GreatHorn

February 2021

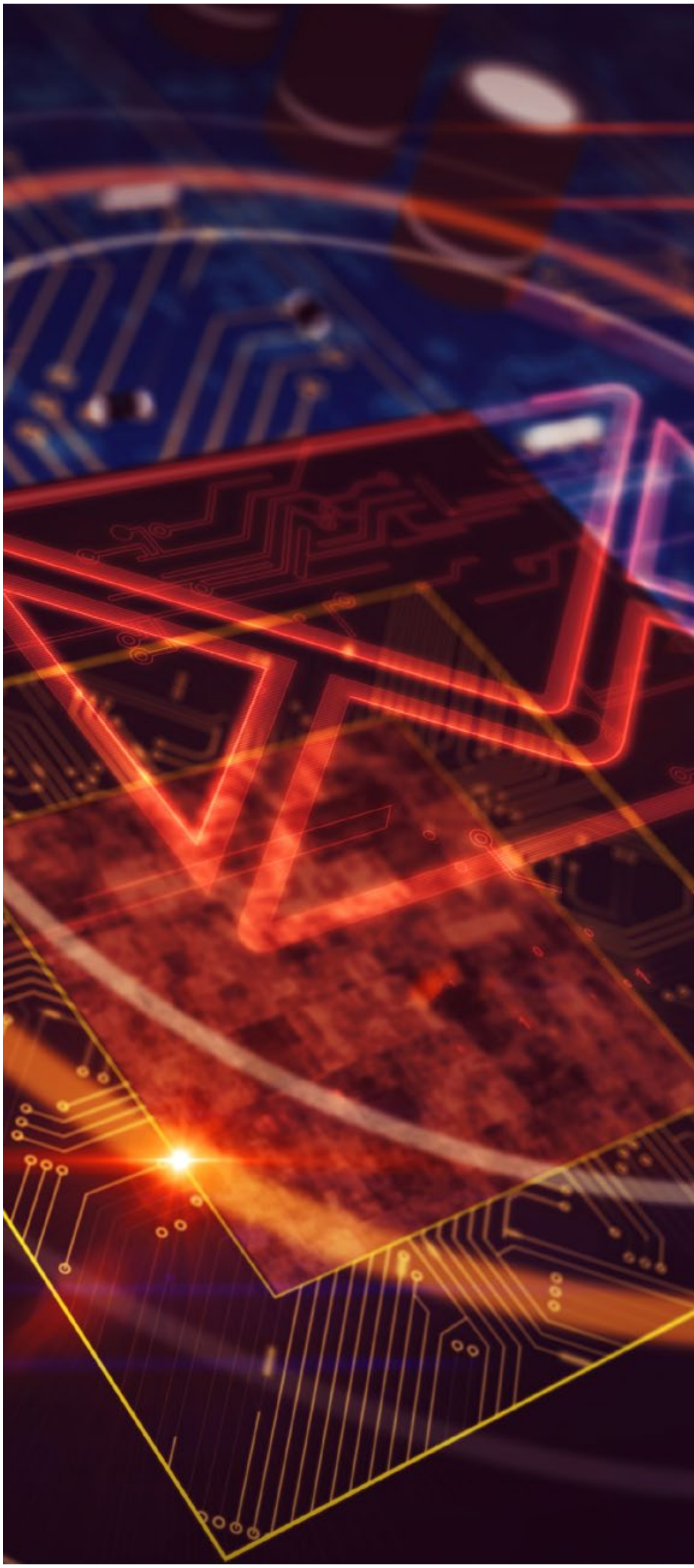
4TH ANNUAL SURVEY REPORT

2021 EMAIL SECURITY BENCHMARK REPORT

INTRODUCTION

For the past four years, the GreatHorn Threat Intelligence team surveys several hundred people across various businesses and industries who manage email security within their organization. This survey allows us to gather new insights and research into new and emerging email security threat vectors, new strategies for combating attacks, and various issues that are impacting the email security space at large.

