TESSIAN

STATE OF EMAIL SECURITY 2022

Every Company's Riskiest Channel

Tessian's "State of Email Security Report 2022" examines the continued use of email across corporate environments, which is increasingly the most vulnerable threat vector for gaining initial access to corporate networks.

EXECUTIVE SUMMARY

TODAY'S CYBERSECURITY THREAT LANDSCAPE REMAINS HIGHLY DYNAMIC AND EVER EVOLVING.

In it, threat actors are attempting to access corporate networks and are leveraging novel exploits to seize a business' crown jewels, namely its data. Email remains a leading initial attack vector, and according to Tessian's latest data on the "State of Email Security 2022," that does not appear likely to change.

The issue of email as a go-to channel for threat actors is further complicated by the macroeconomic climate throughout the back-half of 2022, with fears of a looming recession altering markets and potentially headcounts moving into the next calendar year. The related stress has impacted already-stretched security teams, with chief information security officers (CISOs) working longer hours and perhaps becoming more prone to avoidable mistakes. In fact, according to our latest "**CISO Lost Hours**" survey, some 18% of security leaders are working 25 extra hours per week! Mistakes stemming from being overworked can prove dangerous, particularly if it leads to more malicious emails reaching end-user inboxes and eventually malware propagation across the network, or data exfiltration.

Our September 2022 survey of **600 information technology (IT) and security leaders worldwide** tapped into a number of these trends, and found that email – which persists as the "lifeblood" of today's organizations despite the advent of messaging programs like Slack or Microsoft Teams – has cemented its place as the sought-after entryway into the corporate network. Typically, malicious actors carry this out by baiting users with social engineering campaigns that can include impersonated pleas from trusted figures of authority or other fraudulent scams or promotions. Regardless, threat actors view the channel as one of the easiest inroads to compromising businesses. That's increasingly true amid a major shift from on-premises to cloud email security providers like Microsoft 365 and Google Workspace, as native protections on these platforms simply are not enough to match the increasing sophistication of social engineering and business email compromise (BEC) campaigns, including the growing challenge of email-delivered ransomware, among other cyber threats.

At **Tessian**, we're working tirelessly to keep organizations safe and secure by preventing advanced email threats, protecting against data loss, insider risk and building a smarter cybersecurity culture. We're guided in this effort by our annual "State of Email Security Report," which captures the true state of this high-risk attack vector. In the pages that follow, we will outline the latest data-driven trends and key findings around email threats across the enterprise.

Some of those findings include...

TESSIAN

STATE OF EMAIL SECURITY 2022

71%

71% OF SECURITY LEADERS EXPERIENCED CREDENTIAL OR ACCOUNT COMPROMISE AS A RESULT OF A SUCCESSFUL ADVANCED EMAIL ATTACK THIS YEAR

92%

92% OF ORGANIZATIONS HAVE DEALT WITH A DATA BREACH CAUSED BY AN END-USER ERROR ON EMAIL

45%

JUST UNDER HALF OF RESPONDENTS (45%) ARE USING A NEXT-GENERATION EMAIL SECURITY SOLUTION

1 IN 5

NEARLY 1 IN 5 ADVANCED EMAIL ATTACKS ARE SUCCESSFUL

X2

COMPANIES WITH >1,000 WORKERS RECEIVED TWICE AS MANY SPEAR PHISHING AND EMAIL IMPERSONATION ATTACKS THAN COMPANIES WITH 100-250 EMPLOYEES

6 IN 10

DESPITE HAVING AN EXISTING EMAIL SECURITY SOLUTION IN PLACE OR UTILIZING THE NATIVE EMAIL SECURITY CAPABILITIES OF A CLOUD PRODUCTIVITY SUITE, OVER 6 IN 10 SECURITY LEADERS (62%) SAID SPECIFIC ADVANCED THREATS BYPASSED THOSE DEFENSES

CONTENTS

PART 1

EMAIL_THE LIFEBLOOD OF THE ORGANISATION

Despite the proliferation of several messaging platforms, the communication method of choice across business settings remains email.

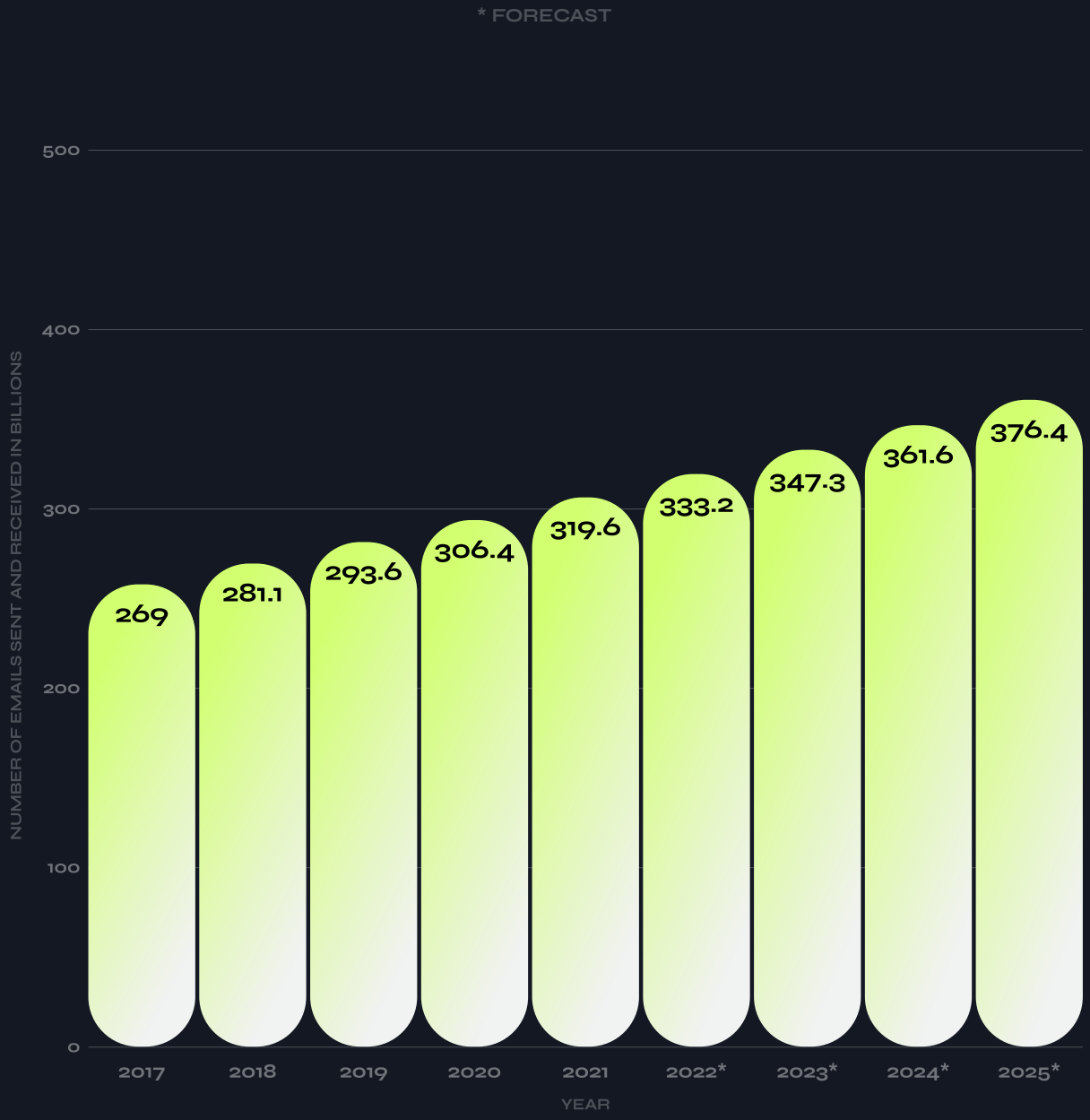
In fact, survey respondents confirmed that their organizations send and receive thousands of emails every day.

