GreatHorn

REPORT

2018 EMAIL SECURITY:

TRENDS, CHALLENGES, AND BENCHMARKS

A look at differences based on organization size, professional role, and email

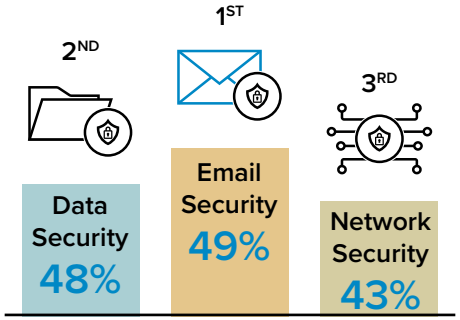
TABLE OF CONTENT

INTRODUCTION

In an effort to understand the current state of email security in terms of environments, threat prevalence, remediation frequency, and importance within the wider security landscape, GreatHorn conducted a survey of 295 professionals, mostly (but not all) in IT roles, across a wide variety of industries. Collected in June 2018 through both online and offline sources, the data provides a unique window into the state of email security today.

The panel's diversity (panel details can be found at the end of this report) enabled us to explore how different characteristics (level of involvement in email security, company size, email platform, etc.) correlated into drastically different – and in some cases, surprisingly similar – trends.

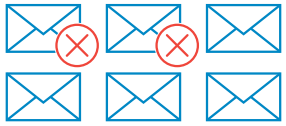
Top three security priorities



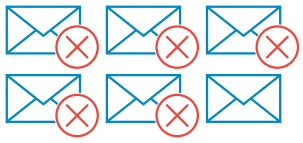
Source: GreatHorn "2018 Email Security Benchmark"

Who sees email threats in their inboxes?

33.9%
Lay people



84.5%
Email security professionals



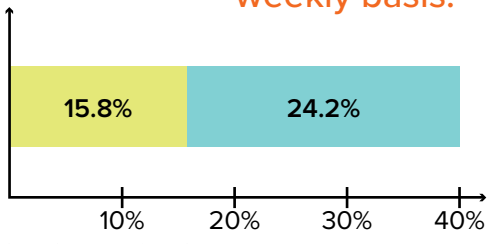
Source: GreatHorn "2018 Email Security Benchmark"

For example, we learned that email security, data security, and network security were almost universally the top three security priorities, regardless of organization size or role, with identity & access management a close fourth. But we also learned that two-thirds of people with limited or no involvement in email security say they don't see anything but spam in their inbox, while only 15.5 percent of people that do have email security involvement say the same – a staggering difference.

Keep reading to learn more about our findings and how your organization compares to our sample group.

THREAT FREQUENCY

40% see email threats in inboxes on a weekly basis.



Source: GreatHorn "2018 Email Security Benchmark"

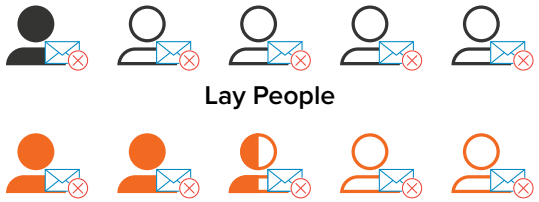
daily email threats weekly email threats

On average, an organization has three security products in place to combat email threats.

Let's start with some simple benchmarking data. Across our entire sample size, 15.8 percent of all respondents indicated that – despite whatever email security measures they have in place – they or their users see email threats (categorized as impersonations, wire transfer requests, W2 requests, payload attacks / malware, business services spoofing, or credential theft) on a daily basis, with an additional 24.2 percent seeing threats weekly – a total of 40 percent seeing email threats at least weekly.

When we separate our sample into people who are involved in some way in email security decisions ("email security professionals", representing 61 percent of our panel) from those who have limited or no involvement ("laypeople", representing 39 percent of our panel), we find a stark difference in how frequently the respondents reported seeing email threats.

