2020

Cybersecurity
INSIDERS

Phishing Attack

LANDSCAPE REPORT

GreatHorn

INTRODUCTION

Phishing, the fraudulent attempt to obtain sensitive information such as usernames, passwords, or credit card data through email spoofing, is on the rise. The recent COVID pandemic has further accelerated this trend.

The 2020 Phishing Attack Survey reveals the latest trends, challenges and best practices for email security, arming organizations with the information required to better protect against today's advanced threats. To provide this information, we surveyed cybersecurity professionals ranging from executives to IT security practitioners, representing a balanced cross-section of organizations of various sizes across multiple industries.

Key findings include:

- Over a third of respondents (36%) were not confident that employees at their organizations would be able to spot and avoid an email phishing attack in real-time. Furthermore, 38% of respondents said that over the past year, someone within their organization has fallen victim to a phishing attack.
- 53% of respondents say that their organization has seen an increase in email phishing attacks during COVID-19. Nearly a third (30%) say that email phishing attacks have become more successful during COVID-19.
- On average, organizations in the survey are remediating 1,185 phishing attacks every month, an average of 40 each day. However, only 6% of phishing attacks result in a breach.

Many thanks to GreatHorn for supporting this important research project.

We hope you find this report informative and helpful as you continue your efforts in protecting sensitive data and email communications.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

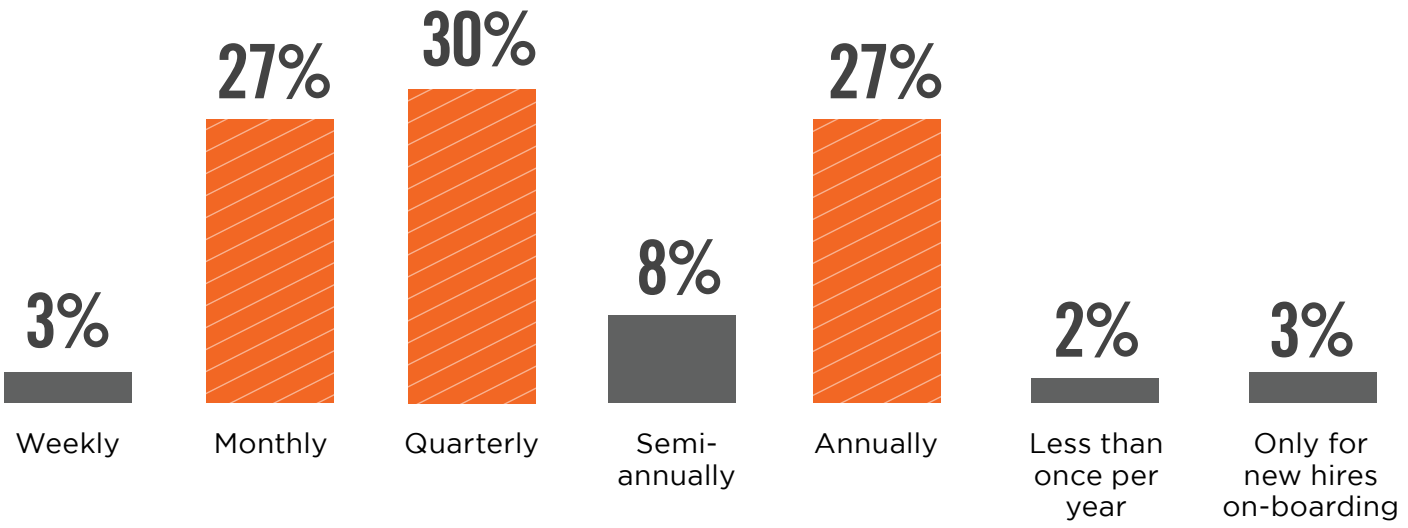
IMPLEMENTING CYBERSECURITY AWARENESS TRAINING

CYBERSECURITY AWARENESS TRAINING

Most organizations (76%) conduct cybersecurity awareness training for employees to mitigate the threat of phishing emails – although over a quarter (27%) of organizations only train employees once a year and 30% train employees quarterly.