We compared the 2021 survey results to the 2020 survey results, highlighting some primary trends and key emerging perspectives among professionals and executives on the front lines who are fighting email attacks each year. Survey responses were collected in the first two weeks of January 2021.



EXECUTIVE SUMMARY

2021 data shows that attacks leveraging email as the attack vector are here to stay. With the impact of the COVID-19 pandemic, the election year, remote work and many other changes, the impact of email-based threats are increasing.

Key findings include:

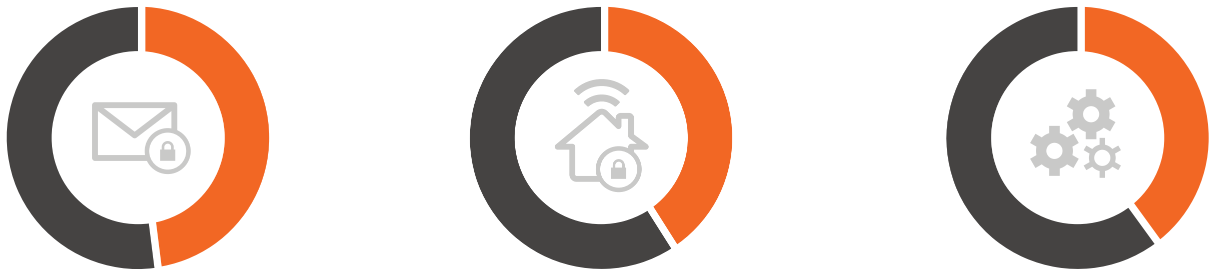
- **Email security ranked first in the list of top IT security projects of 2021.**
  - Email security (48%), securing telework (41%) and cloud security posture management (40%) are the top 3 security projects for 2021.
- **Business-related applications are the most frequently seen impersonation attempts across users.**
  - Business-related applications (Zoom, Microsoft, DocuSign) account for 45% of impersonation-related phishing attacks, much more than social media-related applications (Facebook, LinkedIn, Twitter) at 34% or consumer-related applications (Amazon, PayPal) at 20%.
- **While daily occurrences of phishing attacks decreased, weekly and monthly occurrences have increased significantly.**
  - Though daily occurrences of phishing attacks have decreased from 36% to 25% between 2020 and 2021, weekly and monthly phishing attacks have increased from 28% to 42% and 11% to 17%, respectively, supporting evidence that cybercriminals are becoming more sophisticated and targeted in their attacks.
- **A disconnect in the approach to email security leads to missing phishing attacks.**
  - Missing phishing attacks remains the top issue in current email security solutions with 39% of respondents noting this as a top concern in both 2020 and 2021.
- **Weekly and monthly remediation of phishing attacks on the rise.**
  - While the need to remediate phishing attacks daily has decreased from 34% to 18% YoY, weekly and monthly occurrences have increased weekly from 28% to 41% on average and monthly from 11% to 16%.
- **Challenging the Status Quo**
  - Fewer organizations report being “satisfied” with their current email security solution, decreasing from 76% in 2020 to 53% in 2021.

WHAT ARE THE TOP IT SECURITY CONCERNS FOR 2021?

Without a doubt, email continues to be a chosen method of attack for cybercriminals. Not only is it simple to deploy but email itself is vulnerable to cybercriminals' development of attacks and cannot be completely locked down as a critical form of business communication. IT and cybersecurity professionals and their teams are in a continuous cycle of detection and remediation, struggling to mitigate risks across the organization.

While there is a clear increase in phishing attacks, there is also a greater awareness among security professionals that email security remains an area for improvement.

