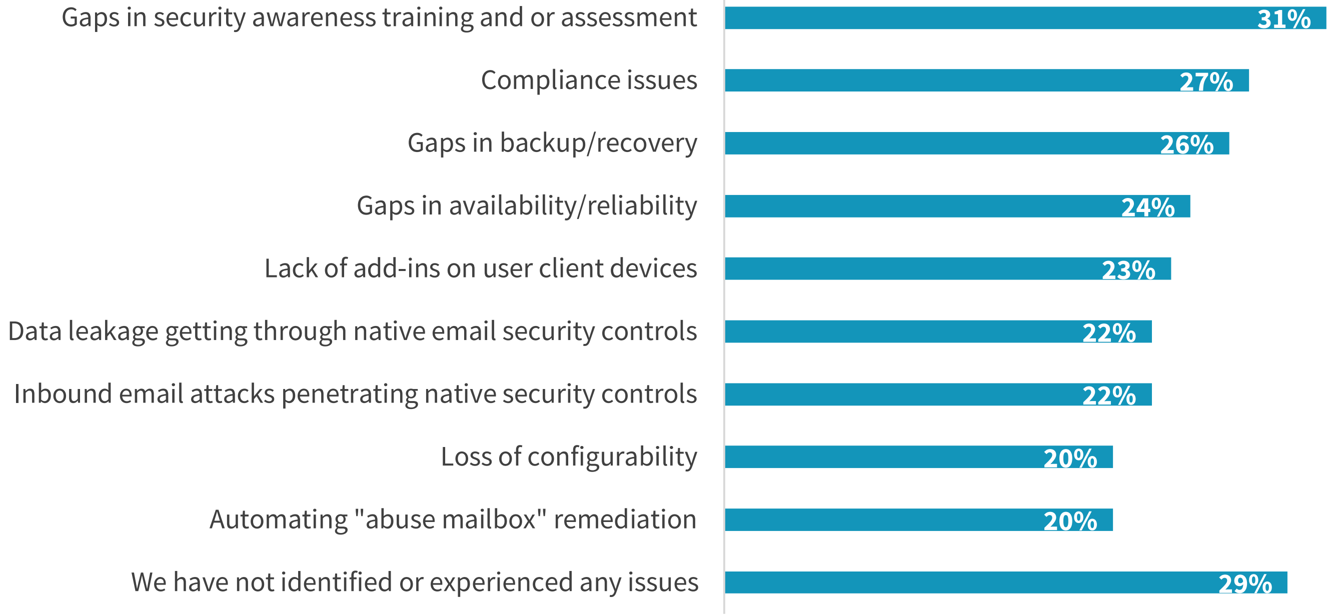
Source: Enterprise Strategy Group

Most see gaps in native email security controls offered by cloud solution providers (see Figure 3). While many want to see security training delivered as a native control, gaps in availability, reliability, and compliance also rank high in the list. It is worth noting that nearly one-third (29%) of respondents have not identified any issues with their organization's cloud-delivered email solution.

The vast majority of those organizations that have found gaps expect to use third party solutions to close them.. Specifically, nearly half (49%) expect to implement third-party controls and tools, while an additional 45% will leverage a managed service to offset the current shortcomings (see Figure 4).

Figure 3. Gaps in Native Security Controls for Cloud-delivered Email

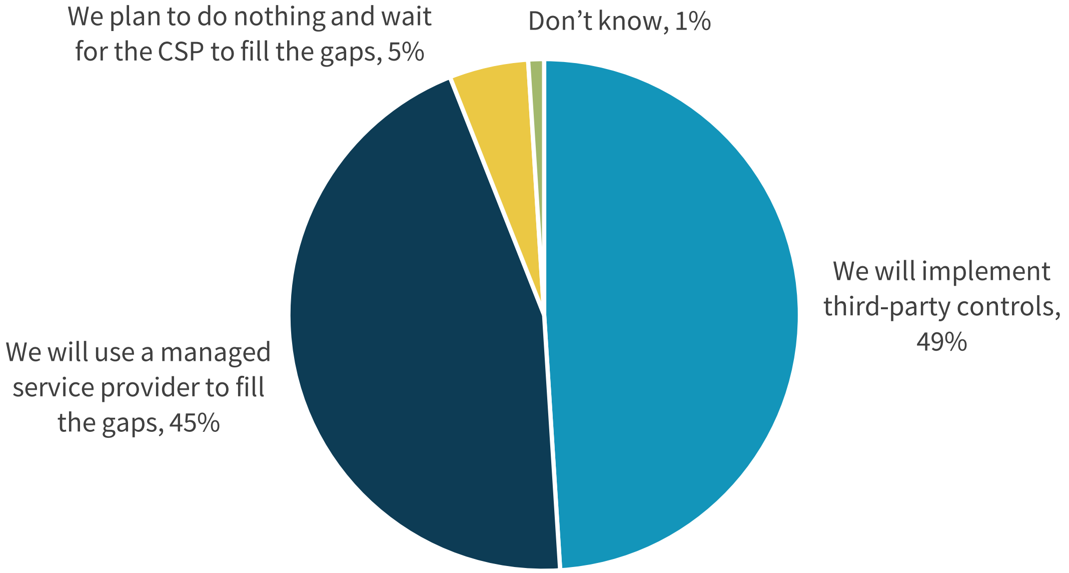
What issues have you identified or experienced since your organization started using a cloud-delivered email solution? (Percent of respondents, N=361, multiple responses accepted)



