



Enterprise Strategy Group | Getting to the bigger truth.™

Trends in Email Security

**Security Controls and the Move to
Cloud-delivered Email**

Dave Gruber, Senior Analyst

APRIL 2020

CONTENTS

Research Objectives 3

Executive Summary 4

Most view email as a top five cyber threat vector, with phishing considered the leading email security concern. 5

A majority of organizations run cloud-delivered email, and most plan to use third-party controls to fill native security gaps. 10

Use of encryption and DLP solutions is driven by higher levels of sensitive data flowing through email. 13

Security awareness training and phishing simulation are becoming mainstream. 16

More than half believe that email security is in a state of transformation and plan on reevaluating all email security controls. 19

Research Methodology 23



Research Objectives

With most organizations standardizing on cloud-delivered email in an effort to shift costs from CapEx to OpEx, many have assumed that email service providers would automatically include comprehensive security controls. Many of these same organizations found it necessary to add third-party controls either during their migration or at a later date.

Many have suffered from phishing-related attacks that led to credential theft and BEC, while others faced the loss of sensitive data through both unintentional and intentional actions.

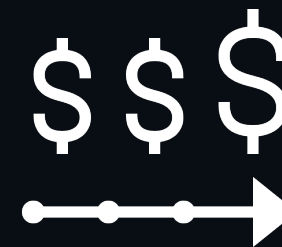
In order to gain insight into these trends, ESG surveyed 403 IT and cybersecurity professionals at organizations in North America (US and Canada) responsible for evaluating, purchasing, and managing email security products, processes, and services. **This study sought to:**



Determine the awareness of specific email security controls and the current state of cloud-delivered email service provider security controls offerings.



Gain insights into the dynamics between IT teams and cybersecurity teams with respect to the selection, deployment, and management of email security controls.

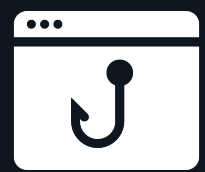


Understand the trigger points influencing investment in email security controls and how decision makers are prioritizing and timing purchasing decisions.



Examine the buying intentions and buyer preferences of email and desktop security teams in regards to email solutions, services, and security controls.

Executive Summary



Most view email as a top five cyber threat vector, with phishing considered the leading email security concern.

More than two-thirds consider email to be one of their top five cybersecurity priorities relative to other security threat vectors. Nearly half experienced email-borne attacks on at least a monthly basis in the past year.



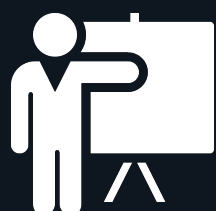
A majority of organizations run cloud-delivered email, and most plan to use third-party controls to fill native security gaps.

Cloud-delivered email solutions dominate the world today, with 90% of organizations reporting usage of these platforms and 73% identifying cloud as their primary platform. More than half of respondents say that native email security controls are insufficient, though only 23% chose to incorporate additional, third-party controls before migrating to cloud-delivered email to compensate.



Use of encryption and DLP solutions is driven by higher levels of sensitive data flowing through email.

Nearly half say that more than 40% of their sensitive data flows through email. Among those organizations that report that more than 60% of their sensitive data flows through email, 88% use email encryption and 53% use data leakage prevention solutions.



Security awareness training and phishing simulation are becoming mainstream.

More than eight in ten organizations currently have a formal end-user security training program, with 55% requiring ongoing training. These organizations that have continual training are much less likely to be victimized by successful email attacks. Organizations that consider email their top overall security priority are twice as likely to be using a phishing simulation service.



More than half believe that email security is in a state of transformation and plan on reevaluating all email security controls.

Given the current, rapidly evolving email threat landscape, 62% of organizations are planning on reevaluating their email security controls, and nearly two-thirds plan to increase spending on email security controls in the next 12 months. Increased investment in automated phishing controls, end-user security awareness training, and encryption services lead the list of email security priorities.

Most view email as a top five cyber threat vector, with phishing considered the leading email security concern.



Most Consider Email One of Their Top Five Cybersecurity Priorities and Many Experience Regular Attacks

Respondents were asked to assess email security relative to other security threat vectors, such as network incursion, DDoS, and stolen passwords, in terms of how much of a risk it is to their organization. More than two-thirds (69%) consider email to be one of their top five cybersecurity priorities relative to other security threat vectors, with nearly one in five identifying it as their top cybersecurity priority.



18%

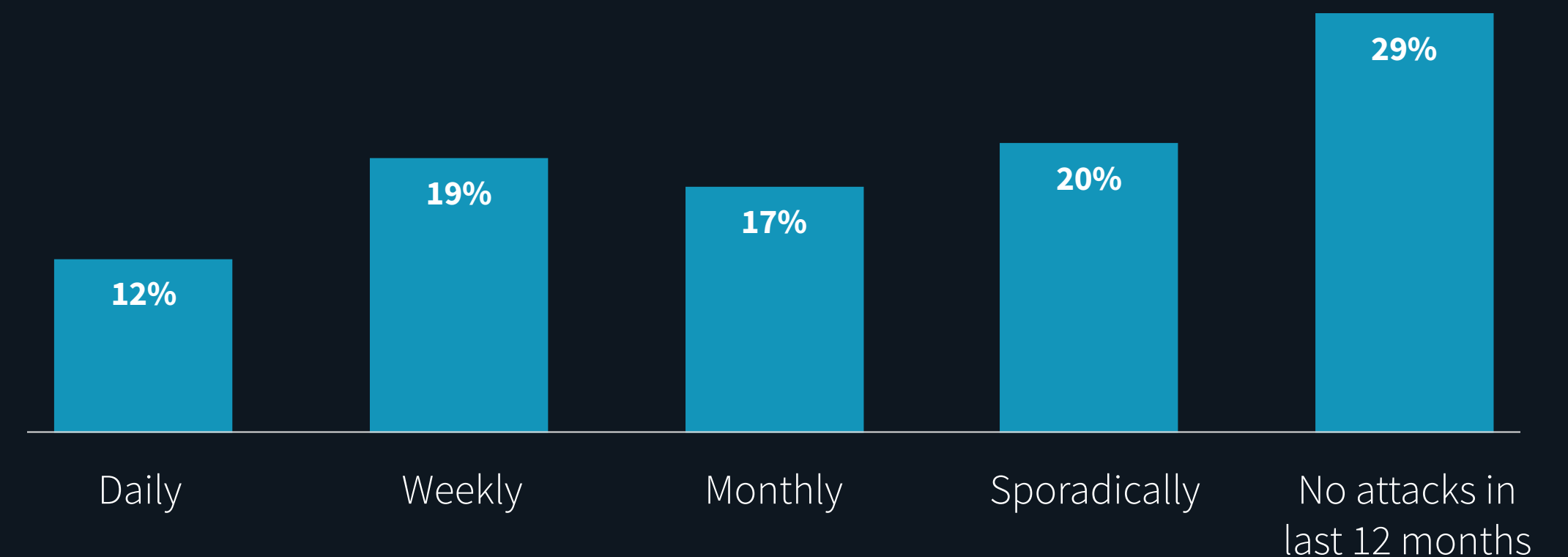
Email security is our **most important** cybersecurity priority

51%

Email security is one of our top 5 cybersecurity priorities

Given the importance assigned to email by most organizations, it is not surprising to see many experienced attempted email attacks on a regular cadence over the past 12 months. Specifically, 68% experienced persistent email attacks, with 48% reporting attacks on at least a monthly basis. It is worth noting that half of those reporting daily email-borne attacks over the past 12 months consider email security to be their organization's number one cybersecurity priority.

