EMAIL SECURITY BENCHMARK

BY THE NUMBERS

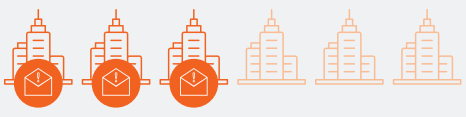
2ND ANNUAL SURVEY RESULTS

GreatHorn

BUSINESS: **COMPROMISED**

Business email compromise (BEC)
48% of Internet crime-driven financial loss*

Average cost of a BEC attack:
$58,901.49*

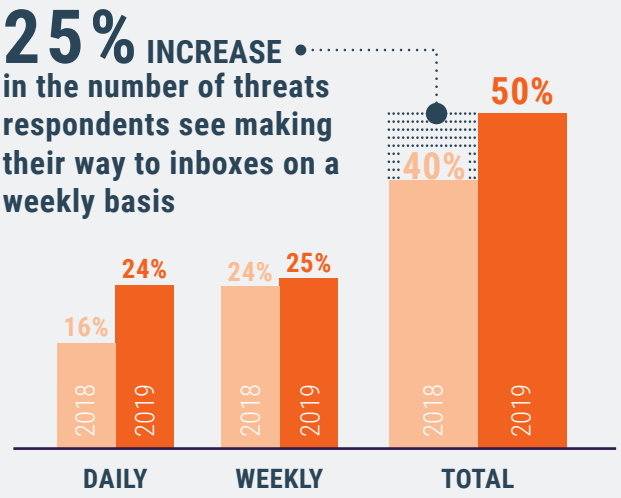


50% of respondents see **email threats weekly** despite existing email security

22% of organizations have experienced a breach within **the past three months** (due to an email-borne threat)

THREATS **ON THE RISE**

25% INCREASE in the number of threats respondents see making their way to inboxes on a weekly basis



How often do email threats require manual remediation?

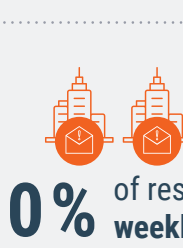
2018	2019
1 IN 5 say weekly	**1 IN 3** say weekly

RISKY BUSINESS

53% have opened email from spam or junk folders in the past month

2/3 white-collar professionals mischaracterize advanced email threats as "just spam"

THE STRANGER **WITHIN**



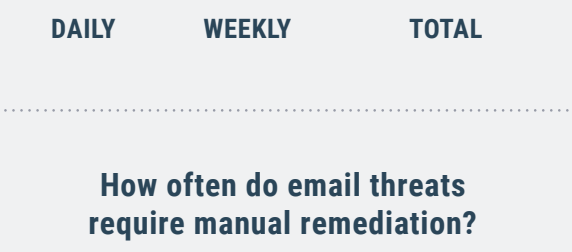
IMPERSONATIONS are the most likely threats to bypass email security solutions

45% still see executive, internal, or external impersonations in their inboxes

Impersonations are the
NUMBER ONE
concern of email security pros

- **34%** Impersonations
- **23%** Payload Attacks
- **20%** Credential Theft

BUSINESS **INTERRUPTED**



79% of respondents report fundamental technical issues with existing email security solutions

1 in 3
RESPONDENTS
have to do **manual remediation actions** at least weekly due to malicious email messages

GreatHorn

To read the 2019 Email Security Trends, Challenges, and Benchmark Survey Report, visit:
greathorn.com/2019-benchmark-report

Sources: * FBI's 2018 Internet Crime Report | All other statistics collected from Mar-Jun 2019 survey of 1021 information security and white-collar professionals.