Does your organization conduct cybersecurity awareness training for employees to mitigate the threat of phishing emails?

If yes, how often?



LIKELIHOOD OF FALLING VICTIM TO A PHISHING ATTACK

VICTIMS OF EMAIL PHISHING ATTACKS

Most respondents (62%) thought the likelihood of falling victim to an email phishing attack is equal across all generations, suggesting that everyone is vulnerable, even those who grew up with technology.

Which generation do you think is the most likely to fall victim to an email phishing attack?

EMAIL PHISHING ATTACK TARGETS

Nearly half of respondents (49%) thought the CEO or the head of the company would be more likely to be targeted with an email phishing attack. However, 56% of respondents thought the mid-level manager would be the most targeted and 51% highlighted that entry level staffers would be most likely targeted. This indicated that again, no matter the job title or age of the victim, everyone is just as vulnerable and targeted by phishing attacks.

At your organization, who is more likely to be targeted with an email phishing attack?

56%

Mid-level manager

49%

CEO/head of the company

51%

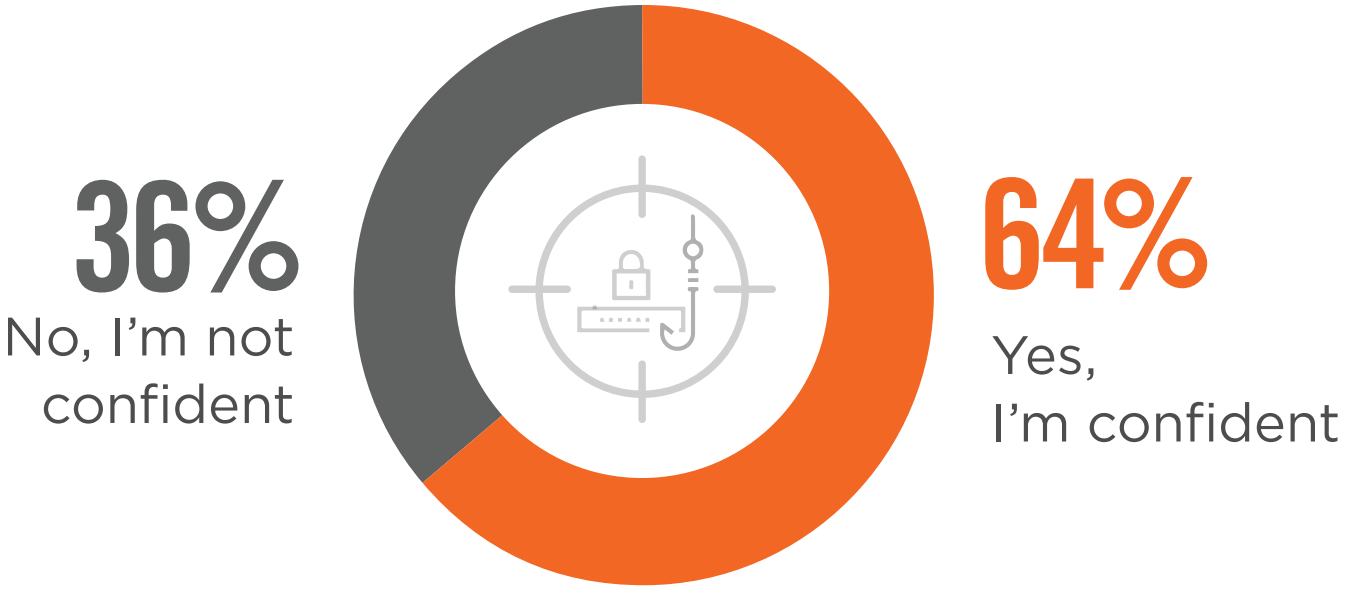
Entry-level staffer

Other 12%

SPOTTING AN ATTACK

Over a third (36%) of respondents were not confident that employees at their organizations would be able to spot and avoid an email phishing attack in real time.