Organizations of all sizes continue to rely on this form of electronic communication, and experts predict that email volume will continue rising through 2025. In fact, the number of emails sent and received **around the world has climbed** each year since 2017 – with a whopping 319.6 billion sent or received per day in 2021. That number is expected to hover somewhere near 376.4 billion daily emails by 2025.

These towering figures, combined with the open nature of the communications tool (where messages are routed to user accounts across several different servers through an email client or a web interface), make it the number one threat vector in organizations today.

Our data acknowledges the continued and heavy reliance on email across the business, and threat actors have – for quite some time – recognized this usage and ultimate vulnerability. They often initiate phishing efforts to infiltrate and use that initial access to move deeper into a network to compromise sensitive, high-value data.

NUMBER OF SENT AND RECEIVED E-MAILS PER DAY WORLDWIDE FROM 2017 TO 2025 (IN BILLIONS)

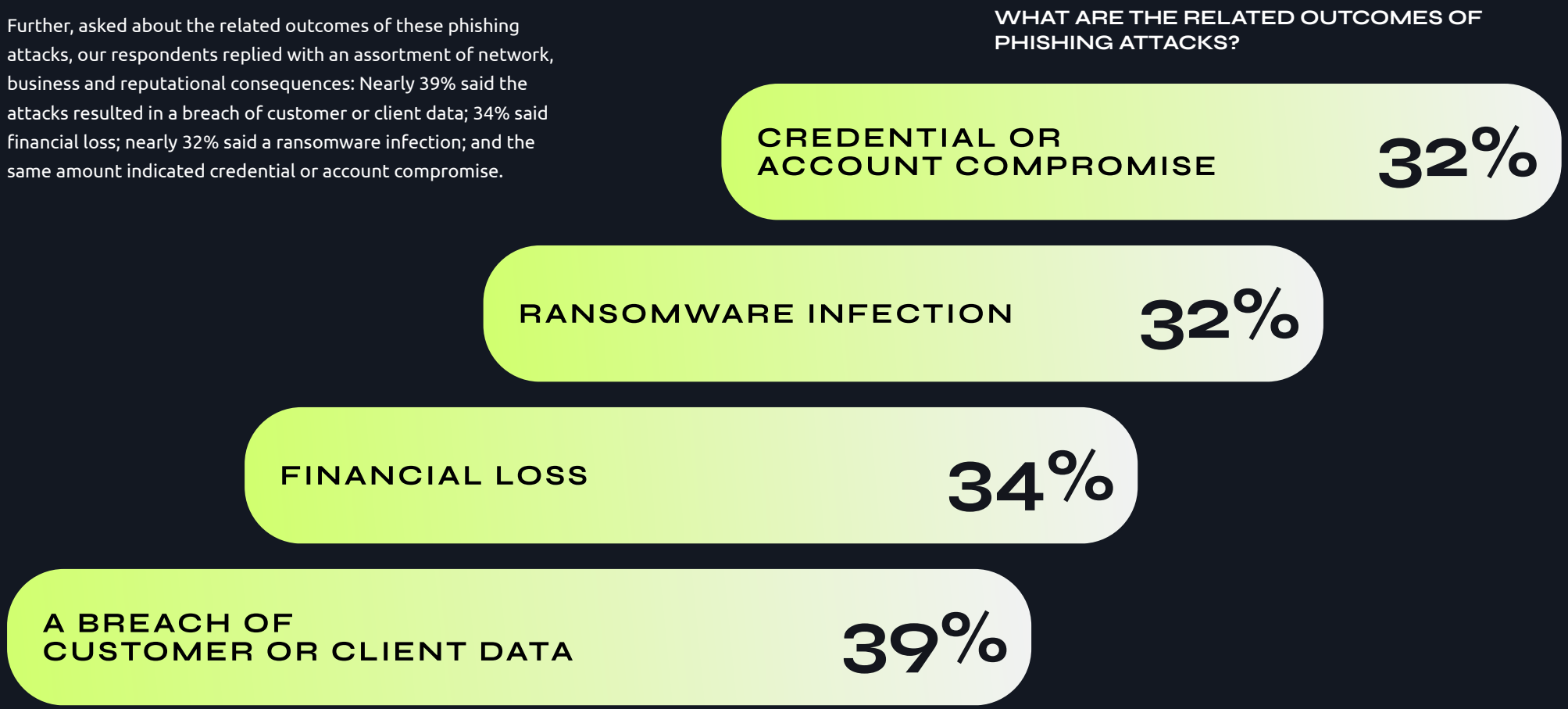


PART 2

PHISHING ATTACKS AND OUTCOMES

Due in part to its success in duping users, phishing has persisted as a threat actor's easiest means to access a network. When asked how many successful email-based phishing attacks their organizations experienced in 2022, **nearly 30% of organizations indicated experiencing 30 or more successful phishing attacks**, with the global average landing at approximately 26 successful attacks in 2022. The figures skewed a bit higher in the U.S., in particular, with 50% of those polled indicating 30 or more successful phishing attacks, with an average of 37 successful phishing attacks in 2022.

Further, asked about the related outcomes of these phishing attacks, our respondents replied with an assortment of network, business and reputational consequences: Nearly 39% said the attacks resulted in a breach of customer or client data; 34% said financial loss; nearly 32% said a ransomware infection; and the same amount indicated credential or account compromise.



PART 3

NEARLY 1 IN 5 ADVANCED EMAIL ATTACKS IS SUCCESSFUL

As email usage widely persists and enterprise teams sharpen their efforts to secure the channel and raise user awareness, adversaries are matching that defense by targeting specific enterprise users.

This is occurring largely through spear-phishing, or the practice of sending targeted messages (ostensibly from a known or trusted sender) that urges users to click malicious links, share sensitive data or to comply with a request (for example, paying a fraudulent invoice).

In fact, our survey found that 94% of organizations experienced a spear-phishing or impersonation attack in 2022. That figure rises to 99% in the U.S.

