2021

Cybersecurity
INSIDERS

BUSINESS EMAIL COMPROMISE REPORT

GreatHorn

INTRODUCTION

Welcome to the 2021 Business Email Compromise Report. Business Email Compromise (BEC) attacks are one of the financially most damaging cyber crimes. They typically involve phishing emails and social engineering tactics to attack organizations and trick unsuspecting employees and executives into conducting tasks under the guise of legitimate business activity, often appearing to come from a trusted sender.

This report is designed to explore the state of evolving email threats and how organizations are responding to protect themselves (including specific concerns and challenges, solution priorities, and budget trends.)

Key findings include:

- The most commonly seen type of BEC attack is spoofed email account (71%) followed by spear phishing at 69%
- Almost 1 out of 3 organizations (30%) state that more than 50% of links received via email lead to a malicious site
- 57% of malicious links in phishing emails intend to steal credentials
- The finance department has a target on its back, 34% of respondents said finance employees are the most frequent victims of spear-phishing attempts
- 43% of organizations have experienced a security incident in the last 12 months, with 35% stating that BEC/phishing attacks account for more than 50% of the incidents

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

MOST COMMON EMAIL ATTACKS

We asked organizations what types of Business Email Compromise (BEC) attacks they experience most often. The most commonly seen type of BEC attack is spoofed email account or website (71%) followed by spear phishing at (69%).

Of the following Business Email Compromise (BEC) attacks, what do you see most often?

71%
Spoofed email account or website

69%
Spear phishing

24%
Malware

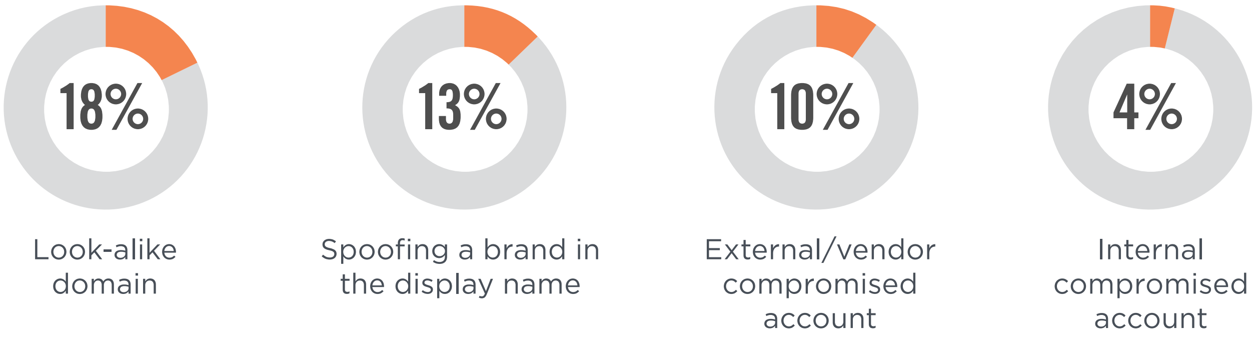
Other 6%

MOST MISUSED INFORMATION FOR PHISHING

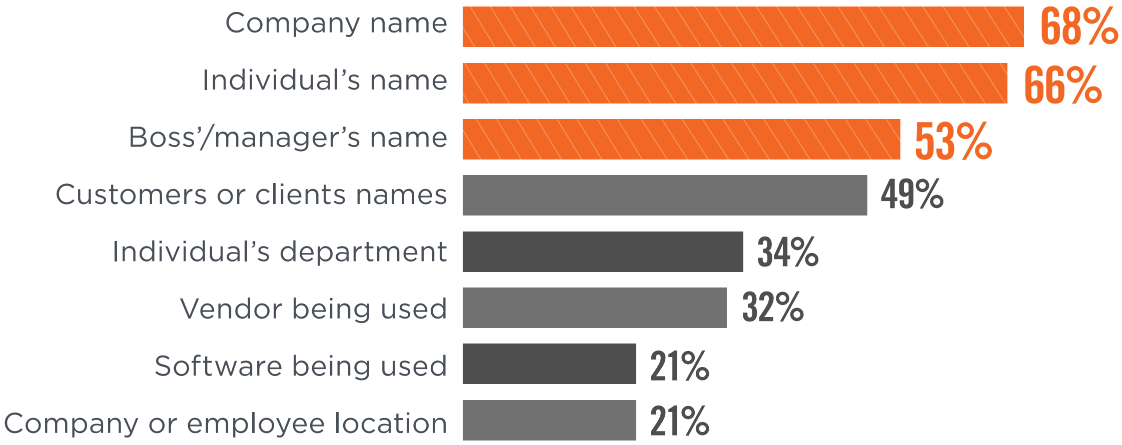
The easy availability of personal information online, combined with screen and email fatigue, is priming the landscape for successful spear phishing attacks. Nearly 50% of all BEC attacks are spoofing an individual's identity in the display name; among spear phishing emails, cybercriminals are using company names (68%), targeted individual names (66%), boss/manager names (53%) – all to trick unsuspecting employees and executives into conducting tasks under the guise of legitimate business activity.