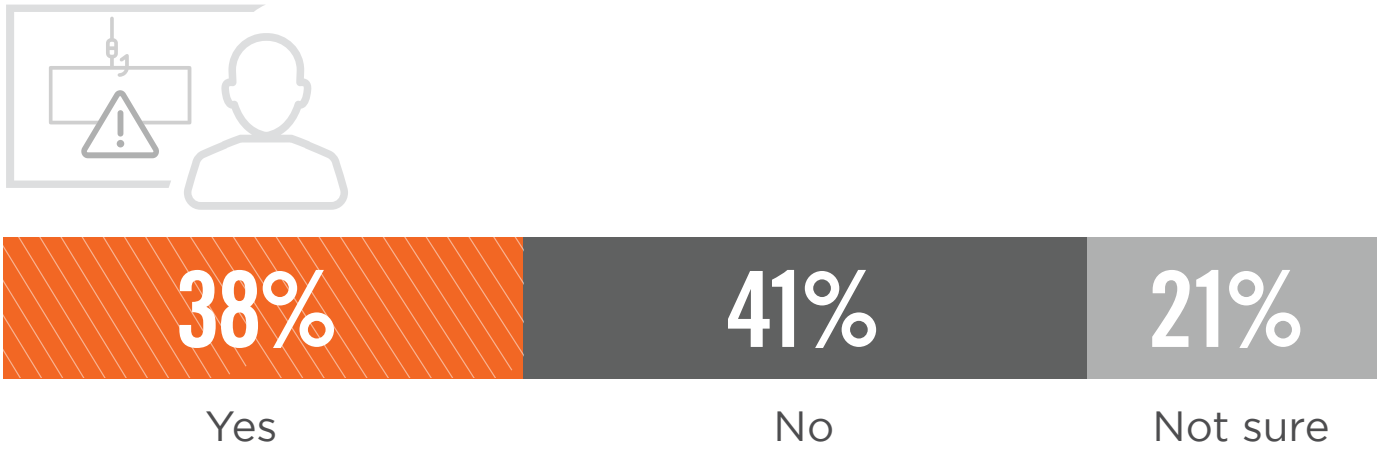
Overall, are you confident that the employees at your organization would be able to spot and avoid an email phishing attack in real time?



