



PHISHING RESPONSE TRENDS

It's a *Cluster*



OVERVIEW

HOW GOES THE WAR? Not so good...

Organizations today take strong measures to guard against data breaches. With 91% of breaches starting with phishing emails,¹ we find ourselves in an arms race against phishing attackers.

So, are we winning the war or just holding ground?

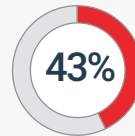
The findings of this report suggest the latter. The following data on phishing and responses show that businesses are flooded with suspicious emails targeting employees but are ill-prepared to process and respond to those threats. In fact, most organizations feel they have little, if any, expertise in anti-phishing and many feel their incident response processes are weak. **Notable findings include:**



Nearly 2/3 of surveyed IT executives have dealt with a security incident originating with a deceptive email.



Nearly 1/2 of respondents say their biggest challenge is too many threats and too few responders.



43% of respondents say their phishing response ranges from "totally ineffective" to "mediocre."



90% still worry most about email-related threats.

In other words, despite all their investments in technology, 66% of the organizations surveyed have experienced a phishing-related incident and almost all still worry about email-related threats. With little more than half of the organizations believing they have sufficient controls in place, it's obvious there's much work to be done in implementing solutions. And that work includes automation to analyze phishing emails and to help incident responders distinguish noise from real threats.

Read on to learn the implications of our phishing response data and what organizations can do to improve their anti-phishing security.

SURVEY METHODOLOGY: Phishing Response Data

Senior Decision-Makers

In May 2017, Gatepoint Research surveyed select IT executives on phishing response strategies. Two hundred executives participated, largely senior decision-makers:

- 18% C-suite
- 32% Managers
- 18% VPs
- 32% Directors

Numerous Industries

The surveyed companies represented a wide variety of industries: business services, high tech, manufacturing, healthcare, financial, retail trade, wholesale trade, transportation, consumer services, telecom and general. One hundred percent of respondents participated voluntarily; none were engaged using telemarketing.

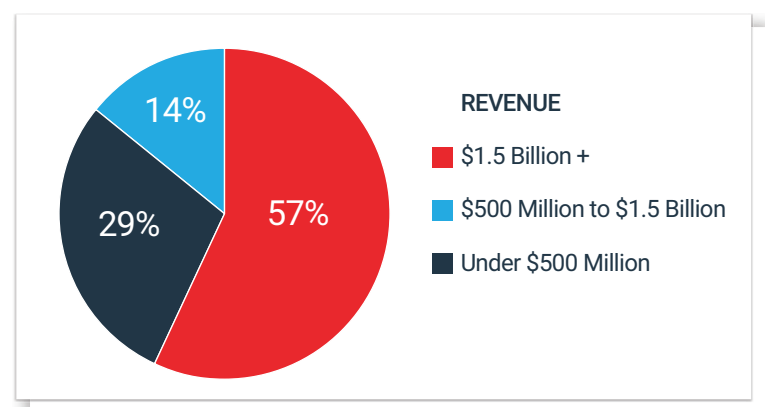


Figure 1: Businesses of all sizes and industries participated in our Phishing Response Survey.

Nearly 1/3 of respondents see more than 500 suspicious emails weekly.

Among those 500 suspicious emails companies receive, something is often missed by filtering technologies. The result? A potentially costly security breach.

With the average office worker receiving 122 emails each day,² it's no wonder phishing is the top attack vector in data breaches.³ Now imagine being a small team of incident responders receiving every forwarded employee email, some truly suspicious, some just spam. Given limited staff and time, how do you sort through hundreds to thousands of emails to find the real threats? **The answer:** better solutions that (a) leverage broader teams to identify phishing and (b) automate and orchestrate response. By reducing noise in the reporting inbox (if they have one), companies can free responders to focus on real threats.