What is the most commonly used BEC impersonation attack?

49% Spoofing an identity in the display name



When identifying a spear phishing email, what information has the cybercriminal used?

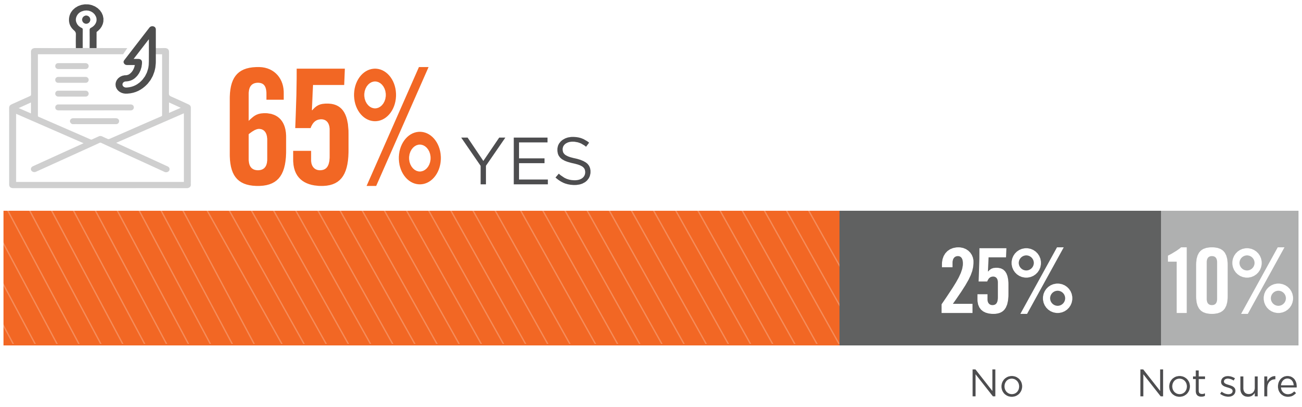


RISE IN SPEAR PHISHING

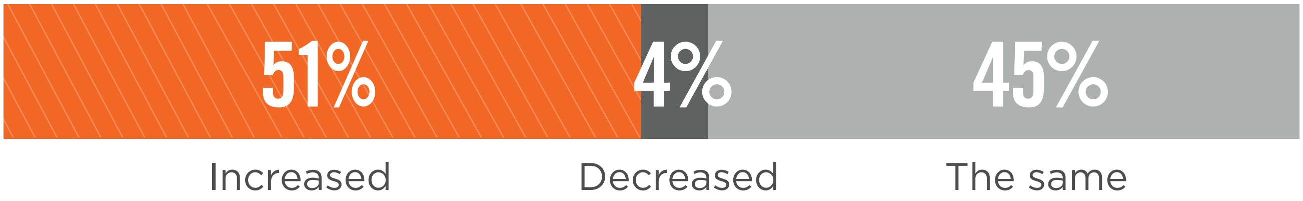
Sixty-five percent of IT security pros say that their organization has experienced spear phishing in 2021. Over half say that spear phishing has increased in the last 12 months (51%). Thirty-nine percent report that their organization now experiences spear phishing on a weekly basis.