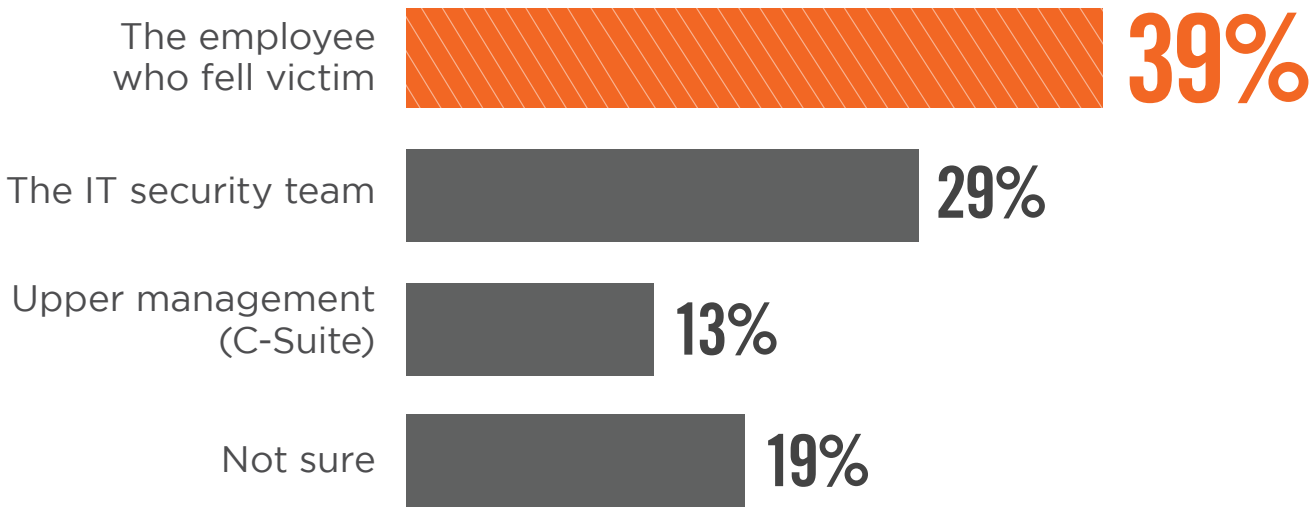
ATTACKS REFLECT NEGATIVELY ON VICTIMS

Thirty-eight percent of respondents said that over the past year, someone at their organization has fallen victim to a phishing attack. Thirty-nine percent of respondents say that this reflects poorly on the employee who fell victim, while 29% said it reflects poorly on the IT security team.

Over the past year, has anyone at your organization fallen victim to a phishing attack?



If an employee falls victim to an email phishing attack at your organization, on whom would it reflect more poorly?



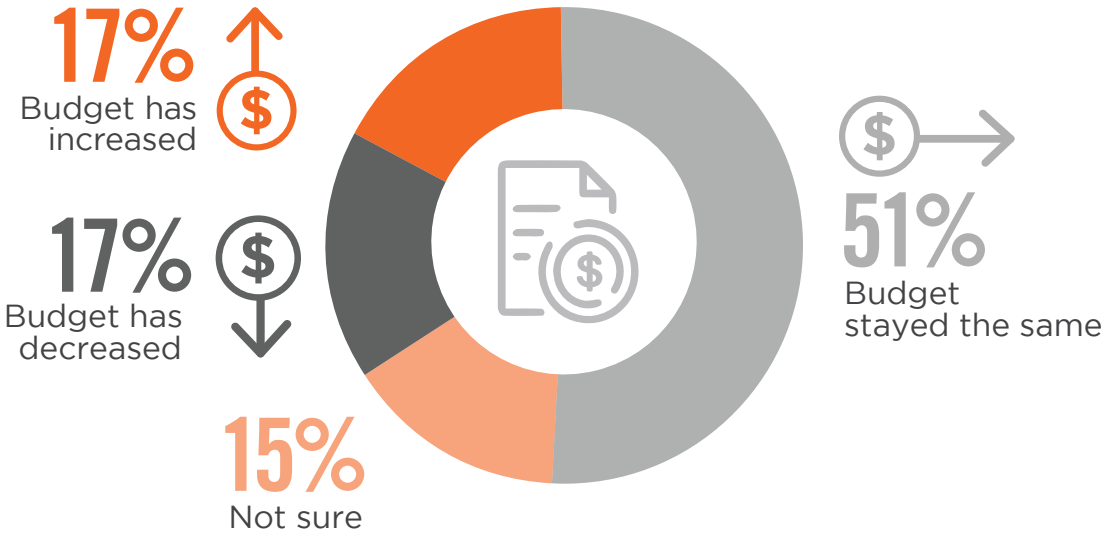
BUDGET AND RESOURCES TOWARDS CYBER-SECURITY DURING COVID-19

CYBERSECURITY BUDGET

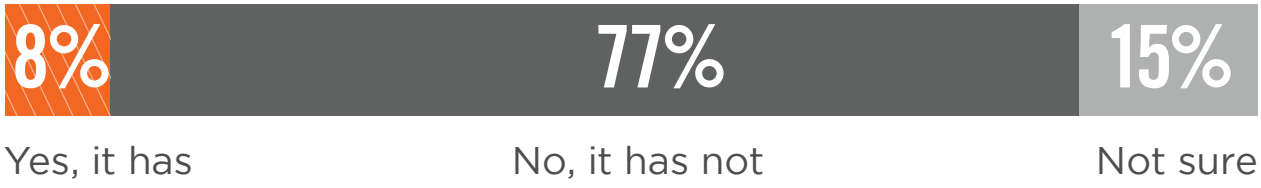
Fifty-six percent of respondents say that their organization allocates enough budget and resources towards cybersecurity; and 51% say that their budget has stayed the same during the COVID-19 pandemic. Seventy-seven percent have said that an email phishing attack has not had a direct monetary impact on their organization.