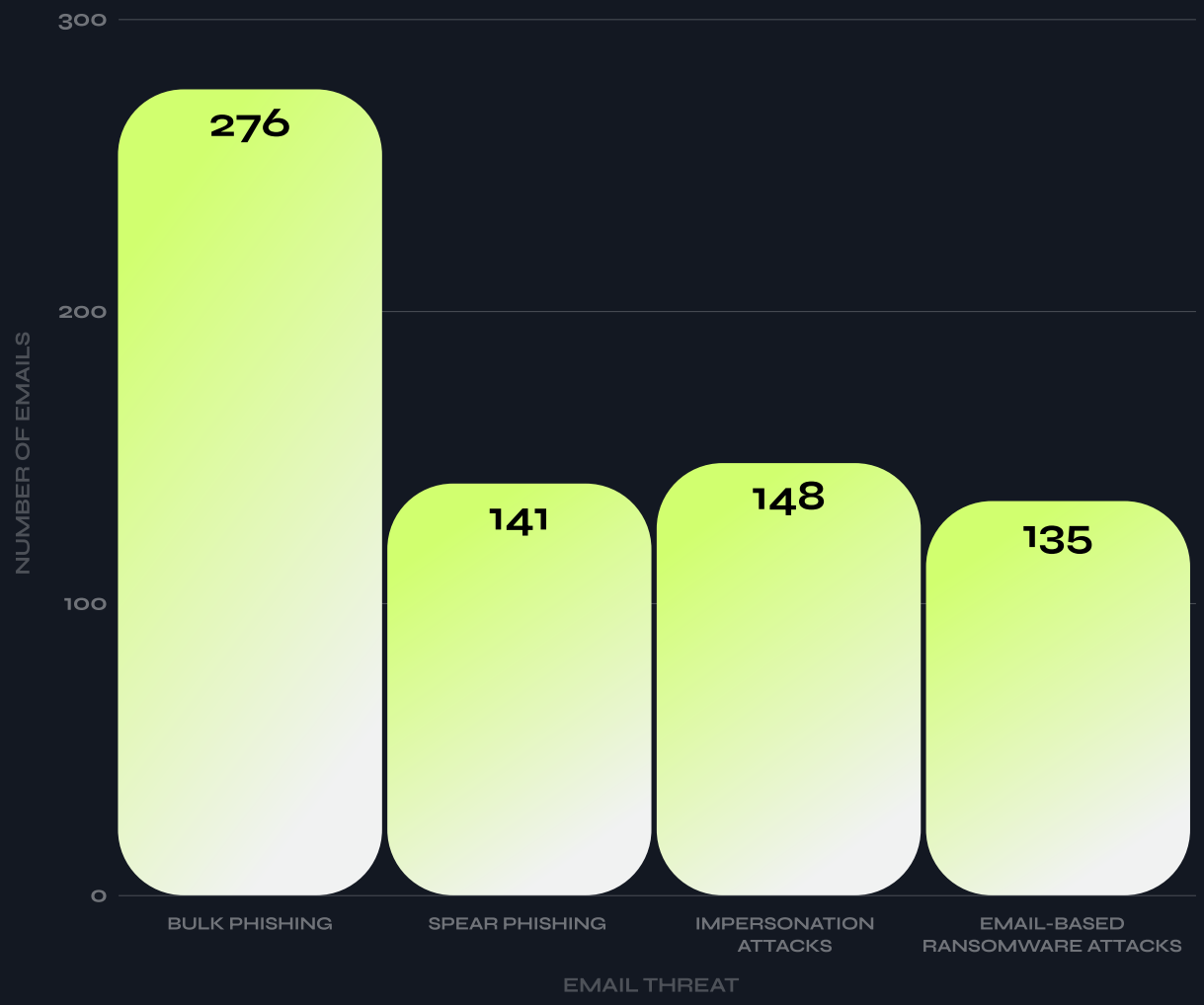
Additionally, on average, 1 in 5 advanced email attacks received were successful (18%).

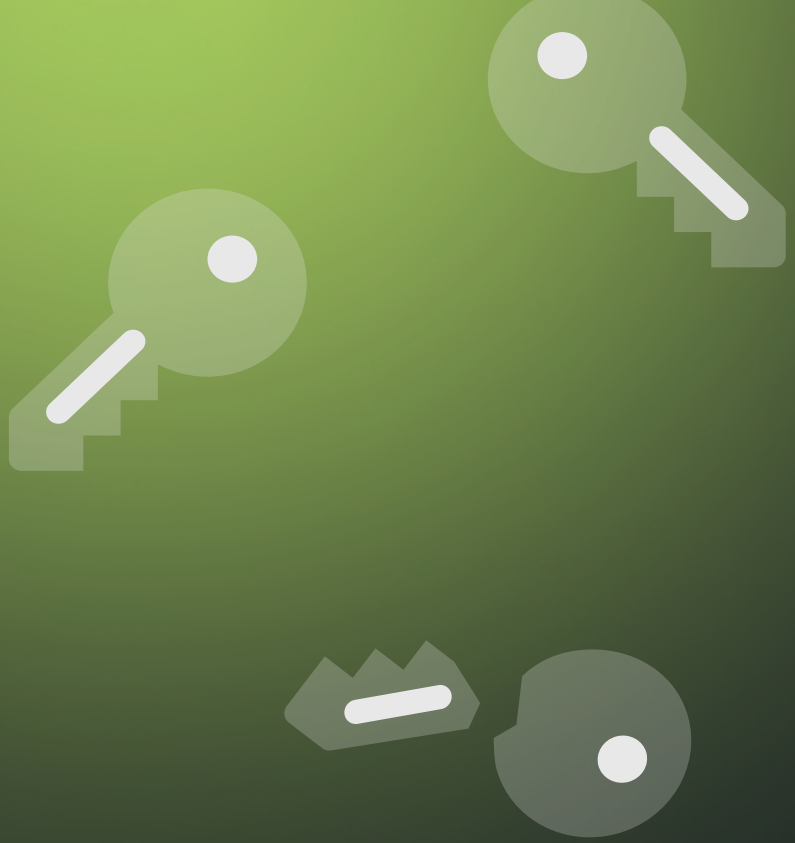
Indeed, impersonation attacks – which consist of attempts to impersonate authoritative and trusted figures known to a user – topped the list of the most common types of "advanced email attack" experienced by global organizations through the first nine months of 2022 (not counting bulk phishing to dupe larger sets of users). Such attacks also ranked as the top email threat that security leaders are most concerned about, followed by ransomware and account takeover.

Security practitioners reported an average of 148 impersonation attacks in 2022, followed by 141 spear-phishing attacks, and 135 email-based ransomware attacks. Just over 1 in 10 global organizations received significantly high volumes of advanced email attacks in 2022 as well; 11% received over 450 spear-phishing and 12% received over 450 impersonation attacks.

What's more, 92% of global organizations experienced at least one email-based ransomware attack in 2022, with 10% of the security leaders surveyed saying they received over 450 email-based ransomware attacks since January 2022.

AVERAGE NO. OF EMAILS THREATS EXPERIENCED BY GLOBAL ORGANIZATIONS IN 2022





PART 4

KEYS TO THE KINGDOM, COMPROMISED?

The prospect of financial loss and wider breaches of customer data certainly keep today's network defenders up at night.

That is particularly true as adversaries' attempts to cloak their activities have achieved new levels of believability. In fact, the U.K.'s National Cyber Security Centre (NCSC), its central cybersecurity agency, has acknowledged the difficulty in properly identifying these threats, saying: "Spotting phishing emails is hard, and spear phishing is even harder to detect. Even experts from the NCSC struggle."

Following initial compromise, adversarial activity may quickly amplify, too: 71% percent of surveyed practitioners said they have experienced credential or account compromise (aka Account Takeover or ATO) related to successful advanced email attacks in 2022.