IT and security respondents identified the top three security projects in 2021, including:



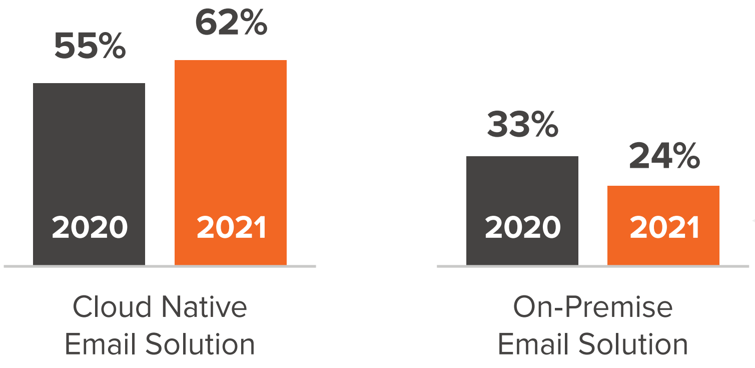
48% Email security

41% Securing telework

40% Cloud security posture management

The Current Email Security Landscape Heading into 2021

Organizations are continuing their migration from on-premise email solutions to cloud native solutions. While 24% of organizations are still running on-premise email solutions, 77% have plans to move to cloud native email solutions.



77%

Plan to move to cloud native email

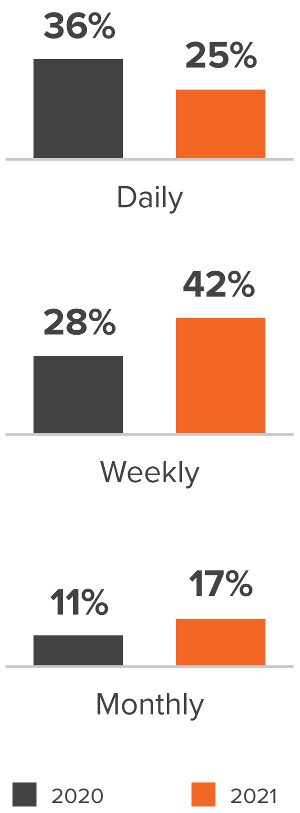
A Reduction in Quantity, in Lieu of Quality, Phishing Attacks

Phishing attacks have become more sophisticated, utilizing several inherent vulnerabilities in email to increase success. Though daily occurrences of phishing attacks have decreased from 36% to 25% between 2020 and 2021, weekly and monthly phishing attacks have increased from 28% to 42% and 11% to 17%, respectively.

What is causing this trend? The GreatHorn Threat Intelligence Team has analyzed billions of emails and assess the trends occurring throughout phishing attacks. The firsthand perspective of this overarching analysis aligns with those IT security professionals at individual organizations, whereby there is a reduction in daily occurrences of phishing attacks, but a dramatic increase in more sophisticated attacks that target specific users within organizations. These attacks are also increasingly difficult to detect, as they bypass standard volumetric detection models.

Cybercriminals have moved from the "batch and blast" methodology, previously used by marketers in the early days, trending towards the highly tuned, socially engineered phishing campaigns. As a result, the quantity of phish being experienced by organizations may have dropped daily, but the impact of those campaigns that bypass traditional email security is increasing.