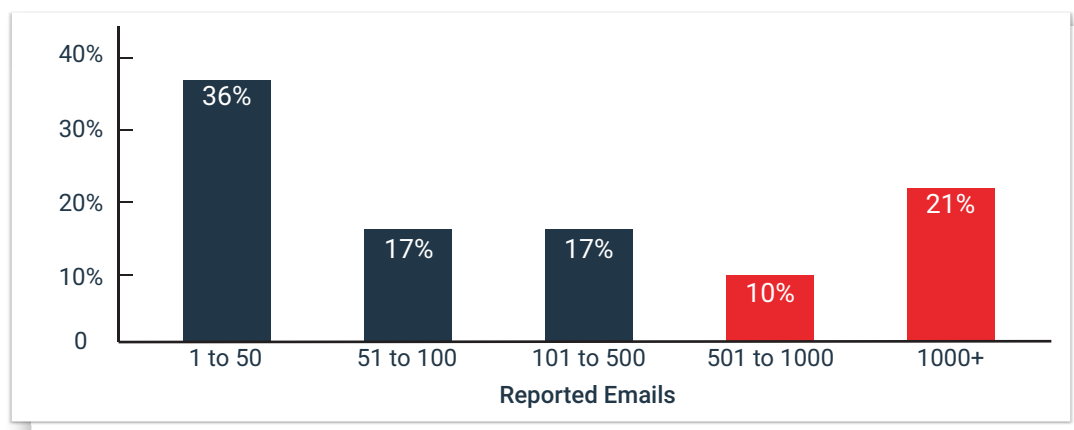


Figure 2: How many suspicious emails are reported in your organization each week?

Only 26% of respondents have a dedicated inbox for suspicious emails.

Whether it's managing emails from 100 employees or 10,000, helpdesk teams can be overwhelmed with suspicious email reports. Sifting through emails – spam and potential attacks alike – is a boring and thankless task for IT teams that would rather hunt for spear phishing and ransomware. Hmm...perhaps if incident responders had a dedicated location or inbox for suspicious emails, the numbers in Figure 2 might be different.

On top of that, helpdesk teams are often spread thin and lack the right phishing detection training and skills. Thus, many may fail to identify and escalate threats or establish protective measures such as blocking access to known malicious sites at the perimeter. It's a "lose-lose" when reported threats go unnoticed that can lead to disastrous breaches. The global median time from compromise to discovery is 99 days⁴ – giving phishers ample time to wreak their havoc.

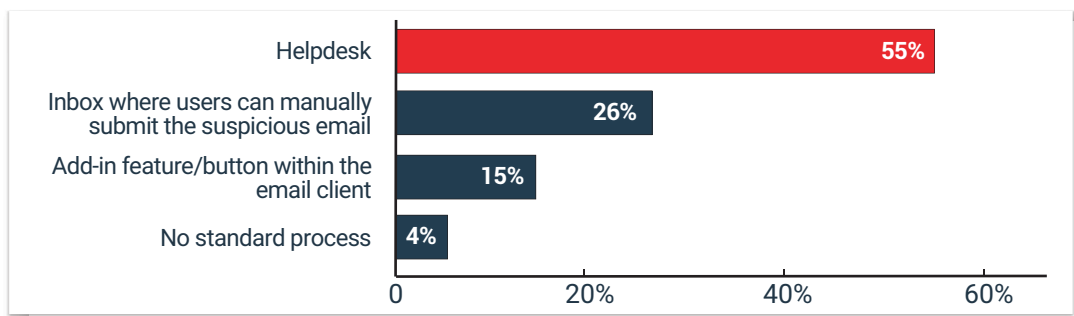


Figure 3: How do users report suspicious emails in your organization?

100% of respondents have layers of security in place.

The combinations may differ but virtually all surveyed organizations have at least one and many have more than four security solutions in place to help them combat email and phishing threats. Many companies rely on technology alone with more than 80% utilizing email filtering and anti-malware solutions.