Source: Enterprise Strategy Group

Figure 4. Addressing Gaps in Native Security Controls

How has your organization addressed or do you plan to address these gaps until your email provider addresses them? (Percent of respondents, N=254)



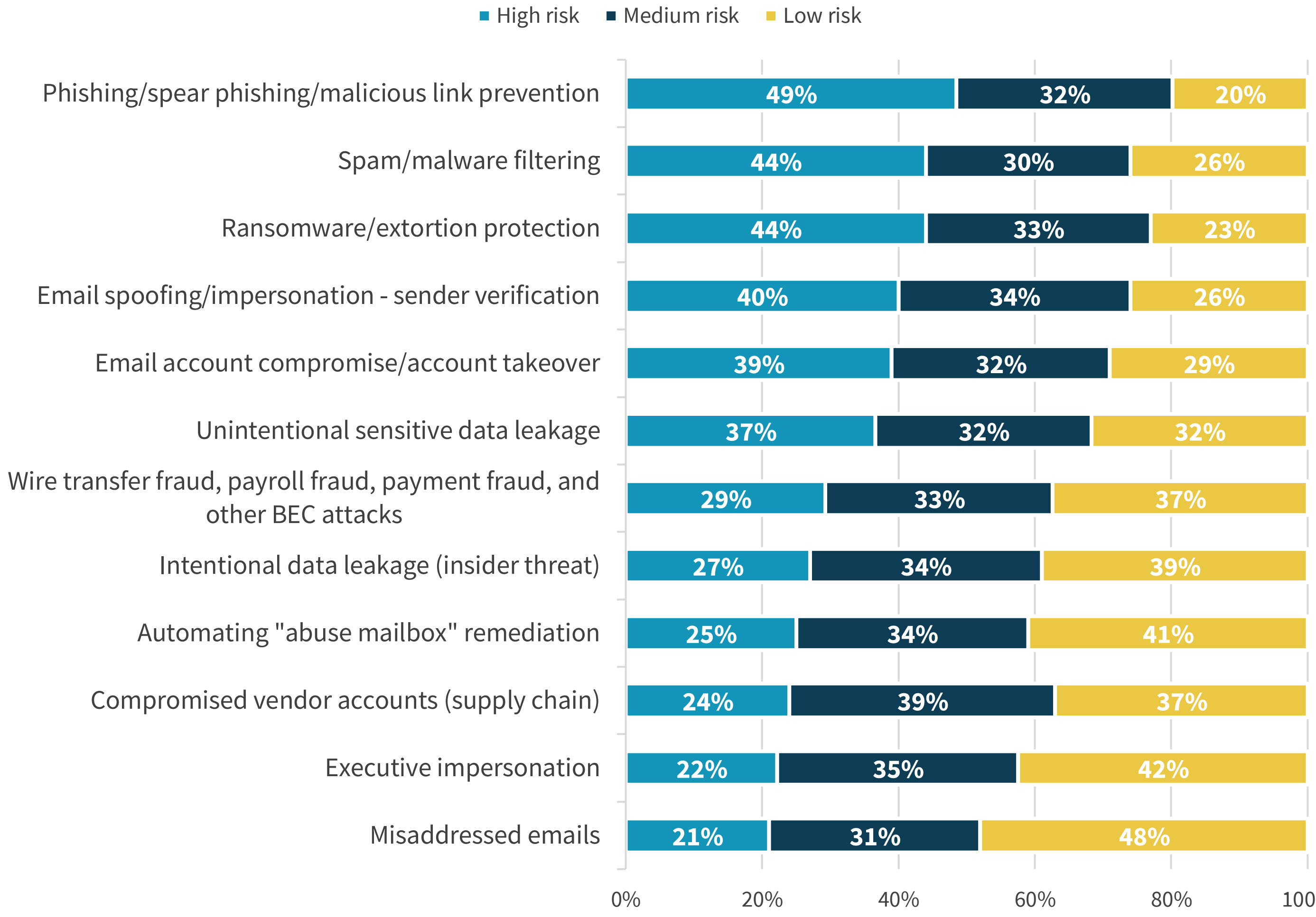
Source: Enterprise Strategy Group

Email Threat Landscape

There are a broad category of more complex attacks involving email today, frequently involving phishing and other impersonation techniques (see Figure 5). Combinations of these attack techniques are applied with many variations, leading to the loss of