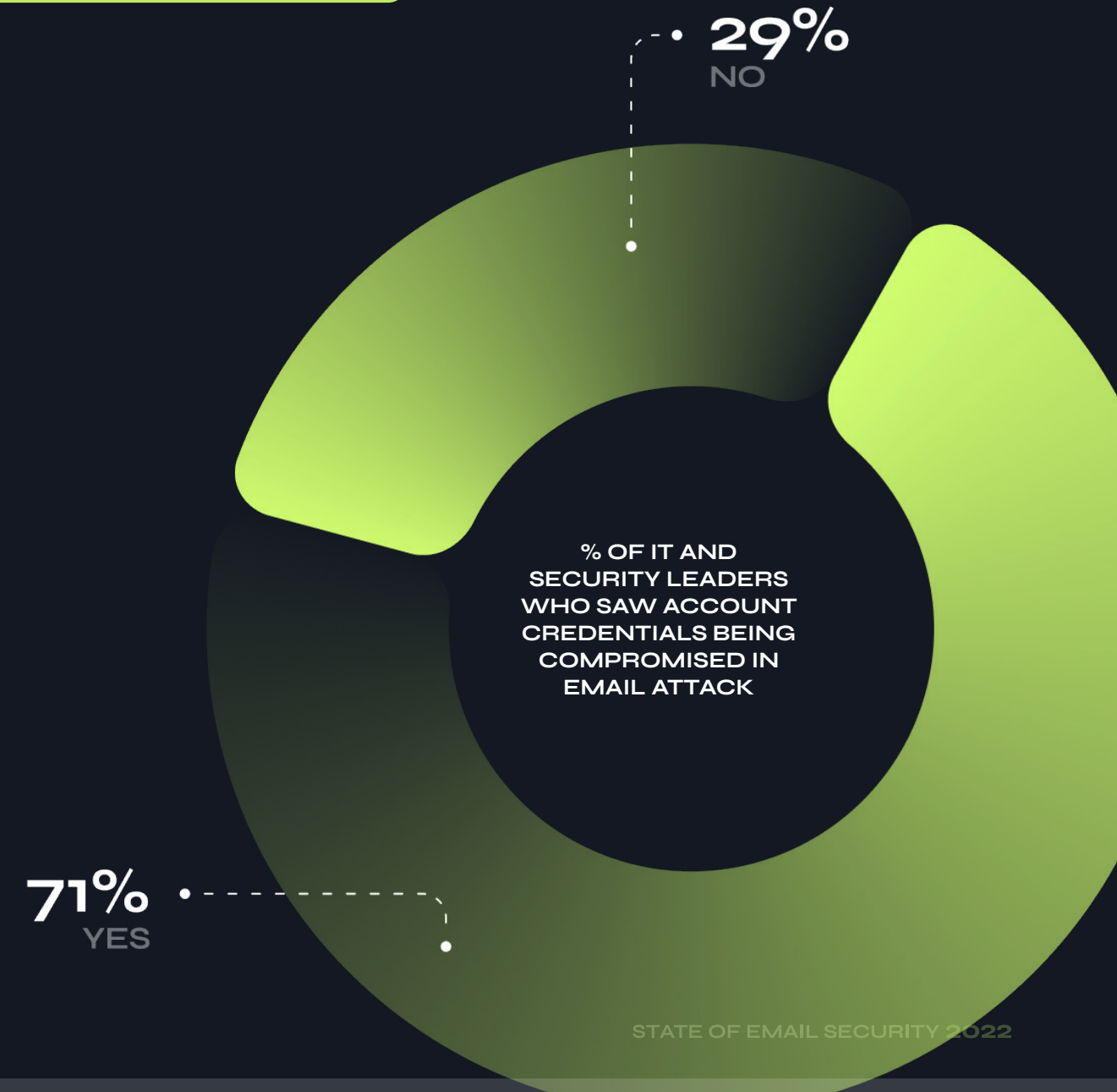
When a threat actor acquires legitimate login credentials, they can leverage those credentials to levy more attacks – by compromising an end-user's account and posing as the identity of the end-user. Oftentimes, the modus operandi of an ATO attack is an attempt to later steal money or sensitive data stored on-premises or in cloud workspaces.

It remains incredibly difficult for the recipient of a malicious impersonation email to determine whether they are receiving an email from a cybercriminal or their trusted connection. Today, employees may see comparable efforts with threat actors posing as CEOs, managers, third-party vendors, or other trusted, internal sources. Again, these are often efforts to simply hijack user accounts and pick through the corporate network.

While the NCSC notes that "advice given in many [security] training packages, based on standard warnings and signs, will help users spot some phishing emails," these, too, are not a cure-all.

What is Account Takeover and why is it a threat?

READ MORE →



PART 5

FAR TOO MANY THREATS BYPASSING TRADITIONAL DEFENSES

Today, although a majority of businesses have a rule-based email security solution in place, like a Secure Email Gateway (SEG), advanced email threats are continuing to bypass legacy defenses and reach end-user inboxes.

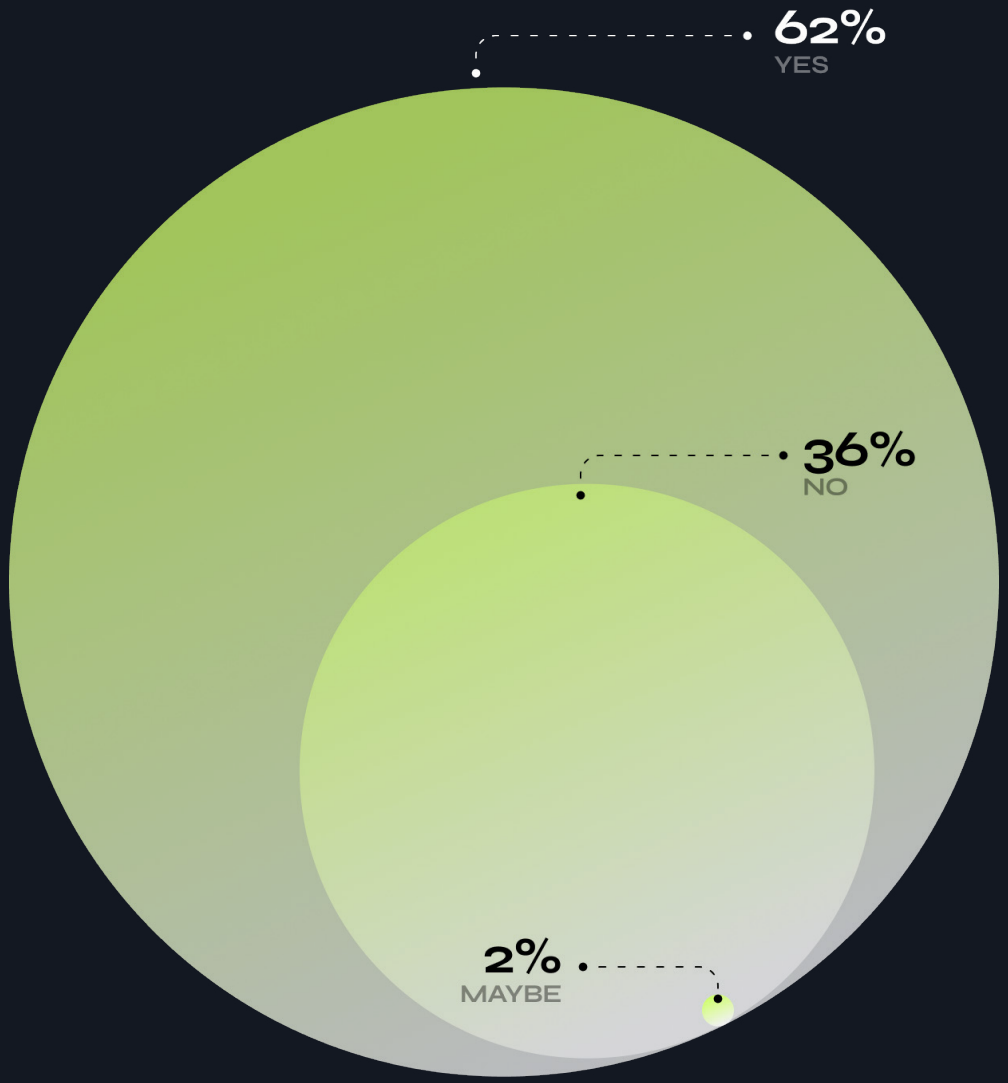
In fact, while scores of organizations employ SEG solutions, sophisticated threat actors are sidestepping these controls with increasingly advanced social engineering-based attacks. That's also true of those employing native security tools from cloud providers such as Microsoft or Google.