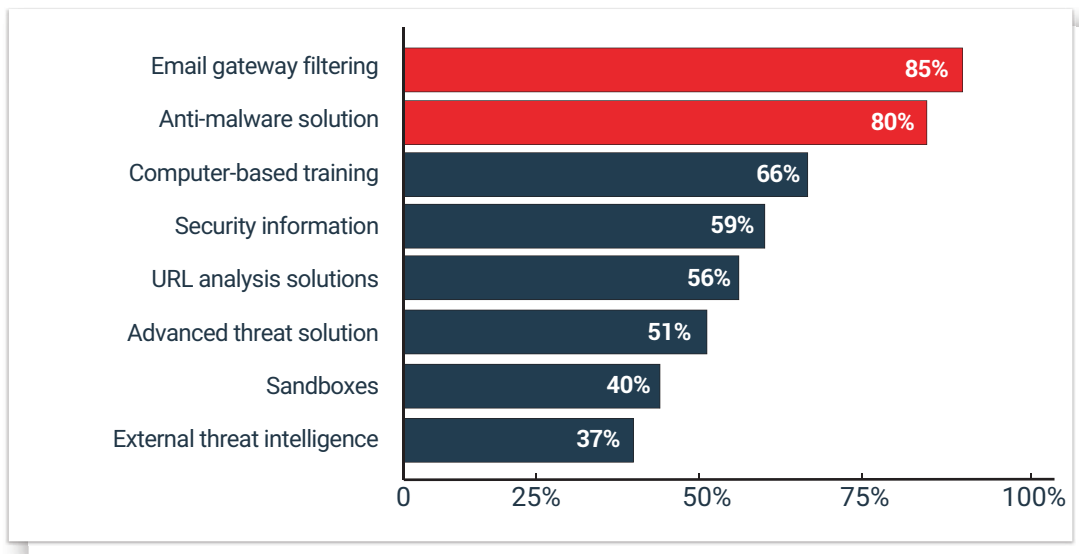


Figure 4: What type(s) of security solutions does your organization use or plan to use?

Nearly 2/3 of surveyed IT executives have dealt with a security incident originating with a deceptive email.

Even with global spending for information security products at an estimated \$81.6 billion in 2016,⁵ it's clear that no matter how good your perimeter defenses are, malicious emails will get through. Our phishing response survey shows that 65% of companies have faced an email-related security incident and almost 20% aren't sure whether an incident was caused by emails or other events.

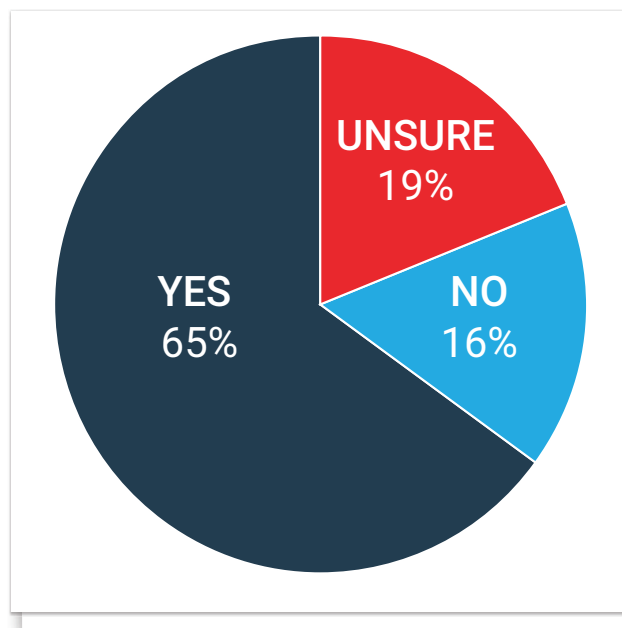


Figure 5: Has your organization ever experienced a security incident that originated with a deceptive email?

90% worry most about email-related threats: spear phishing, phishing in general or whaling.

Even with significant and strategic investments in security, most organizations are still concerned about phishing emails getting through. According to the Ponemon Institute, companies experienced an average of four ransomware attacks and paid \$2,500 per attack in 2016.⁶ And the FBI recently reported that BEC scams resulted in \$5.3 billion in actual and attempted losses last year alone.⁷ With even the most tech-savvy companies – think Google and Facebook – being swindled out of millions by phishing scams, concern over email-related threats is valid.