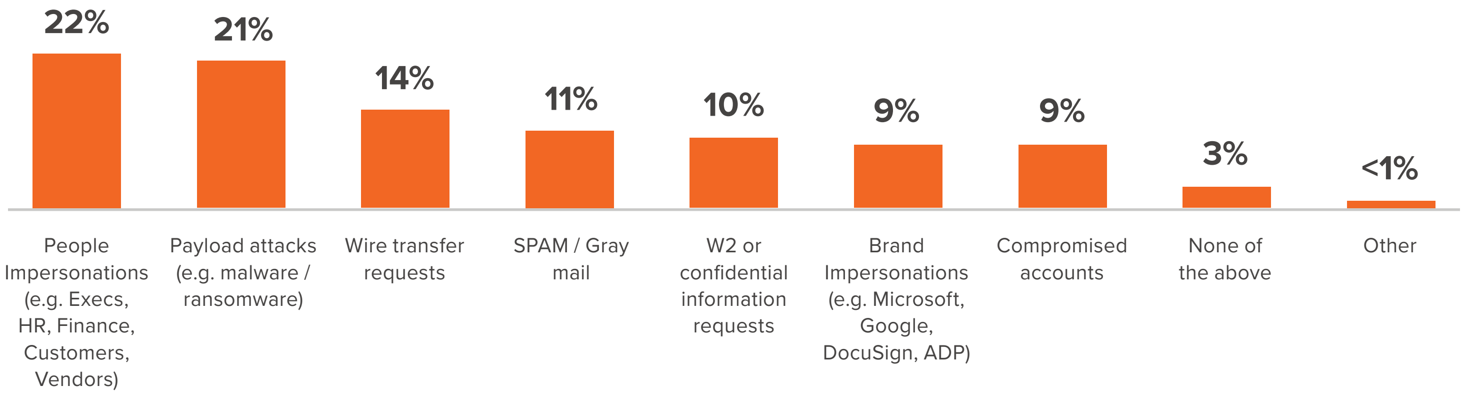
Daily occurences of phishing attacks



Top Threats in Phishing Attacks

Organizations are still experiencing a high volume and wide variety of phishing attacks, the top threat that is still most concerning for IT professionals are people impersonations (e.g., from executives, finance, customers, and vendors) remaining at 22% in 2021.

Which email threat worries you the most?



Impersonating individuals is a prolific technique that is becoming more successful with cybercriminals. As employees leverage social media networks, including LinkedIn, and employers expand their digital presence to attract customers, more information is available for social engineering. And being able to impersonate a trusted entity to get the user to act allows the phishing campaign to be more successful.

For IT professionals, having an email security solution that can immediately detect anomalous activities and educate the end user immediately is important to mitigating risk. An end user will not always look beyond the Sender Name to identify that the email alias or domain being sent from are not from the usual source, forcing the user to take extra precautions before acting with the email.

These three phishing threats are in line with what organizations should be concerned about. You do not have to look far to see how phishing campaigns leveraging payload attacks often contain ransomware. The risk associated with this type of attack can cause detrimental financial and brand damage.

Again, with wire transfer requests, a user is usually tricked into transferring substantial amounts of money to the cybercriminal. In many of these, cybercriminals have used social engineering to better understand the people involved across the organization and are using impersonations to achieve greater success.

Compromised accounts are starting to become a more important threat for IT professionals. Over the past year, cybercriminals have capitalized on the remote workforce using Microsoft, SharePoint, Google, and other major application login pages as part of their phishing campaigns. Because employees have changed their behaviors and often need to use their credentials more often throughout the day, an additional login (though using an impersonated URL) is not uncommon.

With these credential harvesting attacks, we are now seeing more account takeover attacks. Once the users' credentials have been compromised, it is often quite difficult for IT professionals to uncover. However, this is one area where there is newer technology that can prevent account takeovers from occurring by using biometric authentication.

Though brand impersonations rated #5 on the list of top threats that concern IT professionals (9%), business-related applications are the most frequently seen impersonation attempts across users. Phishing attacks that use impersonations of business-related applications were 45%, much more than social media-related applications (34%) or consumer-related (20%).

The subsequent top three threats that concern IT professions

Payload attacks

16% → **21%**
2020 2021

SEND $$$

Wire Transfer requests

8% → **14%**
2020 2021

Compromised accounts

8% → **10%**
2020 2021

Examples of applications provided to respondents

Business-related applications:

Microsoft

DocuSign

zoom

Social Media-related applications:

facebook

TikTok

Consumer-related applications:

PayPal

amazon

FedEx

It is rare for a phishing campaign to just use one technique. Typically, cybercriminals have a multi-pronged attack that utilizes multiple vulnerabilities within email including: a URL to click, an attachment to download, and an impersonation of a person or brand. Having advanced threat detection, including relationship analytics and additional layers to detect account takeovers, is important for IT security professionals to protect against these top threats.

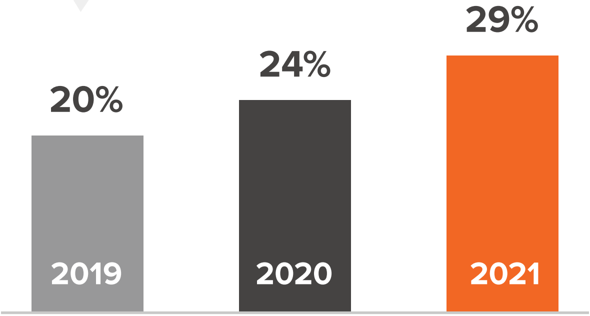
Weekly and Monthly Remediation of Phishing Attacks on the Rise

While the need to remediate phishing attacks daily has decreased from 34% to 17% YoY, weekly and monthly occurrences have increased: weekly from 28% to 41% on average and monthly from 11% to 16%.