It remains to be seen whether the return to the corporate office will reduce the amount of successful impersonation attacks, as IRL access to colleagues will be more readily available.

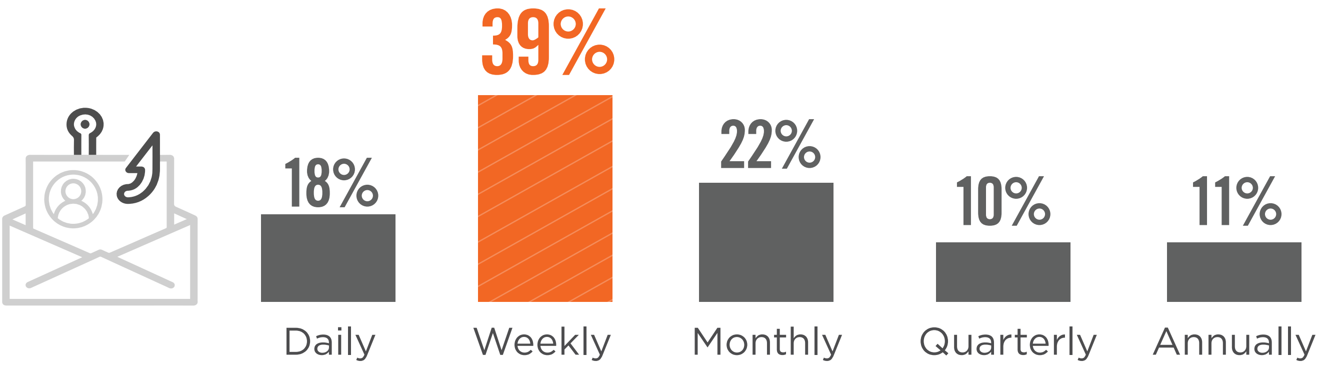
Has your organization experienced spear phishing in 2021?



Has spear phishing increased or decreased in the last 12 months?



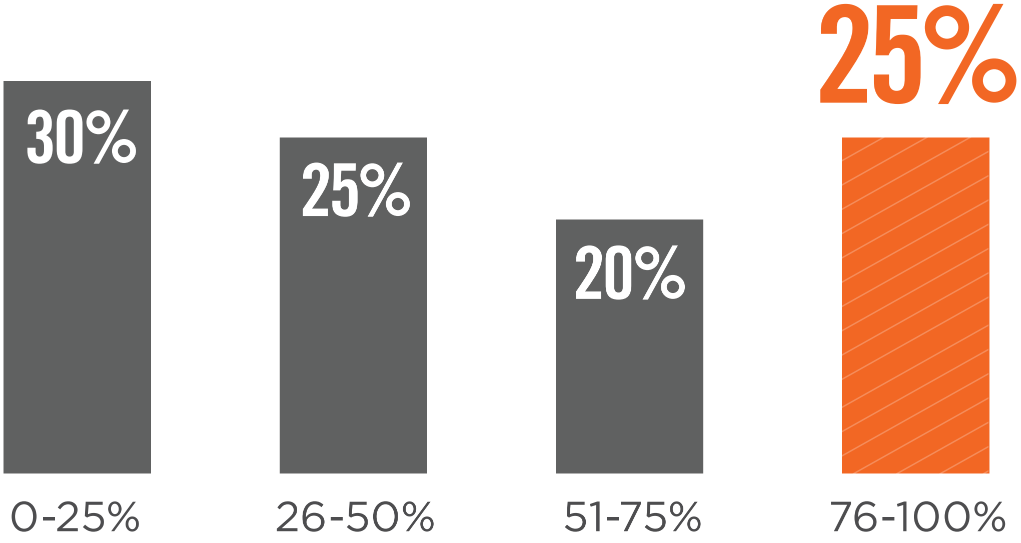
How often does your organization experience spear phishing?



MALWARE VIA EMAIL

We asked organizations what percentage of the malware detected was delivered by email. One out of four organizations say 76-100% of malware they detect is delivered via email.