Does your organization allocate enough budget and resources towards cybersecurity?

How has your cybersecurity budget been impacted by the COVID-19 pandemic?



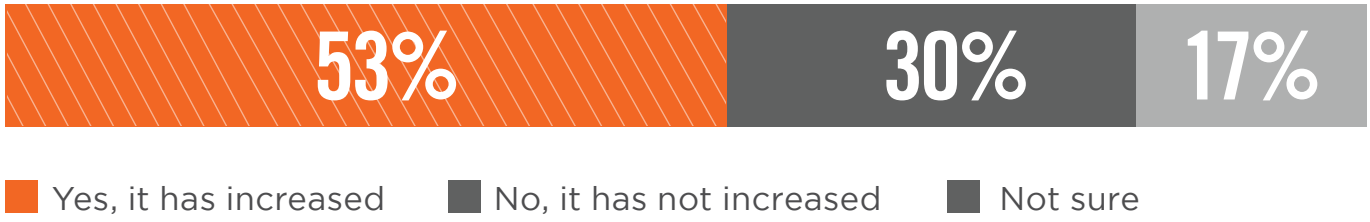
Has an email phishing attack had a direct, monetary impact on your organization over the past year?



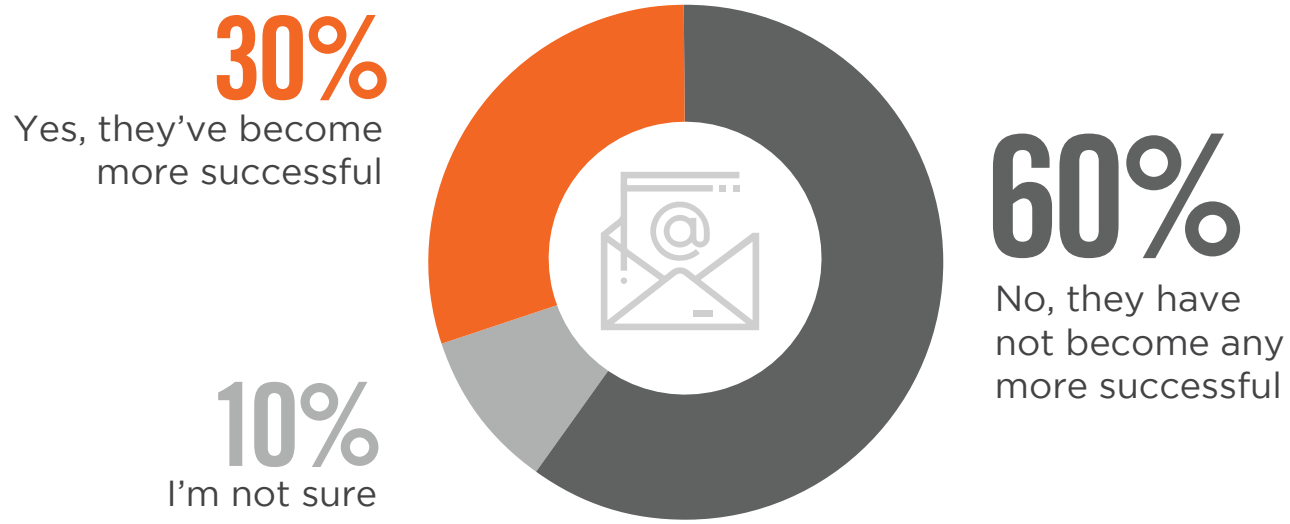
EMAIL PHISHING ATTACKS ARE RISING

Fifty-three percent of respondents say that their organization has seen an increase in email phishing attacks during COVID-19. Nearly a third (30%) say that email phishing attacks have become more successful during COVID-19.