Like the quantity of phishing attacks being experienced by organizations, the need to remediate phishing attacks every day has decreased from 34% to 17% YoY, while weekly and monthly remediation has increase 25% to 30% and 14% to 21%, respectively.

These sophisticated phishing attacks are bypassing traditional email security solutions and increasing the remediation requirements of IT professionals. With many solutions, remediation often includes resetting or suspending compromised accounts and applications, running PowerShell scripts, and manually going through the entire environment to locate other users who could have been impacted. Given that email security is one of the top 3 projects for 2021, remediation tools to allow security teams to become more efficient is a requirement.

Remediating phishing attacks on a weekly basis have continued to rise



One of the top challenges that organizations are having with their existing email security solution is also the remediation being manual/non-existent/takes too long, rising slightly from 18% to 19% YoY. Organizations with the appropriate email security tools should be able to granularly search any data field across the entire email envelope to identify all users impacted, then immediately eliminate the phish and subsequently discover any users who may have acted with the email.

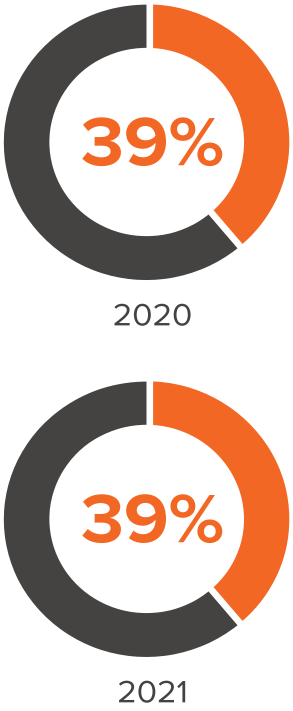
IT professionals and leaders could reduce the time to detect and time to respond or remediate attacks by ensuring a multi-layered defense to email security is put in place. While it is impossible to prevent all attacks, it is possible to get better at detection, quarantining illegitimate emails, and improving user awareness to aid in email risk mitigation.

The Disconnect: Email Security and Missed Attacks

Missing phishing attacks remains the top issue in current email security solutions (at 39% for both 2020 and 2021). Unfortunately, IT security professionals should consider a different approach. The “Catch” vs “Didn’t Catch” approach is not the most effective for email security. There is no vendor that can “catch” 100% of all phishing attacks. Instead, organizations should be looking at deviations from the norm. Is this email unusual in any way and what automated process should be put in place? Many organizations want to “catch” phish and quarantine them. Of course, this is important, but it will only address 0.2% of known bad emails. What about the other 1.8% of unusual email that could pose risk?

Having additional control mechanisms outside of quarantining is important for effective email security posture. Respondents also stated that false positives are negatively impacting their business operations, increasing slightly from 18% to 20% YoY. Thinking about having layered controls such as customized banners, link protection, and user reported phish buttons can provide a better balance for business operations.