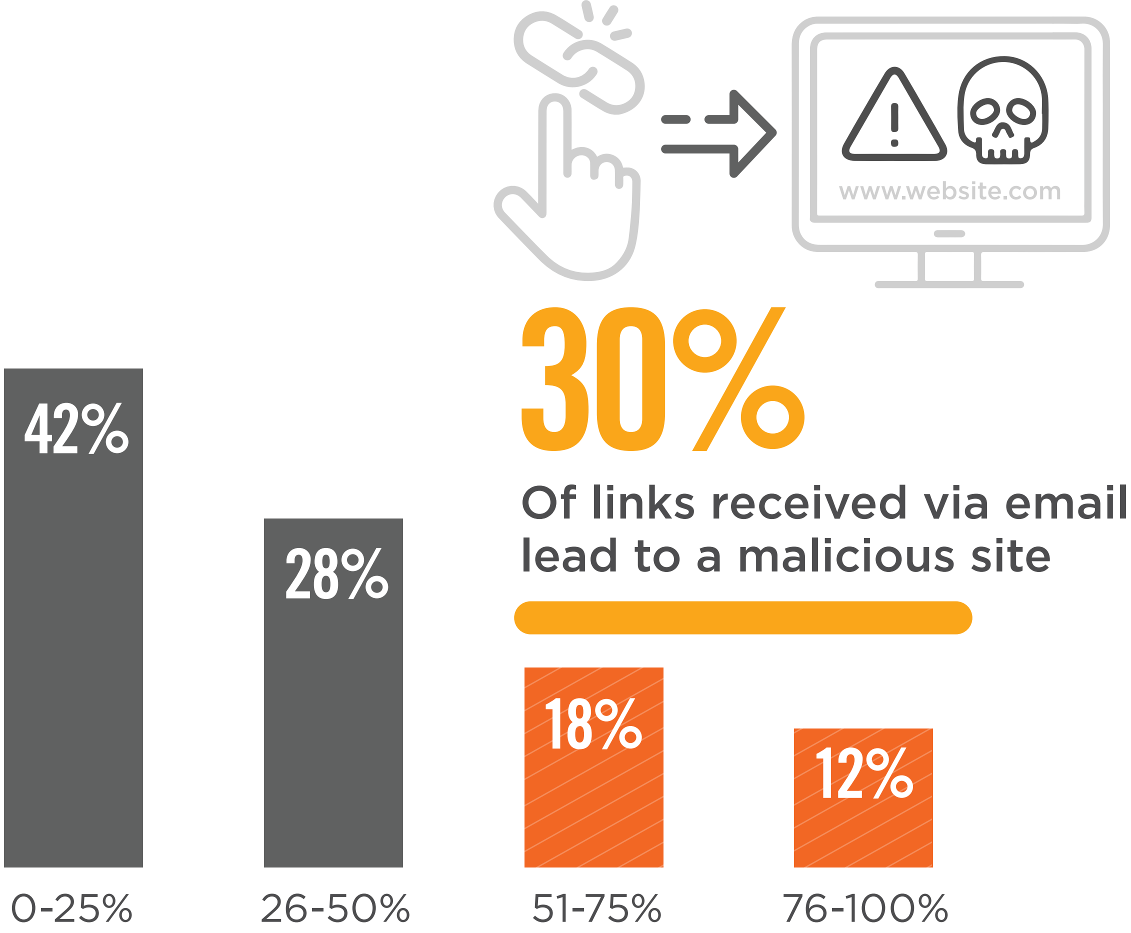
Of the malware detected by your organization in the last year, what percentage was delivered via email?



MALICIOUS EMAIL LINKS

When asked what percentage of email links point to malicious sites, almost one out of three organizations (30%) state that more than 50% of links lead to a malicious site.

▶ **Of the links received via email, what percentage lead to malicious sites?**



MALICIOUS INTENT

Fifty-seven percent of malicious links in phishing emails intend to steal credentials - cybercriminals want the keys to the castle, ideally C-suite and finance employees, as they offer access to the most privileged information and financials. This is followed by websites delivering malicious payloads such as ransomware (22%) and payment fraud (20%).