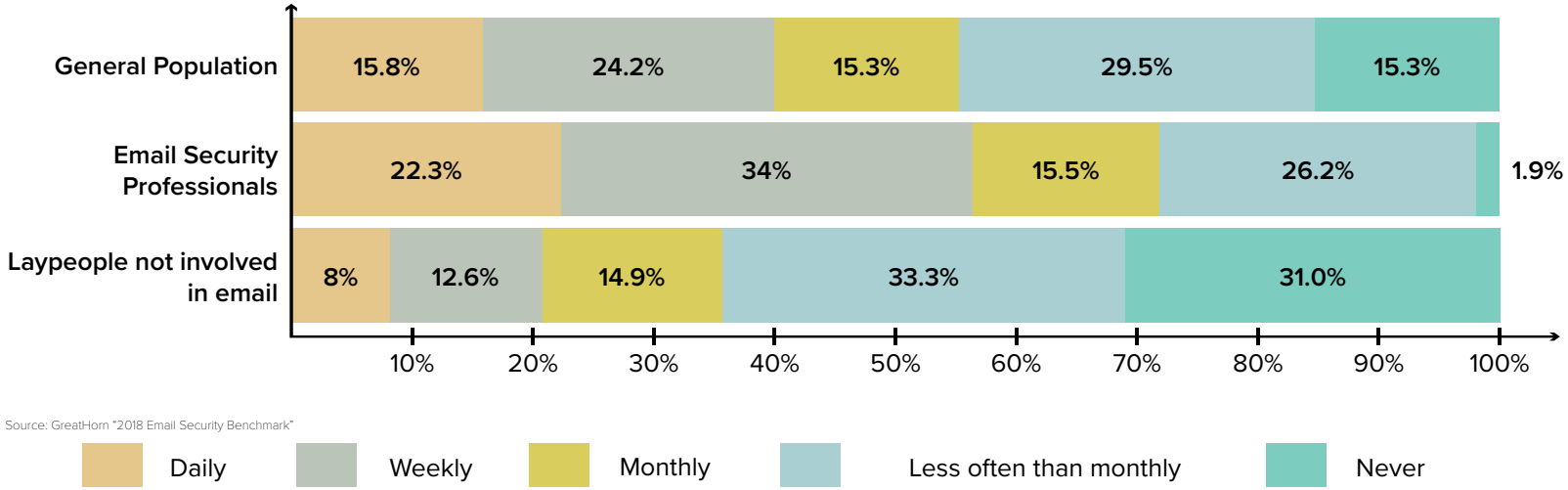
Approximately 1 in 5 users (20.6%) report seeing email-based threats on at least a weekly basis. In contrast, a greater percentage of email security professionals (22.3%) report seeing daily threats, and an additional 34 percent report weekly, for a total of 56.3 percent seeing at least weekly threats. These same email security professionals also report an average of three security products deployed to protect their email.



Source: GreatHorn "2018 Email Security Benchmark"

Compared with the average user, email security professionals are **2.5x** more likely to recall seeing email-based threats in their inboxes on a weekly basis.

Not including spam, how often do you see email-based threats (i.e. phishing / spoofing, malware / viruses)?

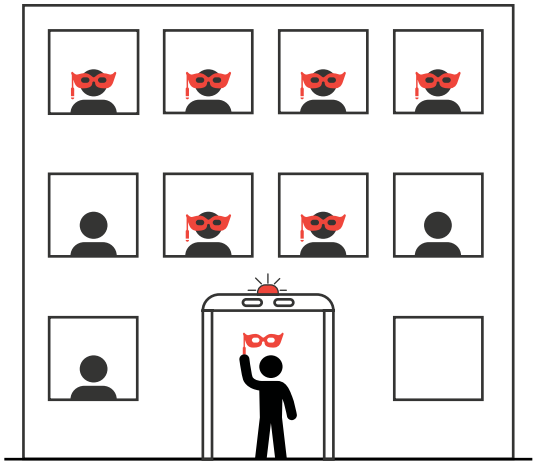


Source: GreatHorn "2018 Email Security Benchmark"

For the purpose of our analysis, we categorized someone as an email security professional if they played one of the following roles for email security:

- Final say on technical requirements
- Owns the budget
- Technical evaluator
- Sets overall security strategy (e.g. CISO)
- Business evaluator
- Investigates and recommends

THREAT PREVALENCE



Source: GreatHorn "2018 Email Security Benchmark"

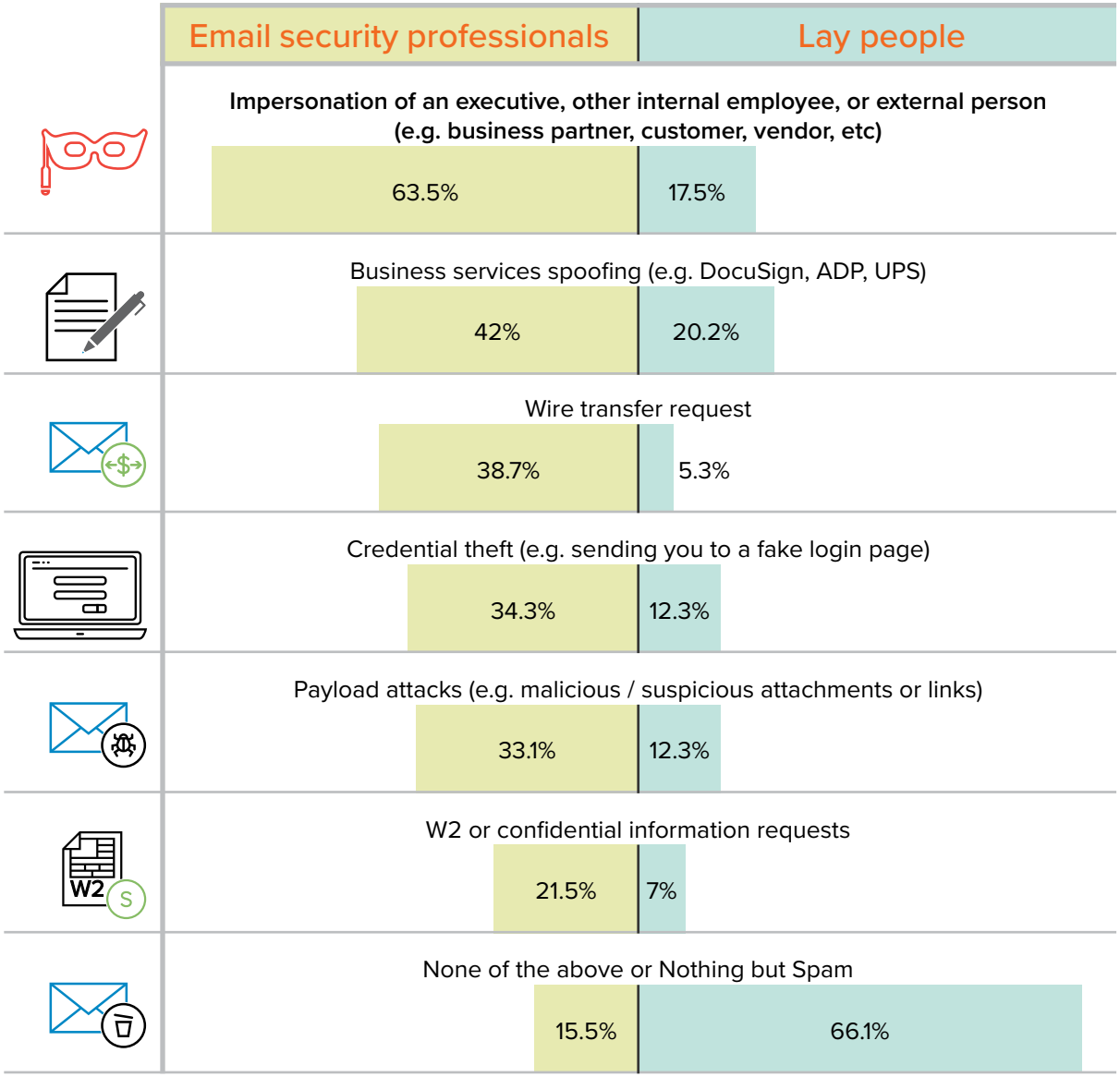
63.5% of email security professionals **see impersonation attack bypass their email security** tools and make it to the inbox.