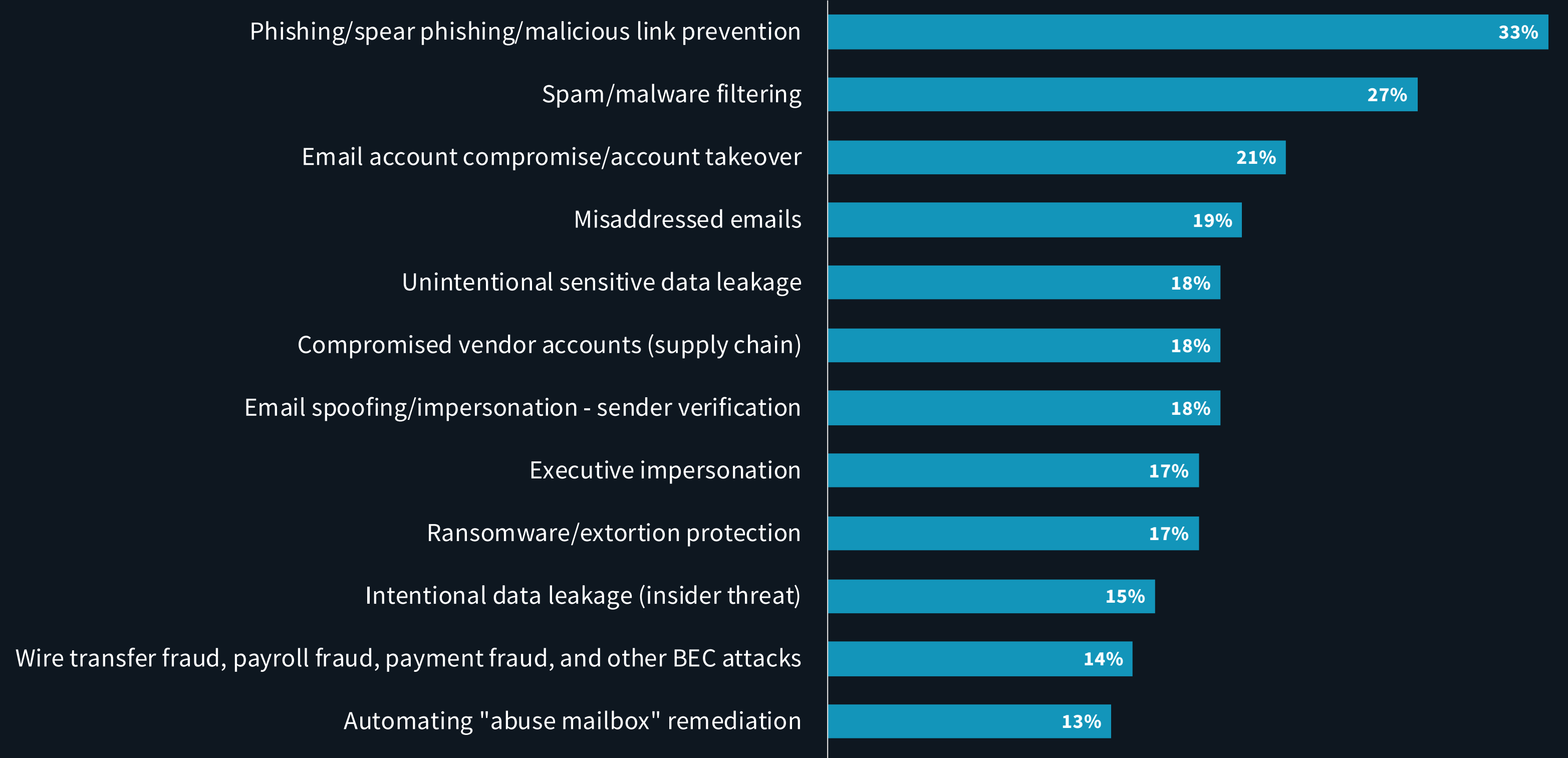
FREQUENCY WITH WHICH ORGANIZATIONS EXPERIENCED EMAIL-BORNE CYBER ATTACKS IN 2019.



Successful Phishing and Malware Attacks Are Most Prevalent

With phishing widely used to support the theft of credentials and other sensitive data, security professionals rank phishing controls at the top of their list when considering the purchase of new email security controls. Executive impersonation, business email compromise (BEC), and vendor/supply chain impersonation all ranked high as downstream threats involving phishing.

Phishing and malware get through existing security controls most often, with one-third reporting successful phishing attacks in the past 12 months and 27% reporting successful malware attacks. Loss of sensitive data through misaddressed emails is also a growing issue.



Phishing often leads to email account compromise, which enables attackers to impersonate executives and supply chains to fraudulently convince unsuspecting users to make payments or payroll changes that move funds into criminal accounts. BEC has been involved in many successful criminal activities leading to some of the largest breaches.

Nearly 60% of organizations report experiencing these types of business email compromise attacks within the last 12 months, with email account compromise being the most commonly cited attack methodology.



60%

have Experienced a BEC
Attack in the Past Year

TOP 5 BEC ATTACK METHODS



37%

Email account compromise/account takeover



27%

Executive impersonation



23%

Vendor/supply chain fraud



20%

Wire transfer or payment fraud

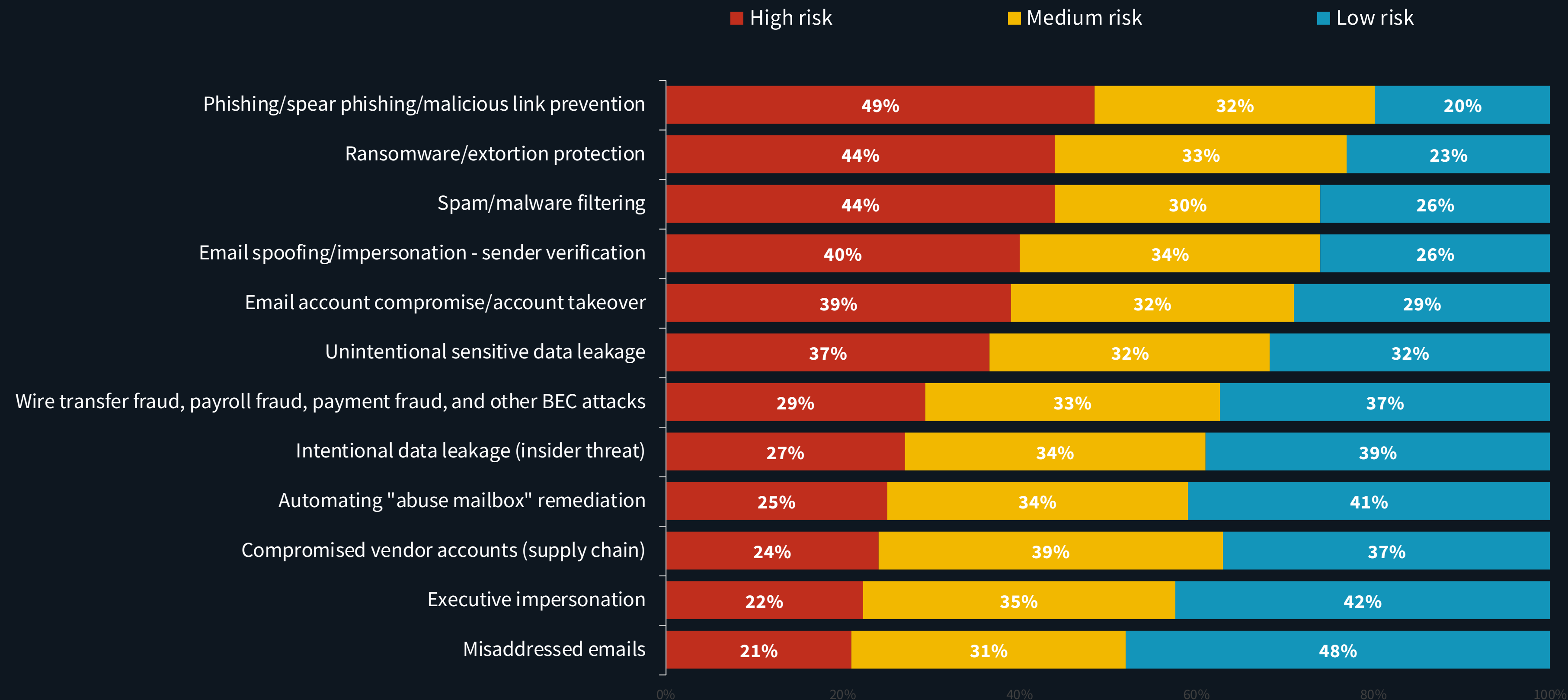



17%

Payroll fraud

Phishing, Ransomware, and Malware Top Perceived Risk Areas

When organizations look at risk, they are assessing the broader potential impact to their organizations. Given that phishing and malware attacks were most successful in penetrating security controls, it makes sense that more than four in ten organizations classify them as high risk. Note that ransomware ranks high as an overall risk, despite successful ransomware attacks being much less prevalent. While executive impersonation and compromised vendor accounts ranked lower on the risk scale, these attack types have historically led to some of the largest breaches.



