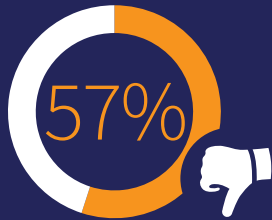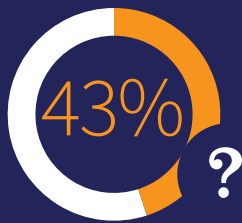# THREAT INTELLIGENCE AND ITS IMPACT ON ORGANIZATIONS

74% think **HUMAN ERROR + PHISHING** represent the biggest cyber security risks. And actionable Threat Intelligence can help address both of them

57% Are **not confident** that their service providers are **sufficiently using Threat Intelligence** to protect their organizations

43% Don't know how their service providers are using Threat Intelligence

69% OF ALL ORGANIZATIONS had at least one person dedicated to **managing Threat Intelligence**

And for organizations with **five or more members** on their security team **88%** had at least one **person** dedicated to **Threat Intelligence**

FREE 68% use at least **one free** Threat Intelligence feed

PAID 62% use at least **one paid** Threat Intelligence feed

systems

USED TO COLLECT & MANAGE THREAT INTELLIGENCE

- SIEMs — 54%
- Threat Intel Platforms (TIPs) — 20%
- Excel, Custom Databases, Other — 26%

according to customers who are **currently paying for feeds**

TOP THREE AREAS

MISSING FROM Threat Intelligence:

#1	Recommended Actions	39%
#2	Organizational Impact	22%
#3	Attacker Attribution	10%

*TECHVALIDATE SURVEY 2019

mimecast®

Want to get inside the minds of your attackers?

Mimecast provides Threat Intelligence as a new standard feature* with our Secure Email Gateway

LEARN MORE