We found consistent results when we asked what kind of threats respondents see in their inbox (i.e. those that don't get pushed into quarantine). In this case, **two-thirds (66.1%) of laypeople reported nothing but spam, but only 15.5 percent of email security professionals say the same.**

Overall, nearly half (45.8%) of all respondents actively see executive, internal, or external impersonations bypass their email security solutions. As we narrow our focus to email security professionals (whose job responsibilities make them more acutely aware of such incidents), we find that 63.5 percent of this population reports impersonations. Business services spoofing was the second most prevalent threat in this group (42%), followed by wire transfers (38.7%), credential theft (34.3%), and payload / malware (33.1%).

When breaking down the data by company size, we find the prevalence of threats to be roughly the same (within ~ five percentage points), with smaller companies (defined as fewer than 500 employees) seeing slightly higher incidence of wire transfer requests (42.6% vs 36.1%), payload / malware attacks (36.1% vs. 31.1%), and credential theft scams (37.7% vs 31.9%). Meanwhile, companies with more than 500 employees were more likely to see executive impersonations (65.5% vs 59%) and W2 scams (22.7% vs 18%).

Which of the following types of email do you / your users see in your inboxes (NOT what gets quarantined)? (Select all that apply)



Source: GreatHorn "2018 Email Security Benchmark"

As you can see in the above graph, it's not just the sophisticated and personalized phishing attacks that make it through email security filters. One-third of email security professionals report that payload attacks (e.g. malicious / suspicious attachments or links) – despite being the threats most heavily guarded against – are still making it through their cybersecurity defenses.

Not surprisingly, people who indicated themselves as "dissatisfied" or "very dissatisfied" with their email security solution were much more likely to see threats reach inboxes, with two-thirds reporting business services spoofing, 57 percent seeing payload-based threats, 57 percent credential theft, and an astonishing 76 percent seeing impersonations.

There was minimal correlation between the prevalence of a given type of attack and the importance assigned to it. When asked "Which email-based threat worries you the most?", email security professionals consistently ranked three threats at the top, regardless of organization size: impersonations (28.8%), credential theft (24.7%), payload-based attacks (22.5%).