The background is a dark blue color with a complex, glowing circuit board pattern. A large, stylized cloud icon is positioned in the upper center. Various other icons, including a smartphone, a laptop, and a tablet, are scattered throughout the scene, all rendered in a light blue, glowing style.

A majority of organizations run cloud-delivered email, and most plan to use third-party controls to fill native security gaps.

Cloud-delivered Email Dominates, but Most Believe Native Security Controls Are Missing

Cloud-delivered email solutions dominate the world today, with 90% of organizations reporting usage of these platforms and 73% identifying cloud as their primary platform. However, 65% still utilize on-premises email, at least to some extent. This means that hybrid email security controls are still needed to provide consistent email security controls for most.



73%

say Office 365 and Google are their primary email platforms.

62%

Office 365

11%

Google

More than half (53%) of respondents say that native email security controls are insufficient. Among those organizations, only 23% chose to incorporate additional, third-party controls before migrating to cloud-delivered email. More than one in five (21%) assumed native controls would be sufficient, which proved not to be true, leaving most to add controls post migration.



53%

of cloud email users believe native security is insufficient.

23%

We assumed that controls were missing, so we incorporated third-party controls before migrating

21%

We assumed that the security control would be sufficient, which proved to not be true

6%

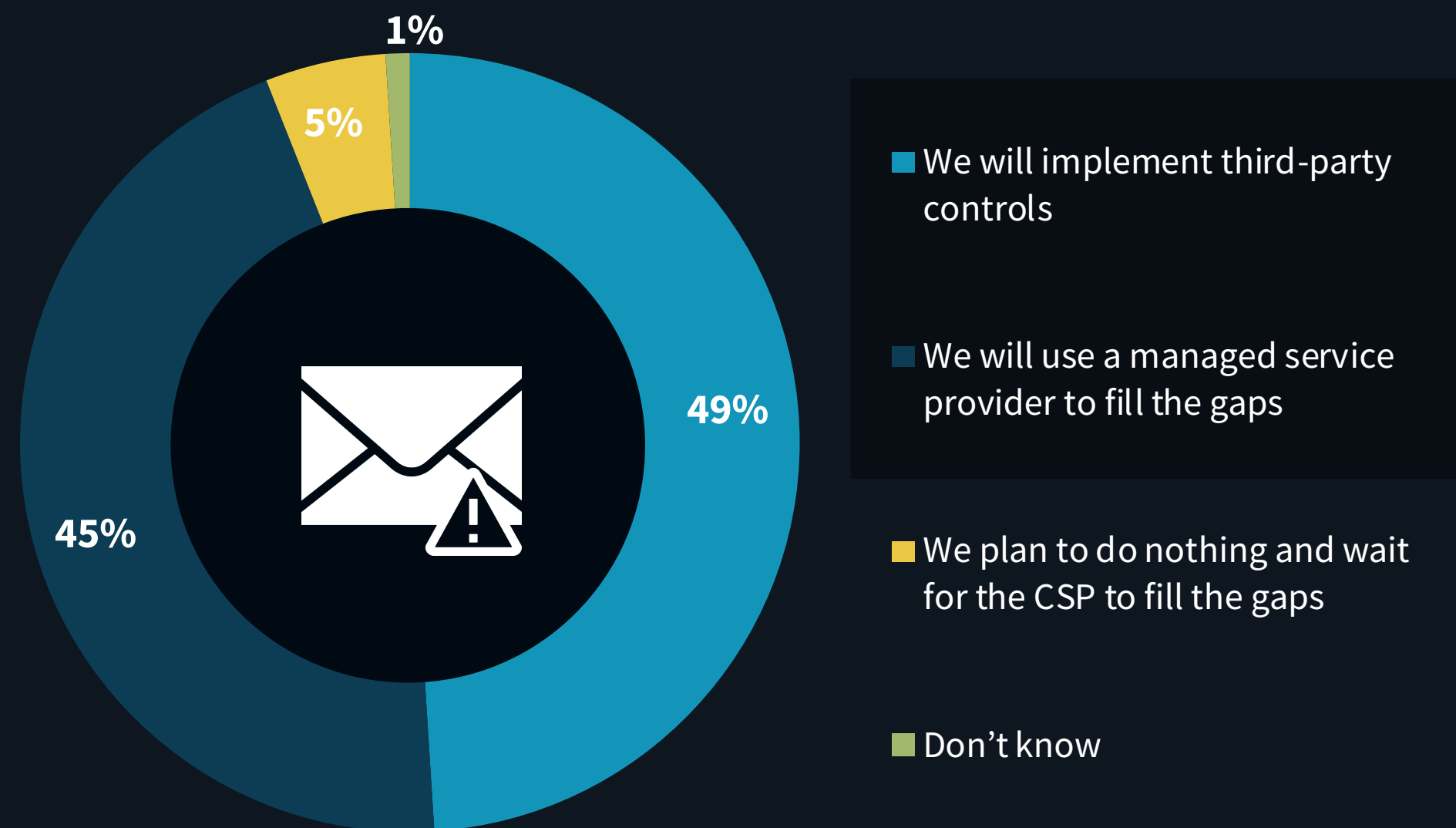
We assumed that controls were missing but decided to proceed without them with a plan to implement additional controls post migration

3%

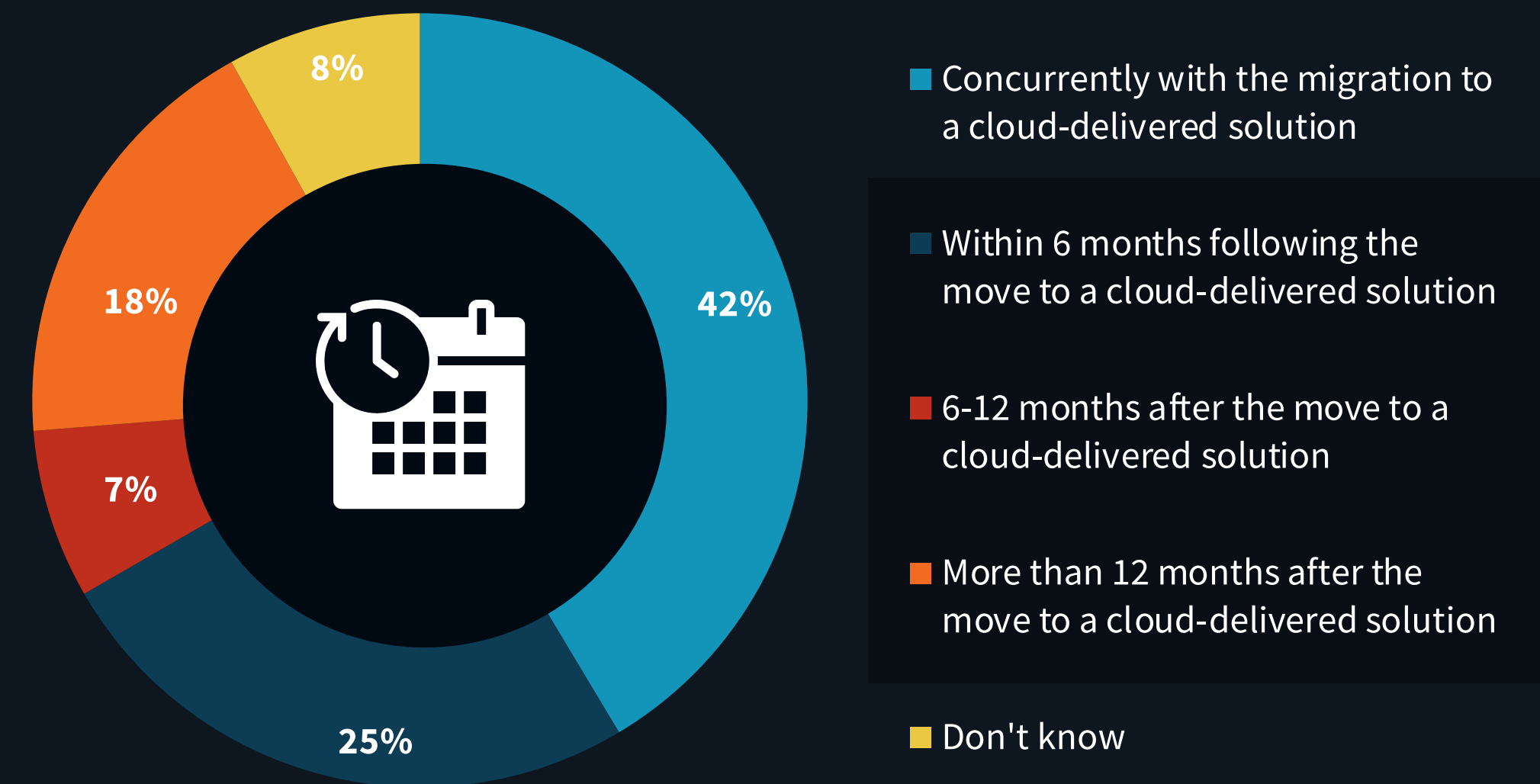
We knew that controls were missing but made an assumption that they would get implemented over time and therefore decided to use only native controls