Missing phishing attacks remains consistent

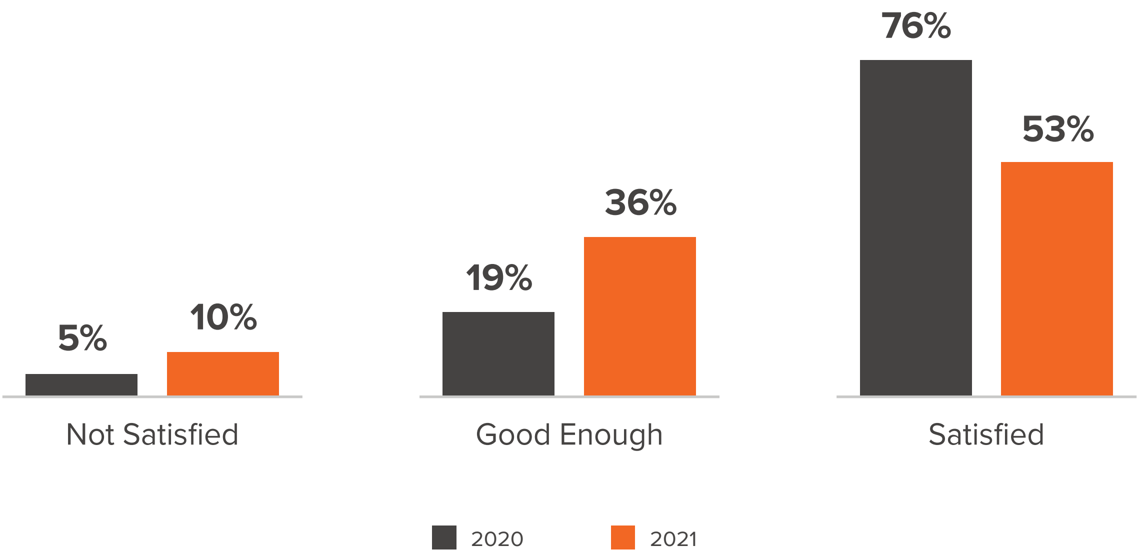


Challenging the Status Quo

Fewer organizations report being “satisfied” with their current email security solution, decreasing from 76% in 2020 to 53% in 2021.

As an industry, email security has made a lot of promises, but little has been delivered in terms of complete security and prevention protocols.

How satisfied are you with your email security solution?



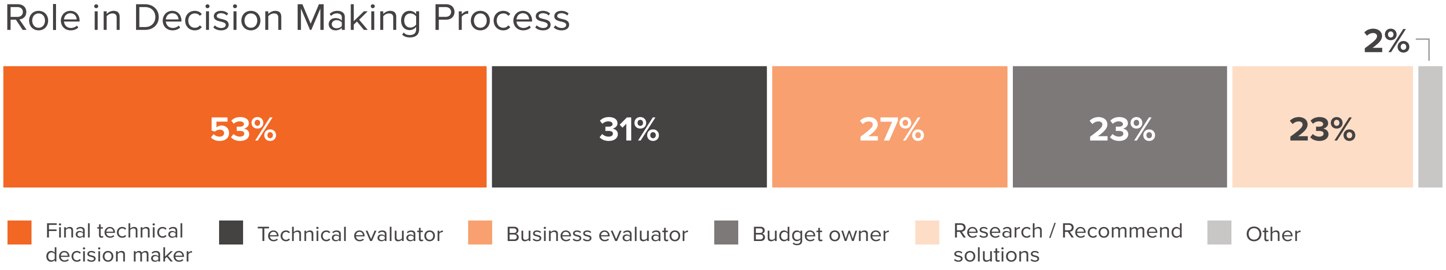
Based on the continued shift year-over-year in satisfaction levels by organizations, it is no doubt a tipping point when email security has become one of the top 3 IT security projects for 2021. And organizations are now beginning to invest in alternatives to traditional approaches.

Even though more companies have settled for good enough solutions, email will remain a top threat vector to compromise organizations. IT security professionals must begin to shift their focus and reevaluate the status quo. What most organizations should consider is a best-of-breed solution that offers a layered approach to mitigating risk versus a one-size-fits-all approach. While no vendor can prevent 100% of all phishing attacks, email security has drastically changed to adapt to the current sophisticated attacks.