76% of "dissatisfied" respondents see impersonation attacks hit user inboxes

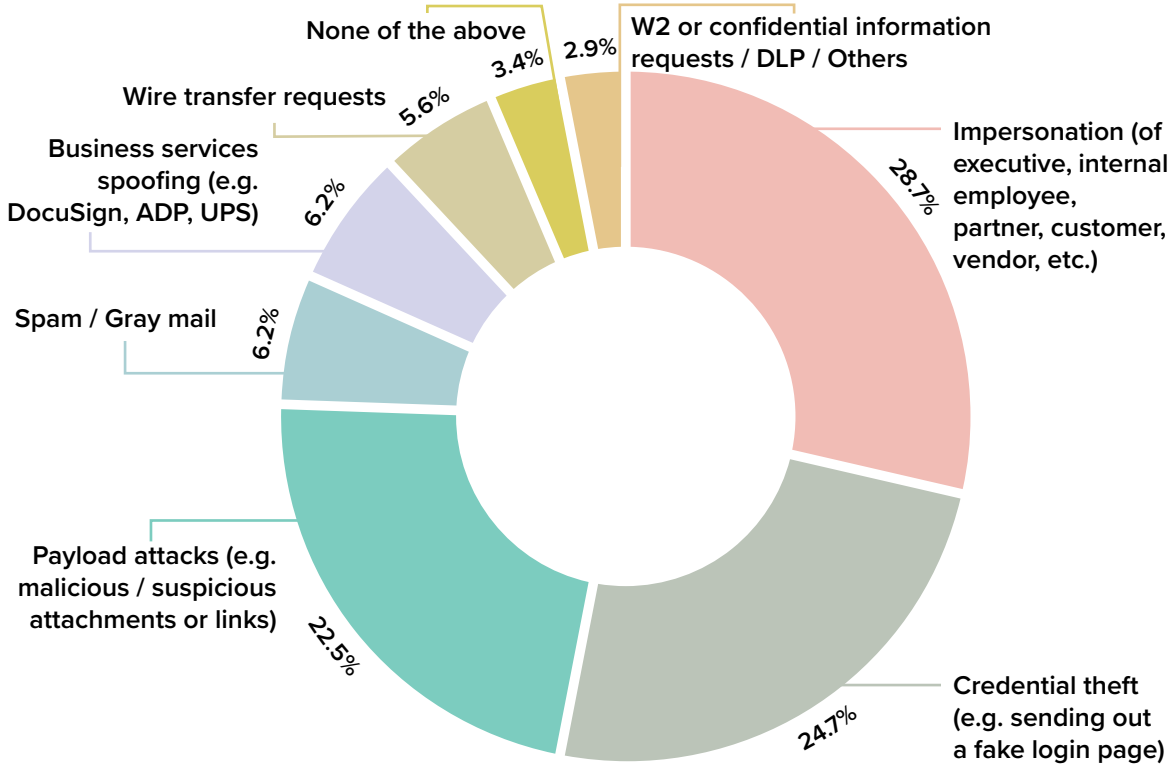
Source: GreatHorn "2018 Email Security Benchmark"

In contrast, data loss prevention was consistently the least cause of concern (0.6%), followed by W2 or confidential information requests (1.7%). 3.4 percent of respondents expressed that they had no concerns about any email-based threats.

However, when we look at this by role, we find that more technical decision makers and budget owners (32%) worry "the most" about credential theft compared to their peers, though for technical decision makers, the most popular number one worry remains impersonations at 35.1 percent.

Meanwhile those that indicate that they "set the overall security strategy for our organization" are disproportionately concerned most about payload attacks (33.9% vs the average of 22.5%).

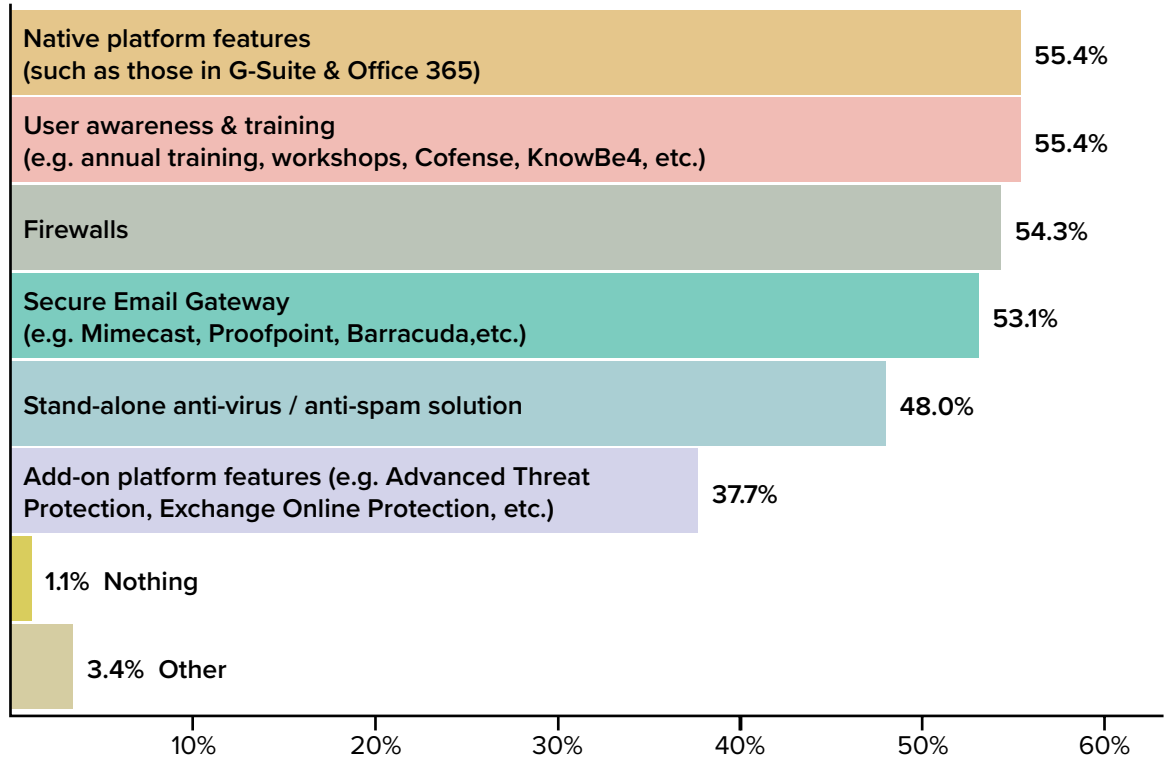
Which email-based threat worries you the most?