Over 6 in 10 security leaders (62%) whose organizations have a SEG in place noted that advanced email threats bypassed those defenses in 2022, reaching end-users inboxes. That figure rises to 75% in the U.S. This could help explain why 63% of respondents say they find it challenging to demonstrate the return on investment (ROI) of their current email security tools.

Why Legacy Secure Email Gateways Are No Match for Today's Cyber Threats

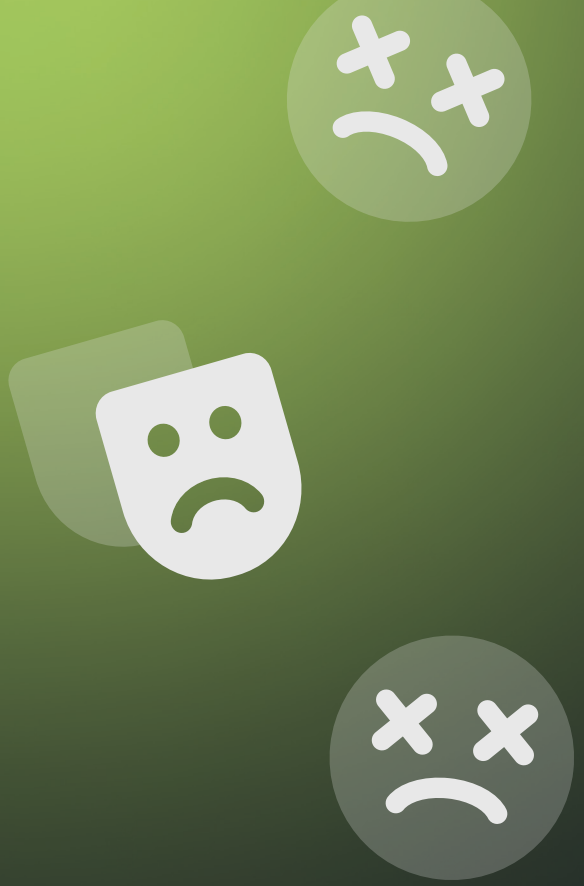
READ MORE →

% OF IT AND SECURITY LEADERS WHO SAY ADVANCED EMAIL THREATS HAVE BYPASSED SEGS IN 2022



“CYBERCRIMINALS ARE PULLING OUT ALL THE STOPS TO BREACH CORPORATE EMAIL ACCOUNTS, AND THEY’RE BYPASSING TRADITIONAL DEFENSES TO DO SO. WE NEED TO STAY SERIOUS ABOUT EMAIL SECURITY – AND PART OF THAT INVOLVES DEPLOYING NEXT-GEN, AI-POWERED TOOLS TO MAKE THREAT DETECTION BOTH FASTER AND MORE ACCURATE.”

JOSH YAVOR
CHIEF INFORMATION SECURITY OFFICER AT TESSIAN



PART 6

IMPERSONATION ATTACKS_WHAT YOU NEED TO KNOW

“THERE ARE SEVERAL CORE PRINCIPLES OF INFLUENCE AND ONE OF THEM IS SOCIAL PROOF. A STRONGER VERSION OF SOCIAL PROOF IS ONE THAT INVOKES AUTHORITY. AS HUMANS, WE ARE DEFERENTIAL TO AUTHORITY SO IF OUR DEFAULT IS TO ‘DO WHAT THE BOSS SAYS’, AND A CYBERCRIMINAL IMPERSONATES A SENIOR EXECUTIVE AT THE COMPANY, IT INCREASES THE PROBABILITY THAT THE ATTACK WILL WORK.”

JEFF HANCOCK
PROFESSOR AT STANFORD UNIVERSITY

With email attacks growing more sophisticated and leveraged for things like delivering malware payloads or even network reconnaissance ahead of more crippling ransomware campaigns, experts see it often rooted in human error leading to that dreaded initial access.

When asked who threat actors were impersonating in their malicious emails, more than one-third of IT and security leaders (37%) indicated fellow employees. The goal of course: tricking end-users within the organization to leak private or sensitive information, including log-in credentials that can lead to ATO.

Other responses here were actually quite similar, as fellow employees were closely followed by the impersonation of vendors (32%) and C-level executives (31%).