sensitive data, direct financial loss, and credential theft. While phishing, ransomware, and spam/malware lead the list, email spoofing/impersonation continues to be a major threat that challenges most security controls. Email account compromise is often used as a lead into other more sophisticated attacks, include business email compromise.

Figure 5. Threats and Associated Organizational Risk Projections

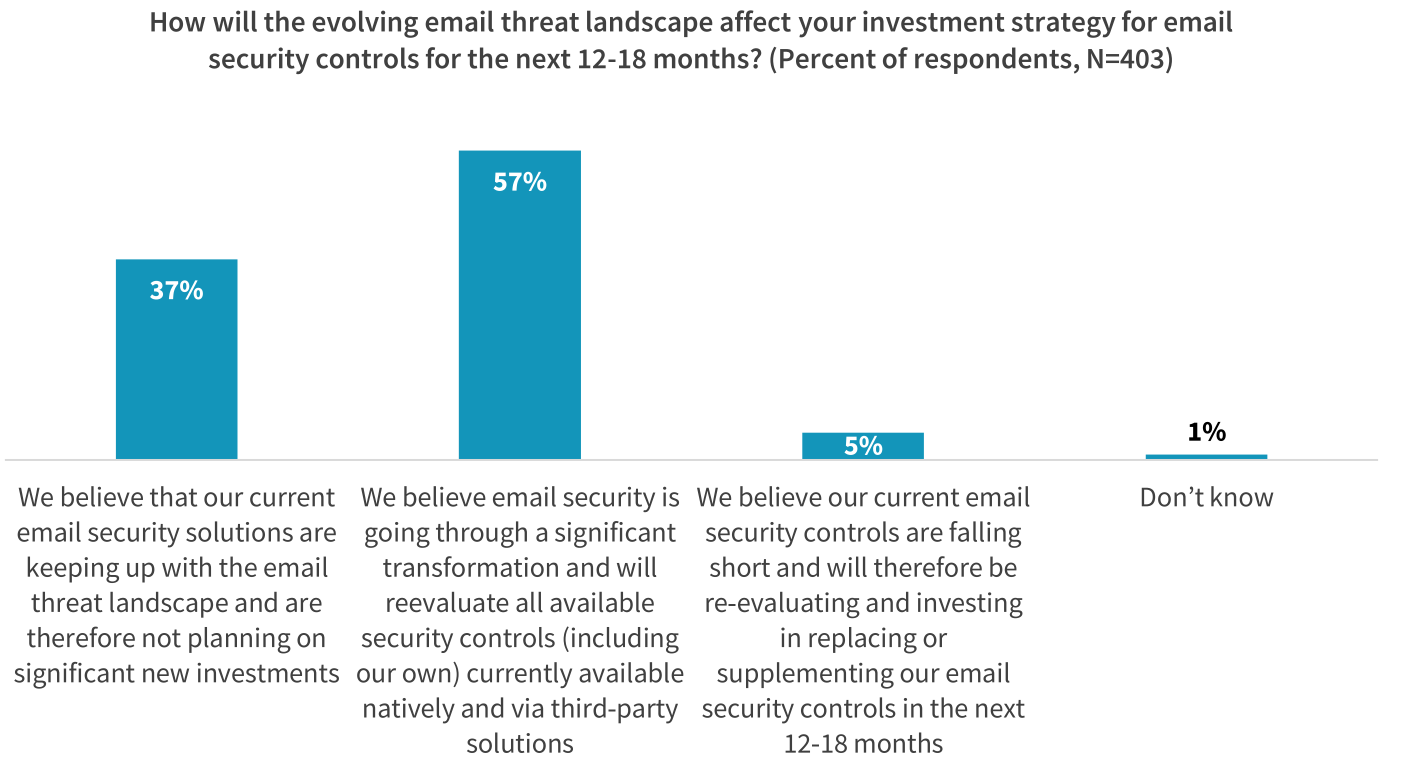
How would you prioritize the following threats in terms of the risk you believe they pose to your organization? (Percent of respondents, N=403)