Confidence Is High that Native Security Controls Will Be Added Over Time, but Interim Gaps Will Be Addressed with Third-party Solutions

The vast majority (94%) of those organizations that identified gaps in native cloud email security controls plan to or are already using third-party controls to address those gaps.



But of those who already use third-party controls, 50% waited until after they migrated to cloud-delivered email solutions, with many waiting more than 12 months.

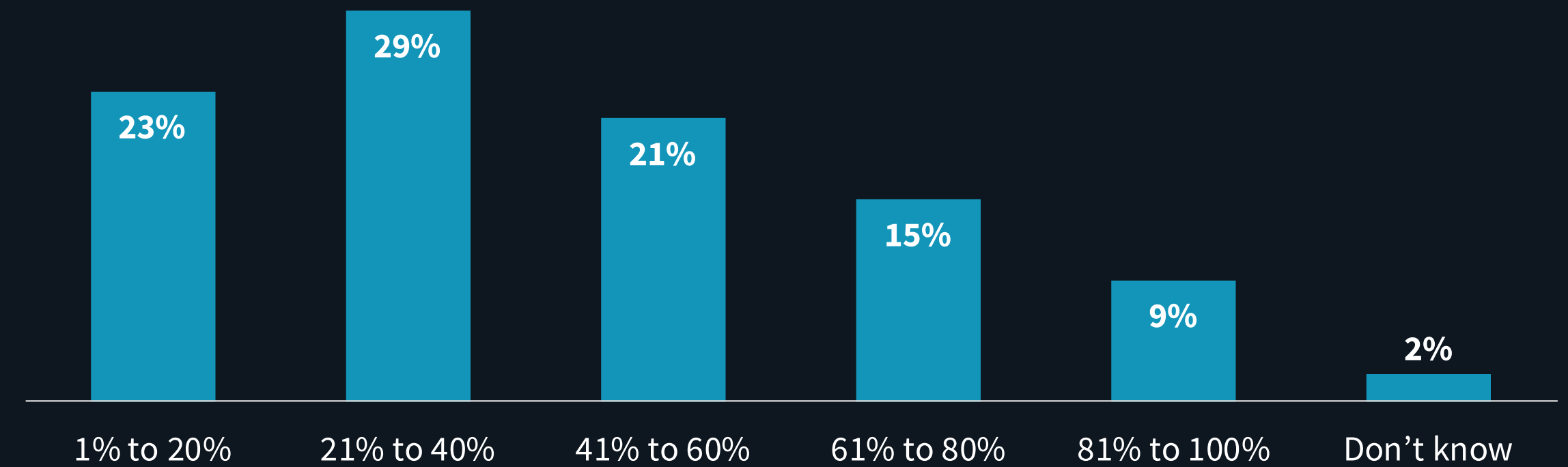


**Use of encryption
and DLP solutions
is driven by higher
levels of sensitive
data flowing
through email.**

Sensitive Data Both Flows Through and Resides at Rest in Email and Drives Encryption and DLP Usage

How much sensitive data, such as intellectual property and employee/customer personally identifiable information, do organizations believe flows through their email application? Nearly half (45%) say that more than 40% of their sensitive data flows through email. Therefore, protecting the data that both flows through and resides at rest within email databases is critical for many.

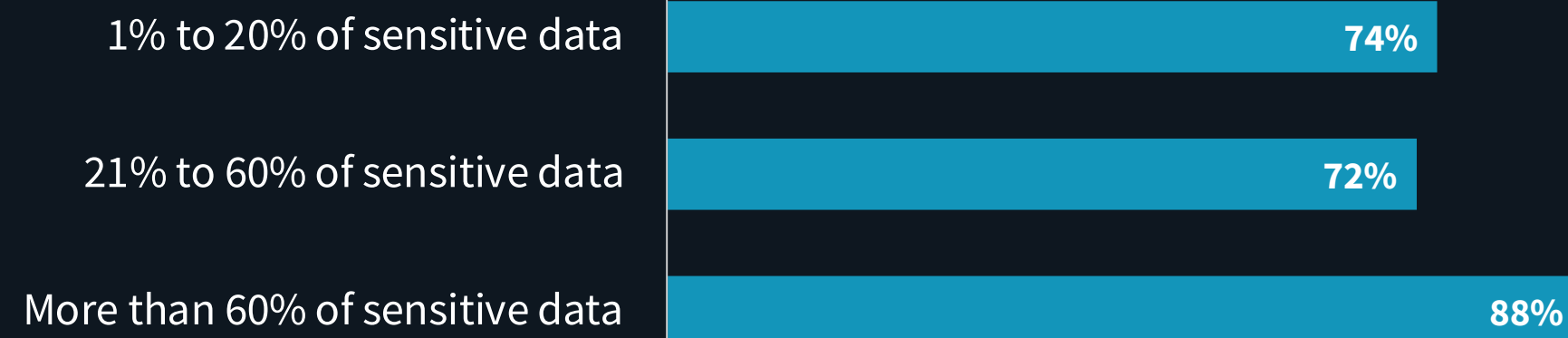
PERCENT OF SENSITIVE DATA FLOWING THROUGH THE EMAIL APPLICATION



75% of organizations use email encryption services and 43% of organizations use email data leakage prevention (DLP) solutions. However, there is a strong correlation between the usage of these technologies and the amount of sensitive data that flows through email. Specifically, among those organizations that report that more than 60% of their sensitive data flows through email, 88% use email encryption and 53% use data leakage prevention solutions.