PART 7

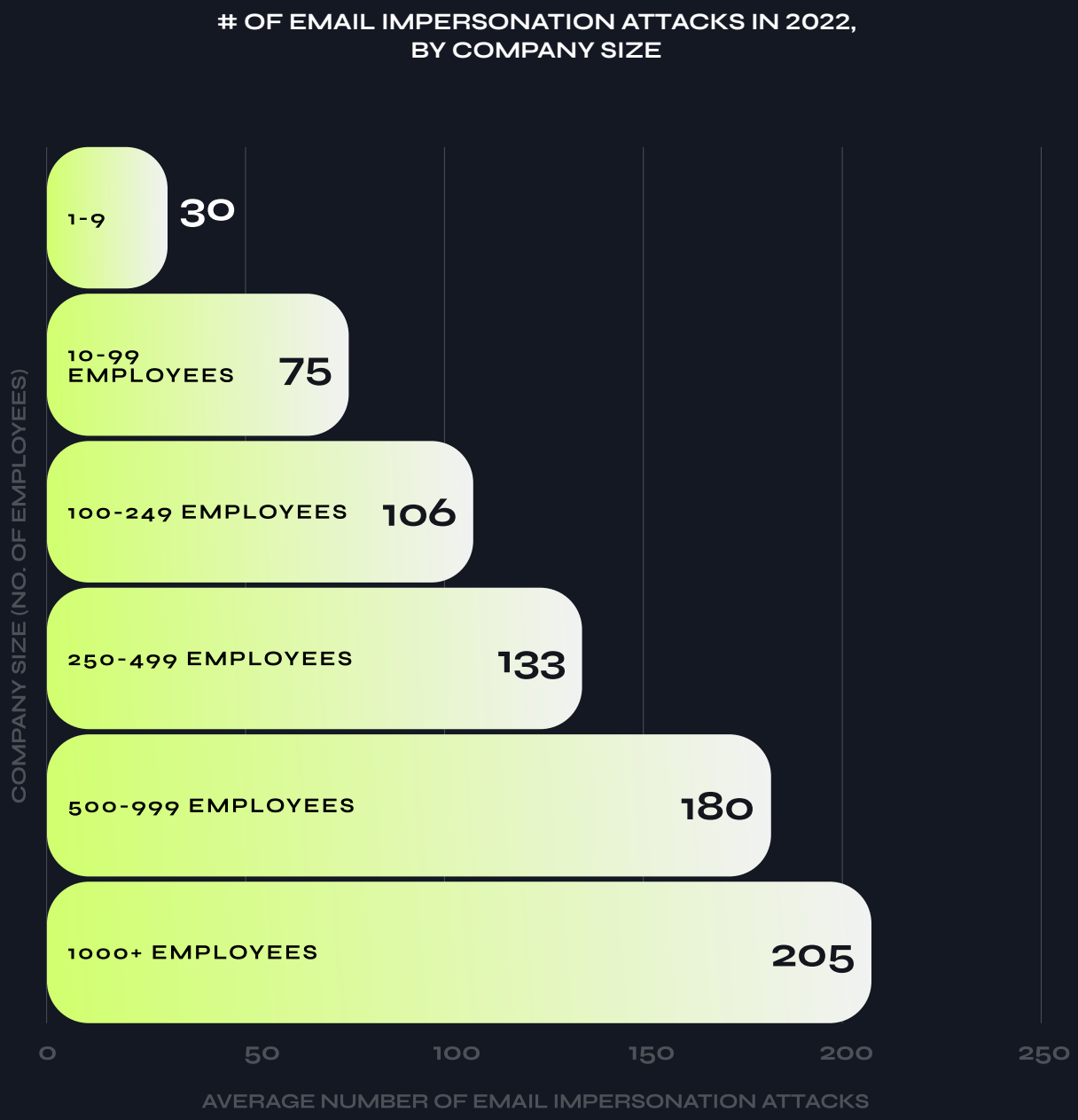
THE BIGGER THE COMPANY, THE MORE EMAIL THREATS RECEIVED

Unsurprisingly, respondents from larger companies indicated that their organizations see incrementally more threats.

On average, companies with more than 1,000 workers received twice as many spear-phishing and email impersonation attacks than companies with 100-250 employees, and three times more than companies with under 100 employees.

Smaller companies – those with under 250 employees – were most likely to receive email attacks from threat actors impersonating board members and investors. This no doubt reflects how cybercriminals tailor their scams to make them more believable, given that most companies of this size will likely be startups.

In larger organizations, users were more likely to receive impersonation emails from threat actors pretending to be employees or company vendors.



PART 8

INSIDER THREATS LEAVE SECURITY LEADERS EXPOSED

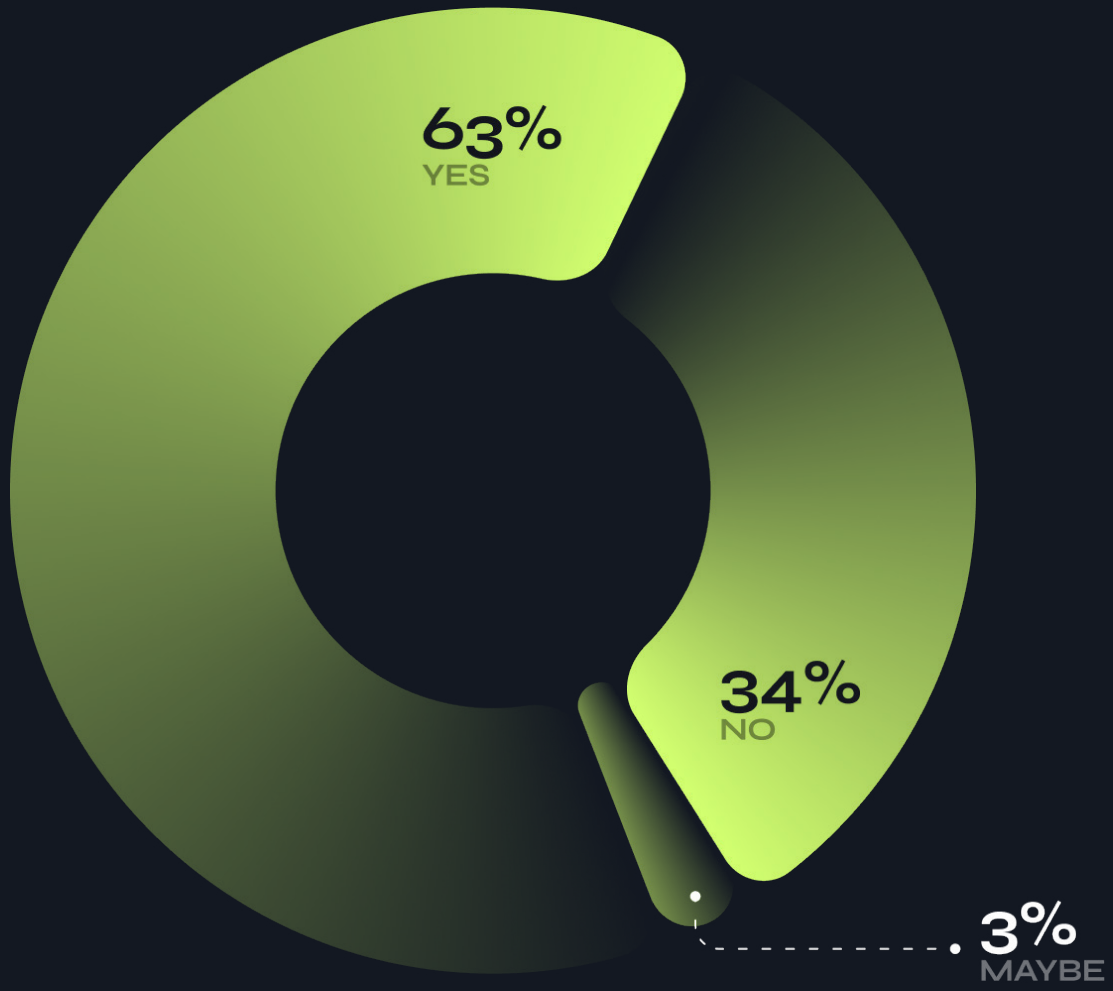
Despite the many advanced email threats that could jeopardize corporate environments, another threat remains: **THE INSIDER.**

Viewed as the other side of the coin of email security risk, insider threats can manifest in a multitude of ways. And as we have shown in The Ponemon Institute Report on Email Data Loss , email remains the riskiest channel for data loss. For example, it could be a disgruntled employee that exfiltrated data via email prior to resigning or departing an organization, or negligence on the part of the employee – perhaps sending corporate data to unauthorized recipients, including their own freemail domains. Threat actors that have already gained access to the corporate network via an ATO or other compromise also pose the risk of readily exfiltrating sensitive data via email.

Nearly two-thirds of security leaders (63%) indicated that their staff exfiltrated data over email in some form in 2022, while 9 out of 10 (92%) companies experienced a data breach caused by an end-user mistake on email. That includes sending an email to the wrong person or failing to send the correct attachment to the recipient. As noted, there can also be the case of malicious insiders (i.e., disgruntled employees or threat actors) as well, with many of these types of incidents often only detected months after the transgression.

The big challenge surrounding conventional approaches to data loss prevention (DLP) until recently has been the limitations and retroactive nature of legacy approaches to DLP. In fact, some security leaders are not entirely confident in their existing visibility into the data leaving their organizations: An average of 5% of those polled rated their visibility as “Poor.” In the U.K., specifically, nearly 11% of the IT and security leaders responded the same way, with nearly 3% even calling their email-based data visibility “Very Poor.”

% OF SECURITY LEADERS WHO HAVE SEEN END-USERS EXFILTRATING DATA OVER EMAIL IN 2022



This means defenders have to deploy intelligent email security that is able to detect and prevent both malicious and accidental data loss events – bringing much needed visibility to the email environment and having the ability to prevent data loss attempts from becoming security incidents.