Source: Enterprise Strategy Group

Higher level terminology/nomenclature is often used today to describe categories of attacks, causing some amount of confusion in how people are describing both threats and successful attacks. For instance, *business email compromise (BEC)* is often used to describe highly targeted, orchestrated attacks that involve a combination of phishing, executive impersonation, and supply-chain impersonation that leads to the criminal transfer of funds. Because of the many variations in BEC-style attacks, IT and security teams often perceive and talk about them differently, causing confusion in the reporting of these attacks. The combination of cloud-delivered email solution use and a more complex email threat landscape are disrupting traditional email security approaches, causing most to believe that email security is going though significant transformation (see Figure 6).

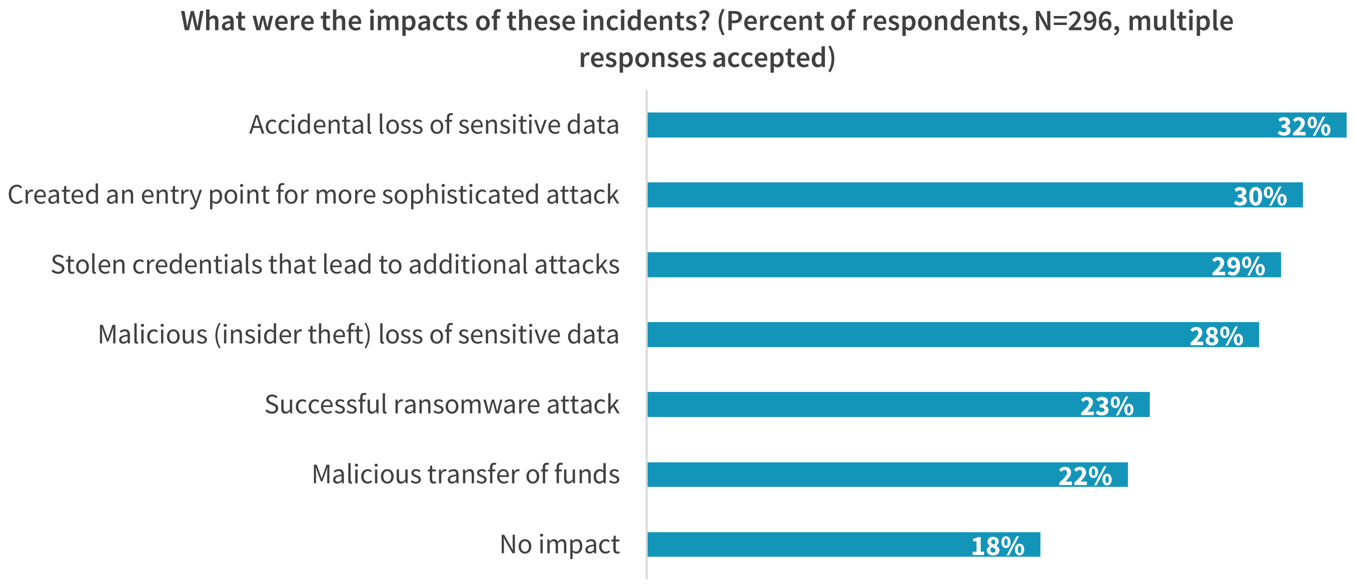
Figure 6. The Evolving Threat Landscape and Its Impact on Investment Strategy



Source: Enterprise Strategy Group

Nearly three-quarters of organizations believe at least one email-borne attack penetrated their defenses within the last year, and according to Figure 7, the loss of sensitive data was the most commonly cited impact. However, email attacks are commonly used as an entry point for more sophisticated, complex attacks—many involving stolen credentials.