AMOUNT OF SENSITIVE DATA THAT IS FLOWING THROUGH EMAIL, BY PROTECTION MEASURE

CURRENTLY USE ENCRYPTION



CURRENTLY USE THIRD-PARTY DLP



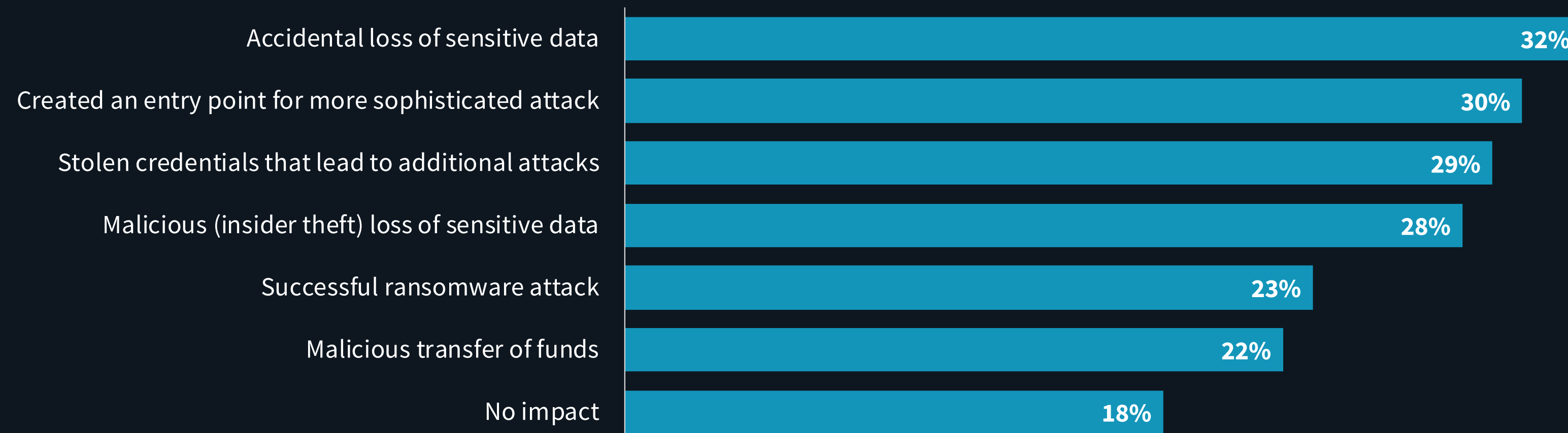
Protecting Unintentional Sensitive Data Leakage Is a Top Concern

With this much sensitive data residing in email, it makes sense that the loss of sensitive data through unintentional data leakage is a top driver of third-party email security solutions.

When looking at the impact of email-borne attacks, the loss of sensitive data rises to the top. When phishing and BEC are involved, security teams consider this loss unintentional. While many attacks start using email as an initial entry point for a more sophisticated attack, others involve credential theft that enables attackers to impersonate others, leading to further criminal theft.

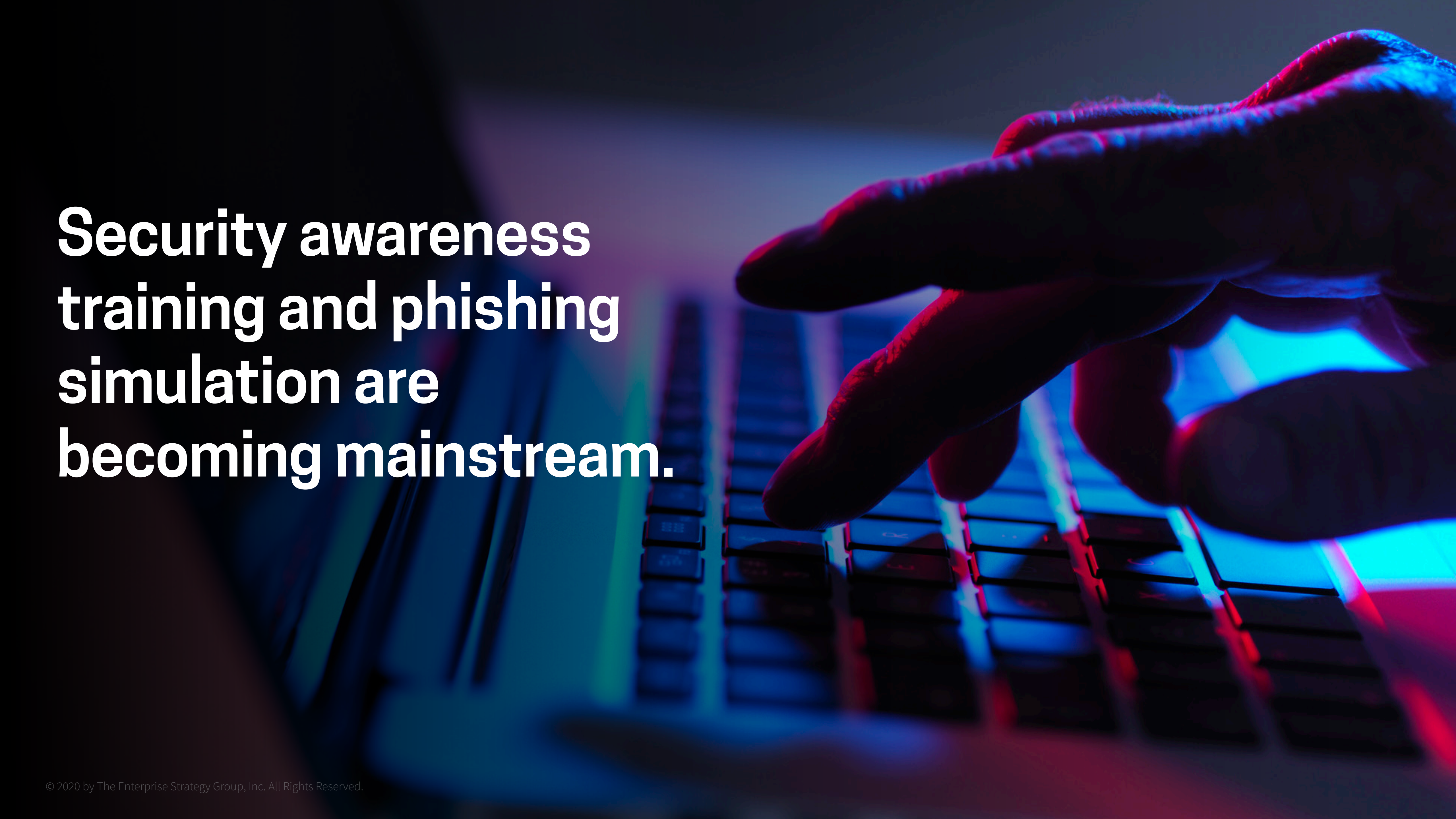
Nearly one-quarter (23%) have experienced successful ransomware attacks, reinforcing the continued attention on protecting against ransomware.

IMPACTS OF EMAIL SECURITY INCIDENTS



19% of organizations added third-party email security controls to combat unintentional sensitive data leakage.