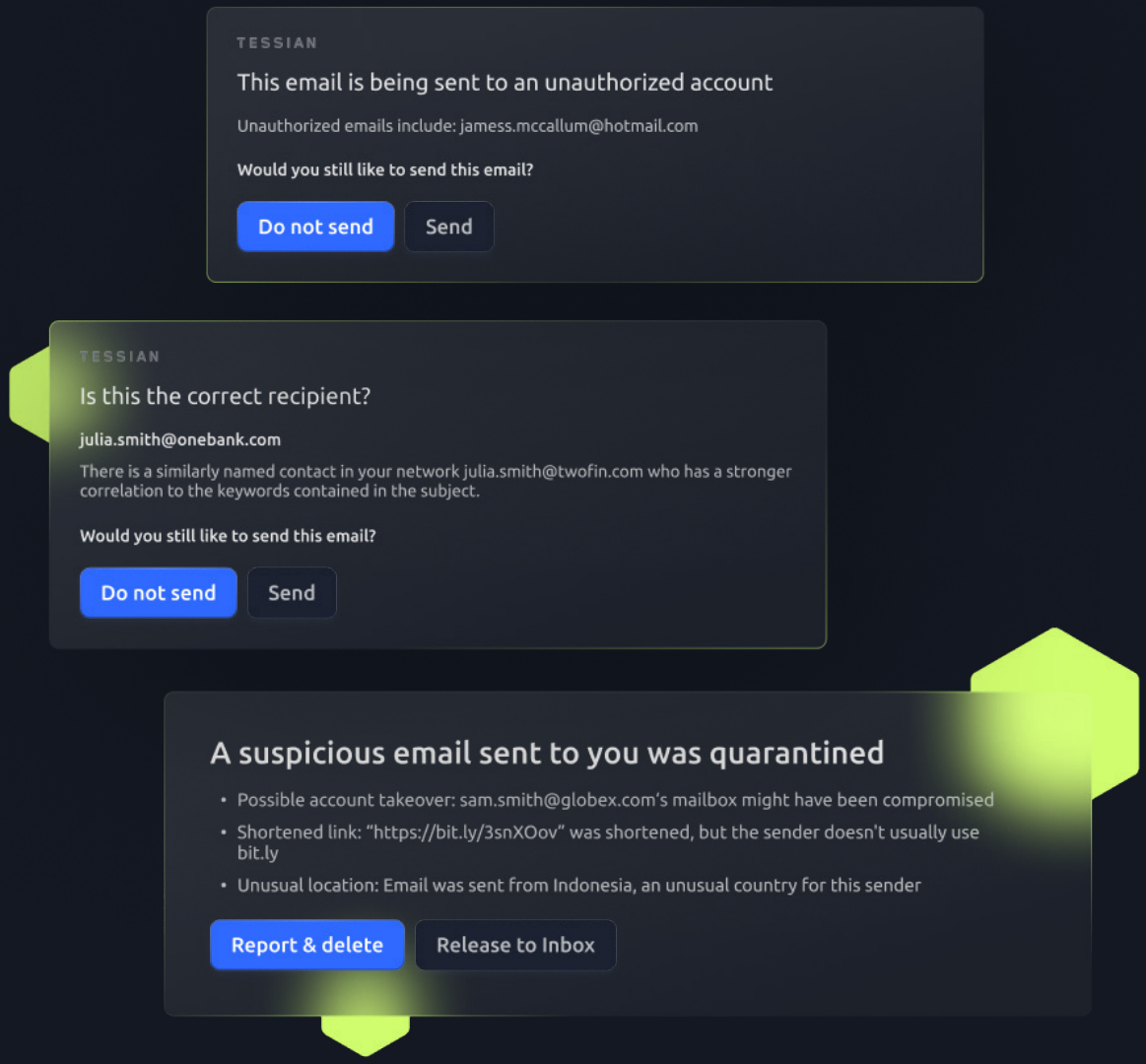
In the wrong hands, sensitive data can be exceedingly harmful, regardless of how it was leaked – resulting in account compromise and giving threat actors network access.

For reference, nearly 1 in 5 companies (16%) dealt with over 50 data breaches caused by users' errors on email in 2022 alone.

In addition to adopting intelligent email security solutions that bring a greater degree of visibility and control to security teams, it is imperative that these tools also include an element of end-user security awareness training. For example, one approach is to enable end-users to "do the right thing" by prompting them with an in-the-moment security banner when they're about to send an email to an unauthorized or unintended recipient. Not only is the end result a stronger security culture but also a significantly reduced insider risk footprint.

Conventional approaches to user training (both ongoing and for onboarding) also have a place but need to be used responsibly and in a considered way. For example, training and intentional phish-tests to the user base have proven, in some environments, to be too punitive (e.g., the sense of shaming or feeling penalized). So, it bears repeating that even the best training – neatly embedded into the company's operations – cannot be a silver bullet.

These proactive efforts will curb the problem, but it won't prevent mistakes from happening altogether. Instead, security leaders need to bolster training with technology that detects and prevents an assortment of threats in-the-moment.



PART 9

USING AUTOMATION TO MITIGATE EMAIL THREATS

Nearly every respondent to our September 2022 survey (that is, 99.5%) recognized that artificial intelligence (AI) and machine learning (ML) can enhance and improve their email security. These next-generation capabilities boost the efficacy of today's security solutions, providing supplemental user and message-based context and round-the-clock analysis beyond the abilities of human defenders.

The number one benefit of leveraging both AI and ML cited by IT and security leaders was: faster threat detection (66%), closely followed by more accurate threat detection (56%).

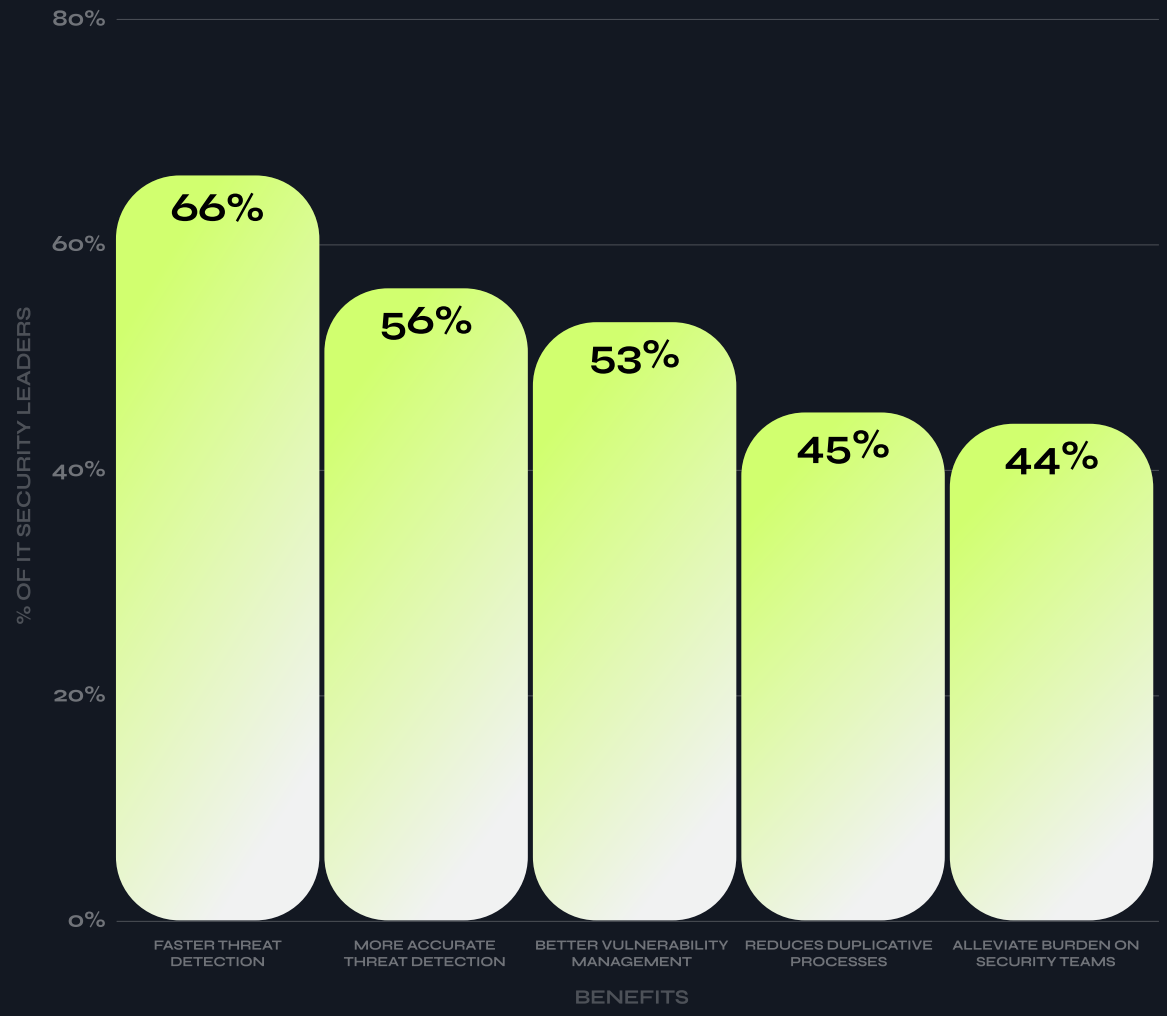
With limited bandwidth, already overstretched security teams are often left to manage the entirety of the aforementioned (and very consequential) threat landscape in addition to other security responsibilities.