Source: GreatHorn "2018 Email Security Benchmark"

PREVENTION

What strategies / technology do you use to guard against email threats?



Source: GreatHorn "2018 Email Security Benchmark"

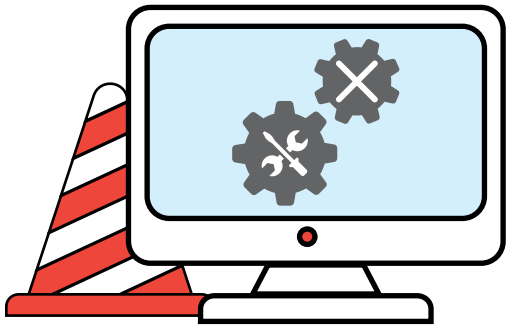
On average, small companies and cloud-based companies had slightly fewer email security countermeasures in place than their enterprise and on-premises peers, but the difference was slight (average of 2.85, 2.96, 3.19, and 3.30 products / services respectively).

On-premises companies are **1.9x** more likely to use a **secure email gateway** than a company that uses cloud email.

Source: GreatHorn "2018 Email Security Benchmark"

However, when we compare different groups against their usage of specific strategies, we find some more remarkable differences. For example, more than three-quarters (77%) of on-premises companies use secure email gateways compared to just 41 percent of cloud-email companies. On-premises companies were also far more likely to use stand-alone anti-virus / anti-spam solutions (57.4% vs 43.8%), user awareness & training (63.9% vs 51.8%), and firewalls (60.7% vs. 51.8%) than cloud-email companies. Meanwhile cloud-email companies were far more likely (22.3%) to either use "nothing", just "native cloud-email features", or "other", compared to on-premises organizations (8.2%). Details on the "Other" indicate a variety of options, such as environmental segregation (on-prem) and newer cloud-native email security products.

REMEDIATION



1 in 5 respondents have to **take a direct remediation action weekly** due to an email threat.

Source: GreatHorn "2018 Email Security Benchmark"

In addition to understanding the frequency and type of threats organizations see, we asked them how often such threats require direct remediation such as suspending compromised accounts, PowerShell scripts, resetting compromised third-party accounts, board-level notifications of compromise, etc.

On average, one in five respondents need to take such remediation actions on at least a weekly basis. An additional 20 percent need to do so at least monthly. Not surprisingly, the more often they reported seeing threats in their inboxes, the more likely they were to require daily or weekly remediation. Of the respondents who see threats reach inboxes on a daily basis, 40.9 percent of them have to take remediation actions on at least a weekly basis.

Change that very slightly to look at respondents who report threats weekly, and the weekly remediation percentage drops down to 28.6 percent.

OVERALL SATISFACTION

Senior roles were **more "dissatisfied"** or **"very dissatisfied"** by their email security solution. (19.7% vs 11.8%)

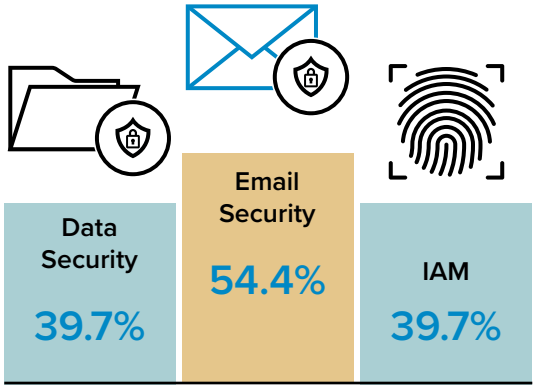
Source: GreatHorn "2018 Email Security Benchmark"

Overall, almost half (46.1%) of all respondents reported themselves less than "satisfied" with their current email security solution, and only 10.1% were "very satisfied." Roughly a third (34.3%) indicated that their solution was just "good enough." These percentages held roughly true regardless of which email platform they were using (i.e. Outlook 365/G Suite vs. on-premises), within 3-4 percentage points.

Interestingly, however, when broken out by role, the more senior roles (technical decision maker, budget owner, and CISO), were much more likely to be either "dissatisfied" or "very dissatisfied" by their email security solution (19.7% compared to 11.8% in general).

PRIORITIZING SECURITY INITIATIVES

More **CISOs** considered email security to be a top **3 critical security initiative** than any other security initiative.