▶ **What are the intentions of those malicious sites?**

57%
Credential theft

22%
Malicious payloads

20%
Payment fraud

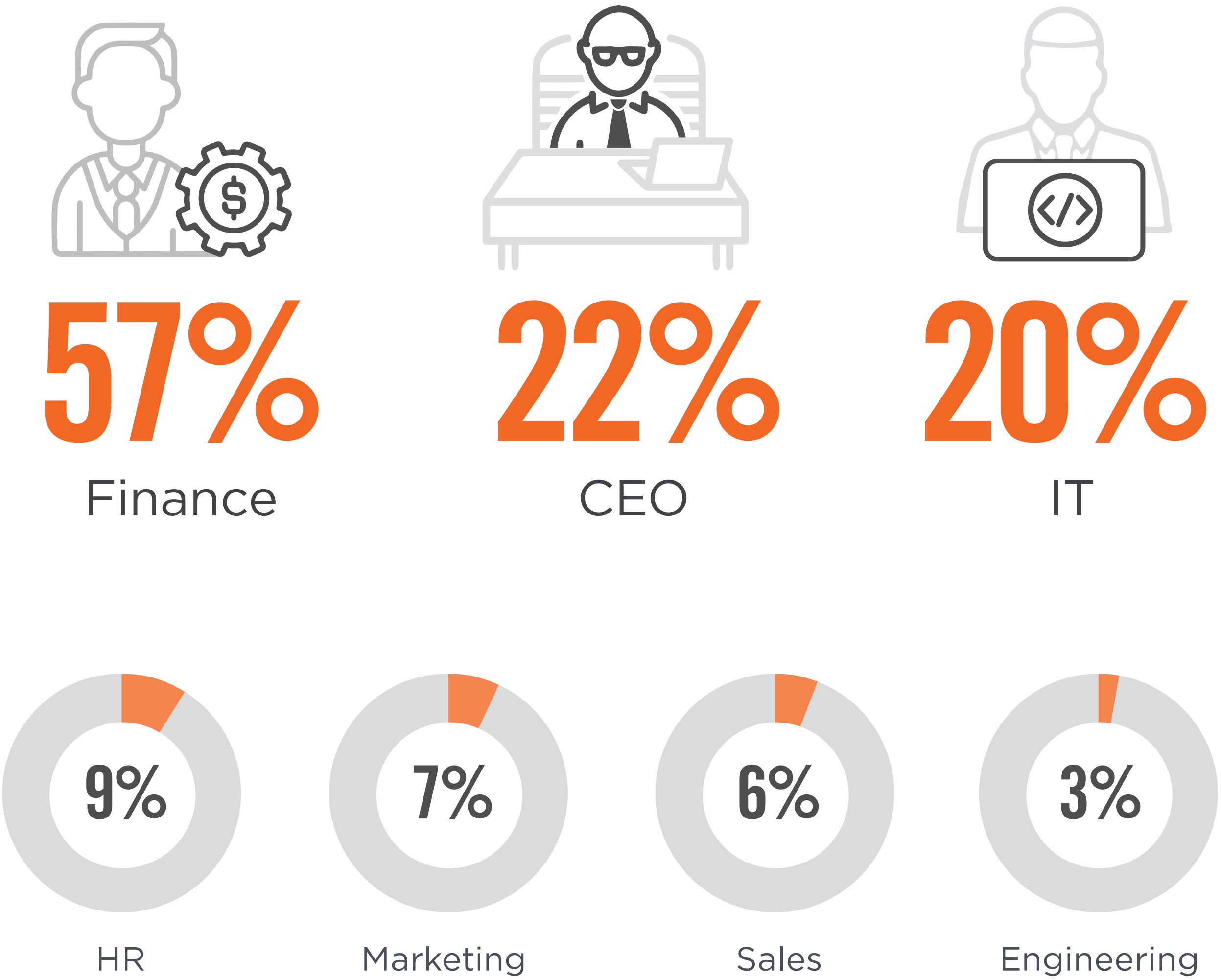
Other 1%

TARGETED DEPARTMENTS

The finance department has a target on its back - 57% of respondents said finance folks are the most frequent victims of spear-phishing attempts.

It's interesting to see that this is a reality for many companies across all of the industries surveyed. Previously we have seen financial institutions targeted. It is noteworthy to highlight that now hackers are specifically targeting finance departments within companies across industries.