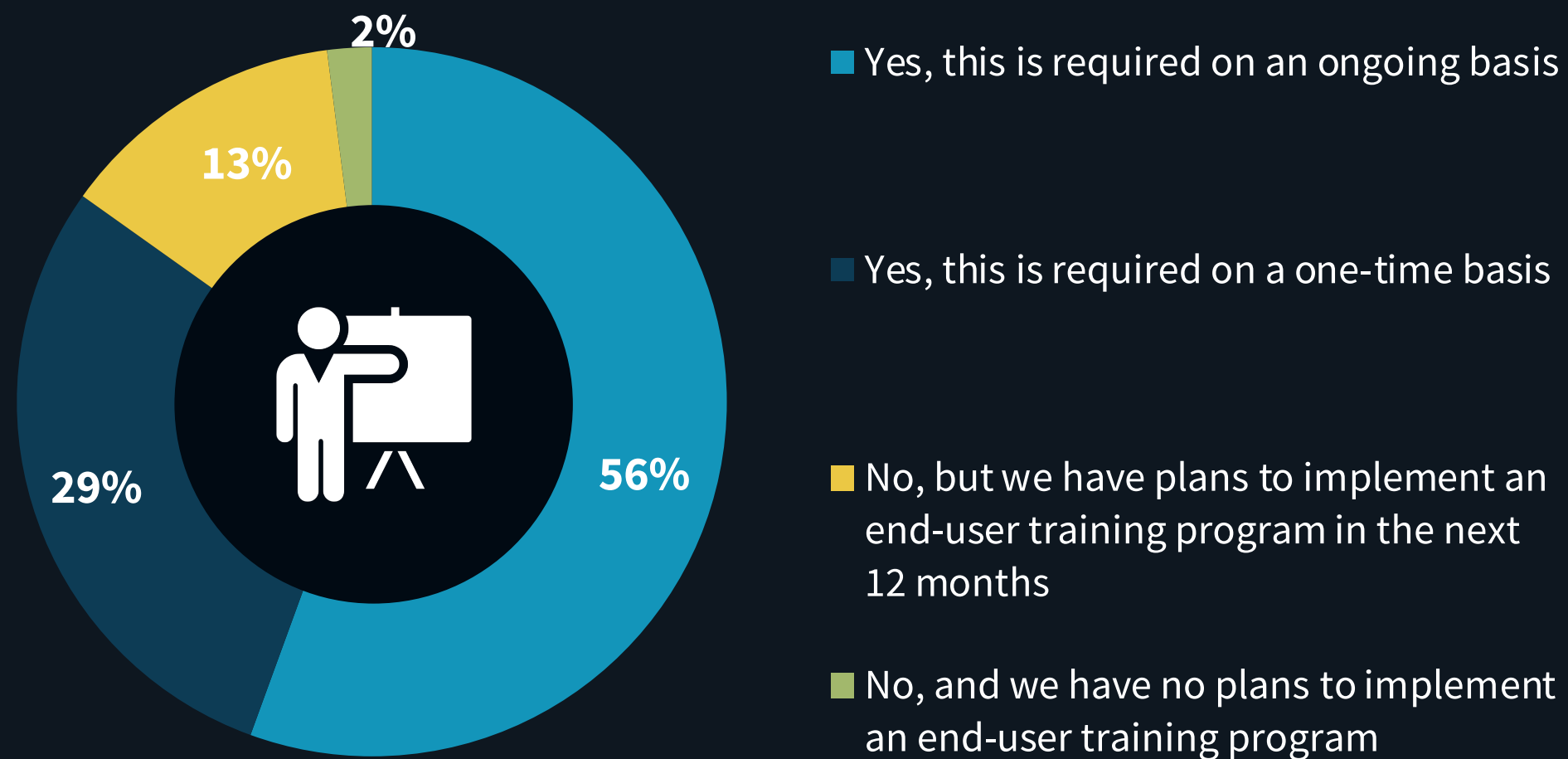


A close-up photograph of a hand typing on a laptop keyboard. The scene is dramatically lit with blue and red light, creating a high-tech, digital atmosphere. The hand is positioned in the upper right, with fingers pressing keys. The keyboard is in the foreground, slightly out of focus, with keys visible. The background is dark and blurred, suggesting a computer workstation or office environment.

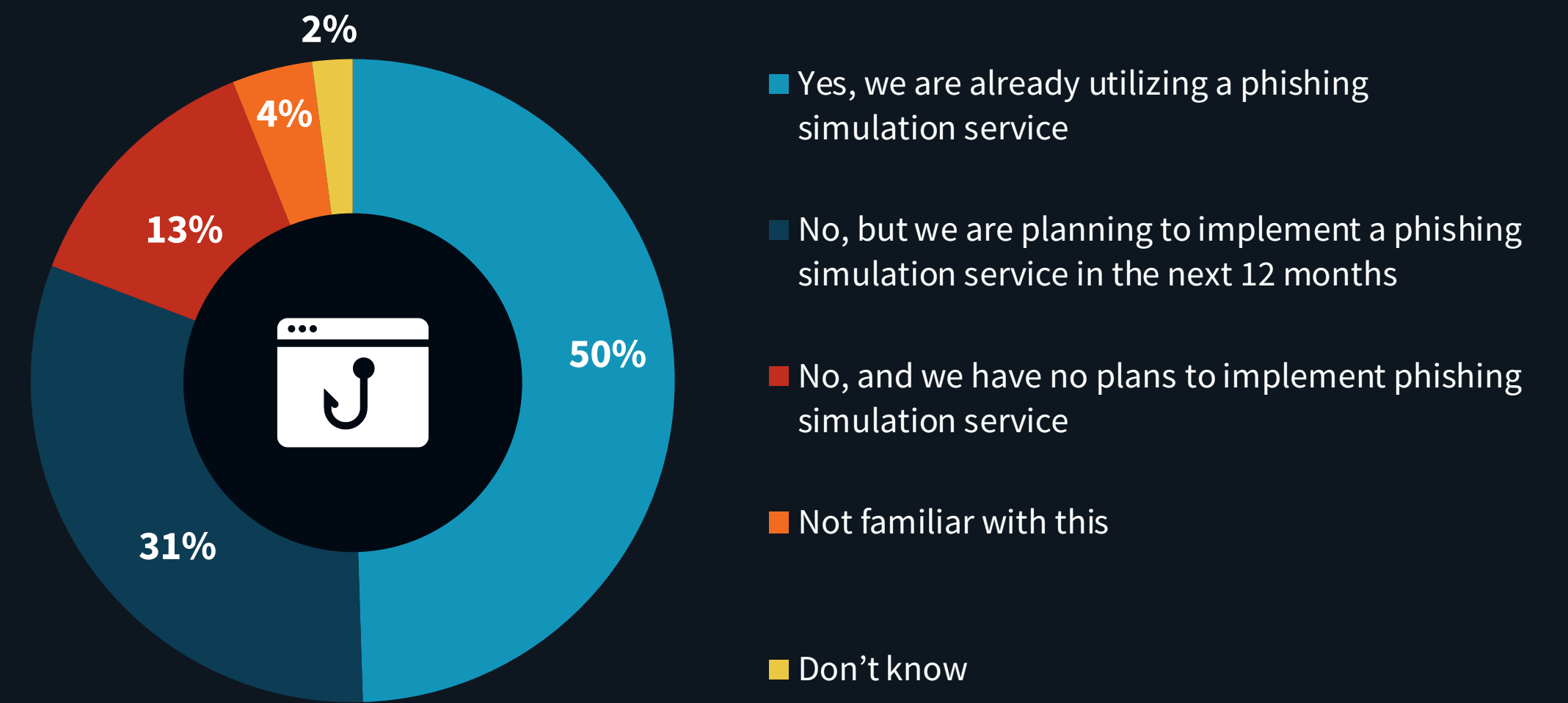
**Security awareness
training and phishing
simulation are
becoming mainstream.**

End-user Security Awareness Training and Phishing Simulation Programs Are Becoming Mainstream

More than eight in ten organizations currently have a formal end-user security training program, with 55% requiring ongoing training. These organizations that have continual training are much less likely to be victimized by successful email attacks.