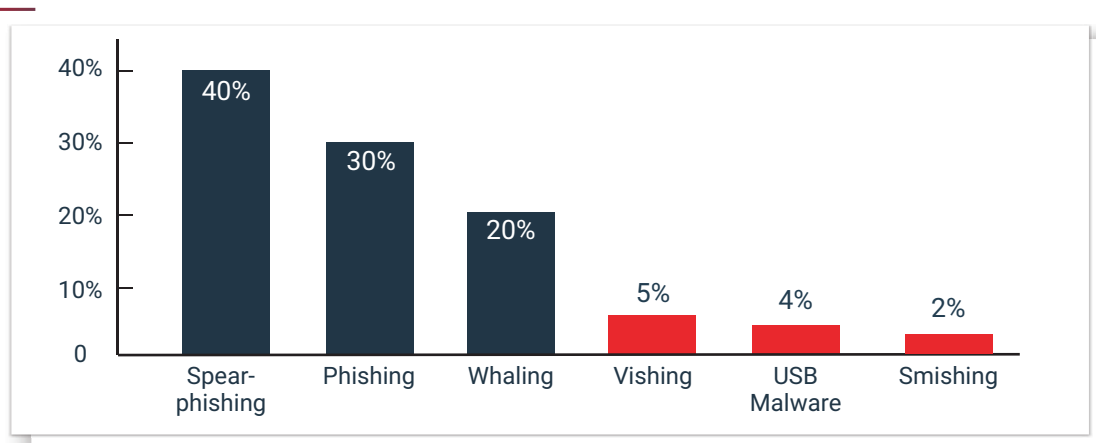


Figure 6: Which of the following security threats concerns you most?

Nearly 1/2 of respondents say their biggest challenge is too many threats and too few responders.

This isn't anything new. Hackers only need to get one threat through while IT-Security teams must block every shot on goal. When small teams of incident responders handle so many threats, it typically creates a bottleneck. It's often time-consuming to prioritize and investigate incidents and difficult to respond in an efficient and effective way.

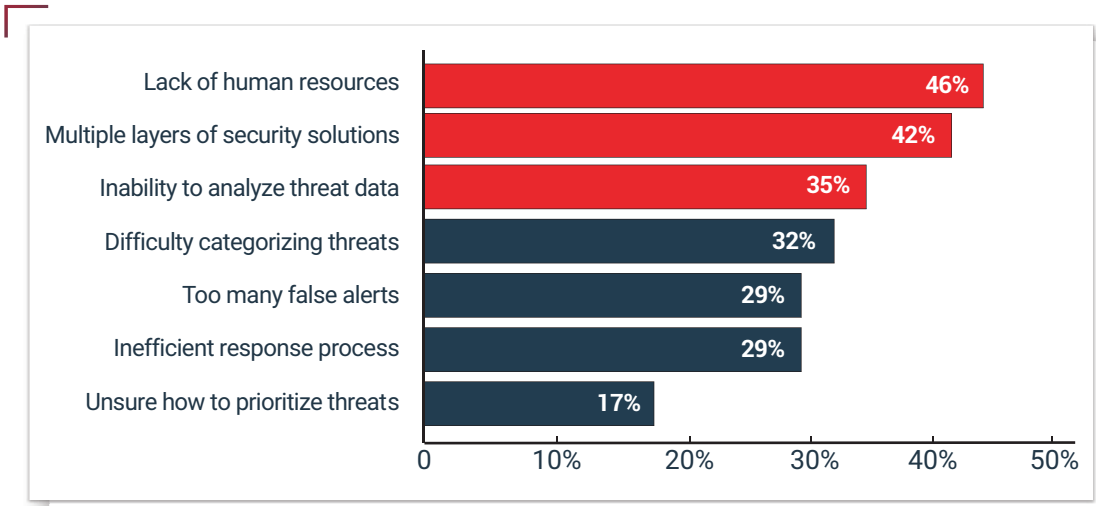
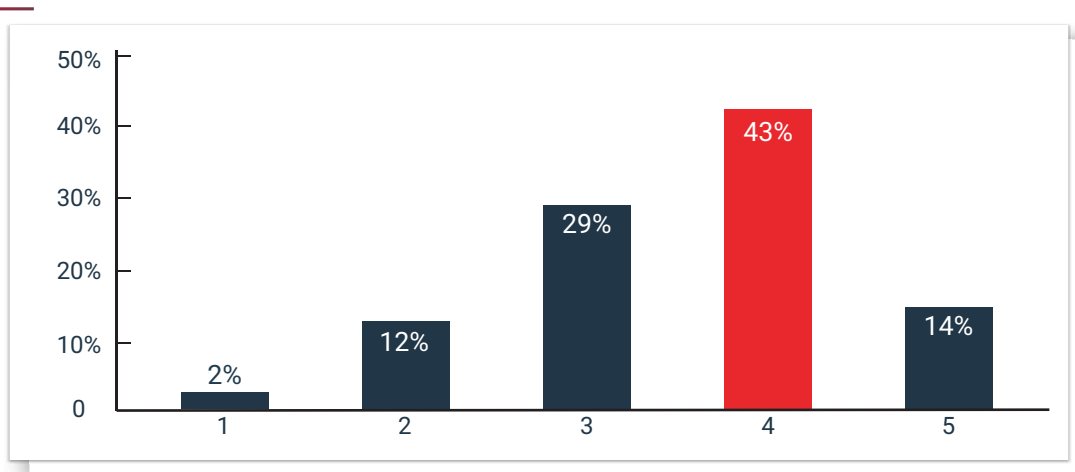