What department is most targeted by spear phishing?

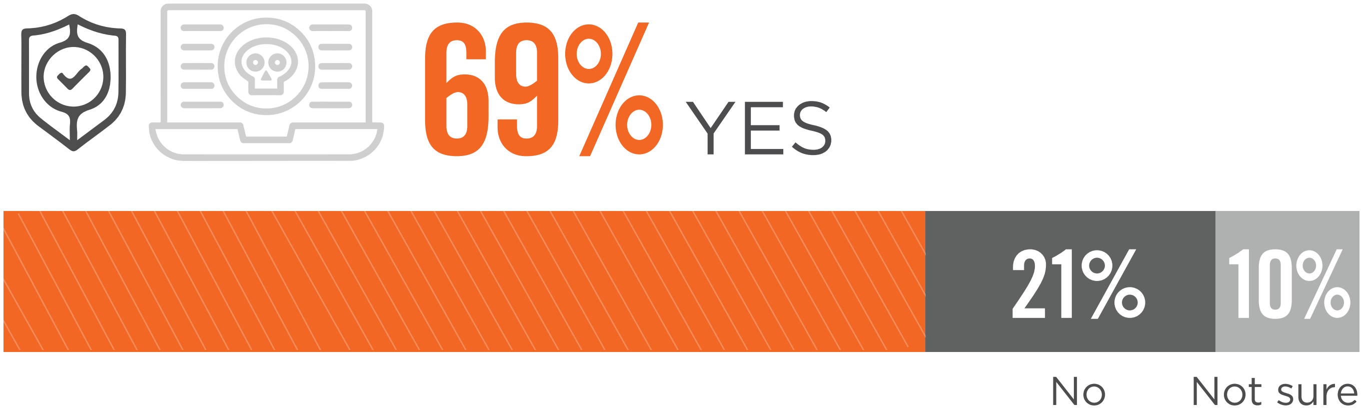


Legal 1% | Other 9%

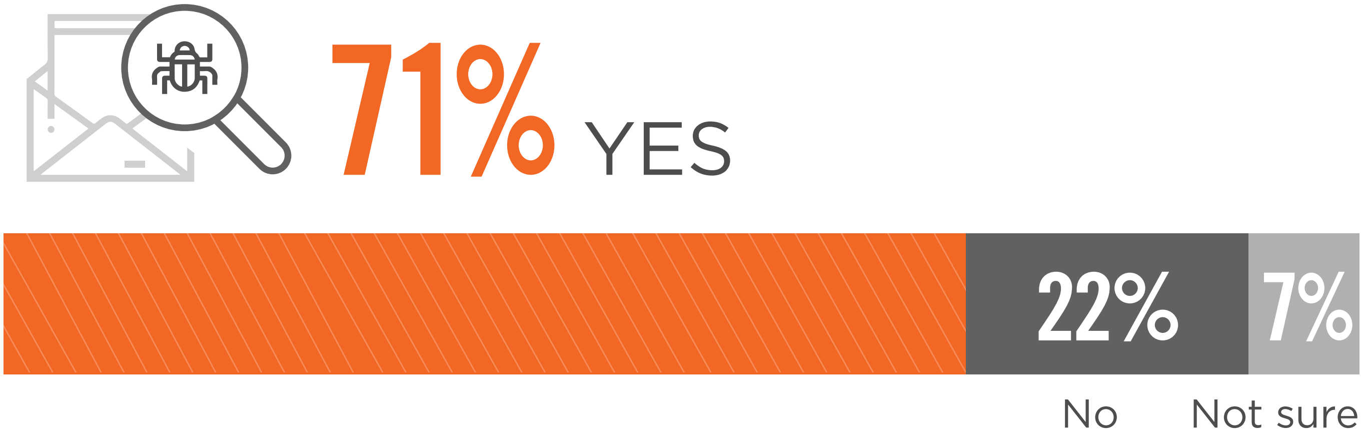
ORGANIZATION PREPAREDNESS

The good news, 69% of organizations claim they are prepared to handle a cyber-attack and 71% believe that their employees can identify a malicious email.

Do you believe your organization is adequately prepared to handle a cyber-attack?