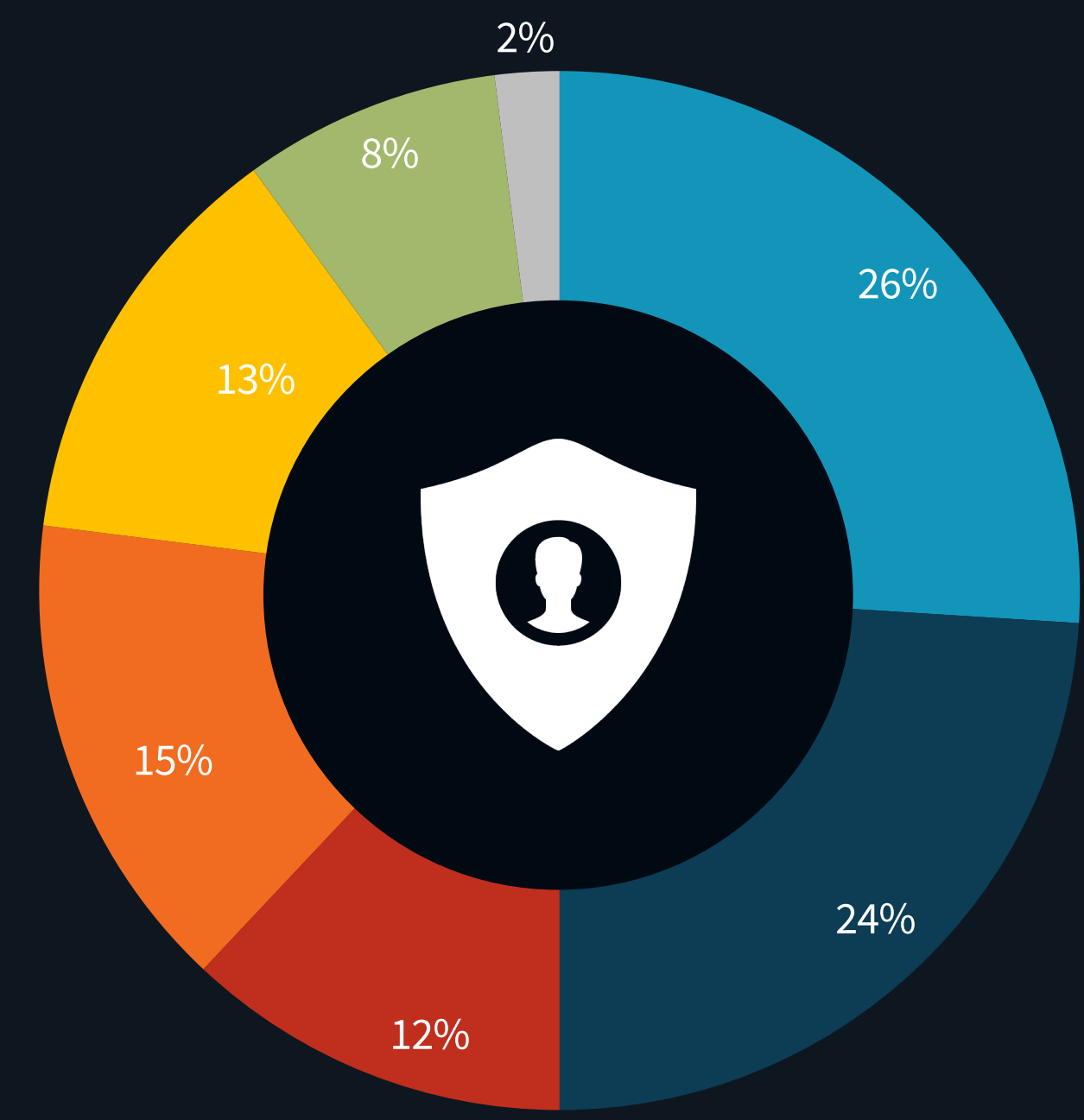
Nearly half (49%) of respondents indicate their organization is using a phishing simulation service. Organizations that consider email their top overall security priority are twice as likely (84% versus 42%) to be using a phishing simulation service.





Sender Verification Matters, but DMARC Has Challenges

While Domain-based Message Authentication, Reporting, and Conformance (DMARC) is widely known, only 26% of organizations have deployed a solution and are in full enforcement. While another 24% have deployed a solution, they are not in full enforcement, and another 13% bailed out because they couldn't see a path to full enforcement. 27% are investigating or have future plans to implement a DMARC solution.



- Yes and we are in full enforcement
- Yes, but we are not in full enforcement
- We are investigating DMARC now, but don't yet have a committed plan
- Not yet, but we are planning to implement a DMARC solution in the future
- We have experimented with DMARC but have since cancelled the initiative because we couldn't see a path to full enforcement
- I'm not familiar with DMARC
- Don't know

More than half believe that email security is in a state of transformation and plan on reevaluating all email security controls.



Nearly Two-thirds Will Reevaluate Email Security Controls

Given the current, rapidly evolving email threat landscape, 62% of organizations are planning on reevaluating their email security controls, including 57% that believe email security is going through a significant transformation. With no end in sight for phishing-based attacks, sender impersonation, and business email compromise, email security solutions must expand their scope to help organizations protect themselves from this expanding threat landscape. Nearly two-thirds (64%) of organizations plan to increase spending on email security controls in the next 12 months compared with last year's investments.

57% believe that email security is going through a significant transformation.



64%
are increasing spending

16%
Increase substantially

48%
Increase somewhat



Strengthening malware and ransomware protection join the list of top considerations.

As organizations struggle to stop phishing-based attacks, increased investment in automated phishing controls, end-user security awareness training, and encryption services lead the list of email security priorities.

Strengthening malware and ransomware protection join the list of top considerations, in addition to email encryption services to prevent the loss of sensitive information.

Migration to cloud-delivered email security tools and the consolidation of email security controls show that organizations still want to simplify controls, while the focus on email spoofing and sender verification shows that slowing down impersonation attempts is a high priority.

MOST IMPORTANT EMAIL SECURITY PRIORITIES OVER THE NEXT 12-18 MONTHS



27%

Phishing detection and prevention



22%

End-user training



22%

Email encryption services



21%

Ransomware/extortion protection



21%

Improved spam/malware filtering



Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today. Discover more at newsroom.cisco.com and follow us on Twitter at @Cisco.