Figure 7: What challenges do you have related to managing phishing attempts?

43% of respondents say their phishing response ranged from “totally ineffective” to “mediocre.”

In other words, according to our phishing response data, over 4 in 10 companies aren't feeling too secure. With scattered technology, processes and limited resources, it's really no surprise.

Phishing response can be tough. It's not like the attacks are aimed at network resources – they target the receptionist, the CEO, the admins, etc. Too often, technology fails at the top of the phishing-detection funnel, so response is inconsistent, depending on the situation.



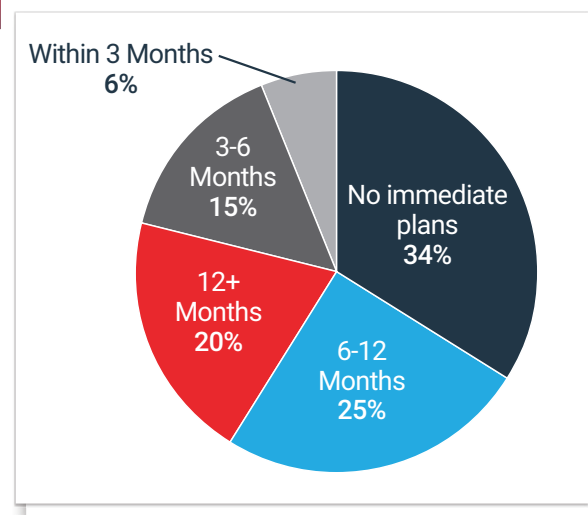
 **Figure 8:** How effective do you think your current phishing response process is?


But with the right systems, software and education, they can sleep better. At Cofense, we've seen susceptibility to phishing drills drop almost 20 percent in just a few weeks – after just one failed simulated attack and better engagement among all employees to help fight phishing.

80% of surveyed IT execs plan to upgrade their phishing prevention and response.

In Q4 2016 alone there were over 1.2 million phishing attacks.⁸ BEC attacks, delivered through spear phishing emails, target over 400 businesses a day.⁹ And ransomware attacks have spiked 250%¹⁰ to the tune of \$2,500¹¹ per attack.

As phishing email attacks become more sophisticated and dangerous, businesses know they need to keep defenses up-to-date. Most aren't waiting with plans to make upgrades within 12 months.



 **Figure 9:** When do you expect to update or augment your phishing prevention and response processes?

Automated analysis: #1 on the wish list of anti-phishing solutions.

Manually analyzing phishing emails and possible malware is difficult and time-intensive. And although many have various analysis tools, they usually don't work in concert, complicating the responder's job—while malware may be spreading throughout the organization. Automation could be the answer to eliminating the manual tasks spread across already thin resources.