Has your organization seen an increase in email phishing attacks during the COVID-19 pandemic?



At your organization, have email phishing attacks become more successful during the COVID-19 pandemic?

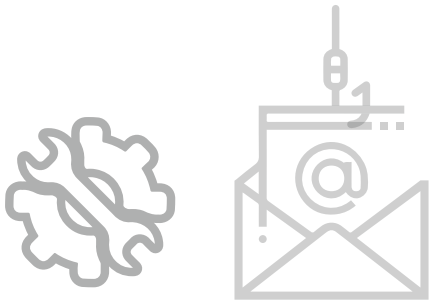


IMPACT OF PHISHING ATTACKS ON ORGANIZATIONS

REMEDIATION FREQUENCY AND TIMING

On average, organizations in the survey are remediating 1,185 phishing attacks every month, an average of 40 each day. However, only 6% of phishing attacks result in a breach.

How many phishing attacks do you need to remediate on a monthly basis?



1,185 Phishing attacks every month

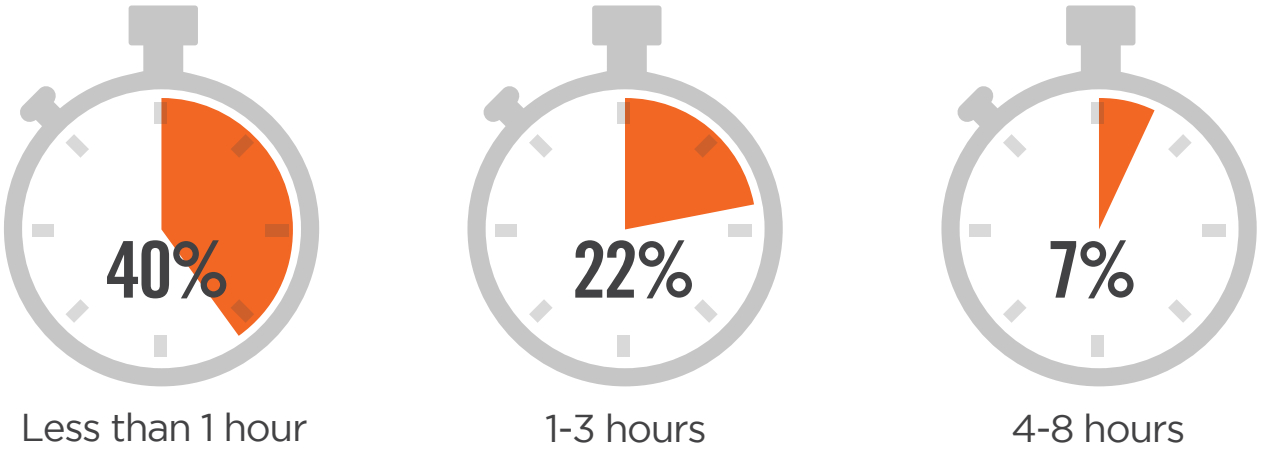
What percentage of reported phishing attacks that reach end users result in a data breach for your organization?

6% Of phishing attacks result in a breach

TIME TO REMEDIATE AN ATTACK

While 40% take less than one hour to remediate a phishing attack, 15% of organizations are spending one to four days remediating phishing attacks.

How long, on average, does it take your organization to remediate a phishing attack (in resource hours)?