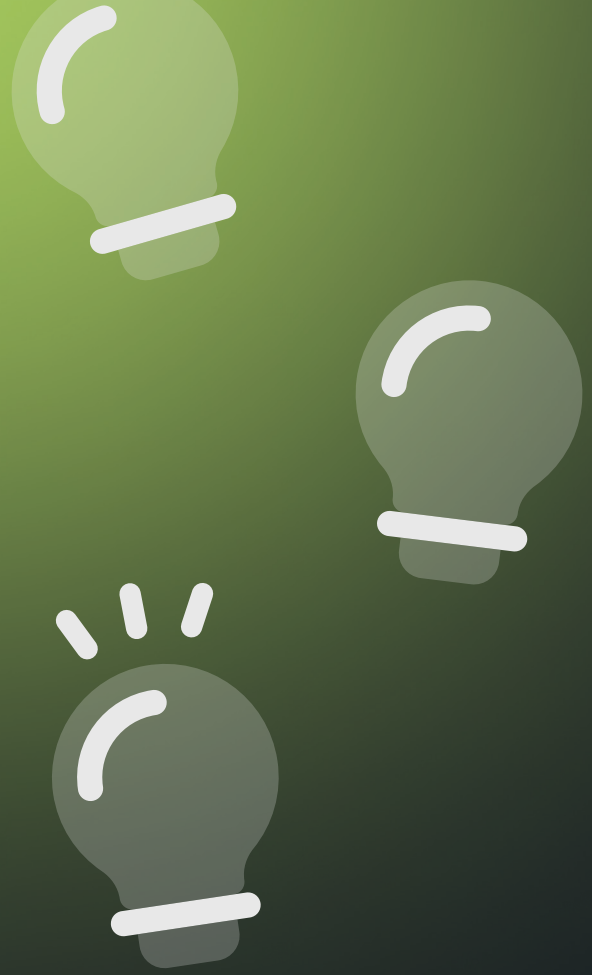
Our surveyzfinds that security personnel are working an average of 17 hours more than their contracted hours per week. As such, questions are arising over security teams' ability to cover all their bases and protect their organizations against a growing cyber threatscape while avoiding burnout. However, both AI and ML capabilities in email security tools appear to show a light at the end of the tunnel:

44% OF RESPONDENTS NOTED THAT AUTOMATED APPROACHES TO EMAIL SECURITY COULD ALLEVIATE ADMINISTRATIVE BURDENS ON THEIR ALREADY STRETCHED SECURITY TEAMS.

Despite recognizing the benefits of adopting ML intelligent email security technology to protect against email threats, just under half of respondents (45%) say they are using a next-generation email security solution that leverages AI or ML.

RECOGNIZED BENEFITS OF USING AI OR MACHINE LEARNING IN EMAIL SECURITY





CONCLUSION

THE FUTURE STATE OF EMAIL SECURITY

WHAT'S NEXT?

While email continues to be a go-to channel for bad actors with all sorts of motivations, cybersecurity defenders are getting more effective in their efforts to stand-up defenses and keep their organizations secure.

Recall that while 62% of respondents saw threat actors bypass traditional email security defenses in their attempts to zero in on sensitive data, our team at Tessian remains confident that by leveraging behavioral-based email security, we can significantly reduce your risk of an email-related breach.

Moving forward, more and more companies will move to the cloud (67% of enterprise infrastructure is now cloud-based), and even more users will become reliant on digital channels to share data with customers, colleagues and vendors. That means the threat of data loss on email increases.

What's more, there is no doubt that social engineering attacks will persist and continue to evolve. In fact, the Anti-Phishing Working Group (APWG), an international consortium that aims to eliminate fraud and identity theft carried out via web-based phishing, observed 1,097,811 total phishing attacks in the second quarter of 2022 alone, marking a new record (2022 was also the first year the group observed quarterly figures north of 1 million attacks).

We expect the threat to intensify across email, too, with increasingly deceptive messages forced into end-user inboxes that may result in perpetrating fraud, or delivering a malware payload, resulting in a system compromise. We predict that more threat actors will evade legacy, rule-based corporate email security measures by targeting end users relentlessly. After all, it takes just one click to compromise an information system.

Concerted efforts to defend against this evolving threatscape include training the user base – with tailored security awareness training programs. Still, this won't be enough in itself; teams must use intelligent email security solutions that are able to detect and prevent threats using a behavioral-based approach as they arise – providing advanced and "always-on" security. In addition to the advanced protection, innovative solutions like Tessian also coach end-users towards safer behavior with in-the-moment security alerts, strengthening security culture.

This must be at the core of the enterprise security response, if businesses are to tackle this dynamic threat.

TESSIAN

Tessian is a leading cloud email security platform that intelligently protects organizations against advanced threats and data loss on email, while coaching people about security threats in-the-moment. Using machine learning and behavioral data science, Tessian automatically stops threats that evade legacy Secure Email Gateways, including advanced phishing attacks, business email compromise, accidental data loss and insider threats. Tessian's intelligent approach not only strengthens email security but also builds smarter security cultures in the modern enterprise.

TESSIAN.COM

Learn more about Tessian.

Email is the lifeblood of the enterprise, but the most vulnerable channel.
Discover how Tessian's Intelligent Cloud Email Security Platform can keep your company's sensitive data safe and increase customer trust while saving you time and money.

Calculate Savings

More insights, every week.

Subscribe to our newsletter to get more insights straight to your inbox.

- Helpful resources and
- shareable guides
- Tips for CISOs
- Early access to our latest research

Subscribe

SHARE THE REPORT

METHODOLOGY

In September 2022, Tessian commissioned third-party research house Censuswide to survey 600 IT and security leaders in organizations across the U.S., U.K., Middle East and Africa. The survey has a margin of error of +/-4%.