LEARN MORE

About ESG



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

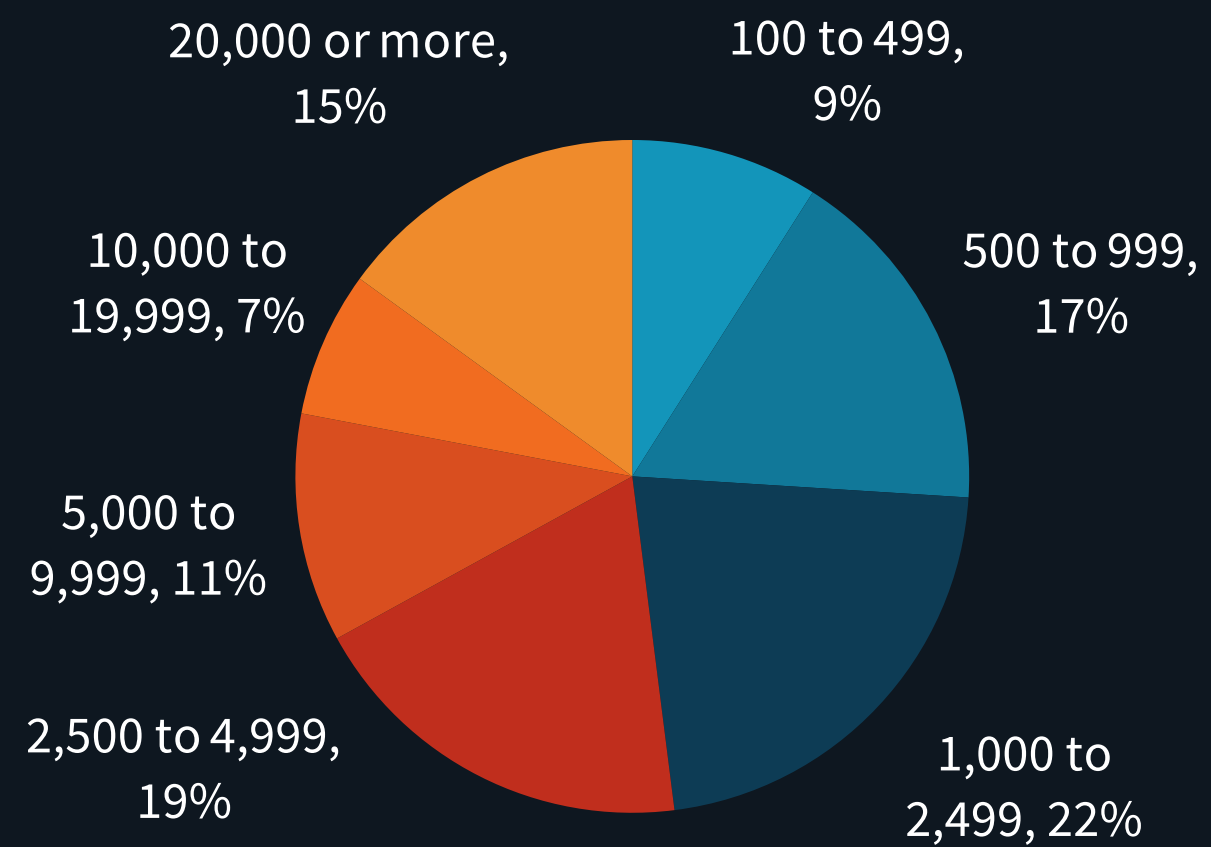


Research Methodology

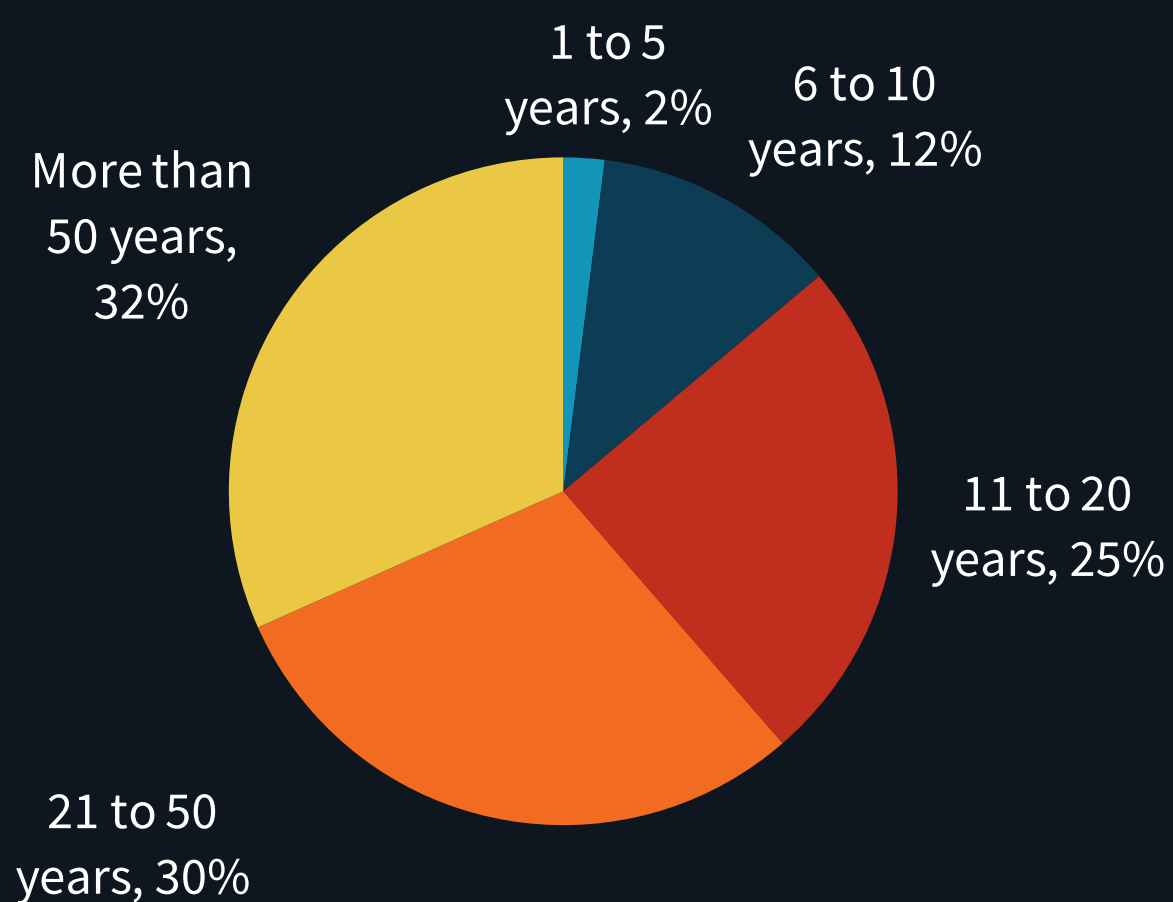
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between January 24, 2020 and February 2, 2020. To qualify for this survey, respondents were required to be IT or cybersecurity professionals personally responsible for evaluating, purchasing, and managing email security products, processes, and services. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 403 IT and cybersecurity professionals.

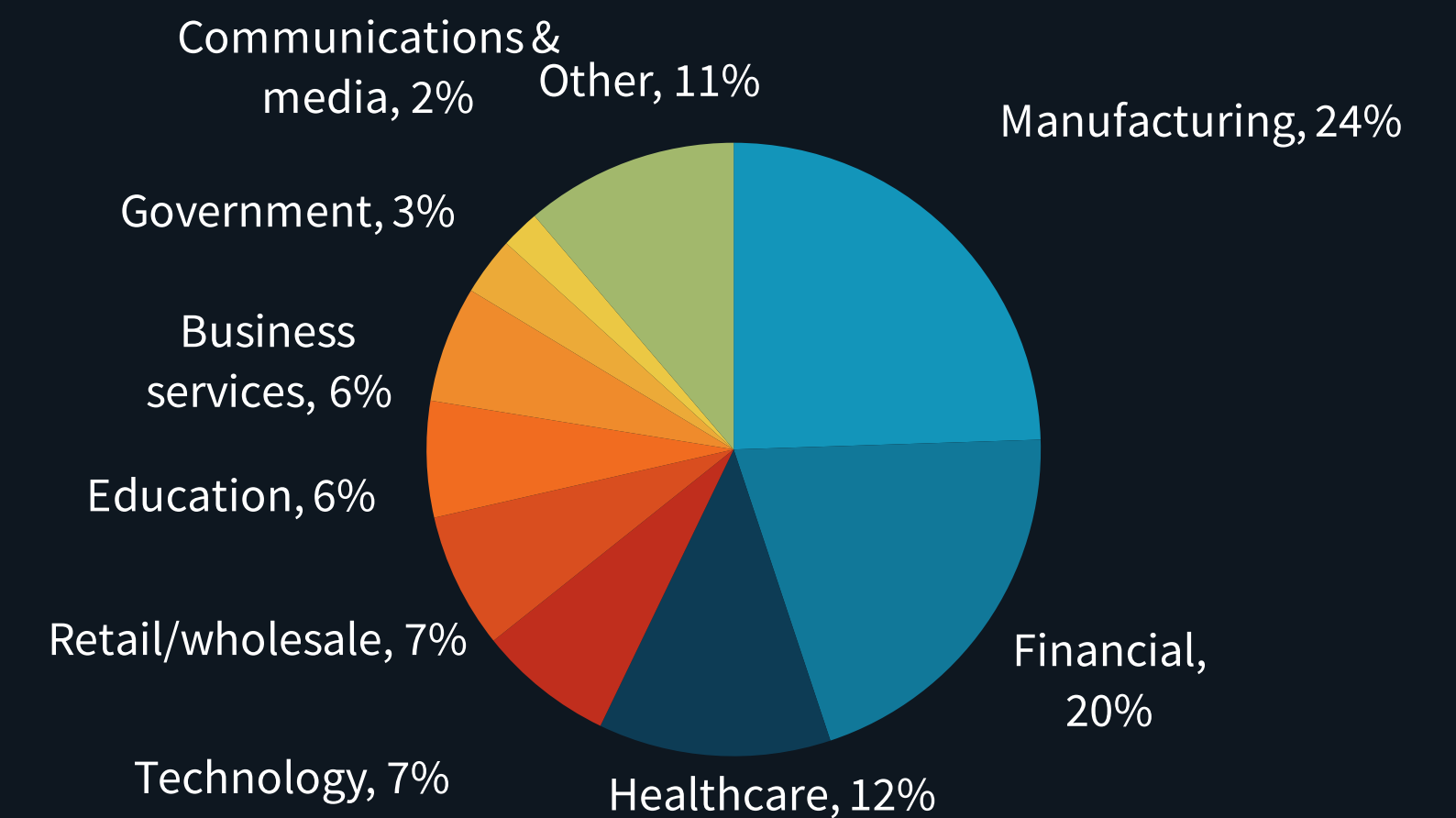
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



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 from time to time. 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 action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company



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

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.