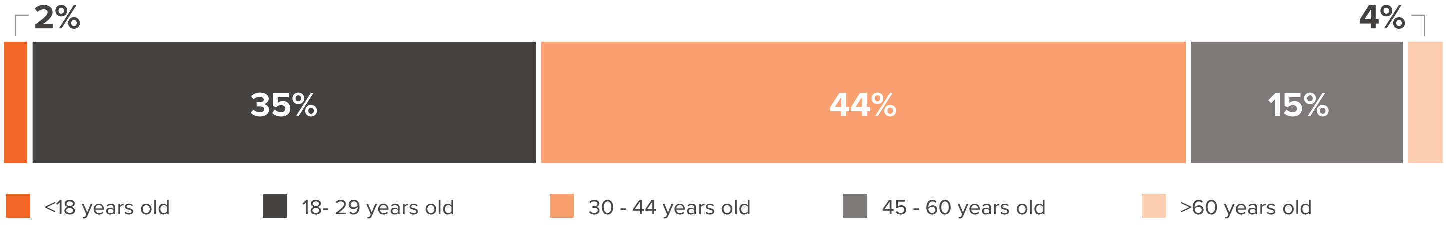
SURVEY METHODOLOGY

This year we received responses from over 588 participants working across a diverse set of roles within the information technology security market segment. The respondents hold various roles in IT as well as in the C-suite, making decisions about tools and technologies. The results of this report identify not only the challenges, but also the changes companies have encountered in the past year and the email threats that remain present today.

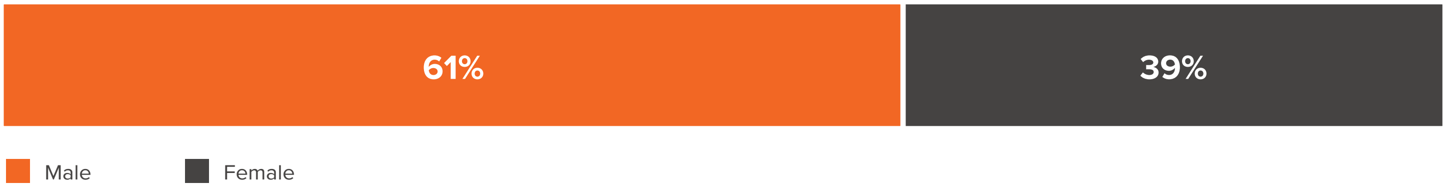
Role in Decision Making Process



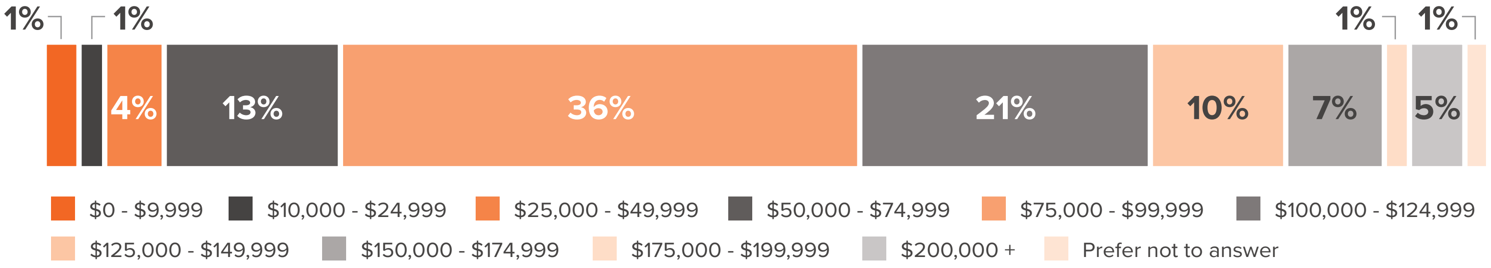
Age



Gender



Household Income



About GreatHorn

GreatHorn protects organizations from more advanced threats than any other email security platform. By combining its highly sophisticated threat detection engine with accessible user context tools and integrated incident response capabilities, GreatHorn Email Security shields businesses from both sophisticated phishing attacks and fast moving zero-day threats, freeing security teams from the tedium of email security management while enabling them to respond to genuine threats faster than ever before.

By combining deep relationship analytics with continuously evolving user and organizational profiling, GreatHorn's cloud-native email security platform provides adaptive, anomaly-based threat detection that secures email from malware, ransomware, executive impersonations, credential theft attempts, business services spoofing, and other social engineering-based phishing attacks.

GreatHorn