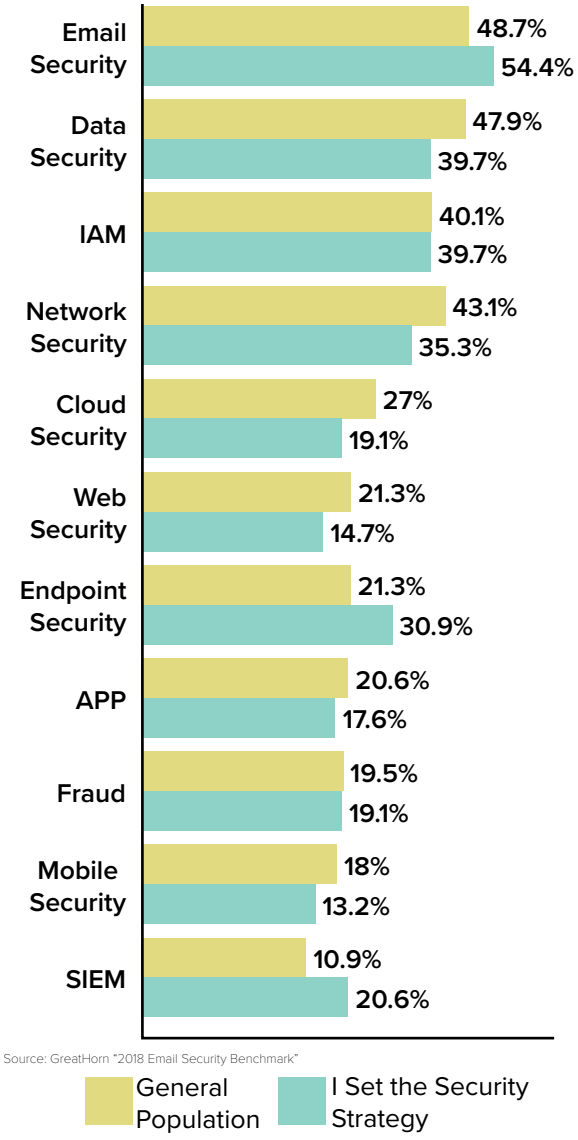


Source: GreatHorn "2018 Email Security Benchmark"

Finally, we wanted to understand the importance of email security within the broader security landscape. We presented respondents with 11 different security initiatives and asked them to select the three most critical to the security of their organization.

Across the entirety of the panel, more people (48.7%) selected email security as a top 3 security initiative than any other. This was particularly true of respondents who "set the security strategy" for their organization (e.g. the CISO role), who overwhelmingly selected email security as the top priority, with 54.4 percent putting email security as a top three initiative, with the next closest being data security and identity and access management tied for second at 39.7 percent.

In fact, no matter how we looked at the data, email security consistently landed in the top 3, followed typically by data security (47.9% in the general population) and network security (43.1%), though IAM was a close fourth at 40.1 percent (and often, as indicated in the CISO roles, the third priority). Even respondents that had no involvement in email security considered it a top three initiative.



Source: GreatHorn "2018 Email Security Benchmark"

SUMMARY

65% highlighted **fundamental technical issues** with their existing email security solution.

Source: GreatHorn "2018 Email Security Benchmark"

It's clear from our survey that email security remains both a top priority and a security hole for organizations. According to Verizon's 2018 Data Breach Investigations Report, one in 25 people will click on or respond to any given phishing attack, and only 17 percent of phishing attacks are reported. If you consider then that 40 percent of the general population sees email threats on at least a weekly basis, the chances for exposure are high. Our data shows that senior security leaders clearly recognize the severity of this threat given their ranking of email security as the top priority among all security initiatives.

Of the respondents that ranked email security as a top 3 initiative, nearly half (48.9%) were less than "satisfied" with their solution. When asked, "Which of the following are problems for you despite your current email security solution? (Select all that apply)", 64.6% of all respondents indicated fundamental issues with their solution (this percentage rose to 71.3% when evaluating just users that ranked email security as a top 3 initiative):

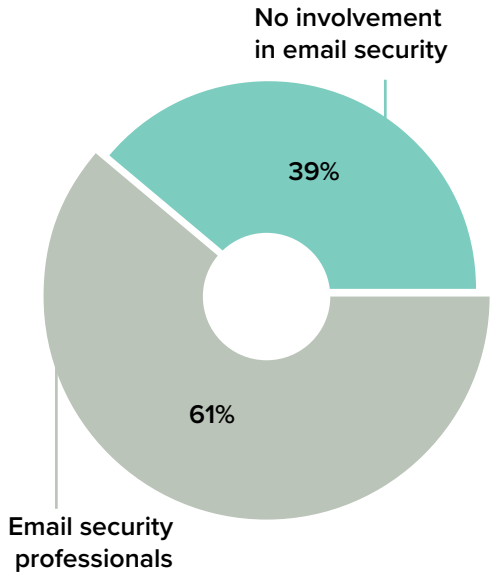
- 34.8% report that their current solution "Doesn't stop internal threats (e.g. if a user account is compromised)"
- 16.3% report "Missing payload attacks (e.g. malicious attachments and/or links)"
- 20.2% report "Missing payload-free attacks (e.g. impersonations, social engineering)"
- 19.1% report "Weak (or no) remediation capabilities if something gets through"
- 20.8% express concern that their solution "Negatively impacts business operations (e.g. too many false positives)"

In the interest of keeping this benchmark factual, the authors of this report will constrain additional analysis to our blog (www.greathorn.com/blog). Check it out to find out what we think of our findings, see additional cuts of the data, and leave comments to give us your view.