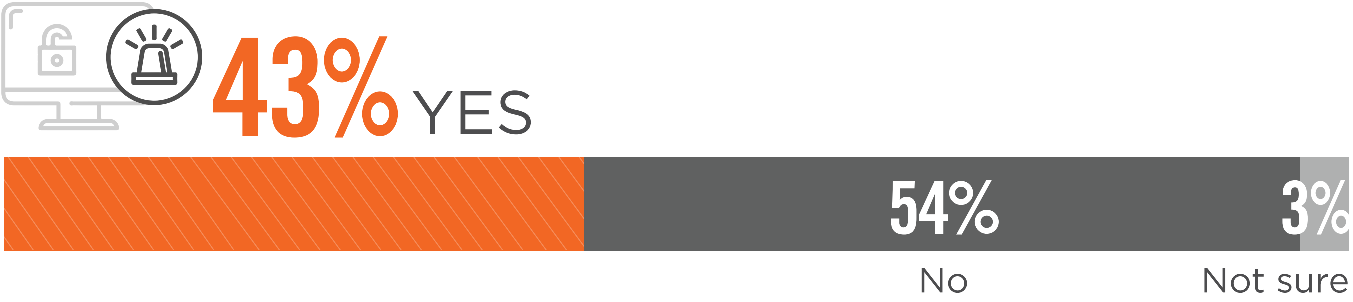
Do you think your employees are adequately prepared to identify a malicious email or link?



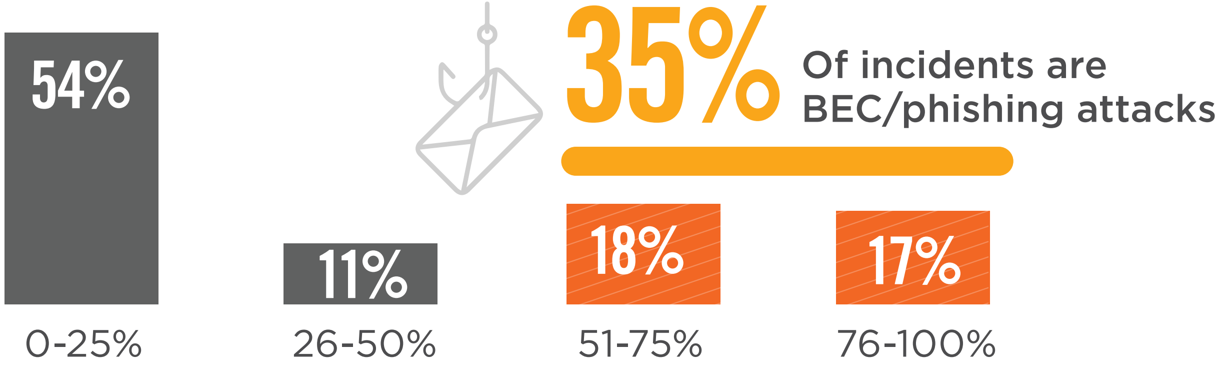
IMPACT OF SPEAR PHISHING

Forty-three percent of organizations experienced a security incident within the last year. Thirty-five percent of security professionals claim that phishing/BEC attacks account for more than 50% of the incidents. The impact of these attacks were significant and included compromised accounts (36%), loss of data (16%), and payment fraud (16%). Just about one quarter of respondents (24%) claim they installed malware to protect against these breaches.

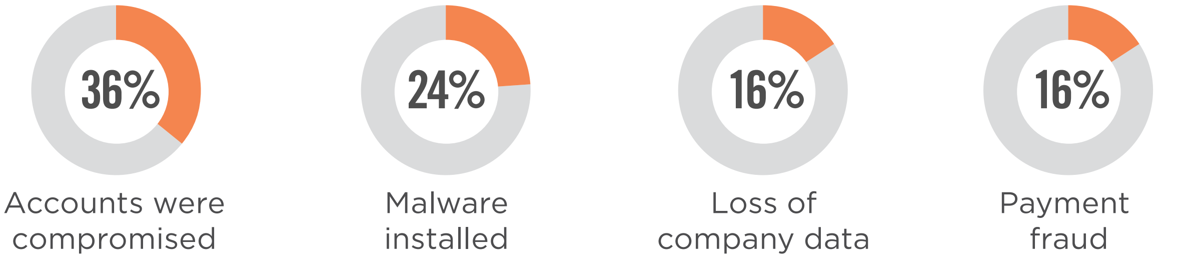
Has your organization experienced a security incident in the last 12 months?