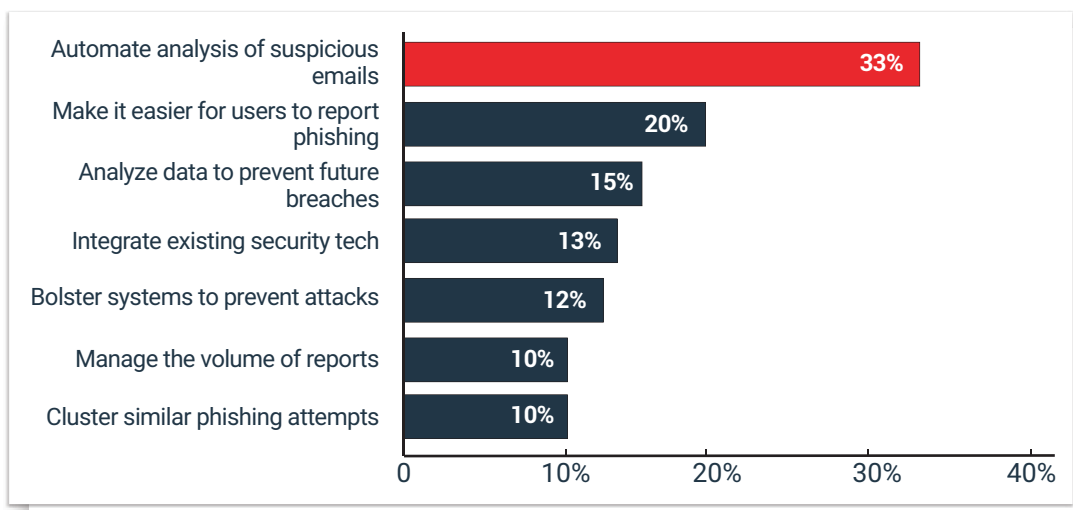


Figure 10: What do you wish you could do better regarding phishing attempts?

The Missing Link.

Investments in anti-phishing technology alone aren't doing the job. Phishing threats of all types continually reach employees, so companies need to view them as their last hope – the last line of defense.

Popular technologies like email gateway filtering and anti-malware solutions work, to a point. But trained, vigilant employees are often better at detecting attacks such as Business Email Compromise (BEC). Human-reported intelligence can be invaluable to incident responders, who, in turn, can use automation to analyze and react.

Are all employees going to “get it?” every time? Probably not. But they don't have to if the rest of the organization is ready to recognize and report suspicious emails. It only takes one to report it so the incident response team can substantially reduce the impact of phishing attacks.



CASE STUDY: What a Large Energy Utility Did...

After conditioning employees to recognize and report phishing attacks, the company saw a huge surge in malicious emails forwarded to the helpdesk. “We needed some sort of tool to handle all this volume,” said its cybersecurity engineer. The energy utility then implemented Cofense Triage, an automated phishing incident response solution to analyze reported emails, prioritize threats and let incident responders make better use of their time.¹²

| [Read More >>](#)

ABOUT Cofense

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyberattacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization-wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response and reduce the risk of compromise.

--- CITATIONS

1. Dark Reading, “91% of Cyberattacks Start with a Phishing Email,” 2016.
2. The Radicati Group, Inc., “Email Statistics Report, 2015-2019.”
3. Verizon, “2017 Data Breach Investigations Report 10th edition,” 2017.
4. Mandiant, “M-Trends 2017: A View from the Front Lines,” 2017.
5. Information Week, “Global IT Security Spending Will Top \$81 Billion in 2016,” 2016.
6. The Ponemon Institute, “The Rise of Ransomware,” January 2017.
7. FBI, “Business Email Compromise Email Account Compromise: The 5 Billion Dollar Scam,” 2017.
8. Cisco Continuum News, 2017.
9. Symantec, “2017 Internet Security Threat Report,” 2017.
10. Kaspersky Lab, “Kaspersky Lab Quarterly Malware Report: IT threat evolution Q1 2017. Statistics,” May 22, 2017.
11. APWG News, 2017.
12. Cofense, “Cofense Helps Multistate Energy Utility Defend Against Cyberthreats,” 2017.
13. Verizon, “2017 Data Breach Investigations Report 10th edition,” 2017.