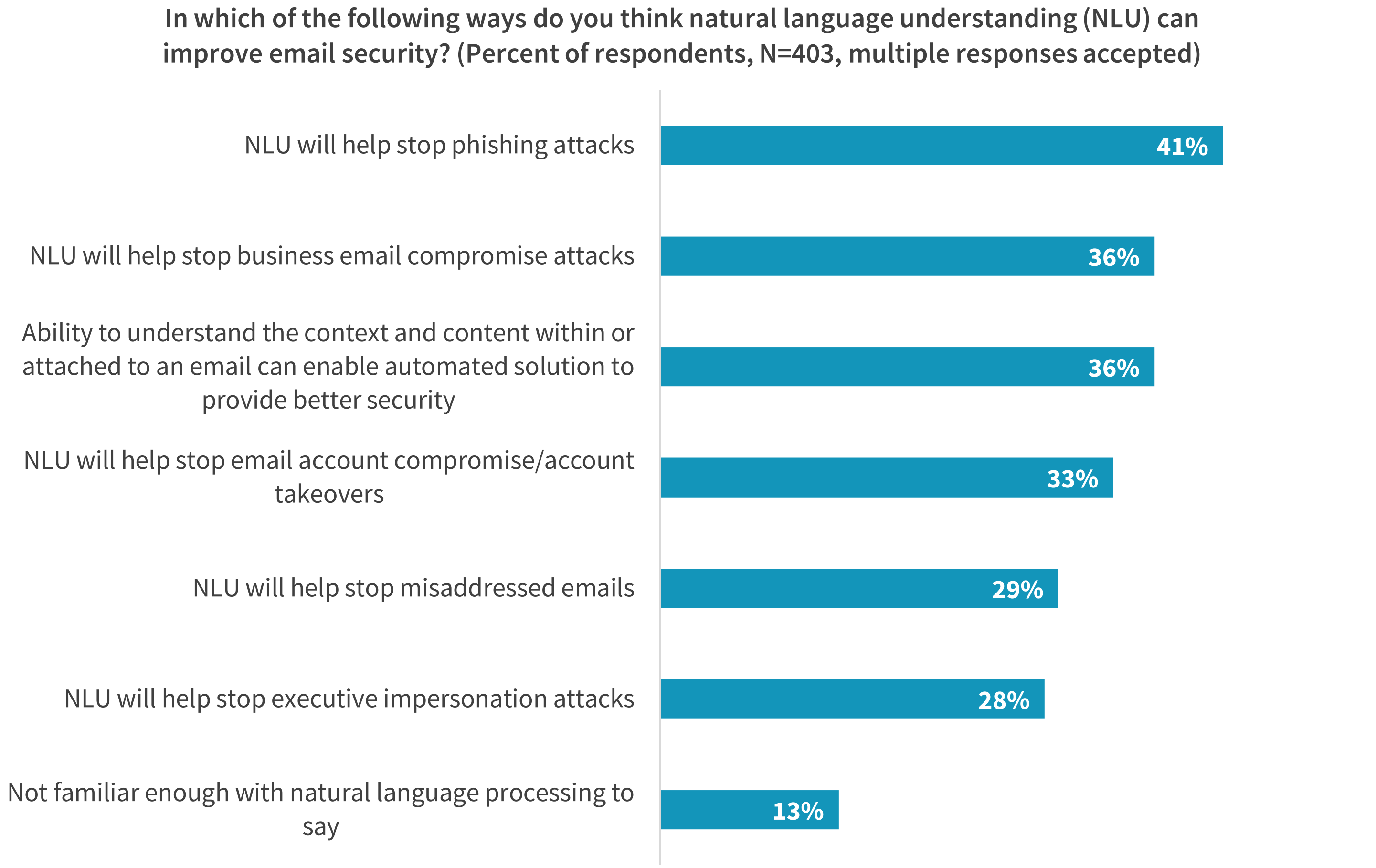
Figure 7. Impact of Email-borne Threats Penetrated Security Controls in Past 12 Months



Source: Enterprise Strategy Group

With traditional security controls often struggling to accurately identify phishing and impersonation-related attacks, new approaches to detection capable of understanding user identity and user behavior are needed. According to Figure 8, many believe that natural language processing (NLP) can help to stop phishing attacks, many of which combine multiple techniques including phishing, executive impersonation, and account compromise.

Figure 8. Attacks Organizations Think Natural Language Processing Will Help with Email Security



Source: Enterprise Strategy Group

The Bigger Truth

With the move to cloud-delivered email solutions and the expanding email threat landscape, organizations are facing new email security challenges that are causing them to reconsider email security controls. Attackers continue to innovate and discover new ways to leverage email to penetrate organizations, leveraging email users.

Complex, targeted email attacks continue to be seen as a significant threat to most. However, confusion around industry terminology and nomenclature is often blurring the way attacks are reported and solutions are described. Email and security vendors need to do a better job helping users understand the dynamics of these attacks together with what security controls can be applied to protect against them.

While cloud service providers continue to invest in adding security controls to strengthen the security of their solutions, most organizations are finding that they need to supplement native controls with third-party controls. With so many attacks leveraging phishing and other impersonation techniques, more sophisticated email security controls are needed. Natural language processing is seen as one approach to solving many of these more complex attacks.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com

contact@esg-global.com

508.482.0188