Of the security incidents that have occurred, what percentage are a result of phishing/BEC attacks?



What was the result of the security incident?

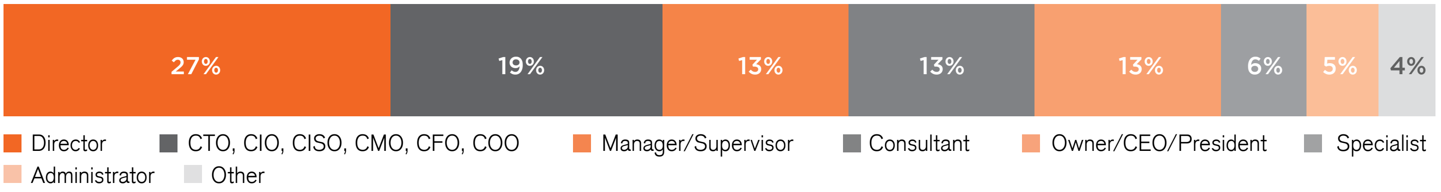


Other 8%

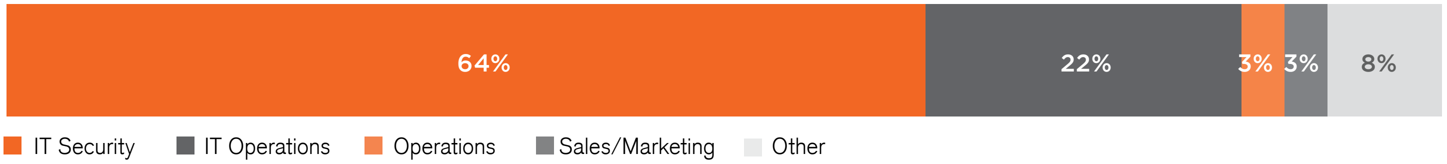
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 270 IT and cybersecurity professionals in the US, conducted in May 2021, 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.

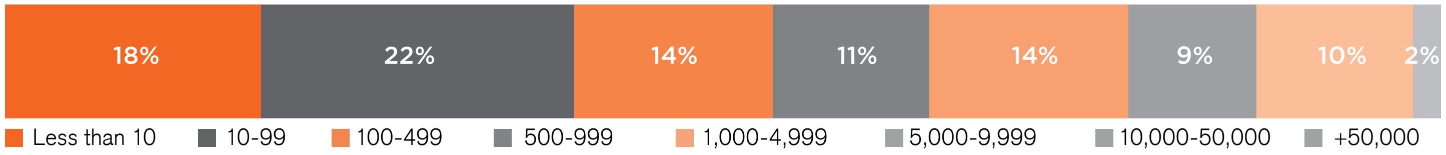
CAREER LEVEL



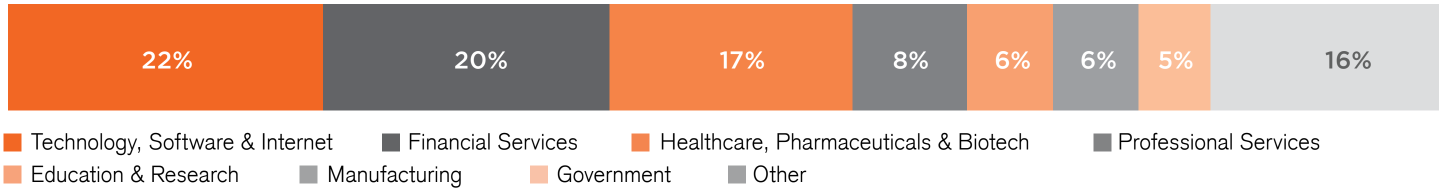
DEPARTMENT



COMPANY SIZE



INDUSTRY



GreatHorn

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