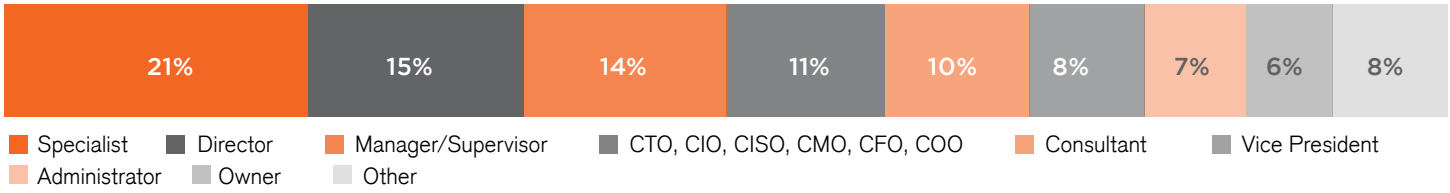


15% Of organizations are spending 1-4 days remediating phishing attacks

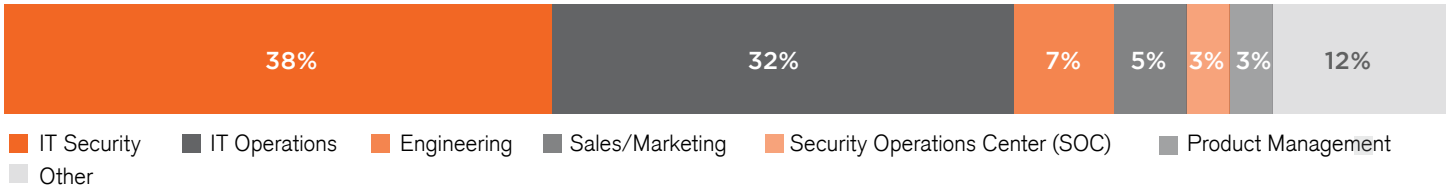
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 317 IT and cybersecurity professionals in the US, conducted in August 2020, to identify the latest enterprise adoption trends, challenges, gaps and solution preferences related to phishing attacks. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

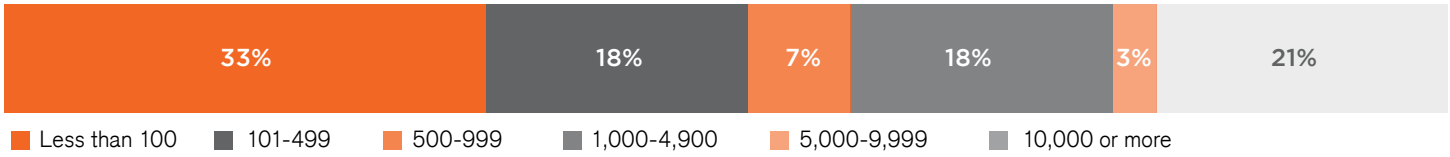
CAREER LEVEL



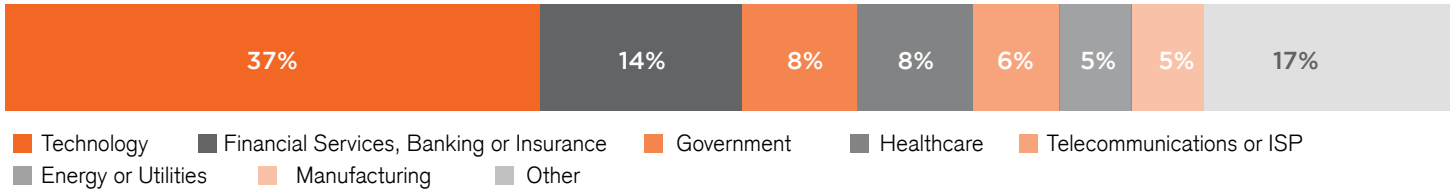
DEPARTMENT



COMPANY SIZE



INDUSTRY



Respond at the Speed of Deception

Cybercriminals are exploiting the absence of facts to create chaos. And, they're reaching your organization through the easiest point of entry. Email.

GreatHorn provides the most comprehensive cloud-native email security platform built on facts, giving organizations the sophisticated security controls required to protect against today's advanced threats.

Get the facts you need to detect and remediate phishing attacks in seconds. It's the difference between a security incident and a breach.

www.greathorn.com