ABOUT THE PANEL

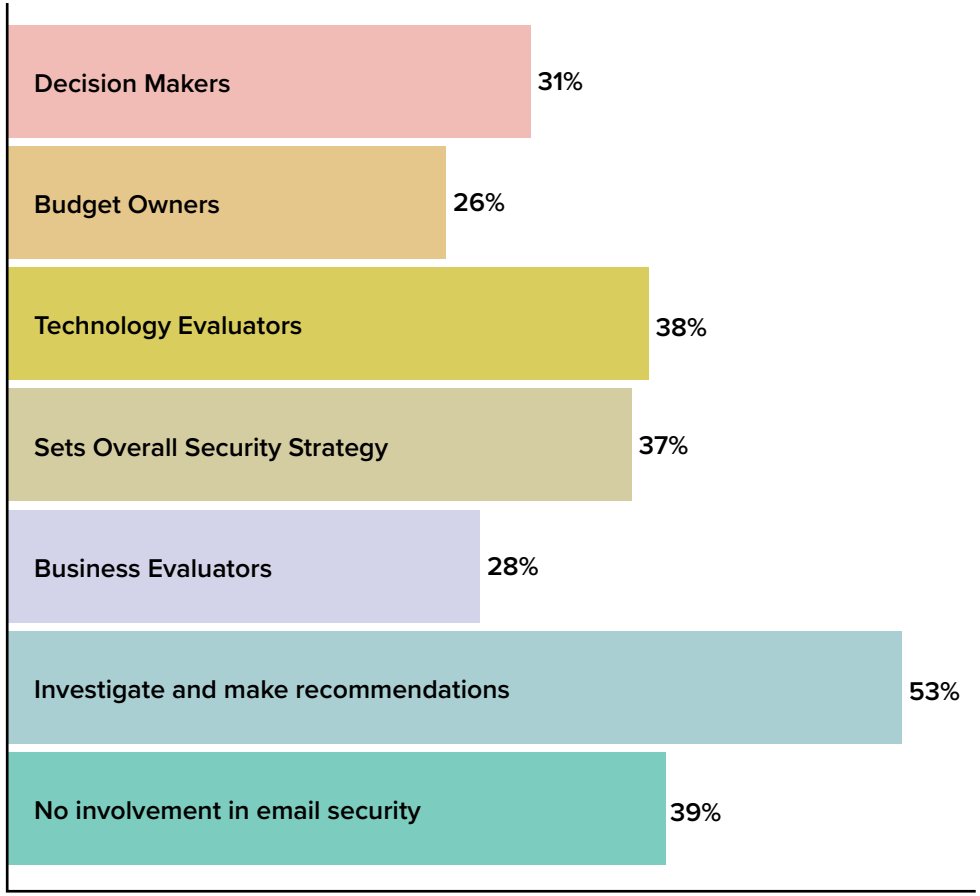
This survey of 295 professionals, mostly (but not all) in IT roles was gathered through both offline sources (Gartner Security & Risk Management Summit) as well as online (two separate panels, one more security focused and one IT focused, from two different sources). Respondents were predominantly from North America.

Involvement in email security



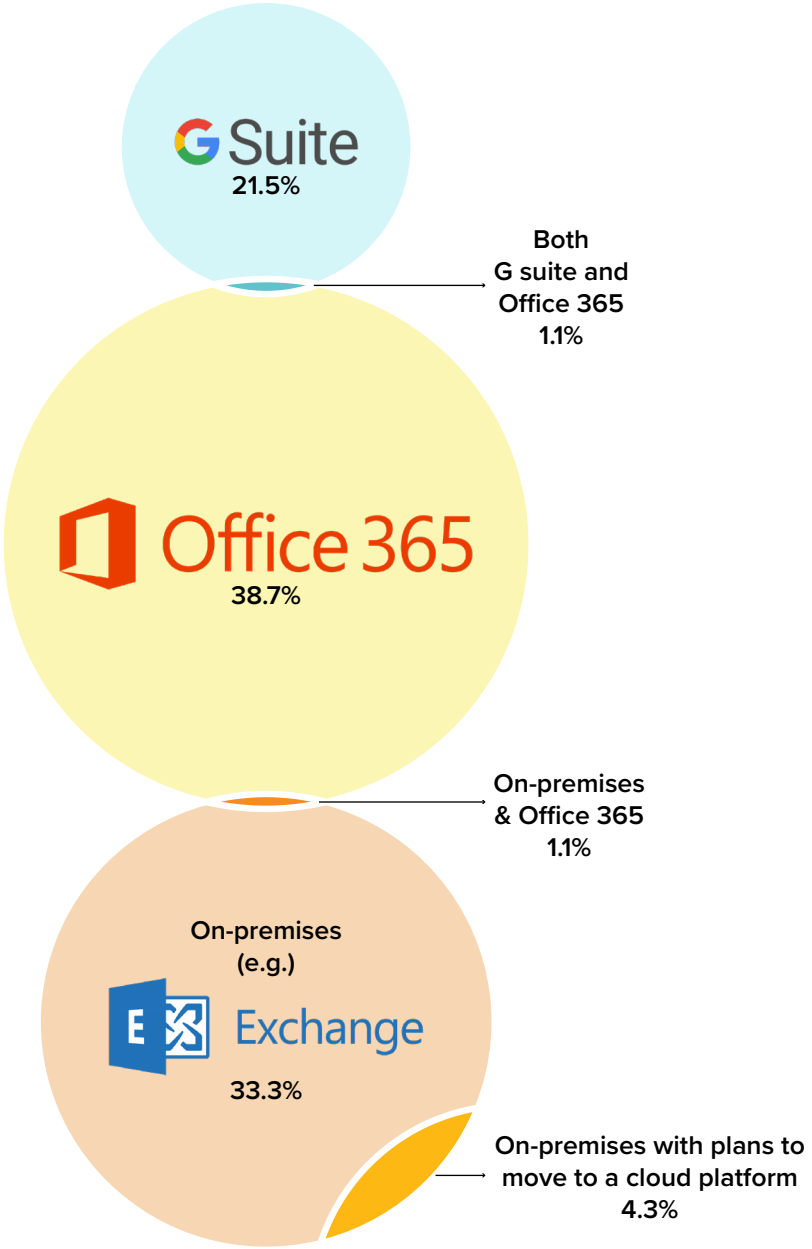
Source: GreatHorn "2018 Email Security Benchmark"

Respondents by role (multiple answers allowed)



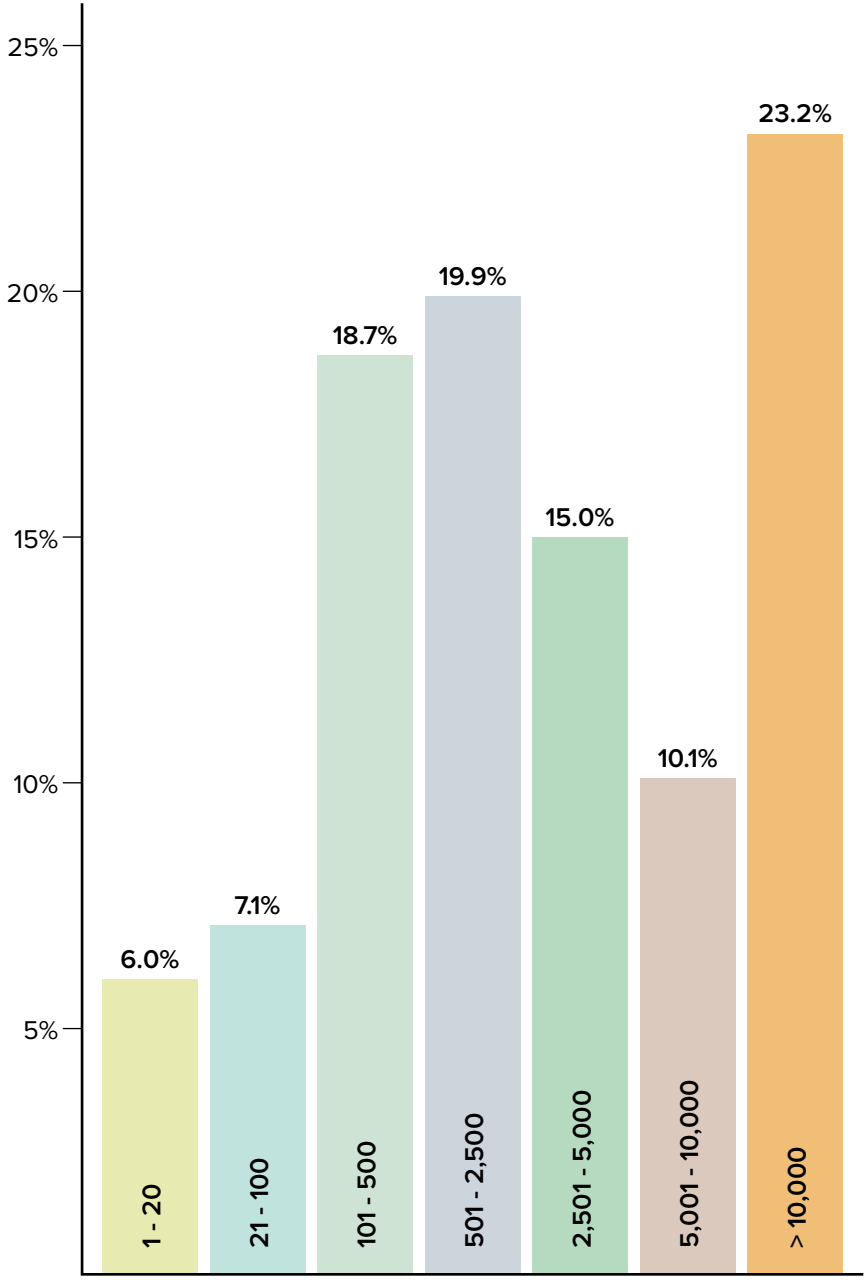
Source: GreatHorn "2018 Email Security Benchmark"

Email platform (Over 60% using cloud email)



Source: GreatHorn "2018 Email Security Benchmark"

Company Size



Source: GreatHorn "2018 Email Security Benchmark"

ABOUT GREATHORN

GreatHorn protects Office 365 and G Suite customers from today's sophisticated email threats by automating detection, remediation, and post-delivery incident response. 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.

More information is available at www.greathorn.com